Cisco Unified Computing System の概要

この章は、次の内容で構成されています。

- Cisco Unified Computing System について，1 ページ
- ユニファイド ファブリック，3 ページ
- IPv6 への準拠，4 ページ
- サーバのアーキテクチャおよび接続性，6 ページ
- CIMC インバンド管理，12 ページ
- トラフィック管理，14 ページ
- オプトイン機能，21 ページ
- Cisco UCSのバーチャライゼーション，23 ページ

Cisco Unified Computing System について

Cisco Unified Computing System（Cisco UCS）は、アクセス レイヤ ネットワーキングとサーバを融合します。 この高性能次世代サーバ システムは、作業負荷に対する敏捷性およびスケーラビリティの高いデータセンターを実現します。

ハードウェア コンポーネントおよびソフトウェア コンポーネントは、1 つの統合ネットワーク アダプタ上に複数のタイプのデータセンター トラフィックを通過させる、シスコ ユニファイド ファブリックをサポートします。

アーキテクチャの単純化

Cisco UCS の簡素化されたアーキテクチャは、必要なデバイスの数を削減し、スイッチング リソースを中央に集中させることができます。 シャーシ内部でのスイッチングを止めると、ネットワーク アクセス レイヤのフラグメンテーションが大きく減少します。

Cisco UCS は、ラック、またはラックのグループでシスコ ユニファイド ファブリックを実装し、10 ギガビット シスコ データセンター イーサネット リンクおよび Fibre Channel over Ethernet（FCoE）リンク経由でイーサネットおよびファイバ チャネル プロトコルをサポートします。

この徹底的な単純化により、スイッチ、ケーブル、アダプタ、および管理ポイントの最高 3 分の 2 が削減されます。 Cisco UCS ドメイン内のデバイスはすべて、1 つの管理ドメイン下にとどまり、冗長コンポーネントの使用中、ハイ アベイラビリティを保ちます。

ハイ アベイラビリティ

Cisco UCS の管理およびデータ プレーンはハイ アベイラビリティおよび冗長アクセス レイヤ ファブリック インターコネクトのために設計されています。 さらに、Cisco UCS は、データ レプリケーションやアプリケーション レベルのクラスタ処理テクノロジーなど、データセンターに対する既存のハイ アベイラビリティおよびディザスタ リカバリ ソリューションをサポートします。

拡張性

単一の Cisco UCS ドメインは、複数のシャーシおよびそれらのサーバをサポートします。それらはすべて、1 つの Cisco UCS Manager を介して管理されます。 スケーラビリティの詳細については、シスコの担当者にお問い合わせください。

柔軟性

Cisco UCS ドメインは、データセンターのコンピューティング リソースを、急速に変化するビジネス要件にすばやく合せることができます。 この柔軟性を組み込むかどうかは、ステートレス コンピューティング機能の完全な実装が選択されているかどうかによって決定されます。

必要に応じて、サーバやその他のシステム リソースのプールを適用し、作業負荷の変動への対応、新しいアプリケーションのサポート、既存のソフトウェアおよびビジネス サービスの拡張、スケジュール済みのダウンタイムおよび予定されていないダウンタイムの両方への適応を行うことができます。 サーバの ID は、最小のダウンタイムで、追加のネットワーク設定を行わずにサーバからサーバへ移動できるモバイル サービス プロファイルに抽象化することができます。

このレベルの柔軟性により、サーバの ID を変更したり、サーバ、ローカル エリア ネットワーク（LAN）、または Storage Area Network（SAN）を再設定したりせずに、すばやく、簡単にサーバの容量を拡張することができます。 メンテナンス ウィンドウでは、次の操作をすばやく行うことができます。

- 予測していなかった作業負荷要求に対応し、リソースとトラフィックのバランスを取り戻すために新しいサーバを導入します。
- あるサーバでデータベース管理システムなどのアプリケーションをシャットダウンし、I/O 容量とメモリ リソースを拡張した別のサーバでこれを再度起動します。

サーバ バーチャライゼーションに向けた最適化

Cisco UCS は、VM-FEX テクノロジーを実装するために最適化されています。 このテクノロジーは、より優れたポリシーベースの設定とセキュリティ、会社の運用モデルとの適合、VMware の VMotion への順応など、サーバ バーチャライゼーションに対してより優れたサポートを実現します。

ユニファイド ファブリック

ユニファイド ファブリックを使用すると、単一のデータセンター イーサネット（DCE）ネットワーク上で複数の種類のデータセンタートラフィックを行き来させることができます。 さまざまな一連のホスト バス アダプタ（HBA）およびネットワーク インターフェイス カード（NIC）をサーバに搭載させる代わりに、ユニファイドファブリックは統合された単一のネットワークアダプタを使用します。 このタイプのアダプタは、LAN および SAN のトラフィックを同一のケーブルで運ぶことができます。

Cisco UCS は、Fibre Channel over Ethernet（FCoE）を使用して、ファブリック インターコネクトとサーバ間をつなぐ同一の物理イーサネット接続でファイバ チャネルおよびイーサネットのトラフィックを運びます。 この接続はサーバ上の統合されたネットワーク アダプタで終端し、ユニファイド ファブリックはファブリック インターコネクトのアップリンク ポートで終端します。 コア ネットワークでは、LAN および SAN のトラフィックは分かれたままです。 Cisco UCS では、データセンター全体でユニファイド ファブリックを実装する必要はありません。

統合されたネットワーク アダプタは、オペレーティング システムに対してイーサネット インターフェイスおよびファイバ チャネル インターフェイスを提示します。 サーバ側では、標準のファイバ チャネル HBA を確認しているため、オペレーティング システムは FCoE のカプセル化を認識していません。

ファブリック インターコネクトでは、サーバ側イーサネット ポートでイーサネットおよびファイバ チャネルのトラフィックを受信します。 （フレームを区別する Ethertype を使用する）ファブリック インターコネクトは、2 つのトラフィックの種類に分かれます。 イーサネット フレームおよびファイバ チャネル フレームは、それぞれのアップリンク インターフェイスにスイッチされます。

Fibre Channel over Ethernet

Cisco UCS は、Fibre Channel over Ethernet（FCoE）標準プロトコルを使用して、ファイバ チャネルを提供します。 上部のファイバ チャネル レイヤは同じであるため、ファイバ チャネル動作モデルが維持されます。 FCoE ネットワーク管理と設定は、ネイティブのファイバ チャネル ネットワークと同様です。

FCoE は、物理イーサネット リンク上のファイバ チャネル トラフィックをカプセル化します。 FCoE は専用のイーサタイプ 0x8906 を使用して、イーサネット上でカプセル化されるため、FCoE トラフィックと標準イーサネット トラフィックは同じリンク上で処理できます。 FCoE は ANSI T11 標準委員会によって標準化されています。

ファイバ チャネル トラフィックには、ロスレス トランスポート層が必要です。 ネイティブ ファイバ チャネルが使用するバッファ間クレジット システムの代わりに、FCoE はイーサネット リンクを使用して、ロスレス サービスを実装します。

