Cisco UCS Central 運用ガイド

初版:2016 年 6 月 10 日

最終更新日:

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel : 408 526-4000
800 553-NETS (6387)
Fax : 408 527-0883

Text Part Number:

【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、米国シスコシステムズ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。

CONTENTS

はじめに

対象読者

このガイドは、次の 1 つ以上に責任を持つ、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	説明
GUI 要素	タブの見出し、領域名、フィールドのラベルのような GUI 要素は、[GUI 要素] のように示しています。 ウィンドウ、ダイアログボックス、ウィザードのタイトルのようなメイン タイトルは、[メイン タイトル] のように示しています。
マニュアルのタイトル	マニュアルのタイトルは、イタリック体(*italic*)で示しています。
TUI 要素	テキストベースのユーザ インターフェイスでは、システムによって表示されるテキストは、`courier` フォントで示しています。

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

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

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

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

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。

警告 安全上の重要な注意事項

「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

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

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

管理用の UCS Manager と統合されたラック サーバでサポートされるファームウェア バージョンとサポートされる UCS Manager バージョンについては、『Release Bundle Contents for Cisco UCS Software』を参照してください。

その他のマニュアル リソース

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

マニュアルに関するフィードバック

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

TAC の準備

Cisco TAC でのサポート ケースを必要とする問題について、`show tech-support` からの出力を提供する準備をします。

GUI からテクニカル サポート ファイルを生成するには、[System Tools] アイコンをクリックし、[Tech Support] を選択します。ドメインを選択して [Generate Tech Support] をクリックします。レポートを作成したら、[Download] をクリックしてローカル システムにダウンロードします。

CHAPTER 1

概要

概要

Cisco UCS Central は Cisco UCS の管理を簡素化します。単一の Cisco UCS ドメインから複数の Cisco UCS ドメインまで、Cisco UCS Central は標準化、集約、グローバル ポリシーの適用、およびグローバル ID の一貫性を提供します。

Cisco UCS Manager が単一の Cisco UCS ドメインに対してポリシー駆動型の管理を提供するのに対し、Cisco UCS Central はドメインのアクティビティをグローバルで管理および監視します。これらの機能は、世界中の複数の Cisco UCS Manager ドメインにわたり、より強力な管理パワー、運用効率、およびポリシー駆動型の自動化を提供します。

Cisco UCS Central は 10,000 台のサーバへのスケーリングと管理をサポートします。これはドメインのサイズに応じて、約 70 ～ 125 の Cisco UCS Manager ドメインを表します。シスコでは、200 以上の Cisco UCS ドメインと 6,000 以上のサービス プロファイルを持つ Cisco UCS Central を厳密にテストしました。

UCS Central のセットアップ アーキテクチャには柔軟性があります。登録済みの UCS ドメイン、およびこれらのドメインの数と地理的な分散を管理できます。さまざまなアーキテクチャ全体に適用される原則もあれば、特定のサイズにより関連した原則もあります。

Cisco UCS Central の導入時に、成長を計画し、UCS の展開の最終的な規模と範囲を予測することが重要です。少数の UCS ドメインから開始できた組織も、1 ～ 3 年の間に大幅に拡大することがあります。大幅な成長が見込めない場合でも、常に将来の管理のために構築および計画することが重要です。

また、環境がブラウンフィールドなのかグリーンフィールドなのかも考慮します。

ブラウンフィールド

ブラウンフィールド環境には、以前に構築され、Cisco UCS Manager を介して展開された UCS ドメインを含む Cisco UCS Central が含まれます。これらには、プール、ポリシー、VLAN、VSAN、テンプレート、および各 UCS ドメインのサービス プロファイルなどのローカライズされたオブジェクトが含まれます。ブラウンフィールド環境では、オブジェクトがローカルの場合、Cisco UCS Manager がそのオブジェクトを所有していることを意味するため、Cisco UCS Manager の管理者のみがオブジェクトを追加、変更、削除できます。

グリーンフィールド

グリーンフィールド環境には、Cisco UCS Central を通じて作成されたオブジェクトのみを含む Cisco UCS Central が含まれます。したがって、これらのオブジェクトはグローバル範囲です。Cisco UCS Central 管理者のみが Cisco UCS Central からこれらのオブジェクトを追加、変更、削除できます。Cisco UCS Manager 管理者はこれらを変更できません。Cisco UCS Central は、すべてのグローバル オブジェクトの読み書き所有権を維持します。

Cisco UCS Central からグローバル サービス プロファイルを UCS ドメイン内のブレード サーバに展開すると、グローバル サービス プロファイルのシャドウ コピーが Cisco UCS Manager に展開されます。Cisco UCS Manager では、[Server]、[LAN]、[SAN] の各タブに、グローバル ポリシー、VLAN、VSAN、vNIC/vHBA テンプレート、およびグローバル サービス プロファイルがグローバル アイコンと共に表示されます。これは、これらがグローバルであるため、Cisco UCS Central によって制御されていることを示しています。グローバル サービス プロファイル テンプレートは、Cisco UCS Manager にコピーされません。

Cisco UCS Central の使用事例

Cisco UCS Central には、あらゆる規模の UCS 環境への実装を正当化する多くの使用事例があります。Cisco UCS Central が存在する以前は、UCS ドメインの展開は繰り返しが多く、手作業によって時間がかかっていました。ID プール、ポリシー、VLAN、VSAN、テンプレート、サービス プロファイルの作成と一貫性には、厳密な注意が必要でした。

ID プールの設定は間違いやすくなっています。たとえば、同じ環境内の別の既存の UCS ドメインの正確な方式を使用して、MAC アドレス プールが設定できます。これにより MAC アドレスの競合が発生します。Cisco UCS Central は登録済みの UCS 環境全体のインベントリを作成し、このような衝突を排除します。

範囲

このガイドでは、さまざまな規模のクライアントの異なるアーキテクチャに関する考慮事項について説明します。

既存の UCS Central クライアント ベースの平均サイズに基づいて、環境を分類しました。また、登録済みドメインが 300 超、管理対象サーバが 6,000 超の最大規模の UCS Central 環境についてもいくつか検討しました。UCS Central の現行バージョンは、最大 10,000 の登録済みサーバを含む環境をサポートできることが確認されています。

このガイドでは、次のサイズ範囲を定義しています。

- 小規模環境:1 ～ 3 の登録済み UCS ドメイン
- 中規模環境:4 ～ 12 の登録済み UCS ドメイン
- 大規模環境:13 以上の登録済み UCS ドメイン

用語

用語	説明
Cisco UCS Manager	Cisco UCS ドメインを管理する Cisco UCS ファブリック インターコネクトに内蔵された ASIC ソフトウェア。
Cisco UCS ドメイン	ファブリック インターコネクトと次の接続されたシステムとのペアを含むリソースの集合: • 1–20 B シリーズ シャーシ • C シリーズ サーバ • UCS Mini • UCSM ドメイン
Cisco UCS Central	1 つ以上の Cisco UCS ドメインの管理を集約し簡素化する仮想アプライアンス。
ドメイン グループ	設定の類似性および多くの場合は地域に基づく、複数の Cisco UCS ドメインの名前付きグループ。ドメイン グループでは、Cisco UCS Central は、ドメイン グループの識別のため、運用ポリシー、サーバ ポリシー、VLAN、および VSAN を適用します。ドメイン グループ構成は、Cisco UCS Central 内にのみ存在し、適用されます。UCS ドメイン内ではドメイン グループの概念はありません。
サブドメイン グループ	ドメイン グループの子。親からプロパティを継承します。サブドメイン グループ内のドメイン用に固有のポリシーを設定できます。ドメイン グループの階層では、最大 5 つの入れ子のレベルがサポートされます。
グループ解除されたドメイン	どのドメイン グループにも属さないドメイン。Cisco UCS ドメインの登録では、Cisco UCS ドメインがドメイン グループ内に配置されるまで、運用ポリシーは継承されません。
ローカル	1 つの Cisco UCS Manager ドメインで所有され変更可能なオブジェクト(ローカル ポリシーやローカル プールなど)を指します。
グローバル	Cisco UCS Central で所有され変更可能なオブジェクト(グローバル サービス プロファイル、グローバル ポリシー、グローバル プールなど)を指します。
ローカライズ	グローバル オブジェクトのローカル コピーを作成します。これはローカル ドメインから変更可能で、Cisco UCS Central では読み取り専用になります。

用語	説明
グローバル化	プールまたはポリシーの参照をローカルからグローバルに変更します。たとえば、Cisco UCS Manager でグローバル アクションを使用してグローバル オブジェクトへの参照を作成します。グローバル オブジェクトが存在しない場合は、参照は満たされません。参照を満たすようにグローバル オブジェクトを作成します。グローバル オブジェクトが存在しない場合、参照は保留中のグルーバル状態のままとなります。
登録	Cisco UCS Manager ドメインが Cisco UCS Central に接続し、Cisco UCS Central から自身の管理を設定するまでの初期プロセス。
登録解除	Cisco UCS Central の管理から Cisco UCS ドメインの意図的な削除。恒久的に登録解除する場合を除き、これは推奨されません。
可視性の喪失	Cisco UCS Manager と Cisco UCS Central 間の接続の意図しない喪失。
一時停止状態	Cisco UCS Central と Cisco UCS Manager 間の管理通信を意図的に停止します。Cisco UCS Manager は Cisco UCS Central に登録されますが、この 2 つの間に管理通信はありません。これは意図しない変更を防止するセキュリティ機能です。 通常、予期しない状態が原因で Cisco UCS ドメインによって開始されます。たとえば、Cisco UCS Central が古いバージョンに復元された場合や、Cisco UCS ドメインが定期的なポリシー解決時に古いバージョンのポリシーを受け取った場合などです。
確認応答状態	Cisco UCS Central と Cisco UCS Manager 間の正常な状態。Cisco UCS Central と Cisco UCS Manager 間で管理通信が再確立されます。確認応答は、Admin-Cisco UCS Central の登録のペインの Cisco UCS Manager 内で発生します。

ドメイン、ポッド、クラスタ、またはブロック

1 ～ 20 個のシャーシを管理する Cisco UCS ファブリック インターコネクトには、ポッド、クラスタ、またはブロックの用語を使用せずに、ドメインを使用します。単一の Cisco UCS Manager のコンテキストでの特定の用語の過去の使用は、Cisco UCS Central の真にグローバルなコンテキストで再検討する必要がある場合があります。たとえば、Cisco UCS Manager 2.1 より前のバージョンでは、VLAN は単一の UCS ドメイン内でグローバル範囲と呼ばれていました。これは、A と B の両方のファブリックで作成され使用される VLAN とも呼ばれていました。共通名、用語、およびコンテキストを理解することが重要です。

所有権

通常、プール、ポリシー、サービス プロファイル、アダプタ、ブレード、シャーシなどの Cisco UCS の管理対象オブジェクト（MO）に関しては、ローカルおよびグローバルの用語を使用します。管理対象オブジェクトはローカル（特定の Cisco UCS ドメイン）またはグローバル（Cisco UCS Central）のいずれかで所有されます。ローカルで所有されているオブジェクトには、ローカル ドメインでの読み取り/書き込みアクセス権がありますが、Cisco UCS Central では読み取り専用アクセス権しかありません。

対して、グローバルで所有されているオブジェクトには、Cisco UCS Central での読み取り/書き込みアクセス権がありますが、任意のローカル ドメインでは読み取り専用アクセス権しかありません。Cisco UCS Central はグローバル オブジェクトを所有しますが、（ドメイン レベルで）ローカル コピーを直接変更しません。代わりに、Cisco UCS Central は、Cisco UCS Central 内のグローバル オブジェクトを更新し、XML-API に更新イベントを発行してそのグローバル オブジェクトのローカル シャドウ コピーを更新します。

ベスト プラクティスの用語

「ベスト プラクティス」という用語は、目的の機能を実行する唯一の方法を指定するのではなく、ガイドライン、推奨、および提案を定義することを意図しています。唯一の有効なベスト プラクティスは、適切なコンテキストとすべての例外条件を考慮して、ユーザの組織および運用要件にとって最適に機能するものすべてです。

柔軟性、適応性、および一貫性は、Cisco UCS Manager の特徴のすべてであり、Cisco UCS Central のアーキテクチャの目標として進展しています。Cisco UCS Central 管理モデルの影響は、スタンドアロンのローカル管理モデルとは大きく異なります。管理パワーは Cisco UCS Central 内に主に集中していて、変更の範囲は広範囲になる場合があります。予期しないサービスの中断は、推奨プラクティスに従わない結果である可能性があります。管理者には次のことが強く推奨されます。

- 実稼働環境への導入前に、できる限りモデル化とテストを行います。Cisco UCS Central インスタンスと登録済みの Cisco UCS エミュレータを使用したテスト環境を使用します。
- ローカル サービスに影響を与える可能性のあるグローバル コンフィギュレーションの変更は慎重に行います。
- アクションで **Estimate Impact** を実行し、潜在的な影響が把握されていることを確認します。パーソナル化を設定することで、ほとんどの適用可能なアクションで Estimate Impact を実行するように設定できます。
- サービス プロファイルのメンテナンス ポリシーと USER-ACK に設定されているサービス プロファイル テンプレートを使用します。

Cisco UCS Central は Cisco UCS Manager と統合され、Cisco UCS Manager を利用してそのアクションを実行します。Cisco UCS Central は、ポリシー定義を一元化し、複数の Cisco UCS ドメインを一貫した方法で利用できる、グローバル識別子のプールを作成するように設計されています。

Cisco UCS Central の機能が強化され、機能が追加されても、Cisco UCS Manager は Cisco UCS ドメインの直接管理のためのインターフェイス、およびグローバル ポリシーの適用の一貫性を確保するための手段であり続けます。

Cisco UCS Central ユーザ マニュアルのリファレンス

リリース 1.4 から、Cisco UCS Central のユーザ ガイドは、複数の使用事例ベースのドキュメントに分けられました。Cisco UCS Central を理解および設定するのに適切なガイドを使用できます。

ガイド	説明
Cisco UCS Central Getting Started Guide	Cisco UCS インフラストラクチャ、Cisco UCS Manager、および Cisco UCS Central について簡単に説明します。HTML5 UI の概要、Cisco UCS Central に Cisco UCS ドメインを登録する方法、およびライセンスをアクティブにする方法を説明します。
Cisco UCS Central Administration Guide	ユーザ管理、通信、ファームウェア管理、バックアップ管理、Smart Call Home などの管理タスクについて説明します。
Cisco UCS Central Authentication Guide	パスワード、ユーザ、ロール、RBAC、TACACS+、RADIUS、LDAP、SNMP などの認証タスクについて説明します。
Cisco UCS Central Server Management Guide	機器ポリシー、物理インベントリ、サービス プロファイルとテンプレート、サーバ プール、サーバのブート、サーバ ポリシーなどのサーバ管理について説明します。
Cisco UCS Central Storage Management Guide	ポートとポート チャネル、VSAN と vHBA の管理、ストレージ プール、ストレージ ポリシー、ストレージ プロファイル、ディスク グループ、ディスク グループ設定などのストレージ管理について説明します。
Cisco UCS Central Network Management Guide	ポートとポート チャネル、VLAN と vNIC の管理、ネットワーク プール、ネットワーク ポリシーなどのネットワーク管理について説明します。

CHAPTER 2

UCS Central の実装：アプローチと課題

実装の概要

シスコは、Cisco UCS Central が Cisco UCS 管理の中心となることを意図しています。既存の Cisco UCS ドメインがあるデータ センターの場合、実装によって将来的な拡張と管理の課題を最小限にします。

Cisco UCS Central には Cisco UCS Manager と共通する部分が多くありますが、独自の機能の習得には、時間をかける必要があります。

Cisco UCS の新規導入

Cisco UCS ドメインの新規導入のベスト プラクティスは、最初から（特に新しいワークロードに対して）Cisco UCS Central を導入し、グローバル プール、ポリシー、テンプレートを参照することです。

以前に Cisco UCS を設置していないインストールでは、ローカルに管理されているオブジェクトのインスタンスを回避するため、Cisco UCS Central のみを使用することが推奨されます。グローバル プールとポリシーを排他的に参照するグローバル サービス プロファイルは、グローバルな一貫性を保証することに役立ちます。

最初に Cisco UCS Central を使用すると、Cisco UCS の管理エクスペリエンスの大幅な簡素化と強化ができます。最初に Cisco UCS Central を使用していない環境では、ブラウンフィールド環境を展開しています。ブラウンフィールド環境を Cisco UCS Central に変更するのは困難です。しかし、十分に計画すれば、Cisco UCS Central への移行は実現できます。ブラウンフィールドとグリーンフィールドが混在する環境でも、すべての UCS ドメインを Cisco UCS Central に登録することは非常に大きな価値があります。

CHAPTER 3

小規模な Cisco UCS Central 環境

小規模な環境

小規模な Cisco UCS Central 環境は、1 ～ 3 の登録済み UCS ドメインで構成されます。この環境では、ルート ドメインの下で単一のドメイン グループを使用することを検討してください。これにより、将来ドメイン グループを追加することができます。これは、運用ポリシーの 1 つのセットがすべての登録済み UCS ドメインに公開されることも防止します。ただし、特定のポリシーはルート レベルに配置するのが適しています。たとえば組織に 1 つの LDAP リモート認証設定がある場合、これらの LDAP ポリシー設定をルート ドメイン グループに配置します。これによりできる限り広範囲な導入が保証されます。

（注） LDAP の設定をサブドメイン グループ ポリシーで誤って上書きしないようにします。

小規模なグリーンフィールドの展開

Cisco UCS Central を初めて実装する場合、Cisco UCS Central を使用して、仮想アーキテクチャ全体をグローバルで作成することを強く推奨します。統合された単一のマネージャからグローバル オブジェクトを管理すると、多くの利点があります。

- 一貫した運用ポリシーの作成と適用
- 登録済みのすべての UCS ドメインに対し、最大限のグローバル サービス プロファイル モビリティの実現
- できる限り少ない管理および運用のオーバーヘッドで、できる限り最高の実装の保証

たとえば、Cisco UCS Central ではすべてのグローバルおよびローカル プールの一覧を作成し、重複 ID または競合がある場合はそれらを表示します。また、それらの重複 ID のソースを簡単に識別します。

小規模なブラウンフィールドの展開

既存の展開済みの UCS ドメインを Cisco UCS Central に登録すると、Cisco UCS Central によって設計と運用のオプションが提示されます。しかし、既存のローカルの論理構成をグローバル オブジェクト変更するための妥当な理由がない場合があります。既存の設定をそのまま維持して、新しくグローバル コンフィギュレーションとして構築することができます。古いローカライズされたドメインのサポートが終了し、廃止される際に、それらをグローバル化した UCS ドメインに置き換えることができます。

逆に、グローバル コンフィギュレーションが必要な場合は、ローカル設定をミラー化したグローバル コンフィギュレーション全体を構築できます。将来のメンテナンスの時間帯を利用して、サーバの電源を安全にオフにし、既存のローカル サービス プロファイルを削除して、対応するグローバル サービス プロファイルと交換します。このシナリオを計画します。

実稼働環境に導入する前に、必ずラボでテストしてください。これは Cisco UCS Central をラボにインストールしてから、UCS エミュレータをダウンロード、インストールして、ラボに登録することで行えます。これにより、既存の実稼働構成をモデル化し、移行プロセスをテストすることができます。

ドメイン グループ構造

UCS に登録されている UCS ドメインの一部については、単純なドメイン グループ構造で十分です。これを分析する最良の方法は、[Cisco UCS Manager] > [Admin] タブ > [Communication Management] > [UCS Central] > [FSM] > [Policy Resolution Control] の順に選択して調べることです。表示されたポリシー（ローカルまたはグローバル）は、Cisco UCS Central ドメイン グループまたはサブドメイン グループで定義されている運用ポリシーです。リストについて調べる際に、アーキテクチャ全体のドメイン グループを作成するための最善の方法を分析して決定できます。リストにある運用ポリシーはすべて、Cisco UCS Central のドメイン グループ レベルまたはサブレベルで設定されたポリシーです。したがって、これらのポリシーをグローバルに制御したり、ルートから個別のサブドメイン グループまでの有効な階層を作成することができます。

