Cisco UCS Central のベスト プラクティス

1.1(1a) リリースの更新

改訂 2.05　　2013 年 8 月 20 日

目次

UCS Central 1.1(1a) リリース 3
概要/目的/対象読者/対象範囲 4
一般的な略称 4
インストールおよびアップグレードの前提条件 5
UCS Central 仮想マシン（VM）のシステム要件 5
UCS Central の UCS ドメイン（ポート、ファイアウォールなど）への管理アクセス 6
UCS Central のライセンス 6
用語 7
「ベスト プラクティス」 8
1. ドメイン グループ（DG）の設計 9
2. UCS Central 認証 10
3. 組織およびドメイン グループの階層化 11
4. 名前の曖昧さと解決 12
5. 登録と証明書 14
6. ID 管理 14
a) プールのサイジング 14
b) 重複の確認 15
c) グローバル プールへの移行 16
d) 新しいグローバル ID プールの作成 17
e) 既存の ID プールからの移行 18
f) ID 範囲の認定 19
7. グローバル運用ポリシー 20
a) 一般的なベスト プラクティス 24

b) 認証 24
c) モニタリング（SNMP、Syslog、Call Home） 24
d) DNS 管理 24
e) RBAC 25
f) 電源管理 25
g) 運用ポリシーのインポート 25
8. UCS Central の導入：アプローチと課題 26
a) UCSM Platform Emulator 26
b) 新規 UCS での展開（「既存への影響、依存性のない環境」） 26
c) 既存システムでの移行（「既存への影響のある環境」） 26
d) 個別環境の密接さ、親和性（ローカル アフィニティ）の課題 27
9. UCS Central のバックアップ 28
10. UCS ドメインのバックアップ 28
11. UCS Central のアップグレード 28
a) インプレース アップグレード 29
b) 新しい VM によるアップグレード 29
12. 統計情報データベースのサポート 30
13. UCS ドメインのためのファームウェア管理 31
a) サービスの品質低下と中断 31
b) 確認保留中 31
14. シスコサポート（TAC）への連絡 32
15. メモ（注意事項） 32
a) グローバル オブジェクトのローカル可視性 32
b) メンテナンス ポリシー（ローカルおよびグローバル） 33
c) UCS Central 1.0(1a) から 1.1(1a) までのホスト OS のバージョン 33
d) 外部統計データベースのバックアップ 33
e) UCSM に強制時刻同期が必要な場合 33
f) ハイパーバイザのコンテンションの回避 34
g) 高可用性クラスタ モード 34
16. 1.1(1a) における 2013 年 8 月時の既知の注意事項 35
a) 「ルート」DG の UCS Central 管理ポリシー 35

b) LDAP 認証 35
c) ロケールのグローバル組織のマージ 36
d) グローバル MAC/WWxN プールの導入 36
e) グローバル UUID プール 37
f) ドメイン グループ ポリシーからのドメイン グループの再割り当て 37
g) RBAC でサーバ プールのメンバーがマスクされない 37
h) UCS 障害の要約が空白になる場合がある 37
i) ホスト FW パッケージとメンテナンス ポリシー 38
j) VLAN が未参照で表示される 38
k) デフォルトの FCoE VLAN ID が VSAN の場合は「1」になる 39
l) VLAN と VSAN がローカルで持続する場合がある 39
m) ローカル UCS バックアップにグローバル参照がない 39
n) ローカリゼーションとグローバリゼーション 39
o) SDK のサポート 39
17. まとめ 39
18. 付録 I（登録のトラブルシューティング） 40
19. 付録 II（証明書のトラブルシューティング） 41

UCS Central 1.1(1a) リリース

UCS Central 1.1(1a) リリースは、グローバル化された UCS 環境に対応したグローバル ID、グローバル ポリシー、グローバル サービス プロファイルをサポートしたリリースです。このリリースは、Cisco UCS Manager 自体の提供以降、シスコのサーバ管理における最も重要な強化の 1 つです。この 1.1(1a) リリースでは、UCS 管理者がグローバル アイデンティティの管理、グローバル ポリシーの一貫性、およびグローバル サービス プロファイルのモビリティを利用できます。

UCS Central 1.0 リリース[1] で、以下が導入されました。

- グローバル インベントリ、障害、ログ
- グローバル ID プール（UUID、MAC、WWNN、WWPN）
- グローバル ファームウェア アップデート、グローバル バックアップ
- グローバル管理ポリシーと運用ポリシー

[1] UCS Central 1.0 リリース ノート:
http://www.cisco.com/cisco/web/support/JP/docs/UCS/UCSCentralSW/UCSCentralSW/RN/001/UCS_28314.html

この 1.1(1a)[2] リリースの代表的な機能として、以下が含まれています。

- グローバル ポリシー、グローバル サービス プロファイル、およびグローバル テンプレート
- 履歴レポート用外部データベースの統計情報
- クラスタ モードによる UCS Central 仮想マシンの高可用性の強化

拡張性の面では、UCS Central により最大 10,000 台のサーバを管理できます。これはドメインの規模に応じて、およそ 70 ～ 125 の UCS 管理ドメインに相当します。

さらに今後のリリースでは、拡張性を高め、機能の強化、現状の注意点/制約事項への対応を目標としています。

概要/目的/対象読者/対象範囲

Cisco UCS Central は、標準化、グローバル ポリシーの適用、および一貫したグローバル ID により複数の Cisco UCS ドメインの管理をシンプルにします。UCS Manager では単一の UCS ドメインをポリシーベースで管理できますが、UCS Central は世界中に存在する複数の各 UCS 管理ドメインをグローバル ベースで管理し監視することを目標とし、UCS の管理能力、業務の効率化、ポリシーベースの自動化をより強力に押し進めます。

このドキュメントは複数の UCS 管理ドメインを担当する管理者を対象としており、UCS Central の導入に関する手順、影響などについて解説しています。読者としては、UCS 管理者として十分な経験のある人を想定しています。このドキュメントは、UCS Central 製品リファレンス ガイドおよびドキュメント[3] を補完するドキュメントであり、それらに代わるものではありません。

一般的な略称

この文書では、以下の一般的な略称を使用します。

略称	正式名称
UCSM	UCS Manager
SP	サービス プロファイル（Service Profile）
LSP	ローカル サービス プロファイル（Local Service Profile）
GSP	グローバル サービス プロファイル（Global Service Profile）
DG	ドメイン グループ（Domain Group）

[2] UCS Central 1.1(1a) リリース ノート:
http://www.cisco.com/en/US/docs/unified_computing/ucs/release/notes/RN-CiscoUCSCentral_1-1.html
[3] UCS Central のすべての製品ダウンロードおよびドキュメントは次のリンク先からご利用いただけます。
http://www.cisco.com/en/US/products/ps12502/tsd_products_support_series_home.html

インストールおよびアップグレードの前提条件

UCS Central とその基本となっている UCS Manager のリリース バージョンには、次のバージョン互換性があります。

- UCS Central 1.0(1a) は UCSM 2.1.1 および UCSM 2.1.2 での連携をサポート
- UCS Central 1.1(1a) は UCSM 2.1.2 **とのみ**を連携をサポート

したがって、UCS Central を 1.1(1a) にアップグレードする前に、まず、登録されるすべての UCS ドメインを UCSM 2.1.2 にアップグレードする必要があります。

UCS Central のどのリリースを使用するにも、UCSM リリース 2.1.1 以降が必要となります。

UCS Central 仮想マシン（VM）のシステム要件

UCS Central は数千台のサーバを含む複数の UCS ドメインに対してモニタリング、設定、および管理を一元的に行います。このため、運用を円滑に行うために、UCS Central VM（主にディスクアクセス関連）に、最小限のパフォーマンスのしきい値を設定する必要があります。

基盤となる VM ストレージのサイズを 80 GB 程度に設定する必要があります。共有ストレージには最低でも 40 GB の容量が必要です（H/A クラスタ モードが有効になっている場合）。
UCS Central は、すべてのファームウェア バンドルのイメージ リポジトリとして機能します。いずれの UCSM リリースでも、製品画像をダウンロードし、ローカルに保存する場合、全リリース（インフラストラクチャ、ブレードおよびラックのバンドル）のサイズは 1.5 GB になります。

UCS Central VM 内の空き容量のモニタリングは、CLI でのみ表示できます。VM コンソール（GUI ではなく）からログインして、「`scope monitoring; show storage`」と入力すると、VM 内のディスクの使用率を表示できます。

UCS Central は高速のデータストア（できれば高速 SAN で提供されるデータストア）に展開する必要があります。

UCS Central 1.0 と 1.1(1a) では、動作基盤となる VM 構造が以下のように大幅に変更されています。

- 4 個の vCPU（コア）
- 12 GB のメモリ
- VM 仮想ハードウェア バージョンのフォーマットがバージョン 7 から 8 に変更（VMware のみに該当）

UCS Central の UCS ドメイン（ポート、ファイアウォールなど）への管理アクセス

一般的に、既存のすべての UCS 管理ドメインの IP アドレスは、共通管理サブネットまたは VLAN に存在しています。上記に該当しない場合でも、UCS Central から配下のすべての管理ドメインへのルーティング アクセスができれば、UCS Central は機能します。このため、UCS Central と配下のすべての UCS ドメインとの間の通信を途切れなく行えるように、ファイアウォール、プロキシなどが以下のポートへの読み取り/書き込みアクセスを許可するように設定しておく必要があります。

LOCKD_TCPPORT=32803
MOUNTD_PORT=892
RQUOTAD_PORT=875
STATD_PORT=32805
NFS_PORT="nfs"(2049)
RPC_PORT="sunrpc"(111)

また、これらのポートのファイアウォール セッション タイムアウトの制限に、非アクティブによって切断されるセッションがないか見直す必要があります。インストール前の前提条件の一覧は、『UCS Central Deployment Guide』[英文] を参照してください。

UCS Central のライセンス

UCS Central のライセンスでは、最初の 5 個の UCS ドメインまでは無償で利用できますが、サポートは別途必要です。また、最初のドメインを登録後、120 日間の「トライアル期間」があります。

標準的な注文手順で最初の 5 個の UCS ドメイン管理に有効なライセンス（“L-UCS-CTR-INI=”）を購入します。最初のライセンス費用は無償ですが、サポートは含まれていません。6 個目以降のドメインの追加ライセンスは、“L-UCS-CTR-LIC=”を使用して購入します。

ライセンスをアクティブ化しなかった場合は、追加ドメインが登録できないだけでなく、UCSM でエラーが発生し、ドメインのトライアル期間が終了しているというメッセージが表示されます。

1.0(1a) リリースではライセンス要件と制限は特にかけられていませんでした。1.1(1a) リリースでは、ライセンス要件と制限が有効になっています。

用語

以下の定義の表は、命名規則と用語を順守しています。

用語	説明
UCS Manager	UCSドメインを管理する組み込みソフトウェア
UCSドメイン	UCS Manager に管理されるリソースの集まりであり、UCS Central のクライアント
UCS Central	グローバルな制御および可視性を提供するため、複数のグローバルデータセンターに UCS 管理ドメインを拡張する製品
ドメイン グループ（Domain Group）	複数のドメインから構成されるグループの名前 グループ内の全ドメインに関係する運用ポリシーをこのレベルで定義できる
サブ ドメイン グループ（Sub Domain Group）	ドメイン グループの子グループ 親グループからプロパティを継承するサブ ドメイン グループ内のドメイン用に固有のローカル ポリシーを設定できる
未グループ化ドメイン（Ungrouped Domains）	どのドメイン グループにも属さないドメイン
ドメイン全体（Domain-wide）	UCSドメイン全体に共通する、または反映されるプロパティおよび設定（過去には、UCSM 内で「グローバル」と**誤って**呼ばれていたこともある）。
ローカル	単一の UCS Managerドメイン内で所有され、存在するオブジェクトを指す言葉。たとえば、ローカル ポリシーやローカル プールなど。
グローバル	UCS Central 内で所有され、存在するオブジェクトを指す言葉。たとえば、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。
ローカル化（Localize）	グローバル コンテキストから何かをローカル コンテキストに移動すること。たとえば UCS Central のポリシーを UCSドメインでインスタンス化するなど。
グローバル化（Globalize）	UCSドメインから何かを UCS Central に移動すること。たとえば UCS Manager で定義されたポリシーを UCS Central に移動すること。たとえば運用ポリシーをインポートするなど。[4]
登録（Register）	UCS Manager が UCS Central に接続するための初期プロセス。
登録解除（Unregister）	UCS Central 管理から UCSドメインを意図的に削除すること。
切断（Disconnect）	UCS Manager と UCS Central の間の接続が意図せずに切れること。

[4] サーバ/ネットワーク/ストレージ ポリシーをインポートする機能は今後のリリースで提供する予定。

一時停止（Suspend）	UCS Central と UCS Manager の間の管理コミュニケーションが一時的に中断されるアクション。「登録解除」操作とは異なる。
一時停止モード（Suspended Mode）	UCS Manager が UCS Central に登録されているが、両者の間に管理コミュニケーションがない状態。
保留解除（Resume）	UCS Central と UCS Manager の間の管理コミュニケーションが再確立されるアクション。

「ポッド」、「クラスタ」、「ブロック」という用語の使用を避け、「ドメイン」を使用しています。単一の UCS Manager でこれまで使用されてきた用語は、複数 UCS をグローバルに管理するコンテキストの UCS Central では、その用法を再度確認しておく必要があります。たとえば、UCSM 2.1 より前は、VLAN は単一ドメイン内では「グローバル」と称されていました。将来的には、名称、用語、コンテキストの一般的な理解が不可欠になります。

「ベスト プラクティス」

「ベスト プラクティス」という用語は、教義ではなく、一連のガイドラインや推奨事項を指します。唯一の本来の「ベスト プラクティス」とは、利用者の特定の運用要件でベストに機能するものです。

柔軟性、適応性、および制御は、UCS Manager の特徴のすべてであり、UCS Central の目標であり続けています。UCS Central 管理モデルは、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。管理権限は UCS Central に「強く」集中し、その制御と影響の範囲は非常に広いものです。予期していないサービスの中断は、推奨事項を順守しなかった結果である可能性があります。UCS Central を導入し、展開する場合は、これをよく理解してください。以下を強く推奨します。

- 展開前にできる限りモデル化し、テストすること。
- グローバル コンフィギュレーションの変更に慎重であること。

UCS Central は UCS Manager に代わるものではありません。UCS Central は、ポリシー定義を一元化し、複数の UCS ドメインで使用できるグローバル ID プールを作成するための手段です。時とともに UCS Central を通じてより多くの機能が利用できるようになっても、UCS Manager は UCS ドメインを直接管理するためのインターフェイスであり、ポリシーの終端および解決手段であり続けます。

1. ドメイン グループ（DG）の設計

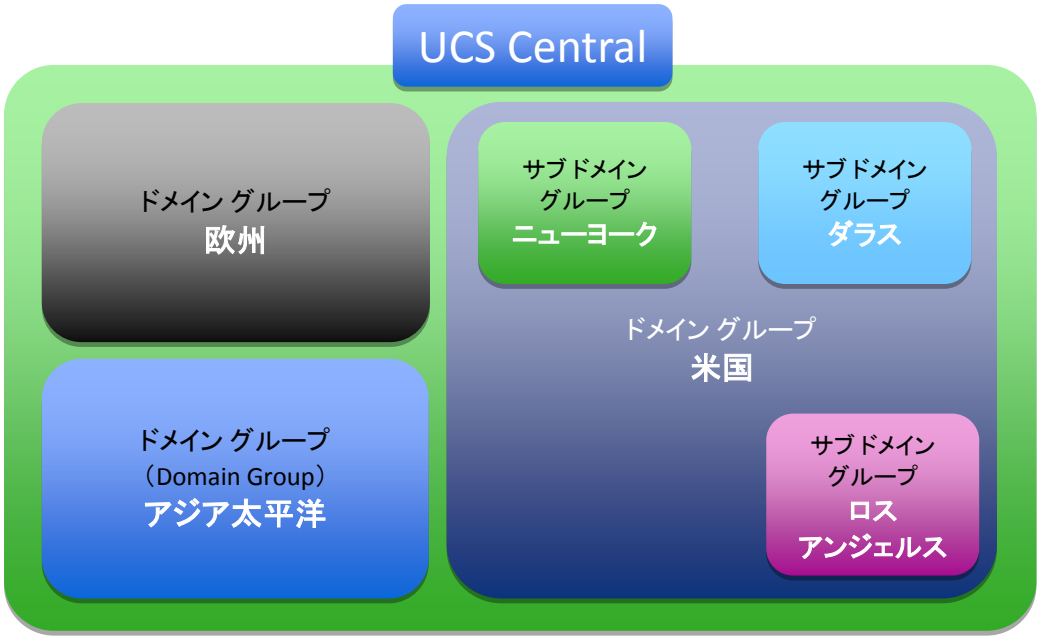
ドメイン グループ（DG）の階層設計は、多くの場合、設計における最も重要な意思決定になります。これに関して、正しい方法も間違った方法もありません。この機能の目的は、利用者の特定の環境と管理設計の選択を最もよく反映させることです。ドメイン グループ（DG）について、次の特性を理解する必要があります。