ファブリック インターコネクト上のイーサネット リンクは、2 つのメカニズムを使用して、FCoE トラフィックのロスレス トランスポートを保証します。

- リンク レベル フロー制御

- プライオリティ フロー制御

リンクレベル フロー制御

IEEE 802.3x リンクレベル フロー制御では、輻輳の発生している受信側からエンドポイントに対して、少しの間、データの送信を一時停止するように信号を送ることができます。 このリンクレベル フロー制御では、リンク上のすべてのトラフィックが一時停止します。

送受信方向は個別に設定できます。 デフォルトでは、リンクレベル フロー制御は両方向でディセーブルです。

各イーサネットインターフェイスで、ファブリックインターコネクトは、プライオリティフロー制御、またはリンクレベル フロー制御のいずれかをイネーブルにできます。両方をイネーブルにはできません。

プライオリティ フロー制御

プライオリティフロー制御（PFC）機能は、イーサネットリンク上の特定のトラフィック クラスにポーズ機能を適用します。 たとえば、PFC は FCoE トラフィックにロスレス サービスを、標準イーサネット トラフィックにベストエフォート サービスを提供します。 PFC は、（IEEE 802.1p トラフィック クラスを使用して）特定のイーサネット トラフィック クラスに、さまざまなレベルのサービスを提供することができます。

PFC は、IEEE 802.1p の CoS 値に基づき、ポーズを適用するかどうかを判断します。 ファブリック インターコネクトは、PFC をイネーブルにするときに、特定の CoS 値を持つパケットにポーズ機能を適用するように、接続されたアダプタを設定します。

デフォルトでは、ファブリック インターコネクトは、PFC 機能をイネーブルにするかどうかのネゴシエーションを行います。 ネゴシエーションに成功すると、PFC がイネーブルにされますが、リンクレベル フロー制御は（設定値に関係なく）ディセーブルのままです。 PFC ネゴシエーションに失敗した場合は、PFC をインターフェイスで強制的にイネーブルにするか、IEEE 802.x リンクレベル フロー制御をイネーブルにできます。

IPv6 への準拠

Cisco UCS Manager は、IPv6 アドレッシングをサポートします。 これは次の理由により重要になります。

- IPv4 アドレスは、IPv6 アドレスよりアドレス空間が小さい。
- 一意の IPv4 アドレスの数は有限であり、インターネットのアドレス資源管理団体が使用するアドレス指定方式が使用可能なアドレスの減少に拍車をかけている。
- IPv6 アドレスには大きなアドレス空間があり、使用可能な IPv6 アドレスのプールは、IPv4 アドレスのプールよりもはるかに多い。
- 顧客によっては、購入するすべてのネットワーキング ソフトウェアが IPv6 規格に準拠していることが求められる。

IPv4 アドレッシングをサポートする Cisco UCS Manager の機能はすべて IPv6 もサポートします。

（注） 公開グローバル ユニキャスト IPv6 アドレスのみがサポートされます。

IPv6 アドレスは、SoL 上の管理インターフェイス、CiscoCisco UCS Manager GUI、KVM コンソール、および SSH へのインバンド アクセスの設定に使用できます。

（注） IPv6 アドレスは、CIMC へのアウトオブバンド アクセスではサポートされません。

サポートされるサービス

IPv6 アドレスをサポートするサービスは次のとおりです。

- HTTP と HTTPS
- SSH
- Telnet
- CIM XML
- SNMP
- フラッシュ ポリシー サーバ

クライアントのサポート

IPv6 アドレスをサポートする外部クライアントは次のとおりです。

- NTP
- DNS
- DHCP
- LDAP
- RADIUS
- TACACS+
- SSH
- Syslog
- vCenter
- Call Home
- NFS

Fabric Interconnects

ファブリック インターコネクトの初期設定は、管理 IP アドレス、デフォルト ゲートウェイ、および DNS サーバに対する IPv6 アドレスの使用をサポートします。
クラスタのセットアップでは、ファブリック A が IPv6 アドレスを使用して設定され、クラスタ設定がイネーブルの場合は、ファブリック B をその後に設定すると、セットアップ プロセスがファブリック A からアドレス タイプを取得し、IPv6 アドレスを使用するようユーザに促します。 初期セットアップが完了したら、IPv4 アドレスをアウトオブバンド（OOB）アクセスの両方のファブリック インターコネクト用に設定する必要があります。

Cisco UCS Manager およびファブリック インターコネクトは、IPv4 アドレスと IPv6 アドレスの両方で OOB アクセスをサポートします。

IPv6 アドレッシングをサポートする設定

IPv6 アドレスを使用して、キーリング証明書の要求、SNMP トラップ、管理 IP プールとアドレスブロック、サービスプロファイル、サービスプロファイルテンプレート、VLAN グループ、バックアップと復元操作、コア ファイル エクスポータ、Cisco UCS Manager Syslog、NTP サーバ、管理インターフェイス モニタリング ポリシーでの ARP ターゲット、システム イベント ログ（SEL）管理、ライセンス管理、ファームウェアのダウンロード、Call Home、および vCenter を設定できます。

LDAP、RADIUS および TACACS+ 認証サービス プロバイダーの設定はすべて、IPv6 アドレッシングをサポートします。

サーバ

Cisco UCS ブレードおよびラックマウント サーバは、スタティック IPv6 アドレスを使用するように設定できます。 サーバ Cisco Integrated Management Controller（CIMC）へのインバンド アクセスは、IPv6 アドレスを使用して行うことができます。 管理トラフィックがより広い帯域幅のアップリンク ポートを使用してファブリック インターコネクトとサーバ間を流れるため、インバンド アクセスの方が高速です。

（注） Cisco UCS M3 および M4 サーバのみが、IPv6 アドレスをサポートしています。 Cisco UCS M1 および M2 サーバに対する IPv6 アドレッシングはサポートされません。

サーバのアーキテクチャおよび接続性

サービス プロファイルの概要

サービス プロファイルは Cisco UCS の中心コンセプトです。 各サービス プロファイルにより具体的な目的のサービスが提供されるため、関連付けられたサーバ ハードウェアでホスティングされるアプリケーションをサポートするために必要な設定が確実にハードウェアに設定されます。

サービスプロファイルには、サーバハードウェア、インターフェイス、ファブリック接続、およびサーバとネットワークの ID に関する設定情報が保持されます。 この情報は、Cisco UCS Manager を使って管理できる形式で保存されています。 すべてのサービスプロファイルは一元的に管理され、ファブリック インターコネクト上のデータベースに格納されます。

各サーバは、サービス プロファイルと関連付けられる必要があります。

重要 各サーバは、いつの時点においても 1 つのサービス プロファイルだけに関連付けることができます。 同様に、各サービス プロファイルは一度に 1 つのサーバだけに関連付けることができます。

サービスプロファイルをサーバと関連付けると、サーバではオペレーティングシステムとアプリケーションをインストールする準備が整います。サーバの設定はサービス プロファイルで確認することができます。 サービスプロファイルに関連付けられたサーバが失敗した場合でも、サービス プロファイルが別のサーバに自動的にフェールオーバーすることはありません。

