Cisco UCS Central ソフトウェア ユーザ マニュアル リリース 1.2

初版：2014 年 07 月 23 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。

M シリーズのすべてのマニュアルのリストについては、で入手可能な『*Cisco UCS M-Series Servers Documentation Roadmap*』 を参照してください。

その他のマニュアル リソース

B シリーズと C シリーズのすべてのドキュメントが格納された ISO ファイルは、次の URL から入手できます。http://www.cisco.com/cisco/software/type.html?mdfid=283853163&flowid=25821 このページで、[Unified Computing System (UCS) Documentation Roadmap Bundle] をクリックします。

ISO ファイルは、ドキュメントのメジャー リリースの後に更新されます。

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、HTML ドキュメント内のフィードバック フォームよりご連絡ください mailto:ucs-docfeedback@cisco.com。 ご協力をよろしくお願いいたします。

第 1 章

Cisco UCS Central の概要

この章は、次の内容で構成されています。

Cisco UCS Central について

Cisco UCS Central は、拡大する Cisco UCS環境を対象としたスケーラブルな管理ソリューションです。 Cisco UCS Central では、標準化、グローバル ポリシー、およびグローバル ID プールによって、1 つの管理ポイントからの複数の Cisco UCS ドメインの管理が簡素化されます。 Cisco UCS Central は、1 つの UCS ドメインのポリシーに基づく管理機能である 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 では、世界中に分散する多数の個別 Cisco UCS クラシックおよびミニ管理ドメインを対象とした、グローバル レベルでの UCS ドメインの管理と監視に重点を置いています。

Cisco UCS Central では、次の機能を使用してクラシック、ミニ、または混合 Cisco UCS ドメインを個別またはグループで管理できます。

- すべての Cisco UCS コンポーネントが含まれる集中型インベントリ。インフラストラクチャ全体の明確な理解と、現行 Information Technology Infrastructure Library（ITIL）プロセスとの簡素化された統合が実現します。
- 集中型のポリシー ベース ファームウェア アップグレード。自動スケジュールに従って、またはビジネス ワークロードの要求に応じて、アップグレードを一括または選択して適用できます。
- グローバル ID プール。ID の競合を解決します。

- グローバル管理ポリシー。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します。
- 高度なデータ センター管理フレームワークとの統合を容易にするため、Cisco UCS Manager API に基づいて構築された XML API。
- 帯域幅統計情報の収集および集約。2 週間または 1 年間にわたり保存されます。
- 登録済み Cisco UCS ドメインのさまざまなエンド ポイントを管理するリモート管理

Cisco UCS Central では、API などの Cisco UCS Managerのローカル管理機能が変更または低下することはありません。 これにより、Cisco UCS Central が導入されていない場合と同様の方法でCisco UCS Managerを使用できます。また、既存のサードパーティ統合は変更せずに引き続き動作できます。

Cisco UCS Central の機能

Cisco UCS Central の管理機能の一覧と簡単な説明を次の表に示します。

機能	説明
集中型インベントリ	Cisco UCS Central は、すべての登録済み Cisco UCS コンポーネントがドメイン別に編成されたグローバル インベントリをカスタマイズ可能な更新スケジュールに基づいて自動的に作成します。また XML インターフェイスからインベントリに直接アクセスできる機能により、ITIL プロセスとの統合をさらに容易にします。
集中型障害サマリー	Cisco UCS Central では、グローバル障害サマリー パネルで、すべての Cisco UCS インフラストラクチャのステータスと、ドメインおよび障害タイプ別の障害サマリーを表示できます。 また、個々の Cisco UCS Manager ドメインを表示できるため、障害の詳細情報を確認し、問題解決にかかる時間を短縮できます。 障害をドリルダウンすると、UCS Manager がコンテキスト内で起動し、シームレスな統合エクスペリエンスが実現します。
集中型のポリシー ベース ファームウェア アップグレード	Cisco.com から Cisco UCS Central 内のファームウェア 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、業務上の要件に基づき、自動ファームウェア更新を一括または選択的に実行することをスケジュールします。 ファームウェアを一元的に管理することで、IT 標準に準拠し、ポイント アンド クリック操作でリソースの再プロビジョニングを実行できるようになります。

機能	説明
グローバル ID プール	Cisco UCS Central は、ID の競合を排除し、ソフトウェア ライセンスのポータビリティを実現します。 ユニバーサル ユーザ ID（UUID）、MAC アドレス、IP アドレス、およびワールドワイド ネーム（WWN）などのすべての ID をグローバル プールから取得する操作を一元化し、リアルタイムで ID 使用状況のサマリーを確認できます。 サーバ ID 情報の集中化により、世界中の Cisco UCS ドメイン間でのサーバ ID の移動と、新しいサーバで実行する既存のワークロードのリブートが簡単になります。
ドメイン グループ	Cisco UCS Central では、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、ポリシー管理が簡素化されます。 ドメイン グループとは、システムを地理的なグループまたは組織的なグループにまとめるために使用できる Cisco UCS ドメインの任意のグループ化方式です。 各ドメイン グループには、最大 5 つのドメイン サブグループ レベルを使用できます。 これにより、多数の Cisco UCS ドメインを管理するときにポリシー例外を管理できます。 各サブグループと親ドメイン グループとの間には階層関係があります。
グローバル管理ポリシー	Cisco UCS Central では、グローバル管理ポリシーによりコンプライアンスと従業員の効率性を確保できます。 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、装置の電力およびシステム イベント ログ（SEL）ポリシーまで、あらゆるものをインフラストラクチャで管理できます。
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により、短期間での簡素化されたインフラストラクチャの展開が可能になり、社内全体での設定の整合性が実現します。 この機能により、グローバル ベアメタル ワークロード モビリティが有効になります。これは、ハイパーバイザによって仮想ワークロード モビリティが実現したことと非常によく似ています。

機能	説明
統計情報管理	Cisco UCS Central では、Cisco UCS ドメインがどのように機能し、時間の経過に伴い動作が向上し、ワークロードの定期的なピークと変動に円滑に対応できるようになるのかを理解できます。 Cisco UCS Central GUI からレポートを設定および生成できます。 統計情報の収集を促進するため、集中型データベース スキーマはオープンであり、データに直接アクセスするか、または Cisco UCS Central ソフトウェア GUI、コマンドライン インターフェイス（CLI）、または XML API を使用してデータにアクセスすることができます。
バックアップ	Cisco UCS Central の自動バックアップ機能により、登録済み Cisco UCS ドメインと UCS Central 設定の設定情報が迅速かつ効率的にバックアップできるようになります。
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 は単一障害点が発生しないように設計されています。 Cisco UCS Central ソフトウェアのハイ アベイラビリティにより、アクティブ Cisco UCS Central が応答しない場合に自動的にフェイルオーバーするハートビートを使用するアクティブ スタンバイ モデルを使用して、Cisco UCS Central を実行できます。
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およびオーケストレーション ツールとのインターフェイスに高度な業界標準 XML API を採用しています。 Cisco UCS Central ソフトウェア向けの XML API は、Cisco UCS Manager の XML API に似ており、高度なマネージャとの統合にかかる時間を大幅に短縮します。
Remote Management	Cisco UCS Central では、登録済み Cisco UCS ドメインのさまざまなエンドポイントを 1 つの管理ポイントから管理できます。 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 Cisco UCS Central GUI または CLI から管理できます。 Cisco UCS Central から登録済み UCS ドメインのテクニカル サポート ファイルにもアクセスできます。
ポリシー/ポリシー コンポーネントおよびリソースのインポート	Cisco UCS Central には、1 つの登録済み UCS ドメインで完全なポリシー/ポリシー コンポーネントまたはリソースを柔軟に検索し、Cisco UCS Central にインポートできます。 その後、このポリシーまたはリソースを他の管理対象ドメインに展開できます。

マルチバージョン管理サポート

Cisco UCS Central リリース 1.1(2a) 以降では、複数のバージョンの Cisco UCS Manager で複数の Cisco UCS ドメインを同時に管理する機能が提供されます。 Cisco UCS Central では、ドメイン登録時に各 Cisco UCS ドメインの機能が識別されます。 この機能により、複数バージョンの Cisco UCS Manager を Cisco UCS Central とシームレスに統合し、管理とグローバル サービス プロファイルの展開を実現できます。

Cisco UCS Central を新しいリリースにアップグレードする場合は、使用している機能によっては、登録された UCS ドメインが Cisco UCS Central と互換性があることを確認するのに Cisco UCS Manager のリリース バージョンすべてをアップグレードする必要がない場合があります。

Cisco UCS ドメインを Cisco UCS Central に登録するときは、Cisco UCS Central はインベントリ情報とともにドメインから次の情報を取得します。

- Cisco UCS Manager のリリース バージョン
- ドメインの使用可能なサポート対象機能のリスト

使用可能な機能は、管理機能マトリクスとして Cisco UCS Central に送信されます。 この情報に基づいて、Cisco UCS Central は登録済みの各ドメインでサポートされる機能のリストを作成します。 Cisco UCS ドメインの機能に基づいて、Cisco UCS Central は特定のグローバル管理オプションがドメインで使用可能かどうかを決定します。 Cisco UCS Manager インスタンスの旧バージョンを含むドメインのグループ上でのグローバルサービスプロファイルの配置などの管理タスクを実行するときは、機能マトリクスに基づいて Cisco UCS Central が次の項目を実行します。

- サポートされるドメインのみへのタスクの提供。
- 機能がサポートされていないドメインに対するバージョン非互換性メッセージの表示。

Cisco UCS Manager でサポートされる機能

Cisco UCS Central CLI を使用して Cisco UCS ドメインでサポートされている機能を確認できます。 登録された Cisco UCS ドメインの Cisco UCS Manager のバージョンに基づいて、Cisco UCS Central CLI はサポートされる機能のリストを次の 4 つのカテゴリーで作成します。

- **サーバ機能マスク**：グローバル サービス プロファイル、ポリシー マッピングおよびインバンド管理、詳細ブート順を含む
- **ネットワーク機能マスク**：なし
- **ストレージ機能マスク**：FC ゾーン分割および ISCSI IPv6
- **環境機能マスク**：電源グループ、リモート操作、UCS 登録、再接続への予測影響

管理の除外

マルチバージョンのサポートでは、グローバル管理から一部の機能を除外する機能も提供されます。 登録された UCS ドメインにログインし、Cisco UCS Manager CLI から特定の機能をオフにできます。 次のグローバル管理機能を無効にできます。

- **グローバル サービス プロファイルの展開**：サーバ プールでグローバル サービス プロファイルを展開し、プール内のサーバの 1 つでグローバル サービス プロファイルの展開を無効にすると、Cisco UCS Central はグローバル サービス プロファイルの展開からサーバを除外します。
- **インバンド管理**：インバンド管理機能を有するサービスプロファイルは、インバンド管理機能を除外したサーバには展開されません。
- **ポリシー マッピング**：この Cisco UCS ドメインから Cisco UCS Central へのポリシーまたはポリシー コンポーネントのインポートを無効にします。
- **リモート管理**：Cisco UCS Central からの Cisco UCS ドメイン内の物理デバイスの制御を制限します。

いつでも Cisco UCS Manager CLI を使用してこれらの機能を有効にして、登録された Cisco UCS ドメインのグローバル管理機能をいつでも復元できます。

機能サポート マトリクス

次の表は、Cisco UCS Central の機能と、その機能がサポートされる Cisco UCS Manager のリリースバージョンのリストです。

Cisco UCS Central の機能	サポートされる Cisco UCS Central のバージョン	サポートされる Cisco UCS Manager のバージョン			
		2.1(2a)/2.1(3x)	2.2(1x)	2.2(2x)/2.2(3x)	3.0(1x)
マルチバージョン管理サポートとサポートされる Cisco UCS Manager の機能の表示	1.1(2a)	No	Yes	Yes	Yes
ポリシー/ポリシーコンポーネントおよびリソースのインポート		No	Yes	Yes	Yes
バックアップ イメージファイル用のリモートロケーションの指定		No	No	Yes	Yes
サードパーティ証明書		No	No	Yes	Yes
IPv6 インバンド管理サポート		No	No	Yes	Yes
再接続への予測影響	1.2(1a)	No	No	Yes （注） 2.2(3x) 以降でのみサポート	Yes
高精度のブート順制御		No	Yes	Yes	Yes

（注）

- ポリシー/ポリシー コンポーネントまたはリソースの検索は、Cisco UCS Manager リリース 2.1(2x) および 2.1(3x) でサポートされています。 ポリシーをインポートするには、Cisco UCS Manager リリース 2.2(1b) 以降が必要です。
- Precision Boot Order Control については、ブレード サーバが CIMC バージョン 2.2(1b) 以降でなければなりません。

Cisco UCS Central GUI の概要

Cisco UCS Central GUI は、Cisco UCS Central にグラフィカル インターフェイスを提供します。『*Release Notes for Cisco UCS Central*』の「*System Requirements*」セクションに記載されている要件を満たす任意のコンピュータから GUI にアクセスできます。

Cisco UCS Central GUI には、次の領域とペインがあります。

- トップ レベルのサマリー パネルには、[UCS Central Fault Summary]、[UCS Domains Fault Summary]、および [Pending Activities] の概要が表示されます。
- Cisco UCS Central の情報の主なカテゴリにアクセスできるウィンドウの上部全体にわたるメニュー バー。
- 各メニュー カテゴリの下で入手できる情報の展開可能なツリー表示を提供する左側の [Navigation] ペイン。
- [Navigation] ペインで選択されたノードに関連付けられたタブを表示する、右側の **[Work]** ペイン。

メニュー バーには、次のものが含まれています。

- [Domains]：Cisco UCS Central ドメイン グループ、ドメイン グループ ポリシー、登録済み Cisco UCS ドメイン、および Cisco UCS ドメインの障害サマリーにアクセスできます。
- [Servers]：グローバル サービス プロファイルとポリシーを作成するオプションが提供され、登録済み Cisco UCS ドメインで設定されたサービス プロファイルおよびサービス プロファイル テンプレートと、Cisco UCS Central で設定されたグローバル UUID 接尾辞プールにアクセスできます。
- [Network]：Cisco UCS Central で設定されたグローバル ネットワーク ポリシー、共通 VLAN、IP プール、および MAC プールにアクセスできます。
- [Storage]：Cisco UCS Central で設定されたグローバル ストレージ ポリシー、ファブリック固有の VSAN、グローバル IQN プール、および WWN プールにアクセスできます。
- [Operations Management]：登録済み Cisco UCS ドメインの設定とグローバル設定を管理できます。
  - ファームウェア イメージ

- バックアップ ファイルとインポート ファイル
- 通信プロトコル、SNMP、Call Home、リモート ユーザ認証、電力割り当て、およびエラーロギングなど、バックアップおよびエクスポート、ファームウェア管理、メンテナンス、および操作機能のドメイン グループ レベル ポリシー。

- [Statistics]：ネットワーク、冷却、温度、および電力に関するレポートを生成するオプションが提供されます。 標準レポートとカスタム レポートを作成できます。
- [Logs and Faults]：監査ログ、イベント ログ、およびエラーを表示できます。
- [Administration]：Cisco UCS Central 管理設定を管理できます。 Cisco UCS Central でのすべてのコントローラ、プロバイダー、およびクライアントのレジストリ、および診断情報（テクニカル サポート ファイル、監査ログ、イベント ログ、エラーなど）。
- [Import]：ポリシー/ポリシー コンポーネントとリソースを登録済み Cisco UCS ドメインから Cisco UCS Central にインポートできます。

HTTP を使用した Cisco UCS Central GUI へのログイン

Cisco UCS Central GUI のデフォルトの HTTP Web リンクは、`http://UCSCentral_IP` です。ここで *`UCSCentral_IP`* は、Cisco UCS Central に割り当てられている IP アドレスを表します。

手順

ステップ 1 Web ブラウザで、Cisco UCS Central GUI の Web リンクを入力するか、ブラウザでブックマークを選択します。

ステップ 2 起動ページで、次の手順を行います。

a) ユーザ名とパスワードを入力します。

b) [Log In] をクリックします。

HTTPS を使用した Cisco UCS Central GUI へのログイン

Cisco UCS Central GUI のデフォルトの HTTPS Web リンクは、`https://UCSCentral_IP` です。ここで *`UCSCentral_IP`* は、Cisco UCS Central に割り当てられている IP アドレスを表します。

手順

ステップ 1 Web ブラウザで、Cisco UCS Central GUI の Web リンクを入力するか、ブラウザでブックマークを選択します。

ステップ 2 起動ページで、次の手順を行います。

a) ユーザ名とパスワードを入力します。
b) [Log In] をクリックします。

Cisco UCS Central GUI からのログアウト

手順

Cisco UCS Central GUI で、右上にある [Log Out] をクリックします。
Cisco UCS Central GUI からただちにログアウトされ、ブラウザの起動ページに戻ります。

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。

Cisco UCS Central でのライセンスの管理

各登録済み Cisco UCS ドメインのドメイン ライセンスにより、Cisco UCS Central からドメインを管理できるようになります。 Cisco UCS Central GUI と CLI の両方を使用して Cisco UCS ドメインのライセンスを管理できます。

猶予期間

初めて Cisco UCS Central を使用する場合、最長 120 日間の猶予期間にわたり、最大 5 つの Cisco UCS ドメインを無料で登録できます。 5 つ目のドメインの登録後に新たなドメインを登録する場合、新しい登録済みドメインごとに猶予期間（120 日）が開始されます。 猶予期間が終了すると、Cisco UCS Centralを使用してドメインを管理するには、アクティブなドメイン ライセンスが必要となります。 猶予期間は Cisco UCS ドメイン の登録日から、ライセンスを取得してインストールする日までです。

登録済み Cisco UCS ドメインの猶予期間の使用状況は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、ドメインを無料で登録し、猶予期間が 40 日間の場合に、40 日間の猶予期間が経過した後に登録を解除すると、そのドメインについて 40 日間が記録されます。 この Cisco UCS ドメインを再び登録すると、ドメインの猶予期間が再開され、40 日間が既に使用されてい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。 猶予期間の終了前にライセンスを取得しないと、ライセンス取得を促す通知として複数のエラーが生成されます。

License Types

次の 2 種類のライセンスが使用可能です。

- **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完了後に、システムから初期ライセンスを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初期ライセンスインストール ステータスに影響しないため、削除できます。
- **ドメイン ライセンス**：Cisco UCS Central に登録する予定のドメインが 6 つ以上の場合は、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 ドメインの登録時にドメインを選択し、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

シスコの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 1 つ以上が該当しない場合は、ライセンスを入手する方法についてシスコ担当者に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 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 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。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで [License Management] をクリックします。

ステップ 3 [Work] ペインで [License] タブを選択します。

ステップ 4 [UCS Central Details] 領域で [GUID] をクリックし、GUID をクリップボードにコピーします。

GUID は、ライセンスを取得する Cisco UCS Central インスタンスに固有です。

ステップ 5 [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 6 ライセンス管理ポータルにログインし、[Continue to Product License Registration] をクリックします。

ステップ 7 [Quickstart] ページの [Enter a Single PAK or Token to fulfill] フィールドに PAK を入力し、[Fulfill Single PAK/Token] をクリックします。

ステップ 8 [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 9 GUID を [GUID] フィールドに入力し、[Assign] をクリックします。

ステップ 10 [Next] をクリックします。

ステップ 11 [Review] ページで、電子メール アドレスを入力し、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 12 [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信されます。 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 ファイルを取得したら、ライセンス コードを不正に変更してはなりません。手動で編集すると改竄防止が解除され、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、Cisco UCS Central GUI を使用してライセンスをシステムにダウンロードします。

ローカル ファイル システムからのライセンスのダウンロード

はじめる前に

ローカル ファイル システムから Cisco UCS Central にライセンスをダウンロードするには、次の作業を行っており、次の権限があることを確認します。

- シスコからライセンスを取得し、ローカル システムに保存している。
- このタスクを実行するための Cisco UCS Central の管理権限。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで [License Management] をクリックします。

ステップ 3 [Work] ペインで [Licenses] タブをクリックします。

ステップ 4 [Licenses] タブで [Download] をクリックします。

ステップ 5 [Filename] ダイアログボックスで、ライセンスのフル パスと名前を入力します。
ライセンスが含まれているフォルダの正確なパスがわからない場合は、[Choose File] をクリックしてファイルの場所にナビゲートし、ファイルを選択します。

ステップ 6 [OK] をクリックします。
Cisco UCS Central によりライセンスのダウンロードが開始されます。 [Download Tasks] タブで、ダウンロードのステータスをモニタできます。

リモート ファイル システムからのライセンスのダウンロード

はじめる前に

リモート ロケーションから Cisco UCS Central にライセンスをダウンロードするには、次の作業が済んでおり、次の情報と権限があることを確認します。

- シスコからライセンスを入手し、ダウンロード元のリモート ロケーションに保存している。FTP、SCP、または SFTP サーバの場合、アクセス認証に使用するユーザ名とパスワード。
- このタスクを実行するための Cisco UCS Central の管理権限。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで [License Management] をクリックします。

ステップ 3 [Work] ペインで [Licenses] タブをクリックします。

ステップ 4 [Licenses] タブで [Download] をクリックします。

ステップ 5 [Download License] ダイアログボックスで、[Remote File System] オプション ボタンをクリックします。

ステップ 6 リモート サーバとの通信に使用するプロトコルを選択します。
次のいずれかのプロトコルを選択できます。

- FTP

- TFTP
- SCP
- SFTP

ステップ 7 [Server] フィールドに、ライセンス ファイルが存在するサーバの IP アドレスまたはホスト名を入力します。

ステップ 8 [License File Name] フィールドに、ダウンロードするライセンス ファイルの名前を入力します。

ステップ 9 必要に応じて、[Path] フィールドにリモート サーバのライセンス ファイルの絶対パスを入力します。
SCP を使用する場合、絶対パスは常に必要です。 他のプロトコルを使用する場合は、ファイルがデフォルトのダウンロードフォルダにあれば、リモートパスを指定する必要はありません。 ファイル サーバの設定方法の詳細については、システム管理者に問い合わせてください。

ステップ 10 [User Name] フィールドに、リモート サーバにログインするためのユーザ名を入力します。
[TFTP] を選択した場合は、このフィールドは適用されません。

ステップ 11 [Password] フィールドに、リモート サーバ ユーザ名のパスワードを入力します。
[TFTP] を選択した場合は、このフィールドは適用されません。

ステップ 12 [OK] をクリックします。
Cisco UCS Central によりライセンスのダウンロードが開始されます。 [Download Tasks] タブで、ダウンロードのステータスをモニタできます。

ライセンスのインストール

ライセンスが Cisco UCS Central にダウンロードされていることを確認します。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで [License Management] をクリックします。

ステップ 3 [Work] ペインで [Licenses] タブをクリックします。
ここではダウンロードされたすべてのライセンスのリストを確認できます。 [Overall License Status] カラムのステータスが [Validated] のライセンスを確認します。 これらは、インストール可能です。

ステップ 4 インストールするライセンスを選択して、[Install] をクリックします。
[Overall License Status] カラムに、インストールのステータスが表示されます。 インストールを開始すると、このカラムのステータスが [Install-pending] になります。 ライセンスのインストール後には、ステータスが [Installed] に変更されます。

ライセンスの削除

登録済み UCS ドメインに関連付けられていないライセンスを Cisco UCS Central から削除できます。 UCS ドメインに関連付けられているライセンスを削除する場合は、ライセンスを削除する前に、ドメインを登録解除してください。 ライセンスを削除すると、システムは使用可能なライセンス数を自動的に調整します。

重要 ライセンスを Cisco UCS Central から削除すると、システムからライセンス ファイルだけが削除されます。 システムからライセンスを削除した後で、同じライセンスをダウンロードしようとすると、ライセンス ダウンロード エラーが発生することがあります。 したがってライセンスを削除する場合は、そのライセンスの関連ダウンロード タスクも削除する必要があります。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで [License Management] をクリックします。

ステップ 3 [Work] ペインで [Licenses] タブをクリックします。

ステップ 4 アンインストールするライセンスを選択します。

ステップ 5 [Delete] をクリックします。

ステップ 6 確認ダイアログボックスで [Yes] をクリックします。
ライセンス ファイルが Cisco UCS Central から削除されます。

次の作業

このライセンスの [Operations Management] > [License Management] > [Download Tasks] タブから関連するライセンス ダウンロード タスクを削除します。 これにより、システムからこのライセンスの関連インスタンスがすべて削除されます。

第 3 章

管理設定の管理

この章は、次の内容で構成されています。

Cisco UCS Central の管理設定

Cisco UCS Central では、GUI の [Administration] タブからポリシーおよびユーザ認証をネイティブに設定できます。これは、[Operations Management] タブから UCS ドメインに対して定義されているタスクと似ています。 この 2 つのタブではほとんどの機能が共通していますが、ユーザ ロールとサーバ サポートが異なります。

[Administration] タブの次の領域で管理タスクを実行できます。

- [General Settings]
- [Users and Authentication]

ユーザと認証

Cisco UCS Central では、システムにアクセスするローカル ユーザとリモート ユーザの作成がサポートされています。 各 Cisco UCS Central ドメインでは最大 128 のユーザ アカウントを設定できます。 各ユーザには固有のユーザ名とパスワードが必要です。 詳細については、User Management,（79 ページ）を参照してください。

Cisco UCS Central では、ネイティブ認証に LDAP を使用しますが、このリリースでは RADIUS および TACACS+ 認証は除外されています。 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。 詳細については、管理設定の管理,（17 ページ）を参照してください。

ローカル認証されたユーザの作成

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。

ステップ 2 [Navigation] ペインで [Users and Authentication] をクリックします。

ステップ 3 [Work] ペインで [Local Users] をクリックします。

ステップ 4 [Actions] 領域で、[Create Locally Authenticated Users] をクリックし、すべてのフィールドに入力します。

ステップ 5 [Roles/Locales] タブをクリックしてロールまたはロケールのタイプを割り当て、[SSH] タブをクリックしてセキュリティ キーのタイプを割り当てます。

ステップ 6 [OK] をクリックします。

ステップ 7 [Save] をクリックします。

リモート ユーザの作成

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。

ステップ 2 [Navigation] ペインで [Users and Authentication] をクリックします。

ステップ 3 [Work] ペインで [Remote Users] をクリックします。

ステップ 4 [Actions] 領域で、[Create Remote Users] をクリックし、すべてのフィールドに入力します。

ステップ 5 [Roles/Locales] タブをクリックしてロールまたはロケールのタイプを割り当て、[SSH] タブをクリックしてセキュリティ キーのタイプを割り当てます。

ステップ 6 [OK] をクリックします。

ステップ 7 [Save] をクリックします。

ユーザ ロールの作成

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。

ステップ 2 [Navigation] ペインで [Users and Authentication] をクリックします。

ステップ 3 [Work] ペインで [Roles] をクリックします。

ステップ 4 [Actions] 領域で、[Create Role] をクリックし、すべてのフィールドに入力します。

ステップ 5 [OK] をクリックします。

ステップ 6 [Save] をクリックします。

ユーザ ロケールの作成

はじめる前に

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。

ステップ 2 [Navigation] ペインで [Users and Authentication] をクリックします。

ステップ 3 [Work] ペインで [Locales] をクリックします。

ステップ 4 [Actions] 領域で、[Create Locales] をクリックし、すべてのフィールドに入力します。

ステップ 5 [Assign/Unassign Organization] または [Assign/Unassign Domain Group] あるいはこの両方をクリックし、組織またはドメイン グループを、Cisco UCS Central で選択されたロケールに割り当てるか、または割り当て解除します。

ステップ 6 [OK] をクリックします。

ステップ 7 [Save] をクリックします。

認証ドメインの作成

Cisco UCS Central では、ネイティブ認証に LDAP を使用しますが、このリリースでは RADIUS および TACACS+ 認証は除外されています。 ただし RADIUS、TACACS+、または LDAP リモート認証は、Cisco UCS Central ドメイン グループ ルートから Cisco UCS ドメインでサポートされています。

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。
ステップ 2 [Navigation] ペインで [Users and Authentication] をクリックします。
ステップ 3 [Work] ペインで [Authentication Domains] をクリックします。
ステップ 4 [Actions] 領域で、[Create Authentication Domain] をクリックし、すべてのフィールドに入力します。
ステップ 5 [OK] をクリックします。
ステップ 6 [Save] をクリックします。

LDAP プロバイダーの作成

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。
ステップ 2 [Navigation] ペインで [Users and Authentication] をクリックします。
ステップ 3 [Work] ペインで [LDAP] をクリックします。
ステップ 4 [Providers] をクリックします。
ステップ 5 [Actions] 領域で、[Create LDAP Provider] をクリックし、すべてのフィールドに入力します。
ステップ 6 [OK] をクリックします。
ステップ 7 [Save] をクリックします。

LDAP プロバイダー グループの作成

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。
ステップ 2 [Navigation] ペインで [Users and Authentication] をクリックします。
ステップ 3 [Work] ペインで [LDAP] をクリックします。
ステップ 4 [Provider Groups] をクリックします。
ステップ 5 [Actions] 領域で、[Create LDAP Provider Group] をクリックし、すべてのフィールドに入力します。
ステップ 6 [OK] をクリックします。
ステップ 7 [Save] をクリックします。

LDAP グループ マップの作成

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。
ステップ 2 [Navigation] ペインで [Users and Authentication] をクリックします。
ステップ 3 [Work] ペインで [LDAP] をクリックします。
ステップ 4 [Group Maps] をクリックします。
ステップ 5 [Actions] 領域で、[Create LDAP Group Map] をクリックし、すべてのフィールドに入力します。
ステップ 6 [OK] をクリックします。
ステップ 7 [Save] をクリックします。

LDAP プロバイダーの削除

はじめる前に

LDAP プロバイダーを作成する必要があります。

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。
ステップ 2 [Navigation] ペインで [Users and Authentication] をクリックします。
ステップ 3 [Work] ペインで [LDAP] をクリックします。
ステップ 4 [LDAP Providers] をクリックします。
ステップ 5 [Actions] 領域で削除する LDAP プロバイダーを右クリックし、[Delete LDAP Provider] をクリックします。
ステップ 6 [Save] をクリックします。

LDAP プロバイダー グループの削除

はじめる前に

LDAP プロバイダー グループを作成する必要があります。

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。

ステップ 2 [Navigation] ペインで [Users and Authentication] をクリックします。

ステップ 3 [Work] ペインで [LDAP] をクリックします。

ステップ 4 [Provider Groups] をクリックします。

ステップ 5 [Actions] 領域で削除するプロバイダー グループを右クリックし、[Delete LDAP Provider Group] をクリックします。

ステップ 6 [Save] をクリックします。

LDAP グループ マップの削除

はじめる前に

LDAP グループ マップを作成する必要があります。

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。

ステップ 2 [Navigation] ペインで [Users and Authentication] をクリックします。

ステップ 3 [Work] ペインで [LDAP] をクリックします。

ステップ 4 [Group Maps] をクリックします。

ステップ 5 [Actions] 領域で削除する LDAP マップを右クリックし、[Delete LDAP Group Map] をクリックします。

ステップ 6 [Save] をクリックします。

General Settings

Cisco UCS Central GUI でポリシーを設定できます。 これらの管理ポリシーは組織レベルで定義され、インフラストラクチャのあらゆる項目（日付と時刻、SNMP トラップ、バックアップ ポリシーとエクスポート ポリシーなど）を管理できます。

SNMP トラップの作成

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。

ステップ 2 [Navigation] ペインで [General] をクリックします。

ステップ 3 [Work] ペインで、[SNMP] をクリックします。

ステップ 4 [Properties] 領域で、[enabled] オプション ボタンをオンにします。
デフォルトでは、[Admin State] は無効です。 手動で有効に変更する必要があります。

ステップ 5 [Actions] 領域で、[Create SNMP Trap] をクリックし、すべてのフィールドに入力します。

ステップ 6 [OK] をクリックします。

ステップ 7 [Save] をクリックします。

次の作業

SNMP ユーザを作成する。

SNMP ユーザの作成

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。

ステップ 2 [Navigation] ペインで [General] をクリックします。

ステップ 3 [Work] ペインで、[SNMP] をクリックします。

ステップ 4 [Actions] 領域で、[Create SNMP User] をクリックし、すべてのフィールドに入力します。

ステップ 5 [OK] をクリックします。

ステップ 6 [Save] をクリックします。

HTTPS 証明書の設定

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。

ステップ 2 [Navigation] ペインで [General] をクリックします。

ステップ 3 [Work] ペインで [HTTPS] をクリックします。

ステップ 4 [Actions] 領域で、[Key Ring] ドロップダウン リストからサードパーティのキー リングを選択します。

ステップ 5 [Save] をクリックします。

NTP サーバの設定

Cisco UCS Central では、国際タイム ゾーンと定義された NTP サーバに基づいてグローバル日時ポリシーがサポートされます。

はじめる前に

Cisco UCS Central の NTP サーバを設定するには、まず日時ポリシーを作成する必要があります。

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。

ステップ 2 [Navigation] ペインで [General] をクリックします。

ステップ 3 [Work] ペインで、[Date/Time] をクリックし、[Time Zone] ドロップダウン リストからタイム ゾーンを選択します。

ステップ 4 [Actions] 領域で、[Add NTP Server] をクリックします。

ステップ 5 [OK] をクリックします。

ステップ 6 [Save] をクリックします。

DNS サーバの設定

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。
ステップ 2 [Navigation] ペインで [General] をクリックします。
ステップ 3 [Work] ペインで、[DNS] をクリックします。
ステップ 4 [Actions] 領域で、[Add DNS Server] をクリックし、すべてのフィールドに入力します。
ステップ 5 [OK] をクリックします。
ステップ 6 [Save] をクリックします。

障害ポリシーの設定

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。
ステップ 2 [Navigation] ペインで [General] をクリックします。
ステップ 3 [Work] ペインで [Fault Policy] をクリックします。
ステップ 4 [Actions] 領域で、すべてのフィールドに入力します。
ステップ 5 [Save] をクリックします。

次の作業

エクスポート ポリシーの設定

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。
ステップ 2 [Navigation] ペインで [General] をクリックします。
ステップ 3 [Work] ペインで [TFTP Core Export Policy] をクリックします。
ステップ 4 [Actions] 領域で、すべてのフィールドに入力します。
ステップ 5 [Save] をクリックします。

IPv6 Configuration

Cisco UCS Central では、スタンドアロン モードとハイ アベイラビリティ（HA）モードで IPv6 を有効にできます。 1 つの仮想マシン上で設定された Cisco UCS Central はスタンドアロン セットアップです。 スタンドアロンセットアップはどのクラスタにも属しません。 UCS Central HA セットアップは、2 つの仮想マシン（プライマリ ノードとセカンダリ ノード）で構成されます。

これらの仮想マシンが HA クラスタを構成し、この HA クラスタへは共通 IP アドレスを使用してアクセスできます。 この IP アドレスは、クラスタ IP アドレスまたは仮想 IP アドレスと呼ばれます。 仮想 IP アドレス（VIP）には、IPv4 アドレスの他に IPv6 アドレスを割り当てることができます。

スタンドアロン モードでの IPv6 設定

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。

ステップ 2 [Navigation] ペインで、[General] を選択します。
デフォルトでは、[General] タブにより [Work] ペインにタブが表示されます。

ステップ 3 [Management Interface] タブの [Node A] 領域で [IPv6] タブをクリックし、すべての必須フィールドに入力します。

ステップ 4 [Save] をクリックします。

HA モードでの IPv6 の設定

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。

ステップ 2 [Navigation] ペインで、[General] を選択します。
デフォルトでは [General] タブにより [Work] ペインにタブが表示されます。

ステップ 3 [Management Interface] タブのノード A およびノード B 領域で [IPv6] タブをクリックし、すべての必須フィールドに入力します。

ステップ 4 [Save] をクリックします。

ステップ 5 [Nodes] の上のメイン エリアで、仮想 IPv6 アドレス情報を追加します。

ステップ 6 [Save] をクリックします。

キー リング

Cisco UCS Central では、より強力な認証のためにキー リングをサードパーティの証明書として作成できます。 HTTPS は 2 つのデバイス間でセキュアな通信を確立するために Public Key Infrastructure（PKI）コンポーネントを使用します。

各 PKI デバイスは、内部キー リングに非対称の Rivest-Shamir-Adleman（RSA）暗号キーのペア（1 つはプライベート、もう 1 つはパブリック）を保持します。 いずれかのキーで暗号化されたメッセージは、もう一方のキーで復号化できます。 暗号化されたメッセージを送信する場合、送信者は受信者の公開キーで暗号化し、受信者は独自の秘密キーを使用してメッセージを復号化します。 送信者は、独自の秘密キーで既知のメッセージを暗号化（「署名」とも呼ばれます）して公開キーの所有者を証明することもできます。 受信者が該当する公開キーを使用してメッセージを正常に復号化できる場合は、送信者が対応する秘密キーを所有していることが証明されます。 暗号キーの長さはさまざまであり、通常の長さは 2048 ビット ～ 4096 ビットです。 一般的に、短いキーよりも長いキーの方がセキュアになります。 Cisco UCS Central では、最初に 2048 ビットのキー ペアを含むデフォルトのキー リングが提供されます。そして、追加のキー リングを作成できます。

クラスタ名が変更されたり、証明書が期限切れになったりした場合は、デフォルトのキー リング証明書を手動で再生成する必要があります。

（注） Cisco UCS Central は、UCS Central から UCS Manager への通信と、UCS Central とユーザの Web ブラウザ間の通信の両方に、同一のサードパーティ証明書を使用します。 現時点では、UCS Central では 2 種類の通信での異なる証明書の使用はサポートされていません。 現在、サードパーティ証明書は Cisco UCS Manager リリース 2.2(2c) 以降でのみサポートされます。

（注） キー リングと証明書要求を作成すると、Cisco UCS Central により証明書署名機能を使用した証明書要求が生成されます。 CA サーバによる署名後の証明書要求には、キーの用途の 1 つが「証明書署名」として設定されている必要があります。 Microsoft Windows を Internal Enterprise Certification Authority Server として使用する場合は、[Subordinate Certification Authority] テンプレートを使用して証明書を生成する必要があります。 ただしスタンドアロン CA サーバを使用する場合は、証明書テンプレートを選択する必要はありません。

キー リングの作成

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。
ステップ 2 [Navigation] ペインで [Users and Authentication] をクリックします。
ステップ 3 [Work] ペインで [Certificates] をクリックします。
ステップ 4 [Actions] 領域で、[Create Key Ring] をクリックし、すべてのフィールドに入力します。
ステップ 5 [Certificate Request Actions] 領域で、[Create] をクリックし、すべてのフィールドに入力します。
ステップ 6 [OK] をクリックします。
ステップ 7 [Save] をクリックします。

トラスト ポイントの作成

Cisco UCS Central では、ルート認証局（CA）および従属 CA の証明書がバンドル形式で含まれているトラスト ポイントを作成できます。 ルート CA にはプライマリ証明書と自己署名証明書が含まれている必要があります。

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。
ステップ 2 [Navigation] ペインで [Users and Authentication] をクリックします。
ステップ 3 [Work] ペインで [Certificates] をクリックします。
ステップ 4 [Actions] 領域で、[Create Trusted Point] をクリックし、すべてのフィールドに入力します。
ステップ 5 [OK] をクリックします。
ステップ 6 [Save] をクリックします。

キーリングの削除

はじめる前に

HTTPS がキー リングを使用していないことを確認します。

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。

ステップ 2 [Navigation] ペインで [Users and Authentication] をクリックします。

ステップ 3 [Work] ペインで [Certificates] をクリックします。

ステップ 4 [KeyRings Actions] 領域で、削除するキー リングを右クリックし、[Delete] を選択します。

ステップ 5 確認ダイアログボックスで [Yes] をクリックします。
キー リングが Cisco UCS Central から削除されます。

トラスト ポイントの削除

はじめる前に

トラスト ポイントが使用されていないことを確認します。

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。

ステップ 2 [Navigation] ペインで [Users and Authentication] をクリックします。

ステップ 3 [Work] ペインで [Certificates] をクリックします。

ステップ 4 [KeyRings Actions] 領域で、削除するトラスト ポイントを右クリックし、[Delete] を選択します。

ステップ 5 確認ダイアログボックスで [Yes] をクリックします。
トラスト ポイントが Cisco UCS Central から削除されます。

ブラウザへの CA 証明書のインポート

インターネット ブラウザで Cisco UCS Central アプリケーションを初めて実行するときに、信頼できない Web サイトであるか、または Web サイトの証明書の発行元が信頼できないことを示すエラーが表示されることがあります。 このような場合、ルート CA と従属 CA（存在する場合）の証明書をブラウザにインポートする必要があります。 さまざまなブラウザでこの機能がサポートされています。 証明書をインポートするには、次の手順を実行します。

Mozilla Firefox

手順

ステップ 1 [Menu] バーで [Tools] > [Options] [Advanced] > [Certificates] をクリックします。

ステップ 2 [View Certificate] をクリックします。

ステップ 3 [Authorities] をクリックします。

ステップ 4 [Import] をクリックします。

ステップ 5 コンピュータに保存されている CA 証明書を選択して開きます。
[Downloading Certificate] ポップアップ ウィンドウが開きます。

ステップ 6 [Trust this CA to identify Websites] チェックボックスをオンにします。

ステップ 7 [OK] をクリックします。

Microsoft Internet Explorer

手順

ステップ 1 [Menu] バーで [Tools] > [Internet Options] [Content] > [Certificates] をクリックします。

ステップ 2 [Trusted Root Certification Authorities] をクリックします。

ステップ 3 [Import] をクリックします。
[Certificate Import Wizard] ポップアップ ウィンドウが開きます。

ステップ 4 コンピュータに保存されている CA 証明書を選択するまで、ウィザードの手順に従います。

ステップ 5 [Finish] をクリックします。

Google Chrome

手順

ステップ 1 [URL address] バーの右側で [Settings] を選択します。

ステップ 2 [HTTPS/SSL] セクションで [Manage Certificates] をクリックします。

ステップ 3 [Trusted Root Certification Authorities] をクリックします。

ステップ 4 [Import] をクリックします。
[Certificate Import Wizard] ポップアップ ウィンドウが開きます。

ステップ 5 コンピュータに保存されている CA 証明書を選択するまで、ウィザードの手順に従います。

ステップ 6 [Finish] をクリックします。

Cisco UCS ドメインの管理設定

リモート アクセス ポリシー

Cisco UCS Central は、インターフェイス モニタリング ポリシーを定義し、SSH 設定ステータスを表示し、HTTP、Telnet、Web セッション制限、および CIM XML のポリシー設定を提供するグローバル リモート アクセス ポリシーをサポートしています。

HTTP の設定

HTTP リモート アクセス ポリシーの設定

はじめる前に

ドメイン グループ下で HTTP リモート アクセス ポリシーを設定する前に、最初にこのポリシーを作成する必要があります。 ドメイン グループ ルート下にあるポリシーは、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

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 5 [Work] ペインで、[Remote Access] をクリックします。

ステップ 6 [Work] ペインで、[HTTP] タブをクリックします。

ステップ 7 [Actions] 領域で、[Create] をクリックし、該当するすべてのフィールドに入力します。
[Domain Group root] ノード下の [Operational Policies] では、[Create] をクリックして該当するすべてのフィールドに入力する必要はありません。

ステップ 8 [Save] をクリックします。

次の作業

必要に応じて、次のリモート アクセス ポリシーを設定します。

- Telnet
- Web セッション制限
- CIM XML
- インターフェイス モニタリング ポリシー

- SSH の設定

HTTP リモート アクセス ポリシーの削除

HTTP リモート アクセス ポリシーは、ドメイン グループ ルート下にあるドメイン グループから削除されます。 ドメイン グループ ルート下の HTTP リモート アクセス ポリシーは、削除できません。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 削除するポリシーを含むドメイン グループのノードを展開します。

ステップ 4 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 5 [Work] ペインで、[Remote Access] をクリックします。

ステップ 6 [Work] ペインで、[HTTP] タブをクリックします。

ステップ 7 [Actions] 領域で、[Delete] をクリックします。
削除されたポリシーは、再設定されるまでドメイン グループの親から設定を継承します。

ステップ 8 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。

ステップ 9 [Save] をクリックします。

Telnet の設定

Telnet リモート アクセス ポリシーの設定

はじめる前に

ドメイン グループ下で Telnet リモート アクセス ポリシーを設定する前に、最初にこのポリシーを作成する必要があります。 ドメイン グループ ルート下にあるポリシーは、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

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 5 [Work] ペインで、[Remote Access] をクリックします。

ステップ 6 [Work] ペインで、[Telnet] タブをクリックします。

ステップ 7 [Actions] 領域で、[Create] をクリックし、該当するすべてのフィールドに入力します。
[Domain Group root] ノード下の [Operational Policies] では、[Create] をクリックして該当するすべてのフィールドに入力する必要はありません。

ステップ 8 [Save] をクリックします。

次の作業

必要に応じて、次のリモート アクセス ポリシーを設定します。

- HTTP
- Web セッション制限
- CIM XML
- インターフェイス モニタリング ポリシー
- SSH の設定

Telnet リモート アクセス ポリシーの削除

Telnet リモート アクセス ポリシーは、ドメイン グループ ルート下にあるドメイン グループから削除されます。 ドメイン グループ ルート下の Telnet リモート アクセス ポリシーは、削除できません。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 削除するポリシーを含むドメイン グループのノードを展開します。

ステップ 4 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 5 [Work] ペインで、[Remote Access] をクリックします。

ステップ 6 [Work] ペインで、[Telnet] タブをクリックします。

ステップ 7 [Actions] 領域で、[Delete] をクリックします。

削除されたポリシーは、再設定されるまでドメイン グループの親から設定を継承します。

ステップ 8 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。

ステップ 9 [Save] をクリックします。

Web セッション制限の設定

Web セッション制限の設定

はじめる前に

ドメイン グループ下で Web セッション制限リモート アクセス ポリシーを設定する前に、最初にこのポリシーを作成する必要があります。 ドメイン グループ ルート下にあるポリシーは、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

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 5 [Work] ペインで、[Remote Access] をクリックします。

ステップ 6 [Work] ペインで、[Web Session Limits] タブをクリックします。

ステップ 7 [Actions] 領域で、[Create] をクリックし、該当するすべてのフィールドに入力します。
[Domain Group root] ノード下の [Operational Policies] では、[Create] をクリックして該当するすべてのフィールドに入力する必要はありません。

ステップ 8 [Save] をクリックします。

次の作業

必要に応じて、次のリモート アクセス ポリシーを設定します。

- HTTP
- Telnet
- CIM XML
- インターフェイス モニタリング ポリシー

Web セッション制限の削除

Web セッション制限リモート アクセス ポリシーは、ドメイン グループ ルート下にあるドメイン グループから削除されます。 ドメイン グループ ルート下の Web セッション制限リモート アクセス ポリシーは削除できません。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 削除するポリシーを含むドメイン グループのノードを展開します。

ステップ 4 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 5 [Work] ペインで、[Remote Access] をクリックします。

ステップ 6 [Work] ペインで、[Web Session Limits] タブをクリックします。

ステップ 7 [Actions] 領域で、[Delete] をクリックします。
削除されたポリシーは、再設定されるまでドメイン グループの親から設定を継承します。

ステップ 8 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。

ステップ 9 [Save] をクリックします。

CIM XML の設定

CIM XML リモート アクセス ポリシーの設定

はじめる前に

ドメイン グループ下で CIM XML リモート アクセス ポリシーを設定する前に、最初にこのポリシーを作成する必要があります。 ドメイン グループ ルート下にあるポリシーは、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

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 5 [Work] ペインで、[Remote Access] をクリックします。

ステップ 6 [Work] ペインで、[CIM XML] タブをクリックします。

ステップ 7 [Actions] 領域で、[Create] をクリックし、該当するすべてのフィールドに入力します。

[Domain Group root] ノード下の [Operational Policies] では、[Create] をクリックして該当するすべてのフィールドに入力する必要はありません。

ステップ 8 [Save] をクリックします。

次の作業

必要に応じて、次のリモート アクセス ポリシーを設定します。

- HTTP
- Telnet
- Web セッション制限
- インターフェイス モニタリング ポリシー

CIM XML リモート アクセス ポリシーの削除

CIM XML リモート アクセス ポリシーは、ドメイン グループ ルート下にあるドメイン グループから削除されます。 ドメイン グループ ルート下の CIM XML リモート アクセス ポリシーは、削除できません。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 削除するポリシーを含むドメイン グループのノードを展開します。

ステップ 4 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 5 [Work] ペインで、[Remote Access] をクリックします。

ステップ 6 [Work] ペインで、[CIM XML] タブをクリックします。

ステップ 7 [Actions] 領域で、[Delete] をクリックします。
削除されたポリシーは、再設定されるまでドメイン グループの親から設定を継承します。

ステップ 8 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。

ステップ 9 [Save] をクリックします。

インターフェイス モニタリングの設定

インターフェイス モニタリング リモート アクセス ポリシーの設定

はじめる前に

ドメイン グループ下のインターフェイス モニタリング リモート アクセス ポリシーを設定する前に、最初にこのポリシーを作成する必要があります。 ドメイン グループ ルート下にあるポリシーは、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

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 5 [Work] ペインで、[Remote Access] をクリックします。

ステップ 6 [Work] ペインで、[Interfaces Monitoring] タブをクリックします。

ステップ 7 [Actions] 領域で、[Create] をクリックし、該当するすべてのフィールドに入力します。

a) [Monitoring Mechanism] 領域で、[Mii Status] を選択して [Media Independent Interface Monitoring] を選択します。

b) [Monitoring Mechanism] 領域で、[Ping ARP Targets] を選択して [ARP Target Monitoring] を選択します。

c) [Monitoring Mechanism] 領域で、[Ping Gateway] を選択して [Gateway Ping Monitoring] を選択します。

ステップ 8 [Save] をクリックします。

次の作業

必要に応じて、次のリモート アクセス ポリシーを設定します。

- HTTP
- Telnet
- Web セッション制限
- CIM XML

インターフェイス モニタリング リモート アクセス ポリシーの削除

インターフェイス モニタリング リモート アクセス ポリシーは、ドメイン グループ ルート下にあるドメイン グループから削除されます。 ドメイン グループ ルート下のインターフェイス モニタリング リモート アクセス ポリシーは、削除できません。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 削除するポリシーを含むドメイン グループのノードを展開します。

ステップ 4 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 5 [Work] ペインで、[Remote Access] をクリックします。

ステップ 6 [Work] ペインで、[Interfaces Monitoring] タブをクリックします。

ステップ 7 [Actions] 領域で、[Delete] をクリックします。
削除されたポリシーは、再設定されるまでドメイン グループの親から設定を継承します。

ステップ 8 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。

ステップ 9 [Save] をクリックします。

認証サービス

Cisco UCS Central は、ネイティブ認証に LDAP を使用し、リモート認証に RADIUS と TACACS+ を使用します。

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があり、その場合は読み取り専用権限だけが付与されます。

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 で LDAP ユーザを作成する場合と同様の方法で、リモート ユーザを設定し、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。 常に Cisco UCS Central ドメイン グループ ルートから LDAP プロバイダーを作成してください。

LDAP プロバイダー グループ

最大 28 の LDAP プロバイダー グループを定義できます。また Active Directory では Cisco UCS Central でのネストがサポートされているため、任意の数のレベルまでネストできます。 ネスト グループにプロバイダーを割り当てると、プロバイダーが異なる 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サーバが使用できない場合、または到達不能な場合、Cisco UCS Central は、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自動的にフォールバックします。

LDAP プロバイダーの作成

Cisco UCS Central は最大 16 の LDAP プロバイダーをサポートします。

はじめる前に

Active Directory を LDAP サーバとして使用している場合は、Active Directory サーバで Cisco UCS Central にバインドするユーザ アカウントを作成します。 このアカウントには、期限切れにならないパスワードを設定します。

- Cisco UCS Central で、次のいずれかを設定します。
  - LDAP グループ：LDAP グループには、ユーザのロールとロケール情報が含まれています。
  - Cisco UCS Central のユーザ ロールおよびロケール情報を保持する属性が指定されているユーザ：この属性のために LDAP スキーマを拡張するかどうかを選択できます。 スキーマを拡張しない場合は、既存の LDAP 属性を使用して Cisco UCS Central ユーザ ロールとロケールを保持します。 スキーマを拡張する場合は、CiscoAVPair 属性などの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

- クラスタ設定では、両方のファブリック インターコネクトに対する管理ポート IP アドレスを追加します。 この設定では、1 つめのファブリック インターコネクトで障害が発生し、システムが 2 つめのファブリック インターコネクトにフェールオーバーしても、リモート ユーザは引き続きログインできることが保証されます。 ログイン要求はすべて、これらの IP アドレスから送信されます。Cisco UCS Central によって使用されている仮想 IP アドレスではありません。

- セキュア通信を使用するには、Cisco UCS Central で LDAP サーバのルート認証局（CA）の証明書を含むトラスト ポイントを作成します。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[Security] をクリックします。

ステップ 5 [Work] ペインで、[LDAP] を展開し、[Providers] をクリックします。

ステップ 6 [Create LDAP Provider] をクリックし、すべてのフィールドに必要な情報を入力します。

ステップ 7 [OK] をクリックします。

次の作業

単一の LDAP データベースが関係する実装の場合は、認証サービスとして LDAP を選択します。

（注） 実装に複数のデータベースを指定すると、データベース内で特定のユーザを選択した場合に、サーバはユーザを認証する前に、指定した LDAP データベースの順になります。

LDAP プロバイダーのデフォルト設定

この [Properties (LDAP)] ダイアログボックスで Cisco UCS Centralに定義されているすべてのプロバイダーのデフォルト設定を設定できます。 個々のプロバイダーにこれらのうちいずれかのプロパティの設定が含まれている場合、Cisco UCS でその設定が使用され、デフォルト設定は無視されます。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[Security] をクリックします。

ステップ 5 [Work] ペインで、[LDAP] を展開し、[Providers] をクリックします。

ステップ 6 [Actions] 領域で、[Properties] をクリックし、すべてのフィールドに入力します。

ステップ 7 [Properties (LDAP)] ダイアログボックスで、[General] タブのすべてのフィールドに入力し、[OK] をクリックします。

LDAP プロバイダーの削除

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[Security] をクリックします。

ステップ 5 [Work] ペインで、[LDAP] > [Provider] を展開します。

ステップ 6 [Work] ペインで、削除する LDAP プロバイダーをクリックします。

ステップ 7 [Actions] 領域で、[Delete] をクリックします。
また、削除する [LDAP Provider] を右クリックして、そのオプションにアクセスすることもできます。

ステップ 8 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。

LDAP プロバイダーの LDAP グループ ルールの変更

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[Security] をクリックします。

ステップ 5 [Work] ペインで、[LDAP] > [Provider] を展開します。

ステップ 6 グループ ルールを変更する LDAP プロバイダーの名前を右クリックします。

ステップ 7 [Properties (LDAP Provider name)] ダイアログボックスの [LDAP Group Rules] セクションで、グループ ルールを変更します。

ステップ 8 [OK] をクリックします。

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の場合、グループ メンバーシップ情報は、ログイン中にロールまたはロケールを LDAP ユーザに割り当てるために Cisco UCS ドメインで使用できます。 これにより、Cisco UCS Central が展開されるときに LDAP ユーザ オブジェクトの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 グループを判別します。 ユーザがログインすると、Cisco UCS Centralはユーザのロールとロケールに関する情報を LDAP グループ マップから取得します。 ロールとロケールの条件がポリシーの情報に一致すると、Cisco UCS Centralはそのユーザにアクセス権を提供します。

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 ディレクトリへの変更に基づいて自動的に更新されません。 LDAP ディレクトリで LDAP グループを削除または名前変更する場合、Cisco UCS Centralで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いずれかの組み合わせを含むように設定できます。

- ロールのみ
- ロケールのみ
- ロールとロケールの両方

例：特定のロケーションのサーバ管理者グループを表すLDAPグループの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 LDAP グループに含めることができます。

特定のロケーションのサーバ管理者に対しアクセスを制限する場合は、特定のサイト名をロケールに指定できます。

（注） Cisco UCS Central には、すぐに使用可能な多くのユーザ ロールが含まれていますが、ロケールは含まれていません。 このため LDAP プロバイダー グループをロケールにマップするカスタム 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 マップで定義されている別のグループ内にネストされた LDAP グループを検索できます。 この新しい機能を使用すると、Cisco UCS Central のグループ マップでサブグループを常に作成する必要がなくなります。

（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。
- MS-AD 内でネストされた LDAP グループを作成する場合、名前に特殊文字を使用するには、\\ を使用して特殊文字を設定してください（ , \\）。 次に、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 グループのメンバーとして追加し、メンバー 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。

デフォルトでは、LDAP グループを別のグループ内にネストするときにユーザ権限が継承されます。 たとえば、Group_2 のメンバーとして Group_1 を作成する場合、Group_1 のユーザは Group_2 のメンバーと同じ権限が与えられます。 その結果、Group_1 のメンバーであるユーザを検索するときは、LDAP グループ マップで Group_2 だけを選択します。Group_1 と Group_2 を別々に検索する必要はありません。

LDAP グループ マップの作成

はじめる前に

- LDAP サーバで LDAP グループを作成します。
- LDAP サーバで LDAP グループの識別名を設定します。
- Cisco UCS Central でロケールを作成します（任意）。
- Cisco UCS Central でカスタム ロールを作成します（任意）。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[Security] をクリックします。

ステップ 5 [Work] ペインで、[LDAP] を展開し、[Group Maps] をクリックします。

ステップ 6 [Actions] 領域で、[Create LDAP Group Map] をクリックし、すべてのフィールドに入力し、[OK] をクリックします。

次の作業

LDAP グループ ルールを設定します。

LDAP グループ マップの削除

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[Security] をクリックします。

ステップ 5 [Work] ペインで、[LDAP] > [Group Maps] を展開します。

ステップ 6 [Work] ペインで、削除するグループ マップをクリックします。

ステップ 7 [Actions] 領域で、[Delete] をクリックします。
また、削除する [Group Map] を右クリックして、そのオプションにアクセスすることもできます。

ステップ 8 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。

RADIUS プロバイダーの設定

RADIUS プロバイダーのプロパティの設定

このタスクで設定するプロパティは、Cisco UCS ManagerCisco UCS Central で定義されたこのタイプのすべてのプロバイダー接続のデフォルト設定です。 個々のプロバイダーにこれらのうちいずれかのプロパティの設定が含まれている場合、Cisco UCS ManagerCisco UCS Central でその設定が使用され、デフォルト設定は無視されます。

（注） RADIUS ネイティブ認証は、このリリースではサポートされていません。また、ドメイン グループ ルートおよびドメイン グループ下の Cisco UCS Central のポリシーの作成には使用できません。 RADIUS は、Cisco UCS ドメイン のグローバル ポリシーの作成に使用される場合があります。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[Security] をクリックします。

ステップ 5 [Work] ペインで [RADIUS] をクリックします。

ステップ 6 [Actions] 領域で、[Properties] をクリックし、すべてのフィールドに入力します。
また、[RADIUS] を右クリックして、そのオプションにアクセスすることもできます。

a) [Properties (RADIUS)] ダイアログボックスで、[General] タブのすべてのフィールドに入力します。

b) [OK] をクリックします。

ステップ 7 [Save] をクリックします。

次の作業

RADIUS プロバイダーを作成します。

RADIUS プロバイダーの作成

Cisco UCS Central は最大 16 の RADIUS プロバイダーをサポートします。 RADIUS ネイティブ認証は、このリリースではサポートされていません。また、ドメイングループルートおよびドメイン グループ下の Cisco UCS Central のポリシーの作成には使用できません。 RADIUS は、Cisco UCS ドメイン のグローバル ポリシーの作成に使用される場合があります。

はじめる前に

RADIUS サーバで、次の設定を行います。

- Cisco UCS Central のユーザ ロールとロケール情報を保持する属性でユーザを設定します。 この属性について RADIUS スキーマを拡張するかどうかを選択できます。 スキーマを拡張しない場合は、既存の RADIUS 属性を使用して Cisco UCS ユーザ ロールとロケールを保持します。 スキーマを拡張する場合は、cisco-avpair 属性などのカスタム属性を作成します。

  シスコによる RADIUS の実装のベンダー ID は 009 であり、属性のベンダー ID は 001 です。

次の構文例は、cisco-avpair 属性を作成する場合に複数のユーザ ロールとロケールを指定する方法を示しています。`shell:roles="admin,aaa" shell:locales="L1,abc"`。 複数の値を区切るには、区切り文字としてカンマ「,」を使用します。

- クラスタ設定では、両方のファブリック インターコネクトに対する管理ポート IP アドレスを追加します。 この設定では、1 つめのファブリック インターコネクトで障害が発生し、システムが 2 つめのファブリック インターコネクトにフェールオーバーしても、リモートユーザは引き続きログインできることが保証されます。 ログイン要求はすべて、これらの IP アドレスから送信されます。Cisco UCS Central によって使用されている仮想 IP アドレスではありません。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[Security] をクリックします。

ステップ 5 [Work] ペインで、[RADIUS] を展開し、[Providers] をクリックします。

ステップ 6 [Actions] 領域で、[Create RADIUS Provider] をクリックし、すべてのフィールドに入力します。
また、[Providers] を右クリックして、そのオプションにアクセスすることもできます。

a) [Create RADIUS Provider] ダイアログボックスで、[General] タブのすべてのフィールドに入力します。

b) [OK] をクリックします。

ステップ 7 [Save] をクリックします。

次の作業

- 単一の RADIUS データベースが関係する実装の場合は、RADIUS をプライマリ認証サービスとして選択します。
- 複数の RADIUS データベースが関係する実装の場合は、RADIUS プロバイダー グループを設定します。

RADIUS プロバイダーの削除

手順

ステップ 1	メニュー バーで、[Operations Management] をクリックします。
ステップ 2	[Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。
ステップ 3	[Domain Groups root] ノードで、[Operational Policies] をクリックします。
ステップ 4	[Work] ペインで、[Security] をクリックします。
ステップ 5	[Work] ペインで、[RADIUS] を展開し、[Providers] をクリックします。
ステップ 6	[Work] ペインで、削除する [RADIUS Provider] をクリックします。
ステップ 7	[Actions] 領域で、[Delete] をクリックします。 また、削除する [RADIUS Provider] を右クリックして、そのオプションにアクセスすることもできます。
ステップ 8	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。

TACACS+ プロバイダーの設定

TACACS+ プロバイダーのプロパティの設定

このタスクで設定するプロパティは、Cisco UCS ManagerCisco UCS Central で定義されたこのタイプのすべてのプロバイダー接続のデフォルト設定です。 個々のプロバイダーにこれらのうちいずれかのプロパティの設定が含まれている場合、Cisco UCS ManagerCisco UCS Central でその設定が使用され、デフォルト設定は無視されます。

（注） TACACS+ ネイティブ認証は、このリリースではサポートされていません。また、Cisco UCS Central でのポリシーの作成には使用できません。 TACACS+ は、Cisco UCS ドメイン のグローバル ポリシーの作成に使用される場合があります。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[Security] をクリックします。

ステップ 5 [Work] ペインで [TACACS+] をクリックします。

ステップ 6 [Actions] 領域で、[Properties] をクリックします。
また、[TACACS+] を右クリックして、そのオプションにアクセスすることもできます。

a) [Properties (TACACS+)] ダイアログボックスで、[General] タブのすべてのフィールドに入力します。

b) [OK] をクリックします。

ステップ 7 [Save] をクリックします。

次の作業

TACACS+ プロバイダーを作成します。

TACACS+ プロバイダーの作成

Cisco UCS Central は最大 16 の TACACS+ プロバイダーをサポートします。 TACACS+ ネイティブ認証は、このリリースではサポートされていません。また、Cisco UCS Central でのポリシーの作成には使用できません。 TACACS+ は、Cisco UCS ドメイン のグローバル ポリシーの作成に使用される場合があります。

はじめる前に

TACACS+ サーバで、次の設定を行います。

- cisco-av-pair 属性を作成します。 既存の TACACS+ 属性は使用できません。

  cisco-av-pair 名は、TACACS+ プロバイダーの属性 ID を提供する文字列です。

  次の構文例は、cisco-av-pair 属性を作成するときに複数のユーザ ロールとロケールを指定する方法を示しています。`cisco-av-pair=shell:roles="admin aaa" shell:locales*"L1 abc"`。cisco-av-pair 属性構文でアスタリスク（*）を使用すると、ロケールがオプションとして指定され、同じ認可プロファイルを使用する他のシスコデバイスで認証の失敗を防ぐことができます。 複数の値を区切るには、区切り文字としてスペースを使用します。

- クラスタ設定では、両方のファブリック インターコネクトに対する管理ポート IP アドレスを追加します。 この設定では、1 つめのファブリック インターコネクトで障害が発生し、システムが 2 つめのファブリック インターコネクトにフェールオーバーしても、リモートユーザは引き続きログインできることが保証されます。 ログイン要求はすべて、これらの IP ア

ドレスから送信されます。Cisco UCS Central によって使用されている仮想 IP アドレスではありません。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[Security] をクリックします。