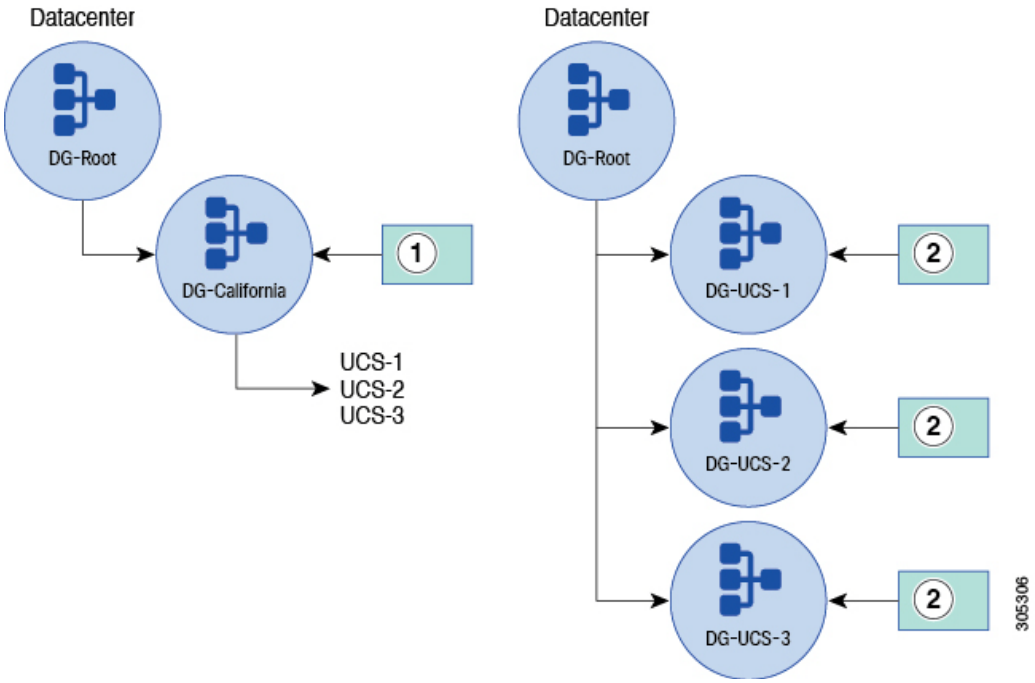
小規模な環境のための Infrastructure & Catalog Firmware

Infrastructure & Catalog Firmware は、ドメイン グループの階層に影響を与える可能性があります。グローバル制御を選択し、だれかがそれを変更すると、そのドメイン グループに登録されているすべての UCS ドメイン（FI）でユーザの確認応答が生成されます。これは、そうした UCS ドメインのアップグレードを促します。これは破壊的ではありませんが、多くのユーザはすぐにアップグレードする準備ができている場合を除き、UCS ドメインの確認応答アクションを行いたくありません。また、複数の UCS ドメインを一度に表示したくないとも考えています。したがって、自由裁量で以下を考慮します。

- 各 UCS ドメインを独自のサブドメイン グループに配置してセグメント化します。
- 単一の UCS ドメインのみが確認応答またはアップグレードを保留にするように、最下位のサブドメイン グループでドメイン グループ ポリシーを定義します。

もう 1 つのオプションは、運用ポリシーを Cisco UCS Manager 内でローカルとして定義してから、アップグレード時に各ドメインをグローバルに変更することです。この方法は、Cisco UCS Central ファームウェアのダウンロードと制御のメリットを活用していますが、一度に 1 つの UCS ドメインのみに影響します。残りのすべての運用ポリシーを階層の上位で個別に設定することもできます。これにより、管理する必要があるポリシーの数が減ります。

図 1 : Infrastructure & Catalog Firmware : 設定例



1	データセンター。グローバル ポリシーはここにあります
2	Infrastructure & Catalog Firmware。グローバル ポリシーもここに存在できます

小規模環境のタイム ゾーン管理

登録時にこのポリシーを Cisco UCS Central に含めることをお勧めします。UCS ドメインが同じタイム ゾーンにある場合は特に、このポリシーをドメイン グループの階層の上位に配置します。一部のクライアントは、同じ NTP サーバ ソースをポイントしますが、各 UCS ドメインに異なるタイム ゾーンが設定されている必要があります。この場合、別のドメイン グループまたはサブドメイン グループを使用して、変更を説明することができます。それとは関係なく、Cisco UCS Central で適切なタイム ゾーンと NTP サーバ設定を定義して、アーキテクチャ内の時刻とタイム ゾーンの一貫性と正確性を保証できるようにします。

小規模環境向けの通信サービス

グローバル ポリシー管理を使用して次の通信サービスを管理することが理想的です。

- 通信サービス（SNMP 設定など）
- グローバル障害ポリシー
- ユーザ管理（LDAP 設定など）
- DNS 管理

- モニタリング（Call Home や Syslog 設定など）
- SEL ポリシー
- 電源割り当てポリシー（手動のブレードまたはシャーシ上限）
- 電源ポリシー（N+1、またはグリッドなど）

グローバル管理は、Cisco UCS Central で一度ポリシーを正しく設定することができます。すると、登録済みの UCS ドメインすべてにそのポリシーが適用されます。

（注） Cisco UCS Central は、SNMP などのポリシーの設定を管理します。UCS ドメインはリソース マネージャから設定されたトラップ マネージャまたは宛先に直接 SNMP トラップを送信します。

小規模環境向けのバックアップおよびエクスポート ポリシー

Cisco UCS Central は、登録された UCS ドメインに対する適切なバックアップのスケジュールと維持に役立ちます。管理者は、UCS ドメインのバックアップが都合のよい日時に行われるように、カスタム スケジュールを作成できます。これは、Cisco UCS Manager 内でネイティブに提供可能なものよりも高い柔軟性を提供します。

Cisco UCS Central によって管理されるバックアップのもう 1 つの特徴は、リモート コピーのオフライン機能を利用できることです。これにより、バックアップ ファイルをローカル サーバからコピーし、リモート サーバに保存して、ファイルの安全を確保します。ベスト プラクティスは、UCS ドメインごとに毎日のバックアップを作成することです。

UCS ドメインをバックアップして、そのバックアップ ファイルをリモート データベースに保存するように Cisco UCS Central を設定します。後続のバックアップでファイルが上書きされる前に、保持するバックアップ ファイルの数（通常は 3 ～ 5 コピー）を定義できます。これにより、Cisco UCS Central データベースとディスク内で使用される空き容量を制限して、無制限に増加することを防止できます。

グローバル機器ポリシー

グローバル機器ポリシーは、Cisco UCS Central で以下を制御できるようにする新機能です。

- シャーシ ディスカバリ ポリシー
- ラック管理アクション
- MAC アドレス テーブルのエージングタイム
- VLAN ポートの最適化
- ファームウェア自動同期サーバ状態

CHAPTER 4

中規模の Cisco UCS Central 環境

グリーンフィールド環境

グリーンフィールド環境では、Cisco UCS Central 管理者のみが Cisco UCS Central からオブジェクトの追加、変更、削除ができます。Cisco UCS Central は、すべてのグローバル オブジェクトの読み書き所有権を維持します。Cisco UCS Central からグローバル サービス プロファイルを UCS ドメイン内のブレード サーバに展開すると、グローバル サービス プロファイルのシャドウ コピーが Cisco UCS Manager に展開されます。Cisco UCS Manager には、グローバル アイコンとともにオブジェクトが表示されます。このアイコンは、オブジェクトがグローバルであるため、Cisco UCS Central によって制御されていることを示します。グローバル サービス プロファイル テンプレートは、Cisco UCS Manager にコピーされません。

グリーンフィールド環境での論理ドメイン グループと組織階層の設定

中規模のグリーンフィールドの展開では、初期設定時に、論理ドメイン グループと組織階層を正しく作成および設定する必要があります。複数の階層レベルで展開済みの UCS ドメイン間の運用ポリシーのさまざまな要件に対応することを検討してください。

ファームウェアの検討事項に加えて、リモートコピー先が異なる可能性の高い、異なるタイムゾーンでスケジュールされた UCS バックアップが必要になることがあります。また、組織および地理的分散に基づくさまざまなユーザ認証の設定がある場合があります。

UUID のグローバル ID プール、MAC アドレス、WWNN、WWPN、および管理 IP を作成することで、将来の成長を計画することが賢明です。ID タイプごとに 1 つのグローバル プールを利用できます。その後、スケールアウトのためにそれぞれのプールに ID のブロックを追加できます。通常、全体のプール数を少なくして、ブロック サイズを小さくした方が、内部 DB にはより効率的です。成長とスケールを実現するために ID のブロックを追加できます。

MAC プールの設定

一部のクライアントは 1 つのプールを使用するよりも、MAC プールをセグメント化する方を好みます。ネットワーク管理者がどのファブリックに特定の MAC アドレスが割り当てられているかを確認する必要がある場合に、セグメンテーションは役立ちます。ただし、すべての UCS 展開のベスト プラクティスでは、VPC または VSS よりも、クラスタ化されたスイッチ テクノロジーへの FI イーサネット アップリンクを推奨しています。その結果、2 つのファブリックからの MAC アドレスがメッシュされます。

WWPN の設定

通常、管理者はファブリック A とファブリック B に 2 つの個別のプールを作成します。管理者はいずれかのフィールドを WWPN 形式で使用して、ファブリック A とファブリック B を定義します。これにより、WWPN ID が属しているファブリックで各 ID を簡単に識別できるようになり、SAN 管理者にメリットをもたらします。これは、ほとんどの SAN ファブリックが各 SAN ファブリック スイッチ内で別々に保持されているためです。各ファブリック識別子により、SAN 管理者は、ファブリック スイッチにクロスファイバの問題があるかどうかをすばやく判断することができます。

ブラウンフィールド環境

ブラウンフィールド環境では、オブジェクトがローカルの場合、Cisco UCS Manager がそのオブジェクトを所有していることを意味し、Cisco UCS Manager の管理者のみがオブジェクトを追加、変更、削除できます。実際には、Cisco UCS Manager は読み取り/書き込みの制御ができます。

ブラウンフィールドからグリーンフィールドへの変換

Cisco UCS Central で管理されている中規模の UCS の展開は、Cisco UCS Central がない環境に比べてよりはるかに管理が容易です。中規模のブラウンフィールドの展開は、すべてのオブジェクトをグローバル インフラストラクチャに変換するとはるかに扱いやすくなります。

ブラウンフィールド環境をグリーンフィールドに、必要に応じてすばやくまたはゆっくり適応させることができます。最初に既存の UCS ドメインを Cisco UCS Central に登録するか、グローバル インフラストラクチャをゆっくりと定義して構築することができます。ローカル ドメインに存在するものをミラーするか、ポリシーとプールに必要な変更を行うことができます。この変換は急いで行う必要はありません。組織にとって適しているものを計画して構築することもできます。また、実稼働中の UCS ドメインにグローバル インフラストラクチャを展開する前に、Cisco UCS Central エミュレータを使用してラボで設定をテストできます。

重複プールを持つことができます。1 つは UCS ドメイン内でローカルで一意に定義されたプールと、それに対応する Cisco UCS Central 内で定義されたグローバル プールです。Cisco UCS Central は、ローカルとグローバルのすべてのプール内の各 ID の状態を追跡します。ID は複数のプール定義に存在できますが、Cisco UCS Central が UCS ドメインに重複 ID を発行することはありません。

UCS ドメインの最終的な移行は、ドメインごとに行うことができます。これによりブレード サーバを安全にシャット ダウンし、ローカル サービス プロファイルを削除してから、それらを対応するグローバル サービス プロファイルと置き換えることができます。このプロセスは明確に定義されています。最小限のリスクで変換を計画し、テストし、正常に実行することがきます。

中規模の UCS Central 環境のドメイン グループの階層

中規模の Cisco UCS Central 環境は、4 ～ 12 の登録済み UCS ドメインで構成されます。登録済みドメインが 12 の場合は、大規模になる場合があります。グローバル VLAN、VSAN、vNIC、vHBA テンプレート、LAN、SAN 接続ポリシー、対応するグローバル サービス プロファイル テンプレート、およびグローバル サービス プロファイルの数が重要です。環境には以下を含めることができます（概算）。

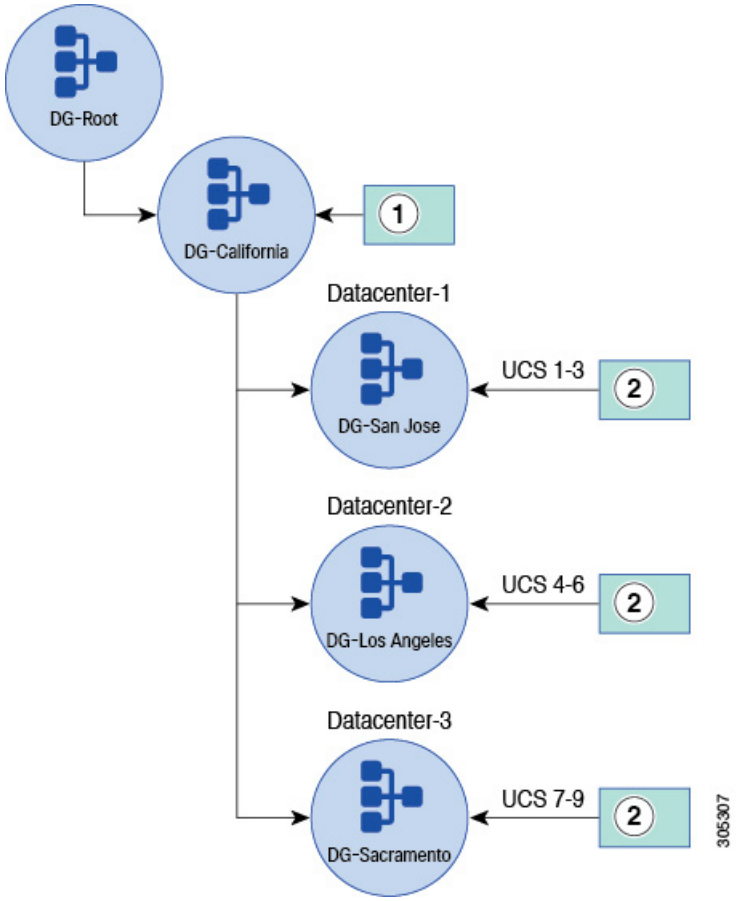
- 768 台以上のサーバ（12 ドメイン x 8 シャーシ x 8 ブレード）。最大で（12 ドメイン x 20 シャーシ x 8 ブレード）
- 1,920 台の B シリーズ ブレード
- 複数のマネージャの C シリーズ サーバ

会社の成長に合わせて環境を適応させることができるように、大きなドメイン グループの階層を使用することを検討してください。12 もの UCS ドメインがある場合、ドメインが異なる地理的領域にある可能性があります。そのため、ドメイン グループ構造がそれを反映しているのが最善です。Cisco UCS Central ドメイン グループ構造の構築に重要な影響を及ぼすことの 1 つは、登録済みの UCS ドメインの地理的位置です。タイム ゾーン、ユーザ認証設定、バックアップ、およびファームウェアなどのグローバル運用ポリシーは、地域に基づいてドメイン グループを作成する場合に最も効果的です。

たとえば、UCS ドメインが地理的に分散している場合、リモート コピー機能はこれらのバックアップを UCS ドメインの近くにある FTP サーバにコピーする必要があります。これにより、これらのバックアップを特にデータ回復（DR）シナリオで利用できるようになります。そのため、ニューヨークの FTP サーバから、サンノゼの FI ペアをターゲットとする DR の復元を行いたいとは思わないでしょう。Cisco UCS Central ドメイン グループ ポリシーを使用すると、FTP サーバのリモート コピーは、UCS ドメインの適切なバックアップを近距離に維持できます。

（注） 一部の組織は、マルチテナント機能をサポートするため、ビジネス グループごとにドメイン グループを分離しています。

図 2 : 中規模の UCS Central 環境 : 設定例



1	グローバル ポリシーはここに存在できます。Cisco UCS Central はそれらをサブドメインにプッシュできます。
2	Infrastructure & Catalog Firmware、バックアップおよびエクスポート、ユーザ管理、および DNS 管理などのポリシーは、ここに存在できます。

中規模環境向けの VLAN

Cisco UCS Central でグローバル VLAN を作成するときに、VLAN が属するドメイン グループを定義します。階層は、最上位（ルート）でも、下位のサブドメイン グループでもかまいません。グローバル VLAN にドメイン グループをアタッチすると、VLAN ID エイリアシングと呼ばれるオプション機能がサポートされます。この機能により、共通名を別のドメイン グループおよび ID と共有する複数のグローバル VLAN を作成することができます。グローバル サービス プロファイルは、VLAN 名のみを参照します。VLAN ID は、特定のドメイン グループで UCS ドメインに関連付けられているときにのみ設定されます。このプロセスはスティッキーバインディングと呼ばれます。VLAN ID エイリアシングを使用すると、必要なサービス プロファイル テンプレートの総数を減らすことができます。すべての面を考慮し、業務のニーズに最も最適なモデルとドメイン グループの構造を導入します。

同じエイリアシングの概念が、VSAN に適用されます。詳細については、このマニュアルの後述のセクション「VLAN と VSAN ID のエイリアシング」を参照してください。

特定の ID を、プールから特定のグローバル サービス プロファイルに誘導できます。ID アクセス コントロール ポリシーを使用して、ID を特定のブロックからドメイン グループまたはサブドメイン グループ階層内の特定の UCS ドメインに割り当てます。この使用事例は、管理 IP をグローバル サービス プロファイル内の KVM に割り当てることです。

VLAN および VSAN ID エイリアシングと ID アクセス コントロール ポリシーを使用して、インフラストラクチャの管理タスクのいくつかを合理化します。これら 2 つの機能は、インフラストラクチャで管理する必要があるテンプレートの総数を減らすことができます。しかしこれらは、異なるネットワークおよびファブリック セグメントの異なるブレード サーバを管理するために必要な一意性を提供します。目標が管理対象オブジェクトの数を削減するか、またはグローバル サービス プロファイル ワークロード モビリティの向上を実現するかに関わらず、これらの機能は、大切な資産となり得ます。

詳細については、「ID 範囲アクセス コントロール ポリシー」を参照してください。

中規模環境の運用ポリシー

ドメイン グループの階層は、運用ポリシーに影響します。UCS では、組織単位がマルチテナントに影響を及ぼし、ID プール、ポリシー、VLAN、VSAN、テンプレート、およびサービス プロファイルにアクセスします。組織の権限は、Cisco UCS Manager でローカルに定義された VLAN ではオプションですが、Cisco UCS Central のグローバル VLAN では必須です。単一の組織の権限をルートとして定義して、組織全体に特定の VLAN へのアクセスを効果的に提供できます。また、セキュリティ上の理由から、下位組織に特定の VLAN のみのアクセスを許可するなど、組織の権限をより詳細に定義することもできます。

中規模環境のための Infrastructure & Catalog Firmware

Infrastructure & Catalog Firmware に対しては、通常、規模に基づいて、UCS ドメインの個々のドメイン グループを構築しません。

（注） Cisco UCS Central Release 1.5 では、ドメイン グループではなく、メンテナンス グループごとにファームウェアを更新します。メンテナンス グループには、選択したドメインが含まれています。

更新する UCS ドメインでユーザの確認応答を求めるように定義できます。この潜在的に破壊的なポリシーは、ドメイン グループの階層の下位に配置することを検討してください。これを登録済みのいくつかの UCS ドメインとともにサブドメイン グループに配置して、登録済みの UCS ドメインで必要とするユーザの確認応答の数を最小限に抑えることができます。

各 UCS ドメインに対し、Infrastructure & Catalog Firmware の運用ポリシーが Cisco UCS Manager 内でローカルに設定されていることを確認します。メンテナンス グループをアップグレードする際に、グローバル ポリシーを結合します。これにより、その UCS ドメインまたはメンテナンス グループで求められるユーザの確認応答を 1 回にすることができます。これはグローバル ファームウェアの管理の問題を解決するための合理的で効率的な方法です。これはグローバル管理の利点を活用しながら、登録済みの UCS ドメイン内で、個々のオプトイン ポリシーの安全性を維持します。

重要 UCS ドメインがそのグローバル ポリシーにオプトインされていない限り、UCS ドメインにグローバル ポリシーは適用されません。例外は、UCS ドメインがドメイン グループ（またはメンテナンス グループ）に属している場合、設定済みのポリシーが設定されている場合、およびポリシー解決コントロールが Cisco UCS Manager 内でグローバルに設定されている場合です。

中規模環境のタイム ゾーン管理

タイム ゾーン管理は、より大規模で地理的に分散した多くの登録済みドメインを管理する場合により深く関わってきます。このドメイン グループの運用ポリシーをドメイン グループの階層のできる限り上位に配置します。これにより、このポリシーの作成および維持にかかる時間が短縮されます。

1 つのタイム ゾーンに収まっている組織は、このポリシーを一度、最も高いレベルで設定できます。複数のタイム ゾーンにまたがる組織は、異なるタイム ゾーンの UCS ドメインに対応するサブドメイン グループ ポリシーを作成する必要があります。

CHAPTER 5

大規模な Cisco UCS Central 環境

大規模な環境に対する UCS Central の利点

UCS の大規模な展開には、Cisco UCS Central が必要です。シスコには、300 以上の登録済み UCS ドメインと 6,000 台以上のサーバがあります。シスコ IT による社内分析では、Cisco UCS Central を利用することで、運用機器のワークロードを約 1 人/年節約できることが示されました。シスコは、Cisco UCS Central を使用して、すべての UCS ドメインを管理します。

シスコでは、1 つのインスタンスで最大 10,000 台のサーバをサポートするために、Cisco UCS Central の最新リリースをテストしました。このタイプのスケーリングのため、HTML-5 のユーザ インターフェイス（UI）が全面的に再設計されました。HTML-5 UI は、スケーリング時の UCS ドメインとサーバの管理により適した設計になりました。古い Flash ベースの UI は、大規模な環境で使用すると、パフォーマンスの問題がありました。