- ドメイン グループ（DG）は個々の UCS ドメインを任意にまとめたものです。グループ化設計は UCS Central 管理者に委ねられます。特定のドメイン グループに親和性をもたらすのは個々の UCS ドメインのコンテキストではありません。実際（とても重要なことですが）、個々の UCS ドメインのコンテキストには「ドメイン グループ」に関してどのようなコンセプトも観念も存在しません。DG は純粋に UCS Central の構成概念です。
- UCS ドメインは同時に複数の DG に所属することはできません。1 つのブレードを複数のサーバ プールに入れられるのとは異なり、1 つの UCS ドメインは同時に 1 つの DG にしか所属できません。
- デフォルトでは、すべての UCS ドメインが登録時に「未グループ化ドメイン グループ」に属します。未グループ化 DG のドメインは、ローカルの UCS 管理者がグローバル ポリシーのレベルにオプトインしたとしても、グローバル ポリシーが適用されることはありません。
- ポリシーは DG ごとに定義され、その DG 内のすべてのドメインに適用されます。DG では運用グローバル ポリシーが解決されます（適用されます）。
- UCS ドメインを DG 間で移動させることができます。ただしドメインを DG 間で移動させると、新しいポリシーによってはドメインが悪影響を受ける場合があります。UCS ドメインは DG から自身のポリシーを解決します。新しいドメインが追加されると、グローバル ポリシーが適用され、それがサービスに影響を与える場合があります。
- ドメインを新しく登録する際、認定ポリシーに基づいて DG に「自動追加」することができます。ドメイン グループ ポリシー認定はプール ポリシー認定と同じような仕組みで機能します（[Equipment（機器）] -> [UCS Domains（UCS ドメイン）] -> [Policies（ポリシー）]）。
- グローバル ポリシーは DG 階層内のどこででも定義できます。したがって、下位の DG ポリシーで定義されたポリシーを上書きできます。
- ドメインを新しい DG に移動する際、古い DG でバインドされていたポリシーを削除（またはリセット）する必要はありません。新しいポリシーで古いポリシーを上書きするまで、古いポリシーは有効なままになります。古いポリシーが新しいバインド ポリシーで上書きされない場合、古いポリシーは「非バインド」ポリシー[5] として有効です。
- ポリシーをより細かく制御するために、サブドメイン グループを作成して階層化することができます。サブドメインをどの程度使用するかは、異なるサブドメインを管理するために必要な追加の作業量を考慮して決定する必要があります。

[5] ホスト パック、メンテナンス ポリシー、スケジュール、ファームウェア配布バンドル（Infra, B, C）など、参照ベースで解決されるポリシーは、新しいドメイン グループに存在しない場合は落とされます。ポリシー制御（ローカル、グローバル）で解決されるポリシーのうち、ロール、ロケール、トラスト ポイントなどのように名前が付いたポリシーは、新しいドメイン グループに存在しない場合は落とされます。

DG パーティショニングのベースとして役に立つと思われる例を以下に示します。

- 地理、タイムゾーンなど
- 組織、部門など
- 製品の工程（製造、開発、テスト/QA、など）
- ネットワークドメイン（内部、外部など）



ドメイン グループの階層の例

運用ポリシーの設定と展開を簡単に行うには、ドメイン グループを使用します。ドメイン グループの階層化は、運用上の困難な課題に最適な場合にのみ実行します。

2. UCS Central 認証

UCS Central バージョン 1.1(1a) は、ローカル[6]と LDAP ベースの認証のいずれもサポートしています。現在、TACACs+ や RADIUS などのほかのタイプのネイティブ認証は UCS Central ではサポートされていません。UCS Central は、瞬時にアクティブになる（ローカルまたは LDAP の）ネイティブ認証の 1 つの定義済み形式のみをサポートしています。UCS Central は現在、UCS Manager のようなログイン処理時に認証形式を選択する機能をサポートしていません。

[6] ローカル認証を使用する場合は、パスワード文字として「$」を使用しないでください。

現在、UCS Central は、LDAP スキーマの変更[7]を必要とする LDAP 属性ベースの認証のみをサポートしています。現在 UCSM でサポートされている LDAP グループ マッピングに対する UCS ロール、UCS 認証プロバイダー グループ、あるいは、ローカル、RADIUS、TACACs+、LDAP の組み合せのような複数の認証スキーマは UCS Central ではサポートしていません。設定オプションでは、現在、LDAP スキーマ(例:説明)で定義されたユーザ クラスの既存の属性を使用するか、UCS Central ユーザの UCS ロールおよびローカル定義を入力するための新しい属性を作成して LDAP スキーマを拡張します。各ユーザを LDAP で変更し、必要とされる適切なロールとローカル定義を追加する必要があります。以下に、各ユーザに定義された LDAP 属性に追加する必要がある構文の例を示します。

```
shell:roles="<role-X>,<role-Y>" shell:locales="<locales-X>,<locales-Y>"
```

パラメータの「role-X」と「role-Y」は認証されるユーザに適用される UCS Central のロールを示し、「locale-X」と「locale-Y」は、ロールを適用する UCS Central 内のロケールを示します。

複数の UCS ドメインにわたる認証またはその他の運用ポリシーをグローバル化する場合は、「ルート」ドメイン グループでなく、ドメイン グループ内のそれらのドメインをグループ化することがベスト プラクティスです。UCS Central は、「ルート」DG から認証、DNS、タイム ゾーンなどの独自の運用ポリシーを解決します。そのため、UCS Central とは異なる定義の、さまざまな運用設定のサブドメイン グループを作成する必要があります。これらのサブドメイン グループで定義された運用設定は、これらの設定をグローバル化するようオプトインしている UCS ドメインにローカルに適用されます。

3. 組織およびドメイン グループの階層化

UCS Manager は、「組織」構造を通じて反映され、事実上、階層化されています。UCS Central では、階層「組織」構造がグローバルなスコープになっています。

UCS Central の DG 構造も階層型です。DG が UCS Central と対照的である重要な違いの 1 つは、ローカル UCS ドメインは DG 内の可視性がないことです。

ベスト プラクティス

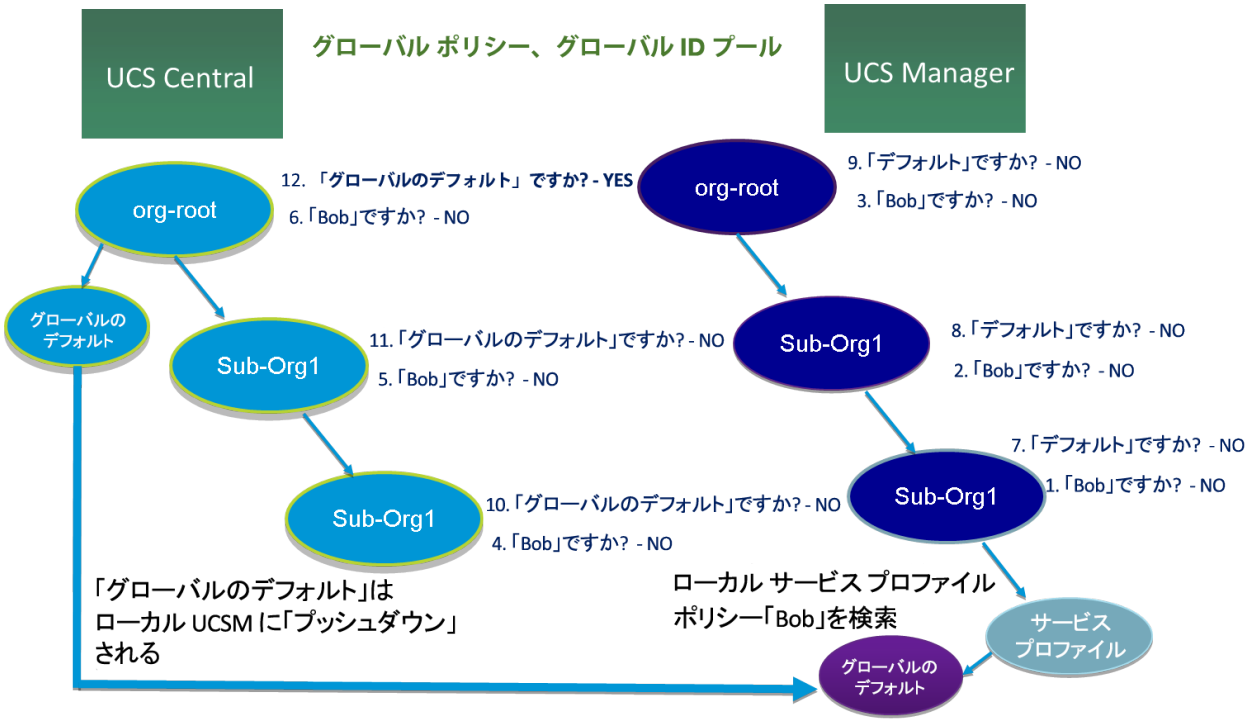
「組織」と DG の両方にとってのベスト プラクティスは、エンタープライズの論理(組織)と物理(DG)のセグメンテーションが最も反映されるように階層を利用することです。「org-root」または「root」DG にあるすべてのプール、ポリシー、またはサービス プロファイルは、すべてのドメインに対するグローバルな適用可能性と可視性を持つようになっていることを確認します。「root」でポリシー(ローカルまたはグローバル)を作成すると、予期していなかった広範に及ぶ(かつ望ましくない)結果をもたらす可能性があることを認識しておいてください。

[7] UCS Manager バージョン 1.3 以前で必要だったものと同様

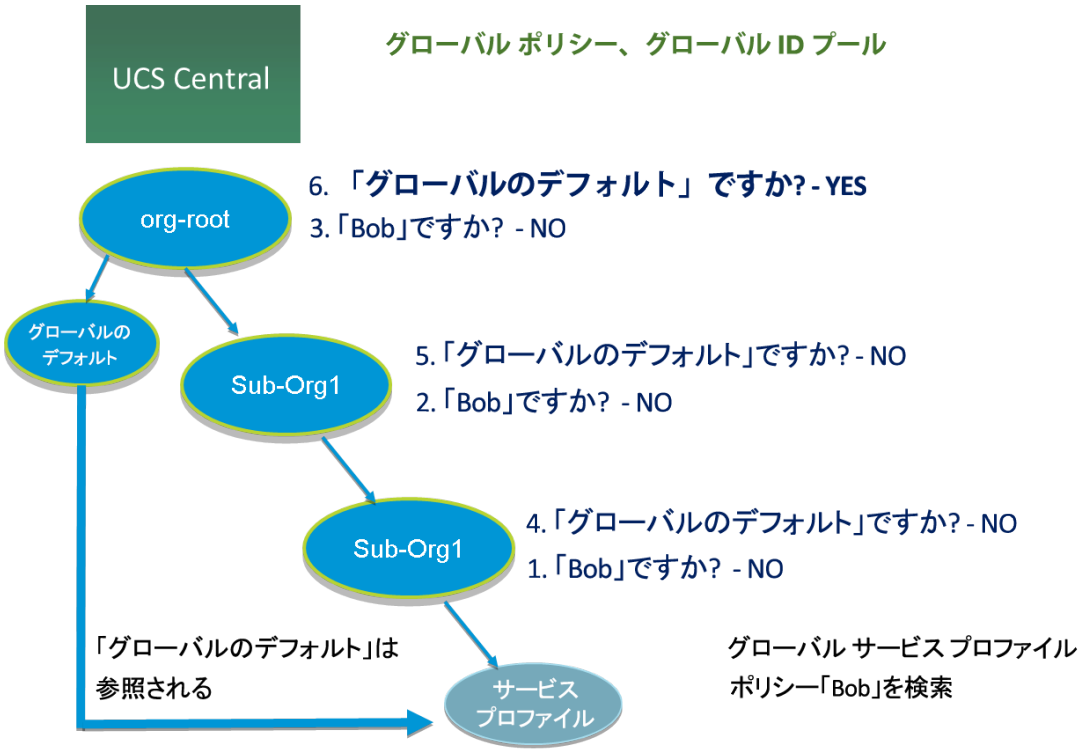
4. 名前の曖昧さと解決

UCSM 内でも、UCS Central 内でも、オブジェクトの命名の制限を少なくすると、曖昧さにつながる可能性があります。プールやポリシーは、UCSM 内の管理オブジェクトに結び付けられているため、ベスト プラクティスを除いては、同じオブジェクト「名」がローカルとグローバルの両方のスコープを持つことを防ぐものがありません。ポリシーまたはプール名がサービス プロファイル、vNIC、または VHBA で指定されている場合、UCSM では明確に定義された「名前解決プロセス」が順守されます。プールとポリシーの両方について、グローバル名よりもローカル名が優先されます。ローカル管理のオブジェクトは、指定された「名前」は次の順序で解決されます。

1. ローカル組織に存在し、定義されたオブジェクト名を使用する --- または…
2. すぐ上の親組織からローカルの「rog-root」までの間に存在し、定義されたオブジェクト名を使用する --- または …
3. グローバル組織に存在し、定義されたオブジェクト名を使用する --- または …
4. すぐ上のグローバル親組織からグローバル「org-root」までの間で定義されたオブジェクト名を使用する。
5. ローカル組織から「org-root」までの間の「デフォルト」のオブジェクトに対応する値を使用する。
6. グローバル組織から「org-root」までの間の「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する。



ローカル サービス プロファイルのポリシー「Bob」という名前の階層による名解決順序の例



グローバル サービス プロファイルのポリシー「Bob」という名前の階層による名解決順序の例

ベスト プラクティス

曖昧さを避けるためのベスト プラクティスは、管理者がローカルとグローバルのコンテキストで同じ「名前」を作成したり、使用したりしないことです。曖昧さを避けるには、グローバル ポリシーとプール名に一意のプレフィクス(例:A 側ファブリックにバインドされたすべての vNIC に「G-MAC-A」や「Global-MAC-A」)を設定します。または、明示的に定義されたプールとポリシーを必ず使用するようにし、「デフォルト」や「グローバル デフォルト」の名前を一緒に使用しないことです。

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 プール、WWPN プール、およびほとんどのポリシー	デフォルト	グローバル デフォルト
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	デフォルト	global-iscsi-initiator-pool
WWNN ID	node-default	global-node-default

5. 登録と証明書

登録は、UCSドメインとUCS Centralが信頼性の高い通信パスを確立するためのプロセスです。UCSMとUCS Central間の通信には、HTTPSと署名入り証明書が使用されます。このため、UCSMとUCS Centralの間で、システム時刻が同じになっている必要があります。

登録の前に、UCS Centralとローカルの UCSドメインが共通の NTP サーバを指し、それぞれの時計がすべて同期していることを確認してください。

登録および証明書の問題のトラブルシューティングの詳細については付録 I および II を参照してください。

6. ID 管理

グローバル ID 管理では、マルチドメイン管理の最大の課題の 1 つである、システム ID（MAC、WWxN、UUID）の一意のアドレス管理を扱います。以前は、UCSM のベスト プラクティスとして、「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を推奨していました。ただし、この方法でも手動による作業が必要で、エラーが発生することもありました。

UCS Central では、すべての UCSドメインにすべての ID プールをグローバルに定義し、アクセスできます。サービス プロファイルの割り当ては、すべての UCSドメインでの ID に一意であり、重複しないことを保証できます。

グローバル ID プールは「org」構造に属しています。UCS Central の「運用ポリシー」とは違い、グローバル プールは DG が終端ではありません。グローバル ID プールの範囲は、UCS Central 内の org 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。このとき、DG 内の区分は無視されます。