ステップ 5 [Work] ペインで、[TACACS+] を展開し、[Providers] をクリックします。

ステップ 6 [Actions] 領域で、[Create TACACS+ Provider] をクリックし、すべてのフィールドに入力します。
また、[Providers] を右クリックして、そのオプションにアクセスすることもできます。

a) [Create TACACS+ Provider] ダイアログボックスで、[General] タブのすべてのフィールドに入力します。

b) [OK] をクリックします。

ステップ 7 [Save] をクリックします。

次の作業

- 単一の TACACS+ データベースが関係する実装の場合は、TACACS+ をプライマリ認証サービスとして選択します。
- 複数の TACACS+ データベースが関係する実装の場合は、TACACS+ プロバイダー グループを設定します。

TACACS+ プロバイダーの削除

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[Security] をクリックします。

ステップ 5 [Work] ペインで、[TACACS+] > [Provider] を展開します。

ステップ 6 [Work] ペインで、削除する TACACS+ プロバイダーをクリックします。

ステップ 7 [Actions] 領域で、[Delete] をクリックします。
また、削除する [TACACS+ Provider] を右クリックして、そのオプションにアクセスすることもできます。

ステップ 8 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。

マルチ認証システムの設定

マルチ認証システム

Cisco UCS を設定して、次の機能を設定することによって複数の認証システムを使用できます。

- プロバイダー グループ
- 認証ドメイン

Cisco UCS Central GUI でプロバイダー グループと認証ドメインを設定すると、**ucs-** *auth-domain* 構文を使用して Cisco UCS Central CLI でシステムにログインできます。

リモート認証サービスで複数の認証ドメインおよびネイティブ認証が設定されている場合、次のいずれかの構文例を使用して SSH または Putty でログインします。

Linux ターミナルから：

- **ssh ucs-***auth-domain\\username@Cisco UCS domain-ip-address*

  ```
  ssh ucs-example\\jsmith@192.0.20.11
  ```

- **ssh -l ucs-***auth-domain\\username* {*Cisco UCS domain-ip-address* | *Cisco UCS domain-host-name*}

  ```
  ssh -l ucs-example\\jsmith 192.0.20.11
  ```

- **ssh** {*Cisco UCS domain-ip-address* | *Cisco UCS domain-host-name*} **-l ucs-***auth-domain\\username*

  ```
  ssh 192.0.20.11 -l ucs-example\\jsmith
  ```

Putty クライアントから：

- Login as: **ucs-***auth-domain\\username*

  ```
  Login as: ucs-example\\jsmith
  ```

SSH クライアントから：

- Host Name: *Cisco UCS domain-ip-address*

  User Name: **ucs-***auth-domain\\username*

  ```
  Host Name: 192.0.20.11
  User Name: ucs-example\\jsmith
  ```

プロバイダー グループ

プロバイダー グループは、認証プロセス中に Cisco UCS によって使用されるプロバイダーのセットです。 Cisco UCS Central では、グループごとに最大 8 個のプロバイダーが許可された、最大 16 個のプロバイダー グループを作成できます。

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サーバが使用できない場合、または到達不能な場合、Cisco UCS Central は、ローカル ユーザ名とパスワードを使用して自動的にローカル認証方式にフォールバックします。

LDAP プロバイダー グループの作成

LDAP プロバイダー グループを作成すると、複数の LDAP データベースを使用して認証できます。

（注） 単一の LDAP データベースを使用した認証では、LDAP プロバイダー グループを設定する必要はありません。

はじめる前に

1 つ以上の LDAP プロバイダーを作成します。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[Security] をクリックします。

ステップ 5 [Work] ペインで、[LDAP] を展開し、[Provider Groups] をクリックします。

ステップ 6 [Actions] 領域で、[Create LDAP Provider Group] をクリックし、すべてのフィールドに入力します。また、[Provider Groups] を右クリックして、そのオプションにアクセスすることもできます。

a) [Create LDAP Provider Group] ダイアログボックスで、[General] タブのすべてのフィールドに入力します。

b) [OK] をクリックします。

ステップ 7 [Save] をクリックします。

次の作業

単一の LDAP データベースが関係する実装の場合は、認証サービスとして LDAP を選択します。

LDAP プロバイダー グループの削除

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[Security] をクリックします。

ステップ 5 [Work] ペインで、[LDAP] > [Provider Groups] を展開します。

ステップ 6 [Work] ペインで、削除する LDAP プロバイダー グループをクリックします。

ステップ 7 [Actions] 領域で、[Delete] をクリックします。
また、削除する [LDAP Provider Group] を右クリックして、そのオプションにアクセスすることもできます。

ステップ 8 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。

RADIUS プロバイダー グループの作成

RADIUS プロバイダー グループを作成すると、複数の RADIUS データベースを使用して認証できます。

（注） 単一の RADIUS データベースを使用した認証では、RADIUS プロバイダー グループを設定する必要はありません。

はじめる前に

1 つ以上の RADIUS プロバイダーを作成します。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[Security] をクリックします。

ステップ 5 [Work] ペインで、[RADIUS] を展開し、[Providers] をクリックします。

ステップ 6 [Actions] 領域で、[Create RADIUS Provider Group] をクリックし、すべてのフィールドに入力します。
また、[Provider Groups] を右クリックして、そのオプションにアクセスすることもできます。

a) [Create RADIUS Provider] ダイアログボックスで、[General] タブのすべてのフィールドに入力します。
b) [OK] をクリックします。

ステップ 7 [Save] をクリックします。

次の作業

認証ドメインを設定するか、デフォルト認証サービスを選択します。

RADIUS プロバイダー グループの削除

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[Security] をクリックします。

ステップ 5 [Work] ペインで、[RADIUS] > [Provider Groups] を展開します。

ステップ 6 [Work] ペインで、削除する RADIUS プロバイダー グループをクリックします。

ステップ 7 [Actions] 領域で、[Delete] をクリックします。
また、削除する [RADIUS Provider Group] を右クリックして、そのオプションにアクセスすることもできます。

ステップ 8 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。

TACACS+ プロバイダー グループの作成

TACACS+ プロバイダー グループを作成すると、複数の TACACS+ データベースを使用して認証できます。

（注） 単一の TACACS+ データベースを使用した認証では、TACACS+ プロバイダー グループを設定する必要はありません。

はじめる前に

1 つ以上の TACACS+ プロバイダーを作成します。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[Security] をクリックします。

ステップ 5 [Work] ペインで、[TACACS+] を展開し、[Provider Groups] をクリックします。

ステップ 6 [Actions] 領域で、[Create TACACS+ Provider Group] をクリックし、すべてのフィールドに入力します。
また、[Provider Groups] を右クリックして、そのオプションにアクセスすることもできます。

a) [Create TACACS+ Provider Group] ダイアログボックスで、[General] タブのすべてのフィールドに入力します。

名前	説明
[Name] フィールド	TACACS+ プロバイダー グループの名前。
[Available Providers] リスト ボックス	TACACS+ グループに追加できる使用可能な TACACS+ プロバイダー。 Shift+Click および Ctrl+Click を使用して、複数のプロバイダーを選択できます。
[>>] ボタン	[Available Providers] リスト ボックスでどのプロバイダーが選択されているかに関係なく、使用可能なすべてのプロバイダーをグループに追加します。
[>] ボタン	[Available Providers] リスト ボックスで選択されたプロバイダーをグループに追加します。
[<] ボタン	[Assigned Providers] リスト ボックスで選択されたプロバイダーをグループから削除します。
[<<] ボタン	[Assigned Providers] リスト ボックスでどのプロバイダーが選択されているかに関係なく、すべてのプロバイダーをグループから削除します。
[Assigned Providers] リスト ボックス	TACACS+ グループに含まれている TACACS+ プロバイダー。 Cisco UCS は、テーブルに表示される順序でプロバイダーを検索します。 プロバイダーのプライオリティを変更するには、プロバイダーを選択し、リストの上にある矢印ボタンを使用して、目的の位置にプロバイダーを移動します。

b) [OK] をクリックします。

ステップ 7 [Save] をクリックします。

TACACS+ プロバイダー グループの削除

認証設定で使用されているプロバイダー グループは削除できません。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[Security] をクリックします。

ステップ 5 [Work] ペインで、[TACACS+] > [Provider Groups] を展開します。

ステップ 6 [Work] ペインで、削除する [TACACS+ Provider Group] グループをクリックします。

ステップ 7 [Actions] 領域で、[Delete] をクリックします。
また、削除する [TACACS+ Provider Group] を右クリックして、そのオプションにアクセスすることもできます。

ステップ 8 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。

認証ドメイン

認証ドメインは、マルチ認証システムを活用するために Cisco UCS ドメインによって使用されます。 各認証ドメインは、ログイン中に指定および設定されます。 認証ドメインを指定しないと、デフォルトの認証サービス設定が使用されます。

最大 8 個の認証ドメインを作成できます。 各認証ドメインは、Cisco UCS ドメイン内のプロバイダー グループと領域に関連付けられています。 プロバイダー グループが指定されていない場合は、領域内のすべてのサーバが使用されます。

（注） このリリースでは LDAP の認証ドメインが Cisco UCS Centralでサポートされます。 ただし、Cisco UCS Central ドメイン グループ ルートの管理対象 Cisco UCS ドメインで認証ドメインがサポートされています。

認証ドメインの作成

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[Security] をクリックします。

ステップ 5 [Work] ペインで、[Authentication] を展開し、[Authentication Domains] をクリックします。

ステップ 6 [Actions] 領域で、[Create Authentication Domain] をクリックし、すべてのフィールドに入力します。
また、[Authentication Domains] を右クリックして、そのオプションにアクセスすることもできます。

a) [Create Authentication] ダイアログボックスで、[General] タブのすべてのフィールドに入力します。

b) [OK] をクリックします。

ステップ 7 [Save] をクリックします。

プライマリ認証サービスの選択

コンソール認証サービスの選択

はじめる前に

システムでリモート認証サービスが使用されている場合は、その認証サービスに対するプロバイダーを作成します。 Cisco UCS を通じたローカル認証のみを使用する場合は、最初にプロバイダーを作成する必要はありません。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[Security] をクリックします。

ステップ 5 [Work] ペインで、[Authentication] を展開し、[Native Authentication] をクリックします。

ステップ 6 [Actions] 領域で、[Properties] をクリックし、すべてのフィールドに入力します。
また、[Properties] を右クリックして、そのオプションにアクセスすることもできます。

a) [Properties (Native Authentication)] ダイアログボックスで、[General] タブのすべての [Default Authentication] フィールドに入力します。
b) [Properties (Native Authentication)] ダイアログボックスで、[General] タブのすべての [Console Authentication] フィールドに入力します。
c) [Properties (Native Authentication)] ダイアログボックスで、[General] タブのすべての [Remote Users Policy] フィールドに入力します。
d) [OK] をクリックします。

ステップ 7 [Save] をクリックします。

デフォルト認証サービスの選択

はじめる前に

システムでリモート認証サービスが使用されている場合は、その認証サービスに対するプロバイダーを作成します。 Cisco UCS を通じたローカル認証のみを使用する場合は、最初にプロバイダーを作成する必要はありません。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[Security] をクリックします。

ステップ 5 [Work] ペインで、[Authentication] を展開し、[Native Authentication] をクリックします。

ステップ 6 [Actions] 領域で、[Properties] をクリックし、すべてのフィールドに入力します。
また、[Native Authentication] を右クリックして、そのオプションにアクセスすることもできます。

a) [Properties (Native Authentication)] ダイアログボックスで、[General] タブのすべての [Default Authentication] フィールドに入力します。
b) [OK] をクリックします。

ステップ 7 [Save] をクリックします。

リモート ユーザのロール ポリシー

デフォルトでは、ユーザ ロールが Cisco UCS Central で設定されていない場合、LDAP プロトコル（このリリースでは RADIUS および TACACS+ 認証を除く）を使用して、リモート サーバから Cisco UCS Central にログインしたすべてのユーザに読み取り専用アクセス権が付与されます。

（注） RADIUS、TACACS+、および LDAP 認証は、ローカルに管理された Cisco UCS ドメインでサポートされています。

リモート ユーザのロール ポリシーは、次の方法で設定できます。

- **assign-default-role**

  ユーザ ロールに基づいて、Cisco UCS Central へのユーザ アクセスを制限しません。 その他のユーザ ロールが Cisco UCS Central で定義されていない限り、読み取り専用アクセス権がすべてのユーザに付与されます。

  これはデフォルトの動作です。

- **no-login**

  ユーザ ロールに基づいて、Cisco UCS Central へのユーザ アクセスを制限します。 リモート認証システムにユーザ ロールが割り当てられていない場合、アクセスが拒否されます。

セキュリティ上の理由から、Cisco UCS Central で確立されたユーザ ロールに一致するユーザへのアクセスを制限するのが望ましい場合があります。

リモート ユーザのロール ポリシーの設定

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[Security] をクリックします。

ステップ 5 [Work] ペインで、[Authentication] を展開し、[Native Authentication] をクリックします。

ステップ 6 [Actions] 領域で、[Properties] をクリックし、すべてのフィールドに入力します。
また、[Native Authentication] を右クリックして、そのオプションにアクセスすることもできます。

a) [Properties (Native Authentication)] ダイアログボックスで、[General] タブのすべての [Remote Users Policy] フィールドに入力します。

b) [OK] をクリックします。

ステップ 7 [Save] をクリックします。

DNS サーバの設定

DNS ポリシーの管理

Cisco UCS Central は、DNS サーバおよびドメイン名を定義するグローバル DNS ポリシーをサポートしています。 登録済み Cisco UCS ドメインでは、そのドメインのポリシー解決コントロール内で DNS 管理をグローバルに定義するようにしている場合、DNS 管理について Cisco UCS Central への登録に従うことになります。

DNS ポリシーの設定

はじめる前に

ドメイン グループ ルート下でドメイン グループの DNS ポリシーを設定する前に、最初にこのポリシーを作成する必要があります。 ドメイン グループ ルート下にあるポリシーは、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

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 5 [Work] ペインで、[DNS] をクリックします。

ステップ 6 [Actions] 領域で、[Create] をクリックし、該当するすべてのフィールドに入力します。

ステップ 7 [Save] をクリックします。

DNS ポリシーの削除

DNS ポリシーを削除すると、そのポリシー内のすべての DNS サーバ設定が削除されます。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 5 [Work] ペインで、[DNS] をクリックします。

ステップ 6 [Actions] 領域で、[Delete] をクリックします。
削除されたポリシーは、再設定されるまでドメイン グループの親から設定を継承します。

ステップ 7 [Save] をクリックします。

DNS ポリシーの DNS サーバの設定

はじめる前に

DNS ポリシーを設定します。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[DNS] をクリックします。

ステップ 5 [Actions] 領域で、[Add DNS Server] をクリックし、すべてのフィールドに入力します。

a) [Add DNS Server] ダイアログボックスで、すべてのフィールドに値を入力します。

b) [OK] をクリックします。

ステップ 6 [Save] をクリックします。

DNS ポリシーからの DNS サーバの削除

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[DNS] をクリックします。

ステップ 5 [Actions] 領域で、削除する DNS サーバを選択し、[Delete] をクリックします。
また、DNS サーバを右クリックして、そのオプションにアクセスすることもできます。

ステップ 6 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。

ステップ 7 [Save] をクリックします。

電力ポリシーの管理

Cisco UCS Central は、グローバルな電力割り当てポリシー（ポリシー ドリブン シャーシ グループ キャップ方式または手動のブレード レベル キャップ方式に基づく）、電力ポリシー（グリッド、n+1、または非冗長方式に基づく）を定義するグローバルな装置ポリシーをサポートしています。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電源管理と電源装置ユニットをグローバルに定義するようにしている場合、電源管理と電源装置ユニットについて Cisco UCS Central への登録に従うことになります。

グローバルな電力割り当て装置ポリシーの設定

はじめる前に

ドメイン グループ下でグローバルな電力割り当て装置ポリシーを設定する前に、最初にこのポリシーを作成する必要があります。 ドメイン グループ ルート下にあるポリシーは、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

ステップ 1 メニュー バーで、[Operations Management] をクリックします。
ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。
ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。
ステップ 4 [Navigation] ペインで、[Operational Policies] をクリックします。
ステップ 5 [Work] ペインで、[Equipment] をクリックします。
ステップ 6 [Work] ペインで [Global Power Allocation Policy] タブをクリックします。
ステップ 7 [Actions] 領域で、[Create] をクリックし、該当するすべてのフィールドに入力します。
ステップ 8 [Save] をクリックします。

グローバルな電力割り当て装置ポリシーの削除

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。
ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。
ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。
ステップ 4 [Navigation] ペインで、[Operational Policies] をクリックします。
ステップ 5 [Work] ペインで、[Equipment] をクリックします。
ステップ 6 [Work] ペインで [Global Power Allocation Policy] タブをクリックします。
ステップ 7 [Actions] 領域で、[Delete] をクリックします。
削除されたポリシーは、再設定されるまでドメイン グループの親から設定を継承します。
ステップ 8 [Save] をクリックします。

電力装置ポリシーの設定

はじめる前に

ドメイン グループ下で電力装置ポリシーを設定する前に、最初にこのポリシーを作成する必要があります。 ドメイン グループ ルート下にあるポリシーは、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

ステップ 1 メニュー バーで、[Operations Management] をクリックします。
ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。
ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。
ステップ 4 [Navigation] ペインで、[Operational Policies] をクリックします。
ステップ 5 [Work] ペインで、[Equipment] をクリックします。
ステップ 6 [Work] ペインで、[Power Policy] タブをクリックします。
ステップ 7 [Actions] 領域で、[Create] をクリックし、該当するすべてのフィールドに入力します。
ステップ 8 [Save] をクリックします。

電力装置ポリシーの削除

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。
ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。
ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。
ステップ 4 [Navigation] ペインで、[Operational Policies] をクリックします。
ステップ 5 [Work] ペインで、[Equipment] をクリックします。
ステップ 6 [Work] ペインで、[Power Policy] タブをクリックします。
ステップ 7 [Actions] 領域で、[Delete] をクリックします。
削除されたポリシーは、再設定されるまでドメイン グループの親から設定を継承します。
ステップ 8 [Save] をクリックします。

タイム ゾーンの管理

タイム ゾーンの管理

Cisco UCS Central は、国際的なタイム ゾーンと定義された NTP サーバに基づいて、グローバルな日付と時刻ポリシーをサポートしています。 登録済み Cisco UCS Manager クライアントでは、そのクライアントのポリシー解決コントロール内で日付と時刻をグローバルに定義するようにしている場合、日付と時刻の設定について Cisco UCS Central への登録に従うことになります。

日付と時刻ポリシーの設定

はじめる前に

ドメイン グループ下で日付と時刻ポリシーを設定する前に、最初にこのポリシーを作成する必要があります。 ドメイン グループ ルート下にあるポリシーは、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

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 5 [Work] ペインで、[DateTime] をクリックします。

ステップ 6 [Actions] 領域で、[Create] をクリックし、該当するすべてのフィールドに入力します。

ステップ 7 [Save] をクリックします。

日付と時刻ポリシーの削除

日付と時刻ポリシーは、ドメイン グループ ルート下にあるドメイン グループから削除されます。ドメイン グループ ルート下の日付と時刻ポリシーは、削除できません。

日付と時刻ポリシーを削除すると、そのポリシー内のすべての NTP サーバ設定が削除されます。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 削除するポリシーを含むドメイン グループのノードを展開します。

ステップ 4 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 5 [Work] ペインで、[DateTime] をクリックします。

ステップ 6 [Actions] 領域で、[Delete] をクリックします。
削除されたポリシーは、再設定されるまでドメイン グループの親から設定を継承します。

ステップ 7 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。

ステップ 8 [Save] をクリックします。

日付と時刻ポリシーの NTP サーバの設定

はじめる前に

ドメイン グループ ルート下にあるドメイン グループの NTP サーバを設定するには、最初に日付と時刻ポリシーを作成しておく必要があります。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[DateTime] をクリックします。

ステップ 5 [Actions] 領域で、[Add NTP Server] をクリックし、すべてのフィールドに入力し、[OK] をクリックします。

ステップ 6 [Save] をクリックします。

NTP サーバのプロパティの設定

既存の NTP サーバのプロパティは、NTP サーバ インスタンスを保存する前に更新される場合があります。 保存された NTP サーバの名前を変更するには、削除して再作成する必要があります。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 5 [Work] ペインで、[DateTime] をクリックします。

ステップ 6 [Actions] 領域で、設定する NTP サーバを選択して [Properties] をクリックし、すべてのフィールドに入力します。
また、NTP サーバを右クリックして、そのオプションにアクセスすることもできます。 NTP サーバが保存されている場合は、[Actions] 領域の [Properties] をクリックしてアクセスできる [Properties (NTP Provider)] ダイアログを編集できません。 保存されている NTP サーバのサーバ名を変更するには、NTP サーバを削除して再作成します。

a) [Properties (NTP Provider)] ダイアログボックスで、すべてのフィールドに値を入力します。

名前	説明
[NTP Server] フィールド	使用する NTP サーバの IP アドレスまたはホスト名。 （注） IPv4 アドレスではなくホスト名を使用する場合、DNS サーバを設定する必要があります。 Cisco UCS ドメインが Cisco UCS Central に登録されていないか、DNS 管理が [ローカル] に設定されている場合は、Cisco UCS Manager で DNS サーバを設定します。 Cisco UCS ドメイン Cisco UCS Central に登録されていないか、DNS 管理が [グローバル] に設定されている場合は、Cisco UCS Central で DNS サーバを設定します。

b) [OK] をクリックします。

ステップ 7 [Save] をクリックします。

日付と時刻ポリシーからの NTP サーバの削除

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[DateTime] をクリックします。

ステップ 5 [Actions] 領域で、削除する NTP サーバを選択し、[Delete] をクリックします。
また、NTP サーバを右クリックして、そのオプションにアクセスすることもできます。 削除される NTP サーバは、再設定されるまでドメイン グループの親からの設定を継承します。

ステップ 6 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。

SNMP ポリシー

Cisco UCS Central は、SNMP トラップおよび SNMP ユーザの有効化と無効化、定義を行うグローバル SNMP ポリシーをサポートしています（通常のパスワードとプライバシー パスワード、認証タイプ md5 または sha、および暗号化タイプ DES と AES-128 により）。 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をリモートでモニタする機能を提供します。 また、Cisco UCS Central ホスト IP を変更し、新しい IP で SNMP エージェントを再起動することもできます。 SNMP が、アクティブとスタンバイの両方の Cisco UCS Central サーバで稼働しており、設定が両方のサーバで保持されます。 Cisco UCS Central は、オペレーティング システムにより管理される情報ベース（MIB）のみへの読み取りアクセス権を提供します。Cisco UCS Central CLI を使用して、SNMP v1、v2c のコミュニティ ストリングを設定し、SNMPv3 ユーザを作成および削除することができます。

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 内のソフトウェア コンポーネントで、Cisco UCS Central のデータを維持し、必要に応じて SNMP にレポートします。 Cisco UCS Central には、エージェントと MIB 収集が含まれます。 SNMP エージェントを有効にし、マネージャとエージェント間のリレーションシップを作成するには、Cisco UCS Central で SNMP を有効にし、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 では OS MIB モードだけがサポートされます。

Cisco UCS Central では SNMPv1、SNMPv2c、および SNMPv3 がサポートされます。 SNMPv1 と SNMPv2c は、ともにコミュニティベース形式のセキュリティを使用します。 SNMP を定義する RFC を次に示します。

- 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 では SNMP 通知がトラップとして生成されます。 SNMP マネージャはトラップ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、トラップの信頼性は低くなります。

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	[Username]	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 に対して set 操作は使用できません。 Cisco UCS Centralでサポートされている MIB を次に示します。

- 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 およびCisco UCS Central MIB をサポートしません。

SNMPv3 ユーザの認証プロトコル

Cisco UCS Central は、SNMPv3 ユーザ向けに次の認証プロトコルをサポートします。

- HMAC-MD5-96（MD5）
- HMAC-SHA-96（SHA）

SNMPv3 ユーザの AES プライバシー プロトコル

Cisco UCS Central は、SNMPv3 メッセージ暗号化用プライバシープロトコルの 1 つとして、Advanced Encryption Standard（AES）を使用し、RFC 3826 に準拠します。 AES が無効であり、プライバシー パスワードが設定されている場合、暗号化に DES が使用されます。

AES-128 設定を有効にし、SNMPv3 ユーザのプライバシー パスワードをインクルードした場合、Cisco UCS Central はプライバシー パスワードを使用して 128 ビット AES キーを生成します。 AES プライバシー パスワードは最小で 8 文字です。 パスフレーズをクリア テキストで指定する場合、最大 64 文字を指定できます。

SNMP ポリシーの設定

はじめる前に

ドメイン グループで SNMP ポリシーを設定する前に、SNMP ポリシーが最初に作成されていることを確認します。 ドメイン グループ ルート下にあるポリシーは、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

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで [Domain Groups] > [Domain Group root] を展開するか、またはポリシーを作成するドメイン グループの名前を指定します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 5 [Work] ペインで、[SNMP] をクリックします。

ステップ 6 [Actions] 領域で、[Create] をクリックし、該当するすべてのフィールドに入力します。
[Domain Group root] ノード下の [Operational Policies] では、[Create] をクリックして該当するすべてのフィールドに入力する必要はありません。

a) [Actions] 領域で [Enabled] をクリックし、[Admin State] を選択します。
[Enabled] の場合、Cisco UCS Central は Cisco UCS Central システムのモニタに SNMP を使用します。 Cisco UCS は、ドメイン グループ自体が SNMP を使用して設定されていない場合は、ドメイン グループのすべての Cisco UCS ドメイン で SNMP を使用します。

デフォルトの状態は [Disabled] であり、フィールドは表示されていません。 デフォルトの状態のままの場合は、SNMP ポリシーが無効になります。

b) [Community/Username] フィールドにコミュニティまたはユーザ名を入力します。
Cisco UCS が SNMP ホストに送信するトラップ メッセージに含めるデフォルトの SNMP v1 または v2c コミュニティ名あるいは SNMP v3 ユーザ名を使用できます。 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。 デフォルトは public です。

c) [System Contact] フィールドにシステム連絡先担当者情報を入力します。
[System Contact] に指定する担当者は、SNMP の実装を担当します。 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。

d) [System Location] フィールドにシステム ロケーションを入力します。
[System Location] により、SNMP エージェント（サーバ）が稼働するホストの場所が定義されます。 最大 510 文字の英数字文字列を入力します。

ステップ 7 [Save] をクリックします。

次の作業

SNMP トラップおよび SNMP ユーザを作成します。

SNMP トラップの作成

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[SNMP] をクリックします。

ステップ 5 [SNMP Traps] 領域で [Create SNMP Trap] をクリックし、[Create SNMP Trap] ダイアログボックスの該当するすべてのフィールドに入力します。

a) [IP Address] フィールドに SNMP ホストの IP アドレスを入力します。
Cisco UCS は、定義された IP アドレスにトラップを送信します。

b) [Community/Username] フィールドにコミュニティまたはユーザ名を入力します。
Cisco UCS が SNMP ホストに送信するトラップ メッセージに含めるデフォルトの SNMP v1 または v2c コミュニティ名あるいは SNMP v3 ユーザ名を使用できます。 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。 デフォルトは public です。

c) [Port] フィールドに、ポート番号を入力します。
Cisco UCS は定義されたポートを使用して、トラップを送信するため SNMP ホストと通信します。 1 ～ 65535 の整数を入力します。 デフォルト ポートは 162 です。

d) SNMP のバージョンを選択するため、[v1]、[v2c]、または [v3] をクリックします。

e) [trap] をクリックして、[Type] で SNMP トラップのタイプを選択します。

f) [auth]、[no auth]、または [priv] をクリックして、[v3Privilege] を定義します。

g) [OK] をクリックします。

ステップ 6 [Save] をクリックします。

SNMP ユーザの作成

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[SNMP] をクリックします。

ステップ 5 [SNMP Users] 領域で [Create SNMP User] をクリックし、[Create SNMP User] ダイアログボックスの該当するすべてのフィールドに入力します。

a) [Name] フィールドに SNMP 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）、-（ハイフン）も指定できます。
（注） ローカル側で認証されたユーザ名と同一の SNMP ユーザ名を作成することはできません。
b) [md5] または [sha] をクリックして、認証タイプを選択します。
c) [AES-128] チェックボックスをオンにします。
オンにすると、このユーザに AES-128 暗号化が使用されます。
d) [Password] フィールドにユーザ パスワードを入力します。
e) [Confirm Password] フィールドにユーザ パスワードもう一度入力します。
f) [Privacy Password] フィールドに、このユーザのプライバシー パスワードを入力します。
g) [Confirm Privacy Password] フィールドに、このユーザのプライバシー パスワードをもう一度入力します。
h) [OK] をクリックします。

ステップ 6 [Save] をクリックします。

SNMP ポリシーの削除

SNMP ポリシーは、ドメイン グループ ルート下にあるドメイン グループから削除されます。 ドメイン グループ ルート下の SNMP ポリシーは、削除できません。

SNMP ポリシーを削除すると、そのポリシー内のすべての SNMP トラップおよび SNMP ユーザ設定が削除されます。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 5 [Work] ペインで、[SNMP] をクリックします。

ステップ 6 [Actions] 領域で、[Delete] をクリックします。
削除されたポリシーは、再設定されるまでドメイン グループの親から設定を継承します。

ステップ 7 [Save] をクリックします。

SNMP トラップの削除

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[SNMP] をクリックします。

ステップ 5 [SNMP Traps] 領域で、削除する SNMP トラップを選択し、[Delete] をクリックします。
また、SNMP トラップを右クリックして、そのオプションにアクセスすることもできます。

ステップ 6 [Save] をクリックします。

SNMP ユーザの削除

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[SNMP] をクリックします。

ステップ 5 [SNMP Users] 領域で、削除する SNMP トラップを選択し、[Delete] をクリックします。
また、SNMP ユーザを右クリックして、そのオプションにアクセスすることもできます。

ステップ 6 [Save] をクリックします。

System Event Log

Cisco UCS Central は、グローバル システム イベント ログ（SEL）ポリシーをサポートしています。

システム イベント ログ（SEL）には、過不足の電圧、温度イベント、ファン イベント、BIOS からのイベントなど、ほとんどのサーバ関連イベントが記録されます。 SELは、主にトラブルシューティングのために使用します。 SEL ファイルのサイズは約 40KB で、ファイルがいっぱいになるとそれ以上イベントを記録できません。 新たなイベントを記録できるようにするには、ファイルの中身をクリアする必要があります。 SEL ポリシーを使用して、SEL をリモート サーバにバックアップできます。また、必要に応じて、バックアップ操作後に SEL をクリアすることもできま

す。 バックアップ操作は、特定のアクションに基づいて起動するか、定期的に実行できます。SEL のバックアップやクリアは、手動で行うこともできます。

SEL ポリシーの設定

はじめる前に

ドメイン グループ下で SEL ポリシーを設定する前に、最初にこのポリシーを作成する必要があります。 ドメイン グループ ルート下にあるポリシーは、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

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 5 [Work] ペインで、[Equipment] をクリックします。

ステップ 6 [Work] ペインで、[SEL Policy] タブをクリックします。

ステップ 7 [Actions] 領域で、[Create] をクリックし、該当するすべてのフィールドに入力します。
[Domain Group root] ノード下の [Operational Policies] では、[Create] をクリックして該当するすべてのフィールドに入力する必要はありません。

a) [General] 領域の必須フィールドに入力します。
b) [Backup Configuration] 領域の必須フィールドに入力します。

ステップ 8 [Save] をクリックします。

SEL ポリシーの削除

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 5 [Work] ペインで、[Equipment] をクリックします。

ステップ 6 [Work] ペインで、[SEL Policy] タブをクリックします。

ステップ 7 [Actions] 領域で、[Delete] をクリックします。

削除されたポリシーは、再設定されるまでドメイン グループの親から設定を継承します。

ステップ 8 [Save] をクリックします。

第 4 章

User Management

この章は、次の内容で構成されています。

Cisco UCS Central ユーザ アカウント

ユーザ アカウントは、システムにアクセスするために使用されます。 最大で 128 個のユーザ アカウントを各 Cisco UCS Central ドメインで設定できます。 各ユーザ アカウントには、一意のユーザ名とパスワードが必要です。

ユーザ アカウントは、SSH 公開キーを付けて設定できます。 公開キーは、OpenSSH と SECSH のいずれかの形式で設定できます。

管理者アカウント

Cisco UCS Central には、admin アカウントがあります。 管理者アカウントはデフォルト ユーザ アカウントで、変更や削除はできません。 このアカウントは、システム管理者またはスーパーユーザ アカウントであり、すべての権限が与えられています。 admin アカウントには、デフォルトのパスワードは割り当てられません。初期システム セットアップ時にパスワードを選択する必要があります。

管理者アカウントは常にアクティブで、有効期限がありません。 管理者アカウントを非アクティブに設定することはできません。

ローカル admin ユーザは、認証がリモートに設定されている場合でも、フェールオーバーのためにログインできます。

ローカル認証されたユーザ アカウント

ローカル認証されたユーザ アカウントは、Cisco UCS Central ユーザ データベースを介して認証され、admin 権限または aaa 権限を持つユーザがイネーブルまたはディセーブルにできます。 ローカル ユーザ アカウントがディセーブルになっている場合、ユーザはログインできません。 無効ローカル ユーザ アカウントの設定の詳細は、データベースによって削除されません。 無効ローカルユーザアカウントを再度有効にすると、アカウントはユーザ名とパスワードを含め、既存のコンフィギュレーションで再びアクティブになります。

リモート認証されたユーザ アカウント

リモート認証されたユーザ アカウントは、LDAP を介して認証される Cisco UCS Central ユーザ アカウントです。 Cisco UCS ドメインは、LDAP、RADIUS および TACACS+ をサポートしています。

ユーザがローカル ユーザ アカウントとリモート ユーザ アカウントを同時に保持する場合、ローカル ユーザ アカウントで定義されたロールがリモート ユーザ アカウントに保持された値を上書きします。

ユーザ アカウントの有効期限

ユーザアカウントは、事前に定義した時間に有効期限が切れるように設定できます。 有効期限の時間になると、ユーザ アカウントはディセーブルになります。

デフォルトでは、ユーザ アカウントの有効期限はありません。

（注） ユーザ アカウントに有効期限日付を設定した後は、アカウントの有効期限をなくすよう再設定できません。 ただし、使用できる最新の有効期限日付でアカウントを設定することは可能です。

ユーザ名の作成に関するガイドライン

ユーザ名は、Cisco UCS Central のログイン ID としても使用されます。 Cisco UCS Central ユーザ アカウントにログイン ID を割り当てるときは、次のガイドラインおよび制約事項を考慮してください。

- ログイン ID には、次を含む 1 ～ 32 の文字を含めることができます。
  - 任意の英字
  - 任意の数字
  - _（アンダースコア）
  - -（ダッシュ）
  - .（ドット）

- ログイン ID は、Cisco UCS Central 内で一意である必要があります。
- ログイン ID は、英文字で開始する必要があります。 数字やアンダースコアなどの特殊文字からは開始できません。
- ログイン ID では、大文字と小文字が区別されます。
- すべて数字のログイン ID は作成できません。
- ユーザ アカウントの作成後は、ログイン ID を変更できません。 ユーザ アカウントを削除し、新しいユーザ アカウントを作成する必要があります。

パスワードの作成に関するガイドライン

それぞれのローカル認証されたユーザ アカウントにはパスワードが必要です。 admin、aaa、または domain-group-management 権限を持つユーザは、ユーザ パスワードについてパスワード強度のチェックを実行するように Cisco UCS Central を設定できます。 パスワード強度チェックをイネーブルにすると、各ユーザが強力なパスワードを使用する必要があります。

シスコでは、各ユーザに強力なパスワードを設定することを推奨します。 ローカル認証されたユーザに対してパスワード強度のチェックを有効にした場合、Cisco UCS Central は、次の要件を満たさないパスワードを拒否します。

- 8 ～ 80 文字を含む。
- 次の少なくとも 3 種類を含む。
  - 小文字
  - 大文字
  - 数字
  - 特殊文字
- aaabbb など連続して 3 回を超えて繰り返す文字を含まない。
- ユーザ名と同一、またはユーザ名を逆にしたものではない。
- パスワード ディクショナリ チェックに合格する。 たとえば、パスワードには辞書に記載されている標準的な単語に基づいたものを指定することはできません。
- 次の記号を含まない。$（ドル記号）、?（疑問符）、=（等号）。
- ローカル ユーザ アカウントおよび admin アカウントのパスワードは空白にしない。

ローカル認証されたユーザのパスワード プロファイル

パスワード プロファイルには、Cisco UCS ManagerCisco UCS Central のローカル認証されたユーザすべてのパスワード履歴やパスワード変更間隔プロパティが含まれます。 ローカル認証されたユーザのそれぞれに異なるパスワード プロファイルを指定することはできません。

（注） パスワードプロファイルプロパティを変更するには、admin または aaa 権限を持っている必要があります。 パスワード履歴を除き、これらのプロパティは、admin または aaa 権限を持つユーザに適用されません。

（注） パスワード プロファイル プロパティを変更するには、admin、aaa、または domain-group-management 権限を持っている必要があります。 パスワード履歴を除き、これらのプロパティはこれらの管理権限を持つユーザには適用されません。

パスワード履歴カウント

パスワード履歴のカウントにより、ローカル認証されたユーザが何度も同じパスワードを再利用しないようにすることができます。 このプロパティが設定されている場合、Cisco UCS ManagerCisco UCS Central は、ローカル認証されたユーザによって以前使用された最大 15 個のパスワードを保存します。 パスワードは最近のものから時系列の逆順で格納され、履歴カウントがしきい値に達した場合に、最も古いパスワードだけを再利用可能にします。

あるパスワードが再利用可能になる前に、ユーザはパスワード履歴カウントで設定された数のパスワードを作成して使用する必要があります。 たとえば、パスワード履歴カウントを 8 に設定した場合、ローカル認証されたユーザは最初のパスワードを 9 番目のパスワードが期限切れになった後まで、最初のパスワードを再利用できません。

デフォルトでは、パスワード履歴は 0 に設定されます。 この値は、履歴のカウントをディセーブルにし、ユーザはいつでも前のパスワードを使用できます。

必要に応じて、ローカル認証されたユーザについてパスワード履歴カウントをクリアし、以前のパスワードの再利用をイネーブルにできます。

パスワード変更間隔

パスワード変更間隔は、ローカル認証されたユーザが特定の時間内に行えるパスワード変更回数を制限することができます。 次の表で、パスワード変更間隔の 2 つの設定オプションについて説明します。

間隔の設定	説明	例
パスワード変更不許可	このオプションでは、ローカル認証されたユーザは、パスワードの変更後、指定された時間内にはパスワードを変更できません。 1 ～ 745 時間の変更禁止間隔を指定できます。 デフォルトでは、変更禁止間隔は 24 時間です。	たとえば、ローカル認証されたユーザが 48 時間の間パスワードを変更できないようにする場合、次のように設定します。 • [Change During Interval] をディセーブルに • [No Change Interval] を 48 に

間隔の設定	説明	例
変更間隔内のパスワード変更許可	このオプションは、ローカル認証されたユーザのパスワードを事前に定義された時間内に変更できる最大回数を指定します。 変更間隔を 1 ～ 745 時間で、パスワード変更の最大回数を 0 ～ 10 で指定できます。 デフォルトでは、ローカル認証されたユーザに対して、48 時間間隔内で最大 2 回のパスワード変更が許可されます。	たとえば、ローカル認証されたユーザがパスワードを変更した後 24 時間以内に最大1回の変更を許可する場合、次のように設定します。 • [Change During Interval] をイネーブルに • [Change Count] を 1 に • [Change Interval] を 24 に

変更間隔のパスワード変更の最大数の設定

パスワード プロファイル プロパティを変更するには、admin または aaa 権限を持っている必要があります。 パスワード履歴を除き、これらのプロパティは、admin または aaa 権限を持つユーザに適用されません。

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。

ステップ 2 [Navigation] ペインで、[Access Control] タブをクリックします。

ステップ 3 [Access Control] タブで、[Locally Authenticated Users] をクリックします。

ステップ 4 [Password Profile] 領域で、すべてのフィールドに入力します。

a) [Change During Interval] フィールド で、 をクリックします。

b) [Change Interval] フィールド で、[Change Count] フィールドで指定したパスワード変更回数が有効になる時間の最大数。 を入力します。
この値は、1 ～ 745 時間から自由に設定できます。

たとえば、このフィールドが 48 に設定され、[Change Count] フィールドが 2 に設定されている場合、ローカル認証されたユーザは 48 時間以内に 2 回を超えるパスワード変更を実行することはできません。

c) [Change Count] フィールド で、ローカル認証されたユーザが、[Change Interval] の間に自分のパスワードを変更できる最大回数 を入力します。
この値は、0 ～ 10 から自由に設定できます。

ステップ 5 [Save] をクリックします。

パスワードの変更禁止間隔の設定

パスワード プロファイル プロパティを変更するには、admin または aaa 権限を持っている必要があります。 パスワード履歴を除き、これらのプロパティは、admin または aaa 権限を持つユーザに適用されません。

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。

ステップ 2 [Navigation] ペインで、[Access Control] タブをクリックします。

ステップ 3 [Access Control] タブで、[Locally Authenticated Users] をクリックします。

ステップ 4 [Password Profile] 領域で、すべてのフィールドに入力します。

a) [Change During Interval] フィールド で、 をクリックします。

b) [No Change Interval] フィールド で、ローカル認証されたユーザが、新しく作成されたパスワードを変更する前に待機する時間の最小数 を入力します。
この値は、1 ～ 745 時間から自由に設定できます。

この間隔は、[Change During Interval] プロパティが [Disable] に設定されていない場合、無視されます。

ステップ 5 [Save] をクリックします。

パスワード履歴カウントの設定

パスワード プロファイル プロパティを変更するには、admin または aaa 権限を持っている必要があります。

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。

ステップ 2 [Navigation] ペインで、[Access Control] タブをクリックします。

ステップ 3 [Access Control] タブで、[Locally Authenticated Users] をクリックします。

ステップ 4 [Password Profile] 領域で、ローカル認証されたユーザが、以前 [History Count] フィールド で使用したパスワードを再使用できるようになる前に、作成する必要がある一意のパスワードの数を入力します。
この値は、0 ～ 15 から自由に設定できます。

デフォルトでは、[History Count] フィールドは 0 に設定されます。これは、履歴カウントをディセーブルにし、ユーザはいつでも前に使用されたパスワードを再使用できます。

ステップ 5 [Save] をクリックします。

ローカル認証されたユーザ アカウントの作成

少なくとも、次のユーザを作成することを推奨します。

- サーバ アドミニストレータ アカウント
- ネットワーク アドミニストレータ アカウント
- ストレージ アドミニストレータ

はじめる前に

システムに次のいずれかがある場合は、該当するタスクを実行します。

- リモート認証サービス：ユーザがリモート認証サーバに存在すること、および適切なロールと権限を持っていることを確認します。
- 組織のマルチテナント機能：1 つ以上のロケールを作成します。 ロケールが 1 つもない場合、すべてのユーザはルートに作成され、すべての組織のロールと権限が割り当てられます。
- SSH 認証。SSH キーを取得します。

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。

ステップ 2 [Navigation] ペインで、[Access Control] タブをクリックします。

ステップ 3 [Access Control] タブで、[Locally Authenticated Users] をクリックします。

ステップ 4 [Create Locally Authenticated User] をクリックします。

ステップ 5 [Create Locally Authenticated User] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Login ID] フィールド	ローカルの Cisco UCS Central ユーザのユーザ名。 ログイン ID は次の制約事項を満たす必要があります。 • ログイン ID には、次を含む 1 ～ 32 の文字を含めることができます。 ◦ 任意の英字 ◦ 任意の数字 ◦ _（アンダースコア） ◦ -（ダッシュ） ◦ .（ドット） • ログイン ID は、Cisco UCS ManagerCisco UCS Central 内で一意である必要があります。 • ログイン ID は、英文字で開始する必要があります。 数字やアンダースコアなどの特殊文字からは開始できません。 • ログイン ID では、大文字と小文字が区別されます。 • すべて数字のログイン ID は作成できません。 • ユーザ アカウントの作成後は、ログイン ID を変更できません。 ユーザ アカウントを削除し、新しいユーザ アカウントを作成する必要があります。
[Description] フィールド	ユーザ アカウントの説明。 256 文字以下で入力します。`（アクセント記号）、\（バックスラッシュ）、^（キャラット）、"（二重引用符）、=（等号）、>（大なり記号）、<（小なり記号）、および'（一重引用符）以外のすべての文字またはスペースを使用できます。
[First Name] フィールド	ユーザの名。 32 文字までの文字またはスペースを入力します。
[Last Name] フィールド	ユーザの姓。 32 文字までの文字またはスペースを入力します。
[Email] フィールド	ユーザの電子メール アドレス。
[Phone] フィールド	ユーザの電話番号。

名前	説明
[Password] フィールド	このアカウントに関連付けられているパスワード。 パスワード強度のチェックボックスをオンにした場合、ユーザ パスワードを強くする必要があります。 強力なパスワードは、次の要件を満たす必要があります。 • 8 ～ 80 文字を含む。 • 次の少なくとも 3 種類を含む。 ◦ 小文字 ◦ 大文字 ◦ 数字 ◦ 特殊文字 • aaabbb など連続して 3 回を超えて繰り返す文字を含まない。 • ユーザ名と同一、またはユーザ名を逆にしたものではない。 • パスワード ディクショナリ チェックに合格する。 たとえば、パスワードには辞書に記載されている標準的な単語に基づいたものを指定することはできません。 • 次の記号を含まない。$（ドル記号）、?（疑問符）、=（等号）。 • ローカル ユーザ アカウントおよび admin アカウントのパスワードは空白にしない。
[Set] フィールド	このユーザにパスワードが設定済みかどうか。
[Confirm Password] フィールド	確認のためのパスワードの再入力。
[Account Expiration] チェックボックス	オンにすると、このアカウントは期限切れになり、[Expiration Date] フィールドに指定した日付以降に使用できなくなります。
[Account Status] ドロップダウンリスト	ステータスが [Active] に設定されている場合、ユーザはこのログイン ID とパスワードを使用して Cisco UCS Central にログインできます。

名前	説明
[Expiration Date] フィールド	アカウントの期限が切れる日付。 日付の形式は yyyy-mm-dd です。 このフィールドの終端にあるカレンダーアイコンをクリックするとカレンダーが表示され、それを使用して期限日を選択できます。

ステップ 6 [Create Locally Authenticated User] ダイアログボックスで、[Roles/Locales] タブをクリックし、次のフィールドに値を入力します。

名前	説明
[Assigned Roles] リスト ボックス	Cisco UCS Central に定義されているユーザ ロールのリスト。 選択したユーザに割り当てられているユーザ ロールは、関連付けられたチェックボックスがオンになっています。
[Assigned Locales] リスト ボックス	Cisco UCS Central に定義されているロケールのリスト。 選択したユーザに割り当てられているロケールは、関連付けられたチェックボックスがオンになっています。

ステップ 7 （任意） システムに組織が含まれている場合は、[Assigned Role(s)] ペインの 1 つ以上のチェックボックスをオンにして、ユーザを適切なロケールに割り当てます。

（注） admin または aaa ロールを持つユーザにロケールを割り当てないでください。

ステップ 8 [Create Locally Authenticated User] ダイアログボックスで、[SSH] タブをクリックし、次のフィールドに値を入力します。

名前	説明
[Type] フィールド	次のいずれかになります。 • [Key]：このユーザがログインするときに、SSH 暗号化が使用されます。 • [Password]：ユーザはログイン時にパスワードを入力する必要があります。
[SSH Data] フィールド	[Type] を [Key] に設定すると、関連付けられた SSH キーがこのフィールドに表示されます。

ステップ 9 [OK] をクリックします。

予約語：ローカル認証されたユーザ アカウント

Cisco UCS および Cisco UCS Central でローカル ユーザ アカウントを作成する場合は、次の単語を使用できません。

- root
- bin
- daemon
- adm
- ip
- sync
- shutdown
- halt
- news
- uucp
- operator
- games
- gopher
- nobody
- nscd
- mailnull
- mail
- rpcuser
- rpc
- mtsuser
- ftpuser
- ftp
- man
- sys
- samdme
- debug

ローカルに認証されたユーザ アカウントの削除

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。
ステップ 2 [Navigation] ペインで、[Access Control] タブをクリックします。
ステップ 3 [Access Control] タブで、[Locally Authenticated Users] を展開します。
ステップ 4 削除する [User] を右クリックし、[Delete] を選択します。
ステップ 5 [Confirm] ダイアログボックスで、[Yes] をクリックします。

ローカル認証されたユーザ アカウントのイネーブル化

ローカルユーザ アカウントを有効または無効にするには、ユーザが admin または aaaadmin、aaa、または domain-group-management 権限を持っている必要があります。

はじめる前に

ローカル ユーザ アカウントを作成します。

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。
ステップ 2 [Navigation] ペインで、[Access Control] タブをクリックします。
ステップ 3 [Access Control] タブで、[Locally Authenticated Users] を展開します。
ステップ 4 修正するユーザ アカウントをクリックします。
ステップ 5 [Work] ペインの [General] タブをクリックします。
ステップ 6 [Account Status] フィールドで、[active] オプション ボタンをクリックします。
ステップ 7 [Save] をクリックします。

ローカル認証されたユーザ アカウントのディセーブル化

ローカルユーザ アカウントを有効または無効にするには、ユーザが admin または aaaadmin、aaa、または domain-group-management 権限を持っている必要があります。

（注） Cisco UCS Manager GUICisco UCS Central GUI を介してディセーブル化されたアカウントのパスワードを変更した場合、アカウントをイネーブルにしてアクティブ化した後、ユーザはこの変更されたパスワードを使用できません。 アカウントをイネーブル化してアクティブ化した後に、必要なパスワードを再び入力する必要があります。

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。

ステップ 2 [Navigation] ペインで、[Access Control] タブをクリックします。

ステップ 3 [Access Control] タブで、[Locally Authenticated Users] を展開します。

ステップ 4 修正するユーザ アカウントをクリックします。

ステップ 5 [Work] ペインの [General] タブをクリックします。

ステップ 6 [Account Status] フィールドで、[inactive] オプション ボタンをクリックします。
admin ユーザ アカウントは常にアクティブに設定されます。 変更はできません。

ステップ 7 [Save] をクリックします。

ローカル認証されたユーザアカウントに割り当てられたロールの変更

ユーザ ロールと権限の変更は、次回ユーザがログインするまで有効になりません。 ユーザ アカウントへの新しいロールの割り当てや既存のロールの削除を行うときにユーザがログインしている場合、アクティブなセッションは以前のロールや権限を引き続き使用します。

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。

ステップ 2 [Navigation] ペインで、[Access Control] タブをクリックします。

ステップ 3 [Access Control] タブで、[Locally Authenticated Users] を展開します。

ステップ 4 修正するユーザ アカウントをクリックします。

ステップ 5 [Work] ペインの [General] タブをクリックします。

ステップ 6 [Work] ペインで、[Roles/Locales] タブをクリックします。

ステップ 7 [Assigned Role(s)] 領域で、ロールの割り当ておよび削除を行います。

- ユーザ アカウントに新しいロールを割り当てるには、適切なチェックボックスをオンにします。

- ユーザ アカウントからロールを削除するには、適切なチェックボックスをオフにします。

ステップ 8 [Save] をクリックします。

ローカル認証されたユーザへのパスワード強度チェックのイネーブル化

パスワードの強度の確認を有効にするには、ユーザが admin または aaaadmin、aaa、または domain-group-management 権限を持っている必要があります。 パスワードの強度の確認が有効になっている場合、Cisco UCS ManagerCisco UCS Central では、強力なパスワードのガイドラインを満たしていないパスワードを選択できません。

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。

ステップ 2 [Navigation] ペインで、[Access Control] タブをクリックします。

ステップ 3 [Access Control] タブで、[Locally Authenticated Users] をクリックします。

ステップ 4 [Work] ペインで、[Properties] 領域の [Password Strength Check] チェックボックスをオンにします。

ステップ 5 [Save] をクリックします。

ローカル認証されたユーザのパスワード履歴のクリア

パスワードプロファイルプロパティを変更するには、admin、aaa、または domain-group-management 権限を持っている必要があります。

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。

ステップ 2 [Navigation] ペインで、[Access Control] タブをクリックします。

ステップ 3 [Access Control] タブで、[Locally Authenticated Users] をクリックします。

ステップ 4 [Password Profile] 領域に、ローカルで認証されたユーザが [History Count][History Count] フィールドフィールドで以前に使用したパスワードを再利用するために作成する必要がある一意のパスワードの数として 0 を入力します。
[History Count] フィールドを 0（デフォルト設定）に設定すると、履歴カウントがディセーブルになり、ユーザは以前に使用したパスワードをいつでも再使用できるようになります。

ステップ 5 [Save] をクリックします。

ユーザ アカウントの Web セッション制限

Web セッション制限は、指定されたユーザ アカウントに対してある 1 つの時点で許容される Web セッション数（GUI と XML の両方）の制限のため Cisco UCS Manager に使用されます。

各 Cisco UCS Manager ドメインは、ユーザ 1 人につき同時 Web セッションを最大 32 件、合計 256 件のユーザ セッションをサポートします。 デフォルトでは、Cisco UCS Manager が許容する同時 Web セッションはユーザ 1 人あたり 32 に設定されます。ただし、この値は最大でシステム上限である 256 まで設定できます。

Cisco UCS Central は、この時点では、複数の同時 Web セッションの管理をサポートしていません。 Cisco UCS Central ユーザに対して 32 個の同時 Web セッションをサポートし、またすべてのユーザでは合計 256 個の同時セッションをサポートします。

ユーザ セッションのモニタリング

CLI と GUI のどちらでログインしているかに関係なく、ローカル認証されたユーザとリモート認証されたユーザの両方について、Cisco UCS Central セッションをモニタできます。

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。

ステップ 2 [Access Control] タブで、[Locally Authenticated Users] または [Remotely Authenticated Users] をクリックします。

ステップ 3 ユーザ セッションは、[Navigation] ペインで、すべてのユーザまたは各ユーザに関して [Locally Authenticated Users] 下でモニタされます。

- [Navigation] ペインで、[Locally Authenticated Users] をクリックして、すべてのユーザ セッションをモニタします。
- [Navigation] ペインで、[Locally Authenticated Users] ノードを展開し、ユーザ名をクリックして個々のユーザをモニタします。

ステップ 4 [Work] ペインで [Sessions] タブをクリックします。
このタブには、ユーザ セッションに関する次の詳細情報が表示されます。

名前	説明
[Filter] ボタン	テーブル内のデータをフィルタリングできます。 フィルタを適用すると、このボタン名は [Filter (on)] に変わります。

名前	説明
[Terminate Session] ボタン	選択したユーザのセッションを終了します。
[Host] カラム	ユーザのログイン元である IP アドレス。
[Login Time] カラム	ユーザがログインした日時。
[Terminal Type] カラム	ユーザのログイン元であるターミナルのタイプ
[Current Session] カラム	セッションが現在アクティブかどうか。

ロールベース アクセス コントロール

ロールベース アクセス コントロール（RBAC）は、ユーザのロールとロケールに基づいてユーザのシステムアクセスを制限または許可する方法です。 ロールによってシステム内でのユーザの権限が定義され、ロケールによってユーザがアクセス可能な組織（ドメイン）が定義されます。 権限がユーザに直接割り当てられることはないため、個々のユーザ権限の管理では、適切なロールとロケールを割り当てることが主な作業になります。

必要なシステム リソースへの書き込みアクセス権限がユーザに与えられるのは、割り当てられたロールによりアクセス権限が与えられ、割り当てられたロケールによりアクセスが許可されている場合に限ります。 たとえば、エンジニアリング組織内のサーバ管理者ロールを持つユーザは、エンジニアリング組織内のサーバ設定を更新できますが、そのユーザに割り当てられたロケールに財務組織が含まれていなければ、財務組織内のサーバ設定を更新できません。

ユーザ ロール

ユーザ ロールには、ユーザに許可される操作を定義する 1 つ以上の権限が含まれます。 各ユーザに 1 つ以上のロールを割り当てることができます。 複数のロールを持つユーザは、割り当てられたすべてのロールを組み合わせた権限を持ちます。 たとえば、Role1 にストレージ関連の権限が含まれ、Role2 にサーバ関連の権限が含まれている場合、Role1 と Role2 の両方を持つユーザは、ストレージ関連の権限とサーバ関連の権限を持つことになります。

Cisco UCS ドメインは、デフォルトのユーザ ロールを含めて、最大 48 個のユーザ ロールを持つことができます。 最初の 48 個の後に設定されたユーザ ロールは受け入れられますが、非アクティブであり障害が上げられます。Cisco UCS Central の各ドメイン グループは、親ドメイン グループから継承したユーザ ロールを含めて、48 個のユーザ ロールを持つことができます。 ユーザ ロールが Cisco UCS Central からCisco UCS Manager にプッシュされると、最初の 48 個のロールだけがアクティブになります。 最初の 48 個より後のユーザ ロールは、非アクティブであり障害が上げられます。

すべてのロールには、Cisco UCS ドメイン内のすべての設定に対する読み取りアクセス権限が含まれています。 読み取り専用ロールを持つユーザは、システム状態を変更できません。

ロールは、作成、変更（新しい権限の追加や既存の権限の削除）、および削除できます。 ロールを変更すると、そのロールを持つすべてのユーザに新しい権限が適用されます。 権限の割り当ては、デフォルトロールに定義されている権限に限定されません。 つまり、カスタムの権限の組み合わせを使用して、独自のロールを作成できます。 たとえば、デフォルトのサーバアドミニストレータ ロールとストレージ アドミニストレータ ロールの持つ権限の組み合わせは異なっていますが、両方のロールの権限を組み合わせた新しい 1 つのサーバおよびストレージ アドミニストレータ ロールを作成できます。

ロールがユーザへの割り当て後に削除されると、それらのユーザ アカウントからも削除されます。

AAA サーバ（RADIUS または TACACS+）上のユーザ プロファイルは、そのユーザに与える権限に対応したロールを追加するように変更する必要があります。 属性はロール情報を保存するために使用されます。 AAA サーバでは、要求とともにこの属性が返され、それを解析してロールが得られます。 LDAP サーバでは、ユーザ プロファイル属性内のロールが返されます。

（注） ローカル ユーザ アカウントとリモート ユーザ アカウントに同じユーザ名がある場合、リモート ユーザに割り当てられたすべての役割は、ローカル ユーザに割り当てられた内容で上書きされます。

デフォルト ユーザ ロール

システムには、次のデフォルトのユーザ ロールが用意されています。

AAA アドミニストレータ

ユーザ、ロール、および AAA 設定に対する読み取りと書き込みのアクセス権。 システムの残りの部分に対する読み取りアクセス権。

管理者

システム全体に対する完全な読み取りと書き込みのアクセス権。 デフォルトの admin アカウントは、デフォルトでこのロールが割り当てられ、変更はできません。

ファシリティ マネージャ

power-mgmt 権限による、電源管理操作に対する読み取りと書き込みのアクセス。 システムの残りの部分に対する読み取りアクセス権。

ネットワーク アドミニストレータ

ファブリック インターコネクト インフラストラクチャとネットワーク セキュリティ操作に対する読み取りと書き込みのアクセス権。 システムの残りの部分に対する読み取りアクセス権。

動作

システムのログ（syslogサーバを含む）と障害に対する読み取りと書き込みのアクセス権。システムの残りの部分に対する読み取りアクセス権。

Read-Only

システム設定に対する読み取り専用アクセス権。システム状態を変更する権限はありません。

Server Compute

サービス プロファイルのほとんどの側面に対する読み取りと書き込みのアクセス権。 ただし、ユーザは vNIC または vHBA を作成、変更、または削除できません。

サーバ機器アドミニストレータ

物理サーバ関連の操作に対する読み取りと書き込みのアクセス権。 システムの残りの部分に対する読み取りアクセス権。

サーバ プロファイル アドミニストレータ

論理サーバ関連の操作に対する読み取りと書き込みのアクセス権。 システムの残りの部分に対する読み取りアクセス権。

サーバ セキュリティ アドミニストレータ

サーバ セキュリティ関連の操作に対する読み取りと書き込みのアクセス権。 システムの残りの部分に対する読み取りアクセス権。

ストレージ アドミニストレータ

ストレージ操作に対する読み取りと書き込みのアクセス権。 システムの残りの部分に対する読み取りアクセス権。

権限

ユーザ ロールを割り当てられたユーザは、権限により、特定のシステム リソースへアクセスしたり、特定のタスクを実行したりできるようになります。 次の表に、各権限と、その権限がデフォルトで与えられるユーザ ロールのリストを示します。

ヒント　これらの権限および権限によってユーザが実行できるようになるタスクの詳細情報は、『*Privileges in Cisco UCS*』は、次の URL で入手可能です。http://preview.cisco.com/en/US/products/ps10281/prod_technical_reference_list.html で利用可能です。

表 *3*：ユーザの権限

特権	説明	デフォルトのロール割り当て
aaa	システム セキュリティおよび AAA	AAA アドミニストレータ
admin	システム管理	管理者
domain-group-management	ドメイン グループ管理	ドメイン グループ管理者
ext-lan-config	外部 LAN 設定	ネットワーク アドミニストレータ
ext-lan-policy	外部 LAN ポリシー	ネットワーク アドミニストレータ
ext-lan-qos	外部 LAN QoS	ネットワーク アドミニストレータ
ext-lan-security	外部 LAN セキュリティ	ネットワーク アドミニストレータ
ext-san-config	外部 SAN 設定	ストレージアドミニストレータ
ext-san-policy	外部 SAN ポリシー	ストレージアドミニストレータ
ext-san-qos	外部 SAN QoS	ストレージアドミニストレータ
ext-san-security	外部 SAN セキュリティ	ストレージアドミニストレータ
fault	アラームおよびアラーム ポリシー	動作
operations	ログおよび Smart Call Home	動作
org-management	組織管理	動作
pod-config	ポッド設定	ネットワーク アドミニストレータ
pod-policy	ポッド ポリシー	ネットワーク アドミニストレータ
pod-qos	ポッド QoS	ネットワーク アドミニストレータ

特権	説明	デフォルトのロール割り当て
pod-security	ポッド セキュリティ	ネットワーク アドミニストレータ
power-mgmt	電源管理操作に対する読み取りと書き込みのアクセス	ファシリティ マネージャ
read-only	読み取り専用アクセス権 読み取り専用は、権限として選択できません。この権限は、すべてのユーザ ロールに割り当てられます。	Read-Only
server-equipment	サーバ ハードウェア管理	サーバ機器アドミニストレータ
server-maintenance	サーバ メンテナンス	サーバ機器アドミニストレータ
server-policy	サーバ ポリシー	サーバ機器アドミニストレータ
server-security	サーバ セキュリティ	サーバセキュリティ アドミニストレータ
service-profile-compute	サービス プロファイルの計算	サーバ計算アドミニストレータ
service-profile-config	サービス プロファイル設定	サーバプロファイルアドミニストレータ
service-profile-config-policy	サービスプロファイル設定ポリシー	サーバプロファイルアドミニストレータ
service-profile-ext-access	サービス プロファイル エンドポイント アクセス	サーバプロファイルアドミニストレータ
service-profile-network	サービス プロファイル ネットワーク	ネットワーク アドミニストレータ
service-profile-network-policy	サービス プロファイル ネットワーク ポリシー	ネットワーク アドミニストレータ
service-profile-qos	サービス プロファイル QoS	ネットワーク アドミニストレータ
service-profile-qos-policy	サービス プロファイル QoS ポリシー	ネットワーク アドミニストレータ

特権	説明	デフォルトのロール割り当て
service-profile-security	サービス プロファイル セキュリティ	サーバセキュリティアドミニストレータ
service-profile-security-policy	サービス プロファイル セキュリティ ポリシー	サーバセキュリティアドミニストレータ
service-profile-server	サービス プロファイル サーバ管理	サーバプロファイルアドミニストレータ
service-profile-server-oper	サービス プロファイル コンシューマ	サーバプロファイルアドミニストレータ
service-profile-server-policy	サービス プロファイル プールポリシー	サーバセキュリティアドミニストレータ
service-profile-storage	サービスプロファイルストレージ	ストレージアドミニストレータ
service-profile-storage-policy	サービスプロファイルストレージ ポリシー	ストレージアドミニストレータ
stats	統計情報管理	統計情報の管理者