大規模な展開では、効率的なドメイン グループの階層を利用することが重要です。大規模な環境には、国中または世界中に分散したすべての UCS ドメインを含めることができます。ドメイン グループには、異なるタイム ゾーン、DNS サーバ、ユーザ認証、ドメイン コントローラ、リモート FTP サーバが含まれる場合があります。効率的なドメイン グループの階層により、ファームウェアのアップグレードと管理によりきめ細かいアプローチが可能になります。

多くの UCS ドメインのバックアップ ジョブのスケジュールを個別に管理することは、面倒でミスも生じやすくなります。Cisco UCS Central を使用することで、このタスクが簡素化されます。バックアップ（`fullstate.bin`）、構成のエクスポート（`allconfig.xml`）、および特定のリモート コピー FTP サーバにカスタム スケジュールを定義して、これらのバックアップが適切に保護されるようにします。

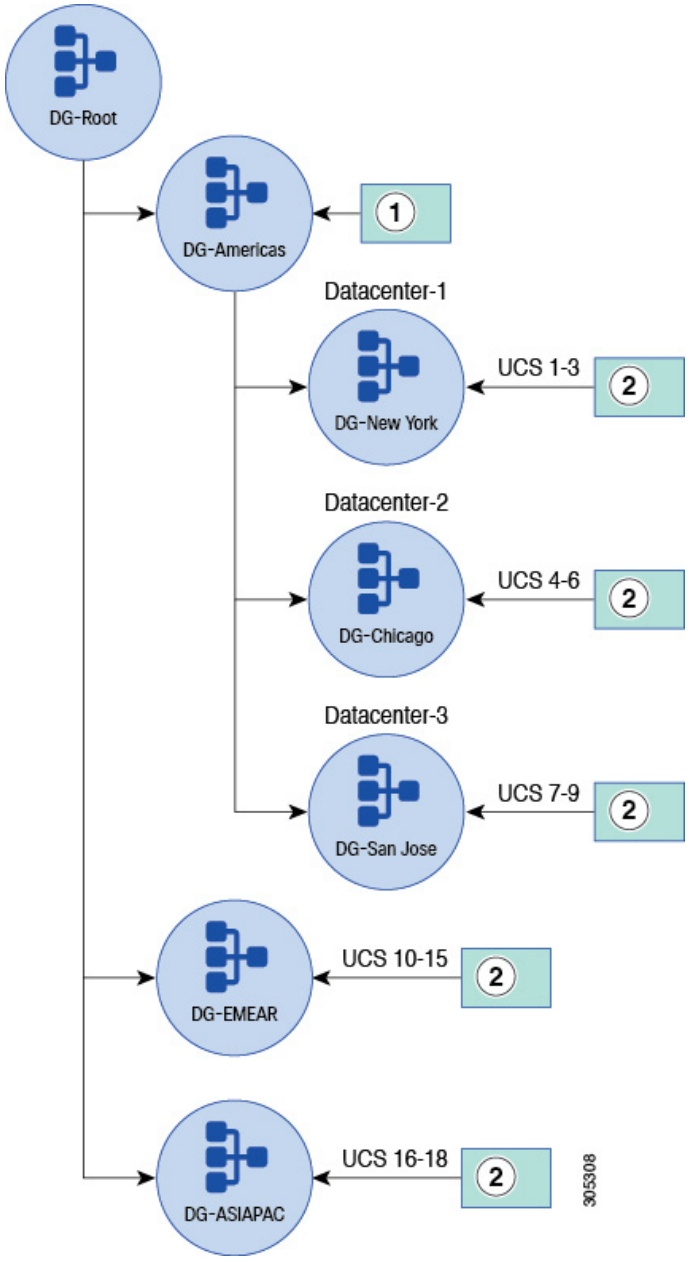
内部の LDAP サーバで UCS ドメインの LDAP 連携を使用している場合、これらの詳細な設定を複製することも、面倒でミスが生じやすくなります。Cisco UCS Central はこのタスクを非常に簡単にします。これは、ドメイン グループの階層型ポリシーの一部として LDAP を設定します。必要に応じて、幅広くまたは詳細にポリシーを定義できます。

（注） Cisco UCS Central は、単一のポリシーとして LDAP ポリシーを扱います。階層のあるレベルでグループ マッピングを定義し、より下位のレベルで LDAP プロバイダーを定義するなど、ポリシーのさまざまなコンポーネントを分解することはできません。

ポリシーは、地理的なドメイン グループに登録されている UCS ドメイン グループに適用可能なドメイン グループの階層の上位に配置できます。また、Infrastructure & Catalog Firmware をより詳細な下位のサブドメイン グループ構造に配置することもできます。

最終的に、自分と組織にとって最適な設定がベスト プラクティスとなります。常にシンプルなアプローチを選択し、サブドメイン グループ構造を変更または拡張できます。ドメイン グループ構造の変更は、組織の構造を変更するよりも容易です。組織構造の変更は、環境の破壊をもたらす変更になる傾向があります。

図 3 : 大規模な UCS Central 環境 : 設定例



1	グローバル ポリシーはここに存在できます。Cisco UCS Central はそれらをサブドメインにプッシュできます。
2	Infrastructure & Catalog Firmware、バックアップおよびエクスポート、ユーザ管理、DNS 管理、タイム ゾーン、および SEL などのポリシーは、ここに存在できます。

大規模環境におけるグリーンフィールド環境

大規模な計画されたグリーンフィールドの展開には、最初から Cisco UCS Central を導入し、グローバル ポリシーとオブジェクト インフラストラクチャを適切に設計することが推奨されます。Cisco UCS Central 内ですべてをグローバルに作成することで、時間とコストが節約でき、スケーリングがはるかに容易になります。また、日常業務を管理するときの時間も節約できます。

Cisco UCS Central は UCS ドメインの初期セットアップでの Cisco UCS Central と Cisco UCS Manager との間に存在するギャップを埋めるものです。Cisco UCS Central に、機器ポリシー、ユニファイド ポートの設定、ポート ロール、およびポート チャネル設定の機能が含まれるようになりました。

ドメイン グループの階層の計画に加えて、組織の階層を考慮してから、最終的なアーキテクチャを展開します。これにはグローバル ID プール、ポリシー、VLAN、VSAN、テンプレート、およびサービス プロファイルの計画が含まれます。インテリジェントに組織の境界を作成する機能は、マルチテナントにメリットをもたらし、環境に必要なグローバル サービス プロファイル テンプレートの数も削減できる場合があります。

VLAN および VSAN エイリアシング、ID 範囲アクセス コントロール ポリシーなどのその他の高度な機能も、管理するグローバル サービス プロファイル テンプレートの数の削減をサポートします。いくつでも必要なだけ管理することができますが、管理をシンプルにすれば運用コストも削減されます。

大規模環境におけるブラウンフィールド環境

Cisco UCS Manager と Cisco UCS Central の大規模なアーキテクチャには、数百または数千のサービス プロファイルが含まれている場合があります。そのため、UCS Central の移行には、慎重な計画と計算が必要です。オブジェクト リポジトリを Cisco UCS Central に移行して、ローカル サービス プロファイルをグローバル サービス プロファイルに変換する場合には注意を払います。グローバル インフラストラクチャを構築して、すべての UCS ドメイン内のローカル インフラストラクチャをミラーします。

ローカル サービス プロファイルをグローバル サービス プロファイルに変換するのは破壊的であることを思い出してください。しかし、1 つのインターフェイスですべてをグローバルに管理して、複数の UCS ドメイン間でワークロードのモビリティが得られる利便性は、欠点を補って余りあります。

大規模なブラウンフィールドのクライアントの中には、オブジェクト リポジトリを移動し、ローカル サービス プロファイルを時間をかけてゆっくりと変換することを選択するところもあります。これは将来のメンテナンスの時間帯を利用して、順番に Cisco UCS Central に移行します。ホスト ファームウェア、コントローラ ファームウェア、BIOS、ネットワーク アダプタ、CIMC、およびストレージ コントローラをアップグレードすることは、すべて破壊的な操作です。ホストには、安全にシャット ダウンして、アップグレードを実行するブレード サーバにサービス プロファイルを登録するためのメンテナンスの時間帯が必要です。この間に、既存のローカル サービス プロファイルを新しいグローバル サービス プロファイルと置き換えることができます。

その他のブラウンフィールドのクライアントは、ブラウンフィールド環境とグリーンフィールド環境を並行して運用するモデルを採用しています。これは、既存の UCS インフラストラクチャがブラウンフィールドとして残っていることを意味します。これは Cisco UCS Manager ドメイン内でローカルに管理され、一方で環境内の新しいものはすべて Cisco UCS Central からグローバル オブジェクトとして展開されます。

ネットワークが進化し、ローカル インフラストラクチャがサポート終了に達したら、環境のさらに多くのものをグローバルに変換します。ローカル サービス プロファイルを保持する場合でも、サービス プロファイルまたはテンプレート内でローカルからグローバルに切り替えることで、グローバル サービス プロファイルを使用します。これにより、ポリシーの数が減り、Cisco UCS Central 内の 1 つの場所からサービスが提供されます。「ブラウンフィールド：ローカル サービス プロファイルを使用したグローバル ID およびポリシーへのアクセス」を参照してください。

Powertools の自動化と XML-API のスクリプトにより、変換処理が非常に簡単になります。「Cisco UCS Central でブラウンフィールドのローカル サービス プロファイルをグローバル サービス プロファイルへ移行する」を参照してください。

CHAPTER 6

サイジングとスケーリングに関する考慮事項

サイジングに関する考慮事項

Cisco UCS Central の一部のお客様は、自身の UCS 環境を数十から数百のドメインに、数百から数千のサーバに拡張しています。ニーズを判断するためのスケーリング メトリックは、登録済みの UCS ドメインの数よりも、ブレードとサーバの数です。Cisco UCS Central では、最大 10,000 台のサーバをサポートできることが確認されています。ソフトウェアの制限はありません。

大規模な環境の場合は、Cisco UCS Central の仮想マシン（VM）のパフォーマンスを分析して、CPU やメモリ リソースを増やす必要があるかどうかを判断します。

『*Cisco UCS Central Installation Guide*』では、Cisco UCS Central を実行するための最小要件が定義されています。OVA ファイルの展開:

- 2 x 40 GB ディスクの作成
- 4 x vCPU の割り当て
- 12 GB RAM の割り当て

小規模から中規模の環境の場合、これらの設定で十分なパフォーマンスが得られます。しかし、大規模な環境では、これらのリソースを 2 倍に増やすことを推奨します。（シスコ IT では、200 以上の UCS ドメインと 6,000 台以上のサーバの Cisco UCS Central のインスタンスに対し、少なくとも 4 個の vCPU と 24 GB RAM を実行しています）。

ベスト プラクティスは次のとおりです。

1. 新規または拡大するインフラストラクチャで、Cisco UCS Central VM のパフォーマンス メトリクスをモニタします。
2. それに応じて CPU と RAM のリソースを調整します。
3. パフォーマンスが著しく低下している場合は、vCPU とメモリの使用率を確認します。
4. 仮想化管理者と必要な変更を行います。

グローバル サービス プロファイルとグローバル サービス プロファイル テンプレートのスケーリング

グローバル サービス テンプレートにアタッチできるグローバル サービス プロファイルの数に制限はありません。

テンプレートを利用して広範な変更を行うと、管理の簡素化に有益ですが、必ずしもすべての環境に最適なわけではありません。環境への破壊的な変更の影響を考慮します。更新するグローバル サービス プロファイル テンプレートに安全にアタッチできるリソースの量を決定します。1 つの間違いが深刻な停止を引き起こす可能性があります。障害の可能性を減らすことを検討します。たとえば、各サービス プロファイル テンプレートにアタッチされた 100 のグローバル サービス プロファイルの比率が最大限度であると判断することができます。

もう 1 つの重要な考慮事項は、ポリシーの数です。たとえば、100 のグローバル サービス プロファイルがアタッチされた 10 のグローバル サービス プロファイル テンプレートがある場合、それは 1,000 台のブレードまたはサーバを表します。10 のテンプレートすべてが同じ破壊的なポリシーにアクセスしている場合、1,000 台のブレードまたはサーバを中断させる可能性がある 1 つのポリシーがあることになります。障害の可能性を減らすには、複数のサービス プロファイル テンプレートと複数のポリシーにわたって拡張するのが最適です。同じ設定を持つが、異なるテンプレートで使用される複数のポリシーを持つこともできます。

少数のテンプレートに対して多すぎるグローバル サービス プロファイルがアタッチされている場合、グローバル サービス プロファイル テンプレートのクローンを作成できます。そして元のテンプレートからいくつかのプロファイルをアンバインドして、それらをクローンにバインドします。システムは、設計および運用に柔軟に対応します。それに応じてバランスを取り、拡張できます。

（注） 実稼働環境に展開する前に、このシナリオをテストすることをお勧めします。

このガイドは、管理を容易にするためにグローバル サービス プロファイル テンプレートの数を減らすことについて説明していますが、テンプレートに多数のグローバル サービス プロファイルをアタッチしないでください。また、1 つのポリシーを多数のグローバル サービス プロファイル テンプレートおよびプロファイルに使用しないでください。これは矛盾しているように聞こえますが、過剰なサービス プロファイルがテンプレートやポリシーにアクセスすることで起こる可能性のある広範囲の損害と、運用コスト（OpEx）改善するためにテンプレートを削減することとのバランスを取ることを検討してください。

CHAPTER 7

ドメイン グループ

ドメイン グループの設計

ドメイン グループの階層設計は、重要なアーキテクチャ設計の決定事項の 1 つです。正しい方法も間違っている方法もありません。目標は特定の環境や管理の設計要件を最適に反映することです。ドメイン グループについて、次の属性を理解する必要があります。

- ドメイン グループは、個別の Cisco UCS ドメインを無作為にグループ化したものです。Cisco UCS Central 管理者がグループ化を設計します。ドメイン グループは、純粋に Cisco UCS Central のグローバル構成です。ドメインは、ドメイン グループのメンバであることを認識していません。
- 1 つのサーバが複数のサーバ プールに存在できるサーバ プールとは異なり、Cisco UCS ドメインは、一度に 1 つのドメイン グループにしか存在できません。
- Cisco UCS Central は登録時に**グループ解除された**ドメイン グループ内にすべてのドメインを配置します。グループ解除されたドメイン グループ内のドメインは、ローカルの Cisco UCS 管理者がグローバル ポリシー解決コントロールを選択している場合でも、いずれのグローバル運用ポリシーを解決**しません**。
- ドメイン グループ内のすべてのドメインに適用するす運用ポリシー。これらはドメイン グループで解決および適用されます。
- ドメイン グループ間で Cisco UCS ドメインを移動できます。ただし、いずれのドメイン グループ間の移動も、移動先のドメイン グループのポリシーによっては、破壊的なものになる場合があります。Cisco UCS ドメイン グループは、自身が存在するドメイン グループから自身のポリシーを解決します。新しいドメインがドメイン グループに参加すると、サービスに影響を与える可能性のある新しいグローバル運用ポリシーが適用されます。
- グローバル ファームウェア管理を考慮する場合には、その影響を評価します。複数の登録済みの Cisco UCS ドメインがそのファームウェアのポリシー定義の影響を受ける可能性があることを認識します。同時に、そのファームウェア ポリシーの任意の変更やアップグレードの影響も受ける可能性があります。

- 新規に登録されたドメインは、認定ポリシーに基づいて登録時に自動的にドメイン グループに参加できます。ドメイン グループのポリシー認定は、サーバ プールのポリシー認定と同じように動作します。
- グローバル運用ポリシーは、ドメイン グループ階層内の任意の場所に配置でき、下位のドメイン グループでポリシーを設定することで、上位で設定されているポリシーをオーバーライドします。
- 管理者がドメインを新しいドメイン グループに移動する際に、古いドメイン グループのポリシーを削除する必要はありません。代わりに、新しいポリシーによって以前のポリシーが上書きされるまで、古いポリシーはそのまま残ります。

  例:UCS ドメインのバックアップ ポリシーがあると仮定します。古いポリシーはバックアップ スケジュールを定義し、新しいポリシーはこのポリシーを省略します。UCS バックアップは、古いスケジュールに基づいて行われます。新しいドメイン グループに新しいポリシーを作成すると、これらが変更されます。

  ポリシーが新しいドメイン グループに存在しない場合、参照を削除することでこれらのポリシーが解決されます。
- サブドメインを使用する度合いと、さまざまなサブドメインを管理するために必要な管理の量を比較検討します。
- ポリシーをより細かく制御するため、階層の最大 5 つのレベルまでサブドメイン グループをネストすることができます。

ドメイン グループのパーティション分割

ドメイン グループのパーティション分割にはいくつかの理由があります。

- 地理(大陸とタイム ゾーン)
- 組織、ビジネス機能、部門(マーケティング、エンジニアリング、財務、人事)
- 実稼働の重要度(実稼働、開発、テスト、QA)
- ネットワーク ドメイン(内部ネットワーク、DMZ、外部ネットワーク)

地理はドメイン グループのパーティション分割の最も一般的な理由です。同じ地理内のドメインは、多くの場合、同じ管理設定と運用設定が必要です。

運用ポリシーの設定と導入を簡素化するため、ドメイン グループを使用します。運用上の課題に最適な場合には、階層を定義します。

ドメイン グループの再割り当て

ドメイン登録後にドメイン グループ ポリシーを変更すると、ドメインがドメイン グループに自動的に再割り当てされなくなります。

[Reevaluate Membership] 機能は、ドメインでのドメイン グループの再割り当てに影響します。この機能は、UCS ドメインをポリシーの変更が発生する可能性がある別のドメイン グループに移動できます。

CHAPTER 8

登録

Cisco UCS Manager と Cisco UCS Central の登録

次のことを確認してください。

- 既存の Cisco UCS Manager ドメインが同じ NTP サーバに解決されること
- FQDN（完全修飾ドメイン名）を使用して Cisco UCS Central サーバに Cisco UCS ドメインを登録すること

名前空間の競合

注意 登録したドメインが登録解除されたか意図せず登録を解除されている期間に注意します。

登録解除されたときにローカルにキャッシュされている任意のグローバル オブジェクトは、Cisco UCS Central に再登録する場合に名前空間の競合を引き起こす可能性があります。Cisco UCS Central によって所有されているオブジェクトに同じ名前が存在していると問題が生じます。このような名前の競合を解決してローカル オブジェクトのグローバル制御に戻るには、ローカル オブジェクトで [UCSM] > [Use Global] オプションを使用します。

（注） [Use Global] オプションにより、登録解除状態の間にローカル ポリシーに行われたすべての変更を上書きします。

CHAPTER 9

ブラウンフィールドからグリーンフィールドへの移行

既存の展開の移行

既存のローカル展開をグローバル展開に移行する際のベスト プラクティスは、グローバル運用ポリシーとサービス プロファイル ポリシーを使用することです。

Cisco UCS Central のポリシー

Cisco UCS Central は、複数のドメインに一貫したグローバルな動作を自動的に適用するグローバル ポリシーを提供します。

Cisco UCS Central には、2 つの主要なタイプのポリシーがあります。

- 運用ポリシー
- ワークロード ポリシー（またはサービス プロファイルで使用されるポリシー）

運用ポリシー

例には、Call Home、ユーザ管理、タイム ゾーン、DNS、NTP、バックアップなどのユーザ認証設定の機能が含まれます。Cisco UCS Central では、ドメイン グループ（またはサブドメイン グループ）とその関連付けられたすべてのドメインとの関係で運用ポリシーが適用されます。

ドメイン グループと運用ポリシーは通常、物理的な場所、地域、またはその他の要因によって影響を受ける、サイト固有の側面を制御します。

ドメイン グループの階層を利用して、定義する運用ポリシーの数を最小限にします。運用ポリシーは非破壊的なものと潜在的に破壊的なものとに分けることができます。

ベスト プラクティスでは、管理者はできる限り多くの非破壊的なポリシーを、ドメイン グループの階層のできる限り上位に配置することが推奨されています。同様に、潜在的に破壊的なポリシーは、ドメイン グループの階層のできる限り下位に配置します。

サービス プロファイル ポリシーとグローバル サービス プロファイルを導入する際には、要件と制約に基づいてこれらの適性を確認します。たとえば、ローカル サービス プロファイルのグローバル サービス プロファイルへの移行は、同じ ID を保持する必要がなければ簡単です。ID を同じままにする必要がある場合には複雑です。ローカル サービス プロファイルを設定できない場合でも、Cisco UCS Central からこれらを表示できることを覚えておいてください。

ワークロード ポリシー

ワークロード ポリシーは通常、ブート ポリシー、VNIC/VHBA テンプレート、ネットワーク QoS、および BIOS ポリシーなどのサービス プロファイルに関連付けられます。Cisco UCS Central では、組織とその関連付けられた子組織にワークロード ポリシーを適用します。

組織とワークロード ポリシーは通常、サービス プロファイルと関連するテンプレート、プール、ポリシーを制御します。

Cisco UCS ドメインに Cisco UCS Central を導入する際は、最新の警告と制限に注意してください。最も重要な制限: ローカル サービス プロファイルはグローバル プールとポリシーを参照できますが、ローカル サービス プロファイルをグローバル サービス プロファイルに変換することはできません。したがって、既存のサービス プロファイルは、ローカルで管理されるモードのままにします。設定を再作成する唯一の方法は、グローバル サービス プロファイルで設定を再構築することです。