ベスト プラクティス

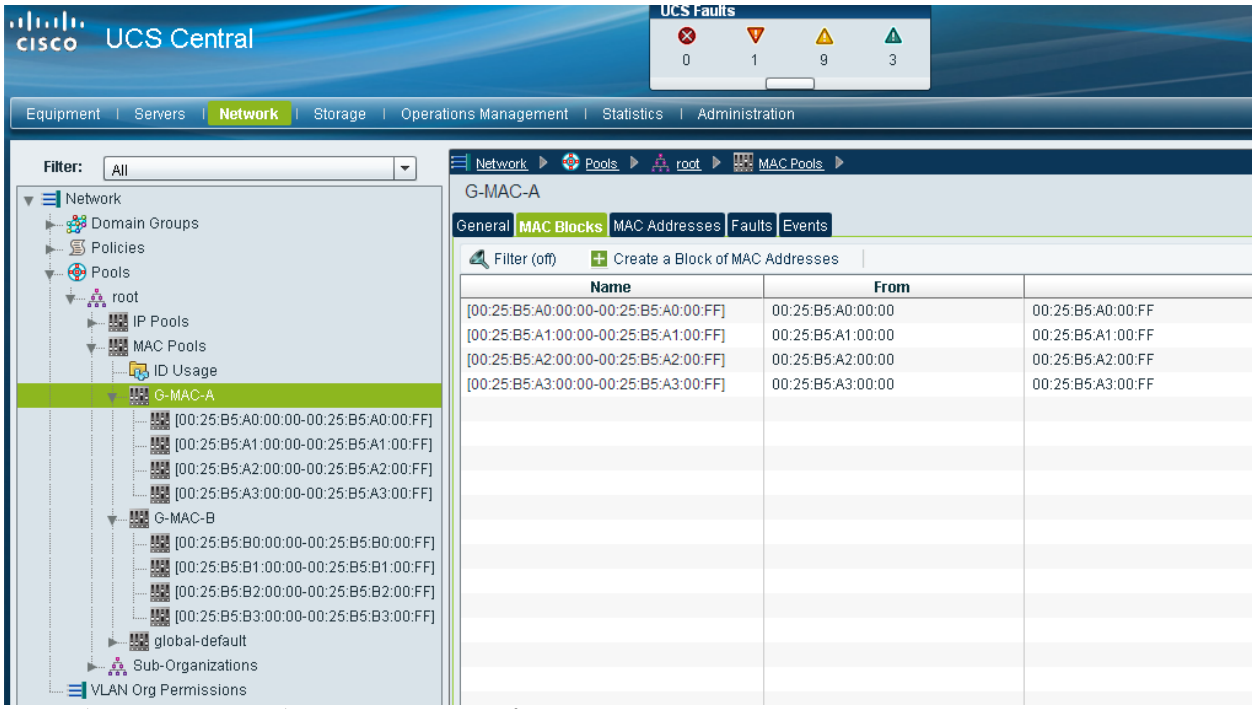
UCS Central を展開する際のベスト プラクティスは、新しい UCSドメインの展開のためのグローバル サービス プロファイルとともに、グローバル ID を導入することです。

a) プールのサイジング

管理するオブジェクトの数を最小限に抑える方法の 1 つに、個々のプールを大量に作成するのではなく、多くのブロックを持つプールを少数作成する方法があります。

既存の UCS ベスト プラクティスとして一般的なのは、対応する A 側と B 側のプール名に、A 側のトラフィックなのか、B 側のトラフィックなのか区別できるように MAC/WWPN アドレス範囲の上位バイトに「A」または「B」を埋め込む方法です。このモデルを UCS Central に拡張して、このようなプール構造の下に複数のブロックを作成します。各ブロックの最適なサイズは、256 アドレス（0xFF）[8] です。

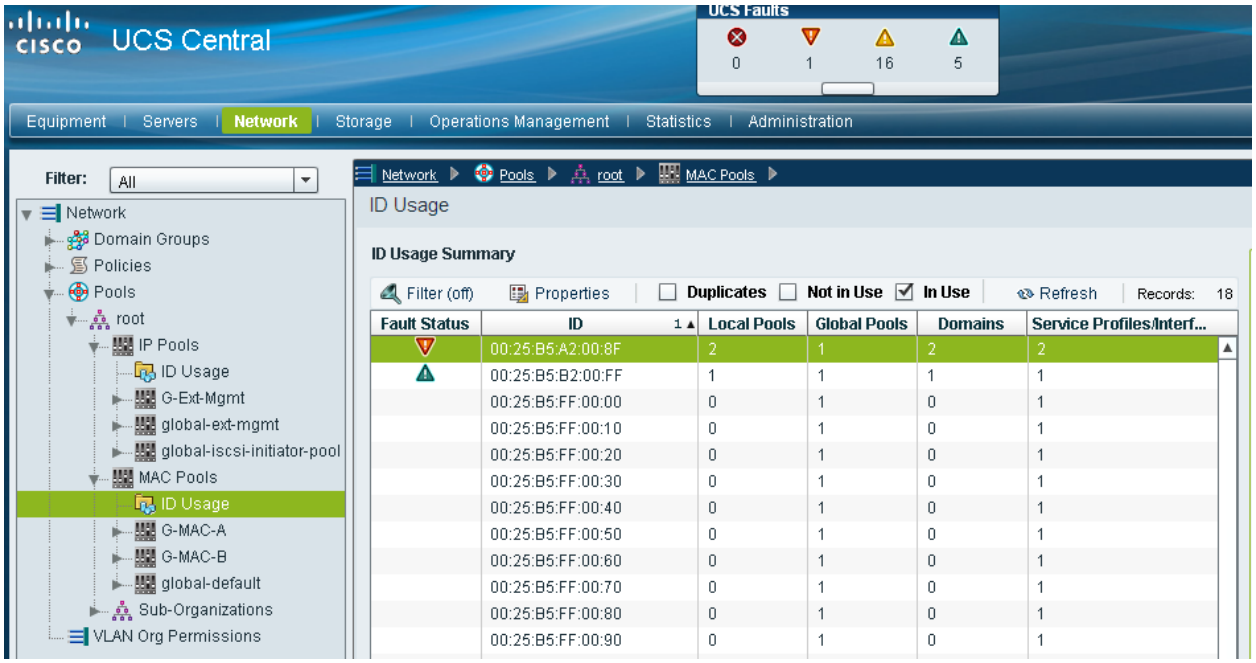
[8] UCS Central では、すべてのプール（UUID、MAC、WWxN）の最大ブロックサイズを 999 アドレス（0x3E7）とします。



複数ブロックを持つグローバル MAC プール（A 側、B 側）の例

b) 重複の確認

UCS Central では、ID の重複使用を検出できます。
すべてのプール タイプ（UUID、MAC、WWxN）で、複数の UCS ドメインをまたいで存在する重複 ID を [ID Usage Summary（ID 使用サマリー）] で表示できます。重複 ID は、複数のサービス プロファイルに存在する場合は [Major（重要）]、複数のローカル プールに存在する場合は [Warning（警告）] というフラグで重大性を表します。
ローカル ID プールの使用量を表示する方法は、個々の ID を選択し、対応するドリルダウンの詳細（ローカル プールおよびローカル サービス プロファイル）を右側に表示することです。



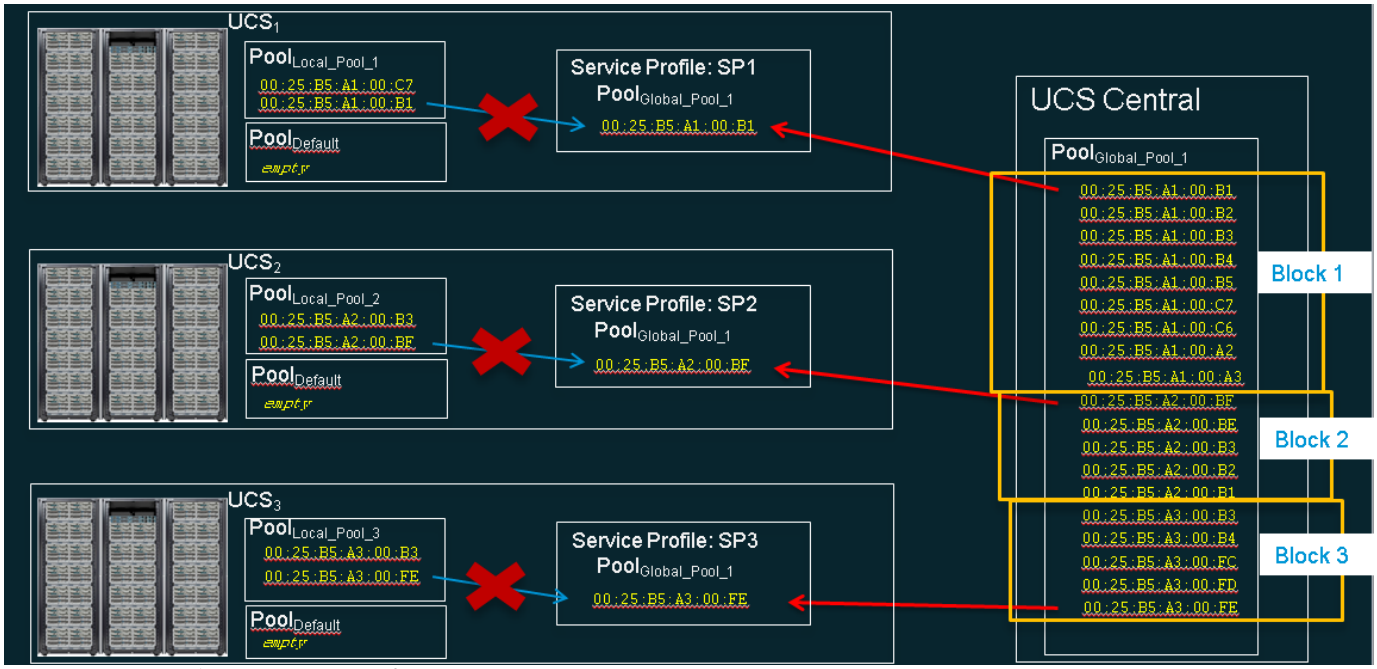
重複 ID の検出例

c) グローバル プールへの移行

現在、ローカル ID プールと呼ばれているローカル サービス プロファイル（LSP）をグローバル ID プールを使用するように再設定できます。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、通常サービスが中断されます。ただし、UCS Central は Global ID プールへの移行を簡易に行えるように設計されており、移行の結果、同じ ID を割り当てることになってもサービスは中断されません。[9]

グローバル ID を使用する LSP は、ID の一意性が保証されますが、グローバル サービス プロファイル（GSP）のモビリティを利用できません。グローバル ID を使用する LSP はローカル ドメインに存在し続けます。次のバージョンの UCS Central では、LSP を GSP に移行する機能が提供される予定です。

[9] これに関する UCS 2.1(2a) および UCS Central 1.1(1a) の既知の問題については、「注意」の項を確認してください。不具合報告 ID CSCud44377 により、残念ながらサービスの中断が発生します。この不具合が解決されるまでは、ローカル サービス プロファイルをグローバル プールに移行しないでください。



ローカルからグローバル ID プールへの移行

d) 新しいグローバル ID プールの作成

既存の UCS のお客様が複数のドメインを持っている場合は、「ドメイン ID」を ID プール範囲[10] の上位バイトに埋め込むなどのベスト プラクティスを通じて複数ドメイン ID の問題に対処することが理想的です。前の項ではグローバル プールへの移行を取り上げました。しかし、以前のローカル ID の使用と、異なる方法でグローバル ID を完全に区別したいと考えている管理者もいます。「ドメイン ID」を埋め込んでいたのとは別の方法で、これを行うことができます。たとえば、MAC ID のローカル ID メソッドが「00:25:B5:**3A**:FE:ED」(**3** はドメイン ID、**A** はファブリック インターコネクトに対応) だった場合、グローバル ID メソッドは「00:25:B5:**A0**:AB:BA」となり、ローカル ID 規則とは異なる ID シグネチャを提供します。

[10] 重複する ID があるサイトでは、これらの問題に加えて、グローバル サーバ管理に関する問題にも対処する必要があります。重複する ID に対する対処方法は、このドキュメントの対象外のため取り上げません。

e) 既存の ID プールからの移行

グローバル ID プールの移行時に LSP に同じ ID を維持するには、対応するローカル ID プールの上位セットとなるグローバル ID プールを構築します（つまり、グローバル ID プールには、ローカル ID プール内に現在存在するすべての ID ブロックが含まれる必要があります）。ベスト プラクティスは、ファブリックに関して「G-MAC-A」や「G-WWPN-B」のような「A/B」命名方法を、MAC および WWPN プールに採用することです。グローバル ID プールを作成した後は、管理者はグローバル ID プールを参照するようにサービス プロファイルを変更できます。まだ割り当てられていない場合は、以前にローカル ID プールで使用していたものと同じ ID を UCS Central が自動的に割り当てます。これにより、サービスの中断が避けられます[11]。

ID スペースが分割済みで、重複がまったく存在しない場合の導入手順は次のとおりです。

1. UCS Central に新しい ID プールを作成します。名前は曖昧さのないものにして、プール名のプレフィクスとして「Global」または「G」を付加します。MAC および WWPN プールの場合、プール名に「-A」または「-B」を末尾に付加します。
2. ローカル プールの ローカル ID ブロックごとに、グローバル プールに対応する ID ブロックを再作成します。
3. 既存のテンプレート（サービス プロファイル、VNIC、VHBA）を変更して、対応するグローバル ID プール名を参照するようにします。
4. 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。
5. ローカル プールの各ローカル 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」をベースにする VNIC/VHBA の場合、ID の参照先をグローバル ID プールに変更すると、その後に作成、管理されるオブジェクトはすべて、新しいグローバル ID プールを参照する必要があります。これは「初期テンプレート」の特性です。

「更新テンプレート」にバインドされる VNIC/VHBA の場合は、ID の参照先をグローバル ID プールに変更すると、テンプレートにバインドされる既存の管理対象のオブジェクトはすべて、新しいグローバル ID プールを参照する必要があります。既存の管理対象のオブジェクトの ID が存在し、グローバル プールで未使用の場合、この移行による、再設定、再起動、あるいはサービスへの影響は発生しません。

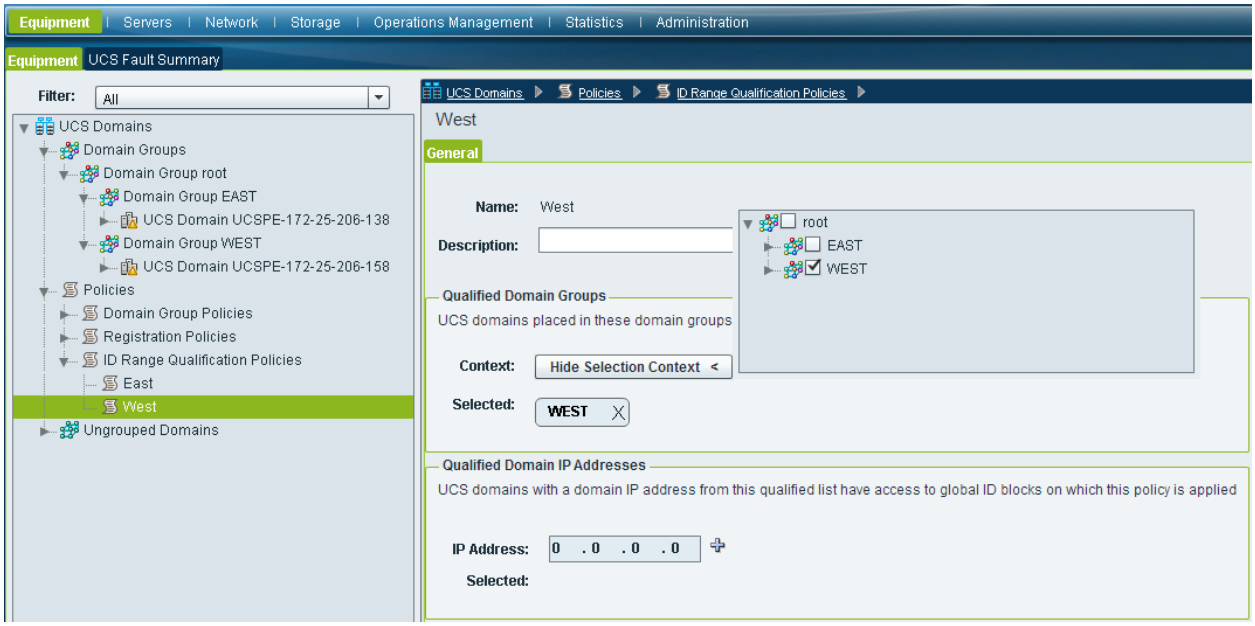
[11] 1.0(1a) および 1.1(1a) リリースでは、この方法でグローバル プールを移行するとサービス中断が発生します。この問題は、不具合報告 ID CSCud44377 として特定されており、UCSM リリース 2.1(3) で解決される予定です。

テンプレートにバインドされていない vNIC/VHBA については、サービス プロファイルのプール名がグローバル プールを参照するように変更され、その既存の 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 プロファイルが新しい ID を取得します。これにより再設定、再起動、およびサービスへの影響が発生します。ID がまだ使用されていない場合は、その ID が保持され、再構成やサービスへの影響を引き起こすことなく、グローバル プールを参照します。