ユーザ ロールの作成

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、ユーザ ロールのドメイン グループを選択します。

a) [Domain Groups] ノードを展開します。

b) [Domain Groups root] ノードを展開します。

ステップ 3 [Domain Groups] ノード下で、次のいずれかを選択して実行します。

- [Operational Policies] をクリックします。
- [Domain Group] ノードを展開し、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[Roles] に移動します。

a) [Security] をクリックします。

b) [User Services] ノードを展開します。

c) [Roles] をクリックします。

ステップ 5 [Create Role] をクリックします。
また、[Roles] を右クリックして、そのオプションにアクセスすることもできます。

ステップ 6 [Create Role] ダイアログボックスで、ロールを割り当てる [Name] を入力します。

ステップ 7 ロールのすべての [Privileges] を選択します。

ステップ 8 [OK] をクリックします。

予約語：ユーザ ロール

次の単語は、Cisco UCS でカスタム ロールを作成するときに使用できません。

- network-admin
- network-operator
- vdc-admin
- vdc-operator
- server-admin

ユーザ ロールの削除

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、ユーザ ロールのドメイン グループを選択します。

a) [Domain Groups] ノードを展開します。
b) [Domain Groups root] ノードを展開します。

ステップ 3 [Domain Groups] ノード下で、次のいずれかを選択して実行します。

- [Operational Policies] をクリックします。
- [Domain Group] ノードを展開し、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、すべてのロールを表示します。

a) [Security] をクリックします。
b) [User Services] ノードを展開します。
c) [Roles] ノードを展開します。

ステップ 5 削除するロールをクリックします。

ステップ 6 [Delete] をクリックします。

また、[Role] を右クリックして、そのオプションにアクセスすることもできます。

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

ユーザ ロールへの権限の追加

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、ユーザ ロールのドメイン グループを選択します。

a) [Domain Groups] ノードを展開します。
b) [Domain Groups root] ノードを展開します。

ステップ 3 [Domain Groups] ノード下で、次のいずれかを選択して実行します。

- [Operational Policies] をクリックします。
- [Domain Group] ノードを展開し、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、すべてのロールを表示します。

a) [Security] をクリックします。
b) [User Services] ノードを展開します。
c) [Roles] ノードを展開します。

ステップ 5 権限を追加するロールを選択します。

ステップ 6 [Properties] をクリックします。
また、[Role] を右クリックして、そのオプションにアクセスすることもできます。

ステップ 7 [Properties] ダイアログボックスで、ロールに追加する権限に対応するチェックボックスをオンにします。

ステップ 8 [Save Changes] をクリックします。

ユーザ ロールからの権限の削除

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、ユーザ ロールのドメイン グループを選択します。

a) [Domain Groups] ノードを展開します。
b) [Domain Groups root] ノードを展開します。

ステップ 3 [Domain Groups] ノード下で、次のいずれかを選択して実行します。

- [Operational Policies] をクリックします。
- [Domain Group] ノードを展開し、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、すべてのロールを表示します。

a) [Security] をクリックします。
b) [User Services] ノードを展開します。
c) [Roles] ノードを展開します。

ステップ 5 権限を削除するロールを選択します。

ステップ 6 [Properties] をクリックします。
また、[Role] を右クリックして、そのオプションにアクセスすることもできます。

ステップ 7 [Properties] ダイアログボックスで、ロールから削除する権限に対応するボックスをオフにします。

ステップ 8 [Save Changes] をクリックします。

ユーザ ロケール

ユーザには、ロケールを 1 つ以上割り当てることができます。 各ロケールには、ユーザからのアクセスを許可する 1 つ以上の組織（ドメイン）を定義します。アクセスは、このロケールで指定された組織の範囲内に制限されます。 このルールの 1 つの例外として、組織が指定されていないロケールがあります。この場合、すべての組織内のシステム リソースに対して無制限のアクセスが可能になります。

Cisco UCS ドメインは、最大 48 個のユーザ ロケールを持つことができます。 最初の 48 個より後に設定されたユーザ ロケールは、非アクティブであり障害が上げられます。 Cisco UCS Central の各ドメイン グループは、親ドメイン グループから継承されたユーザ ロケールを含めて、48 個のユーザ ロケールを持つことができます。 Cisco UCS Central からユーザ ロケールが Cisco UCS Manager にプッシュされると、最初の 48 個のロケールだけがアクティブになります。 最初の 48 個より後のユーザ ロケールは、非アクティブであり障害が上げられます。

admin または aaaadmin、aaa、または domain-group-management の権限を持つユーザは、組織をその他のユーザのロケールに割り当てることができます。 組織の割り当ては、それを行うユーザのロケール内の組織だけに制限されます。 たとえば、ロケールにエンジニアリング組織しか含まれていない場合、そのロケールを割り当てられたユーザは、他のユーザにエンジニアリング組織のみを割り当てることできます。

（注） admin 権限を持つユーザにロケールを割り当てることはできません。

（注） ロケールを次の権限の 1 つ以上を持つユーザに割り当てることはできません。

- aaa
- admin
- fault
- operations

組織は階層的に管理できます。トップ レベルの組織に割り当てられたユーザは、自動的にその下にあるすべての組織にアクセスできます。たとえば、エンジニアリング組織が、ソフトウェアエンジニアリング組織とハードウェア エンジニアリング組織で構成されているとします。 ソフトウェアエンジニアリング組織のみを含むロケールでは、その組織内のシステムリソースにしかアクセスできません。一方、エンジニアリング組織が含まれるロケールでは、ソフトウェア エンジニアリング組織とハードウェア エンジニアリング組織の両方のリソースにアクセスできます。

ユーザ ロケールの作成

はじめる前に

ロケールを作成するには、1 つ以上の組織が存在する必要があります。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、ロケールのドメイン グループを選択します。

a) [Domain Groups] ノードを展開します。
b) [Domain Groups root] ノードを展開します。

ステップ 3 [Domain Groups] ノード下で、次のいずれかを実行します。

- [Operational Policies] をクリックします。
- [Domain Group] ノードを展開し、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[Locales] に移動します。

a) [Security] をクリックします。
b) [User Services] ノードを展開します。
c) [Locales] をクリックします。

ステップ 5 [Create Locales] をクリックします。
また、[Locales] を右クリックしてそのオプションにアクセスすることもできます。

ステップ 6 [Create Locale] ダイアログボックスで、要求された情報を入力します。

a) [Name] フィールドに、ロケールの一意の名前を入力します。
この名前には、1～32 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。

b) [Description] フィールドにロケールの説明を入力します。

ステップ 7 [Filter] をクリックします。

ステップ 8 [Table Filter] ダイアログボックスで、要求された情報を入力します。

a) [Assigned Organization] フィルタを選択します。
b) [Assigned Organization] フィルタの値を入力します。

ステップ 9 [OK] をクリックします。

ステップ 10 [Assign Organization] をクリックします。

ステップ 11 [Assign Organizations] ダイアログボックスで、組織をロケールに割り当てます。

a) [Organizations] 領域を展開して、Cisco UCS ドメイン内の組織を表示します。
b) [root] ノードを展開して、サブ組織を表示します。
c) ロケールを割り当てる組織をクリックします。
d) [Organizations] 領域の組織を右側のペインの設計領域にドラッグ アンド ドロップします。
e) すべての適切な組織をロケールに割り当てるまで、ステップ b および c を繰り返します。

ステップ 12 [OK] をクリックして組織を割り当てます。

ステップ 13 [OK] をクリックしてロケールを作成します。

ユーザ ロケールの削除

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、ロケールのドメイン グループを選択します。

a) [Domain Groups] ノードを展開します。
b) [Domain Groups root] ノードを展開します。

ステップ 3 [Domain Groups] ノード下で、次のいずれかを実行します。

- [Operational Policies] をクリックします。
- [Domain Group] ノードを展開し、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、すべてのロケールを表示します。

a) [Security] をクリックします。
b) [User Services] ノードを展開します。

c) [Locales] ノードを展開します。

ステップ 5 削除するロケールをクリックします。

ステップ 6 [Delete] をクリックします。
また、削除する [Locale] を右クリックして、そのオプションにアクセスすることもできます。

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

ユーザ ロケールへの組織の割り当て

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、ロケールのドメイン グループを選択します。

a) [Domain Groups] ノードを展開します。
b) [Domain Groups root] ノードを展開します。

ステップ 3 [Domain Groups] ノード下で、次のいずれかを実行します。

- [Operational Policies] をクリックします。
- [Domain Group] ノードを展開し、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインでロケールを選択します。

a) [Security] をクリックします。
b) [User Services] ノードを展開します。
c) [Locales] ノードを展開します。

ステップ 5 組織を追加するロケールをクリックします。

ステップ 6 [Assign Organization] をクリックします。
また、[Locale] を右クリックして、そのオプションにアクセスすることもできます。

ステップ 7 [Assign Organizations] ダイアログボックスで、[Organization] を入力します。

ステップ 8 [OK] をクリックします。

ユーザ ロケールからの組織の削除

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、ロケールのドメイン グループを選択します。

a) [Domain Groups] ノードを展開します。

b) [Domain Groups root] ノードを展開します。

ステップ 3 [Domain Groups] ノード下で、次のいずれかを実行します。

- [Operational Policies] をクリックします。
- [Domain Group] ノードを展開し、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、すべてのロケールを表示します。

a) [Security] をクリックします。

b) [User Services] ノードを展開します。

c) [Locales] ノードを展開します。

ステップ 5 削除する組織が割り当てられたロケールをクリックします。

ステップ 6 [Properties] をクリックします。

ステップ 7 [Work] ペインで、削除する [Organization] をクリックします。

ステップ 8 [Delete] をクリックします。
また、削除する [Organization] を右クリックして、そのオプションにアクセスすることもできます。

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

ローカル認証されたユーザアカウントに割り当てられたロケールの変更

（注） admin または aaa ロールを持つユーザにロケールを割り当てないでください。

手順

ステップ 1 メニュー バーで、[Administration] をクリックします。

ステップ 2 [Navigation] ペインで、[Access Control] タブをクリックします。

ステップ 3 [Access Control] タブで、[Locally Authenticated Users] を展開します。

ステップ 4 修正するユーザ アカウントをクリックします。

ステップ 5 [Work] ペインの [General] タブをクリックします。

ステップ 6 [Work] ペインで、[Roles/Locales] タブをクリックします。

ステップ 7 [Assigned Locale(s)] 領域で、ロケールの割り当ておよび削除を行います。

- ユーザ アカウントに新しいロケールを割り当てるには、適切なチェックボックスをオンにします。
- ユーザ アカウントからロケールを削除するには、適切なチェックボックスをオフにします。

ステップ 8 [Save] をクリックします。

ユーザ組織

ユーザは、1 つ以上の組織を作成できます。 各組織では、サブ組織、障害、イベント、UUID 接尾辞プール、および UUID のブロックが定義されます。

Cisco UCS 組織 は、ユーザによって階層的に管理されます。 ルート レベルの組織に割り当てられたユーザは、自動的にすべての組織およびその下にあるドメイン グループにアクセスできます。

ユーザ組織の作成

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、組織を作成します。

a) [Pools] ノードを展開します。

b) [root] をクリックします。

c) [Work] ペインで、[Create Organization] をクリックします。

ステップ 3 [Create Organization] ダイアログボックスで、要求された情報を入力します。

a) [Name] フィールドに、組織の一意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）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。

b) [Description] フィールドに、組織の説明を入力します。

ステップ 4 [OK] をクリックして組織を作成します。

ユーザ組織の削除

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、組織を選択します。

a) [Pools] ノードを展開します。
b) [root] ノードを展開します。
c) [Sub-Organizations] をクリックします。
d) [Sub-Organizations] ペインで、削除する [Organization] をクリックします。

ステップ 3 [Delete] をクリックします。
また、削除する [Organization] を右クリックして、そのオプションにアクセスすることもできます。

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

ユーザのサブ組織の作成

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、サブ組織を作成します。

a) [Pools] ノードを展開します。
b) [root] ノードを展開します。
c) [Sub-Organizations] をクリックします。

ステップ 3 [Sub-Organizations] ペインで、該当する割り当てられた組織名をクリックします。

ステップ 4 [Work] ペインで、[Create Organization] をクリックします。

ステップ 5 [Create Organization] ダイアログボックスで、要求された情報を入力します。

a) [Name] フィールドに、組織の一意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）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。

b) [Description] フィールドに、組織の説明を入力します。

ステップ 6 [OK] をクリックしてサブ組織を作成します。

ユーザのサブ組織の削除

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、組織を選択します。

a) [Pools] ノードを展開します。
b) [root] ノードを展開します。
c) [Sub-Organizations] をクリックします。
d) [Sub-Organizations] ペインで、該当する割り当てられた組織ノードを展開します。
e) [Sub-Organizations] ペインで、削除する [Organization] をクリックします。
該当する組織名に到達するまで、該当する割り当てられた組織ノードを展開します。

ステップ 3 [Delete] をクリックします。
また、削除するターゲットに到達するまで [Organizations] を展開し、[Organization] を右クリックしてそのオプションにアクセスすることもできます。

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

第 5 章

Firmware Management

この章は、次の内容で構成されています。

シスコからのファームウェアのダウンロード

Cisco UCS Central では、指定された間隔でシスコの Web サイトと通信してファームウェア イメージのリストを取得するように、ファームウェアのダウンロードを設定できます。 イメージのダウンロード用にシスコのクレデンシャルを設定した後に、リフレッシュを行うと、Cisco UCS Central によって Cisco.com から使用可能なイメージ データが取得され、ファームウェア イメージ ライブラリにファームウェア イメージが表示されます。 ファームウェア イメージのバージョンを使用してポリシーを作成する場合、または [Store Locally] オプションを使用してイメージをダウンロードする場合には、実際のファームウェア イメージをダウンロードできます。

重要 シスコからファームウェアを Cisco UCS Central にダウンロードするには、次の作業を行ってください。

- Cisco UCS Central から Cisco.com に直接またはプロキシ サーバ経由でアクセスできるようにする必要があります。
- 有効なシスコのユーザ クレデンシャルを設定して、Cisco UCS Central でダウンロード状態をイネーブルにする必要があります。

ファームウェアのイメージ ライブラリ

Cisco UCS Central のイメージ ライブラリには、Cisco.com、ローカル ファイル システム、およびリモート ファイル システムから Cisco UCS Central 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。

Cisco.com からダウンロードされたイメージのソースはシスコであり、ローカルまたはリモートのファイルシステムからダウンロードされたイメージのソースはローカルです。 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。

ライブラリからファームウェア イメージを削除するオプションを次に示します。

- **ファームウェア イメージの削除**：削除オプションを使用すると、ファームウェア ライブラリ内のダウンロードされたイメージを削除できます。
- **ファームウェア イメージのメタデータのパージ**：パージ オプションを使用すると、イメージのメタデータを削除できます。 ライブラリからファームウェア イメージを削除した後でも、メタデータは引き続き存在しています。 このメタデータ情報を使用すると、イメージを削除した後でも Cisco.com から実際のファームウェア イメージをいつでもダウンロードすることができます。 ファームウェア イメージ ライブラリからファームウェア イメージと関連するメタデータを完全に削除する場合は、実際のファームウェアイメージを削除し、ライブラリからメタデータをパージしてください。

重要 メタデータに対応するイメージがファームウェア イメージ ライブラリにすでにダウンロードされている場合は、イメージを削除しないでメタデータをパージすることはできません。

シスコからのファームウェアのダウンロードの設定

シスコからのファームウェアのダウンロードを設定すると、Cisco UCS Central によって Cisco.com からファームウェアのメタデータがダウンロードされ、いつでも Cisco UCS Central からダウンロードして保存できるよう、情報が保存されます。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Images] を展開します。

ステップ 3 [Configure Downloads From Cisco] をクリックします。

ステップ 4 [Work] ペインの [General] タブで、フィールドに必須情報を入力します。
Cisco UCS Central がログインに使用する Cisco.com アカウントのユーザ名とパスワードが正しいことを確認してください。

ステップ 5 [Proxy] タブで、プロキシ アカウントの必須情報を入力します。

ステップ 6 [Save] をクリックします。

シスコからのファームウェア イメージのダウンロード

Cisco.com からのファームウェア イメージのダウンロードを設定し、イメージ ライブラリをリフレッシュすると、Cisco UCS Central で使用可能なすべてのファームウェア イメージのメタデータにアクセスできるようになります。 ファームウェア イメージは次の方法でダウンロードできます。

- **ファームウェア ポリシーの作成**：ファームウェア ポリシーを作成し、特定のイメージを選択すると、ファームウェア ポリシーで指定したイメージが Cisco UCS Central によって自動的にダウンロードされます。
- **イメージをローカルに保存**：ローカルに保存するオプションを選択すると、選択したファームウェア イメージが Cisco.com からダウンロードされ、イメージ ライブラリに保存されます。

ここでは、ローカルに保存するオプションを使用してイメージをダウンロードする手順について説明します。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Images] を展開します。

ステップ 3 [Library] をクリックします。

ステップ 4 [Work] ペインで、[Packages] タブをクリックします。
シスコからダウンロードされたイメージのメタデータには、[Source] として [Cisco] が、[State] として [not-downloaded] が指定されています。

ステップ 5 バンドルを右クリックして、オプションから [Store Locally] を選択します。

リモートからのファームウェアのダウンロード

はじめる前に

選択したファイル転送プロトコルをサポートするリモート サーバを設定し、このサーバから Cisco UCS Central へのアクセスを可能にする必要があります。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Images] を展開します。

ステップ 3 [Library] をクリックします。

ステップ 4 [Work] ペインで、[Downloads] タブをクリックします。

ステップ 5 [Downloads] タブで [Download Firmware] をクリックします。

ステップ 6 [Download Firmware] ダイアログボックスの [Location of the Image File] で、[Remote File System] を選択し、必須フィールドに入力します。

ステップ 7 [OK] をクリックします。

ローカル ファイル システムからのファームウェアのダウンロード

はじめる前に

シスコからファームウェア イメージを入手してローカル ファイル システムに保存し、ファームウェアをローカル システムから Cisco UCS Central にダウンロードするよう設定する必要があります。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Images] を展開します。

ステップ 3 [Library] をクリックします。

ステップ 4 [Work] ペインで、[Downloads] タブをクリックします。

ステップ 5 [Downloads] タブで [Download Firmware] をクリックします。

ステップ 6 [Download Firmware] ダイアログボックスの [Location of the Image File] で、[Local File System] を選択します。

ステップ 7 [Download Image into Image Library] をクリックします。
ダイアログボックスにファイルを選択するオプションが表示されます。

ステップ 8 ローカル システムにあるファームウェア ファイルの場所を参照してファイルを選択するには、[Browse] をクリックします。

ステップ 9 [Submit] をクリックします。`
イメージが正常にダウンロードされると、[Firmware Image Download] ダイアログボックスに確認メッセージが表示されます。

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

イメージのダウンロードのエラーの表示

ファームウェア イメージのダウンロード処理のエラーは、同じ [Library of Images] パネルに表示できます。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Images] を展開します。

ステップ 3 [Library] をクリックします。

ステップ 4 [Work] ペインで [Faults] タブをクリックします。
エラーのテーブルに、ダウンロードに関するすべてのエラーと詳細が表示されます。

ライブラリでのファームウェア イメージの表示

ダウンロードされたファームウェア イメージとイメージのメタデータは、[Library of Images] パネルに表示できます。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Images] を展開します。

ステップ 3 [Library] をクリックします。

ステップ 4 [Work] ペインで [Packages] タブをクリックします。
利用可能なパッケージが表示されます。 パッケージを選択して [Properties] をクリックすると、特定のパッケージの詳細を表示できます。

イメージ ライブラリ上のイメージのメタデータの削除

パージ オプションを使用すると、[Library of Images] からファームウェア イメージのメタデータを削除することができます。 パージ オプションでは、すでにダウンロードされたイメージのメタデータだけをクリアします。

（注） 機能カタログ、インフラストラクチャとホストのファームウェア パッケージなど、ファームウェア パッケージのいずれかを削除するには、各ドメイン グループの下にあるファームウェア管理セクション、またはドメイン グループのルートから削除を実行できます。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Images] を展開します。

ステップ 3 [Library] をクリックします。

ステップ 4 [Work] ペインで [Library of Images] から削除するファームウェア イメージのメタデータを選択し、[Purge] をクリックします。

ステップ 5 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。

Cisco UCS ドメインのファームウェアのアップグレード

登録されている Cisco UCS ドメインに対して、インフラストラクチャとサーバのファームウェアのアップグレードを Cisco UCS Central から実行できます。

必要に応じて、各ドメイン グループの Cisco UCS ドメインを異なるバージョンのファームウェアにアップグレードできます。また、 Cisco UCS Central には、ファブリック インターコネクトのリブートを Cisco UCS Central からグローバルに確認するオプション、または各 Cisco UCS ドメインから個別に確認するオプションがあります。

Cisco UCS ドメイン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ル

[Infrastructure Firmware] パネルで、クラシックまたはミニ Cisco UCS ドメインのインフラストラクチャ ファームウェアのアップグレードまたはダウングレードをスケジュールできます。 Cisco UCS ドメインでのファームウェアの管理の詳細については、『Cisco UCS Manager Firmware Management Guides』を参照してください。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Groups Root] > [Firmware Management] を展開します。

ステップ 3 [Infrastructure Firmware] をクリックします。

ステップ 4 [Firmware Version] セクションで、[UCS] または [UCS Mini] のドロップダウンをクリックし、これらのドメインのファームウェア バージョンを選択します。
いずれか 1 つまたは両方を同時に選択できます。 ファームウェア バージョンを選択すると、[Scheduler] オプションが有効になります。 [UCS] と [UCS Mini] の両方でファームウェア バージョンを削除すると、[Scheduler] が無効にリセットされます。

ステップ 5 [Scheduler] セクションで、スケジュールを指定します。
[User Acknowledged] をオンにすると、保留中のアクティビティのパネルにアップグレードがリストされます。 実際のアップグレードは、このアクティビティを手動で確認した後でのみトリガーされます。

ステップ 6 [Save] をクリックして、インフラストラクチャ ファームウェア アップグレード スケジュールを保存します。

保留中のアクティビティの確認

Cisco UCS ドメインのサービス プロファイルでグローバルなメンテナンス ポリシーおよびグローバルなホスト ファームウェア パッケージを使用している場合、Cisco UCS Central にはファームウェア アップグレードを展開する前にユーザの確認を行うオプションがあります。

[User Ack] リブート ポリシーを使用してメンテナンス ポリシーを作成している場合は、Cisco UCS Manager で実際のファームウェア アップグレードを確認する必要があります。 グローバルのスケジュールでメンテナンス ポリシーを作成し、[User Ack] をイネーブルにしている場合は、Cisco UCS Central ですべての Cisco UCS ドメインの実際のアップグレードを確認する必要があります。

（注） 保留中のアクティビティは、[Infrastructure Firmware] セクションおよび [Host Firmware] セクションで表示および確認できます。 ここでは、[Host Firmware] セクションで保留中のアクティビティを確認する手順について説明します。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Groups Root] > [Firmware Management] を展開します。

ステップ 3 [Work] ペインの [Pending Activities] タブをクリックします。

ステップ 4 表示されたリストから保留中のアクティビティを選択し、右クリックして、[Acknowledge] をクリックします。

インフラストラクチャ ファームウェア パッケージの削除

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Groups Root] > [Firmware Management] を展開します。

ステップ 3 [Work]ペインには、作成されたすべてのインフラストラクチャ ファームウェア パッケージのリストが表示されます。

ステップ 4 [Delete] をクリックします。

ステップ 5 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。

ホスト ファームウェア パッケージの作成

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Groups Root] > [Firmware Management] を展開します。

ステップ 3 [Host Firmware] をクリックします。

ステップ 4 [Work] ペインの [Policies] タブで [Create a Pack] をクリックします。

ステップ 5 [Create a Pack] ダイアログボックスで、次のフィールドに入力します。

a) [Name] と [Description] に入力します。

b) [Blade Version] 領域で、ブレード サーバのバージョンを選択します。

c) [Rack Version] 領域で、ラック サーバのバージョンを選択します。

ステップ 6 [Impacted Endpoints] ダイアログボックスに、このホスト ファームウェア ポリシーの影響を受けるエンドポイントのリストが表示されます。
これらのエンドポイントはファームウェアのアップグレード時にリブートされるため、アップグレード処理中の使用は制限されます。

ステップ 7 [OK] をクリックします。

次の作業

Cisco UCS Central で作成したホスト ファームウェア ポリシーは、ドメイン グループに登録された Cisco UCS ドメインのサービス プロファイルへの関連付けに使用できます。

ホスト ファームウェア アップグレードの展開

Cisco UCS Central で定義したすべてのホスト ファームウェア ポリシーを、[Install Servers] を使用して特定の B と C のバンドルに更新できます。

はじめる前に

ホスト ファームウェア パッケージを作成しておく必要があります。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Groups Root] > [Firmware Management] を展開します。

ステップ 3 [Host Firmware] をクリックします。

ステップ 4 [Work] ペインで、表示されるホスト ファームウェア パッケージのリストから展開するファームウェア バージョンを選択します。

ステップ 5 テーブル ヘッダーの [Install Servers] をクリックします。

ステップ 6 [Install Servers] ダイアログボックスで、[Blade Version]、[Rack version]、[Impacted Endpoints] を選択します。

ステップ 7 [Upgrade host Firmware Warning] メッセージ ダイアログボックスで、[Yes] をクリックします。
選択したエンドポイントのサーバでグローバルなホスト ファームウェア アップグレード ポリシーを使用している場合は、ホスト ファームウェア パッケージによってアップグレードされます。

ホスト ファームウェア パッケージの削除

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Groups Root] > [Firmware Management] を展開します。

ステップ 3 [Work] ペインには、作成したすべてのホスト ファームウェア パッケージのリストが表示されます。

ステップ 4 削除するホスト ファームウェア パッケージの名前をクリックして選択します。
テーブル ヘッダーの領域にアクションのアイコンが表示されます。

ステップ 5 [Delete] をクリックします。

ステップ 6 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。

ファームウェア アップグレードのスケジュール

登録された Cisco UCS ドメイン内のドメイン グループのファームウェアをアップグレードするために、Cisco UCS Central から次の方法でアップグレードをスケジュールできます。

- 1 回のオカレンスとして
- 指定間隔で繰り返すオカレンスとして

ユーザの確認を必要とするスケジュールを設定すると、ファブリック インターコネクトは明示的な確認なしではリブートしません。

メンテナンス ポリシーの作成

Cisco UCS Central では、ホスト ファームウェアの更新に対して、次の種類のメンテナンス ポリシーを作成できます。

- **Immediate**：immediate オプションを指定すると、サーバはユーザの確認なしでただちにリブートされます。
- **Timer-automatic**：timer-automatic オプションを指定すると、サーバのリブートは、このメンテナンス ポリシーに対して選択したスケジュールに基づいて実行されます。

重要 timer-automatic オプションを使用する場合は、Cisco UCS Central でスケジュールを作成し、メンテナンス ポリシーで指定する必要があります。 Cisco UCS Central でスケジュールを作成する場合、このスケジュールされたメンテナンス ポリシーは Cisco UCS Central でのみ確認できます。このメンテナンス ポリシーを使用するサーバは、このスケジュールで定義されたメンテナンス時間帯にのみリブートされます。 スケジュールで user-acknowledgment が有効の場合、サーバのリブートを確認する必要があります。

- **User-acknowledgment**：user-acknowledgment オプションを指定すると、サーバをリブートする前に、各 Cisco UCS ドメインの保留中のアクティビティの通知が送信されます。

重要 user-acknowledgment オプションには、Cisco UCS ドメインの管理者が Cisco UCS ドメイン内の個々のサーバを異なる時刻にリブートすることを決定できるオプションがあります。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group Root] > [Maintenance] を展開します。

ステップ 3 [Work] ペインで、[Create Maintenance Policy] をクリックします。

ステップ 4 [Create Maintenance Policy] ダイアログボックスで、必須フィールドに入力します。

ステップ 5 [OK] をクリックします。

次の作業

Cisco UCS Manager でメンテナンス ポリシーをサービス プロファイルに関連付けます。

1 回のオカレンスのスケジュールの作成

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Groups Root] > [Schedules] を展開します。

ステップ 3 [Work] ペインで、[Create Schedule] をクリックします。

ステップ 4 [Create Schedule] ダイアログボックスで、[Properties] 領域に詳細情報を入力します。

ステップ 5 [One Time Occurrences] タブを選択し、[Create One Time Occurrence] をクリックします。

ステップ 6 [Create One Time Occurrence] ダイアログボックスで、詳細情報を入力します。

ステップ 7 [OK] をクリックします。

ステップ 8 [Create Schedule] ダイアログボックスで [OK] をクリックします。
作成した 1 回のみの実行のスケジュールが [Schedule] テーブルに追加されます。

繰り返すオカレンスのスケジュールの作成

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Groups Root] > [Schedules] を展開します。

ステップ 3 [Work] ペインで、[Create Schedule] をクリックします。

ステップ 4 [Create Schedule] ダイアログボックスで、[Properties] 領域に詳細情報を入力します。

ステップ 5 [Recurring Occurrences] タブを選択し、[Create Recurring Occurrence] をクリックします。

ステップ 6 [Create Recurring Occurrence] ダイアログボックスで、詳細情報を入力します。

ステップ 7 [OK] をクリックします。

ステップ 8 [Create Schedule] ダイアログボックスで [OK] をクリックします。
作成した繰り返し実行のスケジュールがテーブルに追加されます。

ファームウェア アップグレードのスケジュールの削除

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Groups Root] > [Schedules] を展開します。

ステップ 3 [Work] ペインには、スケジュールされているすべてのファームウェア イベントのリストが表示されます。

ステップ 4 削除するスケジュールの名前をクリックして選択します。
テーブル ヘッダーの領域にアクションのアイコンが表示されます。

ステップ 5 [Delete] をクリックします。

ステップ 6 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。

機能カタログ

機能カタログは調整可能なパラメータ、文字列、およびルールのセットです。 Cisco UCS はカタログを使用してサーバの新しく資格を持ったDIMMやディスク ドライブなどのコンポーネントの表示と設定可能性を更新します。

カタログは、シャーシ、CPUローカル ディスク、I/O モジュールなどのハードウェア コンポーネントによって分割されます。 カタログを使用すると、該当するコンポーネントで利用可能なプロバイダーのリストを表示できます。 1 つのハードウェア コンポーネントに対して 1 つのプロバイダーが存在します。 各プロバイダーは、ベンダー、モデル（PID）、およびリビジョンによって識別されます。 各プロバイダーに対して、装置の製造元とフォーム ファクタの詳細を表示することもできます。

特定のカタログのリリースに依存するハードウェア コンポーネントの詳細については、『Service Notes for the B- Series server』のコンポーネントのサポートの表を参照してください。 特定のリリースで導入されたコンポーネントの情報については、『Cisco UCS Release Notes』を参照してください。

機能カタログの内容

機能カタログの内容は次のとおりです。

実装固有の調整可能なパラメータ

- 電力および熱に関する制約
- スロット範囲および番号
- アダプタ機能

ハードウェア固有のルール

- BIOS、CIMC、RAIDコントローラ、アダプタなどのコンポーネントのファームウェア互換性
- 診断
- ハードウェア固有のリブート

ユーザ表示文字列

- CPN や PID/VID などの部品番号
- コンポーネントの説明
- 物理レイアウト/寸法
- OEM 情報

機能カタログの更新

機能カタログの更新は、各Cisco UCS インフラストラクチャ ソフトウェア バンドルに含まれています。 Cisco TAC から特に指示された場合を除いて、Cisco UCS インフラストラクチャ ソフトウェア バンドルをダウンロード、更新、およびアクティブ化した後に、機能カタログの更新をアクティブ化する必要があるだけです。

機能カタログの更新をアクティブ化すると、Cisco UCSによってすぐに新しいベースライン カタログに更新されます。 それ以外の作業は行う必要がありません。 機能カタログの更新では、Cisco UCS ドメイン内のコンポーネントをリブートまたは再インストールする必要はありません。

各 Cisco UCS インフラストラクチャ ソフトウェア バンドルには、ベースライン カタログが含まれます。 まれに、シスコが Cisco UCS リリースの間で機能カタログの更新をリリースし、ファームウェア イメージをダウンロードするのと同じサイトで更新を入手できるようにする場合があります。

（注） 機能カタログのバージョンは、使用している Cisco UCS のバージョンによって決まります。たとえば、Cisco UCS 2.0 リリースは、機能カタログのあらゆる 2.0 リリースを使用できますが、機能カタログの 1.0 リリースを使用することはできません。 特定の Cisco UCS リリースでサポートされている機能カタログのリリースについては、http://www.cisco.com/go/unifiedcomputing/b-series-doc で入手できる『*Cisco UCS B-Series Servers Documentation Roadmap*』にある『*Release Notes for Cisco UCS Administration Software*』を参照してください。

Cisco UCS ドメインの機能カタログの更新の設定

Cisco UCS Central では、Cisco UCS ドメイン グループごとに機能カタログを 1 つに限り作成できます。 グループのメンバーである Cisco UCS ドメインは、すべて同じバージョンのファームウェアを実行します。

（注） 機能カタログの更新は、ドメイン グループのルートまたはドメイン グループのレベルで設定できます。 ドメイン グループのルート レベルで機能カタログを更新すると、ルートの下にあるドメイン グループで機能カタログが定義されていない場合は同じ機能カタログのバージョンになります。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Groups Root] > [Firmware Management] を展開します。

ステップ 3 [Capability Catalog] をクリックします。

ステップ 4 [Work] ペインで、[Create] をクリックします。

ステップ 5 [Version] テーブルで、選択した Cisco UCS Central ドメイン グループに含まれる Cisco UCS ドメインに関連付ける機能カタログのバージョンを選択します。
親グループから継承したバージョンがある場合は、ここで選択した機能カタログのバージョンによって、継承したバージョンは上書きされます。

ステップ 6 [Save] をクリックします。

Cisco UCS Central によって、指定した Cisco UCS ドメインの機能カタログの更新がトリガーされます。

第 6 章

ドメイン管理

この章は、次の内容で構成されています。

Cisco UCS ドメインの登録

Cisco UCS Central から Cisco UCS Manager を管理するには、Cisco UCS Central に Cisco UCS ドメインを登録します。 Cisco UCS ドメインは、ドメイン グループの一部またはグループ化されていないドメインとして登録できます。 ドメイン グループがある場合、ドメイン グループのすべての登録済みドメインは、共通のポリシーやその他の設定を共有できます。

（注） Cisco UCS Central を使用した初期登録プロセス中に、すべてのアクティブな Cisco UCS Manager GUI セッションが終了します。

Cisco UCS Central でドメインを登録する前に、次の手順を実行します

- Cisco UCS Manager と Cisco UCS Central を確実に同期させるために、双方で NTP サーバおよび正しいタイム ゾーンを設定します。 Cisco UCS ドメインと Cisco UCS Central の日時が同期していない場合、登録は失敗する可能性があります。
- Cisco UCS Central のホスト名または IP アドレスを取得します。 スタンドアロン モードの場合、各 VM の IP アドレスを使用します。 クラスタ モードでセットアップする場合は仮想 IP アドレスを使用します。
- Cisco UCS Central を導入したときに設定した共有秘密を取得します。

（注）

- Cisco UCS Central に Cisco UCS ドメインを登録すると、Cisco UCS Manager で使用される IP を変更または交換できません。 IP アドレスを変更または交換する必要がある場合は、Cisco UCS Central からドメインの登録を解除して、IP アドレスを変更し、Cisco UCS Central に再登録してください。
- Cisco UCS Manager の GUI または CLI を使用して、Cisco UCS ドメインを登録または登録解除できます。
- 登録された Cisco UCS ドメインで Cisco UCS Central からのラウンドトリップが 300 ミリ秒以上遅延する場合、Cisco UCS ドメインのパフォーマンスに影響する可能性があります。

警告

Cisco UCS Central に登録する前に、Cisco UCS Manager をリリース 2.1(2) にアップグレードする必要があります。 Cisco UCS Manager リリース 2.1(1) をCisco UCS Central リリース 1.1 に登録しようとすると、Cisco UCS Manager には登録が正常に行われたものとして表示されますが、Cisco UCS Central インベントリには登録済み Cisco UCS ドメインが表示されません。 Cisco UCS Central の障害が、登録の失敗に関する重大なエラーを表示します。

再接続への影響の予測

Cisco UCS Central リリース 1.2 以降と Cisco UCS Manager リリース 2.2(3x) および 3.0(1) 以降を使用すると、再接続への影響を予測できます。 登録済み Cisco UCS ドメインがCisco UCS Centralから切断された場合、または Cisco UCS ドメインを中断状態にすると、そのドメインを再接続するか、または中断状態から別の状態に変更するときに、ドメインに対して再接続への影響の予測を実行できます。 再接続への影響の予測では、ドメインが切断された時点または中断された時点でのドメインに対するすべての累積変更が評価され、その状況が示されます。 これにより、情報に基づいて作業を進めるかどうかを決定できます。

Cisco UCS ドメインの登録解除

Cisco UCS Centralから直接 Cisco UCS ドメインを登録解除することはできません。 Cisco UCS ドメインを登録解除する場合は、Cisco UCS Manager を使用する必要があります。 詳細については、該当する『*Cisco UCS Server Installation and Upgrade Guide*』を参照してください。

（注）

Cisco UCS ドメインを登録解除すると、グローバル ポリシーに影響することがあります。 詳細については、「ポリシー解決の変更結果, （220 ページ）」を参照してください。

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 ポリシーを作成しており、新しい登録済み Cisco UCS ドメインがポリシーで定義された条件を満たしている場合、そのドメインはポリシーで指定されたドメイン グループの下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。

ドメイン グループの作成

[Equipment] タブまたは [Operations Management] タブから、ドメイン グループ ルートの下にドメイン グループを作成できます。 ルートの下には、最大 5 階層レベルのドメイン グループを作成できます。 この手順では、[Equipment] タブからドメイン グループ ルートの下にドメイン グループを作成する手順について説明します。

手順

ステップ 1 メニュー バーで、[Equipment] をクリックします。

ステップ 2 [Equipment] タブで、[UCS Domains] を展開します。

ステップ 3 [Domain Group root] を右クリックし、[Create Domain Group] を選択します。

ステップ 4 [Create Domain Group] ダイアログボックスで、[Name] および [Description] に入力します。

ステップ 5 [OK] をクリックします。

ドメイン グループの削除

手順

ステップ 1 メニュー バーで、[Equipment] をクリックします。

ステップ 2 [Equipment] タブで、[UCS Domains] > [Domain Group root] を選択します。

ステップ 3 削除するドメイン グループの名前を右クリックし、[Delete] を選択します。

ステップ 4 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。

Cisco UCS ドメインのグループ割り当ての変更

次のいずれかのオプションを使用して、ドメイン グループに Cisco UCS ドメインを割り当てることができます。

- [Change Group Assignment] ダイアログボックスを使用してグループ割り当てを変更。
- 特定のドメイン グループ下のグループ割り当てリンクを使用。
- ドメイン グループ ポリシー修飾子を使用。

この手順では、Cisco UCS ドメインのグループ割り当てを変更する手順について説明します。

手順

ステップ 1 メニュー バーで、[Equipment] をクリックします。

ステップ 2 [Equipment] タブで、[UCS Domains] を展開します。

ステップ 3 [Navigation] ペインで、[Ungrouped Domains] を展開します。

ステップ 4 ドメイン名を右クリックし、[Change Group Assignment] をクリックします。

ステップ 5 [Change Group Assignment] ダイアログボックスで、ドメイン グループを選択し、[OK] をクリックします。

ステップ 6 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。

ドメイン グループおよび登録ポリシー

ドメイン グループ ポリシーの作成

手順

ステップ 1 メニュー バーで、[Equipment] をクリックします。
ステップ 2 [Navigation] ペインの [Equipment] タブで、[UCS Domains] > [Policies] を展開します。
ステップ 3 [Domain Group Policies] を右クリックし、[Create Domain Group Policy] を選択します。
ステップ 4 [Create Domain Group Policy] ダイアログボックスで、[Name] と説明（任意）を入力します。
ステップ 5 ドロップダウン リストから [Domain Group] と [Domain Group Policy Qualification] を選択します。
ステップ 6 [OK] をクリックします。

ドメイン グループ ポリシーの削除

手順

ステップ 1 メニュー バーで、[Equipment] をクリックします。
ステップ 2 [Navigation] ペインの [Equipment] タブで、[UCS Domains] > [Policies] を展開します。
ステップ 3 [Domain Group Policies] を展開します。
ステップ 4 削除するポリシーを右クリックし、[Delete] を選択します。
ステップ 5 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。

登録ポリシーの作成

手順

ステップ 1 メニュー バーで、[Equipment] をクリックします。
ステップ 2 [Navigation] ペインの [Equipment] タブで、[UCS Domains] > [Policies] を展開します。
ステップ 3 [Registration Policies] を右クリックして [Create Registration Policy] を選択します。
ステップ 4 [Create Registration Policy] ダイアログボックスで、[Name] と説明（任意）を入力します。
ステップ 5 [OK] をクリックします。

次の作業

ポリシーの資格情報にアドレス条件、所有者条件、およびサイト条件を追加します。

サイト条件の作成

手順

ステップ 1 メニュー バーで、[Equipment] をクリックします。
ステップ 2 [Navigation] ペインの [Equipment] タブで、[UCS Domains] > [Policies] を展開します。
ステップ 3 [Registration Policies] を展開します。
ステップ 4 更新する登録ポリシーを右クリックし、[Create Site Qualifier] を選択します。
ステップ 5 [Create Site Qualifier] ダイアログボックスで、[Name] と [Regex] を入力します。
ステップ 6 [OK] をクリックします。

サイト条件の削除

手順

ステップ 1 メニュー バーで、[Equipment] をクリックします。

ステップ 2 [Navigation] ペインの [Equipment] タブで、[UCS Domains] > [Policies] を展開します。

ステップ 3 [Registration Policies] を展開します。

ステップ 4 [Work] ペインで [Sites] を展開します。

ステップ 5 削除するサイトを右クリックし、[Delete] を選択します。

ステップ 6 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。

アドレス条件の作成

手順

ステップ 1 メニュー バーで、[Equipment] をクリックします。

ステップ 2 [Navigation] ペインの [Equipment] タブで、[UCS Domains] > [Policies] を展開します。

ステップ 3 [Registration Policies] を展開します。

ステップ 4 更新する登録ポリシーを右クリックし、[Create Address Qualifier] を選択します。

ステップ 5 [Create Address Qualifier] ダイアログボックスで、最小 IP アドレスと最大 IP アドレスを入力します。

ステップ 6 [OK] をクリックします。

アドレス条件の削除

手順

ステップ 1 メニュー バーで、[Equipment] をクリックします。
ステップ 2 [Navigation] ペインの [Equipment] タブで、[UCS Domains] > [Policies] を展開します。
ステップ 3 [Registration Policies] を展開します。
ステップ 4 [Work] ペインで [Addresses] を展開します。
ステップ 5 削除するアドレス範囲を右クリックして、[Delete] を選択します。
ステップ 6 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。

所有者条件の作成

手順

ステップ 1 メニュー バーで、[Equipment] をクリックします。
ステップ 2 [Navigation] ペインの [Equipment] タブで、[UCS Domains] > [Policies] を展開します。
ステップ 3 [Registration Policies] を展開します。
ステップ 4 更新する登録ポリシーを右クリックし、[Create Owner Qualifier] を選択します。
ステップ 5 [Create Owner Qualifier] ダイアログボックスで、[Name] と [Regex] を入力します。
ステップ 6 [OK] をクリックします。

所有者条件の削除

手順

ステップ 1 メニュー バーで、[Equipment] をクリックします。
ステップ 2 [Navigation] ペインの [Equipment] タブで、[UCS Domains] > [Policies] を展開します。
ステップ 3 [Registration Policies] を展開します。
ステップ 4 [Work] ペインで [Owners] を展開します。
ステップ 5 削除する所有者を右クリックし、[Delete] を選択します。
ステップ 6 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。

登録ポリシーの削除

手順

ステップ 1 メニュー バーで、[Equipment] をクリックします。

ステップ 2 [Navigation] ペインの [Equipment] タブで、[UCS Domains] > [Policies] を展開します。

ステップ 3 [Registration Policies] を展開します。

ステップ 4 削除するポリシーを右クリックし、[Delete] を選択します。

ステップ 5 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。

ID 範囲資格情報ポリシー

ID範囲資格情報ポリシーにより、ポリシーを作成し、条件を満たしているドメイン グループとドメイン IP アドレスに割り当てることができます。 ID 範囲資格情報ポリシーは、これらのドメイン グループとドメイン IP アドレスに対して表示されます。 また、ID 範囲資格情報ポリシーを作成し、条件を満たしているドメイングループまたはIPアドレスを割り当てないでおくこともできます。 条件を設定しない場合、ポリシーはすべてのドメイングループに対して使用可能になります。 ID 解決は、他のグローバル ポリシーと同様に組織構造内で階層的に行われます。

ID範囲資格情報ポリシーを作成したら、新しいプールまたは既存のプール内のブロックにそのポリシーを適用できます。

ID 範囲資格情報ポリシーは Cisco UCS Central から条件を満たすドメイン グループ内の Cisco UCS Manager インスタンスに自動的にプッシュされません。 Cisco UCS Central で Cisco UCS Manager ドメイン グループのドメイン グループの条件、ドメイン グループ ID、または IP アドレスを変更した場合、Cisco UCS Manager ローカル サービス プロファイルで参照をリセットする必要があります。

（注） このリリースの Cisco UCS Central のグローバル サービス プロファイルでは、ID 範囲資格情報ポリシーはサポートされていません。

ID 範囲資格情報ポリシーの作成

手順

ステップ 1 メニュー バーで、[Equipment] をクリックします。

ステップ 2 [Navigation] ペインの [Equipment] タブで、[UCS Domains] > [Policies] を展開します。

ステップ 3 [ID Range Qualification Policies] を右クリックし、[Create ID Range Qualification Policy] を選択します。

ステップ 4 [Create ID Range Qualification Policy] ダイアログボックスで、[Name] と説明（任意）を入力します。

ステップ 5 [Qualified Domain Groups] 領域で [Context] を選択します。
選択したコンテキストが [Selected] フィールドの横に表示されます。

ステップ 6 [Qualified Domain IP Addresses] 領域で [IP Address] を入力し、正符号アイコンをクリックします。
入力した IP アドレスが [Selected] フィールドの横に表示されます。

ステップ 7 [OK] をクリックします。

次の作業

ID 範囲資格情報ポリシーをブロックに割り当てます。

ID 範囲資格情報ポリシーの削除

手順

ステップ 1 メニュー バーで、[Equipment] をクリックします。

ステップ 2 [Navigation] ペインの [Equipment] タブで、[UCS Domains] > [Policies] を展開します。

ステップ 3 [ID Range Qualification Policies] を展開します。

ステップ 4 削除するポリシーを右クリックし、[Delete] を選択します。

ステップ 5 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。

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 ポリシー

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

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[CallHome] をクリックします。

ステップ 5 （任意） [Actions] 領域で、[Create] をクリックします。
ドメイン グループ ルート下にある Call Home ポリシーは、システムによって作成されており、デフォルトで設定できる状態です。

ステップ 6 [Work] ペインで、[General] タブをクリックします。

ステップ 7 [Actions] 領域で、該当するすべてのフィールドに入力します。

名前	説明
[Create] ボタン	選択したドメイン グループに含まれるすべての Cisco UCS ドメインで使用されるポリシーのインスタンスを作成します。
[Import] ボタン	Cisco UCS Central に登録された Cisco UCS ドメインの 1 つからポリシーをインポートできます。

名前	説明
[Delete] ボタン	選択したドメイン グループに定義されているポリシーのインスタンスを削除します。 ポリシーを削除した後、[Save] をクリックするまでグレーのままになります。 これを行うと、Cisco UCS Central は指定した可能性のあるポリシーとすべての設定データを削除します。 後でポリシーの新しいインスタンスを作成できますが、削除されたインスタンスからの設定データを復元することはできません。 削除要求をキャンセルするには、[Reset] をクリックします。
[State] フィールド	Cisco UCS Central ドメイン グループに含まれている Cisco UCS ドメインに Call Home が使用されるかどうか。 次のいずれかになります。 • [Off]：Cisco UCS ドメインで Call Home は使用されません。 • [On]：Cisco UCS では、ドメイン グループで定義されている Call Home ポリシーおよびプロファイルに基づいて Call Home アラートが生成されます。 （注） Cisco UCS Central GUI では、このフィールドを [On] に設定すると、このタブに残りのフィールドが表示されます。
[Throttling] フィールド	同じイベントについて受信する重複メッセージの数を制限するかどうかを指定します。 次のいずれかになります。 • [On]：送信される重複メッセージの数が 2 時間以内に 30 件を超えると、そのアラート タイプに関するそれ以降のメッセージは破棄されます。 • [Off]：検出された数に関係なく、すべての重複メッセージが送信されます。
[Phone] フィールド	主要連絡先の電話番号。 +（プラス記号）と国番号から始まる国際形式の番号を入力します。 ハイフンは使用できますが、カッコは使用できません。

名前	説明
[Email] フィールド	主要連絡先の電子メール アドレス。 Cisco Smart Call Home によってこの電子メール アドレスに登録メールが送信されます。 （注） 電子メール アドレスに #（ハッシュ記号）、スペース、&（アンパサンド）などの特殊文字が含まれていると、電子メール サーバが電子メール メッセージをそのアドレスに配信できないことがあります。RFC2821 および RFC2822 に準拠し、7 ビット ASCII 文字のみを含む電子メール アドレスを使用することをお勧めします。
[Address] フィールド	主要連絡先の住所。 255 文字以下の ASCII 文字で入力します。
[From] フィールド	システムによって送信される Call Home アラート メッセージの [From] フィールドに表示される電子メール アドレス。
[Reply To] フィールド	システムによって送信される Call Home アラート メッセージの [From] フィールドに表示される返信電子メール アドレス。
[Switch Priority] ドロップダウン リスト	次のいずれかになります。 • Alerts • Critical • Debugging • Emergencies • Errors • Information • Notifications • Warnings

名前	説明
[Hostname] フィールド	シンプル メール転送プロトコル（SMTP）サーバの IP アドレスまたはホスト名。 （注） IPv4 または IPv6 アドレスではなくホスト名を使用する場合、 で DNS サーバを設定する必要があります。 Cisco UCS ドメインが Cisco UCS Central に登録されていないか、DNS 管理が [ローカル] に設定されている場合は、Cisco UCS Manager で DNS サーバを設定します。 Cisco UCS ドメイン Cisco UCS Central に登録されていないか、DNS 管理が [グローバル] に設定されている場合は、Cisco UCS Central で DNS サーバを設定します。
[Port] フィールド	SMTP サーバとの通信に使用されるポート番号。 1 ～ 65535 の整数を入力します。 デフォルトは 25 です。
[Customer ID] フィールド	ライセンス上のサポート契約の契約番号を含む Cisco Connection Online（CCO）ID。 510 文字以下の ASCII 文字を入力します。
[Contract ID] フィールド	お客様の Call Home 契約番号。 510 文字以下の ASCII 文字を入力します。
[Site] フィールド	お客様のサイトに固有の Call Home ID。 510 文字以下の ASCII 文字を入力します。

ステップ 8 [Work] ペインで、[Profiles] タブをクリックします。

ステップ 9 [Actions] 領域で、該当するすべてのフィールドに入力します。

名前	説明
[Create] ボタン	選択したドメイン グループに含まれるすべての Cisco UCS ドメインで使用されるポリシーのインスタンスを作成します。
[Import] ボタン	Cisco UCS Central に登録された Cisco UCS ドメインの 1 つからポリシーをインポートできます。

名前	説明
[Delete] ボタン	選択したドメイン グループに定義されているポリシーのインスタンスを削除します。 ポリシーを削除した後、[Save] をクリックするまでグレーのままになります。 これを行うと、Cisco UCS Central は指定した可能性のあるポリシーとすべての設定データを削除します。 後でポリシーの新しいインスタンスを作成できますが、削除されたインスタンスからの設定データを復元することはできません。 削除要求をキャンセルするには、[Reset] をクリックします。
[Filter] ボタン	テーブル内のデータをフィルタリングできます。 フィルタを適用すると、このボタン名は [Filter (on)] に変わります。
[Create Profile] ボタン	Call Home プロファイルを作成できます。
[Add Email Recipient] ボタン	既存の Call Home プロファイルに電子メール受信者を追加できます。
[Properties] ボタン	テーブルで選択されたオブジェクトの詳細なプロパティを表示します。
[Delete] ボタン	テーブルで選択したオブジェクトを削除します。
[Name] カラム	Call Home プロファイルの名前。
[Level] カラム	プロファイルをトリガーする最小障害レベル。 Cisco UCS はこのレベル以上である各エラーに対して Call Home アラートを生成します。
[Alert Groups] カラム	この Call Home プロファイルに基づいて警告されるグループ。

ステップ 10 [Work] ペインの [Policies] タブをクリックします。

ステップ 11 [Actions] 領域で、該当するすべてのフィールドに入力します。

名前	説明
[Create] ボタン	選択したドメイン グループに含まれるすべての Cisco UCS ドメインで使用されるポリシーのインスタンスを作成します。
[Import] ボタン	Cisco UCS Central に登録された Cisco UCS ドメインの 1 つからポリシーをインポートできます。

名前	説明
[Delete] ボタン	選択したドメイン グループに定義されているポリシーのインスタンスを削除します。 ポリシーを削除した後、[Save] をクリックするまでグレーのままになります。 これを行うと、Cisco UCS Central は指定した可能性のあるポリシーとすべての設定データを削除します。 後でポリシーの新しいインスタンスを作成できますが、削除されたインスタンスからの設定データを復元することはできません。 削除要求をキャンセルするには、[Reset] をクリックします。
[Filter] ボタン	テーブル内のデータをフィルタリングできます。 フィルタを適用すると、このボタン名は [Filter (on)] に変わります。
[Create Policy] ボタン	新しい [Call Home] ポリシーを作成できます。
[Properties] ボタン	テーブルで選択されたオブジェクトの詳細なプロパティを表示します。
[Delete] ボタン	テーブルで選択したオブジェクトを削除します。
[Cause] カラム	このアラートをトリガーするイベント。 各ポリシーは、アラートがいずれかのタイプのイベントに送信されるかどうかを定義します。
[State] カラム	これが [enabled] の場合、Cisco UCS は関連付けられた原因と一致するエラーが発生した場合にこのポリシーを使用します。 それ以外の場合、一致するエラーが発生しても、Cisco UCS はこのポリシーを無視します。 デフォルトでは、すべてのポリシーがイネーブルになります。

ステップ 12 [Work] ペインで [System Inventory] タブをクリックします。

ステップ 13 [Actions] 領域で、該当するすべてのフィールドに入力します。

名前	説明
[Create] ボタン	選択したドメイン グループに含まれるすべての Cisco UCS ドメインで使用されるポリシーのインスタンスを作成します。
[Import] ボタン	Cisco UCS Central に登録された Cisco UCS ドメインの 1 つからポリシーをインポートできます。

名前	説明
[Delete] ボタン	選択したドメイン グループに定義されているポリシーのインスタンスを削除します。 ポリシーを削除した後、[Save] をクリックするまでグレーのままになります。 これを行うと、Cisco UCS Central は指定した可能性のあるポリシーとすべての設定データを削除します。 後でポリシーの新しいインスタンスを作成できますが、削除されたインスタンスからの設定データを復元することはできません。 削除要求をキャンセルするには、[Reset] をクリックします。
[Send Periodically] フィールド	このフィールドを [on] に設定すると、Cisco UCS によってシステム インベントリが Call Home データベースに送信されます。この情報がいつ送信されるかは、この領域の他のフィールドによって決まります。
[Send Interval] フィールド	自動システム インベントリ データ収集の間隔（日数）。 1 ～ 30 の整数を入力します。
[Hour of Day to Send] フィールド	データを送信する時間（24 時間時計形式）。
[Minute of Hour to Send] フィールド	データを送信する時間（分数）。

ステップ 14 [Save] をクリックします。

Call Home ポリシーの削除

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 グループから削除されます。ドメイン グループ ルート下の Call Home ポリシーは、削除できません。

Call Home ポリシーを削除すると、そのポリシー内のすべてのプロファイル、ポリシー、およびシステム インベントリ設定が削除されます。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[CallHome] をクリックします。

ステップ 5 [Actions] 領域で、[Delete] をクリックします。
削除されたポリシーは、再設定されるまでドメイン グループの親から設定を継承します。

ステップ 6 [Save] をクリックします。

Call Home ポリシーのプロファイルの設定

はじめる前に

ドメイン グループ ルート下のドメイン グループの Call Home ポリシーのプロファイルを設定する前に、最初にこのプロファイルとポリシーを作成する必要があります。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[CallHome] をクリックします。

ステップ 5 [Work] ペインで、[Profiles] タブをクリックします。

ステップ 6 [Actions] 領域で、[Create Profile] をクリックし、すべての該当するフィールドに入力します。

a) [Create Profile] ダイアログボックスで、次のフィールドをクリックして値を入力します。

名前	説明
[Name] フィールド	このプロファイルのユーザ定義名。

名前	説明
[Level] フィールド	プロファイルをトリガーする最小障害レベル。 Cisco UCS はこのレベル以上である各障害に対して Call Home アラートを生成します。 次のいずれかになります。 • critical • debug • disaster • fatal • major • minor • normal • notification • warning

b) [Alert Groups] 領域で、次のフィールドに値を入力します。

名前	説明
[Alert Groups] フィールド	この Call Home プロファイルに基づいて警告されるグループ。これは次のいずれか、または複数の値になります。 • ciscoTac • diagnostic • environmental • インベントリ • license • lifeCycle • linecard • スーパーバイザ • syslogPort • system • test

c) [Email Configuration] 領域で、次のフィールドに値を入力します。

名前	説明
[Format] フィールド	次のいずれかになります。 • [xml]：Extensible Markup Language（XML）と Adaptive Messaging Language（AML）XML Schema Definition（XSD）を使用するマシンが読み取り可能な形式。この形式により、Cisco Systems Technical Assistance Center との通信が可能になります。 • [fullTxt]：人間が判読するのに適している完全にフォーマットされたメッセージ（詳細な情報付き）。 • [shortTxt]：ポケットベルまたは印刷されたレポートに適している 1 ～ 2 行の障害の説明。
[Max Message Size] フィールド	指定された Call Home 受信者に送信される最大メッセージ サイズ。 1 ～ 5000000 の整数を入力します。デフォルト値は 5000000 です。 フルテキスト メッセージおよび XML メッセージの推奨最大サイズは 5000000 です。ショートテキスト メッセージの推奨最大サイズは 100000 です。Cisco TAC アラート グループの場合、最大メッセージ サイズは 5000000 である必要があります。

d) [Email Recipients] 領域で、次のフィールドに値を入力します。

名前	説明
[Filter] ボタン	テーブル内のデータをフィルタリングできます。フィルタを適用すると、このボタン名は [Filter (on)] に変わります。
[Add Email Recipients] ボタン	電子メール受信者を追加できます。
[Properties] ボタン	テーブルで選択されたオブジェクトの詳細なプロパティを表示します。
[Delete] ボタン	テーブルで選択したオブジェクトを削除します。
[Email] カラム	受信者の電子メール アドレス。

e) [OK] をクリックします。

ステップ 7 [Save] をクリックします。

Call Home プロファイルへの電子メール受信者の追加

はじめる前に

電子メール受信者を Call Home ポリシーのプロファイルに追加する前に、最初にこのプロファイルを作成する必要があります。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[CallHome] をクリックします。

ステップ 5 [Work] ペインで、[Profiles] タブをクリックします。

ステップ 6 [Work] ペインで、電子メール受信者を追加する既存のプロファイルをクリックします。

ステップ 7 [Action] 領域で、[Add Email Recipients] をクリックします。

ステップ 8 [Add Email Recipients] ダイアログボックスで、受信者の電子メール アドレスを入力します。

ステップ 9 [OK] をクリックします。

ステップ 10 [Save] をクリックします。

Call Home ポリシーのプロファイルの削除

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[CallHome] をクリックします。

ステップ 5 [Actions] 領域で、Call Home 内の削除するプロファイルをクリックします。
また、Call Home 内の削除するプロファイルを右クリックして、そのオプションにアクセスすることもできます。 削除されたプロファイルは、再設定されるまでドメイングループの親からの設定を継承します。

ステップ 6 [Actions] 領域で、[Delete] をクリックします。
Call Home ポリシーのプロファイルを削除すると、すべての電子メール受信者、およびそのプロファイルに定義されたその他の設定が削除されます。

ステップ 7 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。

Call Home ポリシーのポリシーの設定

はじめる前に

ドメイン グループ下で Call Home ポリシーのポリシーを設定する前に、最初にこのポリシーを作成する必要があります。 ドメイン グループ ルート下にある Call Home ポリシーのポリシーは、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

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[CallHome] をクリックします。

ステップ 5 [Work] ペインの [Policies] タブをクリックします。

ステップ 6 [Actions] 領域で、[Create Policy] をクリックし、該当するすべてのフィールドに入力します。

a) [Create Policy] ダイアログボックスで、次のフィールドをクリックして値を入力します。

名前	説明
[State] フィールド	これが [enabled] の場合、Cisco UCS は関連付けられた原因と一致するエラーが発生した場合にこのポリシーを使用します。それ以外の場合、一致するエラーが発生しても、Cisco UCS はこのポリシーを無視します。 デフォルトでは、すべてのポリシーがイネーブルになります。
[Cause] フィールド	このアラートをトリガーするイベント。 各ポリシーは、アラートがいずれかのタイプのイベントに送信されるかどうかを定義します。 ポリシーを保存した後に、原因を変更することはできません。

b) [OK] をクリックします。

ステップ 7 [Save] をクリックします。

Call Home ポリシーのポリシーの削除

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 5 [Work] ペインで、[CallHome] をクリックします。

ステップ 6 [Actions] 領域で、Call Home 内の削除するポリシーをクリックします。
また、Call Home 内の削除するポリシーを右クリックして、そのオプションにアクセスすることもできます。 削除されたポリシーは、再設定されるまでドメイングループの親から設定を継承します。

ステップ 7 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。

ポート設定

ファブリック インターコネクトの固定ポートまたは拡張モジュール ポートは、クラシックおよびミニ Cisco UCS ドメインの両方で Cisco UCS Central から変更できます。

- **イーサネット ポート**：デフォルトでは、イーサネット ポートは未設定です。 Cisco UCS Central から、イーサネット ポートを Cisco UCS ドメインのサーバ ポートまたはアップリンク ポートとして設定できます。
  - サーバ ポートは、ファブリック インターコネクトとサーバ上のアダプタ カードとの間のデータ トラフィックを処理します。
  - アップリンク ポートは、ファブリック インターコネクトと次のネットワーク レイヤとの間のイーサネット トラフィックを処理します。 すべてのネットワーク行きのイーサネット トラフィックは、これらのポートのいずれかにピン接続されます。
- **スケーラビリティ ポート**：ミニ Cisco UCS ドメインにはスケーラビリティ ポートがあります。 このスケーラビリティ ポートはサーバ ポートとしてのみ設定できます。

ファブリック インターコネクトのポートを設定すると、管理状態が自動的にイネーブルに設定されます。 ポートの設定後に、そのポートを無効にできます。

（注） Cisco UCS Central では 2 種類のポート設定を実行できます。 Cisco UCS Manager では、その他のすべてのポート設定オプションが使用可能です。 ポート設定の詳細については、『Cisco UCS Manager Configuration Guide』の「Configuring Ports and Port Channels」を参照してください。

イーサネット ポートの設定

イーサネット ポートは、サーバ ポート またはアップリンク ポート として設定できます。 ポートを設定すると、そのポートは自動的に有効になります。 また、ポートの無効化と設定解除も可能です。

手順

ステップ 1 [Domains] タブで、[Equipment] > [UCS Domains] をクリックします。

ステップ 2 [Navigation] ペインで [Domain Groups] または [Ungrouped Domains] のいずれか適切なほうを展開します。

ステップ 3 [Navigation] ペインで、UCS ドメイン名を展開し、[Fabric Interconnects] > [Fabric Interconnect A or B] > [Fixed Module 1 or 2] を展開し、[Ethernet Ports] をクリックします。
[Work] ペインに、このモジュールで使用可能なすべてのイーサネット ポートが表示されます。

ステップ 4 いずれかのポートを右クリックして、ポート設定オプションを表示します。

ステップ 5 要件に応じて、[Configure as Server Port] または [Configure as Uplink Port] をクリックします。

ステップ 6 確認ダイアログボックスで、[OK] をクリックします。

Cisco UCS Central は、登録済みの Cisco UCS ドメインを介してポートにこの設定を送信します。ポートに対して操作を実行する前に、設定が有効になるまで待ってください。

スケーラビリティ ポートの設定

スケーラビリティ ポートはサーバ ポートとしてのみ設定できます。 ポートを設定すると、そのポートは自動的に有効になります。 また、ポートの無効化と設定解除も可能です。

手順

ステップ 1 [Domains] タブで、[Equipment] > [UCS Domains] をクリックします。

ステップ 2 [Navigation] ペインで [Domain Groups] または [Ungrouped Domains] のいずれか適切なほうを展開します。

ステップ 3 [Navigation] ペインで、UCS ドメイン名を展開し、[Fabric Interconnects] > [Fabric Interconnect A or B] > [Fixed Module 1 or 2] > [Ethernet Port] を展開し、[Scalability Port] をクリックします。
[Work] ペインに、このモジュールで使用可能なすべてのスケーラビリティ ポートが表示されます。

ステップ 4 いずれかのポートを右クリックして、ポート設定オプションを表示します。

ステップ 5 [Configure as Server Port] をクリックします。
スケーラビリティ ポートはアップリンク ポートとして設定できないため、[Configure as Uplink Port] オプションは無効になっています。

ステップ 6 確認ダイアログボックスで、[OK] をクリックします。

Cisco UCS Central は、登録済みの Cisco UCS ドメインを介してポートにこの設定を送信します。ポートに対して操作を実行する前に、設定が有効になるまで待ってください。

第 7 章

Remote Management

この章は、次の内容で構成されています。

Remote Management

Cisco UCS Centralのリモート管理オプションでは、Cisco UCS Central GUIと CLI の両方で登録済み UCS ドメインのシャーシ、サーバ、ファブリック インターコネクト、FEX などの物理デバイスを管理できます。

