Cisco UCS Mini 向け Cisco UCS Manager リリース 3.0 CLI コンフィギュレーション ガイド

初版：2014 年 07 月 14 日

最終更新：2015 年 03 月 09 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

はじめに

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	表示
GUI 要素	タブの見出し、領域名、フィールドのラベルのようなGUI要素は、[GUI要素] のように示しています。 ウィンドウ、ダイアログボックス、ウィザードのタイトルのようなメイン タイトルは、[メインタイトル] のように示しています。
マニュアルのタイトル	マニュアルのタイトルは、イタリック体（*Italic*）で示しています。

テキストのタイプ	表示
TUI 要素	テキストベースのユーザ インターフェイスでは、システムによって表示されるテキストは、courier フォントで示しています。
システム出力	システムが表示するターミナル セッションおよび情報は、courier フォントで示しています。
CLI コマンド	CLI コマンドのキーワードは、ボールド体 **this font** で示しています。 CLI コマンド内の変数は、イタリック体 *this font* 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。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

ワンポイント アドバイス　「時間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。

警告　安全上の重要事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。機器の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。各警告の最後に記載されているステートメント番号を基に、装置に付属の安全についての警告を参照してください。

SAVE THESE INSTRUCTIONS

関連する Cisco UCS ドキュメント

ドキュメント ロードマップ

すべての B シリーズ マニュアルの完全なリストについては、『*Cisco UCS B-Series Servers Documentation Roadmap*』（URL：http://www.cisco.com/go/unifiedcomputing/b-series-doc）を参照してください。

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

管理用の 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、Twitter の Cisco UCS Docs 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、mailto:ucs-docfeedback@cisco.com までご連絡ください。ご協力をよろしくお願いいたします。

第 1 章

新機能および変更情報

この章の内容は、次のとおりです。

このリリースの新規情報および変更情報

次の表に、最新リリースに関するこのガイドでの重要な変更点の概要を示します。ただし、このリリースに関するコンフィギュレーション ガイドの変更点や新機能の中には一部、この表に記載されていないものもあります。このリリースで新しくサポートされるハードウェアについては、『*Cisco UCS B-Series Servers Documentation Roadmap*』（URL：http://www.cisco.com/go/unifiedcomputing/b-series-doc） を参照してください。

表 *1*：*Cisco UCS* リリース *3.0(2)* の新機能と動作変更

機能	説明	参照先
PSU ファームウェア管理	PSU でファームウェアを管理できます。	この機能は、次の設定ガイドで説明されています。 • 『*Cisco UCS GUI Firmware Management Guide for Cisco UCS Mini*』 • 『*Cisco UCS CLI Firmware Management Guide for Cisco UCS Mini*』 ファームウェアの管理ガイドは次の URL から確認できます。http://www.cisco.com/en/US/products/ps10281/products_installation_and_configuration_guides_list.html
NetFlow のモニタリング	netflow 対応ルータから IP トラフィック データを収集できます。	この機能は、次の設定ガイドで説明されています。 • 『*Cisco UCS B-Series GUI System Monitoring Guide for Cisco UCS Mini*』 • 『*Cisco UCS B-Series CLI System Monitoring Guide for Cisco UCS Mini*』 システム モニタリング ガイドは次の URL から確認できます。http://www.cisco.com/en/US/products/ps10281/products_installation_and_configuration_guides_list.html
LACP	Link Aggregation Control Protocol（LACP）ポリシーを使用して、リンク集約グループをさらに制御できます。	LACP ポリシー，（335 ページ）