「ext-mgmt」と「iscsi-initiators」の IP アドレスもグローバル プールで管理できます。同様に、既存のドメインの現在の割り当ては [Network（ネットワーク）] -> [Pools（プール）] -> [Org] -> [IP Pools（IP プール）] -> [ID Usage（ID 使用状況）] で表示できます。

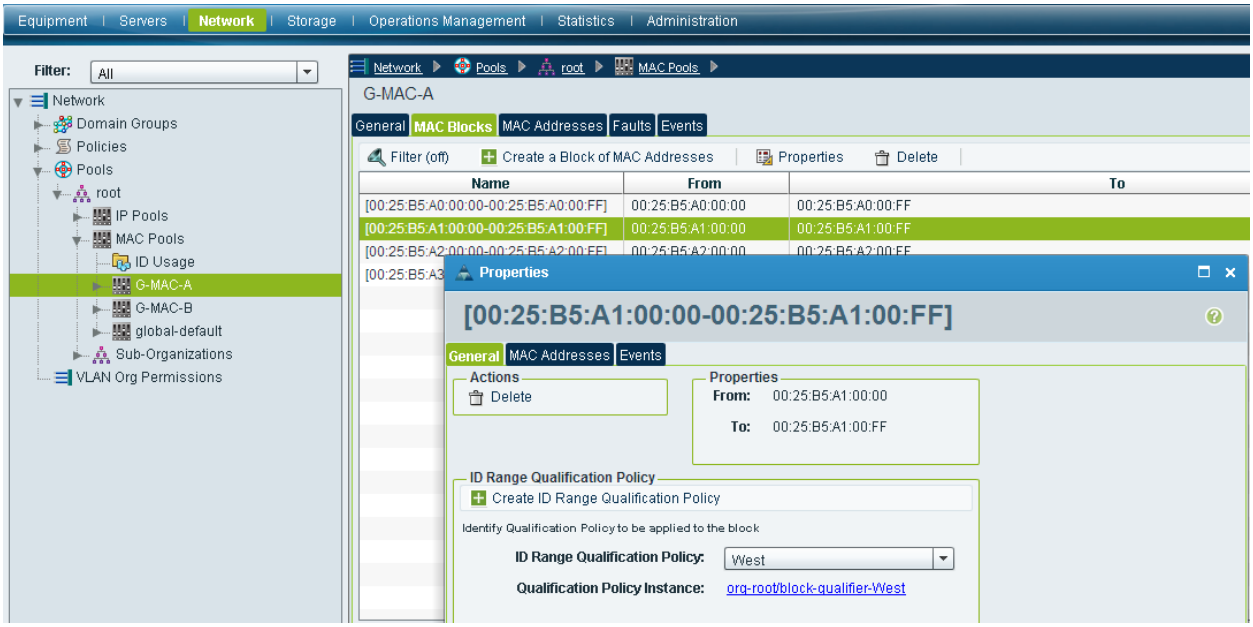
f) ID 範囲の認定

UCS Central では、分割されていない状態では、プールから ID を使用しているすべてのドメインでなく、特定の DG 内にあるローカル サービス プロファイル用のプール内の ID ブロックを分離する機能を提供します[12]。このように、特定の DG の 1 つ以上のドメインが ID の個別の範囲を使用するようにできます。これを下の図に示します。



ドメイン グループの ID 範囲認定ポリシーの作成

[12] グローバル サービス プロファイルの場合は、ID 範囲の認定は利用できません。



ID ブロック内の ID 範囲認定の参照

7. グローバル運用ポリシー

この項では、グローバル運用ポリシーについて説明します。(サービス プロファイル指向のポリシーではありません)

UCS Central は複数の UCS ドメインにグローバル運用ポリシーを提供しますが、ローカルの UCS マネージャがグローバル ポリシーに参加するかどうかは「オプトイン」で選択できます。UCS Central は、ローカルの管理者から委任されない限り、グローバル ポリシーの制御権を「奪う」ことはありません。ローカルの管理者は、後からでも、定義されたポリシーのグローバル管理から「オプトアウト」することで制御権を「取り戻す」ことができます。簡単に言うと、UCS Central を導入しても、UCS ドメインの管理モデルが必ずしも大幅に変更されるわけではありません。

すべての管理ポリシーはデフォルトでローカル ドメインによって制御されます。その状態は、次の 3 つのことが実行されるまで維持されます。

1. ローカル ドメインを UCS Central に登録する。
2. ローカル ドメインを UCS Central の DG に追加する。
3. ローカル ドメインの管理者が、定義されたポリシーを明示的に「ローカル」から「グローバル」レベルに格上げする。

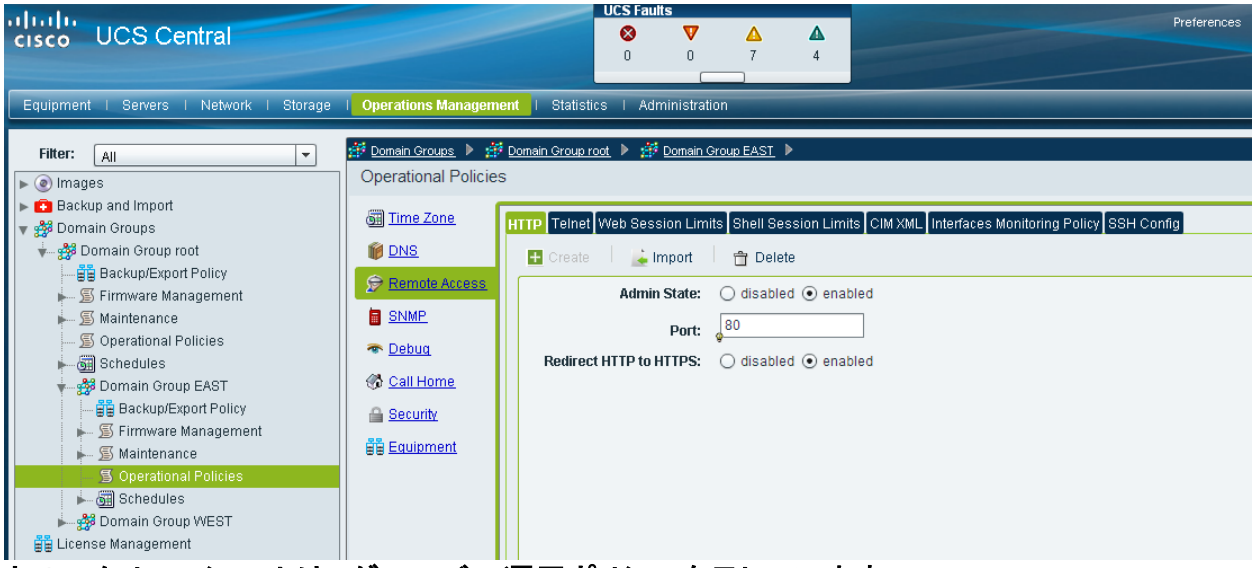
ポリシーの格上げは、他のポリシーに依存せずに行うことができます。たとえば、インフラストラクチャおよびカタログ ファームウェア管理をグローバル化しても、障害ポリシーはローカルで管理し続けることができます。[Admin（管理者）] -> [Communication Management（通信管理）] -> [UCS Central] で表示されるポリシー オプションはすべて依存関係がありません。

ポリシーがローカルからグローバルに変更されると、ポリシー定義は UCS Central のレベルで変更できるようになります。これは、ドメイン間で一貫性を確実にするためです。ただし、管理者はいつでもポリシーをローカル レベルに戻すことができます。ベスト プラクティスとしては、ローカルとグローバル間のポリシーの移行を最小限に抑えることです。

ベスト プラクティス

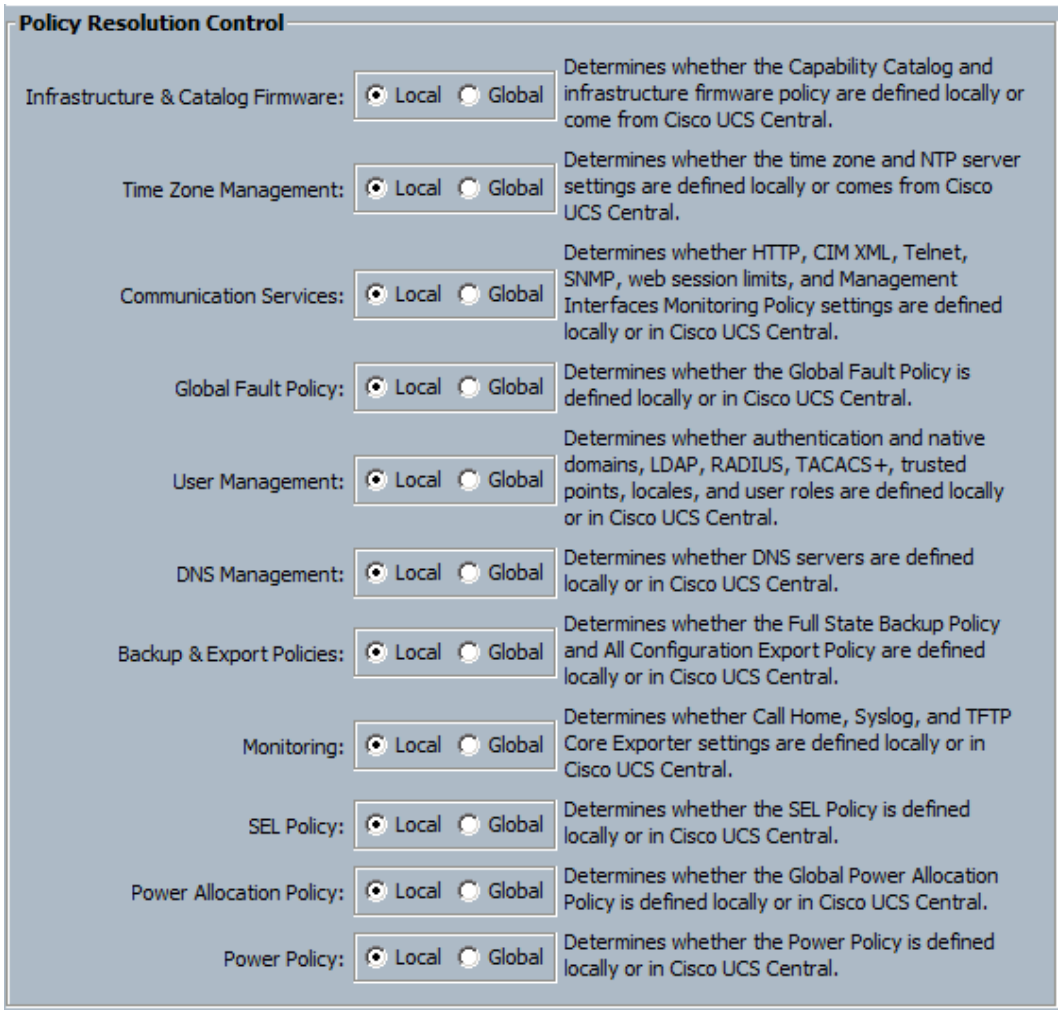
ベスト プラクティス全体として、グローバル ポリシーを広範囲に導入する前に、デフォルトであるローカルのポリシー レベル状態で利用し、これに慣れ、理解するのがいいでしょう。グローバル ポリシーの導入は、使い方に慣れたところで、個々のポリシーごとに段階的に行うべきです。

UCS 管理者は、可能な限り、一貫したポリシーと一元的なポリシーの適応を活用する機会を徐々に増やしていくことをお勧めします。グローバルな一貫性とポリシーの適応は、UCS Central の重要なアーキーテクチャの目標の 1 つです。ポリシーの定義と設定を UCS Central 内で統合することにより、ローカル UCS 管理者の管理上の負担が軽減されます。ポリシーの定義と管理をより上位の中央レベルで行うと、管理上の拡張性がさらに促進されることを留意ください。一般的なベスト プラクティスとして、できる限りポリシーはシンプルに設計し、ポリシー定義を一元化することを管理者は心がけてください。



上のスクリーンショットは、グローバル運用ポリシーを示しています。

下のスクリーンショットは、運用ポリシーのポリシー解決コントロールをどのように「グローバル化」できるかを示しています。



UCS Manager の参照	UCS Central の参照	UCSM GUI ナビゲーション
インフラストラクチャ & カタログ ファームウェア	[Operations Management（運用管理）] -> [DG] -> [Infrastructure Firmware（インフラストラクチャ ファームウェア）]	[Equipment（機器）] -> [Firmware Auto Install（ファームウェア自動インストール）]
タイムゾーン管理	[Operational Policies（運用ポリシー）] -> [DG] -> [Time Zone（タイムゾーン）]	[Admin（管理者）] -> [タイムゾーン管理（Timezone Management）]
通信サービス	[Operational Policies（運用ポリシー）] -> [DG] -> [Remote Access（リモート アクセス）]	[Admin（管理者）] -> [通信管理（Communication Management）] -> 通信サービス
グローバル障害ポリシー	[Operational Policies（運用ポリシー）] -> [DG] -> [Debug（デバッグ）] -> [Global Fault Policy（グローバル障害ポリシー）]	[Admin（管理者）] -> [Faults/Events/Audit（障害/イベント/監査）] -> [Settings（設定）]
ユーザ管理	[Operational Policies（運用ポリシー）] -> [DG] -> [Security（セキュリティ）]	[Admin（管理者）] -> [User Management（ユーザ管理）]
DNS 管理	[Operational Policies（運用ポリシー）] -> [DG] -> [DNS]	[Admin（管理者）] -> [Communications Management（通信管理）] -> [DNS Management（DNS 管理）]
バックアップ/エクスポート ポリシー	[Operational Policies（運用ポリシー）] -> [DG] -> [Backup/Export Policy（バックアップ/エクスポート ポリシー）]	[Admin（管理者）] -> [All（すべて）] -> [Backup and Export Policy（バックアップとエクスポートのポリシー）]
モニタリング	[Operational Policies（運用ポリシー）] -> [DG] -> [Call Home **and** Debug（Call Homeとデバッグ）]	[Admin（管理者）] -> [Faults/Events（障害/イベント）] -> [Syslog] [Faults/Events（障害/イベント）] -> [Settings（設定）] -> [TFTP Core Exporter Communications Mgmt（TFTP コア エクスポータ コミュニケーション管理）] -> Call Home
SEL ポリシー	[Operational Policies（運用ポリシー）] -> [DG] -> [Equipment（機器）] -> [SEL Policy（SEL ポリシー）]	[Equipment（機器）] -> [Policies（ポリシー）] -> SEL ポリシー
電源割り当て	[Operational Policies（運用ポリシー）] -> [DG] -> [Equipment（機器）] -> [Global Power Allocation Policy（グローバル電源割り当てポリシー）]	[Equipment（機器）] -> [Policies（ポリシー）] -> [Global Policies（グローバル ポリシー）] -> [Global Power Allocation Policy（グローバル電源割り当てポリシー）]
電源ポリシー	[Operational Policies（運用ポリシー）] -> [DG] -> [Equipment（機器）] -> [Power Policy（電源ポリシー）]	[Equipment（機器）] -> [Policies（ポリシー）] -> [Global Policies（グローバル ポリシー）] -> [Power Policy（電源ポリシー）]

上記の表は、UCS Central と UCS Manager の対応する参照を示しています。「UCSM GUI ナビゲーション」欄は、ポリシーが UCS Central でグローバルに解決するように設定され、ドメインがドメイン グループに追加されると、GUI がグレー表示になる箇所を示しています。

a) 一般的なベスト プラクティス

ベスト プラクティス

ドメイン グループ階層を利用し、定義する運用ポリシーの数を最小限に抑えます。運用ポリシーは、分割の必要性がないもの（たとえば、「DNS」、「タイムゾーン」、「Call Home」など）と、分割する可能性があるもの（たとえば、「ファームウェア管理」）に分類できます。管理者は、中断のない共通ポリシー設定として、できる限り DG 階層の上位に配置するようにしてください。同様に、中断の可能性のある運用ポリシーは、DG 階層のできるだけ下位に配置します。

b) 認証

現在、認証ドメインとスキームの設定は、UCS ドメインごとに個々に行っています。UCS Central ではすべての UCS ドメインに対して認証の設定をグローバル化できます。