重要

- 登録済み UCS ドメインに対してリモート管理操作を実行する場合は、UCI ドメインでリモート操作機能が有効になっていることを確認します。
- これらのリモート操作のいずれかを実行すると、Cisco UCS Central が UCS ドメインに対して設定要求を開始します。 これには約 30 秒かかります。 リモート操作に基づく変更を確認する前に、30 秒間待ってください。

リモート管理機能を使用して次の操作を実行できます。

- シャーシの確認、稼働中止、および稼働再開。
- サーバ メンテナンス タスク（ブレードおよびラックマウント サーバの稼働中止、稼働再開、取り外し、および再確認など）の実行。

- KVM コンソールの起動、ブートアップ、シャットダウン、リセット、回復、およびファブリック エクステンダ（FEX）、ブレード、およびラックマウント サーバでの診断割り込みの実行。
- シャーシ、ブレード、およびラックマウント サーバ、ファブリック インターコネクト（FI）、および FEX のロケータ LED のオン/オフ。
- 登録済み UCS ドメインのテクニカル サポート ファイルの作成とダウンロード。

サーバがローカルまたはグローバルサービスプロファイルに関連付けられている場合、サービスプロファイルから関連するサーバに対して次のリモート管理アクションを実行できます。

- グローバル サービス プロファイルに関連付けられているブレードおよびラック サーバのブレードおよびラックマウント サーバの KVM コンソールの起動、ブートアップ、シャットダウン、リセット、および回復。
- ローカル サービス プロファイルに関連付けられているブレードおよびラック サーバのブレードおよびラックマウント サーバの KVM コンソールの起動、ブートアップ、シャットダウン、リセット、および回復。

重要 登録済み Cisco UCS ドメインの物理デバイスの管理に関するガイドラインと推奨事項を理解していることを確認します。 物理デバイスの操作とサーバ メンテナンスに関する特定のガイドラインについては、『Cisco UCS Manager GUI Guide』と『CLI Configuration Guide』（http://www.cisco.com/en/US/products/ps10281/products_installation_and_configuration_guides_list.html）にある「**Managing the Chassis**」、「**Managing Blade Servers**」、「**Managing Rack-Mount Servers**」、および「**Managing I/O Modules**」の項を参照してください。

Cisco UCS Central からのブレード サーバ メンテナンスの実行

[Server Maintenance] を使用して、ブレード サーバに対して次のいずれかのメンテナンス アクションを実行できます。

- Remove
- Decommission
- Re-acknowledge

（注） この手順では、[Domains] > [Equipments] > [UCS Domains] > [Chassis] > [Servers] からこのタスクを実行する方法について説明します。 ドメイン グループ内のドメインにサーバがある場合は、[Domain Groups] を展開してそのドメインを見つけます。 それ以外の場合は [Ungrouped Domains] からドメインを見つけます。

手順

ステップ 1 [Domains] タブで、[Equipment] > [UCS Domains] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] または [Ungrouped Domains] のいずれか該当するものを展開し、ブレード サーバが関連付けられている UCS ドメインを見つけます。

ステップ 3 [Navigation] ペインで、UCS ドメイン名を展開し、[Chassis] > [Servers] を展開します。
[Work] ペインに、このドメインに関連付けられているラックマウント サーバがリストされます。

ステップ 4 サーバのリストで該当するサーバをクリックします。メニュー バーに [Server Maintenance] が表示されます。

ステップ 5 [Server Maintenance] をクリックし、[Maintenance Server] ダイアログボックスを表示します。

ステップ 6 3 つのオプション ボタン（[Remove]、[Decommission]、または [Re-acknowledge]）のいずれかをクリックし、このサーバに対してメンテナンス タスクを実行します。
[Decommission] を選択すると、稼働中止の完了後に、サーバが [Decommissioned] タブに移動されます。

（注） 稼働中止には時間がかかることがあります。 [Decommissioned] タブでサーバを確認するには、[decommissioning] ステータスが表示されなくなるまで待ちます。

ステップ 7 [OK] をクリックします。 メンテナンス タスクが正常に完了したことを通知する確認メッセージが表示されます。

サーバのブートアップ

ブレード サーバとラックマウント サーバの両方で、[Servers] ノードからサーバをブートアップできます。このノードでは、[Work] ペインにすべてのサーバがリストされるか、または [Navigation] ペインのサーバ リストの特定のサーバ レベルのサーバが表示されます。 この手順では、特定のサーバ レベルでサーバをブートアップする方法を説明します。

（注） このサーバがサービス プロファイルに関連付けられている場合、ローカルまたはグローバル サービス プロファイルからサーバをブートアップできます。

手順

ステップ 1 [Domains] タブで、[Equipment] > [UCS Domains] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] または [Ungrouped Domains] のいずれか該当するものを展開し、サーバが関連付けられている UCS ドメインの名前を見つけます。

ステップ 3 [Navigation] ペインで、UCS ドメイン名を展開し、[Chassis] > [Server] を展開します。

（注） ラックマウント サーバの場合は [Rack-Mounts] > [Servers] を展開します。

ステップ 4 [Navigation] ペインで [Server] の番号をクリックします。

ステップ 5 [Work] ペインで [General] > [Actions] 領域の [Boot Up Server] をクリックします。

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

サーバのシャットダウン

ブレード サーバとラックマウント サーバの両方で、[Servers] ノードからサーバをシャットダウンできます。このノードでは、[Work] ペインにすべてのサーバがリストされるか、または [Navigation] ペインのサーバ リストの特定のサーバ レベルのサーバが表示されます。 この手順では、特定のサーバ レベルでサーバをシャットダウンする方法について説明します。

（注） このサーバがサービス プロファイルに関連付けられている場合、ローカルまたはグローバルサービス プロファイルからこのサーバをシャットダウンできます。

手順

ステップ 1 [Domains] タブで、[Equipment] > [UCS Domains] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] または [Ungrouped Domains] のいずれか該当するものを展開し、サーバが関連付けられている UCS ドメインの名前を見つけます。

ステップ 3 [Navigation] ペインで、UCS ドメイン名を展開し、[Chassis] > [Server] を展開します。

（注） ラックマウント サーバの場合は [Rack-Mounts] > [Servers] を展開します。

ステップ 4 [Navigation] ペインで [Server] の番号をクリックします。

ステップ 5 [Work] ペインで [General] > [Actions] 領域の [Shutdown Server] をクリックします。

ステップ 6 [Shutdown Server] ダイアログボックスで、[Gracefully Shutdown OS] チェックボックスをオンにします。

サーバのリセット

ブレード サーバとラックマウント サーバの両方で、[Servers] ノードからサーバをリセットできます。このノードでは、[Work] ペインにすべてのサーバがリストされるか、または [Navigation] ペインのサーバ リストの特定のサーバ レベルのサーバが表示されます。 この手順では、特定のサーバ レベルでサーバをリセットする方法について説明します。

（注） このサーバがサービス プロファイルに関連付けられている場合、ローカルまたはグローバル サービス プロファイルからこのサーバをリセットできます。

手順

ステップ 1 [Domains] タブで、[Equipment] > [UCS Domains] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] または [Ungrouped Domains] のいずれか該当するものを展開し、サーバが関連付けられている UCS ドメインの名前を見つけます。

ステップ 3 [Navigation] ペインで、UCS ドメイン名を展開し、[Chassis] > [Server] を展開します。
（注） ラックマウント サーバの場合は [Rack-Mounts] > [Servers] を展開します。

ステップ 4 [Navigation] ペインで [Server] の番号をクリックします。

ステップ 5 [Work] ペインで [General] > [Actions] 領域の [Reset Server] をクリックします。

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

ステップ 7 [Do you want to reset the selected servers?] ダイアログボックスで、該当するオプションを 1 つ（[Power Cycle]、[Gracefully restart OS、[Wait for completion of outstanding UCS tasks on this server] など）を選択して [OK] をクリックします。

ステップ 8 Cisco UCS Central により、選択されたサーバの電源リセット タスクが開始され、[Reset Server] ダイアログボックスに、リセット操作が正常に開始されたことを示すメッセージが表示されます。
（注）

サーバの回復

ブレード サーバとラックマウント サーバの両方で、[Servers] ノードからサーバを回復できます。このノードでは、[Work] ペインにすべてのサーバがリストされるか、または [Navigation] ペインのサーバ リストの特定のサーバ レベルのサーバが表示されます。 この手順では、特定のサーバ レベルでサーバを回復する方法について説明します。

（注） このサーバがサービス プロファイルに関連付けられている場合、ローカルまたはグローバル サービス プロファイルからサーバを回復できます。

手順

ステップ 1 [Domains] タブで、[Equipment] > [UCS Domains] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] または [Ungrouped Domains] のいずれか該当するものを展開し、サーバが関連付けられている UCS ドメインの名前を見つけます。

ステップ 3 [Navigation] ペインで、UCS ドメイン名を展開し、[Chassis] > [Server] を展開します。
（注） ラックマウント サーバの場合は [Rack-Mounts] > [Servers] を展開します。

ステップ 4 [Navigation] ペインで [Server] の番号をクリックします。

ステップ 5 [Work] ペインで [General] > [Actions] 領域の [Recover Server] をクリックします。

ステップ 6 [Recover Server] ダイアログボックスで、該当するオプションを 1 つ（[Reset CIMC (Server Controller)]、[Reset KVM Server]、[Reset CMOS] など）選択します。
[Reset CMOS] を選択すると Cisco UCS Central によりサーバ リブート警告が表示されます。 その他のオプションでは、確認ダイアログボックスが表示されます。

ステップ 7 [OK] をクリックして、サーバの回復プロセスを開始します。

シャーシの確認

[Chassis] ノードでシャーシを確認できます。このノードでは、[Work] ペインにすべてのシャーシが表示されるか、または [Navigation] ペインのシャーシ リストの特定のシャーシ レベルのシャーシが表示されます。 この手順では、特定のシャーシ レベルでシャーシを確認する方法について説明します。

手順

ステップ 1 [Domains] タブで、[Equipment] > [UCS Domains] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] または [Ungrouped Domains] のいずれか該当するものを展開し、シャーシが関連付けられている UCS ドメインの名前を見つけます。

ステップ 3 [Navigation] ペインで、UCS ドメイン名を展開し、[Chassis] を展開します。

ステップ 4 [Navigation] ペインで [Chassis] の番号をクリックします。

ステップ 5 [Work] ペインの [General] > [Actions] 領域で、[Acknowledge Chassis] をクリックします。

ステップ 6 [Acknowledge Chassis] ダイアログボックスで、[OK] をクリックします。
シャーシの確認後に、ポップアップ ダイアログボックスに確認メッセージが表示されます。

シャーシの稼働中止

手順

ステップ 1 [Domains] タブで、[Equipment] > [UCS Domains] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] または [Ungrouped Domains] のいずれか該当するものを展開し、シャーシが関連付けられている UCS ドメインを見つけます。

ステップ 3 [Navigation] ペインで [Chassis] タブをクリックします。
[Work] ペインに、選択した UCS ドメインの [Chassis] リストが表示されます。

ステップ 4 メニュー バーの [Decommission Chassis] オプションを有効にするには、稼働中止する [Chassis ID] をクリックします。

ステップ 5 [Decommission Chassis] 確認メッセージ ダイアログボックスで [OK] をクリックします。
[Status] カラムに、稼働中止が開始されたことを示す [decommissioning] が表示されます。 稼働中止が完了すると、シャーシは [Decommissioned] タブに移動します。

（注） 稼働中止には時間がかかることがあります。 [Decommissioned] タブでシャーシを確認するには、[decommissioning] ステータスが表示されなくなるまで待ちます。

シャーシ ロケータ LED のオン/オフ

[Chassis] ノードでシャーシ ロケータ LED をオンにできます。このノードでは、[Work] ペインにすべてのシャーシが表示されるか、または [Navigation] ペインのシャーシ リストの特定のシャーシ レベルのシャーシが表示されます。 この手順では、特定のシャーシ レベルでシャーシ LED をオンにする方法について説明します。

手順

ステップ 1 [Domains] タブで、[Equipment] > [UCS Domains] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] または [Ungrouped Domains] のいずれか該当するものを展開し、シャーシが関連付けられている UCS ドメインの名前を見つけます。

ステップ 3 [Navigation] ペインで、UCS ドメイン名を展開し、[Chassis] を展開します。

ステップ 4 [Navigation] ペインで [Chassis] の番号をクリックします。

ステップ 5 [Work] ペインの [General] > [Actions] 領域で、[Turn on Locator LED] または [Turn off Locator LED] をクリックします。

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

サーバまたはシャーシの再稼動

シャーシ、ブレードサーバ、またはラックマウントサーバを稼働中止にすると、稼働中止になったオブジェクトは 該当するノード（[Chassis]、[Chassis] > [Servers]、[Rack-Mounts] > [Servers] など）の [Decommissioned] タブに移動します。

手順

ステップ 1 [Domains] タブで、[Equipment] > [UCS Domains] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] または [Ungrouped Domains] のいずれか該当するものを展開し、シャーシが関連付けられている UCS ドメインの名前を見つけます。

ステップ 3 [Navigation] ペインで UCS ドメイン名を展開し、[Chassis] または [Chassis] > [Servers] または [Rack-Mounts] > [Servers] を展開します。

ステップ 4 [Work] ペインで [Decommissioned] タブをクリックします。稼働中止になっているサーバまたはシャーシのリストが表示されます。

ステップ 5 リストでシャーシまたはサーバをクリックすると、メニュー バーに [Recommission] が表示されます。

ステップ 6 [Recommission] をクリックし、[Recommission Server] ポップアップ ダイアログボックスで [OK] をクリックします。

ステップ 7 ポップアップ ダイアログボックスで [OK] をクリックすると、再稼働が開始されたことが示されます。

（注） 再稼動には時間がかかります。 サーバまたはシャーシの再稼働が正常に完了すると、サーバまたはシャーシは [Decommissioned] タブから削除されます。 [Status] タブにサーバまたはシャーシが表示されます。

ファブリック インターコネクタ ロケータ LED のオン/オフ

[Fabric Interconnects] ノードで FI ロケータ LED をオンにできます。このノードでは、[Work] ペインにすべての FI が表示されるか、または [Navigation] ペインの FI リストの特定の FI レベルの FI が表示されます。 この手順では、特定の FI レベルで FI LED をオンにする方法について説明します。

手順

ステップ 1 [Domains] タブで、[Equipment] > [UCS Domains] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] または [Ungrouped Domains] のいずれか該当するものを展開し、シャーシが関連付けられている UCS ドメインの名前を見つけます。

ステップ 3 [Navigation] ペインで、UCS ドメイン名を展開し、[Fabric Interconnects] を展開します。

ステップ 4 [Navigation] ペインで [Fabric Interconnect] の名前をクリックします。

ステップ 5 [Work] ペインの [General] > [Actions] 領域で、[Turn on Locator LED] または [Turn off Locator LED] をクリックします。

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

Cisco UCS Central からのラックマウント サーバ メンテナンスの実行

[Server Maintenance] を使用して、ラック サーバに対して次のいずれかのメンテナンス アクションを実行できます。

- Remove
- Decommission
- Re-acknowledge

（注） この手順では、[Domains] > [Equipments] > [UCS Domains] > [Rack-Mounts] > [Servers] からこのタスクを実行する方法について説明します。 ドメイン グループ内のドメインにサーバがある場合は、[Domain Groups] を展開してそのドメインを見つけます。 それ以外の場合は [Ungrouped Domains] からドメインを見つけます。

手順

ステップ 1 [Domains] タブで、[Equipment] > [UCS Domains] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] または [Ungrouped Domains] のいずれか該当するものを展開し、ラック マウント サーバが関連付けられている UCS ドメインを見つけます。

ステップ 3 [Navigation] ペインで、UCS ドメイン名を展開し、[Rack-Mounts] > [Servers] を展開します。
[Work] ペインに、このドメインに関連付けられているラックマウント サーバがリストされます。

ステップ 4 サーバのリストで該当するサーバをクリックします。メニュー バーに [Server Maintenance] が表示されます。

ステップ 5 [Server Maintenance] をクリックし、[Maintenance Server] ダイアログボックスを表示します。

ステップ 6 3 つのオプション ボタン（[Remove]、[Decommission]、または [Re-acknowledge]）のいずれかをクリックし、このサーバに対してメンテナンス タスクを実行します。
[Decommission] を選択すると、稼働中止の完了後に、サーバが [Decommissioned] タブに移動されます。

（注） 稼働中止には時間がかかることがあります。 [Decommissioned] タブでサーバを確認するには、[decommissioning] ステータスが表示されなくなるまで待ちます。

ステップ 7 [OK] をクリックします。 メンテナンス タスクが正常に完了したことを通知する確認メッセージが表示されます。

ファブリック エクステンダの確認

[Fex] ノードでファブリック エクステンダを確認できます。このノードでは、[Work] ペインにすべてのエクステンダが表示されるか、または [Navigation] ペインのエクステンダ リストの特定のファブリック エクステンダ レベルのファブリック エクステンダが表示されます。 この手順では、特定のエクステンダ レベルのファブリック エクステンダを確認する方法について説明します。

手順

ステップ 1 [Domains] タブで、[Equipment] > [UCS Domains] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] または [Ungrouped Domains] のいずれか該当するものを展開し、ファブリック エクステンダが関連付けられている UCS ドメインの名前を見つけます。

ステップ 3 [Navigation] ペインで、UCS ドメイン名を展開し、[Fex] を展開します。

ステップ 4 [Navigation] ペインで [Fex] の番号をクリックします。

ステップ 5 [Work] ペインの [General] > [Actions] 領域で、[Acknowledge Fex] をクリックします。

ステップ 6 [Acknowledge Fex] ダイアログボックスで、[OK] をクリックします。
ファブリック エクステンダの確認後に、ポップアップ ダイアログボックスに確認メッセージが表示されます。

ファブリック エクステンダの稼働中止

手順

ステップ 1 [Domains] タブで、[Equipment] > [UCS Domains] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] または [Ungrouped Domains] のいずれか該当するものを展開し、ファブリック エクステンダが関連付けられている UCS ドメインを見つけます。

ステップ 3 [Navigation] ペインで [Fex] をクリックします。
[Work] ペインには、選択した UCS ドメインのファブリック エクステンダのリストが表示されます。

ステップ 4 メニューバーの [Decommission Fex] オプションを有効にするには、稼働中止する [Fex ID] をクリックします。

ステップ 5 [Decommission Fex] 確認メッセージ ダイアログボックスで [OK] をクリックします。
[Status] カラムに、稼働中止が開始されたことを示す [decommissioning] が表示されます。 稼働中止が完了すると、Fex は [Decommissioned] タブに移動します。

（注） 稼働中止には時間がかかることがあります。 [Decommissioned] タブでファブリック エクステンダを確認するには、[decommissioning] ステータスが表示されなくなるまで待ちます。

ファブリック エクステンダの再稼動

手順

ステップ 1 [Domains] タブで、[Equipment] > [UCS Domains] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] または [Ungrouped Domains] のいずれか該当するものを展開し、ファブリック エクステンダが関連付けられている UCS ドメインの名前を見つけます。

ステップ 3 [Navigation] ペインで、UCS ドメイン名を展開し、[Fex] を展開します。

ステップ 4 [Work] ペインで [Decommissioned] タブをクリックします。稼働中止になっているファブリック エクステンダのリストが表示されます。

ステップ 5 このリストのファブリック エクステンダをクリックすると、メニューバーに [Recommission] が表示されます。

ステップ 6 [Recommission] をクリックし、[Recommission Fex] ポップアップ ダイアログボックスで [OK] をクリックします。

ステップ 7 ポップアップ ダイアログボックスで [OK] をクリックすると、再稼働が開始されたことが示されます。

（注） 再稼動には時間がかかります。 ファブリック エクステンダが正常に再稼動すると、そのファブリック エクステンダは [Decommissioned] タブから削除され、[Status] タブに表示されます。

ファブリック エクステンダの取り外し

ファブリック エクステンダは、[Properties] ペインの [General] > [Actions] 領域で削除できます。

手順

ステップ 1 [Domains] タブで、[Equipment] > [UCS Domains] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] または [Ungrouped Domains] のいずれか該当するものを展開し、ファブリック エクステンダが関連付けられている UCS ドメインの名前を見つけます。

ステップ 3 [Navigation] ペインで [Fex] タブをクリックします。

ステップ 4 [Navigation] ペインで [Fex] の番号を右クリックします。

ステップ 5 [Work] ペインの [General] > [Actions] 領域で、[Remove Fex] をクリックします。

ステップ 6 [OK] をクリックします。

ファブリック エクステンダ ロケータ LED のオン/オフ

[Fex] ノードでファブリック エクステンダ ロケータ LED をオンにできます。このノードでは、[Work] ペインにすべてのエクステンダが表示されるか、または [Navigation] ペインのエクステンダ リストの特定のファブリック エクステンダ レベルのファブリック エクステンダが表示されます。 この手順では、特定のファブリック エクステンダ レベルで ファブリック エクステンダ LED をオンにする方法について説明します。

手順

ステップ 1 [Domains] タブで、[Equipment] > [UCS Domains] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] または [Ungrouped Domains] のいずれか該当するものを展開し、ファブリック エクステンダが関連付けられている UCS ドメインの名前を見つけます。

ステップ 3 [Navigation] ペインで、UCS ドメイン名を展開し、[Fex] を展開します。

ステップ 4 [Navigation] ペインで [Fex] の番号をクリックします。

ステップ 5 [Work] ペインの [General] > [Actions] 領域で、[Turn on Locator LED] または [Turn off Locator LED] をクリックします。

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

UCS ドメインのリモート テクニカル サポート

Cisco UCS Central から登録済み UCS ドメインのテクニカル サポート ファイルを収集できます。リモート テクニカル サポートの収集では、次の操作を行います。

- テクニカル サポート ファイルの作成：Cisco UCS Central GUI と CLI の両方を使用して、各登録済み UCS ドメインのテクニカル サポート ファイルを作成できます。
- 作成した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できます。

（注） テクニカル サポート ファイルのダウンロードは Cisco UCS Central GUI でのみ実行できます。

UCS ドメインのテクニカル サポート ファイルの作成

登録済み Cisco UCS ドメインから、Cisco UCS Manager で「ucsm」に対応するオプションに関するすべてのテクニカル サポート ファイルを収集できます。

手順

ステップ 1 [Domains] > [Equipment] タブで、[UCS Domains] を展開します。

ステップ 2 [Navigation] ペインで [Domain Group root] または [Ungrouped Domain] を展開し、テクニカル サポート ファイルのダウンロード元の UCS ドメインを探してクリックします。

ステップ 3 [Work] ペインで [Tech Support Files] タブをクリックします。

ステップ 4 メニュー バーで [Create Tech Support] をクリックします。
[Create Tech Support] ダイアログボックスに、テクニカル サポート ファイルの作成が開始したことを示す確認メッセージが表示されます。 テーブルにファイル名が表示され、[Overall Status] カラムに [in-progress] と表示されます。 ファイルの作成が完了すると、このドメインについて作成されたテクニカル サポート ファイルの詳細情報（[Name]、[Size]、[Overall Status]、および [URI] など）が表示されます。

（注） [Create Tech Support] をクリックした後でこの操作を取り消すことはできません。

次の作業

テクニカル サポート ファイルの情報を確認したい場合は、ファイルをローカル システムにダウンロードします。 ドメインのテクニカル サポート ファイルのダウンロード, （166 ページ）を参照してください。

ドメインのテクニカル サポート ファイルのダウンロード

手順

ステップ 1 [Domains] > [Equipment] タブで、[UCS Domains] を展開します。

ステップ 2 [Navigation] ペインで [Domain Group root] または [Ungrouped Domain] を展開し、テクニカル サポート ファイルのダウンロード元の UCS ドメインを探してクリックします。

ステップ 3 [Work] ペインで [Tech Support Files] タブをクリックします。
このドメインについて作成された使用可能なテクニカル サポート ファイルの詳細情報（[Name]、[Overall Status]、[Size]、[URI] など）のリストがテーブルに表示されます。

ステップ 4 ダウンロードするテクニカル サポート ファイルをクリックします。
これにより、メニュー バーの [Delete]、[Download]、および [Properties] オプションが有効になります。

（注） テクニカル サポート ファイル作成プロセスを開始したばかりの場合は、[Overall Status] が [in-progress] から [available] に変わるまで待ちます。 [Overall Status] に [available] が表示されている場合にのみ、テクニカル サポート ファイルをダウンロードできます。

ステップ 5 [Download] をクリックします。
Cisco UCS Central がテクニカル サポート ファイルをダウンロードするためにこの UCS ドメインに初めてアクセスする場合は、次の手順を実行します。

a) システムで [UCSM Communications] エラー ダイアログボックスが表示されたら、証明書を受け入れることを選択します。 [Add Security Exception] ダイアログボックスで、[Confirm Security Exception] をクリックします。

b) Cisco UCS Manager の [Login] パネルで、この UCS ドメインのログイン クレデンシャルを入力します。

ステップ 6 拡張子 .tar が付いたファイル名のポップアップ ダイアログボックスに、[Open with] と [Save file] オプションが表示されます。

ステップ 7 [Save file] をクリックしてファイルをローカル システムに保存するか、またはテクニカル サポート ファイルを開くプログラムをドロップダウン オプションから選択します。

UCS ドメインのテクニカル サポート ファイルの削除

手順

ステップ 1 [Domains] > [Equipment] タブで、[UCS Domains] を展開します。

ステップ 2 [Navigation] ペインで [Domain Group root] または [Ungrouped Domain] を展開し、テクニカル サポート ファイルのダウンロード元の UCS ドメインを探してクリックします。

ステップ 3 [Work] ペインで [Tech Support Files] タブをクリックします。
このドメインについて作成された使用可能なテクニカル サポート ファイルの詳細情報（[Name]、[Overall Status]、[Size]、[URI] など）のリストがテーブルに表示されます。

ステップ 4 削除するテクニカル サポート ファイルをクリックします。
これにより、メニュー バーの [Delete]、[Download]、および [Properties] オプションが有効になります。

ステップ 5 [Delete] をクリックします。

ステップ 6 [Confirmation] ダイアログボックスで、[OK] をクリックします。
システムにより削除プロセスが開始されたことを示すポップアップ メッセージが表示されます。

KVM コンソール

Cisco UCS Central GUI から、登録済み Cisco UCS ドメインで適切に設定されているサーバの KVM コンソールにアクセスできます。

KVM コンソールは、KVM の直接接続をエミュレートする KVM Launch Manager からアクセスできるインターフェイスです。 これにより、ネットワーク上のリモート ロケーションからこのサーバに接続できます。

KVM コンソールは、サーバまたはサービス プロファイルに割り当てられた CIMC IP アドレスを使用して、Cisco UCSCisco UCS ドメイン内の正しいサーバを識別および接続します。 KVM コンソールを使用してサーバにアクセスする場合は、サーバまたはサーバに関連付けられているサービス プロファイルのいずれかが IP アドレスで設定されていることを確認する必要があります。

CD、DVD、またはフロッピー ドライブを使用してサーバに直接接続する代わりに、KVM コンソールでは仮想メディアを使用します。仮想メディアは、仮想 CD、DVD、またはフロッピー ドライブにマップされた実際のディスク ドライブまたはディスク イメージ ファイルです。 次に示す任意の仮想ドライブをマップできます。

- お使いのコンピュータ上の CD/DVD またはフロッピー ドライブ
- コンピュータ上のディスク イメージ ファイル
- ネットワーク上の CD/DVD またはフロッピー ドライブ

- ネットワーク上のディスク イメージ ファイル

サーバからの KVM コンソールの起動

ブレード サーバとラックマウント サーバの両方で、[Servers] ノードから KVM コンソールを開始できます。このノードでは、[Work] ペインにすべてのサーバがリストされるか、または [Navigation] ペインのサーバ リストの特定のサーバ レベルのサーバが表示されます。 この手順では、特定のサーバ レベルで KVM コンソールを起動する方法について説明します。

（注） このサーバがサービス プロファイルに関連付けられている場合、ローカルまたはグローバル サービス プロファイルから KVM コンソールを起動できます。

手順

ステップ 1 [Domains] タブで、[Equipment] > [UCS Domains] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] または [Ungrouped Domains] のいずれか該当するものを展開し、サーバが関連付けられている UCS ドメインの名前を見つけます。

ステップ 3 [Navigation] ペインで、UCS ドメイン名を展開し、[Chassis] > [Server] を展開します。

（注） ラックマウント サーバの場合は [Rack-Mounts] > [Servers] を展開します。

ステップ 4 [Navigation] ペインで [Server] の番号をクリックします。

ステップ 5 [Work] ペインの [General] > [Actions] 領域で [Launch KVM Console] をクリックします。

ステップ 6 [KVM Console] ダイアログボックスで、[Select IP Address] のオプション ボタンをクリックし、[OK] をクリックします。

システムにより、サービス プロファイルに割り当てられている IP アドレスが確認されます。 IP アドレスがサービス プロファイルのサーバに割り当てられていない場合、物理サーバで割り当てられている IP アドレスがあるかどうかが確認されます。

ステップ 7 セキュリティ警告が表示されたら同意し、[Add Security Exception] ダイアログボックスで [Yes] をクリックし、セキュリティ証明書を受け入れて続行します。

ステップ 8 [Security Warning] で [Continue] をクリックします。

ステップ 9 KVM コンソールにログインするため、[KVM Login] で Cisco UCS Manager クレデンシャルを入力します。

ステップ 10 別ウィンドウに KVM コンソールが表示されます。

ヒント KVM セッションを開いたときにキーボードの Caps Lock キーがオンになっており、その後に Caps Lock キーをオフにすると、[KVM Console] は Caps Lock キーがオンのときのように動作する場合があります。 KVM コンソールとキーボードを同期させるには、[KVM Console] にフォーカスがない状態で Caps Lock キーを一度押し、次に [KVM Console] にフォーカスを置いて Caps Lock キーをもう一度押します。

ログイン パネルからの KVM コンソールの起動

Cisco UCS Central ログイン パネルからサーバの KVM コンソールを起動できます。 LDAP、RBAC、および十分な権限を持つ認証ドメイン ユーザが、ログイン パネルから KVM を起動できます。

手順

ステップ 1 Cisco UCS Central ログイン パネルで [Username] と [Password] を入力します。

ステップ 2 [Launch KVM] をクリックします。
これにより、システムで KVM へのアクセス権限があるサービス プロファイルとサーバのリストを示すページが表示されます。

ステップ 3 KVM コンソールを起動するサーバを検索します。
次のいずれかの方法でサーバを検索できます。

- [Service Profile Name] を入力し、[Search] をクリックしてサービス プロファイルを検索します。
- フィルタリングに使用する [Organization]、[Domain Group]、または [UCS Domain] ドロップダウン オプションをクリックし、[Search] をクリックします。

（注） 結果ページに、グローバル サービス プロファイルとローカル サービス プロファイルに関連付けられているサーバのリストだけが表示されます。

ステップ 4 表示される検索結果リストで、KVM コンソールを起動するサーバをクリックして選択します。

ステップ 5 結果のメニューバーで [KVM Console] をクリックします。
[KVM Console] ダイアログボックスが開き、IP アドレスが表示されます。

ステップ 6 [OK] をクリックします。

ステップ 7 セキュリティ警告が表示されたら同意し、[Add Security Exception] ダイアログボックスで [Yes] をクリックし、セキュリティ証明書を受け入れて続行します。

ステップ 8 [Security Warning] で [Continue] をクリックします。

ステップ 9 KVM コンソールにログインするため、[KVM Login] で Cisco UCS Manager クレデンシャルを入力します。

ステップ 10 別ウィンドウに KVM コンソールが表示されます。

ヒント KVM セッションを開いたときにキーボードの Caps Lock キーがオンになっており、その後に Caps Lock キーをオフにすると、[KVM Console] は Caps Lock キーがオンのときのように動作する場合があります。 KVM コンソールとキーボードを同期させるには、[KVM Console] にフォーカスがない状態で Caps Lock キーを一度押し、次に [KVM Console] にフォーカスを置いて Caps Lock キーをもう一度押します。

第 8 章

サービス プロファイルとテンプレート

この章は、次の内容で構成されています。

グローバル サービス プロファイル

グローバルサービスプロファイルは、データセンターに展開された論理設定を集中管理します。この集中化により、Cisco UCS ドメインのすべてのサービス プロファイルを Cisco UCS Central から一元的に保守できます。 グローバル サービス プロファイルを使用すると、データセンター全体で次の操作を実行できます。

- いずれかの Cisco UCS ドメインからサービス プロファイルの計算要素を選択する。
- 要素間でサービス プロファイルを移行する。
- いずれかの Cisco UCS ドメインで使用可能なグローバル サーバ プールからサーバを選択する。
- ID プールやポリシーなどのグローバル リソースを関連付ける。
- Cisco UCS ドメイン内のいずれかのグローバル ポリシーを参照する。

グローバル サービス プロファイルの作成

Cisco UCS Central GUI または Cisco UCS Central CLI からグローバル サービス プロファイルを作成するか、または Cisco UCS Manager から標準サービス プロファイルとしてグローバル サービス プロファイルを作成し、グローバル ポリシーを参照できます。 Cisco UCS Central からグローバル サービス プロファイルを作成すると、Cisco UCS Central で ID プール、vNIC、vHBA を作成し、ID を参照できます。

グローバル サービス プロファイルの管理 IP アドレスの設定

Cisco UCS ドメインの各サーバには、Cisco Integrated Management Controller（CIMC）またはサーバに関連付けられたサービス プロファイルに割り当てられる 1 つ以上の管理 IP アドレスが必要です。 Cisco UCS Central では、サービス プロファイルを作成するために次の管理 IP アドレスを設定できます。

- ゼロまたは 1 つのアウトバンド IPv4 アドレス。トラフィックはこのアドレスを使用して、管理ポートを介してファブリック インターコネクトを通過します。
- ゼロまたは 1 つのインバンド（IPv4 または IPv6）アドレス。トラフィックはこのアドレスを使用して、ファブリック アップリンク ポートを介してファブリック インターコネクトを通過します。

Cisco UCS Central GUI または CLI で、プールされている管理 IP アドレスまたはスタティック管理 IP アドレスを設定できます。 ただし、グローバル サービス プロファイル テンプレートを使用してグローバル サービス プロファイルを作成する場合は、プールされている管理 IP アドレスだけを設定できます。 スタティック IP アドレスは、このリリースではサポートされていません。

グローバル サービス プロファイルのガイドラインと注意事項

グローバル サービス プロファイルを作成する場合は、次の点に留意してください。

- Cisco UCS Central でグローバル サービス プロファイルを作成すると、システムにより次の情報が検証されます。
  - vNIC、vHBA、iSCSI vNIC などでの od ID の使用
  - vLAN および vSAN 割り当て
  - 可用性指標に基づく計算要素への関連付け
  - サーバ資格情報の基準

    これらの情報におけるすべての非互換性にフラグが付けられます。 これらの問題を解決した後でのみ、グローバル サービス プロファイルを正常に作成できます。
- グローバル サービス プロファイルでポリシー参照が解決された後で、リモート ポリシーのいずれかが変更されると、グローバル サービス ポリシーが再設定されます。
- Cisco UCS Central の VLAN および VSAN はドメイン グループに属します。 VLAN または VSAN をドメイン グループ内で作成する必要があります。 VLAN の場合、グローバル サービス プロファイルの vNIC または vHBA が VLAN または VSAN にアクセスする前に、それらを Orgs に割り当てます。
- グローバル サービス プロファイルの変更、関連付け解除、または削除は、Cisco UCS Central でのみ実行できます。
- Cisco UCS Central ではグローバル サービス プロファイルの名前変更だけが可能です。 サービス プロファイル名を変更すると、Cisco UCS Central によりインベントリで古い名前のグ

ローバル サービス プロファイルが削除され、新しいサービス プロファイルが新しい名前で作成されます。

- グローバルサービスプロファイルに関連付けられているサーバがCisco UCSドメインから削除される場合、サーバを再度確認すると、そのサーバとサービスプロファイルとの関連付けが解除されます。
- Cisco UCS Centralでは、マルチキャスト ポリシーやフロー制御ポリシーなどのドメイン固有のポリシーを定義またはアクセスすることはできません。 ただし、グローバル サービス プロファイルのリソースによってCisco UCS Centralからこれらのポリシーを参照できます。 グローバル サービス プロファイルを定義する場合、利用可能なドメイン固有のポリシーを確認し、サービス プロファイルで名前によってこれらのポリシーを参照できます。 サービス プロファイルが展開されている場合、Cisco UCS ドメインはポリシーに解決され、そのドメインのサービス プロファイルにポリシーが含まれます。
- 展開されたCisco UCS Managerからグローバル・サービス プロファイルをローカライズできます。 ローカライズすると、グローバル サービス プロファイルはCisco UCS Centralから削除されます。 ただし、すべてのグローバル ポリシーは引き続きグローバルのままになります。 グローバル ポリシーをローカライズする場合は、各ポリシーを個別にローカライズする必要があります。

グローバル サービス プロファイルの作成

Cisco UCS Centralでグローバル サービス プロファイルを作成する場合、新しいサービス プロファイルの名前を指定し、その他のすべての情報にシステムのデフォルト値を使用できます。

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで [Servers] > [Global Service Profiles] > [root]を展開します。
サブ組織のグローバルサービスプロファイルを作成するか、またはそのプロファイルにアクセスするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 グローバル サービス プロファイルを作成する組織を右クリックし、[Create Service Profile] を選択します。

ステップ 4 [General] 情報パネルで、[Service Profile Name]、[UUID assignment] を指定し、[Next] をクリックします。
このサービス プロファイルに任意で説明を指定できます。 UUIDが使用できない場合、このパネルからUUID接尾辞プールを作成することもできます。

（注） グローバルサービスプロファイルを手早く作成するには、名前を指定した後で、[Finish] をクリックして構いません。 Cisco UCS Centralは、指定された名前とすべてのシステムデフォルト値で新しいグローバル サービス プロファイルを作成します。

ステップ 5 （任意）[Networking] パネルで、[Dynamic vNIC Connections] と [LAN Connectivity] のセクションに必要な情報を指定して、[Next] をクリックします。

このパネルからダイナミック vNIC 接続ポリシーおよび LAN 接続ポリシーを作成できます。

ステップ 6 （任意）[Storage] パネルで、[Local Storage Policy]、[SAN Connectivity]、[WWNN] などの SAN 設定情報を指定して、[Next] をクリックします。
このパネルからローカル ディスク設定ポリシーおよび SAN 接続ポリシーを作成できます。

ステップ 7 （任意）[vNIC/vHBA Placement] パネルで、配置方法と PCI 順序を指定して [Next] をクリックします。
[Assignment Method] に使用するポリシーが見つからない場合は、VNIC/VHBA 配置ポリシーをこのパネルから作成できます。

ステップ 8 （任意）[Boot Order] パネルで、ドロップダウン リストから [Configuration Type] を指定して [Next] をクリックします。
新しいブート ポリシーを指定する場合は、このパネルからブート ポリシーを作成できます。

ステップ 9 （任意）[Maintenance Policy] パネルで、メンテナンス ポリシーを指定して [Next] をクリックします。
このパネルから、新しいメンテナンスポリシーを作成してメンテナンススケジュールを指定できます。

ステップ 10 （任意）[Server Assignment] パネルで、ドロップダウン リストから [Server Assignment Method] を指定し、[Power State to Apply on Assignment] を指定して、[Next] をクリックします。
[Server Assignment Method] ドロップダウンでの選択内容に基づいて、リストからサーバを選択するか、または Cisco UCS ドメイン内のサーバの場所を指定できます。

ステップ 11 （任意）[Operational Policies] パネルで、システム動作情報（[Host Firmware Management]、[BIOS Configuration]、[External IPMI Management]、[Management IP Address Policy]、[Monitoring Threshold Configuration]、[Power Control Configuration]、[Server Scrub Configuration] など）を指定し、[Finish] をクリックします。
（注） アウトバンド IPv4 アドレス、またはインバンド IPv4 または IPv6 アドレスをセットアップするには、それぞれのタブをクリックして、必須フィールドに入力します。
これらの各設定に必要なポリシーが見つからない場合は、このパネルで作成できます。

次の作業

UCS ドメインにグローバル サービス プロファイルを展開します。

グローバル サービス プロファイルの名前変更

グローバル サービス プロファイルが展開遅延状態にある場合、そのサービス プロファイルの名前は変更できません。

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで [Servers] > [Global Service Profiles] > [root]を展開します。
サブ組織のグローバルサービスプロファイルを作成するか、またはそのプロファイルにアクセスするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [Work] ペインで、名前を変更するグローバル サービス プロファイルの名前をクリックします。
メニュー バーに、選択したグローバル サービス プロファイルのオプションが表示されます。

ステップ 4 [Rename Service Profile] をクリックします。

ステップ 5 [Rename Service Profile] ダイアログボックスで、グローバル サービス プロファイルの新しい名前を入力します。

- グローバルサービスプロファイルがサーバに関連付けられていない場合、サービスプロファイルの古い名前はシステムから削除されます。
- グローバル サービス プロファイルがドメイン内のサーバに関連付けられている場合、Cisco UCS Central は名前変更後のプロファイルを Cisco UCS ドメインにプッシュし、古いグローバル サービス プロファイルの名前を変更します。
- Cisco UCS ドメインが表示されなくなったか、または一時停止状態にある場合、Cisco UCS ドメインが Cisco UCS Central に表示された時点で、名前変更がドメインに通知されます。

ステップ 6 [OK] をクリックします。

グローバル サービス プロファイルの複製

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで [Servers] > [Global Service Profiles] > [root]を展開します。
サブ組織のグローバルサービスプロファイルを作成するか、またはそのプロファイルにアクセスするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [Work] ペインで、名前を変更するグローバル サービス プロファイルの名前をクリックします。
メニュー バーに、選択したグローバル サービス プロファイルのオプションが表示されます。

ステップ 4 [Create a Clone] をクリックします。

ステップ 5 [Create a Clone] ダイアログボックスで [New Name] を入力し、[Org] でこの複製したサービス プロファイルを配置する組織を選択します。
組織を選択すると、[Org Instance] に選択した組織へのリンクが表示されます。

ステップ 6 [OK] をクリックします。

サービス プロファイル テンプレートからのグローバル・サービス プロファイルの作成

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで [Servers] > [Global Service Profile Templates] > [root] を展開します。
サブ組織のグローバル サービス プロファイル テンプレートを作成するか、またはそのテンプレートにアクセスするには、[Sub-Organizations] > *[Organization_Name]* を展開します

ステップ 3 サービス プロファイルの作成元のグローバル サービス プロファイル テンプレートをクリックします。

ステップ 4 [Work] ペインで、[Actions] ドロップダウン リストから [Create Service Profiles From Template] を選択します。

ステップ 5 [Create Service Profiles From Template] ダイアログボックスで、[Name Prefix] を入力し、[Number] で作成するサービス プロファイルの数を選択します。

ステップ 6 [OK] をクリックします。

グローバル サービス プロファイルの削除

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで [Servers] > [Global Service Profiles] > [root]を展開します。
サブ組織のグローバル サービス プロファイルを作成するか、またはそのプロファイルにアクセスするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 削除するグローバル サービス プロファイルを右クリックし、[Delete] を選択します。

ステップ 4 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。

グローバル サービス プロファイルの展開

Cisco UCS Centralからグローバル サービス プロファイルを展開する場合、サービス プロファイルの定義は、Cisco UCS ドメインに送信されます。 その後 Cisco UCS ドメインはサーバを識別し、サーバにサービス プロファイルを展開します。 Cisco UCS ドメインに送信されたサービス プロファイル定義には、次の情報が含まれます。

- 参照ポリシー名を含むサービス プロファイル
- vNIC、vHBA、および vLAN バインディング
- 適切な VCON での VIF の配置に関する VCON 割り当て情報
- このサービス プロファイルの vNIC または vHVA により参照されるグローバル VLAN および VSAN 定義

グローバル サービス プロファイルは、次のいずれかの方法で任意の計算要素に展開できます。

- 直接割り当て：任意の登録済み Cisco UCS ドメイン内の使用可能なサーバの 1 つにグローバル サービス プロファイルを割り当てます。 存在しないサーバを事前にプロビジョニングできます。
- サーバ プール割り当て：サーバ プールにグローバル サービス プロファイルを割り当てます。 グローバル サービス プロファイルは、関連付けのためにプールから使用可能なサーバを 1 つ選択します。
- Cisco UCS ドメインはグローバル サービス プロファイルを受信すると、Cisco UCS ドメインは次の処理を実行します。
  - ローカル レベルでグローバル サービス プロファイルを設定します
  - VLAN および VSAN の状態を解決します
  - 設定および動作状態を Cisco UCS Central に報告します。

サービス プロファイルの関連付けの変更

作成時にサービス プロファイルとサーバ プールを関連付けなかった場合、またはサービス プロファイルが関連付けられているサーバ プールを変更する場合には、次の手順を実行します。

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで [Servers] > [Global Service Profiles] > [root]を展開します。
サブ組織のグローバルサービスプロファイルを作成するか、またはそのプロファイルにアクセスするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 変更するグローバル サービス プロファイルをクリックします。

ステップ 4 [Works] ペインの [Actions] ドロップダウン リストから、[Change Service Profile Association] を選択します。

ステップ 5 [Change Service Profile Association] ダイアログボックスで [Server Assignment Method] を選択し、[Power state to apply on assignment] を選択します。

ステップ 6 [Server Pool] 領域で [Server Pool] を選択し、[Restrict migration of server] をオンまたはオフにします。
新しいサーバ プールを作成することもできます。

ステップ 7 [OK] をクリックします。

ステップ 8 [Save] をクリックします。

グローバル サービス プロファイルからのサーバの割り当て解除

サービス プロファイルからサーバの関連付けを解除すると、Cisco UCS Central により、サーバのオペレーティング システムのシャットダウンが試みられます。 ある程度の時間が経過してもオペレーティング システムがシャットダウンされない場合は、Cisco UCS Central により、サーバが強制的にシャットダウンされます。

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで [Servers] > [Global Service Profiles] > [root]を展開します。
サブ組織のグローバル サービス プロファイルを作成するか、またはそのプロファイルにアクセスするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 変更するグローバル サービス プロファイルをクリックします。

ステップ 4 [Works] ペインの [Actions] ドロップダウン リストから、[Unassign SP] を選択します。

ステップ 5 [Yes] をクリックします。

ステップ 6 [Save] をクリックします。

グローバル サービス プロファイルの名前変更

グローバル サービス プロファイルの名前を変更すると、次のことが起こります。

- サービス プロファイルの以前の名前を参照するイベント ログと監査ログは、その名前のまま保持されます。
- 名前変更の操作を記録する、新しい監査データが作成されます。

- サービス プロファイルの以前の名前で生じたすべての障害データは、新しいサービス プロファイル名に転送されます。

（注） 保留中の変更があるグローバル サービス プロファイルの名前は変更できません。

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで [Servers] > [Global Service Profiles] > [root]を展開します。
サブ組織のグローバルサービスプロファイルを作成するか、またはそのプロファイルにアクセスするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 変更するグローバル サービス プロファイルをクリックします。

ステップ 4 [Works] ペインの [Actions] ドロップダウン リストから、[Rename Service Profile] を選択します。

ステップ 5 [Rename Service Profile] ダイアログボックスで [New Name] を入力します。

ステップ 6 [OK] をクリックします。

サービス プロファイルの UUID の変更

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで [Servers] > [Global Service Profiles] > [root]を展開します。
サブ組織のグローバルサービスプロファイルを作成するか、またはそのプロファイルにアクセスするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 変更するグローバル サービス プロファイルをクリックします。

ステップ 4 [Works] ペインの [Actions] ドロップダウン リストから、[Change UUID] を選択します。

ステップ 5 [Change UUID] ダイアログボックスで、使用する UUID 割り当てを選択します。
UUID 接尾辞プールを作成することもできます。

ステップ 6 [OK] をクリックします。

ステップ 7 [Save] をクリックします。

グローバル サービス プロファイルの UUID のリセット

サービス プロファイルの UUID 割り当てが UUID プールの場合、UUID をリセットすると、選択されている UUID プールから新しい UUID が自動的に割り当てられます。

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで [Servers] > [Global Service Profiles] > [root]を展開します。
サブ組織のグローバル サービス プロファイルを作成するか、またはそのプロファイルにアクセスするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 変更するグローバル サービス プロファイルをクリックします。

ステップ 4 [Works] ペインの [Actions] ドロップダウン リストから、[Reset UUID] を選択します。

ステップ 5 [Yes] をクリックします。

グローバル サービス プロファイルの管理 IP のリセット

管理 IP をリセットすると、選択した IP プールから新しい管理 IP が自動的に割り当てられます。

はじめる前に

管理 IP アドレスをリセットする前に、次の点を検討してください。

- 取得した IP アドレスがプールから削除されない場合などに、プールの IP アドレス ブロックを変更していてはなりません。
- Cisco UCS Central からプールを削除しているか、またはプールが削除されています。
- 更新されたテンプレートを使用してグローバル サービス プロファイルを作成し、プールに新しい名前を割り当てています。

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで [Servers] > [Global Service Profiles] > [root]を展開します。
サブ組織のグローバル サービス プロファイルを作成するか、またはそのプロファイルにアクセスするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 変更するグローバル サービス プロファイルをクリックします。

ステップ 4 [General] 情報パネルの [Management IP Address] の [Work] ペインで、[Reset Management IP] をクリックします。

ステップ 5 [Yes] をクリックします。

ステップ 6 [Save] をクリックします。

グローバル サービス プロファイル テンプレート

グローバル サービス プロファイル テンプレートでは、同じ基本パラメータ（vNIC や vHBA の個数など）と、同じプールから取得された ID 情報を使ってすばやく複数のサービス プロファイルを作成できます。 Cisco UCS Central のサービス プロファイル テンプレートは、Cisco UCS Manager のサービス プロファイル テンプレートに似ています。

グローバル サービス プロファイル テンプレートの作成

Cisco UCS Central でグローバル サービス プロファイル テンプレートを作成する場合、新しいサービスプロファイルテンプレートの名前を指定し、その他のすべての情報にシステムのデフォルト値を使用できます。

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで [Servers] > [Global Service Profile Templates] > [root] を展開します。
サブ組織のグローバル サービス プロファイル テンプレートを作成するか、またはそのテンプレートにアクセスするには、[Sub-Organizations] > *[Organization_Name]* を展開します

ステップ 3 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組織を右クリックし、[Create Service Profile Template] を選択します。

ステップ 4 [General] 情報パネルで、[Service Profile Name]、[Type]、[UUID assignment] を指定し、[Next] をクリックします。
このサービス プロファイルに任意で説明を指定できます。 UUID が使用できない場合、このパネルから UUID 接尾辞プールを作成することもできます。

（注） グローバル サービス プロファイル テンプレートを素早く作成するには、名前を指定した後で、[Finish] をクリックします。 Cisco UCS Central は、指定された名前とすべてのシステム デフォルト値を使用して新しいサービス プロファイル テンプレートを作成します。

ステップ 5 （任意）[Networking] パネルで、[Dynamic vNIC Connections] と [LAN Connectivity] の各セクションに必要な情報を指定して、[Next] をクリックします。
このパネルからダイナミック vNIC 接続ポリシーおよび LAN 接続ポリシーを作成できます。

ステップ 6 （任意）[Storage] パネルで、SAN 設定情報（[Local Storage Policy]、[SAN Connectivity]、[WWNN]、[vHBAs] など）を指定して、[Next] をクリックします。
このパネルからローカル ディスク設定ポリシーおよび SAN 接続ポリシーを作成できます。

ステップ 7 （任意）[vNIC/vHBA Placement] パネルで、配置方法と PCI 順序を指定して [Next] をクリックします。
[Assignment Method] に使用するポリシーが見つからない場合は、VNIC/VHBA 配置ポリシーをこのパネルから作成できます。

ステップ 8 （任意）[Boot Order] パネルで、ドロップダウン リストから [Configuration Type] を指定して [Next] をクリックします。
このパネルからブート ポリシーを作成できます。

ステップ 9 （任意）[Maintenance Policy] パネルで、メンテナンス ポリシーを指定して [Next] をクリックします。
このパネルから、新しいメンテナンスポリシーを作成してメンテナンススケジュールを指定できます。

ステップ 10 （任意）[Server Assignment] パネルで、ドロップダウン リストから [Server Assignment Method] を選択し、[Power State to Apply on Assignment] を指定して、[Next] をクリックします。
[Server Assignment Method] ドロップダウンでの選択内容に基づいて、リストからサーバを選択するか、または Cisco UCS ドメイン内のサーバの場所を指定できます。

ステップ 11 （任意）[Operational Policies] パネルで、システム動作情報（[Host Firmware Management]、[BIOS Configuration]、[External IPMI Management]、[Management IP Address Policy]、[Monitoring Threshold Configuration]、[Power Control Configuration]、[Server Scrub Configuration] など）を指定し、[Finish] をクリックします。
（注） アウトバンド IPv4 アドレス、またはインバンド IPv4 または IPv6 アドレスをセットアップするには、それぞれのタブをクリックして、必須フィールドに入力します。
これらの各設定に必要なポリシーが見つからない場合は、このパネルで作成できます。

グローバル サービス プロファイル テンプレートの複製

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで [Servers] > [Global Service Profile Templates] > [root] を展開します。
サブ組織のグローバル サービス プロファイル テンプレートを作成するか、またはそのテンプレートにアクセスするには、[Sub-Organizations] > *[Organization_Name]* を展開します

ステップ 3 複製するグローバル サービス プロファイル テンプレートをクリックします。

ステップ 4 [Works] ペインの [Actions] ドロップダウン リストから、[Clone Service Profile Template] を選択します。

ステップ 5 [Clone Service Profile Template] ダイアログボックスの [New Name] に新しい名前を入力し、[Org] を選択します。

ステップ 6 [OK] をクリックします。

ステップ 7 作成したサービスプロファイルテンプレートに移動し、すべてのオプションが正しいことを確認します。

グローバル サービス プロファイル テンプレートの削除

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで [Servers] > [Global Service Profile Templates] > [root] を展開します。
サブ組織の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か、またはそのテンプレートにアクセスするには、[Sub-Organizations] > *[Organization_Name]* を展開します

ステップ 3 削除するグローバル サービス プロファイル テンプレートを右クリックし、[Delete] を選択します。

ステップ 4 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。

サービスプロファイルテンプレートへのグローバルサービスプロファイルのバインディング

グローバル サービス プロファイルをグローバル サービス プロファイル テンプレートにバインドすることができます。 サービス プロファイルをテンプレートにバインドした場合、Cisco UCS Centralにより、サービスプロファイルテンプレートに定義された値を使って、サービスプロファイルが設定されます。 既存のサービス プロファイル設定がサービス プロファイル テンプレートに一致しない場合、Cisco UCS Central により、サービス プロファイルが再設定されます。 バインドされたサービス プロファイルの設定は、関連付けられたテンプレートを使用してのみ変更できます。

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで [Servers] > [Global Service Profiles] > [root]を展開します。
サブ組織のグローバルサービスプロファイルを作成するか、またはそのプロファイルにアクセスするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 変更するグローバル サービス プロファイルをクリックします。

ステップ 4 [Works] ペインの [Actions] ドロップダウン リストから、[Bind to Template] を選択します。

ステップ 5 [Bind to Template] ダイアログボックスで [Service Profile Template] を選択します。
新しいサービス プロファイル テンプレートを作成することもできます。

ステップ 6 [OK] をクリックします。

ステップ 7 [Save] をクリックします。

サービス プロファイル テンプレートからのグローバル サービス プロファイルのバインド解除

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで [Servers] > [Global Service Profiles] > [root]を展開します。
サブ組織のグローバルサービスプロファイルを作成するか、またはそのプロファイルにアクセスするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 変更するグローバル サービス プロファイルをクリックします。

ステップ 4 [Works] ペインの [Actions] ドロップダウン リストから、[Unbind from Template] を選択します。

ステップ 5 [Save] をクリックします。

サービス プロファイル更新のスケジュール

サービス プロファイルの遅延展開

サービス プロファイルの変更の一部、またはサービス プロファイル テンプレートの更新は、中断をともなうことや、サーバのリブートが必要になることがあります。 ただし、これらの中断を

ともなう設定変更をいつ実行するかを、遅延展開によって制御できます。たとえば、サービスプロファイルの変更をすぐに展開するか、指定されたメンテナンス時間帯に展開するかを選択できます。また、サービスプロファイルの展開にユーザの明示的な確認応答が必要かどうかを選択できます。

遅延展開は、サーバとサービス プロファイルとの関連付けによって発生するすべての設定変更に使用できます。これらの設定変更は、サービス プロファイルへの変更、サービス プロファイルに含まれるポリシーへの変更、更新サービスプロファイルテンプレートへの変更によってプロンプト表示される場合があります。たとえば、サーバ BIOS、RAID コントローラ、ホスト HBA、ネットワーク アダプタなどのホスト ファームウェア パッケージや管理ファームウェア パッケージによって、ファームウェアのアップグレードおよびアクティブ化を延期することもできます。ただし、Cisco UCS ManagerCisco UCS Central、ファブリック インターコネクト、I/O モジュールなど、ファームウェアパッケージを使用しないコンポーネントのファームウェアイメージの直接展開を遅延させることはできません。

遅延展開は、サーバのリブートを必要とする次のアクションに使用できません。

- サーバのサービス プロファイルの最初の関連付け
- サービス プロファイルと別のサーバを関連付けない、サービス プロファイルのサーバからの関連付けの最終解除
- サーバの解放
- サーバの再認識
- サーバのリセット

サービス プロファイル変更の展開を遅延させる場合、1 つ以上のメンテナンス ポリシーを設定し、各サービス プロファイルにメンテナンス ポリシーを設定する必要があります。展開が発生する時間帯を指定する場合、1 つ以上の繰り返しオカレンスまたはワンタイム オカレンスを持つスケジュールを少なくとも 1 つ作成し、そのスケジュールをメンテナンス ポリシーに含める必要があります。

遅延展開に関するガイドラインおよび制限事項

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へのすべての変更を元に戻すことはできない

保留中の変更をキャンセルする場合、Cisco UCS ManagerCisco UCS Central はサーバを再起動せずに変更のロール バックを試みます。ただし、複雑な変更を行った場合、Cisco UCS ManagerCisco UCS Central は変更のロール バックのためサーバを 2 度目にリブートする必要がある場合があります。たとえば、vNIC を削除すると、Cisco UCS ManagerCisco UCS Central はサービス プロファイルに含まれているメンテナンス ポリシーに従ってサーバをリブートします。サービス プロファイルで元の vNIC を復元しても、この再起動および変更はキャンセルできません。代わりに、Cisco UCS ManagerCisco UCS Central は 2 回目の展開とサーバのリブートをスケジュールします。

サービス プロファイルの関連付けはメンテナンス時間の境界を超えてもよい

Cisco UCS ManagerCisco UCS Centralがサービス プロファイルの関連付けを開始した後、スケジューラとメンテナンス ポリシーは手順を制御する方法を持っていません。 サービス プロファイルの関連付けが割り当てられたメンテナンス時間に完了しない場合、プロセスが完了するまで続行されます。 たとえば、いくつかの段階の再試行やその他の問題のため、関連付けが完了しなかった場合に発生することがあります。

保留中のアクティビティの順序を指定できない

スケジュールされた展開は、独立して並行実行されます。 展開が発生する順序は指定できません。 また、あるサービスプロファイルの変更を他のものの完了を条件として実行することもできません。

保留中のアクティビティの部分的な展開を実行できない

Cisco UCS ManagerCisco UCS Central は、サーバ プロファイルに加えられたすべての変更をスケジュールされたメンテナンス時間に適用します。 サービスプロファイルに複数の変更を加えた後にそれらの変更を別々のメンテナンス時間に振り分けることはできません。 サービスプロファイルの変更を展開するとき、Cisco UCS ManagerCisco UCS Central はデータベース内の最新の設定に一致するようにサービス プロファイルを更新します。

遅延展開スケジュール

スケジュールには、一連のオカレンスが含まれます。 これらのオカレンスは、1 回だけ発生させるか、または毎週指定した日時に繰り返し発生させることができます。 オカレンスの時間長や実行されるタスクの最大数といった、オカレンスで定義されるオプションにより、あるサービス プロファイルの変更が展開されるかどうかが決まります。 たとえば、最大時間長またはタスク数に達したため特定のメンテナンス時間帯に変更を展開できない場合、この展開は次のメンテナンス時間に持ち越されます。

各スケジュールは、Cisco UCS ドメインが 1 つまたは複数のメンテナンス時間に入っているかどうか、定期的に確認します。 入っている場合、スケジュールはメンテナンス ポリシーで指定された制限に対し適切な展開を実行します。

スケジュールには、スケジュールに関連付けられたメンテナンス時間を決定する 1 つ以上のオカレンスが含まれています。 オカレンスは次のいずれかになります。

ワンタイム オカレンス

ワンタイム オカレンスは、単一のメンテナンス時間を定義します。 これらの時間帯は、その時間帯の最大時間長まで、または時間帯の中で実行可能なタスクの最大数に達するまで継続されます。

繰り返しオカレンス

繰り返しオカレンスは、一連のメンテナンス時間を定義します。 これらの時間帯は、タスクの最大数に達するまで、またはオカレンスに指定された日の終わりに達するまで継続します。

メンテナンス ポリシー

メンテナンス ポリシーは、サーバに関連付けられたサービス プロファイル、または 1 つ以上のサービス プロファイルに関連付けられた更新中のサービス プロファイルに対して、サーバのリブートが必要になるような変更が加えられた場合の Cisco UCS Central の対処方法を定義します。

メンテナンス ポリシーは Cisco UCS Central によるサービス プロファイルの変更の展開方法を指定します。 展開は、次のいずれかの方法で実行されます。

- 即時
- ユーザが管理者権限で承認したときに実行する
- スケジュールで指定された時間に自動的に実行する

スケジュール済みのメンテナンス ウィンドウ中に変更を展開するように設定されているメンテナンスポリシーでは、ポリシーに有効なスケジュールが含まれていることが必要です。 この場合、最初に使用可能なメンテナンス ウィンドウ中に変更が展開されます。

（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

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] を展開します。

ステップ 3 [Navigation] ペインで、[Domain Groups] を展開します。

ステップ 4 ポリシーを作成するドメイン グループのノードを展開します。

ステップ 5 [Maintenance] を右クリックし、[Create Maintenance Policy] を選択します。

ステップ 6 [Create Maintenance Policy] ダイアログボックスで、[Name] と説明（任意）を入力し、[Reboot Policy] を選択します。

ステップ 7 [OK] をクリックします。

次の作業

ポリシーはサービス プロファイルまたはサービス プロファイル テンプレートにインクルードします。

スケジュールの作成

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] を展開します。

ステップ 3 スケジュールを作成するドメイン グループのノードを展開します。

ステップ 4 [Schedules] を右クリックし、[Create Schedule] を選択します。

ステップ 5 [Create Schedule] ダイアログボックスで、[Name] と説明（任意）を入力し、[User Ack] チェックボックスをオンにして、明示的なユーザ確認が必要であることを指定します。
このダイアログボックスでは、1 回のオカレンスまたは繰り返しオカレンスを作成することもできます。

ステップ 6 [OK] をクリックします。

次の作業

スケジュールに 1 回のオカレンスまたは繰り返しオカレンスを追加します。

1 回のオカレンスのスケジュールの作成

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。
ステップ 2 [Navigation] ペインで、[Domain Groups] を展開します。
ステップ 3 スケジュールを変更するドメイン グループのノードを展開します。
ステップ 4 [Schedules] を展開します。
ステップ 5 変更するスケジュールをクリックします。
ステップ 6 [Work] ペインで [One Time Occurrence] タブをクリックします。
ステップ 7 [Create One Time Occurrence] をクリックします。
ステップ 8 [Create One Time Occurrence] ダイアログボックスで、[Name] を入力し、[Start Time] を選択します。
ステップ 9 [Maximum Number of Tasks]、[Maximum Number of Concurrent Tasks]、[Maximum Duration]、[Minimum Interval Between Tasks] を選択します。
ステップ 10 [OK] をクリックします。

スケジュールへの繰り返しオカレンスの作成

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。
ステップ 2 [Navigation] ペインで、[Domain Groups] を展開します。
ステップ 3 スケジュールを変更するドメイン グループのノードを展開します。
ステップ 4 [Schedules] を展開します。
ステップ 5 変更するスケジュールをクリックします。
ステップ 6 [Work] ペインで [Recurring Occurrence] タブをクリックします。
ステップ 7 [Create Recurring Occurrence] をクリックします。
ステップ 8 [Create Recurring Occurrence] ダイアログボックスで、[Name] を入力し、開始時刻を選択します。
ステップ 9 [Maximum Number of Tasks]、[Maximum Number of Concurrent Tasks]、[Maximum Duration]、[Minimum Interval Between Tasks] を選択します。
ステップ 10 [OK] をクリックします。

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 は保留中のアクティビティすべてを表示することができます。 ユーザの確認応答を待つアクティビティと、スケジュールされたアクティビティを表示できます。

Cisco UCS ドメインに保留中のアクティビティがある場合、Cisco UCS Central GUI は管理者権限を持つユーザがログインしたときに通知します。