管理の簡素化に役立つ場合は、サービス プロファイル ポリシーとグローバル サービス プロファイルのみを導入します。導入によって管理が複雑になる場合は、導入しないでください。

運用ポリシーとサービス プロファイル ポリシーとの間に依存関係はありません。Cisco UCS Central では、グローバル サービス プロファイル ポリシーとグローバル サービス プロファイルの導入を強制する要件はありません。

Cisco UCS Manager ドメインは、自身がドメイン グループに含まれていることを認識していません。そのため、これらは Cisco UCS Central 内で作成された運用構造を共有しません。ただし、組織構造は一貫性を保ち、グローバルな範囲で Cisco UCS Manager と Cisco UCS Central とで相互に共有されます。

グローバルな動作ポリシー

Cisco UCS Central は、1 つ以上の Cisco UCS ドメインにグローバル運用ポリシーを提供します。グローバル ポリシーへのすべての参加が、Cisco UCS Manager ドメインのオプトインの基礎になります。Cisco UCS Central は、このような制御がローカルの Cisco UCS Manager ドメイン管理者から最初に委託されない限り、グローバル ポリシーを制御しません。ローカルの Cisco UCS Manager ドメイン管理者は、任意のポリシーをグローバル管理から外すことで制御を取り消すことができます。

すべての管理ポリシーは、デフォルトでは、以下が発生するまでローカル ドメインで制御されます。

1. ローカル ドメインが Cisco UCS Central に登録される。
2. ローカル ドメインが、グループ解除されたドメインから Cisco UCS Central のドメイン グループに移動される。
3. ローカル ドメイン管理者が、特定のポリシーをローカルからグローバルの解決に明示的にレベルを上げる。

個々のポリシーの格上げの決定には、依存関係はありません。たとえば、Infrastructure & Catalog Firmware をローカルに管理しつつ、障害ポリシーをグローバル化できます。Cisco UCS Manager で、[Admin] > [Communication Management] > [Cisco UCS Central] の順に選択した場合、ポリシー解決コントロールに記載されているポリシーはすべて独立しています。

ポリシーがローカルからグローバルに格上げされると、Cisco UCS Central レベルで有効なポリシー定義のみを変更できます。これは、ドメイン間で一貫性を強制するために設計によって行われます。ただし、管理者は、いつでもローカルで解決されたポリシーに戻ることができます。管理者がポリシーのローカル管理に戻ると、そのポリシー設定はローカル管理者が変更するまでそのままになります。Cisco UCS Central では、そのポリシーが制御されなくなります。

グローバル運用ポリシーのベスト プラクティス

ローカル運用ポリシーの制御からグローバル制御への移行を検討する際、グローバル ポリシーの広範な展開前にローカル ポリシー解決を維持します。精通するまで時間をかけて段階的に個別のポリシーでグローバル ポリシーを導入します。これはファームウェア管理にも当てはまります。

一般的に、システム ヘルスとモニタリングは、グローバル ポリシーで使用するためのリスクの低い候補となります。SNMP、syslog、および Call Home のポリシーを、ドメイン グループの階層のできる限り上位で運用ポリシーとして定義することが最も簡単なアプローチです。下位ドメイン グループ内のドメインはすべて、これらのグローバル ポリシーの定義を継承します。

シスコでは、可能な限りポリシーの一貫性と一元化されたポリシー適用を利用することを推奨しています。グローバルな一貫性とポリシーの適用は、Cisco UCS Central の設計目標の中でもとりわけ重要です。Cisco UCS Central 内でポリシー定義と設定を統合することで、ローカル Cisco UCS 管理者の管理の負担が軽減されます。機会があれば、ポリシーをより高いレベルでより一元的に定義するほど、管理のスケーラビリティが高まることに留意してください。可能な限り、ポリシーの定義を簡素化し、一元化することに重点を置いてポリシーを設計します。

利用可能なグローバル運用ポリシー

次の表に、Cisco UCS Central と Cisco UCS Manager の対応を示します。[UCSM Navigation] 列には、Cisco UCS Central でグローバルに解決するようにポリシーを設定すると、参照が GUI で非アクティブになる個所を示しています。また、ドメインがドメイン グループの一部になると、参照が非アクティブになる個所も示しています。

ポリシー タイプ	Cisco UCS Central の参照	Cisco UCS Manager のナビゲーション
Infrastructure & Catalog Firmware	*ドメイン グループ*> [Firmware Management] > [Infrastructure Firmware]	[Equipment] > [Firmware Auto Install]
タイム ゾーン管理	*ドメイン グループ*> [Operational Policies] > [Time Zone]	[Admin] > [Timezone Management]
通信サービス	*ドメイン グループ*> [Operational Policies] > [Remote Access]	[Admin] > [Communication Management] > [Communication Services]
グローバル障害ポリシー	*ドメイン グループ*> [Operational Policies] > [Debug] > [Global Fault Policy]	[Admin] > [Faults/Events/Audit] > [Settings]

ポリシー タイプ	Cisco UCS Central の参照	Cisco UCS Manager のナビゲーション
ユーザ管理	*ドメイン グループ*> [Operational Policies] > [Security]	[Admin] > [User Management]
DNS 管理	*ドメイン グループ*> [Operational Policies] > [DNS]	[Admin] > [Communication Management] > [DNS Management]
バックアップとエクスポート ポリシー	*ドメイン グループ*> [Backup/Export Policy]	[Admin] > [All] > [Backup and Export Policy]
モニタリング	*ドメイン グループ*> [Operational Policies] > [Call Home and Debug]	[Admin] > [Faults/Events] > [Syslog Faults/Events] > [Settings] > [TFTP Core Exporter] [Communications Mgmt] > [Call Home]
SEL ポリシー	*ドメイン グループ*> [Operational Policies] > [Equipment] > [SEL Policy]	[Equipment] > [Policies] > [SEL Policy]
電源割り当て	*ドメイン グループ*> [Operational Policies] > [Equipment] > [Global Power Allocation Policy]	[Equipment] > [Policies] > [Global Policies] > [Global Power Allocation Policy]
電源ポリシー	*ドメイン グループ*> [Operational Policies] > [Equipment] > [Power Policy]	[Equipment] > [Policies] > [Global Policies] > [Power Policy]

移行

この手順では、ブラウンフィールド環境からグリーンフィールド環境に移行する方法について説明します。各サービス プロファイル内でターゲット イニシエータ（WWPN）にすでに分割されているリモート ストレージ ブート LUN を使用して SAN からブートするといった、難しい使用事例を使用して説明します。

（注） 移行中は ID を同じままにする必要があります。

移行時には、以下を行う必要があります。

- Cisco UCS Central に既存の UCS ドメインを登録します。
- グローバル プール、ポリシー、VLAN、VSAN、vNIC テンプレート、vHBA テンプレート、LAN 接続ポリシー、SAN 接続ポリシー、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 プロファイルを作成します。

  これらのグローバル ID プールとポリシーが、現在 UCS ドメインでローカルに構築されているのと同じ形式、設計とスキームに一致していることを確認します。

  グローバルで同等のものを作成する場合は、すべての名前が一意であることを確認します。
- グローバル VSAN を作成する場合は、Cisco UCS Manager でローカルに定義された VSAN の ID と同じものを使用します。
- VSAN の名前の前に「G-」を使用します。
- 新しく作成されたグローバル VSAN で、FCoE VLAN ID が、対応するローカル VSAN で設定された FCoE VLAN ID と完全に一致することを確認します。

（注） UCS ドメインですでに定義されているグローバル VSAN と同じ ID を持つグローバル VSAN を作成する場合は、FCoE VSAN ID がローカル VSAN とグローバル VSAN との間で正確に一致する必要があります。一致していない場合、グローバル サービス プロファイルの関連付でエラーがトリガーされます。

- それぞれのグローバル ID プールから新しい UUID、MAC、WWNN、WWPN を割り当てるグローバル サービス プロファイルを作成します。
- 簡単な Cisco UCS Central Powertools スクリプトを活用して、元の（正しく区分された）WWPN とその他の ID を割り当てます。

Cisco UCS Central でブラウンフィールドのローカル サービス プロファイルをグローバル サービス プロファイルへ移行する

ステップ 1 ローカル サービス プロファイルの ID プール、ポリシー、VLAN、VSAN、およびテンプレートを文書化します。

ステップ 2 Cisco UCS Central ですべての ID、ポリシー、VLAN、VSAN、テンプレート、グローバル サービス プロファイルを再作成します。

ステップ 3 ローカル サービス プロファイルがあるサーバをグレースフル シャット ダウンします。

ステップ 4 ローカル サービス プロファイルをドメインから関連付けを解除します。

ステップ 5 ローカル サービス プロファイルを削除します。
これにより割り当てられた ID がプールに戻され、未使用として ID がマークされます。

ステップ 6 Cisco UCS Central Powertools スクリプトを実行して、特定のグローバル サービス プロファイルの ID を交換します。
これにより、グローバル サービス プロファイルの外観が対応するローカル サービス プロファイルと同じになります。

ステップ 7 新しいグローバル サービス プロファイルで特定のサーバに対して ID が正しいことを確認します。

ステップ 8 グローバル サービス プロファイルを適切なサーバに関連付けます。

ステップ 9 SAN LUN からサーバを起動します。

次の例では、以下を想定しています。

```
Global service profile Name: G-Sp-TEST-2 (with global pool derived IDs)
Org: root
Global WWNN pool: G-USA-WWNN
Global UUID pool: G-USA-UUID
Global MAC pool: G-USA-MAC
New (from local service profile) UUID: dc81c8de-3b00-11e5-0000-000000000025
New (from local service profile) MAC for vnic0: 00:25:B5:00:00:25
New (from local service profile) MAC for vnic1: 00:25:B5:00:00:26
New (from local service profile) WWNN ID: 20:00:00:25:B5:00:00:25
New (from local service profile) WWpN for A Fabric: 20:00:00:25:B5:AA:00:25
New (from local service profile) WWPN for B Fabric: 20:00:00:25:B5:BB:00:25
```

Cisco UCS Central Powertools スクリプトの例

実稼働環境で使用する前に、このスクリプトをラボでテストします。企業のニーズに応じてスクリプトを編集します。

このスクリプトは、シスコの製品で正式にサポートされていません。利用はお客様の責任の元で行ってください。

```
# Start-UcsCentralTransaction
  Get-UcsCentralOrg -Name root | Add-UcsCentralserviceprofile -Name "G-Sp-TEST-2"
-Modifypresent -IdentpoolName "G-USA-UUID" -Uuid "dc81c8de-3b00-11e5-0000-000000000025"
  $mo = Get-UcsCentralserviceprofile -Name "G-Sp-TEST-2"
  $mo_1 = $mo | Add-UcsCentralVnic -Modifypresent -Name "vnic0" -IdentpoolName "G-USA-MAC"
 -Addr "00:25:B5:00:00:25" -Order "1" -SwitchId "A"
  $mo_2 = $mo | Add-UcsCentralVnic -Modifypresent -Name "vnic1" -IdentpoolName "G-USA-MAC"
 -Addr "00:25:B5:00:00:26" -Order "2" -SwitchId "B"
  $mo_3 = $mo | Add-UcsCentralvhba -Modifypresent -AdaptorprofileName
  "global-default"-Addr
 "20:00:00:25:B5:AA:00:25" -AdminVcon "any" -MaxDataFieldSize "2048" -NwTemplName ""
 -Order
 "3" -pinToGroupName ""-QospolicyName "" -StatspolicyName "global-default" -SwitchId "A"
-Name "vhba0"
  $mo_4= $mo | Add-UcsCentralvhba -Modifypresent -AdaptorprofileName "global-default"-Addr
 "20:00:00:25:B5:BB:00:25" -AdminVcon "any" -MaxDataFieldSize "2048" -NwTemplName ""
 -Order
 "4" -pinToGroupName ""-QospolicyName "" -StatspolicyName "global-default" -SwitchId "B"
-Name "vhba1"
  $mo_5 = $mo | Add-UcsCentralVnicFcNode -Modifypresent -IdentpoolName "G-USA-WWNN" -Addr
 "20:00:00:25:B5:00:00:25"
  Complete-UcsCentralTransaction
```

CHAPTER 10

マニュアルの構成

階層

Cisco UCS Manager は構造を通じて反映されているように、本質的に階層型です。

Cisco UCS Central では、階層構造がグローバル スコープになっています。

Cisco UCS Central 内のドメイン グループの構造も階層型です。重要な違いの 1 つは、「ドメイン グループ」が純粋に Cisco UCS Central の構成であることです。これは、運用ポリシー、VLAN、VSAN、および ID アクセス制御ポリシーなどの一部の特殊なポリシーを、登録された Cisco UCS ドメインにマッピングおよび適用するために使用されます。ローカル Cisco UCS ドメインにはドメイン グループは表示されませんが、運用ポリシーの影響を受けます。

組織およびドメイン グループのベスト プラクティスは、エンタープライズの論理（組織）と物理（ドメイン グループ）のセグメンテーションを最適に反映した階層を作成することです。

- `/root` ドメイン グループ内のすべての運用ポリシーが、すべてのドメインに対するグローバル適用性を持つことを意図して作成されていることを確認します。
- `/root` 組織に配置されたすべてのサービス プロファイルのポリシーが、Cisco UCS ドメイン全体に公開されるようになっていることを確認します。

混合ワークロード環境

ブラウンフィールド環境では、既存の Cisco UCS ドメインに展開される新しいワークロードのため、Cisco UCS とグローバル一貫性の採用を検討してください。このような環境は、グローバルとローカルで管理されるオブジェクトの両方が含まれている場合があるため、混合ワークロード環境と呼ばれます。既存のドメインに Cisco UCS Central と Cisco UCS Manager の両方が所有する管理対象オブジェクトが含まれている可能性がある混合ワークロード環境には 2 つのモデルがあります。

- 分離された組織
- 統合された組織

分離された組織

このモデルでは、組織の階層（/root の下）に Cisco UCS Central または Cisco UCS Manager によって独占的に所有および管理されている管理対象オブジェクトが含まれています。

このアプローチを使用したベスト プラクティスは、組織がグローバルに管理されたオブジェクトのみで構成されている個別のグローバルな名前を持つ組織を作成することです。階層内の同じレベルでは、対応する組織はローカルで所有する管理対象オブジェクトだけが含まれます。

ローカル組織でのワークロードは、ローカル プール、ポリシー、およびテンプレートのみを指します。グローバル組織でのワークロードは、グローバル プール、ポリシー、およびテンプレートのみを指します。

さらに、組織名で **G-** プレフィックスを使用すると、すべてのオブジェクトに対するグローバル スコープを意味します。これにより、組織内の各管理対象オブジェクトへの **G-** プレフィックスの必要性を削減します。

Cisco UCS Central はこのグローバル組織構造を作成し、その後、グローバル サービス プロファイルの関連付けの間に展開します。ベスト プラクティスは、このグローバル組織構造内で名前を区別することです。しかし、それでも下位プール、ポリシー、VLAN、VSAN、テンプレート、グローバル サービス プロファイルには **G-** プレフィックス名を使用することをお勧めします。

CHAPTER 11

Cisco UCS Manager と Cisco UCS Central との間におけるポリシーの違いを理解する

高度なポリシー解決

（注） 高度なポリシー解決のデモのビデオをご覧ください。このビデオは英語です。

グローバル サービス プロファイル テンプレートで任意のポリシーを参照することができます。組織構造の異なるレベルでは、同じ名前のポリシーであっても存在できます。しかし、組織構造の同じレベルに同じ名前の 2 つのポリシーが存在することはできません。

サービス プロファイルは、最初は必ず特定の組織レベルのポリシーに従います。次に、ポリシー名がそのレベルに含まれていなければ、/root レベルで解決されます。

このトピックのビデオでは、高度なポリシー解決のデモを行うため、さまざまな組織で SAN-BOOT ポリシーを別のポリシー設定と入れ替える方法について説明しています。その後、単一のグローバル サービス プロファイル テンプレートを使用して、結果のグローバル サービス プロファイルをこれらの異なる下位組織にインスタンス化します。これにより下位組織が下位組織のレベルで目的のブート ポリシーを取得できるようになります。

ここでは、SAN-BOOT ポリシーが汎用ターゲット イニシエータとともに /root にあると仮定します。このブート ポリシーで SAN ブートするブレード サーバはありません。これはプレースホルダとして機能します。グローバル サービス プロファイル テンプレートはそれを使用します。

サービス プロファイル テンプレートを編集する際に、[Policies] をクリックし、[Boot] ポリシーを選択すると、新しく作成された SAN-BOOT ポリシーの詳細を確認できます。

SAN-BOOT ポリシーで、UCS または Cisco UCS Central SAN-BOOT ポリシーの有効なブート パスの汎用イニシエータを作成します。これは 2 つの有効な VHBA（プライマリとセカンダリ）で構成されています。各 VHBA にも、独自のプライマリとセカンダリのターゲット イニシエータがあります。

ブレード サーバが SAN ブートする方法を反映した組織構造を作成します。たとえば、グローバル サービス プロファイルの半分をあるストレージ アレイ コントローラからブートし、もう半分を別のコントローラからブートすることができます。これにより、ストレージ アレイのブート ロードが分割されます。

実稼働用に作成された下位組織には、SA コントローラ A と SA コントローラ B があります。各 SA コントローラの下位組織内に、ブート コントローラ SAN-BOOT ポリシーを作成しました。SAN-BOOT ポリシーには、ストレージ アレイをブートするための有効な真のターゲット イニシエータが含まれています。ただし、すべてのグローバル サービス プロファイルがストレージ アレイにブートする場合にブート ロードを分離するための異なるイニシエータが含まれている場合は除きます。

SA コントローラ A 下位組織内の SAN-BOOT ポリシーには、次のブート ターゲット イニシエータ値が含まれています。4 つのイニシエータ ターゲットの WWPN は 11、22、33、44 で終ります。SA コントローラ B 下位組織内の SAN-BOOT ポリシーには、次のブート ターゲット イニシエータ値が含まれています。4 つのイニシエータ ターゲットの WWPN は 55、66、77、88 で終ります。

SAN-BOOT ポリシーを使用する単一のグローバル サービス プロファイル テンプレート（G-SP-SAN-BOOT）から、[Create Service Profile from Template] 機能を使用して、これらのグローバル サービス プロファイルをそれぞれの SA コントローラの下位組織にインスタンス化します。

ポリシーが作成され、UCS ドメイン内のブレードに関連付けられると、グローバル サービス プロファイルの展開、SAN-BOOT ポリシー、およびドメインにコピーされたイニシエータを確認できます。ターゲット イニシエータは、SA コントローラ A と B の下位組織の SAN-BOOT ポリシーで設定されたイニシエータと正確に一致します。

Cisco UCS Central がポリシーを適切に展開すると、オブジェクト名の競合は発生しません。同じ名前を持つ 2 つのポリシーは、異なる下位組織構造に含まれています。

VLAN と VSAN ID のエイリアシング

（注） VLAN ID のエイリアシング設定のデモのビデオをご覧ください。このビデオは英語です。

VLAN ID のエイリアシングは、Cisco UCS Central で維持するグローバル サービス プロファイル テンプレートの全体数の削減に役立つ場合があります。これまで、Cisco UCS Manager 内でローカル VLAN または VSAN を作成する際は、ネットワークまたはファブリック内のすべての ID に新しい VLAN または VSAN を作成していました。たとえば、（これらのネットワークのサブネットの物理的な位置と一致する）サブネットごとに異なる VLAN ID がある場合、これらの VLAN を個別に作成していました。これらには、個別の vNIC テンプレート、LAN 接続ポリシー、サービス プロファイル テンプレートが必要でした。同じシナリオが VSAN にも当てはまります。Cisco UCS Central でグローバル ポリシーとオブジェクトを使用すると、このプロセスが非常に効率的になり、グローバル サービス プロファイル テンプレートの数が減ります。インフラストラクチャが減れば、管理も容易になります。