サーバからサービス プロファイルの関連付けが解除されると、サーバの ID および接続の情報は工場出荷時のデフォルトにリセットされます。

サービス プロファイルによるネットワーク接続

各サービスプロファイルは、サーバについて、Cisco UCS インフラストラクチャを経由して外部ネットワークに接続する LAN および SAN ネットワーク接続を指定します。 Cisco UCS サーバおよびその他のコンポーネントについて、ネットワーク接続を手動で設定する必要はありません。すべてのネットワーク設定は、サービス プロファイルを通じて行われます。

サービス プロファイルをサーバに関連付けると、Cisco UCS 内部ファブリックがサービス プロファイルの情報を使って設定されます。 このプロファイルが以前に別のサーバと関連付けられていた場合、ネットワーク インフラストラクチャが再構成され、新しいサーバに対して同じネットワーク接続がサポートされます。

サービス プロファイルによる設定

サービス プロファイルはリソース プールとポリシーを利用して、サーバと接続設定を操作します。

サービス プロファイルで設定されたハードウェア コンポーネント

サービス プロファイルがサーバに関連付けられているときには、プロファイルのデータに応じて次のコンポーネントが設定されます。

- BIOS および CIMC を含むサーバ
- アダプタ
- ファブリック インターコネクト

これらのコンポーネントを直接設定する必要はありません。

サービス プロファイルによるサーバ ID 管理

製造元がサーバ ハードウェアに記録したネットワーク ID およびデバイス ID を使用できます。あるいは、関連付けられたサービス プロファイルで指定した ID を直接または MAC、WWN、UUID などの ID プール経由で使用できます。

次の例は、サービス プロファイルに含めることができる設定情報の方法を示しています。

- プロファイル名と説明
- 一意のサーバ ID（UUID）
- MAC アドレスなどの LAN 接続属性
- WWN などの SAN 接続属性

サービス プロファイルで設定した操作面

次のように、サービス プロファイルで設定できるサーバ操作機能があります。

- ファームウェア パッケージとバージョン
- オペレーティング システム ブート順序と設定
- IPMI と KVM アクセス

サービス プロファイルによる vNIC 設定

vNIC は物理ネットワーク アダプタで設定される仮想化されたネットワーク インターフェイスであり、サーバのオペレーティング システムに物理 NIC として表示されます。 システムのアダプタの種類によって、作成できる vNIC の数は異なります。 たとえば、統合ネットワーク アダプタには NIC が 2 つあります。つまり、アダプタごとに最大 2 つの vNIC を作成できます。

vNIC はイーサネット上で通信し、LAN トラフィックを処理します。 少なくとも、各 vNIC には名前、ファブリック接続、ネットワーク接続を設定する必要があります。

サービス プロファイルによる vHBA 設定

vHBA とは、物理ネットワーク アダプタ上に設定される仮想化されたホスト バス アダプタのことで、サーバのオペレーティング システムには物理 HBA に見えます。 システムのアダプタの種類に応じて作成できる vHBA の数が決まります。 たとえば、統合ネットワーク アダプタには HBA が 2 つあります。つまり、アダプタごとに最大 2 つの vHBA を作成できます。 他方、ネットワーク インターフェイス カードには HBA がありません。これは、アダプタで vHBA を作成できないことを意味します。

vHBA は FCoE 上で通信し、SAN トラフィックを処理します。 少なくとも、各 vHBA には名前とファブリック接続を設定する必要があります。

サーバ ID を上書きするサービス プロファイル

このタイプのサービスプロファイルにより、柔軟性と制御性が最大化されます。 このプロファイルを使用すると、アソシエーション時にサーバに設定された ID 値を上書きし、Cisco UCS Manager で設定されたリソース プールとポリシーを使用して一部の管理タスクを自動化できます。

このサービス プロファイルは、あるサーバとの関連付けを解除して、別のサーバに関連付けることができます。 この再アソシエーションは手動で行うこともできますし、自動サーバ プール ポリシーを通じて行うこともできます。 UUID や MAC アドレスなど、新しいサーバの工場出荷時の設定は、サービスプロファイルでの設定で上書きされます。 その結果、サーバでの変更はネットワークには透過的に行われます。 新しいサーバの使用を開始するために、ネットワークでコンポーネントやアプリケーションを再設定する必要はありません。

このプロファイルにより、次のようなリソースプールやポリシーを通じて、システム リソースを利用し、管理できるようになります。

- MAC アドレスのプール、WWN アドレス、UUID などの仮想 ID 情報
- イーサネットおよびファイバ チャネル アダプタ プロファイル ポリシー
- ファームウェア パッケージ ポリシー
- オペレーティング システム ブート順序ポリシー

サービスプロファイルに電源管理ポリシー、サーバプール資格情報ポリシー、または特定のハードウェア設定が必要な別のポリシーが含まれていない場合は、そのサービスプロファイルを Cisco UCS ドメインのどのタイプのサーバにも使用できます。

これらのサービス プロファイルは、ラックマウント サーバまたはブレード サーバのどちらかに関連付けることができます。 サービス プロファイルの移行の可否は、サービス プロファイルの移行制限を選択するかどうかによって決まります。

（注） 移行を制限しない場合は、既存のサービス プロファイルを移行する前に、Cisco UCS Manager による新規サーバに対する互換性チェックは実行されません。 両方のサーバのハードウェアが類似していない場合、アソシエーションが失敗することがあります。

サーバ ID を継承するサービス プロファイル

このハードウェアベースのサービス プロファイルは使用も作成も簡単です。 このプロファイルは、サーバのデフォルト値を使用して、ラックマウント型サーバの管理を模倣します。 これは特定のサーバに関連付けられているため、別のサーバへの移動や移行はできません。

このサービス プロファイルを使用するために、プールや設定ポリシーを作成する必要はありません。

このサービス プロファイルは、アソシエーション時に存在する次のような ID 情報および設定情報を継承し、適用します。

- 2 つの NIC の MAC アドレス
- 統合ネットワーク アダプタまたは仮想インターフェイス カードについては、2 つの HBA の WWN アドレス
- BIOS バージョン
- サーバの UUID

重要 このプロファイルをサーバに関連付ける前に、製造元でサーバのハードウェアに設定された値が変更された場合、このサービス プロファイルを通じて継承されたサーバの ID および設定情報は、この値とは異なる可能性があります。

サービス プロファイル テンプレート

サービス プロファイル テンプレートを使用して、vNIC や vHBA の個数などの同じ基本パラメータ、および同じプールから取得された ID 情報を使ってすばやく複数のサービス プロファイルを作成できます。

ヒント 既存のサービス プロファイルに類似した値を持つ 1 つのサービス プロファイルだけが必要な場合は、Cisco UCS Manager GUI でサービス プロファイルを複製できます。

たとえば、データベース ソフトウェアをホストするサーバの設定に、類似した値を持つ数個のサービス プロファイルが必要である場合、手動、または既存のサービス プロファイルから、サービス プロファイル テンプレートを作成できます。 その後、このテンプレートを使用して、サービス プロファイルを作成します。