保留中のアクティビティに関連する次の情報を確認できます。

- 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

（注） 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。 メンテナンス期間は、保留中のアクティビティの数およびサービス プロファイルに割り当てられたメンテナンス ポリシーに依存します。 ただし、管理者権限を持つユーザはすべて、ユーザの確認応答を待っているかメンテナンス期間かにかかわらず、手動で保留中のアクティビティを起動し、サーバをすぐにリブートできます。

Cisco UCS Central GUI の次の 2 か所で、保留中アクティビティを確認できます。

- メニュー バーの [Servers] から、[Servers] > [Pending Activities] をクリックします。 保留アクティビティは 2 つのタブ（[User Acknowledged Activities] と [Scheduled Activities]）に表示されます。

- Cisco UCS Central GUI のメニュー バーの上にある障害サマリー パネルでは、次の情報が動的に表示されます。 次の 3 つのオプションのいずれかをクリックすると、関連するページがCisco UCS Central GUI に表示されます。
  - [UCS Central Fault Summary]
  - [UCS Domains Fault Summary]
  - 保留アクティビティ

[Pending Activities] が表示されている場合、このパネルをクリックして、[Servers] > [Pending Activities] に移動し、詳細情報を確認します。

重要 トップ レベルのサマリー パネルには、ローカル スケジューラでローカル メンテナンス ポリシーを使用するローカル サービス プロファイルにより引き起こされた保留アクティビティは表示されません。 これらの保留アクティビティを Cisco UCS Manager から確認する必要があります。

保留アクティビティの表示

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] をクリックします。

ステップ 3 [Work] ペインで [Pending Activities] タブをクリックします。

第 9 章

Global Pools

この章は、次の内容で構成されています。

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。

サーバ プールの作成

サーバを手動でサーバプールに追加するか、またはサーバプールへのサーバの自動追加を選択することができます。 サーバを自動的に追加するには、次のリソースの 1 つ以上がシステムに存在している必要があります。

- 少なくとも 1 つのサーバ プール
- サーバ プール ポリシー資格情報
- サーバ プール ポリシー

サーバ プール、サーバ プール ポリシー資格情報、およびサーバ プール ポリシーの作成方法については、次に示す項で説明します。

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで [Server] > [Pools] > [Root] を展開します。

ステップ 3 [Server Pools] を右クリックし、[Create Server Pool] を選択します。

ステップ 4 [Create Server Pool] ダイアログボックスの [General] タブで、[Name] と説明（任意）を入力します。

ステップ 5 [Next] をクリックします。
サーバ プールにサーバを手動で追加するには、次の手順を実行します。

1. [Create Server Pool] ページで、[Search Server] をクリックします。
2. 追加するサーバのチェックボックスをオンにし、[Select] をクリックします。
3. [Finish] をクリックします。

サーバ プールにサーバを自動的に追加するには、次の手順を実行します。

- サーバポリシー資格情報を作成します。 サーバポリシー資格情報の作成の詳細については、サーバ プール ポリシーの資格情報の作成, （317 ページ）を参照してください。
- サーバ プール ポリシーを作成します。 サーバ プール ポリシーの作成の詳細については、サーバ プール ポリシーの作成, （315 ページ）を参照してください。

サーバ プールの削除

はじめる前に

システムには 1 つ以上のサーバ プールが存在している必要があります。

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、[Server] > [Pools] > [Root] > [Server Pool] を展開します。

ステップ 3 削除するプールを右クリックし、[Delete] をクリックします。
[Estimate Impact] オプションをクリックすると、サーバプールの削除による影響を分析できます。これにより、システムが変更による影響を分析できます。 予測される影響に基づいて、変更を適用するか、またはダイアログボックスを閉じることができます。

ステップ 4 確認のために [Yes] をクリックします。

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 では、IP プールでの IPv4 および IPv6 ブロックの作成と削除がサポートされています。 ただし、iSCSI ブート イニシエータでは IPv4 だけがサポートされています。

IP プールの作成

手順

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Network] タブで、[Network] > [Pools] > [Root] を展開します。
サブ組織のプールを作成したり、それにアクセスしたりするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [IP Pools] を右クリックし、[Create IP Pool] を選択します。

ステップ 4 [Create IP Pool] ダイアログボックスの [General] タブで、必須フィールドに入力します。

ステップ 5 [Create IP Pool] ダイアログボックスの [IP Blocks] タブで、[Create a Block of IPv4 Addresses] をクリックします。

ステップ 6 IPv6 アドレスのブロックを作成するには、[Create IP Pool] ダイアログボックスの [IP Blocks] タブで [Create a Block of IPv6 Addresses] をクリックします。

ステップ 7 該当する [Create a Block of IP addresses]（IPv4 または IPv6）ダイアログボックスで、必須フィールドに入力します。

ステップ 8 [OK] をクリックします。

ステップ 9 [OK] をクリックします。
（注） 別のプールを作成する場合は、5 秒以上待ちます。

次の作業

IP プールをサービス プロファイルとテンプレートのうち一方、または両方に含めます。

IP プールの削除

プールを削除した場合、Cisco UCS ManagerCisco UCS Central は、 Cisco UCS Manager でそのプールの vNIC または vHBA に割り当てられたアドレスを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。

手順

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Network] タブで、[Network] > [Pools] > [Root] を展開します。
サブ組織のプールを作成したり、それにアクセスしたりするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [IP Pools] ノードを展開します。

ステップ 4 削除するプールを右クリックし、[Delete] を選択します。
プールの IPv4 または IPv6 ブロックを削除するには、そのブロックを右クリックして削除します。
（注） 別のプールまたはブロックを削除する場合は、5 秒以上待ちます。

ステップ 5 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。

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、番号の範囲と接尾辞は異なるものの、同じ接頭辞を共有する複数の IQN ブロックを含むことができます。

IQN プールの作成

（注） ほとんどの場合、最大 IQN サイズ（プレフィックス + サフィックス + 追加文字）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。

手順

ステップ 1 メニュー バーで、[Storage] をクリックします。

ステップ 2 [Storage] タブで、[Storage] > [Pools] > [Root] を展開します。
サブ組織のプールを作成したり、それにアクセスしたりするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [IQN Pools] を右クリックし、[Create IQN Pool] を選択します。

ステップ 4 [Create IQN Pool] ダイアログボックスの [General] タブで、必要なプールを入力します。

ステップ 5 [Create IQN Pool] ダイアログボックスの [IQN Blocks] タブで、[Create a Block of IQN Suffixes] をクリックします。

ステップ 6 [Create a Block of IQN] ダイアログボックスで、必須フィールドに入力します。

ステップ 7 [OK] をクリックします。

ステップ 8 [OK] をクリックします。

（注） 別のプールを作成する場合は、5 秒以上待ちます。

次の作業

IQN サフィックス プールをサービス プロファイルとテンプレートのうち一方、または両方に含めます。

IQN プールの削除

プールを削除した場合、Cisco UCS ManagerCisco UCS Central は、 Cisco UCS Manager でそのプールの vNIC または vHBA に割り当てられたアドレスを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。

手順

ステップ 1 メニュー バーで、[Storage] をクリックします。

ステップ 2 [Storage] タブで、[Storage] > [Pools] > [Root] を展開します。
サブ組織のプールを作成したり、それにアクセスしたりするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [IQN Pools] ノードを展開します。

ステップ 4 削除するプールを右クリックし、[Delete] を選択します。

（注） 別のプールを削除する場合は、5 秒以上待ちます。

ステップ 5 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。

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。 残りの桁で構成される UUID 接尾辞は変数です。 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。

UUID 接尾辞プールの作成

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Servers] タブで、[Servers] > [Pools] > [Root] を展開します。
サブ組織のプールを作成したり、それにアクセスしたりするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [UUID Suffix Pools] を右クリックし、[Create UUID Suffix Pool] を選択します。

ステップ 4 [Create UUID Suffix Pool] ダイアログボックスの [General] タブで、必須フィールドに入力します。

ステップ 5 [Create UUID Suffix Pool] ダイアログボックスの [UUID Blocks] タブで、[Create a Block of UUID Suffixes] をクリックします。

ステップ 6 [Create a Block of UUID] ダイアログボックスで、必須フィールドに入力します。

ステップ 7 ブロック資格情報ポリシーを選択します。
ブロック資格情報ポリシーが使用できない場合は、このパネルからブロック資格情報ポリシーを作成できます。

ステップ 8 [OK] をクリックします。

ステップ 9 [OK] をクリックします。
（注） 別のプールを作成する場合は、5 秒以上待ちます。

次の作業

UUID接尾辞プールをサービスプロファイルとテンプレートのうち一方、または両方に含めます。

UUID 接尾辞プールの削除

プールを削除した場合、Cisco UCS ManagerCisco UCS Central は、 Cisco UCS Manager でそのプールの vNIC または vHBA に割り当てられたアドレスを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。

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Servers] タブで、[Servers] > [Pools] > [Root] を展開します。
サブ組織のプールを作成したり、それにアクセスしたりするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [UUID Suffix Pools] ノードを展開します。

ステップ 4 削除するプールを右クリックし、[Delete] を選択します。
（注） 別のプールを削除する場合は、5 秒以上待ちます。

ステップ 5 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。

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 ManagerCisco 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。

MAC プールの作成

手順

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Network] タブで、[Network] > [Pools] > [Root] を展開します。
サブ組織のプールを作成したり、それにアクセスしたりするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [MAC Pools] を右クリックし、[Create MAC Pool] を選択します。

ステップ 4 [Create MAC Pool] ダイアログボックスの [General] タブで、次のフィールドに入力します。

ステップ 5 [Create MAC Pool] ダイアログボックスの [MAC Blocks] タブで、[Create a Block of MAC Addresses] をクリックします。

ステップ 6 [Create a Block of MAC Addresses] ダイアログボックスで、必須フィールドに入力します。

ステップ 7 [OK] をクリックします。

ステップ 8 [OK] をクリックします。
（注） 別のプールを作成する場合は、5 秒以上待ちます。

次の作業

MAC プールを vNIC テンプレートに含めます。

MAC プールの削除

プールを削除した場合、Cisco UCS ManagerCisco UCS Central は、 Cisco UCS Manager でそのプールの vNIC または vHBA に割り当てられたアドレスを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。

手順

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Network] タブで、[Network] > [Pools] > [Root] を展開します。
サブ組織のプールを作成したり、それにアクセスしたりするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [MAC Pools] ノードを展開します。

ステップ 4 削除するプールを右クリックし、[Delete] を選択します。
（注） 別のプールを削除する場合は、5 秒以上待ちます。

ステップ 5 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。

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

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

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。

WWN プールの作成

手順

ステップ 1 メニュー バーで、[Storage] をクリックします。

ステップ 2 [Storage] タブで、[Storage] > [Pools] > [Root] を展開します。
サブ組織のプールを作成したり、それにアクセスしたりするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [WWN Pools] を右クリックし、[Create WWN Pool] を選択します。

ステップ 4 [Create WWN Pool] ダイアログボックスの [General] タブで、必須フィールドに入力します。

ステップ 5 [Create WWN Pool] ダイアログボックスの [WWN Initiator Blocks] タブで、[Create Block] をクリックします。

ステップ 6 [Create Block] ダイアログボックスで、必要なプールを入力します。

ステップ 7 [OK] をクリックします。
（注） 別のプールを作成する場合は、5 秒以上待ちます。

次の作業

- WWPN プールを vHBA テンプレートに含めます。
- WWNN プールをサービスプロファイルとテンプレートのうち一方、または両方に含めます。
- WWxN プールをサービスプロファイルとテンプレートのうち一方、または両方に含めます。

WWN プールの削除

プールを削除した場合、Cisco UCS ManagerCisco UCS Central は、 Cisco UCS Manager でそのプールの vNIC または vHBA に割り当てられたアドレスを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。

手順

ステップ 1 メニュー バーで、[Storage] をクリックします。

ステップ 2 [Storage] タブで、[Storage] > [Pools] > [Root] を展開します。
サブ組織のプールを作成したり、それにアクセスしたりするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [WWN Pools] ノードを展開します。

ステップ 4 削除するプールを右クリックし、[Delete] を選択します。
（注） 別のプールを削除する場合は、5 秒以上待ちます。

ステップ 5 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。

第 10 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 では、LAN クラウド内でドメイン 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 VLAN を定義できます。 1 回の操作で 1 つの VLAN または複数の VLAN を作成できます。

グローバル サービス プロファイルの展開前に、Cisco UCS Central でグローバル VLAN の解決が行われます。 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、その VLAN が存在しない場合は、リソース不足が原因で 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は失敗します。 そのグローバル サービス プロファイルの展開前に、Cisco UCS Central で作成されたすべてのグローバル VLAN を解決しておく必要があります。

グローバル VLAN は、それらを参照するグローバル サービス プロファイルとともに Cisco UCS にプッシュされます。 グローバル VLAN を参照するグローバル サービス プロファイルがその UCS ドメインに展開されている場合にのみ、Cisco UCS Manager がグローバル VLAN 情報を認識できます。 UCS ドメインにグローバル VLAN が展開され、使用可能になると、ローカルで定義されているサービス プロファイルとサービス ポリシーが、そのグローバル VLAN を参照できます。

（注） グローバル VLAN を参照するグローバル サービス プロファイルが削除されても、そのグローバル VLAN は削除されません。

グローバル VLAN を Cisco UCS Manager から削除することはできません。 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 の組織の権限

Cisco UCS Central で設定されたすべての VLAN は、VLAN が作成された組織に共通しています。組織の一部である Cisco UCS Manager インスタンスがリソースをコンシュームできるようにするには、組織の権限を割り当てる必要があります。 VLAN に組織の権限を割り当てると、それらの組織が VLAN を認識できるようになり、組織の一部である Cisco UCS Manager インスタンスによって保守されるサービス プロファイルでそれらの VLAN を参照できます。

VLAN 名前解決は、各ドメイン グループの階層内で行われます。 複数のドメイン グループに同名の VLAN が存在している場合、組織の権限は、それらのドメイン グループで同名のすべての VLAN に適用されます。

VLAN の組織の権限を作成、変更、または削除できます。

（注） VLAN の組織の権限を削除する場合は、必ずその権限を作成した組織から削除してください。Cisco UCS Central GUI では、この VLAN が関連付けられている組織の構造を確認できます。ただし、Cisco UCS Central CLI では、サブ組織レベルでの VLAN の組織の権限の関連付け階層を確認できないため、Cisco UCS Central CLI でサブ組織レベルで VLAN を削除しようとすると削除操作が失敗します。

単一 VLAN の作成

この手順では、ドメイン グループ ルートまたは特定のドメイン グループで 1 つの VLAN を作成する方法について説明します。

重要

VLAN 名の大文字と小文字は区別されます。

手順

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、次のいずれかを実行します。

- ドメイン グループ ルートに VLAN を追加するには、[Domain Group root] > [LAN] > [LAN Cloud] を展開します。
- 特定のドメイン グループに VLAN を追加するには、そのノードを展開し、[LAN Cloud] をクリックします。

ステップ 3 [LAN Cloud] を右クリックし、[Create VLANs] をクリックします。
[Create VLANs] ダイアログボックスでは、[Single VLAN] がデフォルトで選択されています。

ステップ 4 [VLAN Name] と [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
- 他のドメイン グループですでに定義されている他の VLAN ID と重複する ID

ステップ 5 [OK] をクリックします。
[LAN Cloud] の [Common VLANs] のリストに VLAN が追加されます。

複数の VLAN の作成

この手順では、ドメイン グループ ルートまたは特定のドメイン グループで複数の VLAN を作成する方法について説明します。

重要

VLAN 名では、大文字と小文字が区別されます。

手順

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、次のいずれかを実行します。

- ドメイン グループ ルートに複数の VLAN を追加するには、[Domain Group root] > [LAN] > [LAN Cloud] を展開します。
- 特定のドメイン グループに複数の VLAN を追加するには、そのノードを展開し、[LAN Cloud] をクリックします。

ステップ 3 [LAN Cloud] を右クリックし、[Create VLANs] を選択します。

ステップ 4 [Multiple VLANs] をクリックし、[VLAN Prefix] を入力します。

ステップ 5 [VLAN IDs] を入力します。
個々の VLAN ID またはカンマで区切った ID の範囲を指定できます。 VLAN ID には次の値を入力できます。

- 1 ～ 3967
- 4048 ～ 4093
- 他のドメイン グループですでに定義されている他の VLAN ID と重複する ID

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 を入力します。

ステップ 6 [OK] をクリックします。
[LAN Cloud] の [Common VLANs] のリストに、VLAN が追加されます。

VLAN の削除

この手順では、ドメイン グループ ルートまたは特定のドメイン グループから 1 つ以上の VLAN を削除する方法について説明します。

はじめる前に

Cisco UCS Central でグローバル VLAN を削除する前に、以下の事項を検討してください。

- グローバル VLAN を削除する前に、グローバル VLAN を参照しているすべてのグローバル サービス プロファイルが更新されていることを確認します。
- ドメイン グループから最後のグローバル VLAN を削除する前に、その組織の権限を削除する必要があります。
- グローバル VLAN を削除すると、その VLAN が存在するドメイン グループに関連付けられているすべての登録済み Cisco UCS Managerインスタンスからも削除されます。
- Cisco UCS Central で削除されたグローバル VLAN を参照しているグローバル サービス プロファイルは、リソース不足が原因で失敗します。 削除されたグローバル VLAN を参照しているローカル サービス プロファイルは、仮想ネットワーク ID 1 に設定されます。

手順

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、次のいずれかを実行します。

- ドメイン グループ ルートから 1 つ以上の VLAN を削除するには、[Domain Group root] を展開し、[Common VLAN] をクリックします。
- 特定のドメイン グループから 1 つ以上の VLAN を削除するには、ノードを展開し、[Common VLANs] をクリックします。

ステップ 3 [Navigation] ペインで、削除する 1 つ以上の VLAN を強調表示します。
Shift キーを押しながらクリックする操作または Ctrl キーを押しながらクリックする操作を使用して、複数の VLAN を選択できます。

ステップ 4 強調表示された 1 つ以上の VLAN を右クリックし、[Delete] を選択します。

ステップ 5 [Confirm] ダイアログ ボックスで、次のいずれかを選択します。

- 1 つ以上の VLAN を即時に削除する場合は、[Yes] をクリックします。
- [UCS Domain Impact]、[UCS Central Pending Changes]、および [UCS Central Issues Reported] の情報を表示するには、[Estimate Impact] をクリックします。

ステップ 6 [Estimate Impact] を選択した後で削除操作に進むには、[Apply Changes] をクリックします。

VLAN への組織の権限の割り当て

この手順では、VLAN へ組織の権限を割り当てる方法について説明します。

（注） 組織の権限は、一度に 1 つの VLAN だけに割り当てることができます。 Cisco UCS Central で割り当てられた VLAN の組織の権限は、Cisco UCS Manager には影響しません。

手順

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、次のいずれかを実行します。

- ドメイン グループ ルートで VLAN 権限を割り当てるには、[Domain Group root] を展開し、[Common VLANs] をクリックします。
- 特定のドメインで VLAN 権限を割り当てるには、そのドメイン グループのノードを展開し、[Common VLANs] をクリックします。

ステップ 3 組織の権限を割り当てる VLAN を強調表示します。

ステップ 4 右クリックし、[Properties] を選択します。

ステップ 5 [Properties] ダイアログボックスの [Org Permissions] タブをクリックし、[Modify Org Permissions] ボタンをクリックします。

ステップ 6 表示されるウィンドウで [root] を展開し、該当する組織またはサブ組織の横のチェックボックスをオンにします。
[root] を選択すると、ドメイン グループ ルートの下のすべてのドメイン グループに VLAN 権限が割り当てられます。 ルートの下の 1 つの組織（たとえば [Sub-Org 1] など）を選択すると、そのサブ組織に属する組織だけに VLAN 権限が割り当てられます。 ルートの下に複数のサブ組織があり、VLAN 権限を複数のサブ組織に割り当てる場合は、兄弟サブ組織の横にあるチェックボックスをオンにします。

ステップ 7 [OK] をクリックします。

VLAN 権限を割り当てた組織が、[Work] ペインの [Org Permissions] タブの [Selected:] 領域に表示されます。

VLAN の組織の権限の変更

Cisco UCS Central では、VLAN の組織の権限を変更して、組織の権限をすべて削除するか、または現在有効な権限を変更することができます。 この手順では、ルート組織またはサブ組織の VLAN の VLAN 権限を変更する方法について説明します。

（注） 一度に 1 つの VLAN のみについて、組織の権限を変更できます。

手順

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、次のいずれかを実行します。

- ドメイン グループ ルートの VLAN の組織の権限を変更するには、[Domain Group root] > [Common VLANs] を展開します。
- 特定のドメイン グループの VLAN の組織を変更するには、そのノードを展開し、[Common VLANs] をクリックします。

ステップ 3 変更する VLAN を強調表示します。

ステップ 4 強調表示された VLAN を右クリックし、[Properties] をクリックします。

ステップ 5 [Properties] ダイアログボックスの [Org Permissions] タブをクリックし、[Modify Org Permissions] ボタンをクリックします。

ステップ 6 表示されるウィンドウで [root] を展開し、VLAN の権限を変更する組織とサブ組織の横にあるボックスをオンまたはオフにします。

ステップ 7 [OK] をクリックします。

VLAN の組織の権限の削除

VLAN の組織の権限を削除する場合は、その権限を作成した組織から削除する必要があります。このようにしないと、削除操作は失敗します。

手順

ステップ 1 [Network] タブで、[Network] > [VLAN Org Permissions] をクリックします。
[Work] ペインに、システムで使用可能な組織の権限のリストが表示されます。

ステップ 2 クリックして、削除する組織の権限の名前を選択します。

ステップ 3 [Confirm] ダイアログボックスで、[OK] をクリックします。

グローバル VSAN

Cisco UCS Central では、SAN クラウド内でドメイン 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 を定義できます。 Cisco UCS Central で作成されるグローバル VSAN は、作成したファブリック インターコネクトに固有です。 ファブリック A または ファブリック B のいずれか、あるいはファブリック A と B の両方に VSAN を割り当てることができます。 グローバル VSAN は、Cisco UCS Central の共通 VSAN ではありません。

グローバル VSAN を参照するグローバル サービス プロファイルを Cisco UCS Central に展開する前に、Cisco UCS Manager でグローバル VSAN の解決が行われます。 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、その VSAN が存在しない場合、リソース不足が原因でそのグローバル サービス プロファイルの Cisco UCS Manager への展開が失敗します。 そのグローバル サービス プロファイルの展開前に、Cisco UCS Central で作成されたすべてのグローバル VSAN を解決しておく必要があります。

グローバル サービス プロファイルとともに展開される VSAN は、VSAN を参照するグローバル サービス プロファイルが展開されている場合にのみ、Cisco UCS Manager により認識されます。 グローバル サービス プロファイルとともに展開される VSAN が Cisco UCS Manager で利用可能になると、ローカルに定義されているサービス プロファイルとポリシーでその VSAN を参照できます。 グローバル VSAN を参照するグローバル サービス プロファイルが削除されても、そのグローバル VLAN は削除されません。

Cisco UCS Manager インスタンスに対して使用可能なグローバル サービス プロファイルで参照されるグローバル VSAN は、ドメイン グループからの使用の目的で削除される場合を除き、引き続き使用可能です。 グローバル VSAN は Cisco UCS Manager でローカライズできます。この場合、グローバル VSAN はローカル VSAN として機能します。 グローバル VSAN がローカライズされない場合、その VSAN はCisco UCS Manager からは削除できません。

VSAN の作成

次の予約済み範囲の ID を除き、ID が 1 ～ 4093 の範囲の 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 は違っている必要があります。VSAN 内の FCoE VLAN と VLAN に同じ 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が発生し、トラフィックが中断されます。 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。

この手順では、ドメイン グループ ルートまたは特定のドメインで VSAN を作成する方法について説明します。 VSAN の作成時に、VSAN をファブリック A またはファブリック B のいずれかまたは両方に割り当てることができます。

手順

ステップ 1 メニュー バーで、[Storage] をクリックします。

ステップ 2 [Navigation] ペインで、次のいずれかを実行します。

- ドメイン グループ ルートに VSAN を追加するには、[Domain Group root] > [SAN] > [SAN Cloud] を展開します。
- 特定のドメイン グループに VSAN を追加するには、そのノードを展開し、[SAN Cloud] をクリックします。

ステップ 3 [SAN Cloud] を右クリックし、[Create VSAN] をクリックします。
[Create VSAN] ダイアログボックスでは、[Fabric A] がデフォルトで選択されています。

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

- VSAN をファブリック A だけに追加するには、[Name]、[VSAN ID]、および [FCoE VLAN ID] を入力します。
- VSAN をファブリック B だけに追加するには、[Fabric B] オプション ボタンをクリックし、[Name]、[VSAN ID]、および [FCoE VLAN ID] を入力します。
- 両方のファブリック インターコネクトに VSAN を追加するには、[Fabric A and Fabric B] オプション ボタンをクリックします。

両方のファブリック インターコネクトが選択されている場合、[Create VSAN] ダイアログボックスの下部にある [Fabric A] と [Fabric B] の両方で [VSAN ID] と [FCoE VLAN ID] フィールドが表示されます。

ステップ 5 [Name] を入力します。

ステップ 6 必要に応じて、[Fabric A] と [Fabric B] の両方の [ID] と [FCoE VLAN ID] を変更します。

ステップ 7 ファイバ チャネルのゾーン分割を有効にするには、[FC Zoning] パネルの [Enabled] オプション ボタンを選択します。

ファイバ チャネル ゾーン分割を次のいずれかに設定できます。

- [disabled]：アップストリーム スイッチがファイバ チャネル ゾーン分割を設定および制御します。または、ファイバ チャネル ゾーン分割がこの VSAN で実装されていません。
- [enabled]：VSAN の展開時に、Cisco UCS Manager によりファイバ チャネル ゾーン分割が設定、制御されます。

（注） デフォルトではファイバ チャネル ゾーン分割は無効になっています。

ステップ 8 [OK] をクリックします。
Cisco UCS Central GUI が VSAN をファブリック A またはファブリック B の [VSANs] に追加するか、またはファブリック A とファブリック B の両方の [VSANs] に追加します。

VSAN の変更

VSAN ID、FCoE VLAN、または Fibre Connect ゾーン分割設定を変更するには、Cisco UCS Central で VSAN を変更できます。

（注） VSAN の作成後には、ファブリック インターコネクトの割り当ては変更できません。

はじめる前に

手順

ステップ 1 メニュー バーで、[Storage] をクリックします。

ステップ 2 [Navigation] ペインで、次のいずれかを実行します。

- ドメイン グループ ルートで VSAN を変更するには、[Domain Group root] > [SAN Cloud] > [VSANs] > [Fabric A] または > [Fabric B] を展開し、変更する VSAN を見つけます。
- 特定のドメイン グループの VSAN を変更するには、そのノードを展開し、[Fabric A] または [Fabric B] をクリックし、変更する VSAN を見つけます。

ステップ 3 VSAN を強調表示し、右クリックして [Properties] を選択します。

ステップ 4 [Properties] ダイアログボックスで、[ID]、[FCoE VLAN ID]、または [FC Zoning] を変更します。
ファイバ チャネル ゾーン分割を次のいずれかに設定できます。

- [disabled]：アップストリーム スイッチがファイバ チャネル ゾーン分割を設定および制御します。または、ファイバ チャネル ゾーン分割がこの VSAN で実装されていません。
- [enabled]：VSAN の展開時に、Cisco UCS Manager によりファイバ チャネル ゾーン分割が設定、制御されます。

（注） デフォルトではファイバ チャネル ゾーン分割は無効になっています。

ステップ 5 [OK] をクリックします。

VSAN の削除

この手順では、ドメイン グループ ルートまたは特定のドメイン グループから 1 つ以上の VSAN を削除する方法について説明します。

手順

ステップ 1 メニュー バーで、[Storage] をクリックします。

ステップ 2 [Navigation] ペインで、次のいずれかを実行します。

- ドメイン グループ ルートから 1 つ以上の VSAN を削除するには、[Domain Group root] > [SAN] > [SAN Cloud] > [Fabric A] または > [Fabric B] を展開し、[VSANs] をクリックします。
- 特定のドメイン グループから 1 つ以上の VSAN を削除するには、ノードを [Fabric A] または [Fabric B] に展開し、[VSANs] をクリックします。

ステップ 3 [Navigation] ペインで、削除する 1 つ以上の VSAN を強調表示します。
Shift キーを押しながらクリックする操作または Ctrl キーを押しながらクリックする操作を使用して、複数の VSAN を選択できます。

ステップ 4 強調表示された 1 つ以上の VSAN を右クリックし、[Delete] を選択します。

ステップ 5 [Confirm] ダイアログで、次のいずれかを選択します。

- 1 つ以上の VSAN を即時に削除する場合は、[Yes] をクリックします。
- [UCS Domain Impact]、[UCS Central Pending Changes]、および [UCS Central Issues Reported] の情報を表示するには、[Estimate Impact] をクリックします。

ステップ 6 [Estimate Impact] を選択した後で削除操作に進むには、[Apply Changes] をクリックします。

第 11 章

ポリシーの操作

この章は、次の内容で構成されています。

グローバル ポリシー

Cisco UCS Central でグローバル ポリシーを作成、管理し、1 つ以上の Cisco UCS ドメイン のサービス プロファイルまたはサービス プロファイル テンプレートにグローバル ポリシーを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 テンプレートとサービス プロファイルは次のいずれかです。

- 1 つの Cisco UCS ドメイン で Cisco UCS Manager により作成および管理されるローカル 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だけ関連付けることができます。 ローカル サービス プロファイルにグローバル ポリシーを追加すると、Cisco UCS Manager では、そのポリシーのローカル読み取り専用コピーが作成されます。
- Cisco UCS Central により作成および管理されるグローバル 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 つ以上の登録済み Cisco UCS ドメイン 内のサーバにグローバル サービス プロファイルを関連付けることができます。

Cisco UCS Central ではグローバル ポリシーだけを変更できます。 これらの変更は、そのグローバル 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。 Cisco UCS Manager ではすべてのグローバル ポリシーは読み取り専用です。

IPv6アドレスを使用して、ドメイングループ内のすべての動作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] タブにあります。

この機能は、Cisco UCS Central からこれらのポリシーをインポートするときに Cisco UCS Manager が IPv6 アドレスを使用できるようにします。

グローバル ポリシーの作成

[Servers] タブ、[Network] タブ、および [Storage] タブでグローバル ポリシーを作成できます。

はじめる前に

このタスクを実行するための管理権限を持つ管理者またはユーザとしてログインする必要があります。

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Policies] を展開し、次に [root] を展開します。
サブ組織のグローバル ポリシーを作成するには、[Sub-Organizations] > [Organization_Name] を展開します。

ステップ 3 ツリーで、その下にグローバル ポリシーを作成するアイテムを選択します。

ステップ 4 画面の右側のペインで [Create] をクリックします。

ステップ 5 [Create] ウィンドウで、[Name]、[Description]、およびその他の情報を入力します。

ステップ 6 [OK] をクリックします。
グローバル ポリシーが作成され、ツリーに表示されます。

（注） [Network] タブと [Storage] タブにグローバル ポリシーを作成するには、該当するタブをクリックし、前述の手順のステップ 2 から 6 を実行します。

ローカル サービス プロファイルへのグローバル ポリシーの追加

手順

ステップ 1 Cisco UCS Manager を起動します。
Cisco UCS Manager は、Cisco UCS Central GUI で起動できます（を参照）。

ステップ 2 Cisco UCS Manager の [Navigation] ペインで、[Servers] タブをクリックします。

ステップ 3 [Servers] タブで、[Servers] > [Service Profiles] を展開します。

ステップ 4 グローバル ポリシーを追加するサービス プロファイルが含まれる組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

サービス プロファイルがサブ組織に含まれている場合は、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 5 グローバル ポリシーを追加するサービス プロファイルを選択します。

ステップ 6 [Work] ペインの [Policies] タブをクリックします。

ステップ 7 グローバル ポリシーを追加するポリシーをクリックします。

ステップ 8 [Policy] ドロップダウン リストからグローバル ポリシーを選択します。

ステップ 9 [Save Changes] をクリックします。

グローバル ポリシーとローカル ポリシー間の変換

特定の状況では、Cisco UCS Manager でグローバル ポリシーをローカル ポリシーに、またはローカル ポリシーをグローバル ポリシーに変換できます。

グローバル サービス プロファイルおよびテンプレートは、グローバル ポリシーだけを参照できます。 展開時に、グローバル サービス プロファイルおよびテンプレートに含まれているグローバル ポリシーをローカル ポリシーに変換することはできません。 最初にグローバル ポリシーを使用するサービス プロファイルまたはポリシー（LAN または SAN 接続ポリシー、vNIC または vHBA テンプレートなど）をローカルに変換する必要があります。

サービス プロファイルが Cisco UCS Central でグローバル テンプレートを参照し、このテンプレートにグローバル ポリシーが含まれている場合、テンプレートの所有権はサービス プロファイルにあります。 グローバル ポリシーの所有権はCisco UCS Central にあるため、Cisco UCS Manager を使用してこのポリシー所有権を変更することはできません。 ポリシーがローカル サービス プロファイルまたはテンプレートに含まれる場合にのみ、ローカルでポリシー所有権を変更できます。

グローバル ポリシーからローカル ポリシーへの変換

グローバル ポリシーをローカル ポリシーに変更できるのは、そのポリシーがローカル サービス プロファイルまたはサービス プロファイル テンプレートに含まれている場合に限ります。

はじめる前に

このタスクを実行するための管理権限を持つ管理者またはユーザとしてログインする必要があります。

手順

ステップ 1 Cisco UCS Manager を起動します。
Cisco UCS Manager は、Cisco UCS Central GUI で起動できます（Cisco UCS ドメイン の Cisco UCS Manager の起動を参照）。

ステップ 2 Cisco UCS Manager の [Navigation] ペインで、ポリシーがあるタブをクリックします。

たとえば、サーバ関連ポリシーを変換する場合は [Servers] タブ、ネットワーク関連ポリシーを変更する場合は [LAN] タブ、ストレージ関連ポリシーを変換する場合は [SAN] タブをクリックします。

ステップ 3 [Navigation] ペインで [Policies] を展開します。

ステップ 4 変換するポリシーを含む組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ポリシーがサブ組織に含まれている場合は、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 5 ローカルに変換するグローバル ポリシーを選択します。

ステップ 6 [Actions] セクションで [Use Local] をクリックします。

ステップ 7 Cisco UCS Manager 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。

これで、ポリシーがローカル ポリシーになり、Cisco UCS Manager で管理できようになりました。

ローカル ポリシーからグローバル ポリシーへの変換

ローカル ポリシーの所有権をグローバルに変更できるのは、ローカル ポリシーがサービス プロファイルに関連付けられている場合だけです。

はじめる前に

このタスクを実行するための管理権限を持つ管理者またはユーザとしてログインする必要があります。

手順

ステップ 1 Cisco UCS Manager を起動します。
Cisco UCS Manager は、Cisco UCS Central GUI で起動できます（Cisco UCS ドメイン の Cisco UCS Manager の起動を参照）。

ステップ 2 Cisco UCS Manager の [Navigation] ペインで、ポリシーがあるタブをクリックします。
たとえば、サーバ関連ポリシーを変換する場合は [Servers] タブ、ネットワーク関連ポリシーを変更する場合は [LAN] タブ、ストレージ関連ポリシーを変換する場合は [SAN] タブをクリックします。

ステップ 3 [Navigation] ペインで [Policies] を展開します。

ステップ 4 変換するポリシーを含む組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ポリシーがサブ組織に含まれている場合は、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 5 グローバルに変換するローカル ポリシーを選択します。

ステップ 6 [Actions] 領域で、[Use Global] をクリックします。

ステップ 7 Cisco UCS Manager 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。

これでポリシーがグローバル ポリシーになりました。グローバル ポリシーは Cisco UCS Central でのみ管理でき、Cisco UCS Manager では読み取り専用ポリシーとして表示されます。

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。
[Time Zone 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。
[Global Fault 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。

名前	説明
[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]	SEL 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。
[Power Allocation Policy]	グローバル電力割り当て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。
[Power Policy]	電源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。

ポリシー解決の変更結果

Cisco UCS ドメインを登録するときに、ローカルまたはグローバルの解決のポリシーを設定します。 Cisco UCS ドメインの登録時、または登録や設定の変更時の動作は、ドメイン グループ割り当ての有無などのさまざまな要因に応じて異なります。

次の表に、ポリシー タイプ別の予期されるポリシー解決動作を説明します。

ポリシーおよび設定	**Policy Source**		**Cisco UCS Central 登録時の Cisco UCS Manager での動作**		**登録変更時の Cisco UCS Manager での動作**	
	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	ドメイン グループの割り当て	ローカル	ローカル/リモート	最後に確認されたポリシーの状態を維持	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	ドメイン グループの割り当て	ローカル	ローカル/リモート	最後に確認されたポリシーの状態を維持	ローカル ポリシーに変換される
HTTP	該当なし Cisco UCS Manager のみ	ドメイン グループの割り当て	ローカル	ローカル/リモート	最後に確認されたポリシーの状態を維持	ローカル ポリシーに変換される

ポリシーおよび設定	Policy Source		Cisco UCS Central 登録時の Cisco UCS Manager での動作		登録変更時の Cisco UCS Manager での動作	
	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
Telnet	該当なし Cisco UCS Manager のみ	ドメイン グループの割り当て	ローカル	ローカル/リモート	最後に確認されたポリシーの状態を維持	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	ドメイン グループの割り当て	ローカル	ローカル/リモート	最後に確認されたポリシーの状態を維持	ローカル ポリシーに変換される
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	ドメイン グループの割り当て	ローカル	ローカル/リモート	最後に確認されたポリシーの状態を維持	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	ドメイン グループの割り当て	ローカル	ローカル/リモート	最後に確認されたポリシーの状態を維持	ローカル ポリシーに変換される
電力ポリシー（別名 PSU ポリシー）	該当なし Cisco UCS Manager のみ	ドメイン グループの割り当て	ローカル	ローカル/リモート	最後に確認されたポリシーの状態を維持	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	ドメイン グループの割り当て	ローカル	ローカル/リモート	最後に確認されたポリシーの状態を維持	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	ドメイン グループの割り当て	ローカル	ローカル/リモート	最後に確認されたポリシーの状態を維持	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	ドメイン グループの割り当て	ローカル	ローカル/リモート	最後に確認されたポリシーの状態を維持	ローカル ポリシーに変換される
LDAP プロバイダー グループおよびグループ マップ	該当なし Cisco UCS Manager のみ	ドメイン グループの割り当て	ローカル	ローカル/リモート	最後に確認されたポリシーの状態を維持	ローカル ポリシーに変換される

ポリシーおよび設定	Policy Source		Cisco UCS Central 登録時の Cisco UCS Manager での動作		登録変更時の Cisco UCS Manager での動作	
	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
TACACS（プロバイダー グループを含む）	該当なし Cisco UCS Manager のみ	ドメイン グループの割り当て	ローカル	ローカル/リモート	最後に確認されたポリシーの状態を維持	ローカル ポリシーに変換される
RADIUS（プロバイダー グループを含む）	該当なし Cisco UCS Manager のみ	ドメイン グループの割り当て	ローカル	ローカル/リモート	最後に確認されたポリシーの状態を維持	ローカル ポリシーに変換される
SSH（読み取り専用）	ドメイン グループ ルート	ドメイン グループの割り当て	ローカル	ローカル/リモート	最後に確認されたポリシーの状態を維持	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	ドメイン グループの割り当て	ローカル	ローカル/リモート	最後に確認されたポリシーの状態を維持	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	ドメイン グループの割り当て	ローカル	ローカル/リモート	最後に確認されたポリシーの状態を維持	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	ドメイン グループの割り当て	ローカル	ローカル/リモート	最後に確認されたポリシーの状態を維持	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	ドメイン グループの割り当て	ローカル	ローカル/リモート	最後に確認されたポリシーの状態を維持	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	ドメイン グループの割り当て	ローカル	ローカル/リモート	最後に確認されたポリシーの状態を維持	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	ドメイン グループの割り当て	ローカル	ローカル/リモート	最後に確認されたポリシーの状態を維持	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	ドメイン グループの割り当て	ローカル	ローカル/リモート	最後に確認されたポリシーの状態を維持	ローカル ポリシーに変換される

ポリシーおよび設定	Policy Source		Cisco UCS Central 登録時の Cisco UCS Manager での動作		登録変更時の Cisco UCS Manager での動作	
	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
Default Authentication	ドメイン グループ ルート	ドメイン グループの割り当て	ローカル	ローカル/リモート	最後に確認されたポリシーの状態を維持	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	ドメイン グループの割り当て	ローカル	ローカルまたはリモートにできます	最後に確認されたポリシーの状態を維持	ローカル ポリシーに変換される
Roles	ドメイン グループ ルート	ドメイン グループの割り当て	ローカル	ローカル/結合（ローカルがリモートに置き換わる）	リモート ポリシーが削除される	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	ドメイン グループの割り当て	ローカル	ローカル/結合（ローカルがリモートに置き換わる）	リモート ポリシーが削除される	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	ドメイン グループの割り当て	ローカル	ローカル/結合（ローカルがリモートに置き換わる）	リモート ポリシーが削除される	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 パッケージ	該当なし	ドメイン グループの割り当て	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の状態を維持	ローカル ポリシーに変換される

ポリシーおよび設定	**Policy Source**		**Cisco UCS Central 登録時の Cisco UCS Manager での動作**		**登録変更時の Cisco UCS Manager での動作**	
	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**
カタログ	該当なし	ドメイン グループの割り当て	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の状態を維持	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 パッケージ	該当なし	ドメイン グループの割り当て	ポリシー解決でのサービス プロファイルの変更結果, （224 ページ） を参照してください。	ポリシー解決でのサービス プロファイルの変更結果, （224 ページ） を参照してください。	リモート ポリシーが削除される	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 パッケージ	該当なし	ドメイン グループの割り当て	ポリシー解決でのサービス プロファイルの変更結果, （224 ページ） を参照してください。	ポリシー解決でのサービス プロファイルの変更結果, （224 ページ） を参照してください。	リモート ポリシーが削除される	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 パッケージ	該当なし	ドメイン グループの割り当て	ポリシー解決でのサービス プロファイルの変更結果, （224 ページ） を参照してください。	ポリシー解決でのサービス プロファイルの変更結果, （224 ページ） を参照してください。	リモート ポリシーが削除される	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 プロファイルの変更結果

一部のポリシーでは、そのポリシーが含まれている 1 つ以上のサービス プロファイルが更新されたかどうかもポリシー解決の動作に影響します。

次の表に、このようなポリシーで予期されるポリシー解決動作を説明します。

ポリシー（Policy）	Cisco UCS Central 登録時の Cisco UCS Manager での動作		Cisco UCS Central への登録後に割り当てられるドメイン 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 プロファイル未変更	サービス プロファイル変更済み	
メンテナンス ポリシー	ローカル	ローカル。ただしドメイン グループの割り当て時に「デフォルト」ポリシーが更新されます。	ローカル/リモート（登録後に「デフォルト」に解決される場合）。
スケジュール	ローカル	ローカル。ただしドメイン グループの割り当て時に「デフォルト」ポリシーが更新されます。	ローカル/リモート（登録後に「デフォルト」に解決される場合）。
ホスト ファームウェア パッケージ	ローカル	ローカル。ただしドメイン グループの割り当て時に「デフォルト」ポリシーが更新されます。	ローカル/リモート（登録後に「デフォルト」に解決される場合）。

Cisco UCS Manager GUI を使用した Cisco UCS Manager と Cisco UCS Central 間のポリシー解決の変更

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブで、[All] > [Communication Management] を展開します。

ステップ 3 [UCS Central] ノードをクリックします。

ステップ 4 [Actions] 領域の、[UCS Central] をクリックします。

ステップ 5 [Policy Resolution Control] 領域の各フィールドで、次のいずれかのオプション ボタンをクリックします。

- [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。

ステップ 6 [Save Changes] をクリックします。

Cisco UCS Central でのポリシーおよびポリシー コンポーネントのインポート

Cisco UCS Central では、ポリシー、プール、vLAN、vSAN を、1 つの登録済み Cisco UCS ドメインから Cisco UCS Central に直接インポートできます。 いずれかの UCS ドメインに完全なポリシーまたはポリシー コンポーネントがある場合は、そのポリシーをインポートし、複数のドメインに適用できます。 このインポート オプションでは、1 つの登録済み UCS ドメインからポリシーをインポートし、複数の UCS ドメインにポリシーを適用する操作を 1 回のクリックで実行できます。

Cisco UCS Central GUI を使用して、登録済み UCS ドメインのポリシーまたはコンポーネントを検索できます。 また、使用可能なフィルタを使用して検索を絞り込むこともできます。 検索結果からポリシーまたはコンポーネントを選択し、Cisco UCS Central にインポートします。

（注） 検索結果の件数が 1000 を超える場合、結果は切り捨てられます。 フィルタを使用して検索を絞り込んでください。

インポートするポリシーまたはコンポーネントに応じて、次のいずれかの宛先にインポートできます。

- ドメイン グループ ルートまたは特定のドメイン
- 組織ルートまたは特定の組織

インポート時の影響の予測

Cisco UCS Central では、GUI を使用して実行するほとんどの管理アクションによる影響を予測できるオプションがあります。 インポート時の影響の予測を実行してください。 影響予測結果を確認してください。 予測結果から、意図しないサーバのリブートやポリシーの上書きなどの潜在的な問題をすべて特定し、選択したポリシーまたはコンポーネントをインポートする前に適切な予防措置を講じることができます。

ポリシーまたはコンポーネントのインポートに関する注意およびガイドライン

ポリシーまたはポリシー コンポーネントをインポートする前に、以下の点を確認してください。

- 登録済み Cisco UCS ドメインでは、Cisco UCS Manager リリース 2.1(2x) および 2.1(3x) を使用している場合はドメイン内でのポリシーまたはコンポーネントの検索だけが可能です。 ポリシーをインポートするには、Cisco UCS Manager リリース 2.2 を使用する必要があります。

- ルートまたはドメインにポリシーをインポートするときに、同じ名前のポリシーがドメイン内に存在している場合、Cisco UCS Central によりポリシーの上書きを警告する確認ダイアログボックスが表示されます。インポートすることを選択すると、インポートされたポリシーによって既存のポリシーが上書きされます。インポート後に既存のポリシーを取得することはできません。
- Cisco UCS Central では、登録済み UCS ドメインのポリシーのバックアップ コピーは保持されません。たとえばドメインに特定の BIOS ポリシーがあり、影響予測を行わずに別の BIOS ポリシーをインポートすると、既存の BIOS ポリシーが上書きされ、回復できなくなります。[Estimate Impact] をクリックして影響を確認するときに、潜在的なリスクを特定して予防措置を講じることができます。
- ドメインでカスタマイズしたポリシーがインポートによって失われないようにするため、インポートを実行する前に、必ず [Estimate Impact] を実行してください。 影響予測により、潜在的な問題の詳細なリストが示されます。 結果を確認し、情報に基づいてインポートを決定できます。
- インポートするポリシーが原因でサーバがリブートされる場合、影響予測の実行時にそのことを確認できるので、インポートを実行する前に適切な予防措置を講じることができます。影響予測でリブートに関する警告が示される場合でも、リブートが即時に実行されないことがあります。 グローバル デフォルト メンテナンス ポリシーのリブート オプションにより、選択されたオプションに基づいてリブート アクションが実行されます。
- Cisco UCS ドメインからポリシーをインポートするときに、Cisco UCS Central でそのポリシーの一部のコンポーネントがサポートされていない場合には、インポート中にそのサポートされていないコンポーネントがポリシーから削除されます。
- サーバのリブートを引き起こすポリシーをインポートする場合、サーバのリブートがインポートの直後に行われないことがあります。 これはメンテナンス ポリシーに関連付けられているスケジュールに基づいて実行されます。

ポリシーおよびポリシー依存項目

次の表では、Cisco UCS Manager からインポートできるポリシーまたは依存項目をリストします。

ポリシーまたは依存項目	説明
ポリシー	

ポリシーまたは依存項目	説明
	次のポリシーをインポートできます。 • BIOS ポリシー • ブート ポリシー • CIM XML ポリシー • Call Home ポリシー • DNS ポリシー • ダイナミック vNIC 接続ポリシー • イーサネット アダプタ ポリシー • ファイバ チャネル アダプタ ポリシー • グローバル障害ポリシー • グローバル電力割り当てポリシー • HTTP ポリシー • インターフェイス モニタリング ポリシー • LAN 接続ポリシー • ローカル ディスク設定ポリシー • メンテナンス ポリシー • SEL ポリシー • SNMP ポリシー • スクラブ ポリシー • Serial over LAN ポリシー • サーバ プール ポリシー • サーバ プール ポリシー資格情報 • シェル セッション制限ポリシー • syslog ポリシー • TFTP コア エクスポート ポリシー • Telnet ポリシー • しきい値ポリシー • タイム ゾーン ポリシー • Web セッション制限ポリシー

ポリシーまたは依存項目	説明
	• iSCSI チャネル アダプタ ポリシー • vNIC vHBA 配置ポリシー
Pools	• IP プール • IQN プール • MAC Pool • UUID 接尾辞プール • WWN プール
ポリシー依存項目	• ホスト ファームウェア パッケージ • IPMI アクセス プロファイル • スケジュール • サービス プロファイル テンプレート • iSCSI 認証プロファイル • vHBA テンプレート • vNIC テンプレート • vLAN • vSAN

インポート中にサーバのリブートが行われるポリシー

次のポリシーでは、インポート後にインポート先でサーバがリブートされます。

- ブート ポリシー

UCS ドメインからのポリシーまたはポリシー コンポーネントのインポート

インポートするポリシーが原因で、宛先でサーバのリブートが発生しないことを確認します。 インポートできるポリシーまたはポリシー コンポーネントと、サーバのリブートを発生させるポリシーについては、ポリシーおよびポリシー依存項目，（227 ページ） を参照してください。

重要

- ルートまたはドメインにポリシーをインポートするときに、同じ名前のポリシーがドメイン内に存在している場合、Cisco UCS Central によりポリシーの上書きを警告する確認ダイアログボックスが表示されます。 インポートすることを選択すると、インポートされたポリシーによって既存のポリシーが上書きされます。 インポート後に既存のポリシーを取得することはできません。
- ドメインでカスタマイズしたポリシーがインポートによって失われないようにするため、インポートを実行する前に、必ず [Estimate Impact] を実行してください。 影響予測により、潜在的な問題の詳細なリストが示されます。 結果を確認し、情報に基づいてインポートを決定できます。

手順

ステップ 1 [Import] タブをクリックします。

ステップ 2 [Search] を使用して、インポート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。

- インポートするポリシーを見つけるには [Select Type] ドロップダウン オプションをクリックし、[Search] をクリックします。
- ポリシー名がわかっている場合は、[Search policies, pools, vLANs, vSAns in UCS Domains by name] フィールドに名前を入力し、[Search] をクリックします。

（注） [Search] の横の矢印をクリックして検索フィルタ オプションを展開し、ポリシーの検索を絞り込みます。 検索を絞り込むには、[Select Ownership]、[Domain Group]、[UCS Domain]、[Org] などのフィールドにオプションを指定します。

ステップ 3 表示される検索結果リストから、インポートするポリシーを選択します。
ポリシーを選択すると、[Import] と [Properties (UCS View)] が表示されます。

ステップ 4 [Import] をクリックすると、[Import] ダイアログボックスが表示されます。
[Import] ダイアログボックスのオプションは、インポート対象として選択したポリシーによって異なります。 一部のポリシーでは、[Import As] オプションが表示されます。 選択したポリシーを異なる名前で選択した宛先にインポートできます。

ステップ 5 インポートの宛先を指定します。
インポートするポリシーまたはコンポーネントに応じて、次のいずれかの宛先にインポートできます。

- ドメイン グループ ルートまたは特定のドメイン
- ポリシー名または組織レベル

ステップ 6 [Estimate Impact] をクリックします。
経過表示バーに、影響予測のステータスが表示されます。 [100%] に達したら、[Review Impact] をクリックして、指定された宛先におけるインポートの影響を確認します。

ステップ 7 [Import] をクリックします。
インポートが正常に完了すると、システムにより [Import Successful] メッセージが表示されます。

ローカル ポリシー

Cisco UCS Managerで作成、管理するポリシーは、登録済み Cisco UCS ドメインに対してローカルです。 Cisco UCS Central では、登録済み Cisco UCS ドメインで使用可能なポリシーがローカル ポリシーとして表示されます。 これらのポリシーは、Cisco UCS ドメイン内で作成および管理されるサービス プロファイル テンプレートまたはローカル サービス プロファイルだけに含めることができます。

統計情報しきい値ポリシー

統計情報しきい値ポリシーは、システムの特定の側面についての統計情報をモニタし、しきい値を超えた場合にはイベントを生成します。最小値と最大値の両方のしきい値を設定できます。たとえば、CPU の温度が特定の値を超えた場合や、サーバを過度に使用していたり、サーバの使用に余裕がある場合には、アラームを発生するようにポリシーを設定できます。

これらのしきい値ポリシーが、CIMC などのエンドポイントに適用される、ハードウェアやデバイス レベルのしきい値を制御することはありません。 このしきい値は、製造時にハードウェアコンポーネントに焼き付けられます。

Cisco UCS を使用して、次のコンポーネントに対して統計情報のしきい値ポリシーを設定できます。

- サーバおよびサーバ コンポーネント
- アップリンクのイーサネット ポート
- イーサネット サーバ ポート、シャーシ、およびファブリック インターコネクト
- ファイバ チャネル ポート

（注） イーサネット サーバ ポート、アップリンクのイーサネット ポート、またはアップリンクのファイバチャネルポートには、統計情報のしきい値ポリシーを作成したり、削除できません。既存のデフォルト ポリシーの設定だけを行うことができます。

しきい値ポリシーの作成

[Policies] ノードでは、[Network] タブ、[Servers] タブ、および [Equipment] タブで、該当する組織内にしきい値ポリシーを作成および設定できます。

手順

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [Threshold Policies] を右クリックし、[Create Threshold Policy] を選択します。

ステップ 4 [Create Threshold Policy] ダイアログボックスで、[Name] と説明（任意）を入力します。

（注） この時点でしきい値クラスとしきい値定義を作成するか、またはダイアログボックスを閉じて後でしきい値クラスとしきい値定義を追加することができます。 しきい値クラスを作成するために [Create Threshold Class] をクリックし、[Create Threshold Class] ダイアログボックスで [Create Threshold Definition] をクリックします。

ステップ 5 [OK] をクリックします。

次の作業

- しきい値ポリシーにしきい値クラスを追加します。
- しきい値クラスにしきい値定義を追加します。

既存のしきい値ポリシーへのしきい値クラスの追加

手順

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [Threshold Policies] を展開します。

ステップ 4 しきい値クラスを作成するポリシーを選択します。

ステップ 5 [Work] ペインで、[General] タブをクリックします。

ステップ 6 [Threshold Classes] テーブルで [Create Threshold Class] をクリックします。

ステップ 7 [Create Threshold Class] ダイアログボックスで、設定する統計情報クラスを選択します。

ステップ 8 [OK] をクリックします。
新しいクラスが [Threshold Classes] テーブルに表示されます。

ステップ 9 [Work] ペインで、[Save] をクリックします。

次の作業

- しきい値ポリシーへしきい値クラスを追加します。
- しきい値定義を追加します。

既存のしきい値クラスへのしきい値定義の追加

手順

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [Threshold Policies] を展開します。

ステップ 4 しきい値定義を作成するポリシーを選択します。

ステップ 5 [Work] ペインで、[General] タブをクリックします。

ステップ 6 [Threshold Classes] テーブルで、変更するしきい値クラスを右クリックし、[Create Threshold Definition] を選択します。

ステップ 7 [Create Threshold Definition] ダイアログボックスで、[Property Type] を選択し、[Normal Value (packets)] を入力し、標準値の上下のアラーム トリガーを選択します。

ステップ 8 [OK] をクリックします。

ステップ 9 [Work] ペインで、[Save] をクリックします。

しきい値ポリシーの削除

手順

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [Threshold Policies] を展開します。

ステップ 4 削除するポリシーを右クリックし、[Delete] を選択します。

ステップ 5 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。

しきい値ポリシーからのしきい値クラスの削除

手順

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [Threshold Policies] を展開します。

ステップ 4 しきい値クラスを削除するポリシーを選択します。

ステップ 5 [Work] ペインで、[General] タブをクリックします。

ステップ 6 [Threshold Classes] テーブルで、削除するしきい値定義を右クリックし、[Delete] を選択します。

ステップ 7 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。

しきい値クラスからのしきい値定義の削除

手順

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [Threshold Policies] を展開します。

ステップ 4 しきい値定義を削除するポリシーを選択します。

ステップ 5 [Work] ペインで、[General] タブをクリックします。

ステップ 6 [Threshold Classes] テーブルで、しきい値定義を削除するしきい値クラスを展開します。

ステップ 7 削除するしきい値定義を右クリックし、[Delete] を選択します。

ステップ 8 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。

第 12 章

ネットワーク ポリシー

この章は、次の内容で構成されています。

vNIC テンプレート

このポリシーは、サーバ上の vNIC が LAN に接続する方法を定義します。 このポリシーは、vNIC LAN 接続ポリシーとも呼ばれます。

Cisco UCS ManagerCisco UCS Central は、vNIC テンプレートを作成する際に正しい設定で VM-FEX ポート プロファイル自動的には作成しません。 VM-FEX ポート プロファイルを作成するには、vNIC テンプレートのターゲットを VM として設定する必要があります。

このポリシーを有効にするには、このポリシーをサービス プロファイルに含める必要があります。

（注） サーバに 2 つの Emulex NIC または QLogic NIC（Cisco UCS CNA M71KR-E または Cisco UCS CNA M71KR-Q）がある場合は、両方の NIC にユーザ定義の MAC アドレスが取得されるように、サービス プロファイルで両方のアダプタの vNIC ポリシーを設定する必要があります。両方の NIC のポリシーを設定しない場合でも、Windows は PCI バス上で両方の NIC を検出します。そうすると、第2のイーサネットはサービスプロファイルの一部ではないため、Windows はハードウェア MAC アドレスを割り当てます。その後でサービスプロファイルを異なるサーバに移動すると、Windows によって追加の NIC が検出されますが、これは 1 つの NIC でユーザ定義の MAC アドレスが取得されなかったためです。

vNIC テンプレートの作成

手順

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [vNIC Templates] を右クリックし、[Create vNIC Template] を選択します。

ステップ 4 [Create vNIC Template] ダイアログボックスで、[Name] と説明（任意）を入力します。

ステップ 5 [Fabric ID] と [Template Type] を選択し、[MTU] を入力し、[Type] を選択します。
この領域では MAC プールを作成することもできます。

ステップ 6 [VLANs] テーブルで、使用する VLAN を選択します。

ステップ 7 [Policies] 領域で、ドロップダウン リストから [MAC Pool] 、[QoS Policy] 、[Network Control Policy] 、[Stats Threshold Policy] を選択し、[Pin Group Name] を入力します。
この領域では、MAC プール、QoS ポリシー、ネットワーク制御ポリシーとしきい値ポリシーを作成することもできます。

ステップ 8 [OK] をクリックします。

vNIC テンプレートの削除

手順

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。

サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [vNIC Templates] を展開します。

ステップ 4 削除する vNIC テンプレートを右クリックし、[Delete] を選択します。

ステップ 5 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。

デフォルトの vNIC 動作ポリシー

デフォルトの vNIC 動作ポリシーにより、サービス プロファイルに対する vNIC の作成方法を設定できます。 vNICS を手動で作成するか、自動的に作成されるようにするかを選択できます。

デフォルトの vNIC 動作ポリシーを設定して、vNIC の作成方法を定義することができます。 次のいずれかになります。

- [None]：Cisco UCS ManagerCisco UCS Central は、サービス プロファイルにデフォルトの vNIC を作成しません。 すべての vNIC を明示的に作成する必要があります。
- [HW Inherit]：サービス プロファイルが vNIC を必要とし、何も明示的に定義されていない場合、Cisco UCS ManagerCisco UCS Central はサービス プロファイルに関連付けられたサーバにインストールされたアダプタに基づいて必要な vNIC を作成します。

（注） vNIC のデフォルトの動作ポリシーを指定しない場合、[HW Inherit] がデフォルトで使用されます。

vNIC のデフォルト動作の設定

vNIC のデフォルトの動作ポリシーを指定しない場合、[HW Inherit] がデフォルトで使用されます。

手順

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。
ルート組織ではデフォルトの vNIC 動作ポリシーのみを設定できます。 サブ組織ではデフォルトの vNIC 動作ポリシーは設定できません。

ステップ 3 [Default vNIC Behavior] を右クリックし、[Properties] を選択します。

ステップ 4 [Properties (Default vNIC Behavior)] ダイアログボックスで [Action] を選択し、オプションの [vNIC Template] を選択します。

ステップ 5 [OK] をクリックします。

LAN および SAN 接続ポリシー

接続ポリシーは、ネットワーク上のサーバと LAN または SAN 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。これらのポリシーは、プールを使用してサーバにMACアドレス、WWN、および WWPN を割り当て、サーバがネットワークとの通信に使用する vNIC および vHBA を識別します。

（注） これらの接続ポリシーは、サービス プロファイルおよびサービス プロファイル テンプレートに含まれ、複数のサーバを設定するために使用できるので、静的 ID を接続ポリシーで使用することはお勧めしません。

LAN および SAN の接続ポリシーに必要な権限

接続ポリシーにより、ネットワークまたはストレージ権限のないユーザがネットワークおよびストレージ接続をしているサービス プロファイルおよびサービス プロファイル テンプレートを作成および変更することが可能になります。ただし、ユーザは接続ポリシーを作成するための適切なネットワークおよびストレージの権限が必要です。

接続ポリシーの作成に必要な権限

接続ポリシーは、他のネットワークおよびストレージ構成と同じ権限を必要とします。たとえば、接続ポリシーを作成するには、次の権限の少なくとも 1 つを有している必要があります。

- [admin]：LAN および SAN 接続ポリシーを作成できます
- [ls-server]：LAN および SAN 接続ポリシーを作成できます
- [ls-network]：LAN 接続ポリシーを作成できます
- [ls-storage]：SAN 接続ポリシーを作成できます

接続ポリシーをサービス プロファイルに追加するために必要な権限

接続ポリシーの作成後、ls-compute 権限を持つユーザは、そのポリシーをサービス プロファイルまたはサービス プロファイル テンプレートに組み込むことができます。ただし、ls-compute 権限しかないユーザは接続ポリシーを作成できません。

LAN 接続ポリシーの作成

手順

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [LAN Connectivity Policies] を右クリックし、[Create LAN Connectivity Policy] を選択します。

ステップ 4 [Create LAN Connectivity Policy] ダイアログボックスで、[Name] と説明（任意）を入力します。

ステップ 5 vNIC を LAN 接続ポリシーに追加するには、[vNICS] 領域の [Create vNIC] をクリックします。
作成した vNIC が [vNIC] テーブルに追加されます。

ステップ 6 iSCSI vNIC を LAN 接続ポリシーに追加するには、[iSCSI vNICS] 領域の [Create iSCSI vNIC] をクリックします。
作成した iSCSI vNIC が [iSCSI vNIC] テーブルに追加されます。

ステップ 7 [OK] をクリックします。

LAN 接続ポリシー用の vNIC の作成

手順

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [LAN Connectivity Policies] を展開します。

ステップ 4 vNIC を作成する LAN 接続ポリシーを選択します。

ステップ 5 [Work] ペインで、[General] タブをクリックします。

ステップ 6 [vNICs] 領域で [Create vNIC] をクリックします。

ステップ 7 既存の vNIC テンプレートを使用するには、[Create vNIC] ダイアログボックスで名前を入力し、[MAC Address Assignment] を選択して [Use vNIC Template] チェックボックスをオンにします。
この領域では MAC プールを作成することもできます。

ステップ 8 [Details] 領域で、[Fabric ID] を選択し、使用する VLAN を選択し、[MTU] を入力します。

ステップ 9 [Pin Group] 領域で、[Pin Group Name] を選択します。

ステップ 10 [Operational Parameters] 領域で、[Stats Threshold Policy] を選択します。
この領域ではしきい値ポリシーを作成することもできます。

ステップ 11 [Adapter Performance Profile] 領域で、[Adapter Policy]、[QoS Policy]、および [Network Control Policy] を選択します。
この領域では、イーサネットアダプタポリシー、QoS ポリシー、ネットワーク制御ポリシーを作成することもできます。

ステップ 12 [OK] をクリックします。

LAN 接続ポリシー用の iSCSI vNIC の作成

手順

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [LAN Connectivity Policies] を展開します。

ステップ 4 iSCSI vNIC を作成する LAN 接続ポリシーを選択します。

ステップ 5 [Work] ペインで、[General] タブをクリックします。

ステップ 6 [iSCSI vNICs] 領域で [Create iSCSI vNIC] をクリックします。

ステップ 7 [Create iSCSI vNIC] ダイアログボックスで、名前を入力し、[Overlay vNIC] 、[iSCSI Adapter Policy] 、および [VLAN] をドロップダウン リストから選択し、[MAC Address Assignment] を選択します。
このダイアログボックスでは、iSCSI アダプタ ポリシーと MAC プールを作成することもできます。