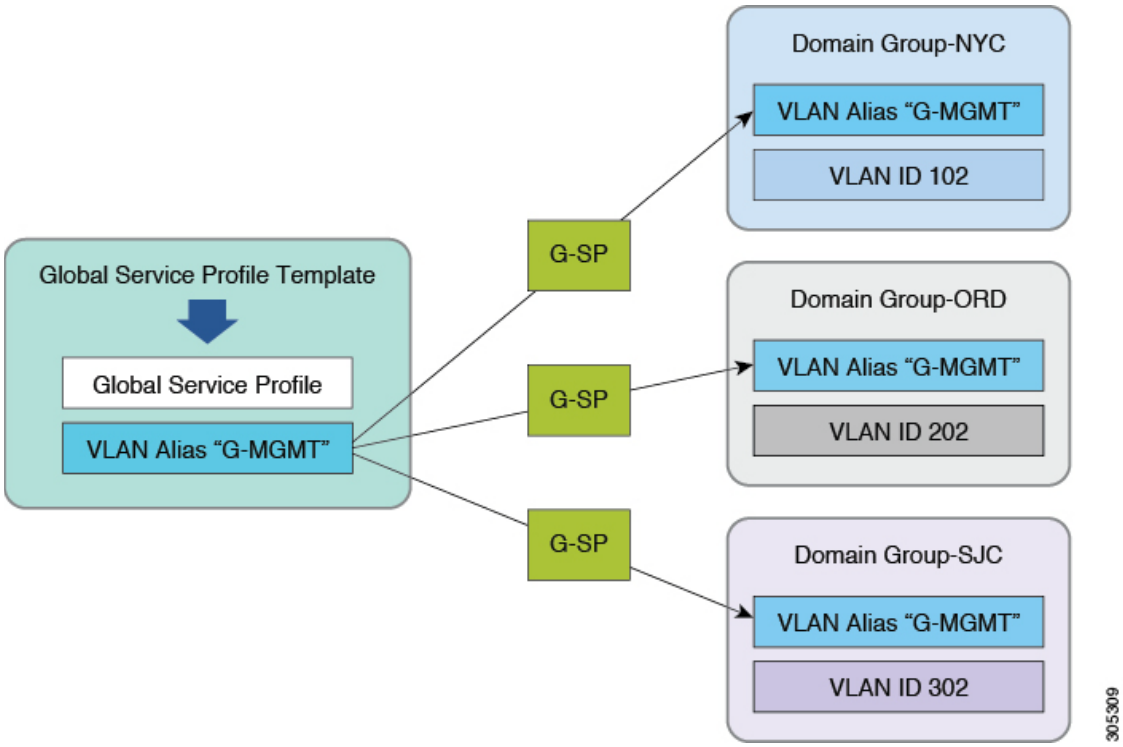
グローバル サービス プロファイルは、対応するグローバル サービス プロファイル テンプレートからインスタンス化されます。Cisco UCS Central でグローバル VLAN を作成する際に、そのドメイン グループの場所を指定する必要があります。この指定により、VLAN または VSAN の使用と対応する ID が、その特定のドメイン グループに結び付けられます。

同じ名前を持つ VLAN を作成できますが、異なる VLAN ID とドメイン グループを使用します。これらを作成すると、[All VLANs] タブでエイリアス処理された VLAN と、単一の VLAN に関連付けられた VLAN ID を確認できます。

VLAN を選択すると、それを編集することができます。[Aliased VLANs] タブに移動しても、対応する VLAN ID を確認できます。

1 つのグローバル サービス プロファイル テンプレートで、異なるドメイン グループ内の複数の UCS ドメインにグローバル サービス プロファイルを提供できます。グローバル サービス プロファイルとドメイン グループとを関連付けると、Cisco UCS Central は、適切な VLAN ID とそのグローバル サービス プロファイルを展開します。

図 4:VLAN と VSAN ID のエイリアシング:設定例



ID 範囲アクセス コントロール ポリシー

（注） UCS Central の ID アクセス コントロール ポリシー。このビデオは英語でのみ用意されています。

ID 範囲アクセス コントロール ポリシーは任意の ID プールに適用できます。これらは、大規模な Cisco UCS Central 環境での IP 管理プール ID の管理に役立ちます。UCS ブレードとサーバの管理 IP は、インバンドまたはアウトオブバンドのどちらでも、企業全体に分散された UCS ドメイン内の異なる IP サブネット上で行えます。

ID 範囲アクセス コントロール ポリシーにより、管理 IP でグローバル サービス プロファイルと UCS ドメインを関連付けるタイミングを調整できます。実際のプロセスは、VLAN または VSAN ID のエイリアシングとは少し異なります。ポリシーは、管理 IP（サブネットあたり）のブロックと UCS ドメインがメンバとなっているドメイン グループ間のポインタとして機能します。

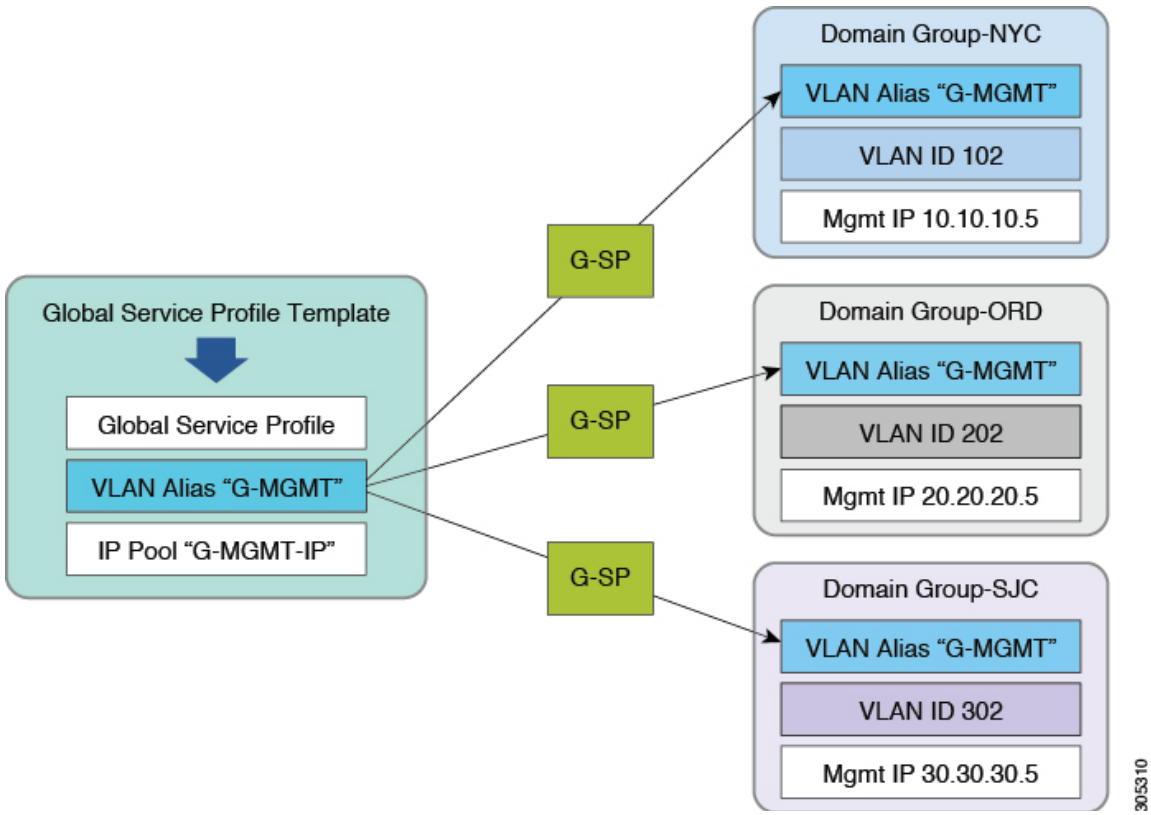
グローバル IP 管理プールを作成する際に、別の UCS ドメインの管理サブネットと一致する管理 IP の該当するブロックを使用します。実際の ID 範囲アクセス コントロール ポリシーの作成は、ドメイン グループと同時に行われるため簡単です。ポリシーを作成したら、管理 IP プールの管理アドレスの特定のブロックごとに適切なポリシーを選択することで、これらのポリシーにアクセスします。

順番に、管理 IP プールのサブネット ブロックごとに適切な ID 範囲アクセス コントロール ポリシーを選択します。新しく作成したプールを使用し、UCS ドメインに関連付けられているグローバル サービス プロファイルはすべて、そのドメイン グループと UCS ドメイン メンバに発行された管理 IP アドレスのみです。そのグローバル サービス プロファイルを別のドメイン グループ内の UCS ドメインに移動すると、ポリシーがそのドメイン グループに別の管理 IP を発行します。

これによりグローバル サービス プロファイル テンプレートの数が減ります。複数の UCS サイト、UCS ドメイン、VLAN ID、管理サブネットがある場合でも、1 つのグローバル サービス プロファイル テンプレートからすべてのグローバル サービス プロファイルを構築できます。

高度なポリシー解決、VLAN、VSAN ID のエイリアシング、ID アクセス コントロール ポリシーはすべて集合的に機能して、グローバル サービス プロファイル テンプレートの総数を減らすことができます。

図 5:ID 範囲アクセス コントロール ポリシー:設定例



ブラウンフィールド：ローカル サービス プロファイルを使用したグローバル ID およびポリシーへのアクセス

UCS ドメインを Cisco UCS Central に登録すると、Cisco UCS Manager 内からすべてのグローバル ID プールとポリシーを確認できます。ブラウンフィールドからグリーンフィールド環境に移行する場合は、Cisco UCS Central 内でグローバル ポリシーを作成します。Cisco UCS Manager は Cisco UCS Manager からこれらのポリシー（具体的には、ローカル サービス テンプレートおよびローカル サービス プロファイル）にアクセスします。デフォルトのホスト ファームウェア パッケージ（ローカル ポリシー）から Cisco UCS Central にある global-default（グローバル ポリシー）にローカル サービス プロファイルを切り替えることができます。

任意のポリシーと ID をローカルからグローバルに切り替えることができます。これには、ローカル UUID、MAC、IP、WWNN、WWPN プールが含まれます。ただし、これは破壊的な場合があります。グローバル ポリシーにローカル ポリシーと**同一の**設定がある場合、実行中のワークロードは中断されません。ID プールをローカルからグローバルに切り替えると場合は、グローバル プールにローカル プールと同じ ID の形式が**含まれている必要があります**。また、特定の ID を割り当てられるようにする必要もあります。これらのガイドラインに当てはまらないものはすべて、サービス プロファイルの中断（再関連付け）を引き起こすか、メンテナンス ポリシーから中断を確認するためのユーザの確認応答を要求します。

（注） これらの変更は必ずラボでテストしてから、実稼働環境に展開します。それが不可能な場合は、実稼働のワークロードを実行していないブレード サーバに割り当てられた単一のサービス プロファイルを選択します。

ユーザの確認応答動作の説明

- グローバル サービス プロファイルとグローバル メンテナンス ポリシー：
  - Cisco UCS Manager で確認応答**できない** Cisco UCS Manager 内の保留中のアクティビティ アラートを表示します。
  - Cisco UCS Central で確認応答できる Cisco UCS Central 内の保留中のアクティビティ アラートを表示します。
- ローカル サービス プロファイルとグローバル メンテナンス ポリシー：
  - Cisco UCS Manager で確認応答**できない** Cisco UCS Manager 内の保留中のアクティビティを表示します。
  - Cisco UCS Central で確認応答する必要がある Cisco UCS Central 内の保留中のアクティビティを表示します。
- ローカル サービス プロファイルとローカル メンテナンス ポリシー（Cisco UCS Central に登録されている UCS ドメイン）：
  - Cisco UCS Manager で確認応答できる Cisco UCS Manager 内の保留中のアクティビティを表示します。
  - Cisco UCS Central で確認応答できる Cisco UCS Central 内の保留中のアクティビティを表示します。

（注） 管理者が UCS ブレード サーバの Cisco UCS Central への確認応答を制限する場合は、すべてのローカル サービス プロファイルにユーザ応答確認のメンテナンス ポリシーが必要です。（管理者はブラウンフィールド環境で Cisco UCS Central に登録されているローカル サービス プロファイルを使用してこれを行えます）。

ルール ベースのアクセス制御と UCS Central のカスタム ビュー

Cisco UCS Central では、Cisco UCS Manager とは異なり、ルール ベースのアクセス制御（RBAC）の一環として、ユーザが表示および管理する内容に応じてカスタマイズしたビューを作成できます。

Cisco UCS Central では、ロケールを使用して、ユーザが表示および管理できるものをフィルタリングします。Cisco UCS Central のロケールは、組織権限だけでなく、Cisco UCS Central ドメイン グループの権限を使用しても定義されます。

たとえば、`root/Americas/NYC` に設定された組織権限と `root/DG-Americas/DG-NYC` のドメイン グループ権限を使用して NYC というロケールを作成します。

ロケールを作成したら、nyadmin というユーザを作成し、NYC ロケールをアカウント nyadmin に割り当てます。

ログオフして、nyadmin としてログインすると、組織構造とドメイン グループ構造の絞り込まれたビューが表示されます。

UCS Central から UCS ドメインを登録解除する

Cisco UCS Manager では、Cisco UCS Central からいつでも UCS ドメインの登録を解除できます。そのため、Cisco UCS Manager の管理者アカウントのセキュリティが必要です。シスコでは、実稼動中の UCS ドメインの登録を解除する前に、Cisco TAC に問い合わせることを強く推奨します。

注意 UCS ドメインを Cisco UCS Central から登録解除すると、そのドメインにプッシュされた以前のグローバル VLAN、VSAN、ポリシー、サービス プロファイルのすべての所有権がすぐにローカル Cisco UCS Manager に転送されます。

アイコンがグローバル アイコンからオブジェクトのローカル アイコンに戻ります。UCS ドメインの登録解除が、UCS ブレード サーバ上で実行中のワークロードに直接影響することはありません。新しくローカライズされたグローバル オブジェクトでは、Cisco UCS Central で作成された名前が保持されます。

シスコのアーキテクチャでは、登録解除が既存のワークロードの運用に影響を及ぼさないことが保証されています。しかし、後で Cisco UCS Central にそのドメインを再登録すると、問題が生じる可能性があります。

考慮すべき点は次のとおりです。

- Cisco UCS Central に再登録する予定がない場合は、Cisco UCS Central から UCS ドメインの登録を解除しても影響はありません。グローバル オブジェクトは、Cisco UCS Manager に復元された絶対オブジェクト コントロールを持つローカル オブジェクトに変換されます。
- 再登録する予定がある場合は、実稼働中の UCS ドメインの登録を解除する前に、Cisco TAC にお問い合せください。
- 登録を解除すると、UCS ドメインにプッシュされたすべてのグローバル オブジェクトはローカル オブジェクトに変換されます。グローバル デフォルト ポリシーおよびカスタム ポリシーは、自身の名前をローカル オブジェクトとして保持します。VLAN、VSAN、vHBA テンプレート、vNIC テンプレート、サービス プロファイルも、自身の名前を保持します。
- UCS ドメインを再登録する場合、グローバル サービス プロファイルをそのドメインにプッシュする際に、同じ名前を持つローカル オブジェクトによってエラーがトリガーされます。ローカル オブジェクトとグローバル オブジェクトは、同じ組織レベルで同じ名前を持つことができないため、このエラーはリソースのネーミングの競合です。これは、UCS ドメインを登録解除してから再登録した場合によく発生するエラーです。

プールとポリシーの名前解決

グローバル サービス プロファイルに関連するエラーをトラブルシューティングするには、プールとポリシーの名前解決を理解することが重要です。Cisco UCS Manager と Cisco UCS Central では、オブジェクトのネーミングにいくつかの制限を設けています。ネーミングの制約がないことが曖昧さにつながる場合があります。管理対象オブジェクトを作成する際に、ローカルとグローバルの両方で同じ名前を使用することを妨げるものはありません。サービス プロファイル（vNIC または vHBA）が任意のポリシー名またはプール名を参照すると、ローカルの Cisco UCS Manager は明確に定義された名前解決プロセスに従います。Cisco UCS Manager は、プールとポリシーのどちらに対しても、グローバル名よりもローカル名を優先します。Cisco UCS Manager はローカル サービス プロファイルを管理する際に、通常のポリシー解決ルックアップではグローバル オブジェクトよりもローカル オブジェクトを優先します。グローバル サービス プロファイルは、Cisco UCS Manager 内のローカル オブジェクトにアクセスしたり、利用することはできません。

ローカルに管理されているオブジェクトの名前解決

Cisco UCS Central がローカルに管理されているオブジェクトの名前を解決する場合、ルールの階層に従います。

1. オブジェクト名がローカル組織で検出され定義されている場合はそれを使用します。
2. オブジェクト名がより上位の親組織（ローカル組織の root まで）で検出され定義されている場合はそれを使用します。
3. オブジェクト名がグローバル組織で検出され定義されている場合はそれを使用します。
4. より上位の親組織（グローバル組織の root まで）で定義されたオブジェクト名を使用します。
5. ローカル組織内（組織の root まで）のデフォルト オブジェクトに対応する値を使用します。
6. グローバル組織内（組織の root まで）のグローバル デフォルト オブジェクトに対応する値を使用します。

グローバルに管理されているオブジェクトの名前解決

Cisco UCS Central がグローバルに管理されているオブジェクトの名前を解決する場合、ルールの階層に従います。

1. オブジェクト名がグローバル組織で検出され定義されている場合はそれを使用します。
2. より上位の親組織（グローバル組織の root まで）で定義されたオブジェクト名を使用します。
3. グローバル組織内（組織の root まで）のグローバル デフォルト オブジェクトに対応する値を使用します。

（注） ローカル サービス プロファイルは、ローカルまたはグローバルのいずれかのプール、ポリシー、テンプレートを参照できますが、グローバル サービス プロファイルが参照できるのはグローバルのプール、ポリシー、またはテンプレートのみです。

この場合、参照は依存関係を通じて別のポリシー テンプレートへの直接参照または間接参照のいずれかが可能です。

推奨される命名規則

（注） ブラウンフィールドの展開において曖昧さを回避するためのベスト プラクティスとして、ローカルおよびグローバルの両方のコンテキストで同じ名前を作成したり、使用しないでください。

曖昧さを回避するには、一意のプレフィックス（たとえば、A サイド ファブリック WWPN ID のグローバル WWPN プールには G-WWPN-A など）を使ってグローバル ポリシー名やプール名を作成します。別のベスト プラクティスは、明示的に定義されたプールとポリシーを常に使用することです。

また、デフォルトと global-default の名前は変更しないでください。デフォルト ポリシーを変更する場合は、ポリシーの目的を最適に反映する新しい名前でポリシーを作成します。たとえば、デフォルトのメンテナンス ポリシーは、ユーザの確認応答を要求するように設定されています。管理者は G-User-Ack という新しいカスタム ポリシーを作成して使用することで、このデフォルト ポリシーを変更することができます。

オブジェクトのクラス	ローカル デフォルト オブジェクト	グローバル デフォルト オブジェクト
MAC/WWPN/UUID プール、およびほとんどのポリシー	default	global-default
アウトオブバンド IP アドレス プール	ext-mgmt	global-ext-mgmt
iSCSI イニシエータ プール	default	global-iscsi-initiator-pool
WWNN ID	node-default	global-node-default

グリーンフィールドの例外

混合(ローカルとグローバル)ブラウンフィールド環境では、「G-」または「Global-」のネーミングプレフィックスを使用して、ネーミングの競合を回避することを強く推奨します。ただし、完全にグローバル化されたグリーンフィールド環境では、この命名規則は必要ありません。プレフィックスの主な機能は、名前空間の衝突を回避することです。すべてのプール、ポリシー、テンプレート、およびオブジェクトが 最初から Cisco UCS Central で排他的に定義されているとすれば、このプレフィックスのプラクティスは不要です。

ネーミング ポリシー

Cisco UCS Central と Cisco UCS Manager には多くのデフォルト ポリシーが含まれています。Cisco UCS Manager 内のローカル レベルにあるものもあれば、Cisco UCS Central 内のグローバル レベルにあるものもあります。デフォルト ポリシーを変更する場合は、そのポリシーのコピーを作成し、元のポリシーではなく、そのコピーを変更することを強く推奨します。

メンテナンス ポリシー

メンテナンス ポリシーでユーザの確認応答(user-ack)を要求して、予期しないサービスの中断を回避します。次のいずれかの方法を使用して、サービスの中断を確認する必要がある場所にそれを設定します。

- サービスの中断をローカルに行う場合は、ローカル サービス プロファイルを使用します。それをユーザの確認応答の設定されたローカルまたはグローバルのメンテナンス ポリシーに指定します。メンテナンス ポリシーがローカルまたはグローバルかに関係なく、Cisco UCS Central コンソールで確認応答することができます。
- グローバル サービス プロファイルを使用する場合、Cisco UCS Central 内でユーザの確認応答を設定します。保留中のアクティビティは Cisco UCS Manager で確認できますが、それに確認応答できるのは Cisco UCS Central でだけです。

CHAPTER 12

設定

DNS 管理

通常、DNS 管理はグローバル レベルまたは企業レベルで定義されます。そのため、DNS ドメイン名と DNS サーバはグローバル ポリシー管理のための最適な候補です。ドメイン グループの階層のできる限り上位の運用ポリシーでこれらを定義します。

電源管理

電源管理に関するポリシーには、2 つの異なるポリシーが含まれます。

- **グローバル電源割り当てポリシー**：シャーシ レベルでパワー キャッピングを適用するかどうか、または個々のブレード レベルでパワー キャップを手動でオーバーライドするかどうかを指定します。
- **電源ポリシー**：非冗長電源、N+1、または物理 AC 電源のグリッドに対するシャーシ レベルの設定。

電源ポリシーは Cisco UCS Central ポリシー定義の有力な候補です。

グローバル電源割り当てポリシーは、環境と場所の依存関係に最も敏感なポリシーの 1 つです。ベスト プラクティスは、ユーザの環境によって異なります。

次に例を示します。

- ラックあたりの電力バジェットは、データセンターや場所によって異なる場合があります。
- 一部のサイトでは、電力グループを実装して、データ センターのレイアウトに特有の複数のラックにまたがるパワー キャップを作成している場合もあります。