Cisco UCS は、次のタイプのサービス プロファイル テンプレートをサポートしています。

初期テンプレート

初期テンプレートから作成されたサービス プロファイルはテンプレートのプロパティをすべて継承します。 初期のサービス プロファイル テンプレートから作成されたサービス プロファイルはテンプレートにバインドされます。 ただし、初期のテンプレートに対して行われた変更は、バインドされたサービス プロファイルに自動的に伝播されません。 バインドされたサービス プロファイルに変更を伝播したい場合は、そのサービス プロファイルをアンバインドしてから、再び初期テンプレートにバインドします。

アップデート テンプレート

アップデート テンプレートから作成されたサービス プロファイルはテンプレートのプロパティをすべて継承し、そのテンプレートへの接続をそのまま保持します。 アップデート テンプレートを変更すると、このテンプレートから作成されたサービス プロファイルが自動的にアップデートされます。

ポリシー

ポリシーは、ある特定の状況で、Cisco UCS コンポーネントがどのように動作するかを決定します。 大半のポリシーで複数のインスタンスを作成することができます。 たとえば、サーバに応じて、PXEブート、SANブート、ローカルストレージからのブートを使い分けられるように、異なるブート ポリシーが必要になる場合があります。

ポリシーにより、システム内で機能を区別することができます。 対象事象のエキスパートは、その対象事象を専門としない他者により作成されたサービス プロファイルで使用されるポリシーを定義できます。 たとえば、LAN アドミニストレータは、そのシステムのアダプタ ポリシー、および Quality Of Service ポリシーを作成できます。 次に、LAN 管理に関する対象事項の専門知識が限られているか、あるいはまったく欠けている他者により作成されたサービス プロファイルで、これらのポリシーを使用できます。

Cisco UCS Manager では、次の 2 つのタイプのポリシーを作成し、使用できます。

- サーバおよびその他のコンポーネントを設定する設定ポリシー
- 特定の管理、モニタリング、およびアクセス コントロール機能を制御する操作ポリシー

プール

プールは、システムで使用できる ID のコレクション、物理リソース、または論理リソースです。 すべてのプールは、サービスプロファイルの柔軟性を高め、ユーザがシステム リソースを中央で集中管理できるようにするものです。

プールを使用して、未設定のサーバや、使用可能なサーバ ID 情報の範囲を、データセンターにとって意味のあるグループに分割することができます。 たとえば、類似する特性を持つ未設定のサーバのプールを作成して、このプールをサービス プロファイルに含めた場合、ポリシーを使用して、このサービス プロファイルと使用可能な未設定のサーバとの関連付けを形成することができます。

MAC アドレスなどの ID 情報をプールした場合、特定のアプリケーションをホストするサーバに範囲をあらかじめ割り当てることができます。 たとえば、MAC アドレス、UUID、および WWN の同じ範囲内のすべてのデータベース サーバを設定できます。

ドメイン プール

ドメイン プールは UCSCisco UCS ドメインにローカル的に定義され、そのCisco UCS ドメインでのみ使用できます。

グローバル プール

グローバル プールは Cisco UCS Central で定義され、Cisco UCS ドメイン間で共有できます。 Cisco UCS ドメインが Cisco UCS Central で登録されている場合は、Cisco UCS Manager にグローバル プールを割り当てることができます。

CIMC インバンド管理

マルチテナント、パブリックまたはプライベート サービス プロバイダー クラウド展開においてプロバイダー トラフィックからテナント トラフィックを分割したいという要望に応える形で、Cisco Integrated Management Controller（CIMC）へのインバンド管理アクセスの提供が推し進められました。 アウトオブバンド（OOB）管理トラフィックは、ファブリック インターコネクト内外を移動し、管理ポート経由で管理プレーンを通過します。 これにより、ボトルネックを引き起し、管理ポートで CPU の帯域幅に影響を及ぼす可能性があります。

インバンド管理によって、CIMC トラフィックはデータ トラフィックと同じパスを使用してアップリンク ポート経由でファブリック インターコネクトに入退出することができます。 アップリンク ポートに使用可能な高帯域幅は、インバンドアクセスが管理トラフィックを大幅に加速し、トラフィック ボトルネックと CPU 負荷のリスクを軽減することを意味します。 アウトオブバンド（OOB）およびインバンド アドレス プールの両方を、Cisco UCS Managerの管理アクセス用に設定できます。 アウトオブバンド アクセスは IPv4 アドレスのみをサポートしています。 インバンド アクセスは、IPv4 および IPv6 アドレス両方をサポートし、シングルまたはデュアル スタック管理が可能です。

Cisco UCS Manager のブレード サーバおよびラック サーバで設定できる 2 つの OOB 管理インターフェイス アドレスは以下になります。

- グローバル ext-mgmt プール経由で物理サーバに割り当てられた OOB IPv4 アドレス
- 物理サーバに関連付けられたサービス プロファイルから取得した OOB IPv4 アドレス

さらに、最大 4 つのインバンド管理インターフェイス アドレスを設定できます。

- 物理サーバに割り当てられたインバンド IPv4 アドレス
- 物理サーバに関連付けられたサービス プロファイルから取得したインバンド IPv4 アドレス
- 物理サーバに割り当てられたインバンド IPv6 アドレス
- 物理サーバに関連付けられたサービス プロファイルから取得したインバンド IPv6 アドレス

各サーバの複数のインバンド管理 IP アドレスは追加の CIMC セッションをサポートします。 OOB アドレスとインバンド アドレスの両方を設定すると、ユーザがサーバ、SSH to SoL、サービス プロファイル、KVM Launch Manager、または Cisco UCS Manager GUI の Web URL から KVM を開始するときに、[KVM Console] ダイアログボックスにあるこれらのアドレスのリストから選択することができます。

CIMC インバンド アクセスは次のサービスをサポートします。

- KVM コンソール
- SoL 用の CIMC への SSH
- ISO の vMedia、仮想 CD/DVD、リムーバブル ディスク、およびフロッピー

（注） Cisco UCS M3 および M4 サーバのみが、インバンド CIMC アクセスをサポートしています。Cisco UCS M1 および M2 サーバに対するインバンド CIMC アクセスはサポートされません。

IPv4 または IPv6 アドレスのインバンド IP プールを設定し、サーバにアドレスを割り当てるために使用できます。 インバンド VLAN グループを設定し、サービス プロファイルを使用してサーバに割り当てることができます。

サービス プロファイルおよびサービス プロファイル テンプレートでインバンド ネットワーク（VLAN）を選択するためには、インバンド VLAN グループでインバンド プロファイルを設定する必要があります。

インバンドプロファイルでネットワークおよびIPプール名を設定して、インバンドCIMCアドレスを Cisco UCS M3 および M4 サーバに割り当てることができます。

Cisco UCS Manager リリース 2.2 からのダウングレードの考慮事項

注意 Cisco UCS Manager をリリース 2.2 からリリース 2.1 以前にダウングレードする前に、次を含むすべてのインバンド設定を削除する必要があります。