ステップ 8 [OK] をクリックします。

LAN 接続ポリシーの削除

手順

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [LAN Connectivity Policies] を展開します。

ステップ 4 削除するポリシーを右クリックし、[Delete] を選択します。

ステップ 5 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。

LAN 接続ポリシーからの vNIC の削除

手順

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [LAN Connectivity Policies] を展開します。

ステップ 4 vNIC を削除するポリシーを選択します。

ステップ 5 [Work] ペインで、[General] タブをクリックします。

ステップ 6 [vNICs] テーブルで、削除する vNIC をクリックします。

ステップ 7 [vNICs] テーブル アイコン バーで [Delete] をクリックします。

ステップ 8 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。

LAN 接続ポリシーからの iSCSI vNIC の削除

手順

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [LAN Connectivity Policies] を展開します。

ステップ 4 iSCSI vNIC を削除するポリシーを選択します。

ステップ 5 [Work] ペインで、[General] タブをクリックします。

ステップ 6 [iSCSI vNICs] テーブルで、削除する vNIC をクリックします。

ステップ 7 [iSCSI vNICs] テーブル アイコン バーで [Delete] をクリックします。

ステップ 8 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。

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 ManagerCisco 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 ManagerCisco 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 ManagerCisco 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

Emulex 統合型ネットワークアダプタ（N20-AE0102）用の MAC アドレスベースのポート セキュリティはサポートされません。 MAC アドレスベースのポート セキュリティがイネーブルになっている場合、ファブリック インターコネクトにより、最初にそれが学習した MAC アドレスが含まれるパケットにトラフィックが制限されます。 これは、FCoE Initialization Protocol パケットで使用される送信元 MAC アドレスか、イーサネット パケットの MAC アドレスのうち、アダプタによって最初に送信されたほうになります。 この設定により、FCoE パケットと Ethernet パケットのいずれかがドロップされることがあります。

手順

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [Create Memory Qualification] を右クリックし、[Create Network Control Policy] を選択します。

ステップ 4 [Create Network Control Policy] ダイアログボックスで、[Name] と説明（任意）を入力します。

ステップ 5 [CDP]、[MAC Register Mode]、[Action on Uplink Fail] を選択します。

ステップ 6 [MAC Security] 領域で、偽装 MAC アドレスの許可または拒否を選択します。

ステップ 7 [OK] をクリックします。

ネットワーク制御ポリシーの削除

手順

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [Network Control Policies] を展開します。

ステップ 4 削除するポリシーを右クリックし、[Delete] を選択します。

ステップ 5 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。

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。

イーサネット アダプタ ポリシー

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。

サーバの移行

（注） ダイナミック vNIC が設定されているサーバを、またはその他の移行ツールを使用して移行すると、vNIC が使用するダイナミック インターフェイスで障害が発生し、Cisco UCS ManagerCisco UCS Central によってその障害が通知されます。

サーバが復旧すると、Cisco UCS ManagerCisco 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

手順

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [Dynamic vNIC Connection Policies] を右クリックし、[Create Dynamic vNIC Connection Policy] を選択します。

ステップ 4 [Create Dynamic vNIC Connection Policy] ダイアログボックスで、[Name]、説明（任意）、[Naming Prefix]、および [Number of Dynamic vNICs] を入力します。

ステップ 5 ドロップダウン リストから [Adapter Policy] を選択し、[Protection] レベルを設定します。

ステップ 6 [OK] をクリックします。

ダイナミック vNIC 接続ポリシーの削除

手順

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [Dynamic vNIC Connections Policies] を展開します。

ステップ 4 削除するポリシーを右クリックし、[Delete] を選択します。

ステップ 5 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。

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。

QoS ポリシーの作成

手順

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [QoS Policies] を右クリックして [Create QoS Policy] を選択します。

ステップ 4 [Create QoS Policy] ダイアログボックスで、[Name] と説明（任意）を入力します。

ステップ 5 [Egress] 領域で [Priority] を選択し、[Burst(Bytes)] と [Rate(Kbps)] を入力し、[Host Control] を選択します。

ステップ 6 [OK] をクリックします。

次の作業

QoS ポリシーは、vNIC または vHBA テンプレートにインクルードします。

QoS ポリシーの削除

手順

ステップ 1 メニュー バーで、[Network] をクリックします。

ステップ 2 [Navigation] ペインで、[Network] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [QoS Policies] を展開します。

ステップ 4 削除するポリシーを右クリックし、[Delete] を選択します。

ステップ 5 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。

第 13 章

サーバ ポリシー

この章は、次の内容で構成されています。

イーサネットおよびファイバチャネルアダプタポリシー

このようなポリシーは、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 ManagerCisco 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 ManagerCisco UCS Central で明らかに異なる場合があります。

- 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 ManagerCisco 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 ManagerCisco UCS Central では、この値をミリ秒で設定します。 したがって、Cisco UCS ManagerCisco UCS Central で 5500 ミリ秒と設定された値は、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 ManagerCisco 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 ManagerCisco 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

デフォルトでは、Cisco UCS は、イーサネット アダプタ ポリシーとファイバ チャネル アダプタ ポリシーのセットを提供します。 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。

重要 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。

ただし、（デフォルトの Windows のアダプタ ポリシーを使用する代わりに）Windows OS 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します。

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

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Adapter Policies] を右クリックし、[Create Ethernet Adapter Policy] を選択します。

ステップ 4 [Create Ethernet Adapter Policy] ダイアログボックスで、[Name] と説明（任意）を入力します。

ステップ 5 [Resources] 領域で、各キューの [Transmit Queues]、[Receive Queues]、[Completion Queues]、および [Ring Size] を入力します。

ステップ 6 [Options] 領域で、[Transmit Checksum Offload]、[Receive Checksum Offload]、[TCP Segmentation Offload]、[TCP Large Receive Offload]、および [Receive Side Scaling (RSS)] を選択します。

ステップ 7 [Failback Timeout (Seconds)] を入力し、[Interrupt Mode] と [Interrupt Coalescing Type] を選択し、[Interrupt Time (us)] を入力します。

ステップ 8 [OK] をクリックします。

イーサネット アダプタ ポリシーの削除

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Adapter Policies] を展開します。

ステップ 4 削除するポリシーを右クリックし、[Delete] を選択します。

ステップ 5 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 BIOS 設定

Cisco UCSでは、Cisco UCS ドメイン内のサーバ上の BIOS 設定をグローバルに変更する方法が 2 通り用意されています。 サーバまたはサーバの集合のニーズに合う特定の BIOS 設定グループを含む BIOS ポリシーを 1 つ以上作成するか、特定のサーバ プラットフォームに対するデフォルトの BIOS 設定を使用できます。

BIOS ポリシーおよびサーバ プラットフォームのデフォルトの BIOS 設定のいずれを使用しても、Cisco UCS ManagerCisco UCS Central によって管理されているサーバの BIOS 設定を微調整できます。

データセンターのニーズに応じて、一部のサービス プロファイルについては BIOS ポリシーを設定し、同じ Cisco UCS ドメイン内の他のサービス プロファイルについては BIOS のデフォルトを使用したり、そのいずれかのみを使用したりできます。 また、Cisco UCS ManagerCisco UCS Central を使用して、サーバの実際の BIOS 設定を表示し、それらが現在のニーズを満たしているかどうかを確認できます。

（注） Cisco UCS ManagerCisco UCS Central は、BIOS ポリシーまたはデフォルトの BIOS 設定による BIOS 設定の変更を Cisco Integrated Management Controller（CIMC）バッファにプッシュします。 これらの変更はバッファ内にとどまり、サーバがリブートされるまでは有効になりません。

設定するサーバでBIOS設定のサポートを確認することをお勧めします。 RAS メモリのミラーリング モードなどの一部の設定は、すべてのCisco UCS サーバでサポートされているわけではありません。

メイン 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
[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。
[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、Error Manager 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。

名前	説明
[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。
[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]：プロセッサの周波数は自動的には上がりません。 • [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。
[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。

名前	説明
[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。
[Core Multi Processing]	CPU あたりのパッケージの論理プロセッサ コアの状態を設定します。 この設定を無効にすると、Intel Hyper Threading テクノロジーも無効になります。 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 あたりの論理プロセッサ コアの数を指定します。 多重処理を無効にして、サーバで実行される CPU あたりの論理プロセッサ コアを 1 個のみにするには、[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。

名前	説明
[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]：プロセッサでメモリ領域を分類しません。 • [enabled]：プロセッサで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。
[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。

名前	説明
[Hardware Pre-fetcher]	プロセッサで、インテル ハードウェア プリフェッチャが必要に応じてデータおよび命令ストリームをメモリから取得し、統合 2 次キャッシュに入れることを許可するかどうか。 次のいずれかになります。 • [Disabled]：ハードウェア プリフェッチャは使用しません。 • [Enabled]：プロセッサで、キャッシュの問題が検出されたときにプリフェッチャを使用します。 • [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） この値を指定するには、 を [Custom] に設定する必要があります。 [Custom] 以外の値の場合は、このオプションよりも、選択された CPU パフォーマンス プロファイルの設定が優先されます。
[Adjacent Cache Line Pre-fetcher]	プロセッサで必要な行のみを取得するのではなく、偶数または奇数のペアのキャッシュ行を取得するかどうか。 次のいずれかになります。 • [Disabled]：プロセッサで必要な行のみを取得します。 • [Enabled]：プロセッサで必要な行およびペアの行の両方を取得します。 • [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） この値を指定するには、 を [Custom] に設定する必要があります。 [Custom] 以外の値の場合は、このオプションよりも、選択された CPU パフォーマンス プロファイルの設定が優先されます。

名前	説明
[DCU Streamer Pre-fetch]	プロセッサで DCU IP Prefetch メカニズムを使用して履歴キャッシュ アクセス パターンを分析し、L1 キャッシュ内で最も関連性の高い行をプリロードします。 次のいずれかになります。 • [Disabled]：プロセッサはキャッシュ読み取り要求を予測しようとせず、明示的に要求された行のみを取得します。 • [Enabled]：DCU Prefetcher でキャッシュ読み取りパターンを分析し、必要と判断した場合にキャッシュ内の次の行を事前に取得します。 • [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。
[DCU IP Pre-fetcher]	プロセッサで DCU IP Prefetch メカニズムを使用して履歴キャッシュ アクセス パターンを分析し、L1 キャッシュ内で最も関連性の高い行をプリロードします。 次のいずれかになります。 • [Disabled]：プロセッサでキャッシュ データをプリロードしません。 • [Enabled]：DCU IP Prefetcher で最も関連性が高いと判断されたデータを含む L1 キャッシュをプリロードします。 • [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
[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]：データは I/O デバイスから直接プロセッサ キャッシュには入れられません。 • [enabled]：データは I/O デバイスから直接プロセッサ キャッシュに入れられます。 • [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。
[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 状態でも引き続き最大周波数で動作します。 • [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 フォーマットを使用して 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 Server の場合、[BIOS Setup] メニューでこれらのオプションに対して [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。
[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。

名前	説明
[Local X2 APIC]	Application Policy Infrastructure Controller（APIC）アーキテクチャ タイプを設定できます。 次のいずれかになります。 • [xapic]：標準の xAPIC アーキテクチャを使用します。 • [x2apic]：拡張 x2APIC アーキテクチャを使用してプロセッサの 32 ビット アドレス指定能力をサポートします。 • [auto]：検出された xAPIC アーキテクチャを自動的に使用します。 • [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。
[Power Technology]	次のオプションの CPU 電源管理設定を指定できます。 • Enhanced Intel Speedstep Technology • Intel Turbo Boost Technology • Processor Power State C6 [Power Technology] は次のいずれかになります。 • [Disabled]：サーバで CPU 電源管理は実行されず、前述の BIOS パラメータの設定が無視されます。 • ：前述の BIOS パラメータに最適な設定が決定され、これらのパラメータの個々の設定は無視されます。 • [Performance]：サーバは前述の BIOS パラメータのパフォーマンスを自動的に最適化します。 • [Custom]：前述の BIOS パラメータの個々の設定が使用されます。 これらの BIOS パラメータのいずれかを変更する場合は、このオプションを選択する必要があります。 • [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。

名前	説明
[Energy Performance]	システム パフォーマンスまたはエネルギー効率がこのサーバで重要かどうかを判断できます。 次のいずれかになります。 • パフォーマンス • balanced-performance • balanced-energy • energy-efficient • [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） を [Custom] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。
[Frequency Floor Override]	アイドル時に、CPUがターボを除く最大周波数よりも低い周波数にできるようにするかどうか。 次のいずれかになります。 • [Disabled]：アイドル中に CPU をターボを除く最大周波数よりも低くできます。 このオプションでは電力消費が低下しますが、システムパフォーマンスが低下する可能性があります。 • [Enabled]：アイドル中に CPU をターボを除く最大周波数よりも低くできません。 このオプションではシステムパフォーマンスが向上しますが、消費電力が増加することがあります。 • [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。

名前	説明
[P-STATE Coordination]	BIOS がオペレーティング システムに P-state サポート モデルを通信する方法を定義できます。 Advanced Configuration and Power Interface（ACPI）仕様で定義される 3 つのモデルがあります。 • [HW_ALL]：プロセッサ ハードウェアが、依存性のある論理プロセッサ（パッケージ内のすべての論理プロセッサ）間の P-state を調整します。 • [SW_ALL]：OS Power Manager（OSPM）が、依存性のある論理プロセッサ（物理パッケージ内のすべての論理プロセッサ）間の P-state を調整します。すべての論理プロセッサで遷移を開始する必要があります。 • [SW_ANY]：OS Power Manager（OSPM）が、依存性のある論理プロセッサ（パッケージ内のすべての論理プロセッサ）間の P-state を調整します。 ドメイン内の任意の論理プロセッサで遷移を開始する場合があります。 • [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。 （注） を [Custom] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。
[DRAM Clock Throttling]	メモリ帯域幅と消費電力に関してシステム設定を調整できます。 次のいずれかになります。 • [Balanced]：DRAM クロック スロットリングを低下させ、パフォーマンスと電力のバランスをとります。 • [Performance]：DRAM クロック スロットリングはディセーブルです。追加の電力をかけてメモリ帯域幅を増やします。 • [Energy Efficient][Energy_Efficient]：DRAMのクロックスロットリングを上げてエネルギー効率を向上させます。 • [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
[Channel Interleaving]	CPUがメモリ ブロックを分割して、データの隣接部分をインターリーブされたチャネル間に分散し、同時読み取り動作をイネーブルにするかどうか。 次のいずれかになります。 • [Auto]：実行するインターリーブを、CPU が決定します。 • [1-way]：何らかのチャネル インターリーブが使用されます。 • 2-way • 3-way • [4-way]：最大量のチャネル インターリーブが使用されます。 • [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。
[Rank Interleaving] ドロップダウン リスト	1 つのランクを更新中に別のランクにアクセスできるよう、CPUがメモリの物理ランクをインターリーブするかどうか。 次のいずれかになります。 • [Auto]：実行するインターリーブを、CPU が決定します。 • [1-way]：何らかのランク インターリーブが使用されます。 • 2-way • 4-way • [8-way]：最大量のランク インターリーブが使用されます。 • [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
[Demand Scrub]	CPU または I/O が読み取りを要求した場合に検出された 1 ビットのメモリ エラーを、システムが修正するかどうか。 次のいずれかになります。 • [Disabled]：1 ビット メモリ エラーは修正されません。 • [Enabled]：1 ビット メモリ エラーがメモリ内部で修正され、修正されたデータが、読み取り要求に対する応答に設定されます。 • [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。
[Patrol Scrub]	システムがサーバ上のメモリの未使用部分でも単一ビット メモリ エラーをアクティブに探して訂正するかどうか。 次のいずれかになります。 • [Disabled]：CPU がメモリ アドレスの読み取りまたは書き込みを行うときのみ、システムはメモリの ECC エラーをチェックします。 • [Enabled]：システムは定期的にメモリを読み書きして ECC エラーを探します。 エラーが見つかると、システムは修正を試みます。 このオプションにより、単一ビット エラーは複数ビット エラーになる前に修正される場合がありますが、パトロールスクラブの実行時にパフォーマンスが低下する場合もあります。 • [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。
[Altitude]	次のいずれかになります。 • — • — • —

名前	説明
[Altitude]	物理サーバがインストールされているおおよその海抜（m）。 次のいずれかになります。 • [Auto]：物理的な高度をCPUによって判別します。 • ：サーバは、海抜約 300 m です。 • ：サーバは、海抜約 900 m です。 • ：サーバは、海抜約 1500 m です。 • ：サーバは、海抜約 3000 m 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。

名前	説明
[Package C State Limit] **set PackageCStateLimit**	

名前	説明
	アイドル時にサーバ コンポーネントが使用できる電力量。 次のいずれかになります。 • [No Limit][No_Limit]：サーバは、使用可能な任意のCステートに入ることがあります。 • [C0 state][C0_state]：サーバはすべてのサーバコンポーネントに常にフルパワーを提供します。 このオプションでは、最高レベルのパフォーマンスが維持され、最大量の電力が必要となります。 • [C1 state][C1_state]：CPUのアイドル時に、システムは電力消費を少し減らします。 このオプションでは、必要な電力が C0 よりも少なく、サーバはすばやくハイ パフォーマンス モードに戻ることができます。 • [C3 state][C3_state]：CPUのアイドル時に、システムはC1 オプションの場合よりもさらに電力消費を減らします。 この場合、必要な電力は C1 または C0 よりも少なくなりますが、サーバがハイ パフォーマンス モードに戻るのに要する時間が少し長くなります。 • [C6 state][C6_state]：CPUのアイドル時に、システムはC3 オプションの場合よりもさらに電力消費を減らします。 このオプションを使用すると、C0、C1、または C3 よりも電力量が節約されますが、サーバがフルパワーに戻るまでにパフォーマンス上の問題が発生する可能性があります。 • [C2 state][C2_state]：CPUのアイドル時に、システムはC1 オプションの場合よりもさらに電力消費を減らします。 この場合、必要な電力は C1 または C0 よりも少なくなりますが、サーバがハイ パフォーマンス モードに戻るのに要する時間が少し長くなります。 • [C7 state][C7_state]：CPUのアイドル時に、サーバはコンポーネントが使用できる電力量を最小にします。 このオプションでは、節約される電力量が最大になりますが、サーバがハイ パフォーマンス モードに戻るのに要する時間も最も長くなります。 • [C7s state][C7s_state]：CPUのアイドル時に、サーバはコンポーネントが使用できる電力量を最小にします。 このオプションでは、C7 よりも多い電力を節

名前	説明
	約できますが、サーバがハイ パフォーマンス モードに戻るのに要する時間も最も長くなります。 • [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。

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
[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。 次のいずれかになります。 • [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。 次のいずれかになります。 • [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。

名前	説明
[Coherency Support]	プロセッサで Intel VT-d Coherency をサポートするかどうか。 次のいずれかになります。 • [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。
[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。 次のいずれかになります。 • [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。 次のいずれかになります。 • [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
[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][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。
[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][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
[Mirroring Mode]	メモリ ミラーリングは、メモリに 2 個の同じデータ イメージを保存することにより、システムの信頼性を向上します。 このオプションは、[Memory RAS Config] で [mirroring] オプションを選択したときのみ使用可能です。 次のいずれかを指定できます。 • [inter-socket]：メモリは、CPU ソケットをまたいで 2 台の Integrated Memory Controller（IMC）間でミラーリングされます。 • [intra-socket]：1 台の IMC が同じソケットの別の IMC とミラーリングされます。 • [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。
[Sparing Mode]	スペアリングはメモリを予備に保持することで信頼性を最適化し、別の DIMM の障害発生時に使用できるようにします。 このオプションは、メモリの冗長性を実現しますが、ミラーリングほどの冗長性は提供されません。 使用可能なスペアリングのモードは、現在のメモリの数によって異なります。 このオプションは、[Memory RAS Config] で [sparing] オプションを選択したときのみ使用可能です。 次のいずれかを指定できます。 • [dimm-sparing]：1 枚の DIMM が予備に保持されます。 DIMM に障害が発生すると、その DIMM の内容はスペア DIMM に移されます。 • [rank-sparing]：DIMM のスペア ランクが予備に保持されます。 あるランクの DIMM に障害が発生した場合、そのランクの内容がスペア ランクに移されます。 • [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
[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][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]	このオプションは、内部メモリの更新頻度を制御します。

シリアル ポートの 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シリアル ポートの BIOS 設定の一覧を示します。

名前	説明
[Serial Port A]	シリアル ポート A がイネーブルかディセーブルか。 次のいずれかになります。 • [disabled]：シリアル ポートはディセーブルになります。 • [enabled]：シリアル ポートはイネーブルになります。 • [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。

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][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]	システムでレガシーUSBデバイスをサポートするかどうか。 次のいずれかになります。 • [disabled]：USBデバイスは、EFI アプリケーションでのみ使用できます。 • [enabled]：レガシーUSB のサポートは常に使用できます。 • [auto]：USB デバイスが接続されていない場合、レガシーUSBのサポートがディセーブルになります。 • [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。

名前	説明
[USB System 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][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 Front Panel Lock Access]	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][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。

PCI 設定の 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 PCI 設定の BIOS 設定の一覧を示します。

名前	説明
[Max Memory Below 4G]	PAE サポートなしで動作しているオペレーティング システムのメモリ使用率を、BIOS がシステム設定に応じて 4GB 以下で最大化するかどうか。 次のいずれかになります。 • [disabled]：メモリ使用率を最大化しません。 PAE をサポートするオペレーティング システムすべてにこのオプションを選択します。 • [enabled]：PAE をサポートしないオペレーティング システムについて 4GB 以下でメモリ使用率を最大化します。 • [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。
[Memory Mapped IO Above 4Gb Config]	64 ビット PCI デバイスの 4 GB 以上のアドレス空間に対するメモリ マップド I/O をイネーブルにするか、ディセーブルにするか。 レガシーなオプション ROM は 4 GB を超えるアドレスにアクセスできません。 PCI デバイスが 64 ビット対応でも、レガシーなオプション ROM を使用する場合は、この設定をイネーブルにしても正しく機能しない場合があります。 次のいずれかになります。 • [disabled]：64 ビット PCI デバイスを 4 GB 以上のアドレス空間にマッピングしません。 • [enabled]：64 ビット PCI デバイスを 4 GB 以上のアドレス空間にマッピングします。 • [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。

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]：ユーザ入力を待機してから非EFIベースのブート オプションを再試行します。 • [enabled]：ユーザ入力を待機せずに非 EFI ベースのブート オプションを継続的に再試行します。 • [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 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][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][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で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][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 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サーバ管理 BIOS 設定の一覧を示します。

General Settings

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]：SERR の発生時に、BIOS は NMI を生成することもエラーをログに記録することもしません。 • [enabled]：SERR の発生時に、BIOS は NMI を生成し、エラーをログに記録します。 [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][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
[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]：PERR の発生時に、BIOS は NMI を生成することもエラーをログに記録することもしません。 • [enabled]：PERR の発生時に、BIOS は NMI を生成し、エラーをログに記録します。 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][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。
[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][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。

名前	説明
[OS Boot Watchdog Timer Timeout Policy]	ウォッチドッグタイマーが切れた場合にシステムで実行されるアクション。 次のいずれかになります。 • [power-off]：OS ブート中にウォッチドッグ タイマーが期限切れになった場合、サーバは電源オフになります。 • [reset]：OS ブート中にウォッチドッグ タイマーが期限切れになった場合、サーバはリセットされます。 • [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。 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。
[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][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 リダイレクション設定

名前	説明
[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][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。
[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][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
[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]：9600 ボー レートが使用されます。 • [19200]：19200 ボー レートが使用されます。 • [38400]：38400 ボー レートが使用されます。 • [57600]：57600 ボー レートが使用されます。 • [115200]：115200 ボー レートが使用されます。 • [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。 （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 端末フォントが使用されます。 • [vt100]：サポートされている vt100 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 文字セットのビデオ端末が使用されます。 • [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。 （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
[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][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。

BIOS ポリシー

BIOS ポリシーは、サーバまたはサーバ グループに対する BIOS 設定の設定を自動化するポリシーです。 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 ManagerCisco 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 ManagerCisco UCS Central はサーバ上の BIOS 設定を BIOS ポリシー内の設定と一致するように変更します。 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。

デフォルトの BIOS 設定

Cisco UCS ManagerCisco UCS Centralには、Cisco UCS がサポートするサーバの各タイプのための 1 セットのデフォルト BIOS 設定が含まれます。 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 ManagerCisco 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 ManagerCisco UCS Central によって提供されるデフォルト 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。

BIOS ポリシーの作成

Cisco UCS Central は、BIOS ポリシーまたはデフォルトの BIOS 設定による BIOS 設定の変更を Cisco Integrated Management Controller（CIMC）バッファにプッシュします。 これらの変更はバッファ内にとどまり、サーバがリブートされるまでは有効になりません。 設定するサーバで BIOS 設定のサポートを確認することをお勧めします。 RAS メモリのミラーリング モードおよび予備モードといった一部の設定は、すべての Cisco UCS サーバでサポートされているわけではありません。

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [BIOS Policies] を右クリックして [Create BIOS Policy] を選択します。

ステップ 4 [Create BIOS Policy] ダイアログボックスで、[Name] と説明（任意）を入力します。

（注） BIOS ポリシーを手早く作成する場合は、名前を指定した後で [Finish] をクリックします。 Cisco UCS Central により、指定された名前とすべてのシステム デフォルト値を使用して新しい BIOS ポリシーが作成されます。

ステップ 5 （任意）[Main] パネルで主要な BIOS 設定（[Reboot on BIOS Change]、[Quiet Boot]、[Post Error Pause]、[Resume Ac on Power Loss]、[Front Panel Lockout] など）を選択し、[Next] をクリックします。

ステップ 6 （任意） [Processor] パネルでプロセッサの設定を選択し、[Next] をクリックします。

ステップ 7 （任意）[Intel Directed IO] パネルで I/O 設定を選択し、[Next] をクリックします。

ステップ 8 （任意）[RAS Memory] パネルでメモリ設定を選択し、[Next] をクリックします。

ステップ 9 （任意）[Serial Port] パネルで [Serial Port A] 設定を選択し、[Next] をクリックします。

ステップ 10 （任意）[Processor] パネルでプロセッサ設定情報を選択し、[Next] をクリックします。

ステップ 11 （任意）[USB] パネルで USB 設定（[Make Device Non Bootable]、[Legacy USB Support]、[USB Idle Power Optimizing Setting]、[USB Front Panel Access Lock] など）を選択し、[Next] をクリックします。

ステップ 12 （任意）[PCI Configuration] パネルで PCI 構成設定（[Max Memory Below 4GB] および [Memory Mapped IO Above 4GB Config] など）を選択し、[Next] をクリックします。

ステップ 13 （任意）[Boot Options] パネルでブート設定（[Boot Option Retry]、[Intel Entry SAS RAID]、[Intel Entry SAS RAID Module]、[Onboard SCU Storage Support] など）を選択し、[Next] をクリックします。

ステップ 14 （任意）[Server Manager] パネルでマスク不能割り込みの設定と [OS Boot Watchdog Timer] を選択し、[Console Redirection] 設定を指定し、[Finish] をクリックします。

BIOS ポリシーの変更

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [BIOS Policies] を展開します。

ステップ 4 変更する BIOS ポリシーをクリックします。

ステップ 5 [Work] ペインで該当するタブをクリックしてから、必要なオプション ボタンをクリックするか、ドロップダウン リストから選択して BIOS 設定を変更します。

ステップ 6 [Save] をクリックします。

BIOS ポリシーの削除

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [BIOS Policies] を展開します。

ステップ 4 削除するポリシーを右クリックし、[Delete] を選択します。

ステップ 5 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。

IPMI アクセス プロファイル

このポリシーでは、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かどうかを決定することができます。 たとえば、CIMC 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

IPMI アクセス プロファイルはには IPMI ユーザが必要です。 IPM アクセス プロファイルと同時に IPMI ユーザを作成できます。あるいは、既存の IPMI アクセス プロファイルに IPMI ユーザを追加できます。

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [IPMI Access Profiles] を右クリックし、[Create IPMI Access Profile] を選択します。

ステップ 4 [Create IPMI Access Profile] ダイアログボックスで、[Name] と説明（任意）を入力します。

ステップ 5 [Create IPMI User] をクリックして、IPMI ユーザを IPMI アクセス プロファイルに追加します。

ステップ 6 [OK] をクリックします。

次の作業

IPMI プロファイルはサービス プロファイルとテンプレートのうち一方、または両方にインクルードします。

IPMI アクセス プロファイルへの IPMI ユーザの追加

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、[Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、[Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [IPMI Access Profiles] を展開します。

ステップ 4 IPMI ユーザを追加する IPMI アクセス プロファイルをクリックします。

ステップ 5 [Work] ペインで、[General] タブをクリックします。

ステップ 6 [IPMI Users] 領域で [Create IPMI User] をクリックします。

ステップ 7 [Create IPMI Users] ダイアログボックスで、[Name] と [Password] を入力し、パスワードを確認し、[Serial over LAN State] を選択します。

ステップ 8 [OK] をクリックします。

IPMI アクセス プロファイルの削除

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、[Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、[Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [IPMI Access Profiles] を展開します。

ステップ 4 削除する IPMI アクセス プロファイルを右クリックし、[Delete] を選択します。

ステップ 5 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。

IPMI アクセス プロファイルからの IPMI ユーザの削除

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [IPMI Access Profiles] を展開します。

ステップ 4 IPMI ユーザを削除する IPMI アクセス プロファイルをクリックします。

ステップ 5 [Work] ペインで、[General] タブをクリックします。

ステップ 6 [IPMI Users] テーブルで、削除する IPMI ユーザをクリックします。

ステップ 7 [IPMI Users] ツールバーの [Delete] をクリックします。

ブート ポリシー

ブート ポリシーは、BIOS 設定メニューのブート順序をオーバーライドし、次のことを決定します。

- 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 ポリシーを含めない場合、UCS ドメインによってデフォルトのブート ポリシーが適用されます。

（注） ブート ポリシーに対する変更は、そのブート ポリシーを含む更新サービス プロファイル テンプレートから作成されたすべてのサービス プロファイルに伝搬されます。 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。

Boot Order

Cisco UCS Central リリース 1.2 では、Cisco UCS Central で作成するグローバル ブート ポリシーで次の 2 種類のブート順序のいずれかを選択できます。

- [Standard boot order]：標準ブート順序はすべての Cisco UCS サーバでサポートされており、ブート順序の最上位の項目を選択できます。 ローカル ディスク、CD-ROM、またはフロッピーなどのローカル デバイス、または SAN、LAN、または iSCSI ブートを追加できます。
- [Enhanced boot order]：拡張ブート順序では、ブート ポリシーに選択するブート デバイスをより詳細に制御できます。 拡張ブート順序は、リリース 2.2(1b) 以上のすべての Cisco UCS B-Series M3 ブレード サーバおよびCisco UCS B-Series M3 ラック サーバでサポートされます。

拡張ブート順序では、ブート順序の第 2 レベルで次のいずれかを選択できます。

- [Add Local LUN]：ローカル ハード ディスクからのブートを有効にします。
- [Add SD Card]：SD カードからのブートを有効にします。
- [Add Internal USB]：内部 USB からのブートを有効にします。
- [Add External USB]：外部 USB からのブートを有効にします。
- [Add Local CD/DVD]：ローカル CD/DVD ドライブからのブートを有効にします。
- [Add Remote CD/DVD]：KVM がマップされている ISO イメージからのブートを有効にします。
- [Add Local Floppy]：ローカル フロッピー ドライブからのブートを有効にします。
- [Add Remote Floppy]：KVM がマップされているイメージ ファイルからのブートを有効にします。
- [Add Remote Virtual Drive]：サーバからアクセス可能なリモート仮想ドライブからのブートを有効にします。
- [Add LAN, SAN or iSCSI Boot]：ブートする特定の vNIC または vHBA を選択できるようにします。

後方互換性を維持するため、ローカル ディスク、CD/DVD ROM ブートが利用可能です。

（注）

- 拡張ブート順序が指定されたブート ポリシーが、Cisco UCS M1 および M2 ブレード サーバとラック サーバ、またはリリース 2.2(1b) より前のリリースがインストールされている Cisco UCS M3 ブレード サーバとラック サーバに適用される場合、設定エラーが原因で関連付けが失敗します。
- 仮想メディアの USB を有効にする必要があります。 BIOS 設定を変更した場合、仮想メディアに影響します。 最適なパフォーマンスを得るために推奨される USB BIOS のデフォルト設定を次に示します。
  - [Make Device Non Bootable]：disabled に設定。
  - [USB Idle Power Optimizing Setting]：high-performance に設定。

UEFI ブート モード

Unified Extensible Firmware Interface（UEFI）は、オペレーティング システムとプラットフォーム ファームウェア間のソフトウェア インターフェースを定義する仕様です。 Cisco UCS Manager は、UEFI を使用して BIOS ファームウェア インターフェイスを置換します。 これにより、BIOS はレガシー サポートを提供する一方で UEFI で動作できるようになります。

ブート ポリシーを作成する場合、レガシーまたは UEFI ブート モードのいずれかを選択できます。 レガシー ブート モードは、すべての Cisco UCS サーバでサポートされます。 UEFI ブート モードは M3 および M4 サーバでのみサポートされており、このモードでは UEFI セキュア ブート モードを有効にできます。

次の制限は、UEFI ブート モードに適用されます。

- UEFI ブート モードは、Cisco UCS B-Series M3 および M4 ブレード サーバ、Cisco UCS C-Series M3 および M4 ラック サーバでのみサポートされます。
- UEFI ブート モードは、次の組み合わせではサポートされません。
  - Cisco UCS ドメインと統合された Cisco UCS ブレードおよびラック サーバ上の Gen-3 Emulex および QLogic アダプタ。
  - Cisco UCS ドメインと統合された Cisco UCS ラック サーバ上のすべてのアダプタに対する PXE ブート。
  - Cisco UCS ドメインと統合された Cisco UCS ラック サーバ上のすべてのアダプタに対する iSCSI ブート。
- 同じサーバで UEFI とレガシー ブート モードを混在させることはできません。
- UEFI 対応オペレーティング システムがデバイスにインストールされていることを確認します。 ブート ポリシーに設定されたブート デバイスにインストール済みの UEFI 対応 OS がある場合にのみ、サーバは UEFI モードで正しく起動します。 互換性のある OS が存在しない

場合、ブート デバイスは [Boot Order Details] 領域の [Actual Boot Order] タブに表示されません。

- UEFI ブート マネージャのエントリが BIOS NVRAM に正しく保存されなかったため、まれに UEFI のブートに成功しない場合もあります。 UEFI シェルを使用して、UEFI ブート マネージャのエントリを手動で入力することができます。 これは、次の状況で発生することがあります。
  - UEFI ブート モードが有効なブレード サーバがサービス プロファイルから関連付けを解除され、[Equipment] タブまたは前面パネルを使用してブレードの電源を手動でオンにする場合。
  - UEFI ブート モードが有効なブレード サーバがサービス プロファイルから関連付けを解除され、直接の VIC ファームウェア アップグレードが試行される場合。
  - UEFI ブート モードが有効なブレード サーバまたはラック サーバが SAN LUN からブートされ、サービス プロファイルが移行される場合。

UEFI セキュア ブート

Cisco UCS Central は、Cisco UCS B-Series M3 および M4 ブレード サーバでの UEFI セキュア ブートをサポートしています。 UEFI セキュア ブートがイネーブルの場合、すべての実行可能ファイル（ブート ローダ、アダプタ ドライバなど）はロードされる前に BIOS によって認証されます。認証されるには、イメージが Cisco 認証局（CA）または Microsoft CA によって署名される必要があります。

次の制限は、UEFI セキュア ブートに適用されます。

- UEFI ブート モードは、ブート ポリシーでイネーブルにする必要があります。
- Cisco UCS Manager ソフトウェアと BIOS ファームウェアは、リリース 2.2 以上である必要があります。
- ユーザ生成された暗号キーはサポートされません。
- UEFI セキュア ブートは、Cisco UCS Manager またはCisco UCS Central でのみ制御できます。
- Cisco UCS Managerの以前のバージョンにダウングレードする必要があり、ブレード サーバがセキュア ブート モードになっている場合は、ダウングレードを実行する前に、ブレード サーバの関連付けを解除し、再び関連付ける必要があります。 これを行わないと、そのブレード サーバは正常に検出されません。

ブート ポリシーのダウングレードに関する注意とガイドライン

次の条件に該当する場合は、以前のバージョンの Cisco UCS Manager にダウングレードできません。

- 関連するサーバのブート ポリシーで、UEFI ブート モードが有効に設定されている。

- 関連するサーバのブート ポリシーで、UEFI セキュア ブートが有効に設定されている。
- 関連するサーバのブート ポリシーで、拡張ブート順序が設定されている。 たとえば、関連するサーバのブート ポリシーに次のいずれかが含まれている場合です。
  - SD カード
  - 内部 USB
  - 外部 USB
- 関連するサーバのブート ポリシーに、SAN とローカル LUN の両方が含まれている。

ブート ポリシーの作成

サービス プロファイルまたはサービス プロファイル テンプレートに制限されたローカル ブート ポリシーを作成することもできます。 しかし、iSCSI ブートを除き、複数のサービス 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インクルードできるグローバルなブート ポリシーの作成を推奨します。

（注） Cisco UCS Central リリース 1.2 では、スクリプト可能な vMedia のサポートは追加されません。

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Boot Policies] を右クリックし、[Create Boot Policy] を選択します。

ステップ 4 [Create Boot Policy] ダイアログボックスで、[Name] と説明（任意）を入力します。

ステップ 5 （任意） ブート ポリシー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には、[Reboot on Boot Order Change] チェックボックスをオンにします。

重要 VIC 以外のアダプタがあるサーバでこのブート ポリシーを適用すると、[Reboot on Boot Order Change] チェックボックスがオンになっていない場合でも、SAN デバイスの順序を追加、削除、または変更すると、ブート ポリシーの変更の保存時にサーバが常にリブートされます。

ステップ 6 （任意） [Qualifications] テーブルにリストされている vNIC、vHBA、または iSCSI vNIC がサーバ プロファイルのサーバ設定と一致するようにするには、[Enforce vNIC/vHBA/iSCSI Name] チェックボックスをオンにします。

ステップ 7 [Boot Mode] を選択するには、[Legacy] または [UEFI] をクリックします。

ステップ 8 [Actions] 領域でブート ポリシーに次の 1 つ以上のブート オプションを設定し、ブート順序を設定します。

- ローカル デバイス ブート：[Add CD/DVD ROM Boot]、[Add Local CD/DVD]、[Add Local Disk]、[Add Floppy]、または [Add Remote Virtual Drive] をクリックし、デバイスをブート ポリシーに追加します。
- LAN ブート：集中型プロビジョニング サーバからブートするには [Add LAN Boot] をクリックします。
- SAN ブート：SAN 上のオペレーティング システム イメージからブートするには、[Add SAN Boot] をクリックします。

  vHBA がブート可能な SAN イメージを指し示す場合は、[Add SAN Boot Target] をクリックしてこれを設定します。
- iSCSI vNIC：iSCSI LUN からブートするには、[Add iSCSI Boot] をクリックします。

ステップ 9 （任意） ブート順序を変更するには、[Qualifications] テーブルの上下矢印をクリックします。

ステップ 10 [OK] をクリックします。

次の作業

ブート ポリシーはサービス プロファイルとテンプレートのうち一方、または両方にインクルードします。

このブート ポリシーを含むサービス プロファイルがサーバに関連付けられた後で、サーバの [General] タブの [Boot Order Details] 領域で実際のブート順序を確認できます。 ブート ポリシーの詳細については、『Cisco UCS Manager Configuration Guide』を参照してください。

ブート ポリシーの変更

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Boot Policies] を展開します。

ステップ 4 変更するブート ポリシーをクリックします。

ステップ 5 [Work] ペインで [General] タブをクリックし、ブート オプションとブート順序を適切に変更します。

ステップ 6 [Save] をクリックします。

ブート ポリシーの削除

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Boot Policies] を展開します。

ステップ 4 削除するポリシーを右クリックし、[Delete] を選択します。

ステップ 5 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。

LAN ブート

LAN の集中プロビジョニング サーバから 1 つまたは複数のサーバをブートするブート ポリシーを設定できます。 LAN（またはPXE）ブートは、そのLANサーバからサーバにOSをインストールする際に頻繁に使用されます。

LAN ブート ポリシーには、複数のタイプのブート デバイスを追加できます。 たとえば、ローカル ディスクや仮想メディア ブートをセカンダリ ブート デバイスとして追加できます。

ブート ポリシー用 LAN ブート ポリシー設定

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Boot Policies] を展開します。

ステップ 4 LAN ブートを設定するブート ポリシーをクリックします。

ステップ 5 [Work] ペインの [General] タブで [Add LAN Boot] をクリックします。

ステップ 6 [Add LAN Boot] ダイアログボックスで [vNIC] を入力し、[Type] ドロップダウン リストから [primary] または [secondary] を選択します。

ステップ 7 [OK] をクリックして、ダイアログボックスを閉じます。

ステップ 8 [Save] をクリックして、ブート ポリシーを保存します。

SAN ブート

SAN 上のオペレーティング システム イメージから 1 つ以上のサーバがブートするように、ブート ポリシーを設定できます。 ブート ポリシーにはプライマリとセカンダリの SAN ブート含めることができます。プライマリ ブートが失敗した場合、サーバはセカンダリからのブートを試行します。

システムに最高のサービスプロファイルモビリティを提供するSANブートの使用を推奨します。SANからブートした場合、あるサーバから別のサーバにサービスプロファイルを移動すると、移動後のサーバは、まったく同じオペレーティングシステムイメージからブートします。 したがって、ネットワークからは、この新しいサーバはまったく同じサーバと認識されます。

SAN ブートを使用するには、次の項目が設定されていることを確認してください。

- Cisco UCS ドメインが、オペレーティング システム イメージをホストしている SAN ストレージ デバイスと通信できること。
- オペレーティング システム イメージが置かれているデバイス上のブート ターゲット LUN。

（注） SAN ブートは、Cisco UCS ブレードおよびラック サーバ上の Gen-3 Emulex アダプタではサポートされていません。

ブート ポリシー用 SAN ブート ポリシー設定

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Boot Policies] を展開します。

ステップ 4 SAN ブートを設定するブート ポリシーをクリックします。

ステップ 5 [Work] ペインの [General] タブで [Add SAN Boot] をクリックします。

ステップ 6 [Add SAN Boot] ダイアログボックスで [vHBA] を入力し、[Type] ドロップダウン リストから [primary] または [secondary] を選択します。

ステップ 7 [OK] をクリックして、ダイアログボックスを閉じます。

ステップ 8 [Save] をクリックして、ブート ポリシーを保存します。

SAN ブート ターゲットの追加

SAN ブート ターゲットを追加する前に、ブート ポリシーの SAN ブートを設定しておく必要があります。

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Boot Policies] を展開します。

ステップ 4 SAN ブート ターゲットを追加するブート ポリシーをクリックします。

ステップ 5 [Work] ペインの [General] タブで [Add SAN Boot Target] をクリックします。

ステップ 6 [Add SAN Boot Target] ダイアログボックスで、[Boot Target LUN] と [Boot Target WWPN] を入力し、[Type] ドロップダウン リストから [primary] または [secondary] を選択します。

ステップ 7 [OK] をクリックして、ダイアログボックスを閉じます。

ステップ 8 [Save] をクリックして、ブート ポリシーを保存します。

iSCSI ブート

iSCSI ブートは、サーバがネットワークにリモートに配置されている iSCSI ターゲット マシンからオペレーティング システムを起動できるようにします。

iSCSI ブートは次の Cisco UCS ハードウェアでサポートされます。

- Cisco UCS M51KR-B Broadcom BCM57711 ネットワーク アダプタを持ち、Broadcom から提供されるデフォルトの MAC アドレスを使用する、 Cisco UCS ブレード サーバ。
- Cisco UCS M81KR 仮想インターフェイス カード

- Cisco UCS VIC-1240 仮想インターフェイス カード
- Cisco UCS VIC-1280 仮想インターフェイス カード
- Cisco UCS M61KR-B Broadcom BCM57712 のネットワーク アダプタを持つ Cisco UCS ラック サーバ。
- Cisco UCS P81E 仮想インターフェイス カード
- Cisco UCS VIC1225 仮想インターフェイス カード

iSCSI ブートを設定する前に満たさなければならない前提条件があります。 これらの前提条件のリストについては、iSCSI ブートのガイドラインと前提条件, （302 ページ）を参照してください。

iSCSI ブート プロセス

Cisco UCS ManagerCisco UCS Central は、サーバにあるアダプタをプログラムするための関連付けプロセスでサービス プロファイル用に作成された iSCSI vNIC と iSCSI のブート情報を使用します。 アダプタのプログラミング後に、サーバは最新のサービスプロファイル値で再起動します。 電源投入時セルフ テスト（POST）の後、アダプタは、次のサービス プロファイル値を使用して初期化を試みます。 アダプタが値を使用して指定されたターゲットにログインできる場合、アダプタは iSCSI Boot Firmware Table（iBFT）を初期化してホスト メモリに、有効なブート可能 LUN をシステム BIOS にポストします。 ホスト メモリにポストされる iBFT には、プライマリ iSCSI VNIC にプログラミングされた、イニシエータとターゲットの設定が含まれています。

（注） 以前は、ホストは LUN 検出が最初に終了したパスに応じて、設定されたブート パスのうち 1 つだけを参照し、そのパスから起動していました。 現在は、設定された iSCSI ブート vNIC が 2 つある場合、ホストは両方のブート パスを参照するようになりました。 したがってマルチパス設定については、単一の IQN が両方のブート vNIC で設定される必要があります。ホストのブート vNIC で異なる IQN が設定されている場合は、ホストは下位の PCI を持つブート vNIC で設定された IQN で起動します。

次の手順であるオペレーティング システム（OS）のインストールでは、iBFT 対応の OS が必要です。 OS のインストール時に、OS インストーラは iBFT テーブルのホストのメモリをスキャンし、iBFT テーブルの情報を使用してブートデバイスの検出とターゲット LUN への iSCSI パス作成を行います。 一部の OS では、このパスを完了するために NIC ドライバが必要です。 このステップが成功した場合、OS インストーラが OS をインストールしする iSCSI ターゲット LUN を検出します。

（注） iBFT は OS インストールのソフトウェア レベルで動作し、HBA モード（別名 TCP オフロード）では動作しない場合があります。 iBFT が HBA モードで動作するかどうかは、インストール中の OS の機能によって異なります。 また、Cisco UCS M51KR-B Broadcom BCM57711 アダプタを含むサーバについては、iBFT は MTU ジャンボ設定に関係なく、最大伝送単位（MTU）サイズ 1500 で正常に動作します。 OS が HBA モードをサポートする場合、iSCSI インストール プロセスの後に HBA モード、デュアル ファブリックのサポートおよびジャンボ MTU サイズの設定が必要な場合があります。

iSCSI ブートのガイドラインと前提条件

iSCSI ブートを設定する前に、これらのガイドラインと前提条件を満たす必要があります。

- iSCSI ブート ポリシーの作成後、ls-compute 権限を持つユーザは、そのポリシーをサービス プロファイルまたはサービス プロファイル テンプレートに組み込むことができます。 ただし、ls-compute 権限しかないユーザは iSCSI ブート ポリシーを作成できません。
- セカンド vNIC（フェールオーバー vNIC）が iSCSI LUN から起動する必要がある Windows 2008 サーバからの iSCSI ブートを設定するには、Microsoft Knowledge Base Article 976042 を参照してください。 Microsoft には、ネットワーキング ハードウェアが変更されたときに、Windows が iSCSI ドライブからの起動に失敗するか、bugcheck エラーが発生する可能性がある、という既知の問題があります。 この問題を回避するには、Microsoft が推奨する解決方法に従ってください。
- ストレージ アレイは、iSCSI ブートのライセンスが付与され、アレイ サイド LUN マスキングが正しく設定されている必要があります。
- 各 iSCSI イニシエータに 1 つずつ、2 つの IP アドレスを決定する必要があります。 可能であれば、IP アドレスは、ストレージ アレイと同じサブネット上にある必要があります。 IP アドレスは、Dynamic Host Configuration Protocol（DHCP）を使用してスタティックまたはダイナミックに割り当てられます。
- グローバル ブート ポリシーのブート パラメータは設定できません。 代わりに、ブート パラメータを設定した後、ブート ポリシーを適切なサービス プロファイルに含める必要があります。
- オペレーティング システム（OS）は iSCSI Boot Firmware Table（iBFT）互換である必要があります。
- Cisco UCS M51KR-B Broadcom BCM57711 ネットワーク アダプタの場合：
  - iSCSI ブートを使用するサーバは、Cisco UCS M51KR-B Broadcom BCM57711 ネットワーク アダプタを含んでいる必要があります。 アダプタ カードを取り付けまたは交換する方法については、『*Cisco UCS B250 Extended Memory Blade Server Installation and Service Note*』を参照してください。 サービス ノートは、http://www.cisco.com/go/unifiedcomputing/b-series-doc の『*Cisco UCS B-Series Servers Documentation Roadmap*』からアクセスできます。

- iSCSI デバイスの MAC アドレスを設定します。
- DHCP Vendor ID（オプション 43）を使用している場合は、iSCSI デバイスの MAC アドレスを /etc/dhcpd.conf に設定します。
- HBA モード（別名 TCP オフロード）および Boot to Target 設定がサポートされます。ただし、インストール中の HBA モードは Windows OS だけがサポートします。
- OS をインストールする前に、iSCSI のアダプタ ポリシーで Boot to Target 設定をディセーブルにし、OS をインストールした後で、Boot to Target 設定を再度イネーブルにします。

（注） アダプタ ポリシーの設定を変更するたびに、アダプタはリブートして新しい設定を適用します。

- OS を iSCSI ターゲットにインストールする場合、iSCSI ターゲットは OS イメージが存在するデバイスの前の順番にしておく必要があります。 たとえば、CD から iSCSI ターゲットに OS をインストールする場合、ブート順序は最初に iSCSI ターゲット、その後 CD とする必要があります。
- サーバが iSCSI ブートされた後は、イニシエータ名、ターゲット名、LUN、iSCSI デバイス IP、ネット マスクやゲートウェイを Broadcom ツールで変更しないでください。
- POST（電源投入時自己診断テスト）プロセスを中断しないでください。中断すると、Cisco UCS M51KR-B Broadcom BCM57711 ネットワーク アダプタは初期化に失敗します。

- Cisco UCS M81KR 仮想インターフェイス カード および Cisco UCS VIC-1240 仮想インターフェイス カード の場合：
  - iSCSI デバイスの MAC アドレスを設定しないでください。
  - HBA モードおよび Boot to Target 設定はサポートされていません。
  - OS を iSCSI ターゲットにインストールする場合、iSCSI ターゲットは OS イメージが存在するデバイスより後の順番にしておく必要があります。 たとえば、CD から iSCSI ターゲットに OS をインストールする場合、ブート順序は最初に CD、その後 iSCSI ターゲットとする必要があります。
  - DHCP Vendor ID（オプション 43）を使用している場合、オーバーレイ vNIC の MAC アドレスを /etc/dhcpd.conf に設定する必要があります。
  - サーバの iSCSI ブート後は、オーバーレイ vNIC の IP 詳細を変更しないでください。
- VMware ESX/ESXi オペレーティング システムは、iSCSI ブート ターゲット LUN へのコア ダンプ ファイルの保存をサポートしていません。 ダンプ ファイルはローカル ディスクに書き込む必要があります。

ブート ポリシーの iSCSI ブートの設定

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Boot Policies] を展開します。

ステップ 4 iSCSI ブートを設定するブート ポリシーをクリックします。

ステップ 5 [Work] ペインの [General] タブで [Add iSCSI Boot] をクリックします。

ステップ 6 [Add iSCSI Boot] ダイアログボックスで [iSCSI vNIC] を入力し、[Type] ドロップダウン リストから [primary] または [secondary] を選択します。

ステップ 7 [OK] をクリックして、ダイアログボックスを閉じます。

ステップ 8 [Save] をクリックして、ブート ポリシーを保存します。

iSCSI アダプタ ポリシーの作成

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Adapter Policies] を右クリックし、[Create iSCSI Adapter Policy]を選択します。

ステップ 4 [Create iSCSI Adapter Policy]ダイアログボックスで、[Name]、説明（任意）、[ConnectionTimeout]、[LUNBusyRetry Count]、および [DHCP Timeout]を入力します。

ステップ 5 [Enable TCP Timestamp]、[HBA Mode] 、および [Boot To Target]チェックボックスをオンにします。

ステップ 6 [OK] をクリックします。

iSCSI アダプタ ポリシーの削除

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Adapter Policies] を展開します。

ステップ 4 削除するポリシーを右クリックし、[Delete] を選択します。

ステップ 5 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。

iSCSI 認証プロファイルの作成

iSCSIブートの場合、イニシエータおよびターゲット認証プロファイルの両方を作成する必要があります。

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [iSCSI Authentication Profile] を右クリックし、[iSCSI Authentication Profile] を選択します。

ステップ 4 [Create iSCSI Authentication Profile] ダイアログボックスで、[Name]、[User ID]、説明（任意）、および [Password] を入力し、パスワードを確認します。

ステップ 5 [OK] をクリックします。

次の作業

認証プロファイルはサービス プロファイルとテンプレートのうち一方、または両方にインクルードします。

iSCSI 認証プロファイルの削除

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [iSCSI Authentication Profile] を展開します。

ステップ 4 削除する iSCSI 認証プロファイルを右クリックし、[Delete] を選択します。

ステップ 5 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。

ローカル ディスク設定ポリシー

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含む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 モードを設定できるようにします。

ローカル ディスク モードには次のものがあります。

- [No Local Storage]：ディスクレス サーバまたは SAN 専用の設定で使用します。 このオプションを選択する場合、このポリシーを使用する任意のサービスプロファイルを、ローカルディスクを持つサーバに関連付けることができません。
- [RAID 0 Striped]：データはアレイのすべてのディスクにストライプ化され、高速スループットを提供します。 データの冗長性はなく、いずれかのディスクで障害が発生すると、すべてのデータが失われます。
- [RAID 1 Mirrored]：データが 2 つのディスクに書き込まれ、1 つのディスクで障害が発生した場合でも完全なデータ冗長性を提供します。 最大アレイ サイズは、2 つのドライブの小さい方の空き容量に等しくなります。
- [Any Configuration]：変更なしのローカルディスク設定を転送するサーバ設定で使用します。
- [No RAID]：RAID を削除し、ディスク MBR およびペイロードを変更しない状態のままにするサーバ設定で使用します。

  [No RAID] を選択し、このポリシーをすでに RAID ストレージが設定されているオペレーティング システムを使用するサーバに適用した場合、ディスクの内容は削除されません。 そのため、[No RAID] モードの適用後にサーバでの違いがわからないことがあります。 よって、ポリシーの RAID 設定と、サーバの [Inventory] > [Storage] タブに表示される実際のディスク設定とが一致しない場合があります。

以前のすべての RAID 設定情報をディスクから削除するには、[No RAID] コンフィギュレーションモードの適用後にすべてのディスク情報を削除するスクラブ ポリシーを適用します。

- [RAID 5 Striped Parity]：データはアレイのすべてのディスクにストライプ化されます。 各ディスクの容量の一部に、ディスクの障害発生時にデータの再構築に使用できるパリティ情報が格納されます。 RAID 5 は、高い読み取り要求レートで、アプリケーションに適切なデータスループットを提供します。
- [RAID 6 Striped Dual Parity]：データはアレイのすべてのディスクにストライプ化され、2 つのパリティ ディスクを使用して、最大 2 つの物理ディスクの障害に対する保護を提供します。 データ ブロックの各行に、2 セットのパリティ データが格納されます。
- [RAID 10 Mirrored and Striped]：RAID 10 はミラー化されたディスクのペアを使用して、完全なデータ冗長性と高いスループット レートを提供します。
- [RAID 50 Striped Parity and Striped]：データが複数のストライプ化されたパリティ ディスクセットにストライプ化され、高いスループットと複数のディスク故障耐性を提供します。
- [RAID 60 Striped Dual Parity and Striped] ：データが複数のストライプ化されたパリティ ディスク セットにストライプ化され、高いスループットと優れたディスク故障耐性を提供します。

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。このポリシーを有効にするには、サーバに関連付ける必要があります。

すべてのローカル ディスク設定ポリシーに関するガイドライン

ローカル ディスク設定ポリシーを作成する前に、次のガイドラインを考慮してください。

HDD と SSD を混合しない

1 台のサーバや RAID 設定に、HDD と SSD を使用しないでください。

B200 M1 または M2 のデフォルト ローカル ディスク設定ポリシーを使用して、B200 M3 にサービス プロファイルを割り当てないでください。

B200 M1 および M2 サーバと B200 M3 サーバのストレージ コントローラで提供される RAID/JBOD サポートは異なっているため、B200M1 または M2 サーバのデフォルト ローカル ディスク設定ポリシーを含むサービス プロファイルを B200 M3 サーバに割り当てたり、再割り当てを行ったりすることはできません。 デフォルトのローカルディスク設定ポリシーには、[Any Configuration] モードまたは JBOD 設定が含まれます。

JBOD モードのサポート

（注） ローカル ディスクの JBOD モードをサポートしているのは、B200 M1、B200 M2、B200 M3、B250 M1、B250 M2、B22 M3 ブレード サーバのみです。

RAID 用に設定されているローカル ディスク設定ポリシーに関するガイドライン

MegaRAID ストレージ コントローラを搭載したサーバ用のローカル ディスク設定ポリシーに RAID 設定を設定する

ブレード サーバまたは統合されたラックマウント サーバに MegaRAID コントローラが搭載されている場合、そのサーバのサービスプロファイルに含まれるローカルディスク設定ポリシーでドライブの RAID 設定を設定する必要があります。 これを実行するには、そのサーバに定義されている RAID モードのいずれかを使用して、サービス プロファイルのローカル ディスク設定ポリシーを設定するか、[Any Configuration] モードと LSI ユーティリティ ツールセットを使用して、RAID ボリュームを作成します。

OS をインストールする前に RAID LUN を設定していないと、インストール時にディスク検出エラーが発生し、「No Device Found」といったエラー メッセージが表示される可能性があります。

サーバ プロファイルで [Any Configuration] モードが指定されている場合、RAID 1 クラスタ移行後にサーバが起動しない

RAID 1 クラスタの移行後、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 プロファイル内のローカルディスク設定ポリシーに RAID 1 ではなく [Any Configuration] モードが設定されていると、RAID LUN は、関連付け中およびその後も「非アクティブ」状態のままになります。 その結果、サーバは起動できなくなります。

この問題を回避するには、サーバに関連付けるサービス プロファイルに、移行前の元のサービス プロファイルとまったく同じローカル ディスク設定ポリシーが含まれるようにし、[Any Configuration] モードは含まれないようにします。

MegaRAID ストレージ コントローラを搭載したサーバ上で JBOD モードを使用しない

MegaRAID ストレージコントローラが搭載されたブレードサーバまたは統合ラックマウントサーバ上で JBOD モードまたは JBOD 操作を設定または使用しないでください。 JBOD モードと操作は、このサーバで完全に機能するよう設計されていません。

統合されたラックマウント サーバ内の RAID ボリュームと RAID コントローラはそれぞれ 1 つまで

Cisco UCS Manager と統合されているラックマウント サーバは、Cisco UCS Central とともに登録されており、サーバ上に存在するハード ドライブの数とは関係なく、RAID ボリュームを 1 つまでしか設定できません。

統合されたラックマウント サーバ内のローカル ハード ドライブは、1 つの RAID コントローラのみにすべて接続される必要があります。 Cisco UCS Manager との統合では、ローカル ハード ドライブが単一のラックマウント サーバ内の複数の RAID コントローラに接続することはサポートされていません。 そのため、Cisco UCS Manager と統合されるラックマウント サーバを発注する際は、単一の RAID コントローラ構成を要求することを推奨します。

また、サードパーティ製のツールを使用して、ラックマウント サーバ上に複数の RAID LUN を作成しないでください。 Cisco UCS Manager では、そのような設定はサポートされていません。

ブレード サーバ内の RAID ボリュームと RAID コントローラはそれぞれ 1 つまで

ブレード サーバは、サーバ内に存在するドライブの数とは関係なく、RAID ボリュームを 1 つまでしか設定できません。 ローカル ハード ドライブは、1 つの RAID コントローラのみにすべて接続される必要があります。 たとえば、B200 M3 に LSI コントローラと Intel Patsburg コントローラが搭載されていても、LSI コントローラだけが RAID コントローラして使用できます。

また、サードパーティ製のツールを使用して、ブレード サーバ上に複数の RAID LUN を作成しないでください。 Cisco UCS ManagerCisco UCS Central では、そのような設定はサポートされていません。

ミラー RAID で選択されるディスクの数は 2 つまでにする

ミラー RAID で選択されたディスクの数が 2 つを超えると、RAID 1 は RAID 10 LUN として作成されます。 この問題は、Cisco UCS B440 M1 サーバと B440 M2 サーバで発生する可能性があります。

一部のサーバの特定の RAID 設定オプションでは、ライセンスが必要

一部の Cisco UCS サーバには、特定の RAID 設定オプションのライセンスが必要です。 Cisco UCS ManagerCisco UCS Central で、このローカル ディスク ポリシーを含むサービス プロファイルとサーバを関連付けると、Cisco UCS ManagerCisco UCS Central によって選択された RAID オプションに適切なライセンスが備わっているかが確認されます。 問題がある場合は、サービスプロファイルを関連付ける際に、Cisco UCS ManagerCisco UCS Central に設定エラーが表示されます。

特定の Cisco UCS サーバの RAID ライセンス情報については、そのサーバの『*Hardware Installation Guide*』を参照してください。

B420 M3 サーバでは全コンフィギュレーション モードはサポートされていない

B420 M3 サーバでは、ローカル ディスク設定ポリシーで、次のような設定オプションはサポートされていません。

- RAID なし
- RAID 6 ストライプ化デュアルパリティ

また、B420 M3 では JBOD モードや操作はサポートされていません。

シングル ディスク RAID 0 設定は、一部のブレード サーバではサポートされていない

シングル ディスク RAID 0 設定は、次のブレード サーバではサポートされていません。

- Cisco UCS B200 M1
- Cisco UCS B200 M2
- Cisco UCS B250 M1
- Cisco UCS B250 M2

ローカル ディスク設定ポリシーの作成

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Local Disk Config Policies]を右クリックし、[Create Local Disk Config Policy].を選択します。

ステップ 4 [Create Local Disk Config Policy] ダイアログボックスに、[Name] とその他のオプションの詳細情報を入力します。

ステップ 5 [OK] をクリックします。

ローカル ディスク設定ポリシーの削除

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Local Disk Config Policies] を展開します。

ステップ 4 削除するポリシーを右クリックし、[Delete] を選択します。

ステップ 5 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。

電源制御ポリシー

Cisco UCS は、電力制御ポリシーの優先順位設定をブレード タイプおよびコンフィギュレーションとともに使用し、シャーシ内の各ブレードへ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。プライオリティを no-cap に設定すると、Cisco UCS がその特定のサーバから未使用の電力を利用することを防止します。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。

（注） 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。

電力制御ポリシーの作成

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Power Control Policies] を右クリックし、[Create Power Control Policy] を選択します。

ステップ 4 [Create Power Control Policy]ダイアログボックスで、[Name] と説明（任意）を入力し、[Power Capping]を使用するかどうかを選択し、[Power Priority]を入力します。

ステップ 5 [OK] をクリックします。

次の作業

ポリシーはサービス プロファイルまたはサービス プロファイル テンプレートにインクルードします。

電力制御ポリシーの削除

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Power Control Policies] を展開します。

ステップ 4 削除するポリシーを右クリックし、[Delete] を選択します。

ステップ 5 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。

ステップ 6

スクラブ ポリシー

このポリシーは、ディスカバリ プロセス中にサーバのローカル データおよび BIOS 設定に何が起こるか、サーバがいつ再認識されるか、またはサーバとサービス プロファイルの関連付けがいつ解除されるかを決定します。

（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、適切なホスト 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

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Scrub Policies] を右クリックし、[Create Scrub Policy] を選択します。

ステップ 4 [Create Scrub Policy]ダイアログボックスで、[Name]と説明（任意）を入力し、[DiskScrub] と [BIOS Setting Scrub]を使用するかどうかを選択します。

ステップ 5 [OK] をクリックします。

スクラブ ポリシーの削除

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Scrub Policies] を展開します。

ステップ 4 削除するポリシーを右クリックし、[Delete] を選択します。

ステップ 5 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。

Serial over LAN ポリシー

このポリシーは、このポリシーを使用するサービス プロファイルと関連付けられているすべてのサーバに対する Serial over LAN 接続の設定を行います。 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

Procedure

Step 1 メニュー バーで、[Servers]をクリックします。

Step 2 [Navigation] ペインで、 [Servers] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

Step 3 [Serial over LAN Policies] を右クリックし、[Create Serial over LAN Policy] を選択します。

Step 4 [Create Serial over LAN Policy] ダイアログボックスで、[Name] と説明（任意）を入力し、[Serial over LAN State] を選択し、ドロップダウン リストから [Speed] を選択します。