グローバル電源割り当てポリシーは、ローカル制約に依存します。定義方法は、ラックごとに電力を制限するための幅広い範囲のポリシーを作成するなど、非常にシンプルです。しかし定義方法はサイト固有で一般化は困難です。

ファブリック インターコネクト ポートの設定

ファブリック インターコネクト ポートの物理デバイスの設定は、Cisco UCS Central から設定します。現在サポートされている設定タイプは次のとおりです。

- サーバ
- アップリンク
- 統合ポート

Cisco UCS Central では、特定のポートのロールの定義に加え、アップリンク ポート チャネルの作成もサポートしています。

（注） 物理ポートに依存するオブジェクト（イーサネットとファイバ チャネルの両方のピン グループとポート チャネルを含む）の管理に Cisco UCS Central を使用することはできません。

Cisco UCS Manager での強制時刻同期

NTP サーバで時刻を設定すると、Cisco UCS Manager ですぐに時刻が同期されない場合があります。

Cisco UCS Manager を NTP と即座に同期するように強制するには、[Admin] タブで NTP サーバを設定します。その後、次のシーケンスを使って CLI からクロックの設定を試みます。

（注） 24 時間表示を使用して時間を設定します。

```
scope system
scope services
set clock month day year hour minute second
```

次の例は、2016 年 2 年 22 日 13:44:00 にクロックを設定します。

```
scope system
scope services
set clock february 22 2016 13 44 00
```

「Clock synchronization successful」のメッセージと、変更を反映した Cisco UCS Manager の時刻が表示されます。次に登録を試行すると成功するはずです。

（注） 数秒の時間差により、登録に失敗する場合があります。正常に登録するには、Cisco UCS Manager のシステム時刻が Cisco UCS Central のシステム時刻より遅れてはいけません。

Cisco UCS Central のサービス ステータス

次の CLI コマンドは、Cisco UCS Central サーバ上で実行されているサービスの状態を確認する方法について説明しています。

```
UCSC-A# connect local-mgmt
UCSC-A (local-mgmt)# show pmon state
```

（注） PMON（サービス）は、Cisco TAC に相談せずにリセットしないでください。

Cisco UCS Central の HTTPS 証明書

Cisco UCS Central の管理インターフェイスの多くの機能は、クライアント マシンで使用可能または（Cisco UCS Central によって管理される各 Cisco UCS ドメインから）インポートされた HTTPS 証明書に依存しています。

ブラウザはこれらの証明書を使用して、Cisco UCS Central を管理するために KVM の起動、Cisco UCS Manager の起動などの機能を呼び出し、Cisco UCS のエラー サマリーで特定のエラーやアラートを照会します。証明書が適切にインポートされていない場合、証明書が期限切れの場合、または特定のセキュリティ設定が有効になっている場合、エラーが発生する可能性があります。

CHAPTER 13

グローバル VLAN および VSAN の展開

VLAN と VSAN ポリシーのプッシュ

Cisco UCS Central では、グローバル VLAN および VSAN を Cisco UCS ドメインにパブリッシュ（プッシュ）することができます。グローバルに定義された VLAN または VSAN を提供するためにグローバル サービス プロファイルを設定して関連付ける必要はありません。

Cisco UCS Central は、適切なすべてのグローバル VLAN および VSAN を登録済みの Cisco UCS へのパブリッシュに使用できるようにします。

（注） これはグローバル VLAN または VSAN がドメイン グループに使用可能なことを前提としています。API の直接統合または Cisco UCS Central CLI を使用して、グローバル VLAN または VSAN のパブリッシュを自動化できます。この機能は、UI では利用できません。

VLAN または VSAN の手動でのパブリッシュ

次の CLI コードは、VLAN および VSAN を手動でパブリッシュする例を示しています。最初にシステムに対してパブリッシュ可能な VLAN および VSAN のクエリを実行し、VLAN をパブリッシュします。

（注） このメカニズムはパブリッシュ専用です。VLAN または VSAN は Cisco UCS Central で事前に作成されている必要があります。

```
UCSC-A# connect resource-mgr
UCSC-A(resource-mgr)# scope domain-mgmt
UCSC-A(resource-mgr) /domain-mgmt # show ucs-domain
UCSC-A(resource-mgr) /domain-mgmt # scope ucs-domain 1008
UCSC-A(resource-mgr) /domain-mgmt/ucs-domain # publish ?
vlan vlan-name
vsan Vsan
```

グローバル VLAN の削除

VLAN を削除する場合、その VLAN が vNIC テンプレートまたは LAN 接続ポリシーのいずれも参照していないことを確認します。また、そのグローバル VLAN を使用しているサービス プロファイルがないことも確認します。グローバル VLAN を削除する場合、必ず最初にその組織の権限を削除してから、グローバル VLAN を削除します。

ローカルに保持するグローバル VLAN と VSAN

グローバル VLAN および VSAN を UCS ドメインにプッシュすると、これらはグローバル サービス プロファイルとの関連付けを解除しても、そこに保持されます。これは設計によるものです。グローバル VLAN または VSAN を再度使用する予定がない場合、および UCS ドメインに展開された VLAN または VSAN を削除する場合、特定の VLAN または VSAN に [Make Local] 機能を使用します。ローカライズすると、VLAN または VSAN を削除できます。

ドメインが登録解除されると、[Deep Remove Global] 機能を使用していない限り、Cisco UCS Central はグローバル VLAN、VSAN、ポリシー、およびサービス プロファイルをすべてローカル オブジェクトに変換します。[Deep Remove Global] は登録解除時に使用できます。これは Cisco UCS ドメインからすべてのグローバル オブジェクトを削除します。

（注） UCS Central から実稼働中の UCS ドメインの登録を解除する前に、Cisco TAC にお問い合せください。

FCoE VLAN ID の競合

SAN クラウドから新しいグローバル VSAN を作成した場合、FCoE VLAN ID のデフォルト値は 1 です。これはグローバル VLAN ID のデフォルト値と競合しています。

新しいグローバル VSAN を作成する際に、FCoE VLAN ID を変更し、現在使用されていない VLAN ID を指定します。

CLI からのグローバル VLAN および VSAN の展開

グローバル VLAN および VSAN を 提供するためにグローバル サービス プロファイルを使用しなくても、これらを UCS ドメインに展開できます。この機能は CLI でのみ使用できます。これは、Cisco UCS Central からグローバル オブジェクトを使用およびアクセスしたい、ローカル サービス プロファイルを使用しているお客様にメリットがあります。

CLI からグローバル VLAN を手動でパブリッシュする

CLI で次のコマンドを入力して、グローバル VLAN を UCS ドメインにパブリッシュします。

はじめる前に

グローバル VLAN Cisco UCS Central を作成します。

ステップ 1 **# connect resource-mgr**

ステップ 2 **# scope domain-mgmt**

ステップ 3 **# show ucs-domain**
次のコマンドで使用するための UCS ドメインの ID が表示されます。

ステップ 4 **# scope ucs-domain** *[domain_name]*

ステップ 5 **# publish vlan** *[vlan_name]*

CLI からグローバル VSAN を手動でパブリッシュする

CLI で次のコマンドを入力して、グローバル VLAN を UCS ドメインにパブリッシュします。

はじめる前に

グローバル VSAN Cisco UCS Central を作成します。

ステップ 1 **# connect resource-mgr**

ステップ 2 # scope domain-mgmt

ステップ 3 # show ucs-domain
次のコマンドで使用するための UCS ドメインの ID が表示されます。

ステップ 4 # scope ucs-domain *[domain_name]*

ステップ 5 # publish vsan *[vsan_name] [fabric]*
コマンドの最後で **a** または **b** を使用して、目的のファブリックを指定します。

CLI のトラブルシューティング コマンド

次の CLI コマンドは、トラブルシューティングで最もよく使用される便利なコマンドです。

ディスク速度の表示

```
# show disk-speed

/dev/mapper/VolGroup00-LogVol00:
Timing cached reads:  12606 MB in 2.00 seconds = 6317.87 MB/sec
Timing buffered disk reads: 106 MB in 3.01 seconds = 35.21 MB/sec

/dev/mapper/VolGroup01-LogVol00:
Timing cached reads:  12600 MB in 2.00 seconds = 6315.33 MB/sec
Timing buffered disk reads: 320 MB in 3.00 seconds = 109.28 MB/sec
```

ディスク使用率の表示

```
# show disk-usage

Filesystem      Size Used Avail Use%  Mounted on
/dev/mapper/VolGroup00-LogVol00:
                37G   3.2G 32G  10%  /
/dev/sda1       99M   13M  81M  14%  /boot

/dev/mapper/VolGroup01-LogVol00:
                39G   177M 37G  1%  /bootflash
tmpfs           5.9G  728K 5.9G 1%  /dev/shm
```

登録済みドメイン ID の表示

```
# connect service-reg

Cisco UCS Central
TAC support: http://www.cisco.com/tac
.
.
.
# show clients

Registered Clients:
 ID: 1008
 Registered Client IP: 172.22.251.106
 Registered Client IPv6:  ::
 Registered Client Connection Protocol: Ipv4
 Registered Client Name: L14-UCS1
 Registered Client Type: Managed Endpoint

 ID: 1009
 Registered Client IP: 172.22.251.10
 Registered Client IPv6:  ::
 Registered Client Connection Protocol: Ipv4
 Registered Client Name: SJC18-L12-UCS1
 Registered Client Type: Managed Endpoint
```

CHAPTER 14

プール

識別子の管理

グローバル識別子の管理は、Cisco UCS におけるマルチドメイン管理の最大の課題の 1 つに取り組んでおり、システム識別子（MAC、WWxN、UUID）に対して一意のアドレス指定が保証されます。以前は、Cisco UCS Manager のベスト プラクティスでは、ID プール範囲の上位バイト内にドメイン ID を埋め込むことを推奨していました。これは、Cisco UCS Central の管理対象グローバル ID には現実的ではありません。

Cisco UCS Central では、ID プールをすべて定義し、すべての Cisco UCS ドメインにわたってそれらにグローバルにアクセスできます。これにより、すべての Cisco UCS ドメインで、重複しない一意の ID がサービス プロファイルに割り当てられることが保証されます。

ユーザがシステム内の別のプールまたはブロックと競合する ID のブロックを作成すると（ローカルおよびグローバル レベルの両方で）、Cisco UCS Central によってすぐに通知されます。

グローバル ID プールは組織構造に属しています。グローバル プールは、Cisco UCS Central の運用ポリシーとは異なり、ドメイン グループに依存しません。代わりに、グローバル ID プールの範囲は、いずれのドメイン グループのパーティションにも関係なく、Cisco UCS Central 内の組織構造の範囲にあるすべての UCS ドメインまで拡張されます。

Cisco UCS Central を展開する際のベスト プラクティスは、新しい Cisco UCS ドメインの展開のためのグローバル サービス プロファイルとともに、グローバル ID を採用することです。

プールのサイジング

管理対象オブジェクトの数を最小限に抑えるために、より多くのブロックでプールの数を減らします。

A サイドと B サイドのトラフィックを区別するには、対応する A サイドまたは B サイドのプール名を作成します。MAC/WWPN アドレス範囲の上位バイトに埋め込まれた「A」または「B」を使用します。このモデルを Cisco UCS Central に拡張するには、このようなプール構造の下に複数のブロックを作成することが含まれます。各ブロックの最も効率的なサイズは、256 アドレス（0xFF）です。

（注） Cisco UCS Central では、すべてのプール（UUID、MAC、WWxN）に対して 1,000 アドレス（0x3E8）の最大ブロック サイズが要求されます。

重複プール ID

Cisco UCS Central では、ID の重複使用の可能性を検出できます。

すべてのプール タイプ（UUID、MAC、WWxN）で、Cisco UCS ドメイン全体に存在する可能性がある重複 ID を表示することができます。ID の使用サマリでそれらを確認します。重複 ID の重大度は、「重大」（複数のサービス プロファイルに表示される ID の場合）、または「警告」（複数のローカル プールに表示される ID の場合）のいずれかでフラグが設定されます。

ローカル ID プールの消費量を確認するための唯一の方法は、個々の ID を選択し、対応するローカル プールとローカル サービス プロファイルの詳細を表示することです。

グローバル ID プールへの移行

現在ローカル ID プールを参照しているローカル サービス プロファイルを再設定して、代わりにグローバル ID プールを使用することができます。関連付けられたサービス プロファイルの ID を変更すると、通常、サービスの中断が発生します。しかし、Cisco UCS Central はグローバル ID プールへのこうした移行を容易にし、サービスの中断が発生しないように設計されています。

ローカル ID プールからグローバル ID プールに参照を変更する場合、UCS Manager の [LAN] タブの [vNIC/vHBA] 参照プルダウンでグローバル プールを選択します。まず、[Reset MAC/WWxN/UUID] を使用して、プールの参照をローカルからグローバルに変更してから、リセットを実行します。[ID Usage] をドリル ダウンして、ローカルまたはグローバル ID プールへの ID の関連付けを確認する明確な方法を確認します。

グローバル ID を使用するローカル サービス プロファイルは、グローバル ID を参照するグローバル サービス プロファイルが排他的な場合に、ID の一意性が保証されます。ただし、グローバル ID プールを参照するローカル サービス プロファイルは、グローバル サービス プロファイルのモビリティを利用できません。これらは特定のローカル Cisco UCS ドメインに常に存在し、限定されます。

新しいグローバル ID プールの作成

複数のドメインを持つ既存の Cisco UCS 顧客は、ドメイン ID を ID プール範囲の上位バイトに埋め込むことで、複数のドメイン ID の課題に対処している場合があります。しかし中には、前のローカル ID の使用方法とは異なる方法でグローバル ID を分離したいと考える管理者もいます。

通常、新規導入のためにグローバル ID プールを作成すると、ドメイン ID は関係なくなります。ただしこの例外は、ドメイン固有の ID 認定ポリシーを使用（またはプール内でブロックを使用）した場合です。

A サイドと B サイドの個別のグローバル プールを作成するためのベスト プラクティスが、トラブルシューティングに役立ちます。

グローバル UUID プールへの移行時の課題

ローカル UUID プールからグローバル UUID プールへの移行により、いくつかの課題が生じます。

課題エリア	説明
プレフィックス	ドメイン レベルで UUID のプレフィックスを定義します。UUID サフィックスを使用して、プール内でブロックを作成できます。すべてのローカル UUID プールの上位集合であるグローバル UUID を採用するには、Cisco UCS ドメインごとに少なくとも 1 つのグローバル UUID プールを作成する必要があります。 このため、グローバル UUID プールの数は、プールの数が統合されないように、ドメインの数と一致している必要があります。
組織（Orgs）	グローバル プールは組織に基づいていますが、UUID プレフィックスはドメインに基づいています（ファブリック インターコネクトの内部 ID）。組織とドメイン間のマッピングはありません。
採用	既存のサービス プロファイルは、再設定サイクルとサーバのリブートを実行しないと、グローバル UUID を利用できません。 既存のローカル サービス プロファイルは、ライフサイクルが終了するまでローカル サービス プロファイルのままにしておくことが推奨されます。新しいローカル サービス プロファイルをグローバル サービス プロファイルとして作成します。

グローバル ID プールへの移行の推奨事項

グローバル ID プールに移行しつつ、ローカル サービス プロファイルに同じ ID を維持するには、対応するローカル ID プールの上位集合になるように、グローバル ID プールを作成します。これは、グローバル ID プールに、ローカル ID プール内にあるすべての識別子ブロックが含まれることを意味します。

ベスト プラクティスは、G-MAC-A や G-WWPN-B といった、ファブリックの MAC および WWPN プールの A/B ネーミングの方向付けを採用することです。グローバル ID プールを作成すると、サービス プロファイル、VNIC、VHBA、またはテンプレートをグローバル ID プールを参照するように変更できます。Cisco UCS Central は、識別子をまだ割り当てていない場合は、以前にローカル ID プールで使用したのと同じ識別子を自動的に割り当てることで、サービスの中断の必要性を排除します。

ID 空間がすでにパーティション化され、重複していない場合は、以下を採用します。

1 一意の名前を使用して、Cisco UCS Central で新しいグローバル ID プールを作成します。プール名のプレフィックスには、**Global-** または **G-** を使用します。MAC および WWPN プールには、必要に応じて、**-A** または **-B** のサフィックスをプール名に追加します。

(注) MAC プールの場合、ネットワークのアップストリームで A と B の MAC がかみ合っていることをネットワーク管理者が常に確認します。これは、Cisco UCS Central が FI からのアップストリーム接続をアグリゲーション レイヤ 2、TOR（top of rack）、EOR（end of row）スイッチにクラスタ化するためです。

2 ローカル プール内のローカル ID ブロックごとに、グローバル プール内に対応する ID ブロックを再作成します。

3 既存のすべてのテンプレート（サービス プロファイル、VNIC、VHBA）を対応するグローバル ID プール名を参照するように変更します。

4 プールの参照をローカルからグローバルに変更します。特定のインスタンス化した管理対象オブジェクト上で、[Reset MAC/WWxN/UUID Address] を実行して、グローバル所有権の変更を有効にします。

5 対応するローカル ID ブロックに割り当てがないことを確認します。

6 ID の使用を通じて、アドレスがグローバル プールを参照していることを確認します。

7 ローカル プールで各ローカル ID ブロックに対応するローカル ID ブロックを削除します。

初期テンプレートから作成された VNIC または VHBA の場合、ID がグローバル ID プールを参照するようになると、その後に作成されるすべての管理対象オブジェクトが新しいグローバル ID プールを参照します。

テンプレートを更新するためにバインドされている VNIC または VHBA の場合、ID がグローバル ID プールを参照するようになると、テンプレートにバインドされている既存の管理対象オブジェクトはすべて、新しいグローバル ID プールを参照します。既存の管理対象オブジェクトの ID がグローバル プール内に割り当てられないまま存在している場合、この移行により再設定やリブートを行う必要はなく、またサービスへの影響もありません。

テンプレートにバインドされていない VNIC または VHBA の場合、サービス プロファイル名がグローバル プールをポイントするように変更され、既存の ID がグローバル プールですでに使用されている場合は、サービス プロファイルは新しい ID を受け取るため、再設定とリブートが発生し、サービスに影響を及ぼします。ID がすでに使用されている場合、その ID は保持され、グローバル プールをポイントします。再設定やサービスへの影響は生じません。

また、グローバル プールを通じて ext-mgmt および iSCSI イニシエータの IP アドレスも管理できます。

ID 範囲認定

Cisco UCS Central では、ID 範囲認定ポリシーを使用して、グローバル プール内の ID ブロックを、グローバル プールを参照する任意のローカルおよびグローバル サービス プロファイルの特定のドメインまたはドメイン グループに割り当てることができます。この方法で、特定のドメイン グループの 1 つ以上の Cisco UCS ドメインが、識別子の個別の範囲を使用することが保証されます。

Cisco UCS Central では、グローバル サービス プロファイルは、1 つ以上の ID ブロックで ID 範囲認定ポリシーの定義を利用するグローバル プールを参照できます。Cisco UCS Central が、ID の割り当てに関する緩やかなバインディングの概念を作成しました。Cisco UCS Central は、関連付けのための Cisco UCS サーバが選択されるまで待機します。次に、少なくとも 1 つの認定済みブロックを含むプールから ID を割り当てます。

グローバル サービス プロファイルによるグローバル ID の使用

グローバル サービス プロファイルの作成、関連付け、および関連付け解除のプロセス中に発生することを次に説明します。

サーバ統合のないグローバル サービス プロファイル

グローバル サービス プロファイルが認定済みのプールから ID を使用しない場合、Cisco UCS Central は適切な ID プールから ID 値を取得します。

グローバル サービス プロファイルが認定済みプールから ID を使用している場合、グローバル サービス プロファイルは設定エラー状態に移行し、次の警告メッセージをトリガーします。
`Using ID pool which contains block with Qualifier (Lazy-Binding)`

関連付けプロセス中の ID の使用

グローバル サービス プロファイルの関連付けプロセス中に、ターゲット サーバとドメインは、グローバル サービス プロファイルにアクセスします。

Cisco UCS Central は、通常の ID 解決を実行して、グローバル プール内のドメインまたはドメイン グループの適切な ID ブロックから ID を使用します。

移行または関連付け解除プロセス中の ID の使用

グローバル サービス プロファイルの移行または関連付け解除プロセス中に、ID の使用は次のように行われます。

- **認定されていない ID プール**：Cisco UCS Central では、すでに使用されている ID をグローバル サービス プロファイルから解除しません。
- **認定済みの ID プール**：グローバル サービス プロファイルの移行プロセス中に、Cisco UCS Central はグローバル プールで使用されている ID を再取得しようとします。これは、それらの ID が新しくターゲットとなったドメインまたはドメイン グループに対してまだ認証済みであることを前提としています。新しくターゲットとなったサーバが同じドメインにある場合、Cisco UCS Central は同じ ID を再取得します。新しくターゲットとなったサーバが異なるドメインまたはドメイン グループにある場合は、Cisco UCS Central はドメインの認定ポリシーを再評価します。前に取得した ID が認定ポリシーに適合していない場合、その ID は解除され、新しい ID が割り当てられます。