グローバル化が望まれ、適切であれば、異なる認証設定に基づいて DG を定義できます。

一般的なベスト プラクティスは、シンプルさを目指し、できる限り認証スキームや定義の数を減らして集中管理することです。同様に、複数の認証スキーム/定義へのアクセスが必要な場合は、UCS Central ドメイン グループへの認証スキーム/定義のマッピングを行う際、シンプルな構成を目指します。

c) モニタリング（SNMP、Syslog、Call Home）

一般的に、システムの健全さとモニタリング（SNMP、Syslog、Call Home など）はすべて、共通グローバル ポリシーの対象になり得ます。最もシンプルにこれを実現するには、SNMP、Syslog、および Call Home のポリシーを運用ポリシーとして DG 階層のできる限り上位に定義します。下位 DG 内のすべてのドメインは、これらのグローバル ポリシーの定義を継承します。

d) DNS 管理

通常、DNS 管理はグローバルまたは企業レベルで定義されます。このため、DNS「ドメイン」名と DNS サーバがグローバル ポリシー管理の対象となりやすく、通常、DG 階層の運用ポリシーのできる限り上位で定義します。

e) RBAC

RBAC は通常、LDAP/AD など、グローバル/企業レベルの認証とリンクします。UCS Central では、できる限りアクセスの一元的な管理として強化を続けることが、ベストプラクティスです。

現状で、一元的な管理の認証とロール管理が行われていない場合は、管理者は UCS Central 内でのロール ベースのアクセスをベスト プラクティスとして、DG 階層の運用ポリシー内のできるだけ上位に定義してください。

f) 電源管理

電源管理に関するポリシーは 2 つあります。

- 「グローバル電源割り当てポリシー」シャーシ レベルで制限を適用するか、個々のブレード レベルで手動で上書きするか決定します。
- 「電源ポリシー」物理的 AC 電源の「N+1」、「グリッド」、または「非冗長」のシャーシ レベルの設定です。

一元管理でのポリシー定義では、おそらく「電源ポリシー」が最も適しています。

ただし、「グローバル電源割り当てポリシー」の方が環境および場所の条件に細やかに対応できる場合があります。例:

- ラックあたりの電源容量がデータセンターや場所ごとに異なる。
- 場所によっては、電源グループを活用し、所定のデータセンターのレイアウトに関して、複数のラックを対象とした電源制限を設けている。

「電源ポリシー」は、多くの場合ローカルの制約に最も依存します。広範囲に及ぶポリシーを作成してラックごとに電力を制限するというような定義方法が最もシンプルです。ただし、その実用性はサイト固有で、一般化が難しいものになります。

g) 運用ポリシーのインポート

ベスト プラクティス

[Operational Management(運用管理)] タブにある [Operational Policies(運用ポリシー)] では、多くのポリシーに既存のドメインからポリシー定義をインポートするというオプションがあります。これはローカルで定義されたポリシーを UCS Central に「格上げ」し、新しいグローバル ポリシーを複数のドメインに適用することで一貫性を保証するという、一般的に簡単で便利な方法です。

8. UCS Central の導入：アプローチと課題

UCS Central の導入を成功させるには、習熟することでのみ得られる安心感と、適応感覚が必要です。UCS Central には UCSM と共通する部分が多くありますが、違いや課題もあります。この項ではそれらについて説明します。

a) UCSM Platform Emulator

使い慣れと習得を進める一方で、すべてのリスクを回避するためのベスト プラクティスは、UCSM Platform Emulator を利用することです。UCSM Platform Emulator（PE）は仮想マシンとして実行しますが、UCS 管理情報ツリーとデータ管理エンジンを維持する UCS Manager の完全なインスタンスであり、UCS XML/API をエクスポートします。さらに、PE には、物理ハードウェア設定と、実際の UCS ドメインの論理設定の両方をインポートする機能が備わっています。

ベスト プラクティス

PE を使用すると、管理者は UCS 環境を UCS Central とともに効率的にモデル化できます。このように、設定変更、テストなどすべてが、実際の実稼働ドメインに影響を及ぼすことなく、「安全なサンドボックス」内で実行されます。

UCS Central との統合をテストする場合は、必ず PE の 2.1(2a) バージョンを使用してください。

b) 新規 UCS での展開（「既存への影響、依存性のない環境」）

UCS Central 管理モデルに慣れた後のベスト プラクティスは、UCS Central とともに、新しい UCS ドメインの展開にグローバル プール/ポリシー/サービス プロファイルを導入することです。これまで UCS が存在しなかった環境の場合は、UCS Central とグローバル サービス プロファイル/プール/ポリシーを Cisco UCS の導入と展開に使用し、可能であればローカル オブジェクトの導入を避けるようにしてください。グローバル サービス プロファイルは独占的にグローバル プールとグローバル ポリシーを参照します。

c) 既存システムでの移行（「既存への影響のある環境」）

管理者は、既存の UCS ドメインに展開される新しい処理に備え、UCS Central を導入してください。ベスト プラクティスに従うことによって、管理者は UCS Central のグローバル管理モデルを徐々に「オプトイン」していき、既存の処理が中断しないようにします。

また、管理者は、既存のローカルの処理の属性およびプロファイルに対応したグローバル プール/ポリシー/GSP テンプレートも構築できます。現在のところ、このような変更は手動で行う必要がありますが、管理者は UCS Central に慣れ、適応する機会となります。

既存の処理がある UCS ドメインに UCS Central を導入する場合は、現在の注意事項と制限に注意してください[13]。特に、既存の作業負荷は当面、ローカルに管理されたモードのままにしておく必要があります。

UCS Central は今後、UCS 管理の中心となるべく設計されています。既存の UCS ドメインが存在するデータセンターの場合は、将来拡張に対する管理の課題を単純化するため、UCS Central の導入を検討してください。

d) 個別環境の密接さ、親和性(ローカル アフィニティ)の課題

ポリシーと制御が UCS Central で一元管理されるようになると、ローカルのリソースやコントロール ポイントの親和性を浮き彫りにする特定の課題が発生します。これらは、ローカル/個別ドメインの「ローカル アフィニティ」の課題と呼ばれています。共通する親和性が求められるポイントと、考えられる回避策を示します[14]。

- **外部 IP プール**:物理ブレード(KVM、電源など)のアウトオブバンド管理に対処します。ただし、UCS Manager とは違い、UCS Central はこれらのアドレスをブレードに自動的に関連付けません。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、グローバル外部 IP プールを参照できるようにします。すべての UCS ドメインと、すべての外部 IP アドレスが共通のサブネット上に存在している必要があります。
- **ブート ポリシー**:特定のストレージ アレイに関連点けられる WWPN は、世界的な規模で(異なるストレージ アレイにわたる可能性もあります)同じブート ポリシーを使用するグローバル サービス ポリシーの設定では難しいものになります。回避策:現在の UCSM でのものと同じ回避策を使用し、SP とストレージ アレイのペアとして名前が付けられた SP テンプレートを作成します。

[13] セクション 15 と 16(「メモ」および「既知の注意事項」)を参照してください。
[14] 外部 IP プールとブート ポリシーは、既存のドメイン グループの「ID 範囲の認定」ポリシーと同様に、次回のリリースでは「エイリアス」機能を対象としています。

9. UCS Central のバックアップ

UCS Central 設定のバックアップは、必ず定期的に実施する必要があります。UCS Central 管理モデルは、コアの UCS 管理モデルを拡張したものです。しかし、ベースの UCS モデルには存在しない、UCS Central 独自の構成概念もあります。たとえば、「ドメイン グループ」の構成概念は UCS Central にしか存在しません。適切で定期的なバックアップを行わずに、DG 設定を自動的（簡単）に再構築することはできません。

同様に、運用ポリシーは DG を終端とするため、UCS Central を適切かつ定期的にバックアップしていない場合は、これらの運用ポリシーの DG、および下位の個々の UCS ドメインへのマッピングを自動的に再構築することはできません。

UCS Central は小さなサイズであること（通常は 1 MB よりもはるかに小さい）を前提としたバックアップとして、1 日に 1 回スケジュールするか、設定変更の回数と頻度に対応して実行してください。

10. UCS ドメインのバックアップ

UCS 管理者には、既存のバックアップの頻度を参考にバックアップを行うことをお勧めします。UCS Central で管理を行うとしても、定期的かつ頻繁に UCS のバックアップをおこなう必要性は変わりません。しかし、UCS Central を使用すると、個々のバックアップ操作がシンプルになり、自動化することができます。

バックアップとエクスポート ポリシーは DG ごとに定義できます。ベスト プラクティスは、これらのポリシーを「ルート」DG で定義して、すべてのドメインのバックアップを簡単に自動で行えるようにすることです。

個々の UCS ドメインのバックアップは通常 100 KB 以下なので、頻繁にバックアップを実行することに問題はありません（全体的なバイナリ バックアップは 2 MB 以下になります）。

11. UCS Central のアップグレード

アップグレード時には、すべて（各バージョン）のリリース ノートを確認してください。
http://www.cisco.com/en/US/products/ps12502/prod_installation_guides_list.html

UCS Central 1.0(1a) と 1.1(1a) 間のバージョン互換性要件に注意してください。

- UCS Central 1.0(1a) は UCSM 2.1.1 および UCSM 2.1.2 との通信をサポートしていること。
- UCS Central 1.1(1a) は UCSM 2.1.2 との通信**のみ**をサポートしていること。

UCS Central を 1.1(1a) にアップグレードする場合には、事前に、登録済みのすべての UCS ドメインを UCSM 2.1.2 にアップグレードする必要があります。

UCS Central 1.0 からのアップグレードには 2 つのアプローチがあります。既存の VM を ISO メソッドでアップグレードするか、UCS Central のまったく新しいインスタンスを作成して移行することによりアップグレードできます。

a) インプレース アップグレード

インプレース ISO アップグレード メソッドについては『Upgrade/Installation Guide』[英文] を参照してください。

UCS Central をアップグレードする前に、インプレース アップグレードを行う場合は、Snapshot Manager を使用して VM のスナップショットを取り、1.0(1a) VM の状態を保存し、元の状態に戻す場合に備えます。また、お客様は 1.0(1a) VM の FULL ステート バックアップと config-all のバックアップも、アップグレードの前に行ってください。

b) 新しい VM によるアップグレード

ベスト プラクティスでは、お客様が既存の 1.0(1a) インスタンスをバックアップとして保存しておくことを推奨しています。この場合のアップグレード手順は次のようになります。

- 1.0(1a) インスタンスの UCS Central「config-all」バックアップを取ります。バックアップの状態が「有効」になっていることを確認します。
- 1.0(1a) UCS Central VM の電源を切ります（削除はしません）。
- 1.1(1a) UCS Central VM を同じネットワーク設定とセキュリティ共有で構築します。
- 「config-all」バックアップ ファイルから [merge（マージ）] オプションを使用して「インポート」します（[replace（置換）] オプションを使用しないでください）。インポートの状態が「有効」であることを確認します。
- ドメイン グループ、グローバル プール、運用ポリシーで健全性チェックを行って、リストア操作で整合性に問題が生じていないことを確認します。
- （オプション）最後に、元々あった VM をディスクから登録解除して削除します（あるいは、アーカイブとして電源オフの状態で残します）。

ローカル UCS ドメインは UCS Central で表示されなくなりますが、アップグレードが完了すれば、「登録済み」の状態に戻ります。「登録解除/登録」のサイクルは UCS Central のアップグレードでは通常発生しませんが、必要になる場合もあります。

UCS Central 設定をバージョン 1.0(1a) からインポートする場合は、[replace（置換）] でなく、必ず [merge（マージ）] を使用します。

アーカイブ済みの 1.0(1a) VM と新しい 1.1(1a) VM が同時に実行することがないことを確認します。

UCS Central または UCSM のいずれかのダウングレードが必要になる場合に備え、UCSM とホスト OS の両方のバージョン互換性の要件を念頭に置きます。

12. 統計情報データベースのサポート

現在、1.1(1a) リリースは、内部 UCS Central データベースまたは外部データベースのいずれかを使用して、長期にわたる履歴動向を維持する統計情報をサポートしています。1.1(1a) の時点でサポートされている外部データベースは Oracle と Postgres です。

1.1(1a) のインストールまたはアップグレード後であれば、いつでも外部データベースを使用するように設定できます。さらに、データベース タイプも事後に変更できますが、UCS Central はアウトオブバンドで実行する必要があり、データベース全体のエクスポート/インポート操作が必要になります。データベースの変換は、SQL/データベース レベルで実行する必要があります。外部データベースの設定は、CLI でのみ実行できます。詳細は、『CLI Configuration Guide』[英文] を参照してください。

以下のガイドラインを使用し、外部データベースのサイズを調整する必要があります[15]。

- 各 5 シャーシ構成の 20 個の UCS ドメイン（合計で 800 台のサーバ）から統計データを 1 年間収集するには、データベース サーバには最低で 400 GB が必要です。
- 各 5 シャーシ構成の 100 個の UCS ドメイン（合計で 4,000 台のサーバ）から統計データを 1 年間収集するには、データベース サーバには最低で 2 TB が必要です。

UCS Central は外部接続の統計データベースをバックアップしません。統計データベースのバックアップは、UCS Centralから個別に管理する必要があります。

事前設定されたPostgres データベース アプライアンスは http://communites.cisco.com/ucsm でデモおよび概念検証テストを利用できますが、実働環境ではサポートされていません。

[15] 一般に、サーバごとに年間 0.5 GB で計画します。

13. UCSドメインのためのファームウェア管理

通常、UCSドメインのアップグレードは、これまで手作業で行われてきました[16]。UCSM 2.1 リリースには、新しい「ファームウェア自動インストール」機能があり、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なります[17]。UCS Central はこの新しい機能を基に構築されていて、複数の UCSドメインでファームウェアのアップグレードを自動で行うことができます。

ファームウェアには 2 つのタイプがあることを憶えておいてください。インフラストラクチャ ファームウェアは、I/O モジュール、ファブリック インターコネクト、UCS Manager を実行するイメージであり、サーバ ファームウェアは、物理サーバの BIOS、CIMS、アダプタおよびコントローラ上で実行するイメージです。一般に、サーバ ファームウェアのベスト プラクティスは、UCS Manager と同様に、サービス プロファイル定義の一部としてホスト ファームウェアのパッケージを利用してアプリケーションレベルでの設定整合性を保証することです。

この機能について、理解しておくべき重要なポイントがいくつかあります。

a) サービスの品質低下と中断

UCS インフラストラクチャ ファームウェアをアップグレードする際、一時的にサービスの品質低下を引き起こす場合があります。これは、各ファブリック インターコネクトが再起動処理を順次行う必要があるからです。管理者とオペレータは、NIC チーミングおよびボンディングやホストベースのストレージ マルチパスなど、適切なアプリケーションレベルの「可用性」スキームが有効であることを確認する必要があります。

b) 確認保留中

ファームウェアのアップグレードと FI の再起動では、UCS Central 管理者が明確に確認を行う必要があります。管理者は、アップグレードされる DG の [Schedules（スケジュール）][18] の下に [Pending Acknowledgements（確認保留中）] が表示されていないか注意する必要があります。デフォルトでは、すべてのファームウェア アップグレード（「infra-fw」）および再起動（「fi-reboot」）に実行前の確認が必要です。UCS Central で進捗状況が最もよくわかるのは、[Schedule（スケジュール）] メニューから [Active Tasks（アクティブ タスク）][19] タブであり、個々の UCSドメインの場合は、[Equipment（機器）] -> [Firmware Management（ファームウェア管理）] -> [Firmware Auto Install（ファームウェア自動インストール）-> [FSM] を選択します。

[16] 以下のEric William の UCS ファームウェア アップグレード スクリプトを使用していなかった場合に限ります。
http://developer.cisco.com/web/unifiedcomputing/community/-/blogs/cisco-ucs-powertool-examples
[17] UCSM 2.1(2a) へのアップグレードの場合は、「自動インストール」機能はお勧めしません。
[18] 各 DG の [InfraPack] -> [Pending-ack（確認保留中）] にも表示されます。
[19] 各 DG の [InfraPack] -> [Status（ステータス）] でも確認できます。

ベスト プラクティス

サーバ ファームウェア バンドルに関して暗黙のメンテナンス ポリシーはありません。このため、ベスト プラクティスは、サーバ ファームウェア バンドル アップグレードを管理するメンテナンス ポリシーを明確に定義することです。さらにベスト プラクティスは、メンテナンス ポリシーを「user-ack」を選択して定義し、予期しないサービスの中断を避けることです。

アップグレード プロセスは「無人」モードでは完了せず、確認作業が複数回必要です。

UCS Central のメリットの 1 つは、複数のアップグレードを並行して処理できることです。個々の UCSM に接続している場合、アップグレードの間に接続がリセットされます。スタンドアロンの UCSM のアップグレードと同様に、プロセスは完了までおよそ 1 時間かかりますが、複数のドメインを並行して実行できます[20]。完了後、UCS Central に再登録する必要はありません。