Step 5 [OK] をクリックします。

Serial over LAN ポリシーの削除

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Serial over LAN Policies] を展開します。

ステップ 4 削除するポリシーを右クリックし、[Delete] を選択します。

ステップ 5 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 ポリシー

このポリシーはサーバ ディスカバリ プロセス中に呼び出されます。 これは、サーバ プール ポリシー資格情報により、サーバと、ポリシーで指定されたターゲット プールが一致した場合にどのような処理が行われるかを定義します。

サーバが複数のプールに適合したときに、これらのプールにサーバ プール ポリシーがあった場合、このサーバはこれらすべてのプールに追加されます。

サーバ プール ポリシーの作成

はじめる前に

このポリシーは、次のリソースの 1 つ以上がシステムにすでに存在していることを前提にしています。

- 少なくとも 1 つのサーバ プール
- サーバ プール ポリシー資格情報（サーバをプールに自動的に追加する場合）

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Server Pool Policies] を右クリックし、[Create Policy] を選択します。

ステップ 4 [Create Policy] ダイアログボックスで、[Name] を入力し、ドロップダウン リストから [Target Pool] と [Qualification] を選択し、説明（任意）を入力します。

ステップ 5 [OK] をクリックします。

サーバ プール ポリシーの削除

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Server Pool Policies] を展開します。

ステップ 4 削除するポリシーを右クリックし、[Delete] を選択します。

ステップ 5 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 ポリシー資格情報

このポリシーは、ディスカバリ プロセス中に実行されたサーバのインベントリに基づいて、サーバを資格認定します。 資格情報は、サーバが選択基準を満たすかどうかを判断するために、ポリシーで設定されたルールです。 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 ポリシーの資格情報の作成

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Server Pool Policy Qualifications] を右クリックし、[Create Policy Qualification] を選択します。

ステップ 4 [Create Policy Qualification] ダイアログボックスで、[Name] と説明（任意）を入力します。

ステップ 5 [Actions] 領域で、ポリシー資格情報オプションを 1 つ以上設定します。

- [Create Domain Qualification]
- [Create Adapter Qualification]
- [Create Memory Qualification]
- [Create Processor Qualification]
- [Create Storage Qualification]
- [Create Server PID Qualification]

ステップ 6 [OK] をクリックします。

ドメイン資格情報の作成

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Server Pool Policy Qualifications] を展開します。

ステップ 4 変更するポリシー資格情報をクリックします。

ステップ 5 [Work] ペインで [General] タブの [Create Domain Qualification] をクリックします。

ステップ 6 [Create Domain Qualification] ダイアログボックスで [Name] を入力します。

ステップ 7 [Actions] 領域で、ドメイン資格情報オプションを 1 つ以上設定します。

- [Create Chassis/Server Qualification]
- [Create Address Qualification]
- [Create Owner Qualification]
- [Create Site Qualification]
- [Create Rack Qualification]

ステップ 8 [OK] をクリックして、ダイアログボックスを閉じます。

ステップ 9 [Save] をクリックしてポリシー資格情報を保存します。

アダプタ資格情報の作成

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Server Pool Policy Qualifications] を展開します。

ステップ 4 変更するポリシー資格情報をクリックします。

ステップ 5 [Work] ペインで [General] タブの [Create Adapter Qualification] をクリックします。

ステップ 6 [Create Adapter Qualification] ダイアログボックスで [Type] を選択し、[PID (RegEx)] を入力します。

ステップ 7 [Units] 領域で、単位の数を入力するか、または [Unspecified] チェックボックスをオンにします。

ステップ 8 [OK] をクリックして、ダイアログボックスを閉じます。

ステップ 9 [Save] をクリックしてポリシー資格情報を保存します。

メモリ資格情報の作成

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Server Pool Policy Qualifications] を展開します。

ステップ 4 変更するポリシー資格情報をクリックします。

ステップ 5 [Work] ペインで [General] タブの [Create Memory Qualification] をクリックします。

ステップ 6 [Create Memory Qualification] ダイアログボックスで、[Clock (MHz)]、[Min Cap (MB)]、[Width]、[Speed]、[Latency (ns)]、[Max Cap (MB)]、または [Units] に値を入力するか、未指定のままにします。

ステップ 7 [OK] をクリックして、ダイアログボックスを閉じます。

ステップ 8 [Save] をクリックしてポリシー資格情報を保存します。

プロセッサ資格情報の作成

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Server Pool Policy Qualifications] を展開します。

ステップ 4 変更するポリシー資格情報をクリックします。

ステップ 5 [Work] ペインで [General] タブの [Create Processor Qualification] をクリックします。

ステップ 6 [Create Processor Qualification] ダイアログボックスで [Processor Architecture] を選択し、[Min Number of Cores]、[Max Number of Cores]、[Min Number of Threads]、[Max Number of Threads]、[CPU Speed (MHz)]、[CPU Stepping]、[Min Number of Procs]、および [Max Number of Procs] に値を入力するか、未指定のままにします。

ステップ 7 [OK] をクリックして、ダイアログボックスを閉じます。

ステップ 8 [Save] をクリックしてポリシー資格情報を保存します。

ストレージ資格情報の作成

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Server Pool Policy Qualifications] を展開します。

ステップ 4 変更するポリシー資格情報をクリックします。

ステップ 5 [Work] ペインで [General] タブの [Create Storage Qualification] をクリックします。

ステップ 6 [Create Storage Qualification] ダイアログボックスで、[Diskless] 状態を選択し、[Number of Blocks]、[Block Size (Bytes)]、[Min Cap (MB)]、[Max Cap (MB)]、[Per Disk Cap (MB)]、および [Units] に値を入力するか、または未指定のままにします。

ステップ 7 [OK] をクリックして、ダイアログボックスを閉じます。

ステップ 8 [Save] をクリックしてポリシー資格情報を保存します。

サーバ PID 資格情報の作成

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Server Pool Policy Qualifications] を展開します。

ステップ 4 変更するポリシー資格情報をクリックします。

ステップ 5 [Work] ペインで [General] タブの [Create Server PID Qualification] をクリックします。

ステップ 6 [Create Server PID Qualification] ダイアログボックスで [PID (RegEx)] を入力します。

ステップ 7 [OK] をクリックして、ダイアログボックスを閉じます。

ステップ 8 [Save] をクリックしてポリシー資格情報を保存します。

シャーシ/サーバ資格情報の作成

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Server Pool Policy Qualifications] を展開します。

ステップ 4 変更するポリシー資格情報をクリックします。

ステップ 5 [Work] ペインで [General] タブの [Create Domain Qualification] をクリックします。

ステップ 6 [Create Domain Qualification] ダイアログボックスで [Create Chassis/Server Qualification] をクリックします。

ステップ 7 [Create Chassis/Server Qualification] ダイアログボックスで、[First Chassis Id] と [Number of Chassis] を入力します。

ステップ 8 [Create Server Qualification] をクリックし、サービス資格情報を [Server Qualifications] テーブルに入力します。

ステップ 9 [OK] をクリックして、ダイアログボックスを閉じます。

ステップ 10 [OK] をクリックして [Domain Qualification] ダイアログボックスを閉じます。

サーバ資格の作成

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。

サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、[Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Server Pool Policy Qualifications] を展開します。

ステップ 4 変更するポリシー資格情報をクリックします。

ステップ 5 [Work] ペインで [General] タブの [Create Domain Qualification] をクリックします。

ステップ 6 [Create Domain Qualification] ダイアログボックスで [Create Chassis/Server Qualification] をクリックします。

ステップ 7 [Create Chassis/Server Qualification] ダイアログボックスで [Create Chassis/Server Qualification] をクリックします。

ステップ 8 [Create Server Qualification] ダイアログボックスで、[First Slot Id] と [Number of Slots] を入力します。

ステップ 9 [OK] をクリックして、ダイアログボックスを閉じます。

ステップ 10 [OK] をクリックして [Create Domain Qualification] ダイアログボックスを閉じます。

ステップ 11 [OK] をクリックして [Domain Qualification] ダイアログボックスを閉じます。

アドレス資格情報の作成

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、[Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、[Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Server Pool Policy Qualifications] を展開します。

ステップ 4 変更するポリシー資格情報をクリックします。

ステップ 5 [Work] ペインで [General] タブの [Create Domain Qualification] をクリックします。

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

ステップ 7 [Create Address Qualification] ダイアログボックスで、[Minimum Address] と [Maximum Address] を入力します。

ステップ 8 [OK] をクリックして、ダイアログボックスを閉じます。

ステップ 9 [OK] をクリックして [Domain Qualification] ダイアログボックスを閉じます。

所有者資格情報の作成

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Server Pool Policy Qualifications] を展開します。

ステップ 4 変更するポリシー資格情報をクリックします。

ステップ 5 [Work] ペインで [General] タブの [Create Domain Qualification] をクリックします。

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

ステップ 7 [Create Owner Qualification] ダイアログボックスで、[First Chassis Id] と [Number of Chassis] に値を入力します。

ステップ 8 [OK] をクリックして、ダイアログボックスを閉じます。

ステップ 9 [OK] をクリックして [Domain Qualification] ダイアログボックスを閉じます。

ラック資格情報の作成

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Server Pool Policy Qualifications] を展開します。

ステップ 4 変更するポリシー資格情報をクリックします。

ステップ 5 [Work] ペインで [General] タブの [Create Domain Qualification] をクリックします。

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

ステップ 7 [Create Rack Qualification] ダイアログボックスで、[First Slot Id] と [Number of Slots] を入力します。

ステップ 8 [OK] をクリックして、ダイアログボックスを閉じます。

ステップ 9 [OK] をクリックして [Domain Qualification] ダイアログボックスを閉じます。

サイト資格情報の作成

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Server Pool Policy Qualifications] を展開します。

ステップ 4 変更するポリシー資格情報をクリックします。

ステップ 5 [Work] ペインで [General] タブの [Create Domain Qualification] をクリックします。

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

ステップ 7 [Create Site Qualification] ダイアログボックスで、[Name] と [Regex] を入力します。

ステップ 8 [OK] をクリックして、ダイアログボックスを閉じます。

ステップ 9 [OK] をクリックして [Domain Qualification] ダイアログボックスを閉じます。

サーバ プール ポリシーの資格情報の削除

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Server Pool Policy Qualifications] を展開します。

ステップ 4 削除するポリシー資格情報を右クリックし、[Delete] を選択します。

ステップ 5 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。

ポリシー資格情報からのドメイン資格情報の削除

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Server Pool Policy Qualifications] を展開します。

ステップ 4 変更するポリシー資格情報をクリックします。

ステップ 5 [Work] ペインで、[General] タブをクリックします。

ステップ 6 [Domain Qualifications] を展開します。

ステップ 7 削除する資格情報を右クリックし、[Delete] を選択します。

ステップ 8 [Save] をクリックしてポリシー資格情報を保存します。

ドメイン資格情報からのシャーシ/サーバ資格情報の削除

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Server Pool Policy Qualifications] を展開します。

ステップ 4 変更するポリシー資格情報をクリックします。

ステップ 5 [Work] ペインで、[General] タブをクリックします。

ステップ 6 [Domain Qualifications] を展開します。

ステップ 7 [Qualifications] テーブルで、変更するドメイン資格情報を展開します。

ステップ 8 [Chassis/Server Qualifications] を展開します。

ステップ 9 削除する資格情報を右クリックし、[Delete] を選択します。

ステップ 10 [Save] をクリックしてポリシー資格情報を保存します。

シャーシ/サーバ資格情報からのサーバ資格の削除

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Server Pool Policy Qualifications] を展開します。

ステップ 4 変更するポリシー資格情報をクリックします。

ステップ 5 [Work] ペインで、[General] タブをクリックします。

ステップ 6 [Domain Qualifications] を展開します。

ステップ 7 [Qualifications] テーブルで、変更するドメイン資格情報を展開します。

ステップ 8 [Chassis Qualifications] を展開します。

ステップ 9 変更するシャーシ資格情報を展開します。

ステップ 10 削除するサーバ資格情報を右クリックして、[Delete] を選択します。

ステップ 11 [Save] をクリックしてポリシー資格情報を保存します。

Creating a Full-State Backup Policy for Cisco UCS Domains

You can specify global full-state backup policy for the Cisco UCS domains at the domain group root and at the domain groups level. This policy will apply to all domain groups under the root.

（注） If you specify a remote location, make sure that location exists. You must have an absolute remote path ready when you select the remote location.

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 In the Navigation pane, expand Domain Groups > Domain Group root or click Domain Group root and expand to navigate to a specific domain group.

ステップ 3 Click the Backup/Export Policy node.

ステップ 4 In the work pane, click Full-State Backup Policy.

a) Provide a description for this backup.

b) In Location of the Image File, select the appropriate radio button to save the image file .

（注） You must have Cisco UCS Manager, release 2.2(2x) to use a remote location to save the backup image file.

c) In Schedule drop-down, select the frequency you want to schedule the backup for.
d) In Max Files, specify the maximum number of files you want to save in this location for ths system.

ステップ 5 Click Save.

Based on the schedule, Cisco UCS Central takes a snapshot of the Cisco UCS domain database and exports the file to the specified location. To view the progress of the backup operation, click the Task tab in the Properties dialog box.

ドメイン資格情報からの所有者資格情報の削除

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Server Pool Policy Qualifications] を展開します。

ステップ 4 変更するポリシー資格情報をクリックします。

ステップ 5 [Work] ペインで、[General] タブをクリックします。

ステップ 6 [Domain Qualifications] を展開します。

ステップ 7 [Qualifications] テーブルで、変更するドメイン資格情報を展開します。

ステップ 8 [Owner Qualifications] を展開します。

ステップ 9 削除する資格情報を右クリックし、[Delete] を選択します。

ステップ 10 [Save] をクリックしてポリシー資格情報を保存します。

ドメイン資格情報からのラック資格情報の削除

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Server Pool Policy Qualifications] を展開します。

ステップ 4 変更するポリシー資格情報をクリックします。

ステップ 5 [Work] ペインで、[General] タブをクリックします。

ステップ 6 [Domain Qualifications] を展開します。

ステップ 7 [Qualifications] テーブルで、変更するドメイン資格情報を展開します。

ステップ 8 [Rack Qualifications] を展開します。

ステップ 9 削除する資格情報を右クリックし、[Delete] を選択します。

ステップ 10 [Save] をクリックしてポリシー資格情報を保存します。

ドメイン資格情報からのサイト資格情報の削除

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Server Pool Policy Qualifications] を展開します。

ステップ 4 変更するポリシー資格情報をクリックします。

ステップ 5 [Work] ペインで、[General] タブをクリックします。

ステップ 6 [Domain Qualifications] を展開します。

ステップ 7 [Qualifications] テーブルで、変更するドメイン資格情報を展開します。

ステップ 8 [Site Qualifications] を展開します。

ステップ 9 削除する資格情報を右クリックし、[Delete] を選択します。

ステップ 10 [Save] をクリックしてポリシー資格情報を保存します。

ポリシー資格情報からのアダプタ資格情報の削除

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Server Pool Policy Qualifications] を展開します。

ステップ 4 変更するポリシー資格情報をクリックします。

ステップ 5 [Work] ペインで、[General] タブをクリックします。

ステップ 6 [Adapter Qualifications] を展開します。

ステップ 7 削除する資格情報を右クリックし、[Delete] を選択します。

ステップ 8 [Save] をクリックしてポリシー資格情報を保存します。

ポリシー資格情報からのメモリ資格情報の削除

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Server Pool Policy Qualifications] を展開します。

ステップ 4 変更するポリシー資格情報をクリックします。

ステップ 5 [Work] ペインで、[General] タブをクリックします。

ステップ 6 削除する資格情報を右クリックし、[Delete] を選択します。

ステップ 7 [Save] をクリックしてポリシー資格情報を保存します。

ポリシー資格情報からのプロセッサ資格情報の削除

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Server Pool Policy Qualifications] を展開します。

ステップ 4 変更するポリシー資格情報をクリックします。

ステップ 5 [Work] ペインで、[General] タブをクリックします。

ステップ 6 削除する資格情報を右クリックし、[Delete] を選択します。

ステップ 7 [Save] をクリックしてポリシー資格情報を保存します。

ポリシー資格情報からのストレージ資格情報の削除

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Server Pool Policy Qualifications] を展開します。

ステップ 4 変更するポリシー資格情報をクリックします。

ステップ 5 [Work] ペインで、[General] タブをクリックします。

ステップ 6 削除する資格情報を右クリックし、[Delete] を選択します。

ステップ 7 [Save] をクリックしてポリシー資格情報を保存します。

ポリシー資格情報からのサーバ資格情報の削除

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [Server Pool Policy Qualifications] を展開します。

ステップ 4 変更するポリシー資格情報をクリックします。

ステップ 5 [Work] ペインで、[General] タブをクリックします。

ステップ 6 削除する資格情報を右クリックし、[Delete] を選択します。

ステップ 7 [Save] をクリックしてポリシー資格情報を保存します。

vNIC/vHBA 配置ポリシー

vNIC/vHBA 配置ポリシーは、次のことを決定するために使用されます。

- 仮想ネットワーク インターフェイス接続（vCon）をサーバ上の物理アダプタにマッピングする方法。
- 各 vCon に割り当てることのできる vNIC または vHBA のタイプ。

各 vNIC/vHBA 配置ポリシーには、物理アダプタの仮想表現である vCon が含まれます。 vNIC/vHBA 配置ポリシーがサービス プロファイルに割り当てられ、サービス プロファイルがサーバに関連付けられると、vNIC/vHBA 配置ポリシー内の vCon が物理アダプタに割り当てられ、vNIC および vHBA がそれらの vCon に割り当てられます。

1 つのアダプタを持つブレード サーバやラック サーバの場合は、Cisco UCS がすべての vCon をそのアダプタに割り当てます。 4 つのアダプタを持つサーバの場合は、Cisco UCS が vCon1 をアダプタ 1 に、vCon2 をアダプタ 2 に、vCon3 をアダプタ 3 に、vCon4 をアダプタ 4 に割り当てます。

2 つまたは 3 つのアダプタを搭載したブレード サーバまたはラック サーバの場合、Cisco UCS は、サーバのタイプと選択された仮想スロット マッピング スキーム（ラウンド ロビンまたは線形順序）に基づいて vCon を割り当てます。 使用可能なマッピング スキームの詳細については、vCon のアダプタへの配置, （333 ページ） を参照してください。

Cisco UCS は、vCon の割り当て後、vNIC と vHBA を各 vCon の選択プリファレンスに基づいて割り当てます。これは、次のいずれかになります。

- ：設定されたすべての vNIC と vHBA が vCon に割り当てられます。明示的な割り当て、割り当て解除、動的のいずれかとなります。 これがデフォルトです。
- ：vNICs と vHBA を vCon に明示的に割り当てる必要があります。 サービス プロファイルや vNIC または vHBA のプロパティにより、明示的に割り当てることができます。
- ：動的な vNIC や vHBA を vCon に割り当てることはできません。 vCon は静的な vNIC と vHBA に使用可能で、割り当て解除または明示的な割り当てを行います。
- ：割り当て解除された vNIC や vHBA を vCon に割り当てることはできません。 vCon は動的な vNIC や vHBA の他、明示的に割り当てられた静的な vNIC や vHBA に使用できます。
- [Exclude usNIC]：Cisco usNICは vCon に割り当てることはできません。 vCon は、明示的に割り当てられている、割り当てられていない、または動的であっても、その他すべての設定された vNIC と vHBA に使用できます。

（注） [Exclude usNIC] に設定されたvCon に、明示的に割り当てられる SRIOV usNIC は、その vCon に割り当てられたままになります。

サービス プロファイルにvNIC/vHBA 配置ポリシーを含めない場合、Cisco UCS ManagerCisco UCS Central はデフォルトの [Round Robin] の vCon マッピング方式と [All] の vNIC/vHBA 選択プリファレンスに従い、各アダプタの機能と相対容量に基づいてアダプタ間で vNIC と vHBA を配布します。

vNIC/vHBA 配置ポリシーの作成

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [vNIC/vHBA Placement Policies] を右クリックし、[Create Placement Policy] を選択します。

ステップ 4 [Create Placement Policy] ダイアログボックスに、[Name] とその他のオプションの詳細情報を入力します。

ステップ 5 [OK] をクリックします。

vNIC/vHBA 配置ポリシーの削除

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、 [Servers] > [Policies] > [root]を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、 [Sub-Organizations] > *[Organization_Name]*を展開します。

ステップ 3 [vNIC/vHBA Placement Policies] を展開します。

ステップ 4 削除するポリシーを右クリックし、[Delete] を選択します。

ステップ 5 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。

vCon のアダプタへの配置

Cisco UCS は、サービス プロファイル内のすべての vCon をサーバ上の物理アダプタにマッピングします。 マッピングの実行方法、およびサーバ内の特定のアダプタへの vCon の割り当て方法は、次の条件によって決まります。

- サーバのタイプ。 2 つのアダプタ カードを搭載した N20-B6620-2 および N20-B6625-2 ブレード サーバは、他のサポートされるラック サーバまたはブレード サーバとは異なるマッピング スキームを使用します。
- サーバ内のアダプタの数。
- vNIC/vHBA 配置ポリシー内の仮想スロット マッピング スキームの設定（該当する場合）。

vNIC および vHBA を vCon に割り当てるための vNIC/vHBA 選択環境設定を設定するときは、この配置を検討する必要があります。

（注） vCon のアダプタへの配置は、アダプタの PCIE スロット番号とは関係ありません。 vCon の配置のために使用されるアダプタ番号は、アダプタの PCIE スロット番号ではなく、サーバ検出中にそれらに割り当てられる ID です。

N20-B6620-2 および N20-B6625-2 ブレード サーバでの vCon のアダプタへの配置

N20-B6620-2 および N20-B6625-2 ブレード サーバの場合は、2 つのアダプタを左から右に、vCon を右から左に数えます。 これらのブレード サーバの 1 台が 1 つのアダプタを持つ場合は、Cisco UCS がすべての vCon をそのアダプタに割り当てます。 サーバが 2 つのアダプタを持つ場合は、vCon の割り当ては仮想スロット マッピング スキームに基づいて行われます。

- ：Cisco UCS が vCon2 と vCon4 をアダプタ 1 に、vCon1 と vCon3 をアダプタ 2 に割り当てます。 これがデフォルトです。
- ：Cisco UCS が vCon3 と vCon4 をアダプタ 1 に、vCon1 と vCon2 をアダプタ 2 に割り当てます。

vCon のアダプタへの配置（他のすべてのサポート対象サーバの場合）

N20-B6620-2 および N20-B6625-2 ブレード サーバに加え、Cisco UCS によりサポートされるその他すべてのサーバでは、vCon の割り当ては、サーバに搭載されるアダプタ数と仮想スロット マッピング スキームに応じて異なります。

1 つのアダプタを持つブレード サーバやラック サーバの場合は、Cisco UCS がすべての vCon をそのアダプタに割り当てます。 4 つのアダプタを持つサーバの場合は、Cisco UCS が vCon1 をアダプタ 1 に、vCon2 をアダプタ 2 に、vCon3 をアダプタ 3 に、vCon4 をアダプタ 4 に割り当てます。

2 つまたは 3 つのアダプタを搭載したブレード サーバまたはラック サーバの場合、Cisco UCS は、選択した仮想スロット マッピング スキーム（ラウンド ロビンまたは線形順序）に基づいて vCons を割り当てます。

表 *4*：ラウンドロビン マッピング スキームを使用した *vCon* のアダプタへの配置

アダプタの数	vCon1 の割り当て	vCon2 の割り当て	vCon3 の割り当て	vCon4 の割り当て
1	アダプタ1	アダプタ1	アダプタ1	アダプタ1
2	アダプタ1	アダプタ2	アダプタ1	アダプタ2
3	アダプタ1	アダプタ2	アダプタ3	アダプタ2
4	アダプタ1	アダプタ2	アダプタ3	アダプタ4

ラウンド ロビンはデフォルトのマッピング スキームです。

表 *5*：線形順序マッピング スキームを使用した *vCon* のアダプタへの配置

アダプタの数	vCon1 の割り当て	vCon2 の割り当て	vCon3 の割り当て	vCon4 の割り当て
1	アダプタ1	アダプタ1	アダプタ1	アダプタ1
2	アダプタ1	アダプタ1	アダプタ2	アダプタ2
3	アダプタ1	アダプタ2	アダプタ3	アダプタ3
4	アダプタ1	アダプタ2	アダプタ3	アダプタ4

（注） Cisco UCS B440 M2 ブレード サーバに搭載された 2 つのアダプタで vCon ポリシーを使用している場合は、次のマッピングに注意してください。

- 最初に vCon 2 からアダプタ 1 へのマッピング
- 2 番目に vCon 1 からアダプタ 2 へのマッピング

vNIC/vHBA の vCon への割り当て

Cisco UCS ManagerCisco UCS Central には、vNIC/vHBA 配置ポリシーを使用して vNIC および vHBA を vCon に割り当てるオプションが 2 つあります。つまり、明示的割り当てと暗黙的割り当てです。

vNIC および vHBA の明示的割り当て

明示的割り当てでは、vCon を指定してから、vNIC または vHBA を割り当てるアダプタを指定します。 この割り当てオプションは、サーバ上のアダプタ間への vNIC および vHBA の配布方法を決定する必要がある場合に使用します。

明示的割り当ての場合に、vCon と関連付けられる vNIC および vHBA を設定するには、次の手順を実行します。

- vCon 設定を任意の使用可能なオプションに設定します。 vCon は、vNIC/vHBA 配置ポリシーを使用して設定するか、サーバに関連付けられているサービス プロファイルで設定できます。 vCon で [All] が設定されている場合でも、vNIC または vHBA をその vCon に明示的に割り当てることができます。
- vNIC および vHBA を vCon に割り当てます。 この割り当ては、vNIC または vHBA の仮想ホスト インターフェイス配置プロパティ、またはサーバに関連付けられたサービス プロファイルで実行できます。

vNIC や vHBA をそれらのタイプに設定されていないvCon に割り当てようとすると、Cisco UCS ManagerCisco UCS Central によって設定エラーが発生したことを示すメッセージ表示されます。

サービス プロファイルの関連付け中に、Cisco UCS ManagerCisco UCS Central は、設定済みの vNIC および vHBA の割り当てを、サーバ内の物理的なアダプタ数および機能と比較して検証し、その後でポリシー内の設定に従って vNIC および vHBA を割り当てます。 負荷分散は、このポリシーで設定された vCon およびアダプタへの明示的な割り当てに基づいています。

アダプタが 1 つ以上の vNIC または vHBA の割り当てをサポートしていない場合は、Cisco UCS ManagerCisco UCS Central によってサービス プロファイルに対するエラーが生成されます。

vNIC および vHBA の暗黙的割り当て

暗黙的割り当てでは、Cisco UCS ManagerCisco UCS Central は vCon を決定した後で、アダプタの機能とそれらの相対的な処理能力に基づいて vNIC または vHBA を割り当てるアダプタを決定します。 この割り当てオプションは、vNIC または vHBA が割り当てられるアダプタがシステム設定で重要ではない場合に使用します。

暗黙的割り当ての場合に vCon を設定するには、次の手順を実行します。

- vCon 設定を [All]、[Exclude Dynamic]、または [Exclude Unassigned] に設定します。 vCon は、vNIC/vHBA 配置ポリシーを使用して設定するか、サーバに関連付けられているサービス プロファイルで設定できます。
- vCon を [Assigned Only] に設定しないでください。 この設定を使用して暗黙的割り当てを実行することはできません。
- vNIC または vHBA を vCon に割り当てないでください。

サービス プロファイルの関連付け中に、Cisco UCS ManagerCisco UCS Central は、サーバ内の物理的なアダプタ数および機能を検証し、必要に応じて vNIC および vHBA を割り当てます。 負荷分散はアダプタの機能に基づいており、vNICおよびvHBAの配置は、システムによって決定される実際の順番に従って実行されます。 たとえば、あるアダプタが他のアダプタより多くの vNIC に対応できる場合、そのアダプタにはより多くの vNIC が割り当てられます。

サーバに設定されている数の vNIC および vHBA をアダプタでサポートできない場合、Cisco UCS ManagerCisco UCS Central は、サービス プロファイルに対する障害を生成します。

デュアル アダプタ環境での vNIC の暗黙的割り当て

各スロットにアダプタ カードが搭載されたデュアル スロット サーバで暗黙的な vNIC 割り当てを使用する場合、Cisco UCS ManagerCisco UCS Central は通常 vNIC/vHBA を次のように割り当てます。

- サーバの両方のスロットに同じアダプタがある場合、Cisco UCS ManagerCisco UCS Central は vNIC の半分と vHBA の半分を各アダプタに割り当てます。
- サーバに 1 つの 非 VIC アダプタと 1 つの VIC アダプタがある場合、Cisco UCS ManagerCisco UCS Central は、2 つの vNIC と 2 つの vHBA を非 VIC アダプタに割り当て、残りの vNIC と vHBA を VIC アダプタに割り当てます。
- サーバに 2 つの異なる VIC アダプタがある場合、Cisco UCS ManagerCisco UCS Central は、2 つのアダプタの相対的な処理能力に基づいて、vNIC と vHBA を比例的に割り当てます。

次の例は、サポートされるアダプタ カードのさまざまな組み合わせに対して、Cisco UCS ManagerCisco UCS Central が vNIC と vHBA をどのように割り当てるのか、その一般的な方法を示しています。

- 4 つ の vNIC と、2 つの Cisco UCS M51KR-B Broadcom BCM57711アダプタ（それぞれ 2 つの vNIC）を搭載したサーバを設定する場合、Cisco UCS ManagerCisco UCS Central は 2 つの vNIC を各アダプタに割り当てます。
- 50 の vNIC と、Cisco UCS CNA M72KR-Eアダプタ（2 つの vNIC）および Cisco UCS M81KR 仮想インターフェイス カードアダプタ（128 の vNIC）を搭載したサーバを設定する場合、Cisco UCS ManagerCisco UCS Central は、2 つの vNIC を Cisco UCS CNA M72KR-Eアダプタに割り当て、48 の vNIC を Cisco UCS M81KR 仮想インターフェイス カードアダプタに割り当てます。
- 150 の vNIC と、Cisco UCS M81KR 仮想インターフェイス カードアダプタ（128 の vNIC）および Cisco UCS VIC-1240 仮想インターフェイス カードアダプタ（256 の vNIC）を搭載したサーバを設定する場合、Cisco UCS ManagerCisco UCS Central は、50 の vNIC を Cisco UCS M81KR 仮想インターフェイス カードアダプタに割り当て、100 の vNIC を Cisco UCS VIC-1240 仮想インターフェイス カードアダプタに割り当てます。

（注） vNIC をファブリック フェールオーバー用に設定し、ダイナミック vNIC をサーバ用に設定した場合に、この暗黙的な割り当てに対する例外が発生します。

vNIC ファブリックのフェールオーバーが含まれる設定で、1 つのアダプタが vNIC のフェールオーバーをサポートしない場合、Cisco UCS ManagerCisco UCS Central は、ファブリックのフェールオーバーが有効になっているすべての vNIC を、それらをサポートするアダプタに割り当てます。 ファブリックのフェールオーバー用に設定された vNIC のみが設定に含まれる場合、それらをサポートしないアダプタに割り当てられる vNIC はありません。 ファブリックのフェールオーバー用に

設定された vNIC と設定されていない vNIC がある場合、Cisco UCS ManagerCisco UCS Central は、すべてのフェールオーバー vNIC を、それらをサポートするアダプタに割り当て、上記の比率に従って、少なくとも 1 つの非フェールオーバー vNIC を、それらをサポートしないアダプタに割り当てます。

ダイナミック vNIC が含まれる設定では、同様の暗黙的な割り当てが発生します。 Cisco UCS ManagerCisco UCS Central は、すべてのダイナミック vNIC をそれらをサポートするアダプタに割り当てます。 ただし、ダイナミック vNIC とスタティック vNIC の組み合わせでは、少なくとも 1 つのスタティック vNIC がダイナミック vNIC をサポートしていないアダプタに割り当てられます。

第 14 章

ストレージ ポリシー

この章は、次の内容で構成されています。

vHBA テンプレート

このテンプレートは、サーバ上の vHBA と SAN の接続方法を定義するポリシーです。 これは、vHBA SAN 接続テンプレートとも呼ばれます。

このポリシーを有効にするには、このポリシーをサービス プロファイルに含める必要があります。

vHBA テンプレートの作成

手順

ステップ 1 メニュー バーで、[Storage] をクリックします。

ステップ 2 [Navigation] ペインで、[Storage] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [vHBA Templates] を右クリックし、[Create vHBA Template] を選択します。

ステップ 4 [Create vHBA Template] ダイアログボックスで、[Name] と説明（任意）を入力します。

ステップ 5 [Fabric ID]、[Select VSAN]、および [Template Type] を選択します。

ステップ 6 ドロップダウン リストから [WWPN Pool] 、[QoS Policy] 、および [Stats Threshold Policy] を選択します。
このダイアログボックスから WWPN プール、QoS ポリシー、およびしきい値ポリシーを作成することもできます。

ステップ 7 [OK] をクリックします。

vHBA テンプレートの削除

手順

ステップ 1 メニュー バーで、[Storage] をクリックします。

ステップ 2 [Navigation] ペインで、[Storage] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [vHBA Templates] を展開します。

ステップ 4 削除する vHBA テンプレートを右クリックし、[Delete] を選択します。

ステップ 5 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。

デフォルトの vHBA 動作ポリシー

デフォルトの vHBA 動作ポリシーにより、サービス プロファイルに対する vHBA の作成方法を設定できます。 vHBAs を手動で作成するか、自動的に作成されるようにするかを選択できます。

デフォルトの vHBA 動作ポリシーを設定して、vHBA の作成方法を定義することができます。 次のいずれかになります。

- [None]：Cisco UCS ManagerCisco UCS Central は、サービス プロファイルにデフォルトの vHBA を作成しません。 すべての vHBA を明示的に作成する必要があります。
- [HW Inherit]：サービス プロファイルが vHBA を必要とし、何も明示的に定義されていない場合、Cisco UCS ManagerCisco UCS Central はサービス プロファイルに関連付けられたサーバにインストールされたアダプタに基づいて必要な vHBA を作成します。

（注） vHBA のデフォルト動作ポリシーを指定しない場合、[none] がデフォルトで使用されます。

vHBA のデフォルト動作の設定

vHBA のデフォルト動作ポリシーを指定しない場合、[none] がデフォルトで使用されます。

手順

ステップ 1 メニュー バーで、[Storage] をクリックします。

ステップ 2 [Navigation] ペインで、[Storage] > [Policies] > [root] を展開します。
ルート組織ではデフォルトの vHBA 動作ポリシーのみを設定できます。 サブ組織ではデフォルトの vHBA 動作ポリシーは設定できません。

ステップ 3 [Default vHBA Behavior] を右クリックし、[Properties] を選択します。

ステップ 4 [Properties (Default vHBA Behavior)] ダイアログボックスで [Action] を選択し、オプションの [vHBA Template] を選択します。

ステップ 5 [OK] をクリックします。

イーサネットおよびファイバチャネルアダプタポリシー

このようなポリシーは、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 ManagerCisco 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 ManagerCisco UCS Central で明らかに異なる場合があります。

- 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 ManagerCisco 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 ManagerCisco UCS Central では、この値をミリ秒で設定します。 したがって、Cisco UCS ManagerCisco UCS Central で 5500 ミリ秒と設定された値は、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 ManagerCisco 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 ManagerCisco 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

デフォルトでは、Cisco UCS は、イーサネット アダプタ ポリシーとファイバ チャネル アダプタ ポリシーのセットを提供します。 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。

重要 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。

ただし、（デフォルトの Windows のアダプタ ポリシーを使用する代わりに）Windows OS 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します。

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

ファイバ チャネル アダプタ ポリシーの作成

手順

ステップ 1 メニュー バーで、[Storage] をクリックします。

ステップ 2 [Navigation] ペインで、[Storage] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [Fibre Channel Adapter Policies] を右クリックし、[Create Fibre Channel Adapter Policy] を選択します。

ステップ 4 [Create Fibre Channel Adapter Policy] ダイアログボックスで、[Name] と説明（任意）を入力します。

ステップ 5 [Resources] 領域で、[Transmit Queues]、[Receive Queues]、[SCSI I/O Queues] の [Ring Size] を入力します。

ステップ 6 [Options] 領域で [FCP Error Recovery] と [Interrupt Mode] を選択し、[Flogi Retries] 、[Flogi Timeout (ms)]、[Plogi Retries]、[Plogi Timeout (ms)]、[Port Down Timeout (ms)]、[Port Down IO Retry]、[Link Down Timeout (ms)]、[IO Throttle Count]、および [Max LUNs Per Target] に値を入力します。

ステップ 7 [OK] をクリックします。

ファイバ チャネル アダプタ ポリシーの削除

手順

ステップ 1 メニュー バーで、[Storage] をクリックします。

ステップ 2 [Navigation] ペインで、[Storage] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [Fibre Channel Adapter Policies] を展開します。

ステップ 4 削除するポリシーを右クリックし、[Delete] を選択します。

ステップ 5 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。

LAN および SAN 接続ポリシー

接続ポリシーは、ネットワーク上のサーバと LAN または SAN 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。 これらのポリシーは、プールを使用してサーバにMACアドレス、WWN、および WWPN を割り当て、サーバがネットワークとの通信に使用する vNIC および vHBA を識別します。

（注） これらの接続ポリシーは、サービス プロファイルおよびサービス プロファイル テンプレートに含まれ、複数のサーバを設定するために使用できるので、静的 ID を接続ポリシーで使用することはお勧めしません。

LAN および SAN の接続ポリシーに必要な権限

接続ポリシーにより、ネットワークまたはストレージ権限のないユーザがネットワークおよびストレージ接続をしているサービス プロファイルおよびサービス プロファイル テンプレートを作成および変更することが可能になります。 ただし、ユーザは接続ポリシーを作成するための適切なネットワークおよびストレージの権限が必要です。

接続ポリシーの作成に必要な権限

接続ポリシーは、他のネットワークおよびストレージ構成と同じ権限を必要とします。 たとえば、接続ポリシーを作成するには、次の権限の少なくとも 1 つを有している必要があります。

- [admin]：LAN および SAN 接続ポリシーを作成できます
- [ls-server]：LAN および SAN 接続ポリシーを作成できます
- [ls-network]：LAN 接続ポリシーを作成できます
- [ls-storage]：SAN 接続ポリシーを作成できます

接続ポリシーをサービス プロファイルに追加するために必要な権限

接続ポリシーの作成後、ls-compute 権限を持つユーザは、そのポリシーをサービス プロファイルまたはサービス プロファイル テンプレートに組み込むことができます。 ただし、ls-compute 権限しかないユーザは接続ポリシーを作成できません。

SAN 接続ポリシーの作成

手順

ステップ 1 メニュー バーで、[Storage] をクリックします。

ステップ 2 [Navigation] ペインで、[Storage] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [SAN Connectivity Policies] を右クリックし、[Create SAN Connectivity Policy] を選択します。

ステップ 4 [Create SAN Connectivity Policy] ダイアログボックスで、[Name] と説明（任意）を入力します。

ステップ 5 [WWNN Assignment] 領域で [Global Pool] または [OUI] を選択します。

ステップ 6 [vHBA] テーブルで [Create vHBA] をクリックし、vHBA を SAN 接続ポリシーに追加します。

ステップ 7 [OK] をクリックします。

SAN 接続ポリシーの削除

手順

ステップ 1 メニュー バーで、[Storage] をクリックします。

ステップ 2 [Navigation] ペインで、[Storage] > [Policies] > [root] を展開します。
サブ組織のポリシーを作成するか、またはそのポリシーにアクセスするには、[Sub-Organizations] > *[Organization_Name]* を展開します。

ステップ 3 [SAN Connectivity Policies] を展開します。

ステップ 4 削除するポリシーを右クリックし、[Delete] を選択します。

ステップ 5 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。

第 15 章

統計情報管理

この章は、次の内容で構成されています。

統計情報管理

Cisco UCS Central の [Statistics] タブから、標準レポートとカスタム レポートを生成できます。 登録済み Cisco UCS ドメインの次のデータのレポートを生成できます。

- 冷却
- ネットワーク
- 電源
- 温度

重要

- 管理者またはレポートを作成、変更、または削除できる統計特権を持つユーザとしてログインする必要があります。 他のユーザは、レポートの実行と使用可能なデータの表示だけが可能です。
- Cisco UCS Central と登録済み Cisco UCS ドメインの間の接続で長い遅延または接続制限が発生している場合、指定された間隔で統計情報データが統計情報データベースに記録されません。 レポートを生成すると、その時間枠の情報がグラフまたはテーブルに表示されません。

レポートの生成時に、レポートをテーブル形式またはグラフ形式で表示するオプションを指定できます。 この表示オプションを使用して、特定のレポートタイプの最上位ドメインまたは最下位

ドメインを選択できます。 また、オーバーレイを使用してレポートタイプのデータを重ねることができきます。 次の 2 つのレポート オプションが用意されています。

- [Standard Reports]：ピーク時ファン速度、受信トラフィック（Rx）、送信トラフィック（Tx）平均電力、およびピーク時温度の事前定義レポート。 任意の時点でこれらの事前定義レポートを実行して、レポートを表示できます。 また、事前の設定を変更できますが、新しい標準レポートを作成することはできません。
- [Custom Reports]：使用可能なレポート オプションからカスタム レポートを作成するオプションです。 要件に基づいて、[Ungrouped Reports] で個々のレポートを作成するか、またはレポート グループを作成し、そのグループまたはサブグループ内でレポートを作成します。 カスタム レポート グループは任意の時点で作成、編集、または削除できます。

Cisco UCS Central での統計情報データの収集

Cisco UCS Central は、登録済み Cisco UCS ドメインからネットワーク、温度、冷却、および電力に関する統計データを収集して集約します。 Cisco UCS Central のインストール時に、統計情報データのデフォルトの保存場所を指定する必要があります。 統計情報データは、「ucscentral-stats-db」という名前の内部 PostgreSQL データベース、または Oracle 11g、MSSQL、または Postgre SQL などの外部データベースに保存できます。 インストール中にデフォルトの場所として内部ストレージを選択した場合、統計情報データの保存期間は最大 2 週間です。 収集されたデータを 2 週間以上保持する場合は、外部データベースをセットアップすることを推奨します。統計情報用の外部データベース，（349 ページ）を参照してください。

収集されたデータは、日次、毎時、週次、およびリアルタイム レコードに基づいて集約され、テーブルに保存されます。 このデータベースで SQL クエリを実行して、各レポート コンポーネント固有のデータを取得できます。外部データベースからのデータの取得，（352 ページ）を参照してください。 Cisco UCS Central データベースは、データを保存するデフォルト データベースです。

Cisco UCS Central CLI を使用して統計情報収集間隔を設定し、登録済み Cisco UCS ドメインから指定された間隔で情報を収集することができます。 新しい Cisco UCS ドメインが Cisco UCS Central に登録されると、Cisco UCS Centralは指定された統計情報収集間隔に新しいドメインをサブスクライブします。 収集間隔を再設定すると、登録済みドメインでデータが更新されます。 登録済み Cisco UCS ドメインは指定された収集間隔に基づいて統計情報を Cisco UCS Central に送信します。

統計情報収集間隔として次のいずれかを選択できます。

- 15 分（デフォルト）
- 30 分
- never：統計情報収集を無効にします。

重要　統計情報収集間隔は Cisco UCS Central CLI だけで指定できます。 Cisco UCS Central GUI で設定することはできません。 統計情報レポートは Cisco UCS Central GUI だけで表示できます。 Cisco UCS Central CLI では表示できません。

統計情報用の外部データベース

収集されたデータを 2 週間以上保持する場合や、6 つ以上の登録済み Cisco UCS ドメインから統計情報データを収集する場合は、外部データベースをセットアップできます。

（注）　外部データベースをセットアップするには、Cisco UCS Central CLI が必要です。

Cisco UCS Central からの統計情報収集では、次のデータベースを外部データベースとして使用できます。

- Oracle Database 11g Enterprise Edition Release 11.2.0.1.0- 64 ビット Production 以降。
- PostgreSQL Server 9.1.8 64 ビット以降
- Microsoft SQL Server 2012 (SP1) - 11.0.3000.0 (X64) 以降
- Microsoft SQL Server 2008 R2 10.50.1600.1 (X64) SP1 以降

外部データベースとして上記のいずれかのデータベースにアクセスし、セットアップする場合は、次の情報がわかっていることを確認してください。

- データベース サーバのホスト名
- データベース名
- [Username]
- パスワード
- ポート番号

（注）　Cisco UCS Central が設定された外部データベースにアクセスできるように、データベース サーバでファイアウォール ポートを開く必要があります。

外部データベースのセットアップ

Cisco UCS Central の初期セットアップ時、または統計情報収集のために外部データベースをセットアップする必要がある場合はいつでも、外部データベースをセットアップできます。

- **初期セットアップ時の外部データベースのセットアップ**：Cisco UCS Central の初期セットアップを実行する場合は、統計情報収集を有効にするように促されます。 [Yes] を選択すると、

外部データベースの情報を入力するように促されます。 [No] を選択すると、登録済み Cisco UCS ドメインからの統計情報データの収集は無効になります。

- **任意の時点**：Cisco UCS Central CLI を使用して外部データベースに接続し、登録済み Cisco UCS ドメイン の統計情報収集をセットアップできます。 Oracle データベースのセットアップの詳細については、外部 Oracle データベースへの接続, （354 ページ）を参照してください。 PostgreSQL データベースのセットアップの詳細については、外部 PostgreSQL データベースへの接続, （355 ページ）を参照してください。 MS SQL データベースでのクエリのセットアップについては、外部 Microsoft SQL Server データベースへの接続 を参照してください。

外部データベースは、登録済み Cisco UCS ドメインのネットワーク トラフィック、温度、電力および冷却に関する統計情報データを保存します。 ネットワーク、温度、電力および冷却に関する統計情報データを取得するため、外部データベースに対してクエリを実行できます。 データベースでのクエリの実行の詳細については、外部データベースからのデータの取得, （352 ページ）を参照してください。

（注） 統計情報データを保存する外部データベースのセットアップ時に、データベースから古いレコードを消去する間隔を設定する必要があります。 ユーザが外部データベースのメンテナンスを実行する必要があります。

外部データベースの設定に関するガイドライン

統計情報収集用のデータベースを設定した場合は、Cisco UCS Central サービスを必ず再起動してください。 サービスを再起動する必要がある状況を次に示します。

- ISO イメージを使用して Cisco UCS Central の最新バージョンへアップグレードした後

  古いバージョンの Cisco UCS Central には統計情報収集機能がありません。 アップグレードプロセスの完了後に、Cisco UCS Central CLI を使用して統計情報データ収集用に外部データベースをセットアップできます。

- Cisco UCS Central のインストール後に統計情報収集用に外部データベースをセットアップします。 外部データベースとして Oracle データベースまたは PostgreSQL データベースを使用できます。

- Oracle データベースから PostgreSQL データベースへの切り替え後、または PostgreSQL データベースから Oracle データベースへの切り替え後。

Cisco UCS Central 統計情報データベースのバックアップと復元

Cisco UCS Central データベースは、Full State バックアップ時にはバックアップされません。 統計情報データを保存する外部データベースをセットアップした場合は、標準のデータベース バックアップと復元の手順に従ってください。 ただし、外部データベースを復元する前に、Cisco UCS Central サービスを停止する必要があります。 このサービスを停止するには、Cisco UCS Central CLI にログインし、**local-mgmt** コマンド モードで **pmon stop** コマンドを実行する必要があります。 データベースの復元後に、Cisco UCS Central CLI で **pmon start** コマンドを実行して Cisco UCS Central サービスを開始します。

外部データベースでのエラーのトラブルシューティング

Cisco UCS Central が外部データベースへの接続に失敗する場合は、エラーが発生します。 Cisco UCS Central CLI のエラーの詳細を表示するには、**show fault** コマンドを使用するか、または Cisco UCS Central GUI の [Fault] パネルを確認します。 問題が解決すると、Cisco UCS Central は外部データベースへの接続を自動的に再試行します。 接続が確立されると、エラーが Cisco UCS Central CLI から消去されます。

外部データベースの統計情報データ

外部データベースでは、収集された統計情報データがテーブルに保存されます。 スクリプトを使用して、外部データベースから古い統計情報データを消去できます。 次の表で、データベーステーブルの名前と各テーブルに保存されるデータを説明します。

テーブル名	テーブルに保存されるデータ
adaptorHBAVnicStats	HBA アダプタのトラフィック データ。
adaptorNICVnicStats	NIC アダプタのトラフィック データ。
adaptorVnicStats	NIC/HBA アダプタのトラフィック データ。
computeMbPowerStats	ブレード サーバの電力データ。
computeMbTempStats	ブレード サーバの温度データ。
computeRackUnitMbTempStats	ラック サーバの温度データ。
equipmentChassisStats	シャーシの電力データ。
equipmentFanStats	シャーシのファン速度データ。
equipmentNetworkElementFanStats	FI のファン速度データ。
equipmentPsuStats	シャーシの PSU データ。
equipmentRackUnitFanStats	ラック サーバのファン速度データ。
equipmentRackUnitPsuStats	ラック サーバの PSU データ。
etherRxStats	受信イーサネット トラフィック データ。
etherTxStats	送信イーサネット トラフィック データ。
fcStats	FC トラフィック データ。
processorEnvStats	CPU 環境データ。

外部データベースからのデータの取得

データベースは、ネットワーク、温度、冷却、および電力に関する統計情報データを収集します。登録済み Cisco UCS ドメインから収集されたデータはデータベースに保存され、その後次のように集約されます。

- リアルタイム レコード
- 親から子への集約

次の表で、データベース テーブルとこのテーブルに保存される情報の特性を説明します。

統計情報の種類	統計情報	Table	MO/テーブル名	プロパティ
温度	吸気温度	1	computeMbTempStats	fmTempSenIo
	プロセッサの温度	2	processorEnvStats	温度
電源	ブレードの DC 電源	3	computeMbPowerStats	consumedPower
	シャーシの AC 電源	4	equipmentChassisStats	inputPower
冷却	FI ファン速度	5	equipmentNetworkElementFanStats	速度
	シャーシ ファン速度	6	equipmentFanStats	speed
FI イーサネット トラフィック	送信	7	etherTxStats	TotalBytes
	Receive（受信）	8	etherRxStats	TotalBytes
FI ファイバ チャネル トラフィック	送信/受信	9	fcStats	BytesTx、BytesRx
サーバ イーサネット トラフィック	送信/受信	10	adaptorNICVnicStats	BytesTx、BytesRx
サーバ FC トラフィック	送信/受信	11	adaptorHBAVnicStats	BytesTx、BytesRx
サーバ イーサネットおよびファイバ チャネル トラフィック	送信/受信	12	adaptorVnicStats	BytesTx、BytesRx

統計情報の種類	統計情報	Table	MO/テーブル名	プロパティ
該当なし	内部 DN マッピング テーブル	13	affectedId2Dn	該当なし

ヒント 統計情報データベースのテーブル名は30文字より長くすることができます。 Oracleデータベースでは 30 文字の制限があるため、テーブル名が切り捨てられることがあります。 Cisco UCS Central はこれを自動的に処理します。

リアルタイム レコードの集約

統計情報収集ポリシーは、登録済み Cisco UCS ドメインからのデータ収集間隔を指定します。 登録済み Cisco UCS ドメインから受信したデータはデータベースに保存され、時間、日次、または週次のレコードとして集約されます。 このリアルタイム レコードに基づく集約は、統計情報収集間隔によって定義されます。 データベースには、各レコード タイプごとに特定の ID または固有の識別情報があります。 次の表に、各レコード タイプの ID をリストします。

レコード タイプ	ID
Real Time	0
Hourly	1
Daily	2
Weekly	3

統計情報収集ポリシーが 15 分に設定されている場合、4 つのリアルタイム レコードごとに 1 つの時間レコードが作成され、データベースに保存されます。 日次レコード集約または週次レコード集約は内部で定義されており、収集間隔によって定義されません。 24 時間ごとに 1 つの日次レコードが作成され、データベースに保存されます。 同様に、7 日間ごとに 1 つの週次レコードが作成され、データベースに保存されます。

親から子への集約

このタイプのデータ集約は、識別名（DN）に基づきます。 DN は、データベースで定義されているすべてのオブジェクトの一意の ID です。 子要素から親要素へのデータの合計バイト数が収集され、データベース テーブルに保存されます。 たとえば、サンプル ネットワークでドメインに 2 つのファブリック インターコネクトがあるとします。 各ファブリック インターコネクトにはスロットがあり、各スロットには異なるポートがあります。 これらのポートの統計情報データは、ドメイン レベルまですべて集約されます。

外部 Oracle データベースへの接続

はじめる前に

- 外部 Oracle データベースをセットアップします。 サポートされているバージョンは、Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - 64 ビット Production 以上です。 データベース サーバのホスト名、データベース名、およびデータベースにアクセスするためのユーザ名とパスワードを書き留めます。 データベースにテーブルを作成し、これらのテーブルでレコードを追加、変更、削除するための特権が必要です。
- Cisco UCS Central が外部データベースにアクセスできるように、データベース サーバでファイアウォール ポートを開く必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	UCSC# **connect stats-mgr**	Statistics Manager モードを開始します。
ステップ 2	UCSC (stats-mgr) # **scope db-configuration**	データベース コンフィギュレーション モードを開始します。
ステップ 3	UCSC (stats-mgr) /db-configuration # **set type** *dbtype*	データベース タイプ（この場合は Oracle）を設定します。
ステップ 4	UCSC (stats-mgr) db-configuration # **set hostname** *hostname*	ホスト名を設定します。
ステップ 5	UCSC (stats-mgr) /db-configuration # **set port** *port-number*	ポートを設定します。 デフォルトの Oracle ポートは 1521 です。
ステップ 6	UCSC (stats-mgr) /db-configuration # **set database** *dbname*	データベース名を設定します。
ステップ 7	UCSC (stats-mgr) /db-configuration # **set user** *dbusername*	データベース ユーザ名を設定します。
ステップ 8	UCSC (stats-mgr) /db-configuration # **set pwd <enter_key>**	データベース パスワードを設定します。
ステップ 9	UCSC (stats-mgr) /db-configuration # **commit-buffer**	トランザクションをシステムの設定にコミットします。

次の例では、デフォルト ポートで外部 Oracle データベースを使用するようにCisco UCS Centralをセットアップし、トランザクションをコミットします。

```
UCSC # connect stats-mgr
UCSC (stats-mgr) # scope db-configuration
UCSC (stats-mgr) /db-configuration # set type oracle
```

```
UCSC (stats-mgr) /db-configuration # set hostname 10.10.10.10
UCSC (stats-mgr) /db-configuration # set port 1521
UCSC (stats-mgr) /db-configuration # set database DB1
UCSC (stats-mgr) /db-configuration # set user User1
UCSC (stats-mgr) /db-configuration # set pwd <enter_key>
Password:
UCSC (stats-mgr) /db-configuration # commit-buffer
```

次の作業

統計情報収集間隔をデフォルトの 15 分から 30 分に変更できます。 これは任意です。

外部 PostgreSQL データベースへの接続

はじめる前に

- 外部 PostgreSQL データベースをセットアップします。 サポートされているバージョンは PostgreSQL (9.2.3) 以上です。 データベース サーバのホスト名、データベース名、およびデータベースにアクセスするためのユーザ名とパスワードを書き留めます。 データベースにテーブルを作成し、これらのテーブルでレコードを追加、変更、削除するための特権が必要です。
- データベースの名前に **postgres** 句を含めることはできません。
- Cisco UCS Central が外部データベースにアクセスできるように、データベース サーバでファイアウォール ポートを開く必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	UCSC# **connect stats-mgr**	Statistics Manager モードを開始します。
ステップ 2	UCSC (stats-mgr) # **scope db-configuration**	データベース コンフィギュレーション モードを開始します。
ステップ 3	UCSC (stats-mgr) /db-configuration # **set type** *dbtype*	データベース タイプ（この場合は postgreSQL）を設定します。
ステップ 4	UCSC (stats-mgr) /db-configuration # **set hostname** *hostname*	ホスト名を設定します。
ステップ 5	UCSC (stats-mgr) /db-configuration # **set port** *port-number*	ポートを設定します。 デフォルトのポートは 5432 です。
ステップ 6	UCSC (stats-mgr) /db-configuration # **set database** *dbname*	データベース名を設定します。
ステップ 7	UCSC (stats-mgr) /db-configuration # **set user** *dbusername*	データベースユーザ名を設定します。

	コマンドまたはアクション	目的
ステップ 8	UCSC (stats-mgr) /db-configuration # **set pwd <enter_key>**	データベース パスワードを設定します。
ステップ 9	UCSC (stats-mgr) /db-configuration # **commit-buffer**	トランザクションをシステムの設定にコミットします。

次の例では、デフォルト ポートで外部postgreSQLデータベースを使用するようにCisco UCS Centralをセットアップし、トランザクションをコミットします。

```
UCSC # connect stats-mgr
UCSC (stats-mgr) # scope db-configuration
UCSC (stats-mgr) /db-configuration # set type postgres
UCSC (stats-mgr) /db-configuration # set hostname 10.10.10.10
UCSC (stats-mgr) /db-configuration # set port 5432
UCSC (stats-mgr) /db-configuration # set database DB1
UCSC (stats-mgr) /db-configuration # set user User1
UCSC (stats-mgr) /db-configuration # set pwd <enter_key>
Password
UCSC (stats-mgr) /db-configuration # commit-buffer
```

次の作業

統計情報収集間隔をデフォルトの 15 分から 30 分に変更できます。 これは任意です。

標準レポート

標準レポートは、Cisco UCS Central の事前定義レポートです。 標準レポートを使用して、ドメイン、シャーシ、またはサーバ レベルで集約された上位/下位 10 件の送信（Tx）データまたは受信（Rx）データを確認できます。 Cisco UCS Centralでは追加の標準レポートを作成することはできませんが、標準レポートのパラメータを変更できます。

重要 標準レポートのパラメータを変更するには、管理ユーザまたは統計特権を持つユーザとしてログインする必要があります。 その他のユーザは、現在利用可能なレポートを実行できますが、レポート パラメータを編集することはできません。

次の表で、Cisco UCS Central標準ネットワーク レポートについて説明します。

名前	説明
Default View	レポートのビュー。 次のいずれかを指定できます。 • グラフ • Table デフォルトでは [Chart] オプションが選択されています。
Display	レポートに含まれるデータの特性。 次のいずれかを指定できます。 • [Top Tx or Rx] • [Bottom Tx or Rx] デフォルトでは、[Top Tx or Rx] オプションが選択されます。
対象	レポートのエンドポイント。 次のいずれかを指定できます。 • [FI Ethernet Ports] • [FI FC Ports] • HBA • NIC デフォルトでは、[Fi Ethernet Ports] が選択されています。
持続時間	指定されているレポート実行期間。 次のいずれかを指定できます。 • [Customized date and time range] • [Last 3 hours] • 過去 6 時間 • Last 12 hours • 過去 24 時間 • [Last 48 hours] デフォルトでは、[Last 12 hours] が選択されます。

名前	説明
オーバーレイ	オーバーレイ情報をレポートに含めます。
コンテキスト	レポートのコンテキスト。 次のいずれかを指定できます。 • ドメイン • シャーシ • サーバ レポートのコンテキストを指定できるのは、エンドポイントが [HBAs] または [NICs] として指定されている場合だけです。 コンテキストを指定すると、ドメイン、シャーシまたはサーバレベルでサーバ NIC または HBA のトラフィックを確認できます。 [FI Ethernet Ports] や [FI FC Ports] などのその他のエンドポイントでは、コンテキストでデフォルトで選択されている [Domains] は変更できません。 コンテキストとして [Domains] を指定すると、ドメイン レベルのレポートがグラフでレンダリングされます。このグラフから、選択されているドメインのシャーシ レベルへさらにドリルダウンできます。 特定のシャーシ レベルからサーバにドリルダウンできます。 コンテキストとして [Chassis] を指定すると、データはシャーシ レベルでレンダリングされ、サーバ レベルまでドリルダウンできます。 コンテキストとして [Servers] を指定すると、データはサーバ レベルでレンダリングされ、それ以上ドリルダウンできません。

デフォルトの選択内容で標準ネットワーク レポートを実行すると、生成されるレポートには、過去 12 時間の Cisco UCS ドメインの [Fi Ethernet Ports] の上位と下位の送信（Tx）データまたは受信（Rx）データが、グラフ形式で表示されます。

関連項目

- ネットワーク レポートの生成, （359 ページ）

ネットワーク レポートの生成

はじめる前に

標準レポートのパラメータを変更するには、管理ユーザまたは統計特権を持つユーザとしてログインする必要があります。 その他のユーザは、現在利用可能なレポートを実行できますが、レポート パラメータを編集することはできません。

手順

ステップ 1 メニュー バーで、[Statistics] をクリックします。

ステップ 2 [Navigation] ペインで、[Standard Reports] を展開します。

ステップ 3 [Network] を展開し、生成するネットワーク レポート タイプを示すオプションをクリックします。

- [Receive Traffic (Rx)]
- [Transmit Traffic (Tx)]

ステップ 4 （任意） レポートのパラメータを変更するには、[Work] ペインで [Configure] をクリックします。

ステップ 5 [Work] ペインで、[Run/Refresh] をクリックします。
[Work] ペインにレポートが表示されます。 グラフ タイプの表示を選択した場合は、グラフにカーソルを合わせると、合計送信トラフィック（Tx）バイト数または合計受信トラフィック（Rx）バイト数が表示されます。 エンドポイントとして [NICs] または [HBAs] を選択し、レポートのコンテキストとして [Domains] または [Chassis] を選択した場合、レポートの棒をクリックするとドリルダウンできます。

ピーク ファン速度レポートの生成

エンドポイント [Chassis Fans]、[Fabric Interconnect Fans]、または [Rack Unit Fans] のピーク ファン速度レポートを生成できます。 ピーク ファン速度レポートには [Average Fan Speed] をオーバーレイできます。 [Context] は [Domains] です。

はじめる前に

レポートを作成する場合、またはレポートのパラメータを変更する場合は、管理者ユーザまたは統計特権を持つユーザとしてログインする必要があります。 統計特権のないユーザまたは管理者以外のユーザは、現在使用可能なレポートの実行のみを行えます。

手順

ステップ 1 メニュー バーで、[Statistics] をクリックします。

ステップ 2 [Navigation] ペインで、[Standard Reports] > [Cooling] を展開し、[Peak Fan Speed] をクリックします。

ステップ 3 既存のオプションを指定してレポートを実行するには、[Run Report To Load Data] をクリックします。

ステップ 4 既存の設定を変更するには、[Configure] をクリックします。 [Configure Peak Fan Speed] ダイアログボックスでオプションを変更し、[Save & Run] をクリックします。

ピーク温度レポートの生成

登録済み Cisco UCS ドメインで、サーバ吸気口温度に関するレポートを生成できます。 ピーク温度レポートには [Average Temperature] をオーバーレイできます。

はじめる前に

レポートを作成する場合、またはレポートのパラメータを変更する場合は、管理者ユーザまたは統計特権を持つユーザとしてログインする必要があります。 統計特権のないユーザまたは管理者以外のユーザは、現在使用可能なレポートの実行のみを行えます。

手順

ステップ 1 メニュー バーで、[Statistics] をクリックします。

ステップ 2 [Navigation] ペインで [Standard Reports] > [Temperature] を展開し、[Peak Temperature] をクリックします。

ステップ 3 既存のオプションを指定してレポートを実行するには、[Run Report To Load Data] をクリックします。

ステップ 4 既存の設定を変更するには、[Configure] をクリックします。 [Configure Peak Temperature] ダイアログボックスでオプションを変更し、[Save & Run] をクリックします。

平均電力レポートの生成

エンドポイント [Chassis (Input Power - AC)]、[Blade (Consumed Power - DC)]、または [Rack (Input Power - AC)] に関する平均電力レポートを生成できます。 平均電力レポートには [Peak Power] をオーバーレイできます。 [Context] は [Domains] です。

はじめる前に

レポートを作成する場合、またはレポートのパラメータを変更する場合は、管理者ユーザまたは統計特権を持つユーザとしてログインする必要があります。 統計特権のないユーザまたは管理者以外のユーザは、現在使用可能なレポートの実行のみを行えます。

手順

ステップ 1 メニュー バーで、[Statistics] をクリックします。

ステップ 2 [Navigation] ペインで [Standard Reports] > [Power] を展開し、[Average Power] をクリックします。

ステップ 3 既存のオプションを指定してレポートを実行するには、[Run Report To Load Data] をクリックします。

ステップ 4 既存の設定を変更するには、[Configure] をクリックします。 [Configure Average Power] ダイアログ ボックスでオプションを変更し、[Save & Run] をクリックします。

カスタム レポート

カスタム レポートは、Cisco UCS Central で作成可能なレポートです。 これらのレポートを作成するには、管理者または統計特権を持つユーザとしてログインする必要があります。 統計特権がないユーザ、または管理者以外のユーザの場合、UCS Central GUI の [Statistics] タブにアクセスできません。 UCS Central ではカスタム レポートを作成、変更、削除できます。