機能	説明	参照先
消耗レベルのモニタリング	特定の Cisco UCS ブレード サーバで、ソリッド ステート ドライブの寿命をモニタリングできます。	この機能は、次の設定ガイドで説明されています。 • 『*Cisco UCS B-Series GUI System Monitoring Guide for Cisco UCS Mini*』 • 『*Cisco UCS B-Series CLI System Monitoring Guide for Cisco UCS Mini*』 システム モニタリング ガイドは次の URL から確認できます。http://www.cisco.com/en/US/products/ps10281/products_installation_and_configuration_guides_list.html
CIMC セキュリティの機能拡張	リモート接続を制限し、vMedia 暗号化を使用できます。	CIMC セキュリティ ポリシー, （503 ページ）
グラフィックス カードのモニタリング	特定の Cisco UCS ラック サーバで、グラフィックス カードとコントローラのプロパティを表示できます。	この機能は、次の設定ガイドで説明されています。 • 『*Cisco UCS B-Series GUI System Monitoring Guide for Cisco UCS Mini*』 • 『*Cisco UCS B-Series CLI System Monitoring Guide for Cisco UCS Mini*』 システム モニタリング ガイドは次の URL から確認できます。http://www.cisco.com/en/US/products/ps10281/products_installation_and_configuration_guides_list.html

機能	説明	参照先
自動インストールファームウェアの機能拡張	アップグレードする前に、警告と潜在的な問題のリストを表示できます。	この機能は、次の設定ガイドで説明されています。 • 『*Cisco UCS GUI Firmware Management Guide for Cisco UCS Mini*』 • 『*Cisco UCS CLI Firmware Management Guide for Cisco UCS Mini*』 ファームウェアの管理ガイドは次のURLから確認できます。http://www.cisco.com/en/US/products/ps10281/products_installation_and_configuration_guides_list.html
スクリプト可能な vMedia のサポート	リモート ファイルの場所から仮想メディアをマウントできます。CLIおよびWebGUI CIMCインターフェイスを通じて使用できます。この機能は、NFS、CIFS、HTTP、HTTPS などの、複数の共有タイプに対応しています。	CIMC マウント vMedia, （569 ページ）
コミュニティ VLAN のサポート	ファブリック インターコネクトでコミュニティ VLAN を作成でき、特定のプライマリ VLAN で複数のコミュニティ VLAN を維持できます。また、サーバvNICのコミュニティ アクセスと共に、無差別アクセスとトランク モードもサポートします。	コミュニティ VLAN, （271 ページ）

機能	説明	参照先
ロギング エクスポータ	ログ ファイルが削除される前に、リモート サーバにエクスポートできます。	この機能は、次の設定ガイドで説明されています。 • *Cisco UCS B-Series CLI System Monitoring Guide for Cisco UCS Mini* システム モニタリング ガイドは次の URL から確認できます。http://www.cisco.com/en/US/products/ps10281/products_installation_and_configuration_guides_list.html
Anonymous Reporting	SMTP サーバから匿名レポートを取得できます。この機能は、Call Home がディセーブルである場合でもイネーブルにできます。	この機能は、次の設定ガイドで説明されています。 • *Cisco UCS B-Series GUI System Monitoring Guide for Cisco UCS Mini* • *Cisco UCS B-Series CLI System Monitoring Guide for Cisco UCS Mini* システム モニタリング ガイドは次の URL から確認できます。http://www.cisco.com/en/US/products/ps10281/products_installation_and_configuration_guides_list.html
ファブリック インターコネクトの情報ポリシー	Cisco UCS に接続されたアップリンク スイッチが表示されます。ファブリック インターコネクトの情報ポリシーを有効にすると、ファブリック インターコネクトの LAN および SAN ネイバーを表示できます。	ファブリック インターコネクトの情報ポリシーの設定
イベント検出とアクション	NiErrStats ポリシーを使用して、アクティブなネットワーク インターフェイス ポートのエラー統計情報を取得します。取得した情報は Cisco UCS Manager に送信されます。	イベント検出とアクション, （111 ページ）