- インバンドで設定されたサービス プロファイルからのインバンド設定
- インバンドで設定されたサービス プロファイル テンプレートからのインバンド設定
- インバンド アクセス用に設定されたサーバ CIMC IP アドレス
- IPv6 アドレスで設定された IP プールとアドレス ブロック
- LAN クラウドに関連付けられている、インバンド VLAN グループ、ネットワーク、IP プール名などの、グローバル ポリシーのインバンド プロファイル

ダウングレードの前にすべてのインバンド設定を削除しない場合、インバンド管理およびIPv6アドレッシングが Cisco UCS Manager リリース 2.1 以前でサポートされていないため、ダウングレード操作に失敗します。

インバンド管理サポート

インバンド管理アクセスは、以下の外部サービスに対しCisco UCS Managerでサポートされます。

- KVM
- ISO の vMedia、仮想 CD/DVD、リムーバブル ディスク、およびフロッピー
- SoL への SSH

IPv4 または IPv6 アドレスのインバンド IP プールを設定し、サーバにアドレスを割り当てるために使用できます。 インバンド VLAN グループを設定し、サービス プロファイルを使用してサーバに割り当てることができます。

トラフィック管理

オーバーサブスクリプション

オーバーサブスクリプションは、同じファブリックインターコネクトポートに複数のネットワークデバイスが接続されているときに発生します。 ポートが短時間でも最高速度で実行されることはほとんどないため、これにより、ファブリックインターコネクトの使用が最適化されます。 その結果、オーバーサブスクリプションが正しく設定されていれば、使用されていない帯域幅を活用できるようになります。 しかし、オーバーサブスクリプションの設定に間違いがあると、帯域幅のコンテンションが起こり、オーバーサブスクライブ ポートを使用しているすべてのサービスで Quality Of Service が低下します。

たとえば、4 つのサーバが 1 つのアップリンク ポートを共有していて、これらのサーバがすべて、このアップリンク ポートで使用できる帯域幅よりも大きい累積率でデータを送信しようとした場合に、オーバーサブスクリプションが発生します。

オーバーサブスクリプションにおける検討事項

Cisco UCS ドメインでのオーバーサブスクリプションの設定に影響を与える要因は次のとおりです。

アップリンク ポートに対するサーバに面したポートの比率

この比率はパフォーマンスに影響を与えるため、システム内のサーバに面したポートの数と、アップリンク ポートの数を知っている必要があります。 たとえば、使用しているシステムに、サーバと通信できるポートが 20 個あるときに、ネットワークと通信できるポートが 2 つだけの場合、このアップリンク ポートはオーバーサブスクライブされます。 この状況では、サーバにより作成されるトラフィックの量もパフォーマンスに影響を与えます。

ファブリック インターコネクトからネットワークへのアップリンク ポートの数

Cisco UCS ファブリック インターコネクトと LAN の上位層の間にさらにアップリンク ポートを追加して、帯域幅を増やすことができます。 Cisco UCS では、すべてのサーバと NIC が確実に LAN にアクセスできるようにするために、ファブリック インターコネクト 1 つにつき、少なくとも 1 つのアップリンク ポートが必要です。 LAN アップリンクの数は、すべての Cisco UCS サーバで使用される帯域幅の合計により決定されます。

6100 シリーズ ファブリック インターコネクトでは、ファイバ チャネル アップリンク ポートは、拡張スロットだけで使用できます。 使用可能なファイバ チャネル アップリンクの数を増やすには、拡張スロットを追加する必要があります。 イーサネット アップリンク ポートは、固定スロットと拡張スロットに存在できます。

Cisco UCS Manager のバージョン 2.0 以降を実行している 6200 シリーズ ファブリック インターコネクトの場合、イーサネット アップリンク ポートとファイバ チャネル アップリンク ポートは、ベース モジュールと拡張モジュールの両方で設定可能です。

たとえば、2 つの Cisco UCS 5100 シリーズ シャーシに、ハーフ幅の Cisco UCS B200-M1 サーバがいっぱいに入っている場合、サーバの数は 16 台です。 ファブリック インターコネクト 1 つあたり LAN アップリンクが 1 つのクラスタ設定では、これら 16 台のサーバは 20GbE の LAN 帯域幅を共有します。 より大きい容量が必要である場合、ファブリック インターコネクトからさらにアップリンクを追加する必要があります。 クラスタ設定では、アップリンクを対称設定にすることを推奨します。 この例で、ファブリック インターコネクト 1 つにつき使用されるアップリンクの数が 4 つである場合、16 台のサーバが 80GB の帯域幅を共有することになるため、各サーバの容量は約 5GB になります。 Cisco UCS ファブリック インターコネクトで複数のアップリンクが使用されている場合、この容量を最大限有効活用するために、ネットワーク設計チームはポート チャネルの使用を検討する必要があります。

I/O モジュールからファブリック インターコネクトへのアップリンク ポートの数

使用するアップリンク ポートの数とケーブルの本数を増やすことにより、I/O モジュールとファブリック インターコネクトの間の帯域幅を増やすことができます。 Cisco UCS では、I/O モジュールと Cisco UCS 6100 シリーズ ファブリック インターコネクトを接続するために、ケーブルを 1 本、2 本、または 4 本使用できます。 2208 I/O モジュールと 6248 ファブリック インターコネクトを接続すると、最大 8 本のケーブルを使用できます。 ケーブルの本数により、アクティブ アップリンク ポートの数、およびオーバーサブスクリプションの比率が決定されます。

サーバからファブリック インターコネクトへのアクティブ リンクの数

各サーバで使用可能なオーバーサブスクライブされていない帯域幅の量は、使用する I/O モジュール数と、それらの I/O モジュールをファブリック インターコネクトに接続するために使用するケーブル数によって異なります。 別の I/O モジュールを設置すると、サーバに追加の帯域幅と冗長性が提供されます。 設計のこのレベルの柔軟性により、80 Gbps（それぞれ 4 つのリンクを持つ 2 つの I/O モジュール）から 10 Gbps（1 つのリンクを持つ 1 つの I/O）までの任意の帯域幅をシャーシに提供できます。

シャーシに対し 80 Gbps を提供する場合、Cisco UCS ドメインの各ハーフ幅サーバが、オーバーサブスクライブされていない設定で最大 10 Gbps に達し、2:1 オーバーサブスクリプションで最大 20 Gbps 使用できます。

オーバーサブスクリプションの概算に関するガイドライン

ファブリック インターコネクト ポートに対する最適なオーバーサブスクリプション率を概算する場合は、次のガイドラインを考慮してください。

コスト/パフォーマンス スライダ

コストとパフォーマンスの優先順位付けは、データセンターによってそれぞれ異なり、オーバーサブスクリプションの設定に直接影響します。 オーバーサブスクリプションにおけるハードウェアの使用方法を計画する場合は、このスライダでデータセンターが位置する場所を知る必要があります。 たとえば、データセンターでコストよりもパフォーマンスを重視する場合は、オーバー