ファームウェア管理はホスト ファームウェア ポリシーを補完できます。新しい UCS ドメインを初めて立ち上げる際、UCS Central からトリガーされたインフラおよびホスト ファームウェア自動インストールを使用することで、新しいドメインを、すべて実稼働前の低レベルのホスト ファームウェアの状態にすることができます。

14. シスコサポート（TAC）への連絡

シスコ TAC のサポート ケースが必要な問題が発生した場合は、「show tech-support」の出力を提出できるように用意してください。これは、[Administration（管理）] -> [Diagnostics（診断）] -> [Tech Support Files（技術サポート ファイル] と進み、さらに [Create and Download Tech Support File（技術サポート ファイルの作成とダウンロード）] を選択することで作成できます。

15. メモ（注意事項）

この項には、管理者が認識しておく必要があるものの、製品についての「警告」とはならない課題が示されています。

a) グローバル オブジェクトのローカル可視性

グローバル オブジェクトを作成しても、UCSM に自動的に表示されたり、プッシュされたりしません。グローバル ID やグローバル ポリシーは、ローカル オブジェクトを作成/変更したときに UCSM GUI ドロップダウン メニューに表示される場合があります。しかし、グローバル オブジェクトについては、作成後に自動的に UCSM GUI に表示されません。グローバル オブジェクトはグローバル サービス プロファイルがサーバに展開された時点で UCSM GUI に表示されるようになります。グローバル オブジェクトの読み取り専用コピーは展開時に、ローカル UCSM によって「プルダウン」され、GUI に表示されます。

[20] 同時実行の設定は、[InfraPack] タブ（インフラ ファームウェア アップグレードの場合）やメンテナンス ポリシー スケジュール（サーバ ファームウェア アップグレードの場合）で行うことができます。

b) メンテナンス ポリシー（ローカルおよびグローバル）

予期しないサービスの中断を避けるには、一般に [user-ack] または [timer-automatic] をお勧めします。サービス中断のユーザ確認応答を UCSM 内でローカルに行う場合は、[user-ack] に基づくメンテナンス ポリシーを作成し、使用します。UCS Central 内で応答確認する場合は、[timer-automatic] を選択し、[user-ack] オプションを使用する [Schedule（スケジュール）] を選択します。

c) UCS Central 1.0(1a) から 1.1(1a) までのホスト OS のバージョン

UCS Central 1.0(1a) は以下のホスト OS バージョンでサポートされています。

- VMWare：ESX4.0u2、4.1u1、5.0
- Windows：W2K8 R2 SP1

UCS Central 1.1(1a) には以下のホスト OS バージョンが必要です。

- VMWare：ESX4、1u2、5.0、5.1
- Windows：W2K8R2 SP1、W2012

UCS Central 1.0(1a) からのアップグレードの場合は、UCS Central をアップグレードする前に、必要に応じてホスト OS をアップグレードしてください。

d) 外部統計データベースのバックアップ

UCS Central は外部接続の統計データベースをバックアップしません。統計データベースのバックアップは、UCS Centralから個別に管理する必要があります。

e) UCSM に強制時刻同期が必要な場合

NTP 設定直後に UCSM の時刻が同期していないように見える場合があります。

UCSM は NTP ですぐに同期させることができます。同期させるには、[Admin（管理者）] タブの [NTP Server（NTP サーバ）] を設定した後、CLI から以下のシーケンスを使用してクロックを設定します。

- “scope system”
- “scope services”
- “set clock x x x x x”(例：“set clock may 22 2013 13 44 00”)

変更を反映した UCSM の時間とともに、[Clock synchronization successful（クロックの同期が成功しました）] というメッセージが表示されます。次回からのの登録試行が成功します。

f) ハイパーバイザのコンテンションの回避

UCS Central は仮想アプライアンスとして動作するため、リソース共有の対象となり、ホスト OS ハイパーバイザによって制御されます。妥当なパフォーマンス特性を促進するには、VMware または Hyper-V 環境のいずれかで「リソース プール」を利用するのも 1 つの方法です。「リソース プール」を使用する目的は、CPU または メモリ、あるいはその両方の競合を必ず回避する、または UCS Central にとって最小限に抑えるためです。UCS Central が的確に有利に扱われるよう、独自の専用リソース プールに配置し、CPU とメモリの共有設定を両方とも [Normal（標準）] ではなく [High（高）] に設定します。『Installation/Upgrade Guide』[英文] を参照してください。

g) 高可用性クラスタ モード

クラスタ モードの UCS Central による高可用性（H/A）とは、UCS Central の単一インスタンスのことです。H/A モードは、2 つのまったく異なるインスタンスを意味するディザスタ リカバリ（DR）モードとは違います。DR と混同しないでください。

UCS Central による H/A は以下により実現できます。

- 新しい UCS Central 1.1(1a) 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 UCS Central 1.1(1a) を H/A クラスタに変換する。
- まず 1.0(1a) インスタンスを 1.1(1a) にアップグレードしてから H/A クラスタ モードを有効にする。

1.0(1a) からのアップグレードは、スタンドアロン モードでのみ実行できます。アップグレードを試行する前に、『Installation/Upgrade Guide』[英文] を必ず参照してください。

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 が個別の物理ホストにあり、共有ストレージにアクセスできる。
- 両方の VM が同じバージョンの ESX または HyperV を実行している。
- 両方の VM が同じバージョンの UCS Central を実行している。
- 両方の VM が同じサブネット上にある。

クラスタ H/A では、ロー デバイスとして存在する共有 LUN の設定が必要です。これには、以下を目的として、SAN の設定権限が必要です。

- ハイパーバイザのクラスタ化されたホストとストレージ アレイを SAN スイッチからゾーン分割する。
- ストレージ アレイ（LUN マスキング）からクラスタ化されたホストの共有 LUN にアクセスできるようにする。

以下を確認してください。

- Thick プロビジョニングを共有 LUN に使用する。(Thin プロビジョニングでなく)
- 共有 LUN へのアクセスは 2 つのクラスタ化されたホスト以外は排他的にする(ほかのホストには使用させない)。
- LUN はホスト上でマルチパス モードで設定する(つまり、LUN は ESX ホストに固定 I/O モードでマップする必要がある)。

共有ストレージの最高パフォーマンスを得るには:

- 高速 SAN 接続を設定し、高速のアクセスを可能にする。
- パフォーマンスが最も高い RAID タイプを共有 LUN に選択する。
- ストレージが書き込みキャッシュに対応しており、適切に設定されていることを確認する[21]。

VM スナップショットの一時停止/再開または復元などの機能を使用する場合は、共有ストレージの「所有権の競合」を発生させる可能性があるため、注意が必要です。共有ストレージは常にプライマリ VM にマウントされます。セカンダリ VM の所有権を主張しながらプライマリ VM がアクティブのままの場合は、クラッシュしたり、クラスタがダウンする場合があります。

16. 1.1(1a) における 2013 年 8 月時の既知の注意事項

このセクションでは、現在のリリース 1.1(1a) の既知の注意事項を示します。これらの注意事項については、最優先で対処する必要があります。

a) 「ルート」DG の UCS Central 管理ポリシー

現在のリリースでは、UCS Central 自体を管理するために、[Operations Management(運用管理)] の「ルート」DG に [Operational Policies(運用ポリシー)] を表示します。ロケールの設定およびローカルに認証された UCS Central のユーザーは [Admin(管理者)] タブに表示されます。UCSM と UCS Central の両方に適用できる設定は [Operational Policies(運用ポリシー)] タブに表示されます。

回避策:「ルート」DG にドメインを入力しないでください。DG は「ルート」DG の下に作成/入力して、UCS Central 自体とのポリシーの競合を回避します。

b) LDAP 認証

詳細は、「ベスト プラクティス: UCS Central の認証」の項を参照してください。

[21] たとえば、EMC ストレージ アレイには、ページ サイズが 8 KB、低基準値が 60%、高基準値が 80% のキャッシュ設定が必要です。

c) ロケールのグローバル組織のマージ

現在のリリースでは、UCSM から UCS Central へサービス プロファイルのある「orgs」が表示対象として提示されますが、これは読み取り専用のローカル オブジェクトです。UCS Central の「ロケール」には本来のマルチテナント機能があり、組織およびドメイン グループのユーザ可視性は、事実上、それらの組織とドメイン グループのペアに対応する「ロケール」に限定されています。

ただし、グローバル「ロケール」はグローバル「組織」にのみ作成できます。このため、「orgs」を使用し、かつ真のマルチテナントが必要なサイトの場合、次の手順をお勧めします。

1) 実際に UCS Central に登録する前に、UCS Central に全 UCS ドメイン用のグローバル組織を作成します。
2) UCS ドメインを UCS Central に登録します。ローカル/グローバルの org 名前空間は登録時にマージされます。
3) UCS Central で、グローバル組織にマッピングするグローバル ロケールを作成します。

この手順に従わないと、実際のマルチテナントを持ったグローバル「ロケール」を作成できません。ここで手順を間違えると、登録解除をして再登録するサイクルが必要になります。また、グローバル組織の再作成も必要です。これを回避するには、UCS Central の [Network（ネットワーク）] タブまたは [Storage（ストレージ）] タブからグローバル組織を作成して、再登録/再作成を繰り返さずにグローバル ロケールを作成できるようにします。

d) グローバル MAC/WWxN プールの導入

UCSM 2.1(2a) リリースは UCS Central 1.1(1a) リリースとともに、サービス プロファイル vNIC/VHBA がローカルからグローバル ID プール参照に変更されるとサービスの中断と ID の再割り当ての**原因に**なります[22]。このドキュメントの前のバージョンでは、更新したテンプレートを使用するとサービスの中断が回避できると誤って記載されていました。

この問題は、UCSM 2.1(3) で対処されます。

可能性のあるサービスの中断を回避するには、既存のローカル SP をライフサイクルの最後に到達するまでローカル SP のままにすることが最も適切な方法です。新しい SP はすべて GSP として作成する必要があります。

[22] 不具合報告 ID CSCud44377

e) グローバル UUID プール

グローバル UUID プールへの移行には、特定の作業が発生します。

プレフィクス：UUID のプレフィクスはドメイン レベルで定義されます。UUID サフィックスはプール内にブロックを作成するために使用できます。すべてのローカル UUID プールの上位セットであるグローバル UUID を導入するには、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 プールの数は少なくともドメインの数と同じになります。プールが統合されることはありません。

組織：グローバル プールは組織を基にしています。しかし UUID のプレフィクスはドメイン（ファブリック インターコネクトの内部 ID）を基にしています。組織とドメイン間のマッピングがないため、ベスト プラクティスの一般化を難しくしています。

適用：既存のリリースでは、設定を繰り返したり、サーバをリブートしたりせずにグローバル UUID を使用するよう既存のサービス プロファイルを簡単かつシームレスに導入できません。

回避策：既存のローカル SP を、そのライフサイクルに到達するまで、ローカル SP のままにします。新しい SP はすべて GSP として作成する必要があります。

f) ドメイン グループ ポリシーからのドメイン グループの再割り当て

ドメイン登録後のドメイン グループ ポリシーの変更では、ドメインは自動的に DG に再割り当てされなくなりました。ドメインの DG への再割り当ては、所定のドメインで明示的に「メンバーシップを再評価」することによってのみ可能になりました。この動作の変更は、人的エラーの影響を軽減するため 1.1(1a) で実装されました。

g) RBAC でサーバ プールのメンバーがマスクされない

現在、グローバル サーバ プールのメンバーの表示は、RBAC でマスクされません。回避策として、サーバ インベントリを表示する場合は「機器ビュー」を使用してください。グローバル サーバ プール ビューを通じてサーバを表示すると、プール メンバーを表示できるようになり、アクセスや設定が RBAC によって実際に制約される場合があります。

h) UCS 障害の要約が空白になる場合がある

これは既知の問題です。ブラウザ セッションを更新してください。

i) ホスト FW パッケージとメンテナンス ポリシー

1.0(1a) リリースでは、ホスト FW パッケージとメンテナンス ポリシーが誤ってドメイン グループのコンテキストで構成されました。その結果の下位互換性により、ドメイン グループと組織のコンテキストからホスト ファームウェア パッケージとメンテナンス ポリシーの両方が表示され、設定が可能になっています。

1.1(1a) 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、組織コンテキストで定義されたホスト FW パッケージのみを参照します。
- UCSM で作成されたローカル サービス プロファイルは、リリース 1.0(1a) と同様に、ドメイン グループ コンテキストからのみホスト FW パッケージを参照できます。
- グローバル サービス プロファイルをサーバと関連付けた後、ホスト FW パッケージとメンテナンスポリシー（およびその他の参照ポリシー）が UCSM から UCS Central に「プル」されます。
- その後に、ローカル サービス プロファイルはホスト FW パッケージとメンテナンス ポリシーを組織またはドメイン グループのいずれかのコンテキストから参照できます。
- グローバル サービス プロファイルは、組織コンテキストからのみ、ホスト FW パッケージとメンテナンス ポリシーを参照します。

この動作は、メンテナンス ポリシー、ホスト FW パッケージ、およびスケジューラがドメイン グループ コンテキストで定義されている 1.0(1a) リリースの下位互換性の問題によるものです。

ベスト プラクティス

ベスト プラクティスとしては、ホスト FW パッケージとメンテナンス ポリシーを組織コンテキストからのみ使用することです。

j) VLAN が未参照で表示される

[Network（ネットワーク）] タブから [Modify VLAN Org Permissions（VLAN 組織権限を修正）] を使用して組織間の VLAN 範囲を制限し、その後、VLAN が削除される場合は、参照された組織内のグローバル サービス プロファイル vNIC が未参照の「VLAN エイリアス」を参照し、それを VLAN として表示します。

これを回避するには、VLAN エイリアスが削除された後に対応する VLAN 自体が削除されるようにします。

k) デフォルトの FCoE VLAN ID が VSAN の場合は「1」になる

「SAN クラウド」から新しい VSAN を作成すると、デフォルトの FCoE VLAN ID の値が「1」になり、「グローバル デフォルト」のVLAN ID 値と競合します。

新しい VSAN 作成時に FCoE VLAN ID を変更し、現在、どこにも使用されていない VLAN を指定します。

l) VLAN と VSAN がローカルで持続する場合がある

VLAN/VSAN がグローバルに作成されたのち、GSP の展開でプッシュ ダウンされた場合は、ドメインが再登録された後もローカル ドメインの MIT で持続する場合があります。

m) ローカル UCS バックアップにグローバル参照がない

ローカル UCSM レベルでバックアップした場合、これらのバックアップには UCS Central で管理されたグローバル オブジェクトへの参照がありません。

UCS Central を使用する場合は、UCS Central が排他的に管理するバックアップ操作とバックアップ/エクスポート ポリシーを使用してください。

n) ローカリゼーションとグローバリゼーション

プール、ポリシー、SP を自動的にローカライズまたはグローバル化する方法はありません。ローカル オブジェクトからグローバル、グローバル オブジェクトからローカルへの移行は手動で実行する必要があります。

o) SDK のサポート

1.1(1a) リリースには、自動化を考慮してシスコが開発した SDK は含まれていません。そのため、UCS Central の自動での監視/設定をサポートする PowerTool や Python SDK はありません。

17. まとめ

協力な力には大いなる影響（責任）が伴います。

ご注意ください。

Jeff Silberman はデータセンター アーキテクトであり、UCS テクニカル マーケティング チームの初期メンバーです。彼は過去 12 年間にサーバおよび I/O の仮想化に取り組んできました。Jeff は最初の『UCS Best Practice/Quickstart Guide』、『UCS Test Drive』、および『UCS Deep Dive Methodology』を作成しました。シスコでは数百ものお客様の概念実証の管理、製品のレビューとデモ、UCS に関する技術的な「Deep Dives（詳細説明）」そして非常に多くの Cisco Live プレゼンテーションを担当してきました。シスコに入社する前は、NetApp の先進製品開発グループに数年間在籍し、Oracle®/NetApp 環境向けに業界初のユニファイド ファブリック ソリューションを開発しました。

18. 付録 I（登録のトラブルシューティング）

登録が正常に完了しない場合は、UCS Central VM を導入した後で、以下のことを行ってください。

1. 「ルート」ドメイン グループの運用ポリシーを介して、UCS Central 内で NTP サーバを設定します。
2. CLI で次のように入力して、UCS Central に証明書を再作成します。
   ```
   connect local-mgmt
   re-generate certificate
   ```
3. http/https「Admin」状態を循環させて内部 Web サーバを再起動することで、証明書を UCSM に再作成します。
4. NTP サーバが UCS ドメイン内に設定されていない場合は設定します。
5. UCS ドメインを UCS Central に登録します。

UCS ドメインから登録するには通常[23]、UCSM GUI で、[Admin（管理者）] -> [Communication Management（管理）] -> [UCS Central] を選択します。