[Report Groups] または [Ungrouped Reports] のいずれかで、独自の要件に基づいてカスタム レポートを作成できます。 レポート グループは、カスタム レポートをグループ化するためのコンテナとして機能します。 カスタム レポートには、標準レポート（[Network]、[Cooling]、[Power]、および [Temperature] など）と同じレポート タイプ オプションがあります。

カスタム レポート グループの作成

Cisco UCS Central のカスタム レポート グループはフォルダのように機能し、グループ内にカスタム レポートを作成できます。 レポート グループ内に別のレポート グループを作成することもできます。

はじめる前に

管理者ユーザまたは統計特権を持つユーザとしてログインする必要があります。

手順

ステップ 1 メニュー バーで、[Statistics] をクリックします。

ステップ 2 ナビゲーション ペインで、[Custom Reports] を右クリックし、[Create Group] を選択します。

ステップ 3 （任意） [Work] ペインで [Create Schedule] をクリックします。

ステップ 4 [Create Group] ダイアログボックスで、レポート グループの [Name] と [Description] 指定します。

ステップ 5 [OK] をクリックします。
このレポート グループは、[Navigation] ペインの [Custom Reports] の下に表示されます。

次の作業

このレポート グループ内にカスタム レポートを作成できます。

レポート グループの削除

重要 Cisco UCS Central GUI からレポート グループを削除すると、そのグループ内に作成したすべてのレポートも削除されます。

はじめる前に

- このタスクを実行するには、管理者ユーザまたは統計特権を持つユーザとしてログインする必要があります。
- レポート グループ内に作成されているカスタム レポートのリストを確認します。

手順

ステップ 1 メニュー バーで、[Statistics] をクリックします。

ステップ 2 ナビゲーション ペインで、[Custom Reports] を展開します。
作成したレポート グループのリストが表示されます。

ステップ 3 削除するレポート グループを右クリックし、[Delete] をクリックします。
ダイアログボックスが開き、レポート グループの削除の確認が求められます。

ステップ 4 [Yes] をクリックします。
レポート グループと、そのグループ内のカスタム レポートが Cisco UCS Central GUI から削除されます。

カスタム レポートの作成

登録済みUCSドメインの特定の統計情報データを表示するために、カスタム レポートを作成できます。 Cisco UCS Centralでは、カスタム レポート グループを作成し、その中にレポートを作成できます。

はじめる前に

カスタム レポートを作成するには、管理ユーザまたは統計の権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 メニュー バーで、[Statistics] をクリックします。

ステップ 2 ナビゲーション ペインで、[Custom Reports] を展開します。

ステップ 3 [Ungrouped Reports] を右クリックし、[Create Report] を選択します。
レポート グループ内にレポートを作成するには、[Navigation] ペインで目的のレポート グループを右クリックし、[Create Report] を選択します。

レポート グループの作成の詳細については、カスタム レポート グループの作成, （361 ページ）を参照してください。

ステップ 4 [Create Report] ダイアログボックスで、レポートの [Name] を指定します。

ステップ 5 （任意） レポートの説明を指定します。

ステップ 6 [Properties] 領域で、必要な情報を指定します。
選択したレポート タイプに基づいて、[Properties] 領域の必須データが変化します 生成するレポートのタイプに必要なすべての情報を指定する必要があります。

ステップ 7 [OK] をクリックします。
このレポートは、[Navigation] ペインの [Custom Reports] の下と作業領域内に表示されます。

次の作業

レポートを実行してデータを表示できます。

カスタム レポートの実行

はじめる前に

レポートを作成する場合、またはレポートのパラメータを変更する場合は、管理者ユーザまたは統計特権を持つユーザとしてログインする必要があります。 統計特権のないユーザまたは管理者以外のユーザは、現在使用可能なレポートの実行のみを行えます。

手順

ステップ 1 メニュー バーで、[Statistics] をクリックします。

ステップ 2 ナビゲーション ペインで、[Custom Reports] を展開します。

ステップ 3 （任意） 実行するレポートがレポート グループに含まれている場合は、そのレポート グループ名を展開します。
実行するレポートがレポート グループに含まれていない場合は、[Ungrouped Reports] を展開します。

ステップ 4 レポートの名前を選択し、[Work] ペインで [Run/Refresh] をクリックします。

ステップ 5 （任意） グラフ表示とテーブル表示を切り替えるには、レポートで該当するオプションをクリックします。
レポートのテーブル ビューには、0 や 1 などの値が表示されることがあります。 値 0 は、レポートに表示されるデータが、登録済みUCSドメインから実際に収集されたデータであることを示します。 値 -1 は、Cisco UCS Central が指定されている期間内に UCS ドメインから統計情報を受信しなかったか、または指定されているエンドポイントの統計情報を UCS ドメインから受信しなかったことを示します。 これは、UCSドメインへの接続が失われ、接続が復元されるまでドメインの統計情報データが収集されなかった場合に発生します。 グラフ ビューでは、これはレポート上の破線で示されます。

カスタム レポートの削除

はじめる前に

このタスクを実行するには、管理者ユーザまたは統計特権を持つユーザとしてログインする必要があります。

手順

ステップ 1 メニュー バーで、[Statistics] をクリックします。

ステップ 2 ナビゲーション ペインで、[Custom Reports] を展開します。
作成したレポート グループのリストが表示されます。

ステップ 3 削除する必要があるレポートが含まれているレポート グループを展開します。
レポート グループがない場合は、[Ungrouped Reports] を展開します。

ステップ 4 レポート名を右クリックし、[Delete] をクリックします。
ダイアログボックスが開き、レポートの削除の確認が求められます。

ステップ 5 [Yes] をクリックします。
レポートが Cisco UCS Central GUI から削除されます。

第 16 章

バックアップと復元の管理

この章は、次の内容で構成されています。

Cisco UCS Central でのバックアップとインポート

Cisco UCS Central では、Cisco UCS Central 自体と登録済み UCS ドメインのバックアップと復元を実行できます。 バックアップおよび復元ポリシーをスケジュールするか、またはバックアップ操作をただちに実行できます。 スケジュールされたバックアップ操作または即時バックアップ操作には、次の 2 種類があります。

Cisco UCS Central と Cisco UCS ドメインの両方で、次のバックアップ ポリシーを個別にスケジュールできます。

- [Full state backup policy]：データベースをバックアップします。
- [Config all export policy]：設定を XML 形式でバックアップします。

UCS ドメインでは、これらのポリシーはローカルで定義するか、または Cisco UCS Central で定義できます。

スケジュール済みバックアップ ポリシーはデフォルトで無効になっています。 Cisco UCS Central または登録済み UCS ドメインをバックアップするには、この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 プロセスは、サーバ トラフィックまたはネットワーク トラフィックを中断せず、またこれらのトラフィックに影響しません。 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。

定期的なバックアップをスケジュールすると、バックアップ リポジトリはデータの蓄積を開始できます。 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。 ポリシー仕様を使用して、各 Cisco UCS ドメインで維持するバックアップの数を指定します。

（注） この最大数は、リモート ロケーションに保存できるバックアップ イメージ ファイルの数には影響しません。

また、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し、保存済みまたは未使用のバックアップ ディレクトリおよび設定を削除できます。

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、（バックアップが行われた）Cisco UCS ドメインが登録解除された後にのみ削除できます。
- config-all、config-logical、および config-system タイプのバックアップは、Cisco UCS Central ではオンデマンド バックアップとしてのみサポートされています。

バックアップ イメージ ファイル

データベースまたは設定のバックアップ ファイルは次の場所に保存できます。

- **ローカル ファイル システム**：ローカル ファイル システム。
- **リモート ロケーション**：TFTP、FTP、SCP、SFTP などのプロトコルを使用するリモート ロケーション。

重要 リモート ロケーションにイメージ ファイルを保存するオプションを使用するグローバル バックアップ ポリシーを指定するには、登録済み Cisco UCS ドメイン に Cisco UCS Manager リリース 2.2(2x) が必要です。 Cisco UCS ドメインに Cisco UCS Manager リリース 2.2(2x) がない場合、リモート バックアップを使用するグローバル バックアップ ポリシーは機能しません。

バックアップのスケジュール時に、いずれかの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できます。

設定の復元

管理対象 Cisco UCS ドメインを復元して設定するには、バックアップ リポジトリに保存されている設定を使用できます。 回復を実行する状況では Full State バックアップを使用してください。 バックアップ設定にアクセスするには、TFTP プロトコルを使用します。 Cisco UCS Central GUI と CLI の両方で、バックアップ ファイルの URL をコピーし、その URL を使用して新しいドメインを設定することができます。

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 ManagerCisco 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 ManagerCisco 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 ManagerCisco 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。

バックアップ タイプ

Cisco UCS Central では次のタイプのバックアップを 1 つ以上実行できます。

- [full-state]：完全な状態のバックアップはインストール時にのみ指定できます。 Full State バックアップは、システム全体のスナップショットを含むバイナリ ファイルです。 このバックアップにより生成されたファイルを使用して、ディザスタ リカバリ時にシステムを復元できます。 このファイルは、インポートには使用できません。

  （注） Full State バックアップ ファイルを使用した場合にのみ、バックアップ ファイルのエクスポート元のシステムと同じバージョンを実行しているシステムを復元できます。

- [config-all]：全設定バックアップは、すべてのシステムおよび論理構成設定を含む XML ファイルです。 このファイルは、インストール時のシステム復元には使用できません。
- [config-logical]：論理設定バックアップは、すべての論理構成設定を含む XML ファイルです。 サービスプロファイル、VLAN、VSAN、プール、ポリシー、ユーザ、ロケール、LDAP、NTP、および DNS 認証と管理設定が含まれます。 これらの構成設定をインポートするときに、このバックアップから生成されたファイルを使用できます。 このファイルは、インストール時の完全な状態のシステム復元には使用できません。
- [config-system]：システム構成バックアップは、統計情報設定とスケジューラ情報を含む XML ファイルです。 これらの構成設定をインポートするときに、このバックアップから生成されたファイルを使用できます。 このファイルは、インストール時の完全な状態のシステム復元には使用できません。

システムの復元

この復元機能は、ディザスタ リカバリに使用できます。

Cisco UCS からエクスポートされた任意の完全な状態のバックアップ ファイルからシステム設定を復元できます。 このファイルは、復元するシステム上の Cisco UCS からエクスポートされたものでなくてもかまいません。 別のシステムからエクスポートされたバックアップ ファイルを使用して復元する場合、ファブリック インターコネクト、サーバ、アダプタ、および I/O モジュールまたは FEX 接続を含めて、同じまたは同様のシステム設定およびハードウェアを持つシステムを使用することを強く推奨します。 ハードウェアまたはシステム設定が一致しない場合、復元されたシステムが完全には機能しないことがあります。 2 つのシステムの I/O モジュール リンク間またはサーバ間に不一致がある場合、復元操作後にシャーシまたはサーバまたはその両方を承認します。

この復元機能は、完全な状態のバックアップ ファイルにだけ使用できます。 完全な状態のバックアップ ファイルはインポートできません。 復元は、初期システム セットアップで実行します。

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。

（注） Full State バックアップ ファイルを使用した場合にのみ、バックアップ ファイルのエクスポート元のシステムと同じバージョンを実行しているシステムを復元できます。

Cisco UCS Central でのバックアップの有効化

デフォルトでは、バックアップ オペレーションは無効になります。データベースまたはシステム設定を自動的にバックアップするには、Cisco UCS Central バックアップと Cisco UCS ドメイン バックアップのバックアップ ポリシーを有効にする必要があります。

（注） この手順では、Cisco UCS Central バックアップを有効にする方法について説明します。[Operations Management] > [Domain Groups root] または特定の [Domain Group] から、Cisco UCS ドメインに対して同じ操作を実行します。

手順

ステップ 1 メニュー バーで、[Administration] タブをクリックします。

ステップ 2 [Navigation] ペインで [General] タブをクリックします。

ステップ 3 [Work] ペインで [Full-State Backup Policy] または [Config-All Backup Policy] をクリックします。

ステップ 4 [Backup State] で [Enable] をクリックします。

ステップ 5 [Save] をクリックします。
Cisco UCS Central は、選択された設定タイプのスナップショットを作成し、ファイルを指定された場所にエクスポートします。 バックアップ操作の進捗を表示するには、[Properties] ダイアログ ボックスの [Task] タブをクリックします。

Cisco UCS Central のバックアップと復元

Cisco UCS Central データベースまたは設定のバックアップは、スケジュールされているバックアップ ポリシーを使用して実行するか、またシステムのオンデマンドバックアップの作成時に実行できます。 次に、[Administration] タブでの Cisco UCS Central の 2 種類のスケジュール済みバックアップ ポリシーを示します。

- [Full-State Backup Policy]：このポリシーは、指定されているスケジュールに基づいて Cisco UCS Central データベース全体をバックアップします。 バックアップ イメージ ファイルはローカル システムに保存するか、または SCP、SFTP、FTP、TFTP などのプロトコルを使用

してリモートの場所に保存することができます。 Full State バックアップでは、管理インターフェイスが完全な状態で保持されます。

- [Config-All Export Policy]：Config-All エクスポート ポリシーは、システム設定だけを XML 形式でバックアップします。

また、[Operations Management] > [Backup and Import] > [UCS Central] > [Create System Backup] から任意の時点で Cisco UCS Central のオンデマンド バックアップを作成することもできます。

Cisco UCS Central の Full State バックアップ ポリシーの作成

指定されたスケジュールでバックアップをトリガーできるように、バックアップ状態が有効になっていることを確認します。

（注） リモート ロケーションを指定する場合は、そのロケーションが存在していることを確認します。 リモート ロケーションを選択する場合は、絶対リモート パスがわかっている必要があります。

手順

ステップ 1 メニュー バーで、[Administration] タブをクリックします。

ステップ 2 [Navigation] ペインで [General] をクリックします。

ステップ 3 [Work] ペインで [Full-State Backup Policy] タブをクリックします。

a) このバックアップの説明を入力します。

b) [Location of the Image File] で、イメージ ファイルの保存先に該当するオプション ボタンを選択します。

c) [Schedule] ドロップダウンで、バックアップをスケジュールする頻度を選択します。

d) [Max Files] に、システムのこの場所に保存するファイルの最大数を指定します。

ステップ 4 [Save] をクリックします。

スケジュールに基づいて、Cisco UCS Central がデータベースのスナップショットを作成し、このファイルを指定された場所にエクスポートします。 バックアップ操作の進捗を表示するには、[Properties] ダイアログボックスの [Task] タブをクリックします。

Cisco UCS Central の Config-All バックアップ ポリシーの作成

指定されたスケジュールでバックアップをトリガーできるように、バックアップ状態が有効になっていることを確認します。

（注） リモート ロケーションを指定する場合は、そのロケーションが存在していることを確認します。 リモート ロケーションを選択する場合は、絶対リモート パスがわかっている必要があります。

手順

ステップ 1 メニュー バーで、[Administration] タブをクリックします。

ステップ 2 [Navigation] ペインで [General] をクリックします。

ステップ 3 [Work] ペインで [Config-all Export Policy] タブをクリックします。

a) このバックアップの説明を入力します。

b) [Location of the Image File] で、イメージ ファイルの保存先に該当するオプション ボタンを選択します。

c) [Schedule] ドロップダウンで、バックアップをスケジュールする頻度を選択します。

d) [Max Files] に、システムのこの場所に保存するファイルの最大数を指定します。

ステップ 4 [Save] をクリックします。

スケジュールに基づいて、Cisco UCS Central がデータベースのスナップショットを作成し、このファイルを指定された場所にエクスポートします。 バックアップ操作の進捗を表示するには、[Properties] ダイアログボックスの [Task] タブをクリックします。

Cisco UCS Central のオンデマンド バックアップの作成

はじめる前に

バックアップ サーバの IPv4 アドレスまたは IPv6 アドレスおよび認証クレデンシャルを取得します。

手順

ステップ 1 [Navigation] ペインで、[Backup and Import] を展開します。

ステップ 2 [UCS Central] ノードをクリックします。

ステップ 3 [Work] ペインで、[Create System Backup] をクリックします。

ステップ 4 [Create System Backup] ダイアログボックスで、必須フィールドに入力します。

ステップ 5 [OK] をクリックします。

ステップ 6 Cisco UCS Central に確認ダイアログボックスが表示されたら、[OK] をクリックします。
[Backup State] をイネーブルに設定すると、Cisco UCS Central によって、選択した設定タイプのスナップショットが取得され、ファイルがネットワークの場所にエクスポートされます。 [Backup

Configuration] ダイアログボックスの [Backup Operations] テーブルに、バックアップ操作が表示されます。

ステップ 7 （任意） バックアップ操作または各モジュールのエクスポート操作の進捗を表示するには、[work] ペインで [Properties] をクリックし、次に [Status] タブをクリックします。

ステップ 8 [OK] をクリックし、[Backup Configuration] ダイアログボックスを閉じます。
バックアップ操作は完了するまで実行し続けます。 進捗を表示するには、[Backup Configuration] ダイアログボックスを再度開きます。

Cisco UCS Central のバックアップ スケジュールの作成

Full State バックアップ ポリシーと Config-All バックアップ ポリシーの両方でバックアップ スケジュールを作成し、イメージ ファイルをネットワーク ロケーションとリモート ファイル システムのいずれかに保存することができます。 スケジュールされている時点で Cisco UCS Central がバックアップをトリガーできるようにするため、[Backup State] は [Enable] に設定されている必要があります。

手順

ステップ 1 メニュー バーで、[Administration] タブをクリックします。

ステップ 2 [Navigation] ペインで [General] タブをクリックします。

ステップ 3 [Work] ペインで [Full-State Backup Policy] または [Config-All Backup Policy] をクリックし、次の操作を行います。

a) このバックアップの説明を入力します。
b) [Location of the Image File] で、イメージ ファイルの保存先に該当するオプション ボタンを選択します。
c) [Schedule] ドロップダウンで、バックアップをスケジュールする頻度を選択します。
d) [Max Files] に、システムのこの場所に保存するファイルの最大数を指定します。

ステップ 4 [Save] をクリックします。
指定したスケジュールに基づいて、Cisco UCS Central は選択された設定タイプのスナップショットを作成し、指定された場所にファイルをエクスポートします。 バックアップ操作の進捗を表示するには、[Properties] ダイアログボックスの [Task] タブをクリックします。

Cisco UCS Central のバックアップ操作の削除

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Backup and Import] を展開します。

ステップ 3 [UCS Central System] ノードをクリックします。

ステップ 4 [Backup] テーブルで、削除するバックアップ操作をクリックします。 操作の管理状態が [Enabled] に設定されている場合、テーブルでバックアップ操作をクリックすることはできません。

ステップ 5 [Backup Configuration] ダイアログボックスの [Backup Operations] テーブルで、削除するバックアップ操作をクリックします。

ヒント 操作の管理状態が [Enabled] に設定されている場合、テーブルでバックアップ操作をクリックすることはできません。

ステップ 6 [Backup Operations] テーブルのアイコン バーの [Delete] アイコンをクリックします。

ステップ 7 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。

ステップ 8 [Backup Configuration] ダイアログボックスで [Yes] をクリックし、バックアップ操作を削除します。

Cisco UCS ドメインのバックアップと復元

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 Cisco UCS Central の登録済み UCS ドメインのグローバル バックアップ ポリシーを作成できます。

グローバル バックアップ ポリシーの作成時に、ドメイン グループに含まれる Cisco UCS ドメインは、ポリシーの作成、更新、および削除イベントを継承します。 これらはグローバルポリシーであり、完全には削除できないため、これらのポリシーをリモートから削除すると管理状態がリセットされ、Cisco UCS Manager でディセーブルになります。 バックアップおよび復元処理をスケジュールするか、またはただちに実行できます。

重要 リモート ロケーションへの UCS ドメインのバックアップは、Cisco UCS Manager リリース 2.2(2x) 以降でのみサポートされています。 これよりも古いリリース バージョンの Cisco UCS Manager で稼働している UCS ドメインをバックアップすることはできません。

推奨事項

- Cisco UCS Manager で [Backup & Export Polices] を [Global] に設定してください。

- グローバル バックアップ ポリシーを有効にするには、ドメイン グループに Cisco UCS ドメインを登録する必要があります。
- セットアップで複数の Cisco UCS Manager リリース バージョンが使用されている場合は、1 つのドメイン グループに登録されている UCS Manager のバージョン リリースが同一であることを確認してください。
- 異なるドメイン グループで複数のバックアップ ポリシーを指定することはできません。 すべてのバックアップ ポリシーにはデフォルトの名前が設定されている必要があります。

Cisco UCS ドメインの Full State バックアップ ポリシーの作成

ドメイン グループのルートとドメイン グループ レベルで Cisco UCS ドメインのグローバル Full State バックアップ ポリシーを指定できます。 このポリシーは、ルートの下のすべてのドメイン グループに適用されます。

（注） リモート ロケーションを指定する場合は、そのロケーションが存在していることを確認します。 リモート ロケーションを選択する場合は、絶対リモート パスがわかっている必要があります。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開するか、または [Domain Group root] をクリックして特定のドメイン グループに移動します。

ステップ 3 [Backup/Export Policy] ノードをクリックします。

ステップ 4 [Work] ペインで、[Full-State Backup Policy] をクリックします。

a) このバックアップの説明を入力します。

b) [Location of the Image File] で、イメージ ファイルの保存先に該当するオプション ボタンを選択します。

（注） リモート ロケーションを使用してバックアップ イメージ ファイルを保存するには、Cisco UCS Manager リリース 2.2 (2x) が必要です。

c) [Schedule] ドロップダウンで、バックアップをスケジュールする頻度を選択します。

d) [Max Files] に、システムのこの場所に保存するファイルの最大数を指定します。

ステップ 5 [Save] をクリックします。

スケジュールに基づいて、Cisco UCS Central が Cisco UCS ドメイン データベースのスナップショットを作成し、このファイルを指定された場所にエクスポートします。 バックアップ操作の進捗を表示するには、[Properties] ダイアログボックスの [Task] タブをクリックします。

Cisco UCS ドメインでの Config-All エクスポート ポリシーの作成

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 Cisco UCS ドメインのグローバル Config-All バックアップ ポリシーを指定できます。 このポリシーは、ルートの下のすべてのドメイン グループに適用されます。

（注） リモート ロケーションを指定する場合は、そのロケーションが存在していることを確認します。 リモート ロケーションを選択する場合は、絶対リモート パスがわかっている必要があります。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開するか、または [Domain Group root] をクリックして特定のドメイン グループに移動します。

ステップ 3 [Backup/Export Policy] ノードをクリックします。

ステップ 4 [Work] ペインで、[Config-All Export Policy] をクリックします。

a) このバックアップの説明を入力します。

b) [Location of the Image File] で、イメージ ファイルの保存先に該当するオプション ボタンを選択します。

重要 リモート ロケーションを使用してバックアップ イメージ ファイルを保存するには、Cisco UCS Manager リリース 2.2 (2x) が必要です。

c) [Schedule] ドロップダウンで、バックアップをスケジュールする頻度を選択します。

d) [Max Files] に、システムのこの場所に保存するファイルの最大数を指定します。

ステップ 5 [Save] をクリックします。

スケジュールに基づいて、Cisco UCS Central が Cisco UCS ドメイン設定のスナップショットを作成し、このファイルを指定された場所にエクスポートします。 バックアップ操作の進捗を表示するには、[Properties] ダイアログボックスの [Task] タブをクリックします。

インポートの設定

Cisco UCS からエクスポートされたコンフィギュレーション ファイルをインポートできます。 ファイルは、同じ Cisco UCS からエクスポートされたものである必要はありません。

インポート機能は、すべてのコンフィギュレーションファイル、システム コンフィギュレーション ファイル、および論理コンフィギュレーション ファイルで使用できます。 インポートは、システムがアップ状態で、稼働中に実行できます。 インポート操作によって情報が変更されるのは、管理プレーンだけです。 インポート操作によって行われる一部の変更（サーバに割り当てら

れた vNIC に対する変更など）により、サーバのリブートまたはトラフィックを中断する他の動作が行われることがあります。

インポート操作はスケジュールできません。 ただし、インポート操作を前もって作成し、そのインポート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 では、管理状態がイネーブルに設定されるまで、コンフィギュレーション ファイルでインポート操作が実行されません。

インポート操作は、コンフィギュレーション バックアップ ファイルを保存する場所ごとに 1 つしか保持できません。

重要 リリース 2.1(1) 以降から古いリリースに設定をインポートすると、対応するサービス プロファイルがデフォルトのホスト ファームウェア パックを使用している場合に、サーバ ファームウェアが自動的にアップグレードまたはダウングレードされることがあります。 ただし設定をインポートする前に、デフォルト以外のホスト ファームウェアを使用するようにサービス プロファイルを変更できます。

インポート方法

次のいずれかの方法を使用して、Cisco UCS によるシステム設定のインポートおよびアップデートを実行できます。

- [Merge]：インポートされたコンフィギュレーション ファイルの情報は、既存の設定情報と比較されます。 矛盾が存在する場合、インポートされたコンフィギュレーション ファイルの情報で Cisco UCS ドメインの情報が上書きされます。
- [Replace]：現在の設定情報が、インポートされたコンフィギュレーション ファイルの情報で一度に 1 つのオブジェクトについて置き換えられます。

Cisco UCS Central の設定のインポート

Full State コンフィギュレーション ファイルはインポートできません。 次のコンフィギュレーション ファイルのいずれもインポートできます。

- All コンフィギュレーション
- システム設定
- Logical コンフィギュレーション

はじめる前に

コンフィギュレーション ファイルのインポートに必要な次の情報を収集します。

- バックアップ サーバの IP アドレスおよび認証クレデンシャル

- バックアップ ファイルの完全修飾名

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Backup and Import] を展開します。

ステップ 3 [UCS Central System] ノードをクリックします。

ステップ 4 [Work] ペインで、[Import] タブをクリックします。

ステップ 5 [Create Import Operation] をクリックします。

ステップ 6 [Create Import Operation] ダイアログボックスで、次のフィールドに値を入力します。

ステップ 7 （任意） [Local File System] を選択した場合は、タスクの終了後にファイルをダウンロードする必要があります。 [Download into backup file library] をクリックします。

ステップ 8 （任意） [Choose file] をクリックし、バックアップ ファイルのライブラリでアップロードおよびインポートするファイルを参照します。

ステップ 9 [OK] をクリックします。

ステップ 10 確認ダイアログボックスで、[OK] をクリックします。
[Import State] をイネーブルに設定した場合、Cisco UCS Central は、ネットワークの場所から設定をインポートします。 選択した処理に応じて、ファイル内の情報が既存の設定と結合されるか、既存の設定と置き換えられます。 インポート操作は、[Import Configuration] ダイアログボックスの [Import Operations] テーブルに表示されます。

ステップ 11 （任意） インポート操作の進捗および個々のモジュールのステータスを表示するには、次の手順を実行します。

a) [Properties] 領域にインポート操作が自動的に表示されない場合は、[Import Operations] テーブルでインポート操作をクリックします。

b) [Properties] 領域で、[FSM Details] バーの下矢印をクリックします。

[FSM Details] 領域が展開され、操作のステータスが表示されます。

ステップ 12 [OK] をクリックして、[Import Configuration] ダイアログボックスを閉じます。
インポート操作は、終了するまで実行されます。 進捗状況を表示するには、[Import Configuration] を再度開きます。

Cisco UCS Manager の設定のインポート

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。
ステップ 2 [Navigation] ペインで、[Backup and Import] を展開します。
ステップ 3 [UCS System] ノードをクリックします。
ステップ 4 [Work] ペインで、[Import] タブをクリックします。
ステップ 5 [+Create Import Operation] をクリックします。
ステップ 6 [Create Import Operation] ダイアログボックスで、次のフィールドに値を入力します。
ステップ 7 [Ok] をクリックします。

インポート操作の実行

[UCS Central System] オプションを選択し、Cisco UCS Central のインポート操作を実行します。
[UCS Central] オプションを使用して、Cisco UCS Manager のインポート操作を実行します。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。
ステップ 2 [Navigation] ペインで、[Backup and Import] を展開します。
ステップ 3 [UCS Central System] ノードをクリックし、Cisco UCS Central のインポート操作を実行します。
ステップ 4 （任意） [UCS Central] ノードをクリックし、Cisco UCS Manager のインポート操作を実行します。
ステップ 5 [Import] テーブルで、インポートするホスト名およびリモート ファイル名をクリックします。
ステップ 6 [Properties] をクリックします。
a) [General] タブをクリックし、[Enabled] オプション ボタンをクリックします。
b) [merge] または [replace] オプション ボタンをクリックします。

ステップ 7 [Ok] をクリックします。
Cisco UCS Central は、選択したバックアップ コンフィギュレーション ファイルをインポートします。 バックアップ操作の進捗を表示するには、[Properties] ダイアログボックスの [Task] タブをクリックします。

インポート操作の削除

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Backup and Import] を展開します。

ステップ 3 [UCS Central System] ノードをクリックします。

ステップ 4 [Work] ペインで、[Import] タブをクリックします。

ステップ 5 [Import] テーブルで、削除するインポート操作をクリックします。 操作の管理状態が [Enabled] に設定されている場合、テーブルでバックアップ操作をクリックすることはできません。

ステップ 6 [Import] テーブルで、削除するインポート操作をクリックします。

ヒント 操作の管理状態が [Enabled] に設定されている場合、テーブルでインポート操作をクリックすることはできません。

ステップ 7 [Import] テーブルのアイコン バーの [Delete] アイコンをクリックします。

ステップ 8 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。

第 17 章

インベントリのモニタ

この章は、次の内容で構成されています。

インベントリ管理

Cisco UCS Central は、すべての登録済み Cisco UCS ドメインからインベントリ詳細を収集します。ドメイン管理パネルから、登録Cisco UCS ドメインのコンポーネントを表示およびモニタできます。

Cisco UCS ドメインが正常に登録されると、Cisco UCS Central は次の詳細の収集を開始します。

- 物理インベントリ
- 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
- 障害情報

デフォルトのデータ収集間隔は10分です。 要件に基づいて、間隔をカスタマイズできます。 Cisco UCS ドメインと Cisco UCS Central 間の接続に失敗した場合、切断された Cisco UCS ドメインが再度検出されるたびに、Cisco UCS Central は、現在のデータの収集を開始し、ドメイン管理パネルに表示します。

[Domain Management] パネルの [General] タブには、登録済み Cisco UCS ドメインのリストが表示されます。 タブをクリックすると、各コンポーネントの詳細を表示できます。 また、このパネルからサーバの個別の Cisco UCS Manager または KVM コンソールも起動できます。

物理インベントリ

Cisco UCS ドメインのコンポーネントの物理インベントリ詳細は、ドメイン下に編成されています。 いずれのドメイン グループにも属していない Cisco UCS ドメインは、グループ化されていないドメイン下に配置されます。 ドメイン管理パネルに、詳細な装置のステータスおよびコンポーネントの次の物理的な詳細を表示できます。

- ファブリック インターコネクト：スイッチ カード モジュール
- サーバ：ブレード/ラック マウント サーバ
- シャーシ：IO モジュール
- ファブリック エクステンダ

サービス プロファイルとテンプレート

[Servers] タブから、登録済み Cisco UCS ドメインで使用可能なサービス プロファイルとサービス プロファイル テンプレートの完全なリストを表示できます。 [Service Profile] パネルには、サービス プロファイルの集約されたリストが表示されます。 同じ名前のサービス プロファイルは、割り当てられている組織下でグループ化されます。 サービスプロファイル名の横のインスタンス数は、特定のサービス プロファイルが Cisco UCS ドメインで使用される回数を示します。

[Service Profile Template] パネルから、使用可能なサービス プロファイル テンプレート、組織、および各サービス プロファイル テンプレートが Cisco UCS ドメインで使用される回数を表示できます。

グローバル論理リソースの概要

Cisco UCS Central Web UI では、[Global Service Profile] セクションでグローバル サービス プロファイルが作成されます。このプロファイルがサーバまたはサーバプールに関連付けられると、Cisco UCS ドメインに展開され、Cisco UCS Central に戻されます。 論理リソース/インベントリの一部として、これらのグローバル サービス プロファイルはローカル サービス プロファイル セクションの下のインスタンスとして報告されます。 [Servers] タブで、登録済み Cisco UCS ドメインで使用可能なローカル サービス プロファイルとローカル サービス プロファイル テンプレートの完全なリストを確認できます。 ローカル サービス パネルには、ローカル サービス プロファイルの集約

リストが表示されます。 同じ名前のローカル サービス プロファイルは、割り当てられている組織下でグループ化されます。 ローカル サービス プロファイル名の横のインスタンス数は、Cisco UCS Central に登録されているすべての Cisco UCS ドメインでこの名前を持つサービス プロファイルの数を示します。

[Local Service Profile Template] パネルで、利用可能なローカル サービス プロファイル テンプレート、組織、およびすべての登録済み Cisco UCS ドメインでこの名前を持つサービス プロファイルが使用された回数を確認できます。

インベントリ データ収集スケジュールの設定

手順

ステップ 1 メニュー バーで、[Equipment] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Management] をクリックします。

ステップ 3 [Work] ペインの [General] タブで、[Summary] > [Polling Interval] を選択し、ドロップダウン オプションをクリックします。
オプションから間隔を選択します。

ステップ 4 [Save] をクリックします。

インベントリ詳細の表示

[UCS Domains] ペインには、すべての登録済み Cisco UCS ドメインの完全なリストが表示されます。

ヒント 個々のドメインの詳細を表示するには、[UCS Name] カラムで、Cisco UCS ドメインの名前をクリックして選択し、[Properties] をクリックします。

手順

ステップ 1 メニュー バーで、[Equipment] をクリックします。

ステップ 2 [Navigation] ペインで、[UCS Domains] を展開します。

ステップ 3 [Work] ペインに、すべての登録済み Cisco UCS ドメインの詳細が表示されます。

サーバのインベントリ詳細の表示

はじめる前に

- Cisco UCS ドメインを Cisco UCS Central に登録する必要があります。
- インベントリ ステータスが OK とマークされている必要があります。

手順

ステップ 1 メニュー バーで、[Equipment] をクリックします。

ステップ 2 [Navigation] ペインで、[UCS Domains] > [Domain Groups] > [Domain Group root] > [UCS Domain] > [Chassis] > [Chassis number] > [Server] を展開します。
ラック サーバのインベントリ詳細を表示する場合は、[UCS Domains] > [Domain Groups] > [Domain Group root] > [UCS Domain] > [Rack-Mounts] > [Server] を展開します。

ステップ 3 インベントリ詳細を表示するサーバを選択します。

ステップ 4 [Work] ペインで [Inventory] タブををクリックします。

ステップ 5 インベントリ詳細を表示するコンポーネントを選択します。

個々の Cisco UCS ドメインの詳細の表示

手順

ステップ 1 メニュー バーで、[Equipment] をクリックします。

ステップ 2 [Navigation] ペインで、[UCS Domains] を展開します。

ステップ 3 [Work] ペインで、[UCS Domains] タブをクリックします。

ステップ 4 [UCS Name] カラムの下の Cisco UCS ドメイン名のリストから、詳細を表示するドメインを選択します。
Cisco UCS ドメインを選択すると、[Filter] の横のメニュー バーに 2 つのメニュー項目が表示されます。

ステップ 5 メニュー バーで、[Properties] をクリックします。
[Properties] ダイアログボックスには、選択した Cisco UCS ドメインに関する詳細情報が表示されます。

サービス プロファイルの表示

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、[Service Profiles] をクリックします。

ステップ 3 [Work] ペインにサービス プロファイルが表示されます。

a) （任意）[Instances] カラムの数値をクリックし、このサービス プロファイルが登録済み Cisco UCS ドメインで使用される回数を表示します。

サービス プロファイルの詳細の表示

また、インスタンスカラムの数値をクリックして、サービスプロファイルの詳細を表示することもできます。 この手順では、ナビゲーション ペインで各サービス プロファイルの詳細情報にアクセスする方法について説明します。

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、[Servers] > [Service Profile] > [Root] を展開し、サービス プロファイル名をクリックします。

ステップ 3 [Work] ペインに、選択されたサービス プロファイルの詳細が表示されます。

サービス プロファイル テンプレートの表示

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、[Service Profile Templates] をクリックします。

ステップ 3 [Work] ペインに、選択されたサービス プロファイル テンプレートの詳細が表示されます。

ローカル サービス プロファイルの表示

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、[Local Service Profiles] > [Root] > [Local Service Profile_Name] を展開します。

ステップ 3 情報を表示するローカル サービス プロファイルの [Instance] をクリックします。

ステップ 4 同様に、その他のリストされているローカル サービス プロファイルのプロパティを表示するには、表示するローカル サービス プロファイルを展開し、[Instance] をクリックします。

サブ組織の下の組織の作成

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで [Server] > [Local Service Profiles] > [Root] を展開します。

ステップ 3 [Sub-Organization] タブをクリックします。 [**Work**] ペインで [Create Organization] タブをクリックします。

ステップ 4 [Work] ペインで、[Sub-OrganizationCreate] > [Create Organization] をクリックします。

ステップ 5 [Create Organization] ダイアログボックスで、必須フィールドに入力します。

ステップ 6 [Ok] をクリックします。

第 18 章

システム管理

この章は、次の内容で構成されています。

DNS ポリシーの管理

Cisco UCS Central は、DNS サーバおよびドメイン名を定義するグローバル DNS ポリシーをサポートしています。 登録済み Cisco UCS ドメインでは、そのドメインのポリシー解決コントロール内で DNS 管理をグローバルに定義するようにしている場合、DNS 管理について Cisco UCS Central への登録に従うことになります。

DNS ポリシーの設定

はじめる前に

ドメイン グループ ルート下でドメイン グループの DNS ポリシーを設定する前に、最初にこのポリシーを作成する必要があります。 ドメイン グループ ルート下にあるポリシーは、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

ステップ 1 メニュー バーで、[Operations Management] をクリックします。
ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。
ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。
ステップ 4 [Navigation] ペインで、[Operational Policies] をクリックします。
ステップ 5 [Work] ペインで、[DNS] をクリックします。
ステップ 6 [Actions] 領域で、[Create] をクリックし、該当するすべてのフィールドに入力します。
ステップ 7 [Save] をクリックします。

DNS ポリシーの削除

DNS ポリシーを削除すると、そのポリシー内のすべての DNS サーバ設定が削除されます。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。
ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。
ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。
ステップ 4 [Navigation] ペインで、[Operational Policies] をクリックします。
ステップ 5 [Work] ペインで、[DNS] をクリックします。
ステップ 6 [Actions] 領域で、[Delete] をクリックします。
削除されたポリシーは、再設定されるまでドメイン グループの親から設定を継承します。
ステップ 7 [Save] をクリックします。

DNS ポリシーの DNS サーバの設定

はじめる前に

DNS ポリシーを設定します。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[DNS] をクリックします。

ステップ 5 [Actions] 領域で、[Add DNS Server] をクリックし、すべてのフィールドに入力します。

a) [Add DNS Server] ダイアログボックスで、すべてのフィールドに値を入力します。

b) [OK] をクリックします。

ステップ 6 [Save] をクリックします。

DNS ポリシーからの DNS サーバの削除

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[DNS] をクリックします。

ステップ 5 [Actions] 領域で、削除する DNS サーバを選択し、[Delete] をクリックします。
また、DNS サーバを右クリックして、そのオプションにアクセスすることもできます。

ステップ 6 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。

ステップ 7 [Save] をクリックします。

電力ポリシーの管理

Cisco UCS Central は、グローバルな電力割り当てポリシー（ポリシー ドリブン シャーシ グループ キャップ方式または手動のブレード レベル キャップ方式に基づく）、電力ポリシー（グリッド、n+1、または非冗長方式に基づく）を定義するグローバルな装置ポリシーをサポートしています。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電源管理と電源装置ユニットをグローバルに定義するようにしている場合、電源管理と電源装置ユニットについて Cisco UCS Central への登録に従うことになります。

グローバルな電力割り当て装置ポリシーの設定

はじめる前に

ドメイン グループ下でグローバルな電力割り当て装置ポリシーを設定する前に、最初にこのポリシーを作成する必要があります。 ドメイン グループ ルート下にあるポリシーは、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

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 5 [Work] ペインで、[Equipment] をクリックします。

ステップ 6 [Work] ペインで [Global Power Allocation Policy] タブをクリックします。

ステップ 7 [Actions] 領域で、[Create] をクリックし、該当するすべてのフィールドに入力します。

ステップ 8 [Save] をクリックします。

グローバルな電力割り当て装置ポリシーの削除

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 5 [Work] ペインで、[Equipment] をクリックします。

ステップ 6 [Work] ペインで [Global Power Allocation Policy] タブをクリックします。

ステップ 7 [Actions] 領域で、[Delete] をクリックします。
削除されたポリシーは、再設定されるまでドメイン グループの親から設定を継承します。

ステップ 8 [Save] をクリックします。

電力装置ポリシーの設定

はじめる前に

ドメイン グループ下で電力装置ポリシーを設定する前に、最初にこのポリシーを作成する必要があります。 ドメイン グループ ルート下にあるポリシーは、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

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 5 [Work] ペインで、[Equipment] をクリックします。

ステップ 6 [Work] ペインで、[Power Policy] タブをクリックします。

ステップ 7 [Actions] 領域で、[Create] をクリックし、該当するすべてのフィールドに入力します。

ステップ 8 [Save] をクリックします。

電力装置ポリシーの削除

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 5 [Work] ペインで、[Equipment] をクリックします。

ステップ 6 [Work] ペインで、[Power Policy] タブをクリックします。

ステップ 7 [Actions] 領域で、[Delete] をクリックします。
削除されたポリシーは、再設定されるまでドメイン グループの親から設定を継承します。

ステップ 8 [Save] をクリックします。

タイム ゾーンの管理

Cisco UCS Central は、国際的なタイム ゾーンと定義された NTP サーバに基づいて、グローバルな日付と時刻ポリシーをサポートしています。 登録済み Cisco UCS Manager クライアントでは、そのクライアントのポリシー解決コントロール内で日付と時刻をグローバルに定義するようにしている場合、日付と時刻の設定について Cisco UCS Central への登録に従うことになります。

日付と時刻ポリシーの設定

はじめる前に

ドメイン グループ下で日付と時刻ポリシーを設定する前に、最初にこのポリシーを作成する必要があります。 ドメイン グループ ルート下にあるポリシーは、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

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 5 [Work] ペインで、[DateTime] をクリックします。

ステップ 6 [Actions] 領域で、[Create] をクリックし、該当するすべてのフィールドに入力します。

ステップ 7 [Save] をクリックします。

日付と時刻ポリシーの削除

日付と時刻ポリシーは、ドメイン グループ ルート下にあるドメイン グループから削除されます。ドメイン グループ ルート下の日付と時刻ポリシーは、削除できません。

日付と時刻ポリシーを削除すると、そのポリシー内のすべての NTP サーバ設定が削除されます。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 削除するポリシーを含むドメイン グループのノードを展開します。

ステップ 4 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 5 [Work] ペインで、[DateTime] をクリックします。

ステップ 6 [Actions] 領域で、[Delete] をクリックします。
削除されたポリシーは、再設定されるまでドメイン グループの親から設定を継承します。

ステップ 7 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。

ステップ 8 [Save] をクリックします。

日付と時刻ポリシーの NTP サーバの設定

はじめる前に

ドメイン グループ ルート下にあるドメイン グループの NTP サーバを設定するには、最初に日付と時刻ポリシーを作成しておく必要があります。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[DateTime] をクリックします。

ステップ 5 [Actions] 領域で、[Add NTP Server] をクリックし、すべてのフィールドに入力し、[OK] をクリックします。

ステップ 6 [Save] をクリックします。

NTP サーバのプロパティの設定

既存の NTP サーバのプロパティは、NTP サーバ インスタンスを保存する前に更新される場合があります。保存された NTP サーバの名前を変更するには、削除して再作成する必要があります。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 5 [Work] ペインで、[DateTime] をクリックします。

ステップ 6 [Actions] 領域で、設定する NTP サーバを選択して [Properties] をクリックし、すべてのフィールドに入力します。

また、NTP サーバを右クリックして、そのオプションにアクセスすることもできます。 NTP サーバが保存されている場合は、[Actions] 領域の [Properties] をクリックしてアクセスできる [Properties (NTP Provider)] ダイアログを編集できません。 保存されている NTP サーバのサーバ名を変更するには、NTP サーバを削除して再作成します。

a) [Properties (NTP Provider)] ダイアログボックスで、すべてのフィールドに値を入力します。

名前	説明
[NTP Server] フィールド	使用する NTP サーバの IP アドレスまたはホスト名。 （注） IPv4 アドレスではなくホスト名を使用する場合、DNS サーバを設定する必要があります。 Cisco UCS ドメインが Cisco UCS Central に登録されていないか、DNS 管理が [ローカル] に設定されている場合は、Cisco UCS Manager で DNS サーバを設定します。 Cisco UCS ドメイン Cisco UCS Central に登録されていないか、DNS 管理が [グローバル] に設定されている場合は、Cisco UCS Central で DNS サーバを設定します。

b) [OK] をクリックします。

ステップ 7 [Save] をクリックします。

日付と時刻ポリシーからの NTP サーバの削除

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[DateTime] をクリックします。

ステップ 5 [Actions] 領域で、削除する NTP サーバを選択し、[Delete] をクリックします。
また、NTP サーバを右クリックして、そのオプションにアクセスすることもできます。 削除される NTP サーバは、再設定されるまでドメイン グループの親からの設定を継承します。

ステップ 6 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。

SNMP ポリシー

Cisco UCS Central は、SNMP トラップおよび SNMP ユーザの有効化と無効化、定義を行うグローバル SNMP ポリシーをサポートしています（通常のパスワードとプライバシー パスワード、認証タイプ md5 または sha、および暗号化タイプ DES と AES-128 により）。 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をリモートでモニタする機能を提供します。 また、Cisco UCS Central ホスト IP を変更し、新しい IP で SNMP エージェントを再起動することもできます。 SNMP が、アクティブとスタンバイの両方の Cisco UCS Central サーバで稼働しており、設定が両方のサーバで保持されます。 Cisco UCS Central は、オペレーティング システムにより管理される情報ベース（MIB）のみへの読み取りアクセス権を提供します。Cisco UCS Central CLI を使用して、SNMP v1、v2c のコミュニティ ストリングを設定し、SNMPv3 ユーザを作成および削除することができます。

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 内のソフトウェア コンポーネントで、Cisco UCS Central のデータを維持し、必要に応じて SNMP にレポートします。

Cisco UCS Central には、エージェントと MIB 収集が含まれます。 SNMP エージェントを有効にし、マネージャとエージェント間のリレーションシップを作成するには、Cisco UCS Central で SNMP を有効にし、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 では OS MIB モードだけがサポートされます。

Cisco UCS Central では SNMPv1、SNMPv2c、および SNMPv3 がサポートされます。 SNMPv1 と SNMPv2c は、ともにコミュニティベース形式のセキュリティを使用します。 SNMP を定義する RFC を次に示します。

- 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）

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 に対して set 操作は使用できません。 Cisco UCS Centralでサポートされている MIB を次に示します。

- 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 およびCisco UCS Central MIB をサポートしません。

SNMPv3 ユーザの認証プロトコル

Cisco UCS Central は、SNMPv3 ユーザ向けに次の認証プロトコルをサポートします。

- HMAC-MD5-96（MD5）
- HMAC-SHA-96（SHA）

SNMPv3 ユーザの AES プライバシー プロトコル

Cisco UCS Central は、SNMPv3 メッセージ暗号化用プライバシー プロトコルの 1 つとして、Advanced Encryption Standard（AES）を使用し、RFC 3826 に準拠します。 AES が無効であり、プライバシー パスワードが設定されている場合、暗号化に DES が使用されます。

AES-128 設定を有効にし、SNMPv3 ユーザのプライバシー パスワードをインクルードした場合、Cisco UCS Central はプライバシー パスワードを使用して 128 ビット AES キーを生成します。 AES プライバシー パスワードは最小で 8 文字です。 パスフレーズをクリア テキストで指定する場合、最大 64 文字を指定できます。

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 では SNMP 通知がトラップとして生成されます。 SNMP マネージャはトラップ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、トラップの信頼性は低くなります。

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 *6*： ***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	[Username]	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。

SNMP ポリシーの設定

はじめる前に

ドメイン グループで SNMP ポリシーを設定する前に、SNMP ポリシーが最初に作成されていることを確認します。 ドメイン グループ ルート下にあるポリシーは、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

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで [Domain Groups] > [Domain Group root] を展開するか、またはポリシーを作成するドメイン グループの名前を指定します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 5 [Work] ペインで、[SNMP] をクリックします。

ステップ 6 [Actions] 領域で、[Create] をクリックし、該当するすべてのフィールドに入力します。
[Domain Group root] ノード下の [Operational Policies] では、[Create] をクリックして該当するすべてのフィールドに入力する必要はありません。

a) [Actions] 領域で [Enabled] をクリックし、[Admin State] を選択します。
[Enabled] の場合、Cisco UCS Central は Cisco UCS Central システムのモニタに SNMP を使用します。 Cisco UCS は、ドメイン グループ自体が SNMP を使用して設定されていない場合は、ドメイン グループのすべての Cisco UCS ドメイン で SNMP を使用します。

デフォルトの状態は [Disabled] であり、フィールドは表示されていません。 デフォルトの状態のままの場合は、SNMP ポリシーが無効になります。

b) [Community/Username] フィールドにコミュニティまたはユーザ名を入力します。
Cisco UCS が SNMP ホストに送信するトラップ メッセージに含めるデフォルトの SNMP v1 または v2c コミュニティ名あるいは SNMP v3 ユーザ名を使用できます。 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。 デフォルトは public です。

c) [System Contact] フィールドにシステム連絡先担当者情報を入力します。
[System Contact] に指定する担当者は、SNMP の実装を担当します。 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。

d) [System Location] フィールドにシステム ロケーションを入力します。
[System Location] により、SNMP エージェント（サーバ）が稼働するホストの場所が定義されます。 最大 510 文字の英数字文字列を入力します。

ステップ 7 [Save] をクリックします。

次の作業

SNMP トラップおよび SNMP ユーザを作成します。

SNMP トラップの作成

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[SNMP] をクリックします。

ステップ 5 [SNMP Traps] 領域で [Create SNMP Trap] をクリックし、[Create SNMP Trap] ダイアログボックスの該当するすべてのフィールドに入力します。

a) [IP Address] フィールドに SNMP ホストの IP アドレスを入力します。
Cisco UCS は、定義された IP アドレスにトラップを送信します。

b) [Community/Username] フィールドにコミュニティまたはユーザ名を入力します。
Cisco UCS が SNMP ホストに送信するトラップ メッセージに含めるデフォルトの SNMP v1 または v2c コミュニティ名あるいは SNMP v3 ユーザ名を使用できます。 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。 デフォルトは public です。

c) [Port] フィールドに、ポート番号を入力します。
Cisco UCS は定義されたポートを使用して、トラップを送信するため SNMP ホストと通信します。 1 ～ 65535 の整数を入力します。 デフォルト ポートは 162 です。

d) SNMP のバージョンを選択するため、[v1]、[v2c]、または [v3] をクリックします。

e) [trap] をクリックして、[Type] で SNMP トラップのタイプを選択します。
f) [auth]、[no auth]、または [priv] をクリックして、[v3Privilege] を定義します。
g) [OK] をクリックします。

ステップ 6 [Save] をクリックします。

SNMP ユーザの作成

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[SNMP] をクリックします。

ステップ 5 [SNMP Users] 領域で [Create SNMP User] をクリックし、[Create SNMP User] ダイアログボックスの該当するすべてのフィールドに入力します。

a) [Name] フィールドに SNMP 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）、-（ハイフン）も指定できます。
（注） ローカル側で認証されたユーザ名と同一の SNMP ユーザ名を作成することはできません。
b) [md5] または [sha] をクリックして、認証タイプを選択します。
c) [AES-128] チェックボックスをオンにします。
オンにすると、このユーザに AES-128 暗号化が使用されます。
d) [Password] フィールドにユーザ パスワードを入力します。
e) [Confirm Password] フィールドにユーザ パスワードもう一度入力します。
f) [Privacy Password] フィールドに、このユーザのプライバシー パスワードを入力します。
g) [Confirm Privacy Password] フィールドに、このユーザのプライバシー パスワードをもう一度入力します。
h) [OK] をクリックします。

ステップ 6 [Save] をクリックします。

SNMP ポリシーの削除

SNMP ポリシーは、ドメイン グループ ルート下にあるドメイン グループから削除されます。 ドメイン グループ ルート下の SNMP ポリシーは、削除できません。

SNMP ポリシーを削除すると、そのポリシー内のすべての SNMP トラップおよび SNMP ユーザ設定が削除されます。

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 5 [Work] ペインで、[SNMP] をクリックします。

ステップ 6 [Actions] 領域で、[Delete] をクリックします。
削除されたポリシーは、再設定されるまでドメイン グループの親から設定を継承します。

ステップ 7 [Save] をクリックします。

SNMP トラップの削除

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[SNMP] をクリックします。

ステップ 5 [SNMP Traps] 領域で、削除する SNMP トラップを選択し、[Delete] をクリックします。
また、SNMP トラップを右クリックして、そのオプションにアクセスすることもできます。

ステップ 6 [Save] をクリックします。

SNMP ユーザの削除

手順

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 4 [Work] ペインで、[SNMP] をクリックします。

ステップ 5 [SNMP Users] 領域で、削除する SNMP トラップを選択し、[Delete] をクリックします。
また、SNMP ユーザを右クリックして、そのオプションにアクセスすることもできます。

ステップ 6 [Save] をクリックします。

グローバル障害ポリシーの設定

はじめる前に

ドメイン グループ下でグローバル障害デバッグ ポリシーを設定する前に、最初にこのポリシーを作成する必要があります。 ドメイン グループ ルート下にあるポリシーは、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

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 5 [Work] ペインで、[Debug] をクリックします。

ステップ 6 [Work] ペインで [Global Fault Policy] タブをクリックします。

ステップ 7 [Actions] 領域で、[Create] をクリックし、該当するすべてのフィールドに入力します。
[Domain Group root] ノード下の [Operational Policies] では、[Create] をクリックして該当するすべてのフィールドに入力する必要はありません。

ステップ 8 [Save] をクリックします。

Core File Exporter

Cisco UCS コア ファイルが発生すると、ただちに Core File Exporter が使用され、それらのファイルが TFTP を介してネットワーク上の指定の場所にエクスポートされます。 この機能を使用することにより、tar ファイルをコア ファイルのコンテンツと一緒にエクスポートできます。

TFTP Core Export ポリシーの設定

はじめる前に

ドメイン グループ下で TFTP Core Export デバッグ ポリシーを設定する前に、最初にこのポリシーを作成する必要があります。 ドメイン グループ ルート下にあるポリシーは、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

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 5 [Work] ペインで、[Debug] をクリックします。

ステップ 6 [Work] ペインで [TFTP Core Export Policy] タブをクリックします。

ステップ 7 [Actions] 領域で、[Create] をクリックし、該当するすべてのフィールドに入力します。
[Domain Group root] ノード下の [Operational Policies] では、[Create] をクリックして該当するすべてのフィールドに入力する必要はありません。

ステップ 8 [Save] をクリックします。

syslog コンソール ポリシーの設定

はじめる前に

ドメイン グループ下で syslog コンソール デバッグ ポリシーを設定する前に、最初にこのポリシーを作成する必要があります。 ドメイン グループ ルート下にあるポリシーは、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

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 5 [Work] ペインで、[Debug] をクリックします。

ステップ 6 [Work] ペインで、[Syslog Policy] タブをクリックします。

ステップ 7 [Work] ペインで、[Console] タブをクリックします。

ステップ 8 [Actions] 領域で、[Create] をクリックし、該当するすべてのフィールドに入力します。
[Domain Group root] ノード下の [Operational Policies] では、[Create] をクリックして該当するすべてのフィールドに入力する必要はありません。

ステップ 9 [Save] をクリックします。

syslog モニタ ポリシーの設定

はじめる前に

ドメイン グループ下で syslog モニタ デバッグ ポリシーを設定する前に、最初にこのポリシーを作成する必要があります。 ドメイン グループ ルート下にあるポリシーは、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

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 5 [Work] ペインで、[Debug] をクリックします。

ステップ 6 [Work] ペインで、[Syslog Policy] タブをクリックします。

ステップ 7 [Work] ペインで、[Monitor] タブをクリックします。

ステップ 8 [Actions] 領域で、[Create] をクリックし、該当するすべてのフィールドに入力します。
[Domain Group root] ノード下の [Operational Policies] では、[Create] をクリックして該当するすべてのフィールドに入力する必要はありません。

ステップ 9 [Save] をクリックします。

syslog リモート宛先ポリシーの設定

はじめる前に

ドメイン グループ下で syslog リモート宛先デバッグ ポリシーを設定する前に、最初にこのポリシーを作成する必要があります。 ドメイン グループ ルート下にあるポリシーは、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

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 5 [Work] ペインで、[Debug] をクリックします。

ステップ 6 [Work] ペインで、[Syslog Policy] タブをクリックします。

ステップ 7 [Work] ペインで、[Remote Destination] タブをクリックします。

ステップ 8 [Actions] 領域で、[Create] をクリックし、該当するすべてのフィールドに入力します。
[Domain Group root] ノード下の [Operational Policies] では、[Create] をクリックして該当するすべてのフィールドに入力する必要はありません。

ステップ 9 [Save] をクリックします。

syslog ソース ポリシーの設定

はじめる前に

ドメイン グループ下で syslog ソース デバッグ ポリシーを設定する前に、最初にこのポリシーを作成する必要があります。 ドメイン グループ ルート下にあるポリシーは、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

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 5 [Work] ペインで、[Debug] をクリックします。

ステップ 6 [Work] ペインで、[Syslog Policy] タブをクリックします。

ステップ 7 [Work] ペインで、[Source] タブをクリックします。

ステップ 8 [Actions] 領域で、[Create] をクリックし、該当するすべてのフィールドに入力します。
[Domain Group root] ノード下の [Operational Policies] では、[Create] をクリックして該当するすべてのフィールドに入力する必要はありません。

ステップ 9 [Save] をクリックします。

syslog ログファイル ポリシーの設定

はじめる前に

ドメイン グループ下で syslog ログファイル デバッグ ポリシーを設定する前に、最初にこのポリシーを作成する必要があります。 ドメイン グループ ルート下にあるポリシーは、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

ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Group root] を展開します。

ステップ 3 [Domain Groups root] ノードで、[Operational Policies] をクリックします。

ステップ 4 [Navigation] ペインで、[Operational Policies] をクリックします。

ステップ 5 [Work] ペインで、[Debug] をクリックします。

ステップ 6 [Work] ペインで、[Syslog Policy] タブをクリックします。

ステップ 7 [Work] ペインで、[LogFile] タブをクリックします。

ステップ 8 [Actions] 領域で、[Create] をクリックし、該当するすべてのフィールドに入力します。
[Domain Group root] ノード下の [Operational Policies] では、[Create] をクリックして該当するすべてのフィールドに入力する必要はありません。

ステップ 9 [Save] をクリックします。

Cisco UCS Central のハイ アベイラビリティについて

Cisco UCS Central を 2 つの仮想ノードに展開する場合、クラスタ セットアップでハイ アベイラビリティが提供されます。 ハイ アベイラビリティにより、安定性と冗長性が Cisco UCS Central には直接反映され、Cisco UCS ドメイン管理には間接的に反映されます。 Cisco UCS Central のハイ アベイラビリティにより、以下が実現します。

- サーバ、シャーシ、ファブリック インターコネクト、およびデータ センターの数の増加に伴う大規模な Cisco UCS 展開の簡素化。
- ハイパーバイザに依存しない環境での UCS Central VM の冗長性。
- データベースとイメージ リポジトリを収容する共有ストレージ デバイス。
- 継続的な運用のための組み込み障害検出（DME、VM、ホスト、またはネットワーク障害）機能と自動フェールオーバー。

ハイ アベイラビリティ アーキテクチャ

ハイ アベイラビリティを実現するため、それぞれ異なるホスト上の 2 つの VM に Cisco UCS Central を展開します。 ハイ アベイラビリティ：

- ハイ アベイラビリティに対応するため、クラスタの Cisco UCS Central に 1 つ以上の Cisco UCS Manager を登録する必要があります。
- 個々の VM および VIP アドレスに対して同じサブネットを使用します。
- 両方のホストからアクセスできる各 VM に、ミラーリングされたマルチパス共有ストレージ ディスクを設定できます。
- UCS Manager を使用して quorum データを保存し、プライマリ ノードを判別します。
- Cisco UCS Manager と同様の方法で、ハートビートや選択プロトコルなどの情報を交換します。 この結果、よりシンプルな設計、コード再利用性の向上、容易なフェールオーバー条件の定義が実現しました。

ハイ アベイラビリティを使用する場合の注意事項とガイドライン

Cisco UCS Central をハイ アベイラビリティ構成でセットアップする際のガイドラインを次に示します。

- クラスタの両方の VM が同じサーバに導入されていないことを確認します。 同じサーバに導入されていると、単一のホスト障害が原因でクラスタがダウンすることがあります。
- クラスタの各ノードは次のようになっている必要があります。
  - プライマリ NIC が、Cisco UCS Manager との通信とクラスタ内のピア ノードとのハートビート通信に使用される実稼働ネットワークに接続している。

- ホスト バス アダプタが、ストレージ ターゲットへアクセスするために使用されるストレージ エリア ネットワーク（SAN）に接続している。

- **管理およびストレージ ネットワークの個別のネットワーク パス**：2 つの Cisco UCS Central 間の通信に使用される管理ネットワークは、ノードが共有ディスク アレイにアクセスするために使用するネットワークと同一のネットワーク上にないことを確認してください。 プライマリ ハートビート メカニズムは、管理ネットワークでのデータグラムの交換を利用しています。 セカンダリ ハートビート メカニズムは、Cisco UCS Manager のクォーラム データを使用します。 管理および共有ディスク アクセスにそれぞれ異なるネットワーク パスを使用すると、2 つのノード間で冗長なパスが実現するため、ノード障害とリンク障害の区別が容易になります。

（注） ハイ アベイラビリティは、DHCP を使用しない IPv4 アドレッシングでのみサポートされます。 インストール時にノード IP とクラスタ VIP をスタティックに設定する必要があります。 これらの IP アドレスは、UCS Central クラスタが UCSM と通信する実稼働ネットワークから割り当てられます。

- 両方の VM を、同一サブネットに属する IP アドレスで設定する必要があります。
- クラスタ ノード インフラストラクチャに単一点障害がないことを確認します。 クラスタ ノードを複数の個別ネットワークに接続できます。 また、冗長スイッチおよびルータ、または単一点障害を排除する同様のハードウェアを使用してネットワークを構築できます。
- ハイ アベイラビリティに対応するため、Cisco UCS Central では最もよく利用されているバスタイプ（SAS、ファイバ チャネル（FC）、iSCSI など）がサポートされています。 永続的な予約（PR）と互換性のある SCSI が推奨されます。 クラスタがアクセスするストレージ ボリュームをネットワーク上の他のホストから切り離すときには、LUN マスキングまたはゾーン分割を使用する必要があります。

ログおよびエラー

登録済み Cisco UCS ドメイン とCisco UCS Central GUI からの Cisco UCS Central で、エラーをモニタおよび確認できます。

- **Cisco UCS Central エラー**：Cisco UCS Central は、すべての Cisco UCS Central システム エラーを収集し、[Logs] および [Faults] タブに表示します。 ここでエラーをモニタし、確認できます。 エラーの詳細情報が分類され、次のタブに表示されます。
  - [mgmt-controller]：管理コントローラ
  - [policy-mgr]：ポリシー マネージャ
  - [resource-mgr]：リソース マネージャ
  - [identifier-mgr]：ID マネージャ

- [operation-mgr]：オペレーション マネージャ
- [service-reg]：サービス レジストリ

  ローカル ユーザとリモート ユーザのアクティブ ユーザ セッションを表示、終了し、サーバ上の指定されたロケーションにあるコア ファイル、プロバイダの内部サービス、コントローラとサービス レジストリ、および登録済みドメインの分類リストを表示できます。

- [UCS Domain Faults]：Cisco UCS Central は、登録済み Cisco UCS ドメインからエラーを収集し、[UCS Faults] パネルの [Equipment] > [UCS Fault Summary] タブに表示します。 エラーは、タイプおよび重大度別に表示されます。 エラー タイプをクリックすると、そのエラーが発生した具体的な Cisco UCS ドメインが展開され、確認できます。 エラー タイプの特定の Cisco UCS ドメインを選択すると、[Work] ペインにそのエラー タイプの詳細が表示されます。 また、ここでは選択したドメインの Cisco UCS Manager GUI も開始できます。

（注）

Cisco UCS Central リリース 1.2 では、トップ レベルのサマリー パネルに Cisco UCS Central GUI での [UCS Central Fault Summary]、[UCS Domains Fault Summary]、および [Pending Activities] の概要が表示されます。

次の 3 つのオプションのいずれかをクリックすると、Cisco UCS Central GUIに関連するページが表示されます。

- [UCS Central Fault Summary]：[Logs and Faults] > [Faults] に移動し、Cisco UCS Central でのエラーが表示されます。
- [UCS Domains Fault Summary]：[Domains] > [UCS Fault Summary] パネルに移動し、登録済み Cisco UCS ドメインのエラーが表示されます。
- [Pending Activities]：[Servers] > [Pending Activities] に移動します。