サブスクリプションを最小限に抑えることができます。 しかし、ほとんどのデータセンターでは、コストは大きい影響を与える要因であるため、オーバーサブスクリプションは慎重に計画する必要があります。

帯域幅使用状況

各サーバで実際に使用されると予想される帯域幅の概算値は、ファブリック インターコネクト ポートへの各サーバの割り当て、およびその結果からポートのオーバーサブスクリプション率を決定するときに重要です。 オーバーサブスクリプションでは、サーバにより消費されるトラフィックの平均値（単位はGB）、設定された帯域幅に対する使用された帯域幅の比率、および帯域幅の使用が上昇する時間を考慮する必要があります。

ネットワーク タイプ

ネットワーク タイプは、アップリンク ポート上のトラフィックだけに関係します。これは、Cisco UCS 以外のところには、FCoE は存在しないからです。 その他のデータセンター ネットワークは、LAN と SAN トラフィックを区別するだけです。 したがって、ファブリック インターコネクト ポートのオーバーサブスクリプションの概算を行う場合、ネットワーク タイプを考慮する必要はありません。

ピン接続

Cisco UCS でのピン接続は、アップリンク ポートだけに関係します。 イーサネット トラフィック、または FCoE トラフィックをあるサーバから、特定のアップリンク イーサネット ポート、またはアップリンク FC ポートにピン接続することができます。

物理サーバと仮想サーバの両方の NIC および HBA をアップリンク ポートにピン接続する場合、ファブリック インターコネクトからユニファイド ファブリックを制御できるようにします。 この制御により、アップリンク ポートの帯域幅の利用がさらに最適化されます。

Cisco UCS は、ピン グループを使用して、どの NIC、vNIC、HBA、vHBA をアップリンク ポートにピン接続するかを管理します。 サーバにピン接続を設定するには、ピン グループを直接的に割り当てるか、ピン グループを vNIC ポリシーに含ませてから、サーバに割り当てられたサービス プロファイルにその vNIC ポリシーを追加します。 サーバ上の vNIC または vHBA からのトラフィックはすべて、I/O モジュールを通って、同じアップリンク ポートに進みます。

サーバ トラフィックのサーバ ポートへのピン接続

サーバ トラフィックはすべて、I/Oモジュールを経由して、ファブリックインターコネクトのサーバポートへ進みます。 このトラフィックがどのようにピン接続されるかは、シャーシに設定されるリンクの数によって決まります。

ピン接続により、どのサーバ トラフィックが、ファブリック インターコネクトのどのサーバ ポートに進むかが決まります。 このピン接続は固定されています。 変更できません。 したがって、シャーシに対する帯域幅の適切な割り当てを決定する場合、サーバの位置を考慮する必要があります。

（注） サーバをスロットに割り当てる前に、ポートからリンクへの割り当てを見直す必要があります。 ケーブルで接続するポートはI/Oモジュールのポート1およびポート2である必要はありません。 ファブリック インターコネクトと I/O モジュールの間のリンク数を変更した場合、トラフィックを再ルーティングするには、シャーシを再認識する必要があります。

ポート番号はすべて、この I/O モジュールのファブリック インターコネクト側ポートを参照します。

1 つの I/O モジュールを持つシャーシ（ファブリック ポート チャネルの場合は設定されません）

（注） サーバ内のアダプタがアダプタ ポート チャネルに対しサポートを行い設定されている場合、これらのポートチャネルは、次の表に示すように、同一のリンクにピン接続されます。 シャーシ内の I/O モジュールがファブリック ポート チャネルに対しサポートを行い設定されている場合、サーバ スロットは、個々のリンクではなくファブリック ポート チャネルにピン接続されます。

シャーシのリンク	リンク 1/ファブリック ポート チャネル	リンク 2	リンク 3	リンク 4	リンク 5	リンク 6	リンク 7	リンク 8
1 リンク	すべてのサーバスロット	なし	なし	なし	なし	なし	なし	なし
2 リンク	サーバスロット 1、3、5、および 7	サーバスロット 2、4、6、および 8	なし	なし	なし	なし	なし	なし
4 リンク	サーバスロット 1 および 5	サーバスロット 2 および 6	サーバスロット 3 および 7	サーバスロット 4 および 8	なし	なし	なし	なし
8 リンク	サーバスロット 1	サーバスロット 2	サーバスロット 3	サーバスロット 4	サーバスロット 5	サーバスロット 6	サーバスロット 7	サーバスロット 8
ファブリック ポート チャネル	すべてのサーバスロット	該当なし	該当なし	該当なし	該当なし	該当なし	該当なし	該当なし

I/O モジュールを 2 つ持つシャーシ

シャーシに I/O モジュールが 2 つある場合、片方の I/O モジュールからのトラフィックは、ファブリック インターコネクトの 1 つに進み、もう 1 つの I/O モジュールからのトラフィックは、2 つめのファブリック インターコネクトに進みます。 1 つのファブリック インターコネクトに 2 つの I/O モジュールを接続できません。

vNIC で設定されたファブリック インターコネクト	サーバ トラフィック パス
A	サーバ トラフィックはファブリック インターコネクト A に向かいます。 A に不具合が生じた場合、サーバ トラフィックは B にフェールオーバーしません。
B	すべてのサーバ トラフィックはファブリック インターコネクト B に向かいます。 B に不具合が生じた場合、サーバ トラフィックは A にフェールオーバーしません。
A-B	すべてのサーバ トラフィックはファブリック インターコネクト A に向かいます。 A に不具合が生じた場合、サーバ トラフィックは B にフェールオーバーします。
B-A	すべてのサーバ トラフィックはファブリック インターコネクト B に向かいます。 B に不具合が生じた場合、サーバ トラフィックは A にフェールオーバーします。

ピン接続に関するガイドライン

ピン グループおよびアップリンク ポートに対するピン接続における最適な設定を判断する場合、サーバについて予想される帯域幅使用状況を考慮します。 システムに含まれるサーバの一部が大量の帯域幅を使用することがわかっている場合は、必ず、これらのサーバを別のアップリンク ポートにピン接続してください。

Quality of Service

Cisco UCS は、Quality of Service を実装するために、次の方法を提供しています。

- 特定のタイプのトラフィックに対するグローバル設定をシステム全体にわたって指定するためのシステム クラス
- 個々の vNIC にシステム クラスを割り当てる QoS ポリシー

- アップリンク イーサネット ポートによるポーズ フレームの扱い方法を決定するフロー制御ポリシー

システム クラス

Cisco UCS は、DCE（Data Center Ethernet）を使用して、Cisco UCS ドメイン内のすべてのトラフィックを処理します。 イーサネットに対するこの業界標準の機能拡張では、イーサネットの帯域幅が 8 つの仮想レーンに分割されています。 内部システムと管理トラフィック用に 2 つの仮想レーンが予約されています。 それ以外の 6 つの仮想レーンの Quality of Service（QoS）を設定できます。 Cisco UCS ドメイン全体にわたり、これら 6 つの仮想レーンで DCE 帯域幅がどのように割り当てられるかは、システム クラスによって決定されます。