登録処理の間に UCSM で共有シークレットが設定されますが、これは後から変更できます（“**connect local-mgmt; set shared-secret**”）。UCS Central で共有シークレットが変更されると、管理者は管理対象のすべての UCS ドメインに新しい共有シークレットを再登録する必要があります。

ローカル ドメインが UCS Central への登録に失敗した場合は、UCSM で「キーリング（Keyring）」の再作成が必要になる場合があります。たとえば、UCSM で「default」キーリングを使用している場合、次の UCSM CLI コマンドを使用します。

```
scope security
scope keyring default
set regenerate yes
commit-buffer
```

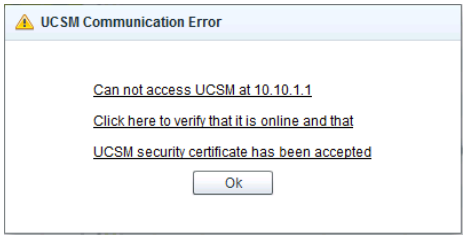
これ以外にも証明書の問題として、UCSM GUI と KVM セッションの相互起動が失敗したり、UCS Central からの障害のクエリーが失敗したりする場合があります。このような場合は、[Admin（管理者）] -> [Communication Services（通信サービス）] で HTTP を HTTPS へのリダイレクションに切り替えると問題が解決する場合があります。

[23] UCSM 2.1 に対応する最新の PowerShell プロバイダーを使うこともできます。

19. 付録 II（証明書のトラブルシューティング）

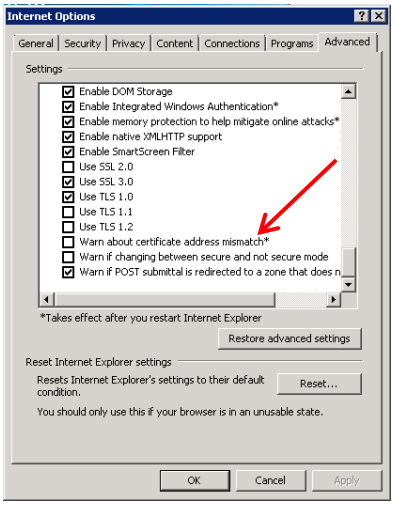
Cisco UCS Central – 証明書エラーのトラブルシューティング
バージョン 1.0 - 2013 年 1 月 17 日

UCS Central 管理インターフェイスの多くの機能は、クライアント マシンで利用したり、インポートしたりするために、（UCS Central に管理される各 UCS ドメインからの）https 証明書を使用します。これらの証明書は、KVM 起動、UCSM GUI 起動や、UCS 障害サマリーでの特定の障害/警告のクエリなどの機能を呼び出すために、UCS Central を管理するブラウザによって使用されます。証明書を適切にインポートできない、期限が切れている、あるいは使用している Web ブラウザで特定のセキュリティ設定が有効になっている場合、次のようなエラーが表示される場合があります。

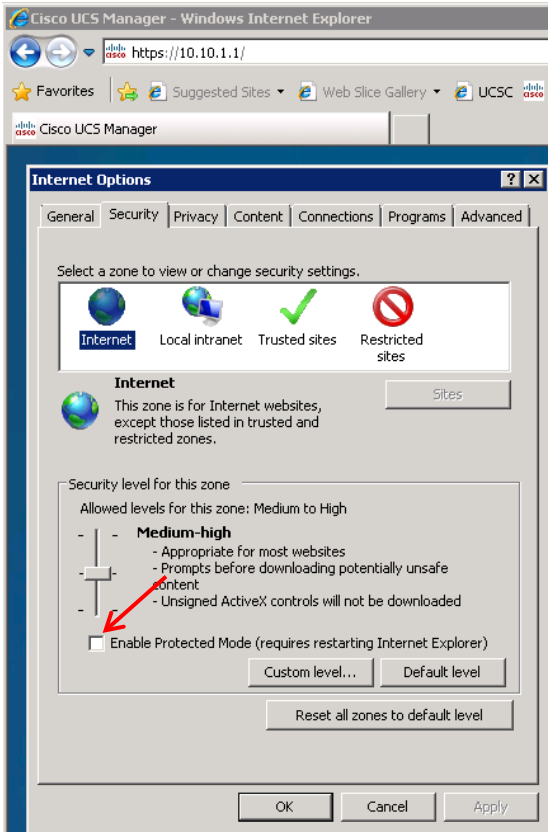


Internet Explorer

1. IE において、証明書のアドレスの不一致について警告が表示されないように設定します。
   a. IE で：[Tools（ツール）] → [Internet Options（インターネット オプション）] → [Advanced（詳細設定）] – [Security（セキュリティ）] セクションの下の方で [Warn about certificate address mismatch（証明書のアドレスの不一致について警告する）] の選択を解除します（IE を再起動する必要があります）。

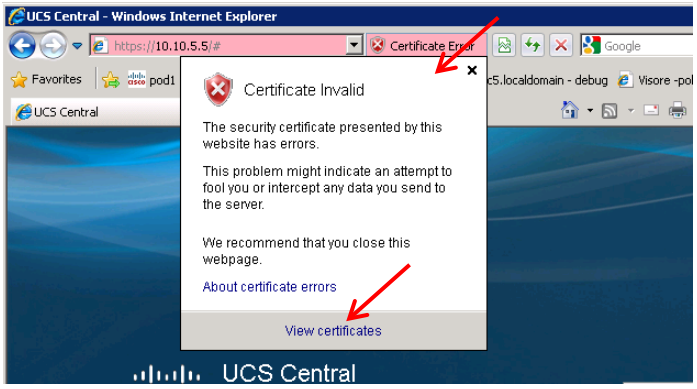


2. 証明書をインポートできるように [Protected Mode（保護モード）] をオフにする必要があります。
    a. [Tools（ツール）] → [Options（オプション）] → [Security（セキュリティ）] タブ → 各ゾーンで [Enable Protected Mode（保護モードを有効にする）] チェックボックスの選択を解除します。

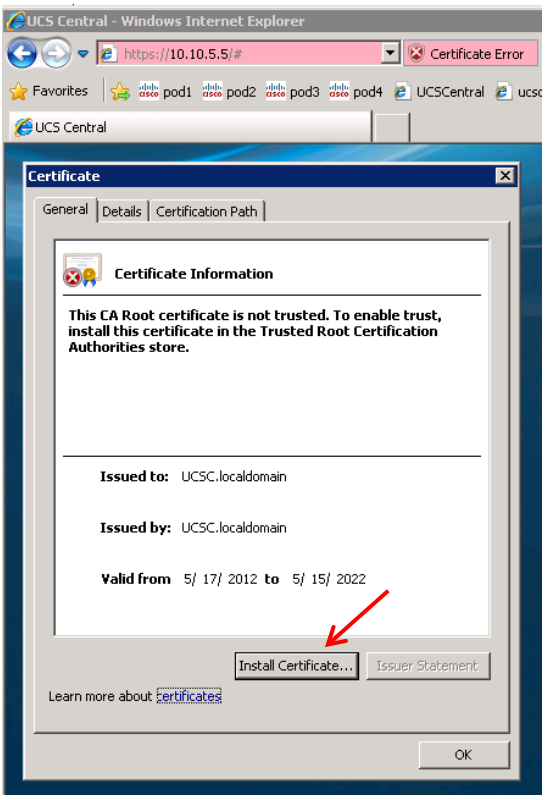


3. UCS Central または UCS Manager に初めて接続すると、証明書エラーが表示されます。次の手順に従って、提供された証明書をインポートします。

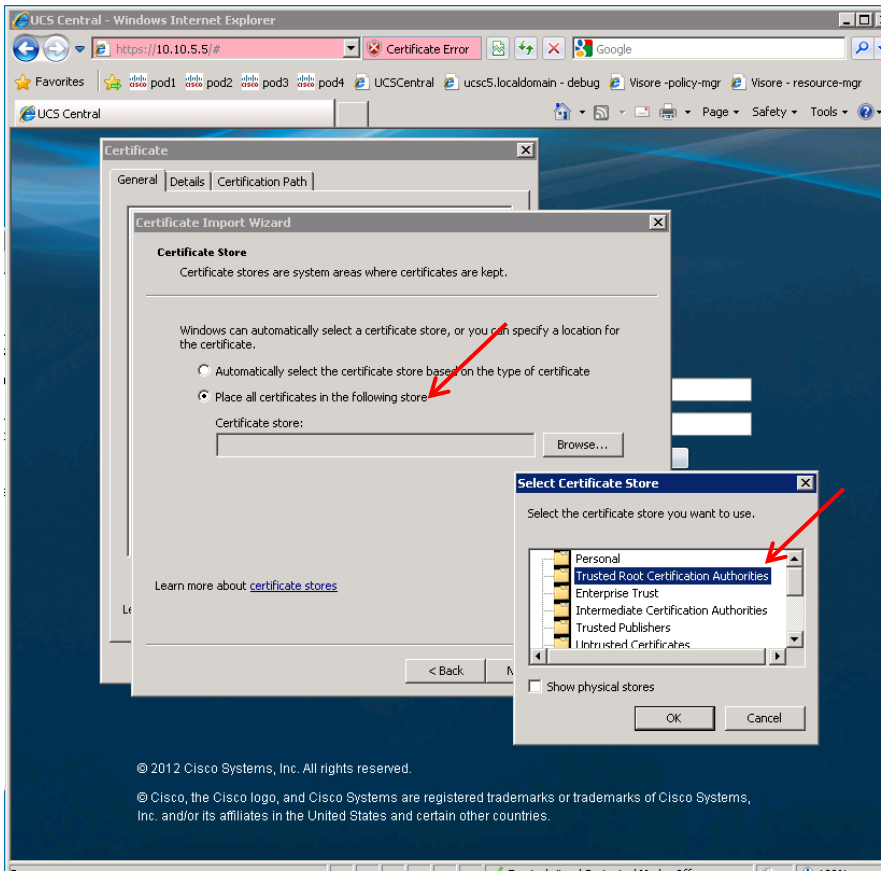
[Certificate Error（証明書エラー）] をクリックして、[View Certificates（証明書の表示）] をクリックし、次に [Import（インポート）] をクリックします。



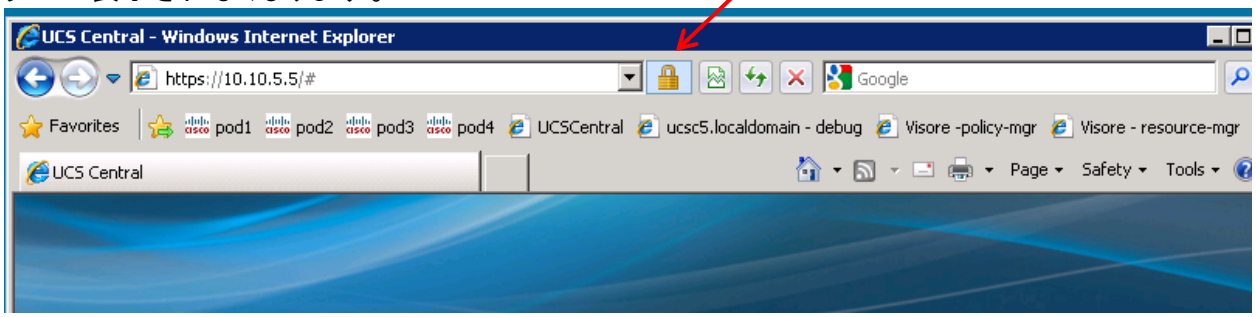
次に、[Install Certificate（証明書のインストール）] をクリックします。



[Next（次へ）] をクリックして、[Place all Certificates in the following store（証明書をすべて次のストアに配置する）] ラジオ ボタンを選択します。



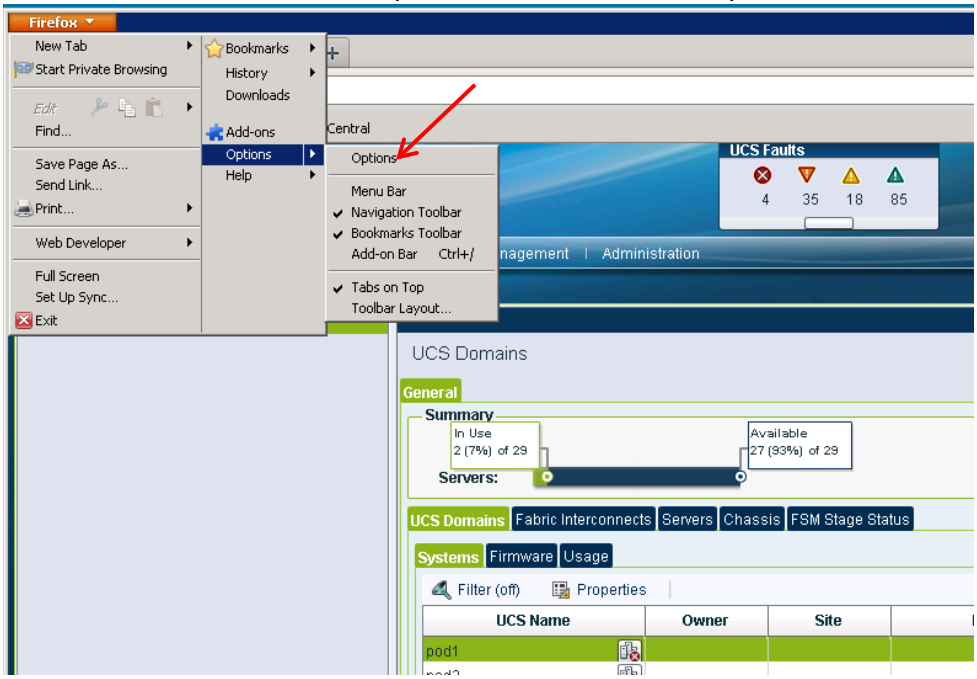
[OK]、次に [Finish（完了）] をクリックし、**IE を再起動します**。次回からは接続時に、証明書エラーが表示されなくなります。

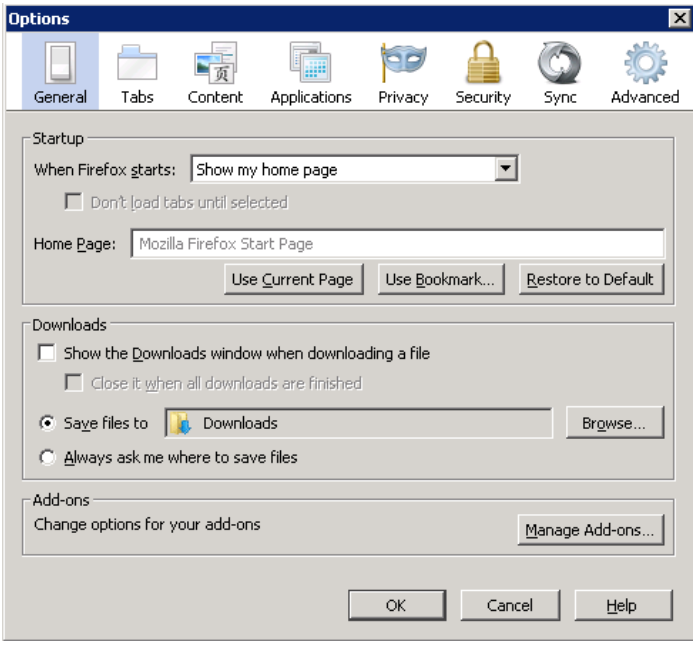


Mozilla Firefox

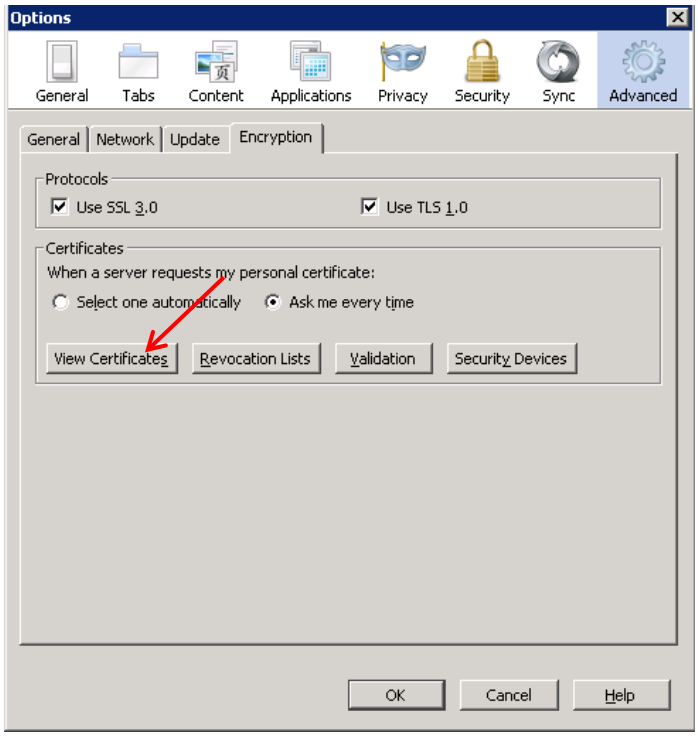
すべての証明書/キャッシュを空にする手順:

Firefox のドロップダウン → [Options（オプション）] → [Options（オプション）] をクリックします。

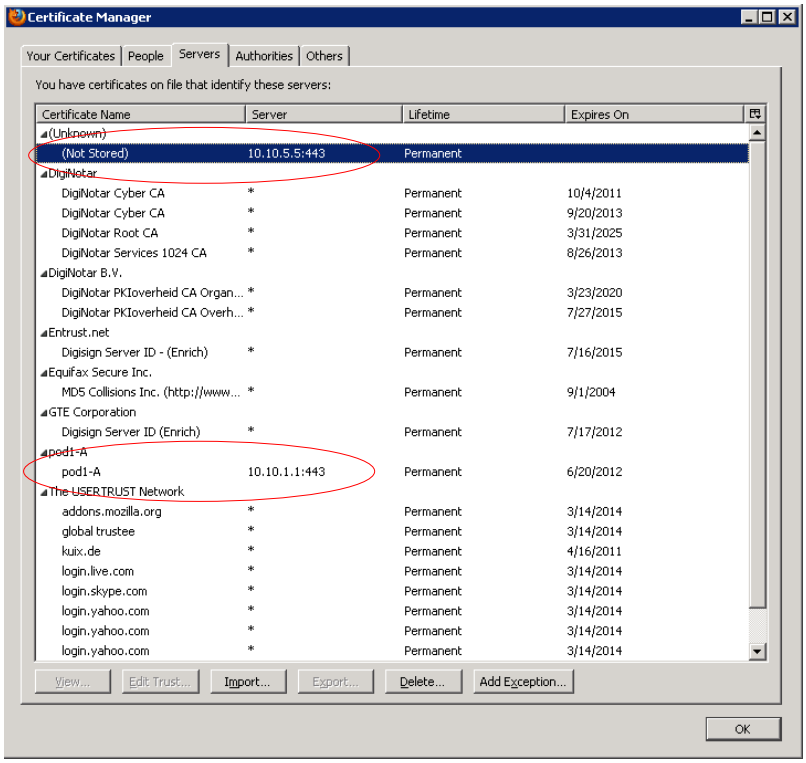




次に、[Advanced（詳細）] → [Encryption（暗号化）] → [View Certificates（証明書を表示）] をクリックします。

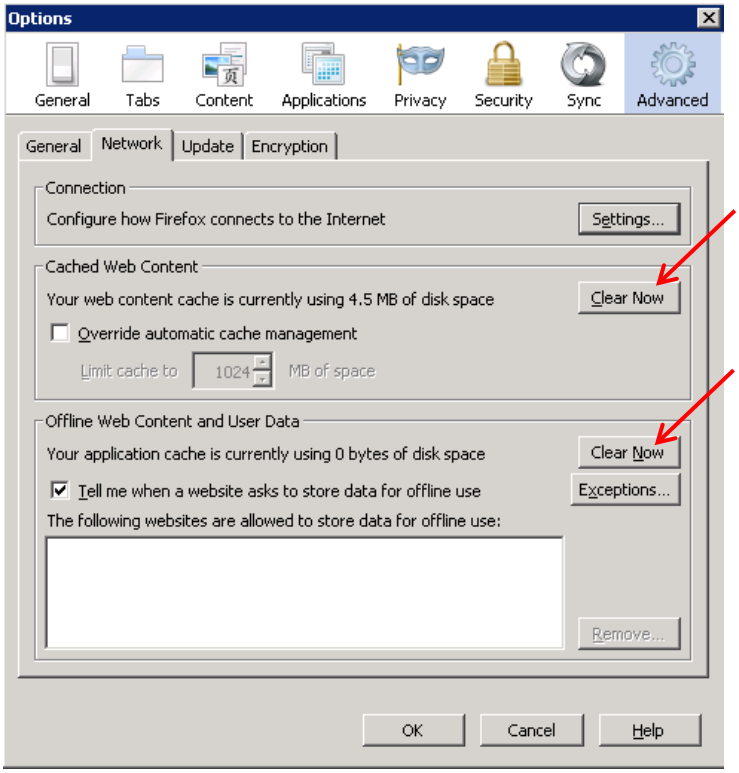


UCS または UCS Central システム（のみ）の証明書をすべて削除します。



完了したら Web キャッシュを消去します。[Firefox] ドロップダウン → [Options（オプション）] → [Options（オプション）] をクリックし、[Advanced（詳細）] ボタン、次に [Network（ネットワーク）] タブをクリックします。

- ページ内に 2 つある [Clear Now（今すぐ消去）] ボタンを両方ともクリックして、[OK] をクリックして閉じます。

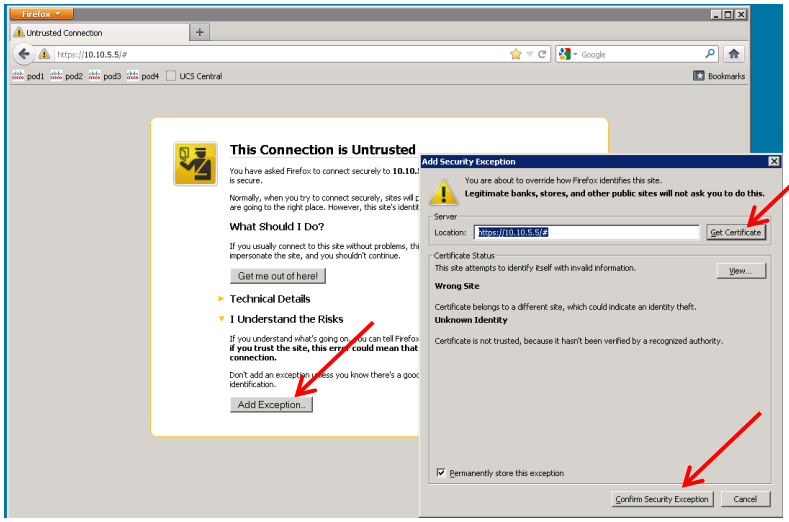


これで UCS Central に接続して（証明書をインポートします）、UCSM を起動できるようになりました。

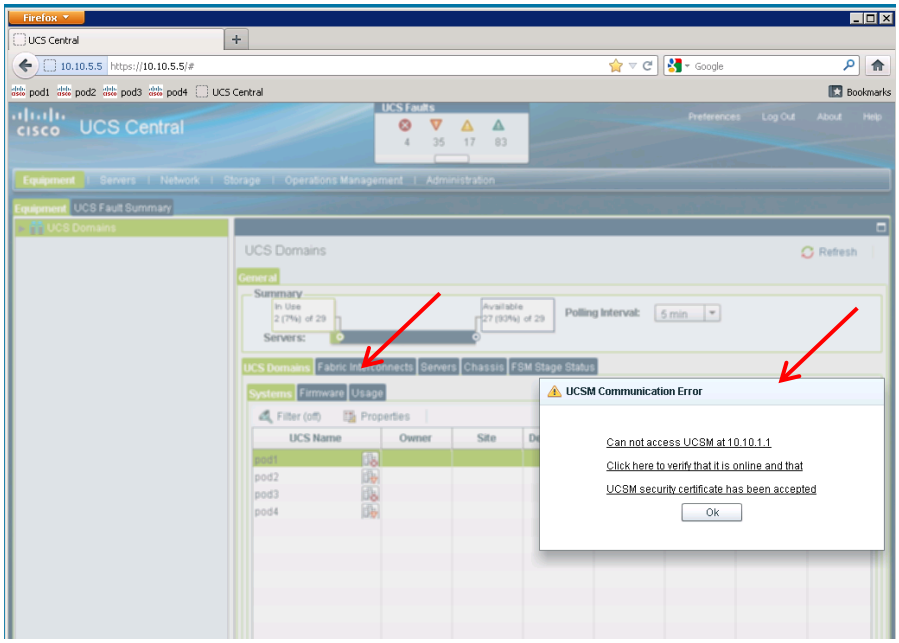
- 注：証明書をインポートするには、各 UCSM システムに（手作業または UCS Central を使って）少なくとも 1 度接続する必要があります。こうすることで、今後 UCS Central から GUI を起動しても証明書エラーが表示されなくなります。

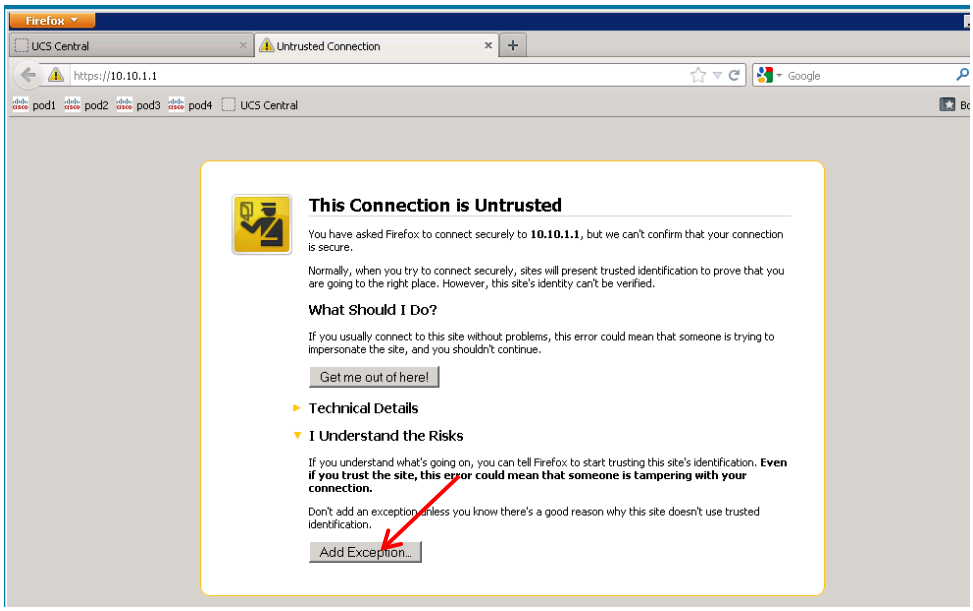
Firefox を使用して証明書を追加する方法は次のとおりです。

- 次に示すように、[Add Exception（例外を追加）]、[Get Certificate（証明書を取得）]、[Confirm Security Exception（セキュリティ例外を承認）] をクリックします。



UCS Central から起動する場合は、以下のリンクのエラーをクリックすると、UCSM が起動し、証明書をインポートすることができます。



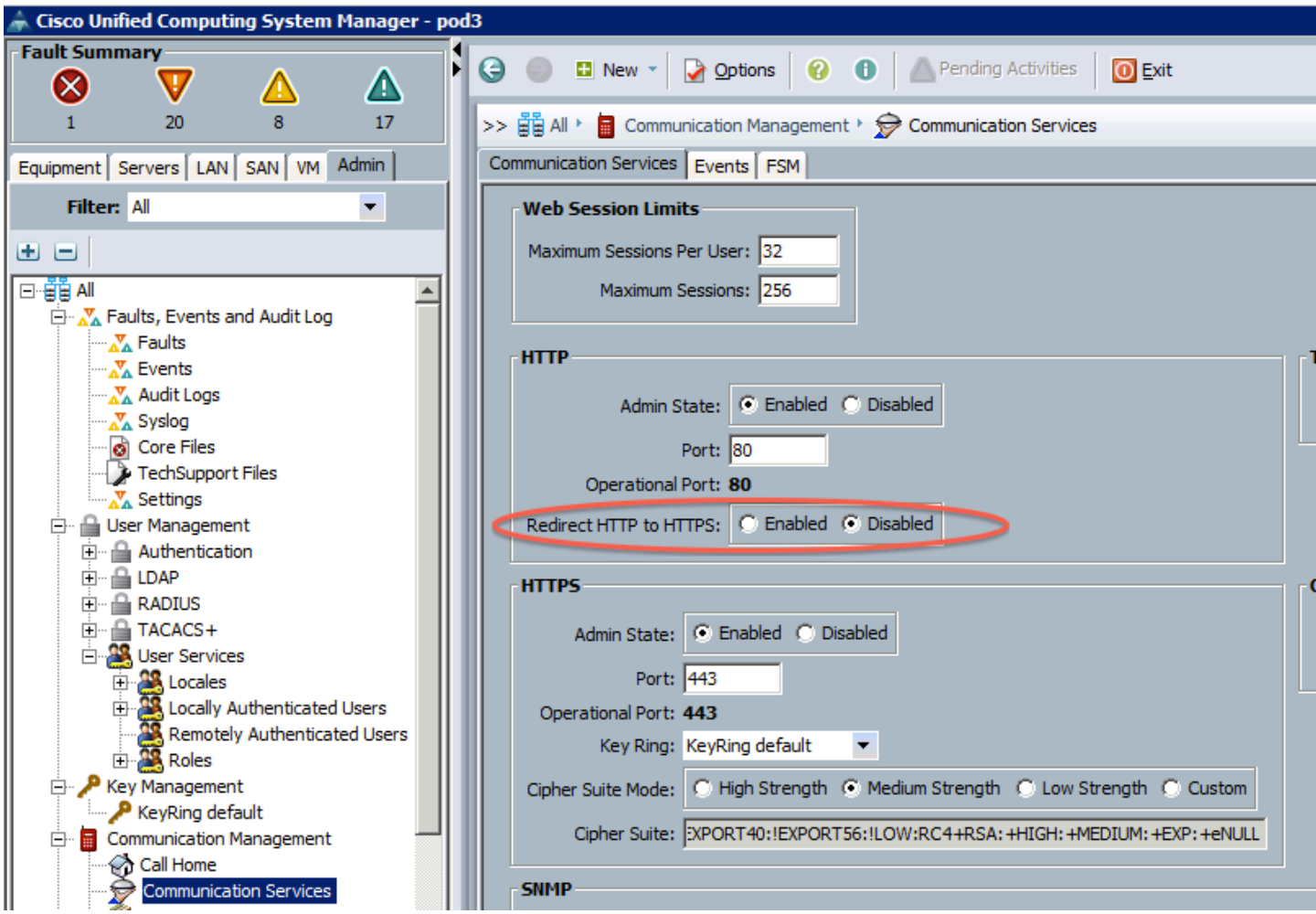


その他

1. 期限切れの証明書:
ファブリック インターコネクトから提示された HTTPS 証明書の期限が切れていないことを確認してください。

- 証明書の期限が切れている場合は、UCS ドキュメントに新しい HTTPS 証明書を「再作成」する手順が詳しく説明されています。
- UCSM CLI コマンド:scope security; scope keyring <keyring_name>; set regenerate yes; commit-buffer

2. ファブリック インターコネクトで新しい HTTPS 証明書の登録に影響を及ぼす不具合:
注:2.1(1a) には、場合によっては、新しい HTTPS 証明書を再生成した後に、ファブリック インターコネクト上の Web サーバに古い証明書がすぐに公開される不具合があります。この不具合を回避するには(次回リリースで修正されるまで)、[Admin(管理者)] タブ/[Communication Services(通信サービス)] で [HTTP] → [HTTPS] リダイレクション設定を切り替えます。


Cisco Unified Computing System Manager - pod3
Fault Summary
1
20
8
17
Equipment
Servers
LAN
SAN
VM
Admin
Filter: All
All
Faults, Events and Audit Log
Faults
Events
Audit Logs
Syslog
Core Files
TechSupport Files
Settings
User Management
Authentication
LDAP
RADIUS
TACACS+
User Services
Locales
Locally Authenticated Users
Remotely Authenticated Users
Roles
Key Management
KeyRing default
Communication Management
Call Home
Communication Services
New
Options
Pending Activities
Exit
>> All
Communication Management
Communication Services
Communication Services
Events
FSM
Web Session Limits
Maximum Sessions Per User: 32
Maximum Sessions: 256
HTTP
Admin State: Enabled Disabled
Port: 80
Operational Port: 80
Redirect HTTP to HTTPS: Enabled Disabled
HTTPS
Admin State: Enabled Disabled
Port: 443
Operational Port: 443
Key Ring: KeyRing default
Cipher Suite Mode: High Strength Medium Strength Low Strength Custom
Cipher Suite: EXPORT40:!EXPORT56:!LOW:RC4+RSA:+HIGH:+MEDIUM:+EXP:+eNULL
SNMP