CHAPTER 15

認証

Cisco UCS Central の認証

Cisco UCS Central は、ローカルまたは LDAP ベースの認証をサポートします。TACACS+ や RADIUS などの他の認証タイプは、v1.4 以降でサポートされています。これより前のバージョンではサポートされていません。Cisco UCS Central を使用して、これらの認証タイプを運用管理ポリシーを通じて Cisco UCS Manager に設定できます。

（注） ローカル認証を使用している場合、パスワード文字に「$」は使用しないでください。

Cisco UCS Central では、ネイティブ認証の 1 つの定義済み形式（ローカルまたは LDAP）のみを有効にすることができます。Cisco UCS Central では、複数の認証ドメインから選択できます。Cisco UCS Manager とは異なり、現在は複数の認証領域の設定をサポートしていません。

Cisco UCS Central は、LDAP 連携およびユーザ認証用に、サードパーティの証明書および自己署名証明書もサポートしています。

認証

Cisco UCS Central は、Cisco UCS Manager GUI の認証モデルの設定を登録されたすべての Cisco UCS ドメインにわたってグローバル化できます。

Cisco UCS Central の v1.4 以降では、RADIUS または TACACS+ を認証領域として使用できます。それより前のバージョンでは使用できません。簡素化、および認証方式と定義の数を最小限にして一元化することを目指します。同様に、複数の認証方式と定義へのアクセスが必要な場合は、Cisco UCS Central ドメイン グループで認証方式マップと定義を作成する際の簡素化を目指します。

RBAC

RBAC（ロールベース アクセス コントロール）は、通常、LDAP や AD などのグローバルまたは企業レベルの認証にリンクされています。Cisco UCS Central では、アクセスの一元管理を適用することが推奨されます。

現在、中央認証とロール管理がない場合、ベスト プラクティスは管理者が Cisco UCS Central 内でロールベースのアクセスを定義することです。それをドメイン グループ階層のできる限り上位の運用ポリシーで定義します。

CHAPTER 16

ファームウェア管理

ファームウェア管理

グローバル ファームウェアの管理を設定して、ドメイン グループ内（v1.4 以前）またはファームウェアおよびハードウェア機能カタログの一貫したバージョンを実行するメンテナンス グループ（v1.5 以降）のすべてのドメインにポリシーを適用します。ドメイン グループまたはメンテナンス グループ内のすべてのドメイン間で一貫したインフラストラクチャ ファームウェアのバージョンを適用する場合、グローバル ポリシーの解決を有効にします。

ドメイン グループまたはメンテナンス グループが複数の Cisco UCS ドメインで構成され、グローバル ファームウェア管理の制御ポリシーに切り替えている場合、そのグループに変更される任意の運用（グローバル）ファームウェア ポリシーに注意します。Cisco UCS Central は、メンテナンス ポリシーで定義されているとおり、そのドメイン グループまたはメンテナンス グループのメンバであるすべてのドメインを、任意のサブドメイン グループとともにアップグレードしようとします。メンテナンス ポリシーのデフォルトの動作では、アップデートが発生する前にユーザの確認応答が必要です。確認応答をスケジュールするか、すぐに確認応答を実行することで、この動作をオーバーライドできます。

Cisco UCS ドメインのファームウェア管理

Cisco UCS ファームウェアのアップグレード スクリプトを使用するまで、Cisco UCS ドメインのアップグレードは手動プロセスでした。

Cisco UCS Manager の最新リリースでは、以前は手作業で行っていたタスクを自動で行えるようにファームウェアの自動インストール機能が含まれています。Cisco UCS Central は、複数の Cisco UCS ドメインでのファームウェアのアップグレードの自動化を支援するため、この新しい機能に基づいて作成されています。

ファームウェアには、いくつかのタイプがあります。

- **インフラストラクチャのファームウェア（A パッケージ）**：I/O モジュール、ファブリック インターコネクト、Cisco UCS Manager で実行されているイメージを参照します。
- **サーバ ブレードのファームウェア（B パッケージ）**：物理的な Cisco UCS ブレード サーバの BIOS、CIMC、アダプタ、およびコントローラで実行されているイメージを参照します。

（注） 現在、Cisco UCS Central では、ブレード サーバのエンドポイントの直接アップグレードはサポートされていません。ホスト ファームウェア ポリシーとグローバル サービス プロファイルの関連付けを使用して、ブレードまたはサーバ ファームウェアをアップグレードします。

- **ラックマウント サーバのファームウェア（C パッケージ）**：物理的な Cisco UCS の管理対象ラックマウント サーバの BIOS、CIMC、アダプタ、およびコントローラで実行されているイメージを参照します。
- **Cisco UCS Mini のファームウェア（E パッケージ）**：Cisco UCS Mini の一部である物理ブレード サーバの BIOS、CIMC、アダプタ、およびコントローラで実行されているイメージを参照します。

サーバ ファームウェアのベスト プラクティスは、アプリケーション レベルでの設定の一貫性を確保するためにサービス プロファイルの定義の一環として、ホスト ファームウェア パッケージを活用することです。

ファームウェア管理の推奨事項

サーバ ファームウェアの更新に関する暗黙的なメンテナンス ポリシーはありません。そのため、ベスト プラクティスは、サーバ ファームウェア バンドルの更新を規定するメンテナンス ポリシーを明示的に定義することです。

インフラストラクチャ ファームウェアの更新ではサーバが中断されます。したがって、グローバル サービス プロファイルを作成する際に、必ずユーザの確認応答の設定を有効にします。メンテナンス ポリシーでユーザの確認応答を使用して、タイミングの悪いサービスの中断を防止します。

ファームウェアの管理に関する次の問題を理解する必要があります。

サービスの低下と中断

各ファブリック インターコネクトが順番にリブートのサイクルを行わなければならないため、いずれの Cisco UCS インフラストラクチャ ファームウェアの更新でもサービスの低下が発生します。サービスの中断を避けるには、適切なアプリケーション レベルの可用性スキーム（Cisco UCS ファブリック フェールオーバー、高可用性（HA）、NIC ボンディング、ホストベースのストレージ マルチパス機能など）があることを確認します。

保留中の確認応答

ファブリック インターコネクトのリブートには、Cisco UCS Central 管理者からの明示的な確認応答が必要です。複数の UCS ドメインのドメイン/メンテナンス グループには、アップグレードしたくないドメインごとにポリシー解決の制御をローカルに切り替えることができます。これにより UCS ドメインのアップグレードの同時要求を防止します。その後、ポリシー解決の制御をグローバルに変更すると、アップグレード プロセスが続行されます。

デフォルトの動作では、続行する前に、すべてのファームウェア アップグレードを確認応答（infra-fw）し、リブート（fi-reboot）する必要があります。インフラストラクチャ ファームウェアのアップグレード ページで、Cisco UCS Central の進捗を確認します。

Cisco UCS Manager 内の個々の Cisco UCS ドメインで、[Operations] > [Firmware] > [FW Operations] の順に選択します。

ファームウェアのアップグレード プロセス

アップグレード プロセスには複数の確認応答が必要です。

Cisco UCS Central では、複数のアップグレードが並行して実行されます。Cisco UCS Manager に接続している場合、アップグレード時に Cisco UCS Manager へのこれらの接続がリセットされます。スタンドアロンの Cisco UCS Manager のアップグレードと同様に、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が完了するまでには約 1 時間ほどかかりますが、複数のドメインで並行して実行できます。ブレード サーバのアップグレードには、関与するサーバの数に応じて、およびホストをアップグレードする前に仮想ワークロードが移行（vMotion/Life Migration）を必要とするかどうかによって、さらに時間がかかる場合があります。

ファームウェアの管理はホスト ファームウェア ポリシーを補完できます。新しい Cisco UCS ドメインを初めてロードする際に、インフラストラクチャとホスト ファームウェアの両方の自動インストール プロセスを使用します。新しいドメインがすべての下位レベルのホスト ファームウェアにより最新の状態になっていることを確認してから、実稼働にリリースします。

ホスト ファームウェア パッケージとメンテナンス ポリシー

ホスト ファームウェア パッケージとメンテナンス ポリシーはどちらもドメイン グループと組織から表示と設定が可能です。

Cisco UCS Central で予期されている動作は以下のとおりです。

- グローバル サービス プロファイルは、ドメイン グループではなく、組織で定義されたホスト ファームウェア ポリシーを参照します。
- メンテナンス ポリシーに確認応答すると、Cisco UCS Central によって、ホスト ファームウェア パッケージ、メンテナンス ポリシー、およびその他の参照されるポリシーが Cisco UCS Manager から Cisco UCS Central にプルされます。
- ローカル サービス プロファイルは、ローカル ホスト ファームウェア ポリシーとローカル メンテナンス ポリシー、グローバル ホスト ファームウェア ポリシー、またはグローバル メンテナンス ポリシーのいずれかを参照できます。

ベスト プラクティスは、ホスト ファームウェア パッケージ、メンテナンス ポリシー、およびスケジュールを組織からのみ設定および使用することです。

CHAPTER 17

バックアップおよびインポート

Cisco UCS Central のバックアップ

Cisco UCS Central 設定のバックアップは定期的に実施する必要があります。定期的にバックアップしないと、運用ポリシーのドメイン グループ、および下位の個々の Cisco UCS ドメインへのマッピングの再構築を自動化する方法がなくなります。

Cisco UCS Central のバックアップ サイズが小さい（1 MB よりはるかに小さい）場合、UCS Central に対してバックアップと設定のエクスポートを 1 日に 1 回実行します。**Config-All**（論理）バックアップと **Full-State**（db）バックアップも使用します。

Cisco UCS Central 仮想アプライアンスからバックアップをオフラインで保存するには、**必ず**リモート コピーを使用します。また、カスタム定義したスケジュールで Cisco UCS Central のバックアップをスケジュールすることもできます。

Cisco UCS ドメインのバックアップ

Cisco UCS Central を使用した管理でも、頻繁に Cisco UCS のバックアップを作成する必要があることに変わりはありません。しかしこれは、個々のバックアップ操作の簡素化と自動化に役立ちます。

ドメイン グループごとにバックアップ ポリシーとエクスポート ポリシーを定義します。バックアップ ファイルのサイズはさまざまですが、個々の Cisco UCS ドメインの一般的なバックアップは 100 KB 未満で、頻繁にバックアップを行えるくらいの小ささです。（完全な状態のバイナリ バックアップは 2 MB 未満です）。

Cisco UCS Central はすべてのバックアップのオリジナル コピーを Cisco UCS Central アプライアンス内に維持します。また、遠隔地にバックアップのコピーを保存することもできます。

Config-All（論理）バックアップを使用して、Cisco UCS を毎日バックアップすることを検討してください。各 UCS ドメインに対し、**Full-State** バックアップと **Config-All** を実行します。また、カスタム定義したスケジュールで Cisco UCS Central のバックアップをスケジュールすることもできます。

ドメイン バックアップの制限

Cisco UCS Central とドメインには、2 種類のバックアップを設定できます。

- 完全な状態のバックアップ:データの回復に使用します
- 設定のエクスポート:論理構成の XML バックアップ

どちらのバックアップも、FTP サーバにリモート コピーを実行するオプションを適用できます。すべてのスケジュールされたバックアップ ジョブでは、障害による損失からバックアップを保護するため、リモート コピーが強く推奨されます。

リモート ファイル システムから UCS Central のバックアップのみをインポートできます。ローカル Cisco UCS Manager を使用して、リモートに保存されたドメイン バックアップをインポートします。

ローカル バックアップのグローバル参照

ローカルの Cisco UCS Manager レベルでバックアップすると、これらのバックアップには Cisco UCS Central で管理されているグローバル オブジェクトへの参照が含まれません。

Cisco UCS Central 内で、バックアップ ポリシーとエクスポート ポリシーを、Cisco UCS Central で排他的に管理されているバックアップ処理とともに使用します。Cisco UCS Central によってスケジュールされ、駆動される UCS ドメインのバックアップは、UCS ドメイン内のすべてのローカル オブジェクトをバックアップします。

CHAPTER 18

ハイ アベイラビリティ

高可用性クラスタ モード

Cisco UCS Central は、主にネイティブ ハイパーバイザを含まない展開にネイティブな高可用性（H/A）機能を提供します。通常は、ネイティブ ハイパーバイザを使用します（利用可能な場合）。ネイティブ ハイパーバイザ H/A が利用できないか、アクティブでない場合、Cisco UCS Central のネイティブ H/A クラスタリングを使用せずに、スタンドアロン モードで Cisco UCS Central を安全に実行できます。

ホスト ハイパーバイザで H/A をサポートしていない場合、一般的なベスト プラクティスは、Cisco UCS Central の H/A 機能を利用することです。

（注） 通常、Cisco UCS Central H/A とネイティブ ハイパーバイザを同時に実行することは推奨されません。

Cisco UCS Central はサービスを中断せずに一時停止を引き起こす可能性があることに注意してください。これは、Cisco UCS Central がデータ プレーンではなく、コントロール管理プレーンでのみ動作しているためです。Cisco UCS Central に登録されている Cisco UCS ドメインで Cisco UCS Central サーバに対する可視性が失われても、各 Cisco UCS ドメイン内のサービスは正常に機能し続けます。ただし、環境への設定変更には、Cisco UCS Central サーバを復元する必要があります。

（注） Cisco UCS Central がダウンしていて、管理のためにグローバル サービス プロファイルを編集する必要がある場合、Cisco UCS Manager で編集できるようにグローバル サービス プロファイルをローカライズすることができます。これは、Cisco UCS Central がダウンしているときにサービス プロファイルを編集する必要がある場合にのみ推奨されます。

クラスタ モードの Cisco UCS Central での H/A は、プライマリおよび下位の Cisco UCS Central VM と共有クラスタ化された 3 番目のディスクを使用して、Cisco UCS Central の単一の論理インスタンスを参照します。

また、ネイティブ ハイパーバイザ H/A 機能を利用することで、H/A を実現することもできます。この場合、Cisco UCS Central の H/A 機能は使用しないでください。これらは必要ありません。

真の DR 機能を求めている管理者は、すでにある可能性がある任意のバックエンド VM DR 機能を活用する必要があります。

次の 2 つのいずれかの方法を使用して、Cisco UCS Central での H/A を実現します。

- 方法 1:
  - 新しい Cisco UCS Central インスタンスを H/A クラスタとしてインストールする
  - スタンドアロン Cisco UCS Central を H/A クラスタに変換する
- 方法 2:
  - ネイティブ ハイパーバイザ機能を利用する
  - RDM クラスタリングまたは NFS クラスタリングを利用する

これらのいずれかの方法を使用する前に、『Installation and Upgrade Guide』を参照してください。

NFS クラスタ モードの推奨事項

NFS クラスタ モードで展開する際は、以下を確認してください。

- 両方の VM が共有ストレージ NFS サーバへのアクセス権を持つ個別の物理ホストにあること
- 両方の VM が同じバージョンの ESX または Hyper-V を実行していること
- 両方の VM が同じバージョンの Cisco UCS Central を実行していること
- 両方の VM が同じサブネット上にあること

クラスタ H/A モードでは、NFS サーバと 40GB 以上のボリュームを設定する必要があります。

1. 『Cisco UCS Central Installation and Upgrade Guide』に従って、NFS をエクスポートします。
2. NFS サービスを再起動します。
3. NFS サーバ ディレクトリの Cisco UCS Central VM へのマウントを妨げる可能性がある、NFS 上の任意のファイアウォール ルールを削除または変更します。
4. Cisco UCS Central のインストール時に、NFS サーバの IP アドレスを指定します。
5. NFS サーバのディレクトリを指定します。
6. 設定スクリプトを使用して、データベースとイメージをプライマリ VM から NFS に移行します。
7. 選択が完了したら、NFS サーバ ディレクトリをプライマリ ノードにマウントします。

スタンドアロン HA からの移行

既存のスタンドアロン Cisco UCS Central の実装から H/A 設定に切り替えることができます。また、RDM の実装から NFS ベースの実装に切り替えることもできます。必要な手順の詳細については、『Installation and Upgrade Guide 』を参照してください。

推奨事項

- Cisco UCS Central H/A オプションを検討している場合は、NFS ベースの H/A を使用することをお勧めします。
- VM スナップショットの中断、再開、または復元などの機能を使用している場合は、所有権が競合する共有ストレージを作成しないように注意してください。共有ストレージは必ずプライマリ VM にマウントします。プライマリ VM がまだアクティブの間に、セカンダリ VM が所有権を要求すると、クラッシュまたはクラスタ障害を引き起こす可能性があります。
- システムにネイティブ ハイパーバイザの高可用性機能がある場合は、それを利用して、スタンドアロン モードで Cisco UCS Central の展開のみを行います。
- プライマリ サイトで、すべてのドメインを HA 対応の Cisco UCS Central インスタンスに登録します。
- Cisco UCS Central インターフェイスを介して、Cisco UCS Central とすべての登録済み Cisco UCS Manager インスタンスのスケジュール バックアップを実行します。
- 障害が発生した場合、バックアップを通じて新しいサイトに Cisco UCS Central を復元できます。

（注） Cisco UCS Central はプライマリ データ パスに存在しないため、Cisco UCS ドメインの可用性に Cisco UCS Central は必要ありません。Cisco UCS Central はコントロール プレーンからドメインを設定、管理、表示するメカニズムです。

CHAPTER 19

一般的なベスト プラクティス

プラットフォーム エミュレータ

リスクを最小限に抑えつつ、Cisco UCS Manager と Cisco UCS Central を習得するための最適な方法は、プラットフォーム エミュレータを利用することです。

プラットフォーム エミュレータ（PE）は仮想マシンとして実行されていますが、Cisco UCS Manager と Cisco UCS Central の完全なインスタンスです。これらは Cisco UCS Management の管理情報ツリーとデータ管理エンジンを維持します。これらは、Cisco UCS XML API の使用をサポートします。また、実際の Cisco UCS ドメインの物理ハードウェア構成と論理構成の両方をインポートできます。

PE を使用することで、Cisco UCS 管理者は Cisco UCS 環境全体を効率的にモデル化できます。サンドボックスを使用して、実稼働中のドメインに影響を及ぼすことなく、すべての変更、テストやその他のあらゆることを設定できます。また、モデリングを使用して、正式な変更管理を Cisco UCS Central のトレーニング用に迅速に有効化することもできます。

Cisco UCS Central との統合をテストするために、PE の最新バージョンを使用していることを確認します。

一般的なベスト プラクティス

Cisco UCS Central の導入方法は、ブラウンフィールド環境またはグリーンフィールド環境のどちらを使用しているかに主に依存しています。

- グローバル運用ポリシー、グローバル障害およびインベントリ レポート、およびグローバル統計情報を、作業負荷プロファイルと既存の Cisco UCS の展開に関係なく、広く使用します。
- 100% グローバルに管理される新規導入では、通常、名前空間の衝突（競合）のリスクはないことを理解します。したがって、管理対象オブジェクトに「G-」プレフィックスを使用するといった注意は必要ありません。
- グローバルでのみ管理される新規ドメインへの新しい負荷を制限することを試みます。
- グローバル プール、ポリシー、テンプレート、ローカル サービス プロファイルを、ローカルでも管理されているドメインに混在しないようにしてください。これは、ローカル サービス プロファイルの作成と展開での名前の競合を回避することに役立ちます。ドメインにローカル オブジェクトとグローバル オブジェクトが混在している場合は、分離された組織構造を使用して、名前の衝突および競合の可能性を低減します。
- デフォルト オブジェクトはインポートしないでください。
- デフォルトのポリシー名よりも、ポリシーの内容を伝える名前を付けたポリシーを使用します。誰かが誤って名前の背後にあるプロパティ値を変更したり非表示にすることがあります。たとえば、デフォルトのスクラブ ポリシーは、通常、ディスク スクラブまたは BIOS 設定のスクラブには [no] が設定されていますが、これを誤って [yes] に変更してしまう場合があります。これは、ローカル サービス プロファイルがオペレーティング システムがインストールされたローカル ディスクを含むブレードから関連付けを解除されるという破壊的な影響を及ぼす場合があります。
- Cisco UCS Platform Emulator 使用して、導入手順をモデル化してテストします。

https://communities.cisco.com/ucs コミュニティ サイトには、Cisco UCS Central および導入に関する役立つコンテンツがあります。これには、Brad TerEick の有用なブログ Cisco UCS Central and My Existing Environment - How do I get there? も含まれます。

UCS Central のベスト プラクティス

- Cisco UCS Central のインストール ディスク（ローカルまたはリモート）の読み込み速度が 125 Mbps を超えていることを確認します。ディスクの読み込み速度は、UCS Central HA モード アーキテクチャにとって重要です。
- お使いのネットワークで、Cisco UCS Central と管理対象 UCS ドメイン間のネットワーク遅延が 500 ms 未満になることを確認します。
- Cisco UCS Central サーバとサーバが管理している任意のリモート UCS ドメイン間に 1.5 Mbps の帯域幅があることを確認します。
- Cisco UCS Central と登録済みのすべての UCS ドメインの毎日のバックアップと設定のエクスポートを実行します。リモート コピー機能を使用して、外部ファイル ディレクトリにファイルをコピーします。
- 特にアップグレードを行う前に、ハイパーバイザのスナップショットを利用して Cisco UCS Central を保護します。
- FQDN（完全修飾ドメイン名）を使用して UCS ドメインを必ず Cisco UCS Central に登録します。IP アドレスは使用しないでください。
- UCS ドメインを Cisco UCS Central に登録する前に、UCS ドメインと Cisco UCS Central に有効な時刻ソースが設定されていることを必ず確認してください。