各システム クラスは特定のタイプのトラフィック用に帯域幅の特定のセグメントを予約します。 これにより、過度に使用されるシステムでも、ある程度のトラフィック管理が提供されます。 たとえば、ファイバ チャネル プライオリティ システム クラスを設定して、FCoE トラフィックに割り当てられる DCE 帯域幅の割合を決定することができます。

次の表は、設定可能なシステム クラスをまとめたものです。

表 *1*：システム クラス

システム クラス	説明
プラチナ ゴールド シルバー ブロンズ	サービスプロファイルの QoS ポリシーに含めることができる設定可能なシステム クラスのセット。 各システム クラスはトラフィック レーンを 1 つ管理します。 これらのシステム クラスのプロパティはすべて、カスタム設定やポリシーを割り当てるために使用できます。
ベスト エフォート	ベーシック イーサネット トラフィックのために予約されたレーンに対する QoS を設定するシステム クラス。 このシステム クラスのプロパティの中には、あらかじめ設定されていて、変更できないものもあります。 たとえば、このクラスには、必要に応じてデータ パケットのドロップを許可するドロップ ポリシーがあります。 このシステム クラスは無効にできません。

システム クラス	説明
ファイバ チャネル	Fibre Channel over Ethernet トラフィックのために予約されたレーンに対する Quality of Service を設定するシステム クラス。 このシステム クラスのプロパティの中には、あらかじめ設定されていて、変更できないものもあります。 たとえば、このクラスには、データ パケットが絶対にドロップされないことを保証するドロップなしポリシーがあります。 このシステム クラスは無効にできません。 （注） FCoE トラフィックには、他のタイプのトラフィックで使用できない、予約された QoS システム クラスがあります。 他のタイプのトラフィックに、FCoE で使用される CoS 値がある場合、その値は 0 にリマークされます。

Quality of Service ポリシー

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

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

フロー制御ポリシー

フロー制御ポリシーは、ポートの受信バッファがいっぱいになったときに、Cisco UCS ドメインのアップリンク イーサネット ポートが IEEE 802.3x ポーズ フレームを送信および受信するかどうかを決定します。 これらのポーズフレームは、バッファがクリアされるまでの数ミリ秒間、送信側ポートからのデータの送信を停止するように要求します。

LAN ポートとアップリンク イーサネット ポートの間でフロー制御が行われるようにするには、両方のポートで、対応する受信および送信フロー制御パラメータを有効にする必要があります。 Cisco UCSでは、これらのパラメータはフロー制御ポリシーにより設定されます。

送信機能を有効にした場合、受信パケット レートが高くなりすぎたときに、アップリンクイーサネット ポートはネットワーク ポートにポーズ要求を送信します。 ポーズは数ミリ秒有効になった後、通常のレベルにリセットされます。 受信機能を有効にした場合、アップリンクイーサネット ポートは、ネットワーク ポートからのポーズ要求すべてに従います。 ネットワーク ポートがポーズ要求をキャンセルするまで、すべてのトラフィックはこのアップリンク ポートで停止します。

ポートにフロー制御ポリシーを割り当てているため、このポリシーを変更すると同時に、ポーズフレームやいっぱいになっている受信バッファに対するポートの反応も変わります。

オプトイン機能

各Cisco UCS ドメインは、すべての機能に対してライセンスされています。 システムの設定方法に応じて、既存の環境への統合を簡単にするために、一部の機能をオプトインするか、これらをオプトアウトするかを決定することができます。 プロセスの変化が起こった場合、システム設定を変更して、オプトイン機能の 1 つまたは両方を加えることができます。

オプトイン機能は次のとおりです。

- サーバ、アダプタなどの各コンポーネントがステートレスであるプールおよびポリシーを持つモバイル サービス プロファイルを利用するステートレス コンピューティング
- 組織およびロールベースのアクセス コントロールを使用して、システムを複数の小さな論理セグメントに分割するマルチテナント機能

ステートレス コンピューティング

ステートレスコンピューティングにより、サービスプロファイルを使用して、あるサーバの固有情報を同じ Cisco UCS ドメイン内の別のサーバに適用できます。 サーバの固有情報には、サーバを認識し、Cisco UCS ドメイン内で一意にするために要素が含まれます。 これらの要素のいずれかを変更すると、サーバはブート ステータスのアクセス、使用、実現ができなくなります。

サーバの固有情報を構成する要素は次のとおりです。

- ファームウェア バージョン
- UUID（サーバの識別に使用される）
- MAC アドレス（LAN 接続に使用される）
- ワールド ワイド名（SAN 接続に使用される）
- ブート設定

ステートレス コンピューティングは、高度に柔軟なサーバを使ったダイナミックなサーバ環境を作成します。 Cisco UCS ドメイン内の物理サーバはすべて、サービス プロファイルとの関連付けが形成されるまで匿名のままです。その後、サービス プロファイルでこのサーバの ID が設定されます。 このサーバでのビジネス サービスが必要なくなったら、このサーバをシャットダウンし、サービス プロファイルの関連付けを解除してから、同じ物理サーバについて異なる ID を作成するために別のサービスプロファイルとの関連付けを形成します。 この「新しい」サーバは、別のビジネス サービスをホストできます。

ステートレス状態の柔軟性をフルに活用するためには、サーバのオプション ローカルディスクはスワップ用スペースまたは一時スペースだけに使用し、オペレーティング システムやアプリケーション データの保存には使用しないでください。

Cisco UCS ドメインのすべての物理サーバに対して、ステートレス コンピューティングを完全に実装することもできますし、ステートレス サーバを使用しないことを選択することもできます。また、これら 2 種類を混在させることも可能です。

ステーレス コンピューティングをオプトインする場合

Cisco UCS ドメイン内の物理サーバはそれぞれ、サービス プロファイルで定義されます。 どのようなサーバでも、あるアプリケーションのセットをホストするために使用しているときに、データセンターの必要に応じて、別のアプリケーションやビジネス サービスのセットに割り当てなおすことができます。

この Cisco UCS ドメインで定義されているポリシーやリソースのプールをポイントするサービス プロファイルを作成します。 サーバ プール、WWN プール、および MAC プールにより、未割り当てのリソースはすべて、必要に応じて使用できることが保証されます。 たとえば、物理サーバで不具合が発生した場合、サービス プロファイルをすぐに別のサーバに割り当てることができます。 サービス プロファイルは、WWN や MAC アドレスを含め、オリジナルのサーバと同じ ID を新しいサーバに与えるため、データセンター インフラストラクチャの残りの部分では、この新しいサーバとオリジナルのサーバは同じものと認識されます。LAN や SAN で設定を変更する必要はありません。

ステートレス コンピューティングからオプトアウトする場合

Cisco UCS ドメイン内の各サーバは、従来のラックマウント型サーバとして扱われます。

ハードウェアに書き込まれた ID 情報を継承するサービス プロファイルを作成し、これらのプロファイルを使用して、サーバに対する LAN または SAN 接続を設定します。 ただし、サーバ ハードウェアに不具合が発生した場合、サービス プロファイルを新しいサーバに割り当てることはできません。