- UCS ドメインにプッシュされたグローバル オブジェクトを含む Cisco UCS Central から UCS ドメインを登録解除しないでください。特定の UCS ドメインを Cisco UCS Central に再登録する予定がない場合にのみ登録を解除します。また、これは、Cisco UCS Central Engineering に裏付けられた Cisco TAC のガイダンスに従って実行します。
- グリーンフィールドとブラウンフィールドが混在している環境では、すべてのグローバル ID プール、ポリシー、テンプレート、およびサービス プロファイルに、「G-」などのプレフィックスを使って、グローバル オブジェクトをローカルの UCS ドメイン オブジェクトと区別するネーミングを検討してください。

ローカル アフィニティの問題

ポリシーを一元化して Cisco UCS Central で制御すると、特定の課題が浮上する場合があります。こうした課題は、ローカル リソースとコントロール ポイントを使用すると最適に管理できます。これらは、ローカル ドメインでは、ローカル アフィニティの問題と呼ばれています。一般的なアフィニティ ポイントは次のとおりです。

- 外部 IP プール（global-ext-mgmt）
- ブート ポリシー
- VLAN および VSAN

外部 IP プールのアフィニティ問題

外部 IP プール（global-ext-mgmt）には、物理ブレード サーバのアウトオブバンド管理用のアドレスが含まれています。しかし、Cisco UCS Central では、Cisco UCS Manager とは異なり、これらのアドレスをブレード サーバおよび CIMC と自動的にアソシエートすることはできません。

UCS Central では、ハードウェアに割り当てられた管理 IP アドレスがありません。そのため、Cisco UCS Central はグローバル サービス プロファイルに管理 IP アドレス プールを割り当てます。柔軟性を高め、グローバル サービス プロファイルを異なる管理サブネットを持つ UCS ドメインに移行するため、ID アクセス コントロール ポリシーを活用することを検討してください。

回避策

サービス プロファイルまたはテンプレートに関連付けられた管理 IP アドレスを使用して、Cisco UCS Central がグローバルな外部 IP プールを参照できるようにします。

（注） 外部管理 IP プールの動作は、Cisco UCS Central と Cisco UCS Manager では異なります。ID 範囲認定ポリシーをサポートする新しいグローバル サービス プロファイルは、グローバル管理 IP アドレスの割り当てで柔軟性と効率性を維持する能力が強化されています。

VLAN と VSAN のアフィニティ問題

VLAN のローカル アフィニティ問題を軽減するには、VLAN ID エイリアス機能を使用します。これは、ドメイン グループと組織の権限に基づいて、ドメインの VLAN ID を変換します。ドメイン グループと組織コンテキストの両方のマッピングが必要な VSAN エイリアシングは存在しません。

（注） VLAN エイリアスを使用するときは、実際の VLAN ID を名前に含めないでください。

VSAN の名前を作成する際に、それぞれのドメイン グループの名前を付加します。たとえば、VHBA テンプレートなどの参照を作成する場合は、“VSAN-DG” の名前ペアを使用します。

グローバル オブジェクトのローカルの可視性

グローバル オブジェクトを作成すると、それらは Cisco UCS Manager に自動的に表示またはプッシュされません。グローバル オブジェクトは、Cisco UCS Manager のナビゲーション ペインに自動的に表示されません。ただし、グローバル ID とグローバル ポリシーは、ローカル オブジェクトを作成または変更する際に、Cisco UCS Manager のドロップダウン メニューに表示される場合があります。

グローバル サービス プロファイルをサーバに展開すると、グローバル オブジェクトが Cisco UCS Manager に表示されます。これは、Cisco UCS Manager で実行されているローカル サービス プロファイルがグローバル オブジェクトを参照していることを意味します。展開時に、ローカルの Cisco UCS Manager は、グローバル オブジェクトとその従属オブジェクトの読み取り専用コピーを受け取り、それを GUI に表示します。

ハイパーバイザの競合

Cisco UCS Central は仮想アプライアンスとして動作するため、ホスト OS ハイパーバイザによって制御されるリソース共有の対象となります。

妥当なパフォーマンス特性のレベルを上げる方法の 1 つは、VMware または Hyper-V 環境でリソース プールを使用することです。リソース プールを使用すると、Cisco UCS Central の CPU とメモリの競合を回避または軽減することができます。

Cisco UCS Central が確実にサポートされるように、CPU とメモリの共有設定がどちらも [High] に設定された独自の専用リソース プールに配置します。詳細については、『Installation and Upgrade Guide』を参照してください。

ドメイン管理用の ID 範囲認定ポリシー

ID 範囲認定ポリシーを使用して、グローバル サービス プロファイルを Cisco UCS ドメイン間で移行する際に、Cisco UCS が適切な管理 IP のブロックを確実に使用するようにします。

ID 範囲認定ポリシーを使用して、IP のブロックをドメインまたはドメイン グループに割り当てることができます。ローカル サービス プロファイルを移行すると、新しい管理 IP が各 Cisco UCS ドメインへの関連付けに付加されます。

グローバル サービス プロファイル テンプレートの数を減らす

一部の組織では、Cisco UCS Central のアーキテクチャで作成し、維持しているグローバル サービス プロファイル テンプレートの数を減らす方法を常に探し求めています。

1 つの方法は、Cisco UCS および Cisco UCS Central の階層ポリシー解決機能を活用することです。一部の組織では、ダウンストリームの組織に基づいて ID を分離する必要性を正当化できないため、高いレベルに ID プールを配置しています。同様に、最も一般的な設定ポリシーも組織構造の上位に配置しています。

これらは、Cisco UCS および Cisco UCS Central のポリシー解決に依存しています。これにより、同じ名前のポリシーを組織の異なるレベルに存在させることができますが、これらのポリシーには異なる値を埋め込みます。そのため、これらが組織内のグローバル サービス プロファイルを作成またはインポートする際に、グローバル サービス プロファイルはその特定の組織に適した値を持つ特定の指定されたポリシーにアクセスします。

一般に、一意の LAN 接続ポリシーおよびストレージ接続ポリシーは、下位のより詳細なレベルで定義します。これらが異なる組織内で同じ名前を持つ限り、グローバル サービス プロファイルは正しい値を持つ適切なポリシーを使用します。

Cisco UCS Central をアップグレードする前に

Cisco UCS Central のアップグレードを行う前に、以下を行います。

1. 登録済みのすべての Cisco UCS ドメインを Cisco UCS Manager Release 2.1(2a) 以降にアップグレードします。Cisco UCS Manager Release 2.1 を使用している場合は、Cisco UCS Manager Release 2.1 ツリー内の最新のメンテナンスおよびパッチ リリースを使用してください。
2. Snapshot Manager を使用して、VM のスナップショットを取得して、元の VM の状態を維持します。
3. Cisco UCS Central の full-state バックアップと config-all バックアップの両方を作成します。両方にバックアップの状態が有効になっていることを確認し、これらのバックアップがオフラインで使用できることを確認します。

（注） バックアップ中、ローカル Cisco UCS ドメインでは Cisco UCS Central への可視性が失われますが、アップグレードが完了すると、状態が登録済みに戻ります。

4. Cisco UCS Central Release 1.5 にアップグレードする前に、すべてのインフラストラクチャ ファームウェア アップデートを完了します。インフラストラクチャ ファームウェアの更新ジョブのスケジュール情報は新しいリリースには転送されません。リリース 1.5 では、ドメイン グループではなく、メンテナンス グループのインフラストラクチャ ファームウェアの更新ジョブを作成します。

Cisco UCS Central のアップグレードの一環として、Cisco UCS ドメインの登録解除/再登録のサイクルは実行**しないでください**。

Cisco UCS Central のアップグレードに関するベスト プラクティス

1. アップグレードの互換性を確認します。Cisco UCS Manager と Cisco UCS Central のリリース ノートを参照してください。
2. Cisco UCS Central でどの操作も実行されていないことを確認します。アクションを実行している管理者がいないことを確認します。
3. Cisco UCS Central に保留中の確認応答がないことを確認します。
4. Cisco UCS Central をバックアップします。完全な状態のバックアップと構成のバックアップを実行します。これらをリモートでオフラインに保存します。
5. CLI からシャットダウン コマンドを使用して、Cisco UCS Central をグレースフル シャットダウンします。
6. シャットダウンした後、既存の Cisco UCS Central の状態のハイパーバイザ スナップショットを取得します。
7. UCS Central の新しいバージョンをダウンロードします。
8. Hypervisor Manager で、既存の Cisco UCS Central VM に新しい Cisco UCS Central ISO をマウントします。
9. Cisco UCS Central が ISO から起動するように、BIOS でブート順序シーケンスを編集します。
10. ISO から Cisco UCS Central を起動します。
11. アップグレード オプションを選択します。
12. アップグレードと自動リブートを完了します。
13. Cisco UCS Central のアップグレードが正常に行われたことを確認します。
14. Cisco UCS Central をバックアップします。完全な状態のバックアップと構成のバックアップを実行します。これらをリモートでオフラインに保存します。

これらのタスクの実行の詳細については、『UCSC Getting Started Guide』を参照してください。

Cisco UCS Central のアップグレード

『Product Installation Upgrade Guides』でアップグレード時に利用可能なすべてのリリース ノートを確認してください。

次のバージョンの互換性要件に注意してください。

- Cisco UCS Central 1.2(1a)以前では、Cisco UCS Manager 2.1.2 以降との通信のみをサポートしています。
- Cisco UCS Central の新機能の中には、Cisco UCS Manager の新しいバージョンでしか使用できないものもあります。たとえば、Policy Search は、Cisco UCS Manager 2.1(2a)以降で動作しますが、Policy Import は 2.2(1b)以降でのみ動作します。

最新の ISO アップグレード方法は、『Product Installation Upgrade Guides』に記載されています。

Cisco UCS Central のよく寄せられる質問（FAQ）

Q. 2 つのドメインからのインポートを比較して、異なっているかどうかを確認できますか。同じ構成だと思われる 2 つのドメインがある場合、両方をインポートして調べることはできますか。

A. いいえ。Cisco UCS Central では現在、ネイティブの Diff 関数はありません。これは今後のリリースで検討される可能性があります。Cisco UCS Central から技術サポート ログを作成し、ログ ファイルを抽出し、それを Diff 関数を実行する XML エディタまたはリポジトリにインポートして、2 つの設定を比較できます。

Q. Cisco UCS Central レポートを CSV または PDF 形式でエクスポートできますか。

A. はい。

Q. 組み込めるデータベースの大きさはどのくらいですか。ドキュメントには、データベースが組み込まれた最大 5 つのドメインが表示されますが、データベースがどのくらいの大きさなのかについては曖昧です。

A. 5 つのドメインで約 240 GB です。制限はありません。Cisco UCS Central では、最大 10,000 台のサーバをサポートできます。

Q. Cisco UCS Central では、VMware Site Recovery Manager（SRM）などの代わりのディザスタ リカバリ アーキテクチャをサポートしていますか。

A. いいえ。VMware HA、VM のスナップショット、複製、毎日のバックアップ、およびターゲットなどのハイパーバイザ HA ツールを使用します。バックアップはディザスタ リカバリの機能です。リモート コピーを設定します。FTP サーバなどの別のサーバ上にリモート コピーを保存します。Cisco UCS Central に障害が発生した場合、バックアップを使用して新しい Cisco UCS Central を展開できます。また、クラスタリングは使用せずに、単一の VM を使用します。

Q. Cisco UCS ドメインに VLAN または VSAN を提供するメカニズムとして、グローバル サービス プロファイルとサーバの関連付けを引き続き使用する必要がありますか。

A. いいえ。ローカル サービス プロファイルは、ローカルにする必要があるものに使用します。ターゲットをプッシュする場合、グローバル VLAN サービス プロファイルを使用します。グローバル VLAN および VSAN は、グローバル サービス プロファイルを削除してもドメインに留まります。現在は、Cisco UCS Central からドメインにグローバル VLAN または VSAN をプッシュするために CLI で使用できる API があります。SSH アプリケーションを使用して、Cisco UCS Central にアクセスしてこれらのタスクを実行します。

APPENDIX A

定義済みの UCS Central 内部プロセス

定義済みの UCS Central 内部プロセス

サービス名	説明
core-svc_cor_secAG	ローカル認証やリモート認証などの認証関連機能を実装します
identifier-mgr-svc_idm_dme	ID プールを管理し、システムに固有の ID を割り当てます
core-solr.sh	SOLR プロセス
resource-mgr-svc_sam_snmpTrapAG	リソース マネージャから SNMP トラップを送信します
central-mgr-svc_centralMgr_dme	Cisco UCS Central NBAPI プロバイダー、NBAPI を特定の DME に転送します
policy-mgr-svc_pol_dme	Cisco UCS Central ポリシーを管理します
identifier-mgr-svc_sam_snmpTrapAG	識別子マネージャから SNMP トラップを送信します
core-svc_cor_snmpTrapAG	管理コントローラから SNMP トラップを送信します
operation-mgr-svc_ops_dme	運用マネージャ DME
policy-mgr-svc_sam_pkiAG	ポリシー マネージャ DME に PKI 関連のサービスを提供します
core-httpd.sh	httpd プロセスを開始します
gch-call_home	Cisco GCH Call Home プロセス、callhome/smartlicense メッセージを Cisco Cloud Smartlicense Manager に転送します
service-reg-svc_sam_snmpTrapAG	service-reg から SNMP トラップを送信します

サービス名	説明
core-svc_cor_sessionmgrAG	Cisco UCS Central HA 実装のセッション監査
core-svc_cor_dme	管理制御の DME、Cisco UCS Central VM の設定を管理します
resource-mgr-svc_sam_cloudAG	GCH call home/スマート ライセンス アプリケーション ゲートウェイ
stats-mgr-svc_sam_snmpTrapAG	統計マネージャから SNMP トラップを送信します
service-reg-svc_reg_dme	別の DME と UCSM に登録サービスを実装します
operation-mgr-svc_ops_imgMgmtAG	運用マネージャのイメージ管理アプリケーション ゲートウェイ
resource-mgr-svc_rsrcMgr_dme	Cisco UCS Manager のインベントリが保持され、グローバル サービス プロファイルを管理するリソース マネージャ DME
core-tomcat.sh	tomcat プロセスの制御スクリプト
service-reg-svc_sam_controller	Cisco UCS Central HA サービスを実装する AG
operation-mgr-svc_sam_snmpTrapAG	運用マネージャから SNMP トラップを送信します
sam_cores_mon.sh	Cisco UCS Central コア ダンプ ファイルを監視および管理するスクリプト
core-svc_cor_controllerAG	Cisco UCS Central VM ポリシーを設定する AG
service-reg-svc_sam_licenseAG	ドメイン ベース ライセンスのライセンス AG
core-sam_nfs_mon.sh	NFS を監視するスクリプト
gch-xosdsd	GCH/smartlicense 機能を実装するためのインフラストラクチャ プロセス
policy-mgr-svc_sam_snmpTrapAG	ポリシー マネージャから SNMP トラップを送信します
stats-mgr-svc_statsMgr_dme	さまざまな Cisco UCS Manager ドメインから統計情報を集め、統計情報レポートを生成する統計マネージャ

APPENDIX B

UCS Central の通信：必要なポート

必須のポート

通常、既存のすべての Cisco UCS Manager ドメインの IP アドレスは、共通の管理ネットワーク上にあります。そうでない場合、Cisco UCS Central では、ユーザがすべて下位の管理ドメインへのルーティング アクセスを保証することが必要になります。Cisco UCS Central と登録済みのすべての UCS ドメイン間の継続的な通信のため、ファイアウォール、プロキシ、およびその他の次のポートへの読み書きアクセスを許可する必要があるものが設定されていることを確認します。

UCSM ドメイン v2.2(1b)以前で必要なポート

UCSM ドメイン v2.2(1b)以前を使用している場合は、次のポートを開きます。

ポート	値
LOCKD_TCPPORT	32803 – Linux NFS ロック。
MOUNTD_PORT	892 – Linux NFS マウント。
RQUOTAD_PORT	875 – Linux リモート クォータ サーバ ポート(NFS)。
STATD_PORT	32805 – Linux – NFS ファイル ロック サービスで使用 – ロック回復。
NFS_PORT	"nfs"(2049) – Linux NFS リスニング ポート。
RPC_PORT	"sunrpc"(111) – Linux RPCBIND リスニング ポート(NFS)。

ポート	値
HTTPS_PORT	“https”(443) – Cisco UCS Central から UCS ドメインおよび UCS Central GUI への通信（常に必要）。
HTTP_PORT	“http”(80) – Cisco UCS Central から UCS ドメインへの通信。このポートは設定可能で、フラッシュベースの Cisco UCS Central GUI でのみ必要です。
PRIVATE_PORT（843）	Cisco UCS Central のフラッシュベースの UI と Cisco UCS Central VM 間の通信に必要です。Cisco UCS Central VM とリモート UCSM ドメイン間の通信には不要です。新しい HTML-5 UI を使用している場合は、ポート 843 は必要ありません。

ポート 80 は古いフラッシュベースの UI の通信に必要です。Cisco UCS Central Release 1.4.1a の時点では、Cisco UCS Central 内のポート 80 を無効にすることはできません。ただし、ファイアウォール ルールを適用することで、Cisco UCS Central とのポート 80 トラフィックを拒否できます。

UCSM ドメイン v2.2(2c)以降のバージョンで必要なポート

UCSM ドメイン v2.2(2c)以降を使用している場合は、次のポートを開きます。

Port	値
HTTPS_PORT	“https”(443) – Cisco UCS Central から UCS ドメインおよび Cisco UCS Manager への通信（常に必要）。
HTTP_PORT	“http”(80) – Cisco UCS Central から UCS ドメインへの通信。このポートは設定可能で、フラッシュベースの Cisco UCS Manager でのみ必要です。
PRIVATE_PORT（843）	Cisco UCS Central のフラッシュベースの UI と Cisco UCS Central VM 間の通信に必要です。Cisco UCS Central VM とリモート UCSM ドメイン間の通信には不要です。新しい HTML-5 UI を使用している場合は、ポート 843 は必要ありません。

（注） ポート 80 は古いフラッシュベースの UI の通信に必要です。Cisco UCS Central Release 1.4.1a の時点では、Cisco UCS Central 内のポート 80 を無効にすることはできません。ただし、ファイアウォール ルールを適用することで、Cisco UCS Central とのポート 80 トラフィックを拒否できます。

UCSM に必要なポート

UCSM が Cisco UCS Central と連動するため、次のポートを開きます。Cisco UCS Central は次のポートにアクセスします。

Port	値
HTTPS_PORT	“https”(443) – Cisco UCS Central から UCS ドメインおよび UCS Central GUI への通信（常に必要）。
HTTP_PORT	“http”(80) – Cisco UCS Central から UCS ドメインへの通信。このポートは設定可能で、フラッシュベースの Cisco UCS Central GUI でのみ必要です。

ポート 80 は古いフラッシュベースの UI の通信に必要です。Cisco UCS Central Release 1.4.1a の時点では、Cisco UCS Central 内のポート 80 を無効にすることはできません。ただし、ファイアウォール ルールを適用することで、Cisco UCS Central とのポート 80 トラフィックを拒否できます。

Active Directory サーバに必要なポート

Active Directory サーバで次のポートを開きます。Cisco UCS Central は、AD サーバとの LDAP 連携にこれらのポートを使用します。

Port	値
LDAP Port 389	Microsoft Active Directory LDAP との統合と通信のために Cisco UCS Central が使用します
STARTTLS	LDAP over SSL/TLS をサポートするために Cisco UCS Central が使用します。ポート 389 も使用されます

APPENDIX C

テストおよび開発環境の構築

テストおよび開発環境の構築

独自のテストと開発環境を構築できます。独自の安全な環境を構築するため、これはオフラインで設定することをお勧めします。

1. UCS エミュレータをダウンロードし、テスト ラボにインストールします。
2. UCS Central をダウンロードし、テスト ラボにインストールします。
3. Cisco UCS Central をテストするテスト エミュレータを登録します。
4. Cisco UCS Manager から運用構成のエクスポートをインポートするか、実稼働環境に適合するように Cisco UCS Central を構築します。
5. Cisco UCS Manager から運用構成のエクスポートをインポートするか、実稼働環境に適合するように UCS ドメインを構築します。
6. ローカル サービス プロファイルをグローバル サービス プロファイルに移行するといった、シナリオと動作をテストします。
7. API に対して自動化と PowerTools スクリプトをテストします。

テストおよび開発環境の構築

APPENDIX D

オンライン リソース

オンライン リソース

- UCS コミュニティ：Tech Talk
- UCS エミュレータ
- DEVnet ラーニング ラボ
- UCS Central PowerTools
- UCS PowerTools
- Cisco dCloud
- UCS Central ドキュメンテーション
- UCS Tech Talk：UCS Manager ドキュメンテーション ビデオ

オンライン リソース