マルチテナント機能

マルチテナント機能を使用すると、Cisco UCS ドメインの大きな物理的インフラストラクチャを組織と呼ばれる論理的なエンティティに分割することができます。 その結果、各組織に専用の物理インフラストラクチャを設けなくても各組織を論理的に分離できます。

マルチテナント環境では、関連する組織を通じて、各テナントに一意のリソースを割り当てられます。 これらのリソースには、各種のポリシー、プール、および Quality of Service 定義などがあります。 また、すべてのユーザにすべての組織へのアクセス権を付与する必要がない場合は、ロケールを実装して、組織ごとにユーザ権限やロールを割り当てたり、制限したりすることもできます。

マルチテナント環境をセットアップすると、すべての組織が階層的になります。 最上位の組織は常にルートです。 ルートに作成したポリシーおよびプールはシステム全体にわたるもので、このシステムに含まれるすべての組織で使用できます。 しかし、他の組織で作成されたポリシーやプールが使用できるのは、同じ階層でそれより上にある組織だけです。 たとえば、あるシステムに Finance と HR という組織があり、これらは同じ階層に存在しないとします。この場合、Finance は HR 組織にあるポリシーは一切使用できず、また、HR は Finance 組織にあるポリシーには一切アクセスできません。 しかし、Finance と HR は両方とも、ルート組織にあるポリシーやプールを使用できます。

マルチテナント環境に組織を作成する場合、各組織、または同じ階層のサブ組織に対して、次のうちの 1 つ以上をセットアップすることもできます。

- リソース プール
- ポリシー
- サービス プロファイル
- サービス プロファイル テンプレート

マルチテナント機能を選択する場合

各 Cisco UCS ドメインは複数の異なる組織に分割されます。 マルチテナント機能の実装で作成される組織のタイプは、企業のビジネスニーズによって異なります。たとえば、次の単位を表す組織があげられます。

- マーケティング、財務、エンジニアリング、人事など、企業内のエンタープライズ グループまたは部門
- サービス プロバイダーに対するさまざまなカスタマー、またはネーム サービス ドメイン

管理が認可されている組織だけにユーザがアクセスできるように、ロケールを作成することができます。

マルチテナント機能を選択しない場合

Cisco UCS ドメインは、ルート組織にすべてのデータが入った 1 つの論理エンティティのままです。 すべてのポリシーおよびリソース プールは、この Cisco UCS ドメイン内のどのサーバにでも割り当てることができます。

Cisco UCSのバーチャライゼーション

バーチャライゼーションの概要

仮想化により、同一の物理マシン上で隣り合いながら分離して実行する複数の仮想マシン（VM）を作成できます。

各仮想マシンは、仮想ハードウェア（メモリ、CPU、NIC）の独自のセットを持ち、その上でオペレーティング システムと十分に設定されたアプリケーションがロードされます。 オペレーティング システムは、実際の物理ハードウェア コンポーネントに関係なく、一貫性があり正常なハードウェア一式を認識します。

仮想マシンでは、物理サーバ間でのプロビジョニング、移動を迅速に行うために、ハードウェアとソフトウェアの両方が単一のファイルにカプセル化されます。 仮想マシンは 1 つの物理サーバから別のサーバへ数秒で移動することができ、メンテナンスのためのダウンタイムを必要とせず、途切れることのない作業負荷を集約します。

仮想ハードウェアは、多数のサーバ（それぞれのサーバは独立した仮想マシン内で実行する）を単一の物理サーバ上で実行できるようにします。 バーチャライゼーションの利点は、コンピュー

ティング リソースをより適切に使用でき、サーバ密度を高め、サーバの移行をスムーズに行えることです。

Cisco Virtual Machine ファブリック エクステンダの概要

仮想サーバの実装は、1 つの物理サーバのゲストとして実行される 1 つまたは複数の VM で構成されます。 ゲスト VM は、ハイパーバイザまたは仮想マシン マネージャ（VMM）と呼ばれるソフトウェア レイヤによってホストされ管理されます。 通常、ハイパーバイザは各 VM で仮想ネットワーク インターフェイスを示し、VM から他のローカル VM または別のインターフェイスへの外部ネットワークへのトラフィックのレイヤ 2 スイッチングを実行します。

Cisco Virtual Interface Card（VIC）アダプタと連携して、Cisco 仮想マシン ファブリック エクステンダ（VM-FEX）はファブリック インターコネクトの外部ハードウェア ベース スイッチング用のハイパーバイザによって、VM トラフィックのソフトウェア ベースのスイッチングをバイパスします。 この方法により、サーバの CPU 負荷を軽減し、高速スイッチングを行い、ローカルおよびリモート トラフィックに豊富なネットワーク管理機能セットを適用することができます。

VM-FEX は IEEE 802.1Qbh ポート エクステンダ アーキテクチャを VM に拡張するために、各 VM インターフェイスに仮想 Peripheral Component Interconnect Express（PCIe）デバイスとスイッチ上の仮想ポートを提供します。 このソリューションにより、VMインターフェイス上で、正確なレート制限と QoS（Quality of Service）保証が可能になります。

ネットワーク インターフェイス カードと統合ネットワーク アダプタを使用したバーチャライゼーション

ネットワーク インターフェイス カード（NIC）と統合ネットワーク アダプタによって、標準的な VMware のサーバにインストールされた ESX との統合による仮想環境と、VC から実行されるすべての仮想マシンの管理がサポートされます。

仮想マシンのポータビリティ

サービス プロファイルを実装すると、1 つのサーバから別のサーバに、サーバの識別情報を簡単に移動できるようになります。 新規サーバをイメージ化すると、ESX はそのサーバを元のサーバのように扱います。

同一サーバ上の仮想マシン間の通信

これらのアダプタは、同一サーバ上の仮想マシン間における標準の通信手段を実装します。 ESX ホストが複数の仮想マシンを含む場合、すべての通信はサーバ上の仮想スイッチを通過させる必要があります。

システムでネイティブな VMware ドライバを使用する場合、仮想スイッチはネットワーク管理者のドメインには参加せず、どのネットワーク ポリシーの制約も受けません。 結果として、たとえば、ネットワークの QoS ポリシーは、仮想スイッチを通って VM1 から VM2 に流れるどのデータ パケットにも適用されません。

Nexus 1000 などの別の仮想スイッチがシステムに含まれている場合、その仮想スイッチは、ネットワーク管理者がそのスイッチ上で設定したネットワーク ポリシーに従います。

仮想インターフェイス カード アダプタでのバーチャライゼーション

Cisco VIC アダプタは、単一 OS の導入と VM ベースの導入の両方に対応するように設計された統合型ネットワーク アダプタ（CNA）です。 VIC アダプタは、最大 128 個の仮想ネットワーク インターフェイス カード（vNIC）を含む、静的または動的な仮想化インターフェイスをサポートします。

VIC アダプタは、VM-FEXをサポートし、仮想マシン インターフェイスとの間の、トラフィックのハードウェアベースのスイッチング機能を提供します。