機能	説明	参照先
DIMMのブラックリスト化のサポート	Cisco UCS C シリーズ ラック サーバがサポートされるようになりました。	DIMMのブラックリスト化, （527 ページ）
C ダイレクト ラック ライセンス	C ダイレクト ラック ライセンスはラック サーバに接続されたポートでサポートされます。	C ダイレクト ラックのライセンスのサポート, （121 ページ）
CIMC セキュア ブート	Ciscoの署名付きファームウェア イメージのみが、Cisco C シリーズ ラック サーバ上でインストールおよび実行できます。	CIMC セキュア ブート, （578 ページ）
UEFI セキュア ブート	Cisco UCS C シリーズ ラック サーバがサポートされるようになりました。	サーバ ブートの設定, （575 ページ）
FX3S コントローラ	SD カードで更新したコントローラにより、コントローラのリセット、SD カードのフォーマット、ペアの SD カードの自動同期の有効化を行うことができます。	FlexFlash FX3S のサポート, （517 ページ）

第 2 章

Cisco Unified Computing System の概要

この章の内容は、次のとおりです。

Cisco Unified Computing System について

Cisco Unified Computing System（Cisco UCS）は、アクセス レイヤ ネットワーキングおよびサーバを結合します。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 のアーキテクチャを単純化することにより、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 つの管理ドメインの下にとどまり、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 では、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。このような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。

サーバ仮想化に向けた最適化

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、サーバ仮想化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。このことは、次の理由により重要です。

- 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している Cisco UCS Manager の機能はすべて、IPv6 もサポートします。

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

IPv6 アドレスは、管理インターフェイス、Cisco Cisco UCS Manager GUI、KVM コンソール、および SSH over SoL 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
- Flash 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

ファブリック インターコネクト

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ています。
クラスタ 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、クラスタ設定が有効になっている場合に、続いてファブリック B が設定されると、セットアップ プロセスはファブリック 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。
初期セットアップの完了後、アウトオブバンド（OOB）アクセス用に、両方のファブリック インターコネクトに IPv4 アドレスを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 と IPv6 の両方のアドレスで 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

IIPv6 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 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 サーバでは 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。個々のサービス プロファイルには、特別な目的、つまり関連するサーバ ハードウェアで、ホストするアプリケーションのサポートに必要な設定が行われていることを保証する役割があります。

サービス プロファイルは、サーバ ハードウェア、インターフェイス、ファブリックの接続性、サーバおよびネットワークの ID に関する設定情報を維持します。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る必要があります。

重要 どのようなときでも、1 台のサーバに 1 つのサービス プロファイルだけを関連付けられます。同様に、1 つのサービス プロファイルは、一度にサーバ 1 つだけに関連付けられます。

サービスプロファイルとサーバとの関連付けを形成すると、このサーバにオペレーティング システムとアプリケーションをインストールできるようになります。また、サービス プロファイルを使用して、サーバの設定を確認することができます。サービス プロファイルとの関連付けを形成しているサーバで不具合が発生しても、サービス プロファイルが自動的に別のサーバにフェールオーバーすることはありません。

サービス プロファイルとサーバとの関連付けが解除されると、このサーバの ID および接続情報は、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、サーバに対して、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、そのサービス プロファイルの情報を使用して Cisco UCS の内部ファブリックが設定されます。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

これらのハードウェア 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。このプロファイルでは、アソシエーション時にサーバに設定されていた 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対して透過的です。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る場合を除き、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 による新規サーバの互換性チェックは実行されません。両方のハードウェアが似ていない場合、関連付け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。

初期テンプレートと既存のテンプレート

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。

（注） 初期テンプレートと標準のサービス プロファイルから作成されたサービス プロファイルは、[リセット（Reset）]がクリックされると、順次プール内で使用可能な最小の ID を取得します。

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、[リセット（Reset）] がクリックされると、順次プール内のより小さい ID が未使用の場合でも、同じ ID を保持します。

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。各分野の専門家は、その分野に関する専門知識を持た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。その後、これらのポリシーは、LAN 管理に関する専門的な知識を持たない、または知識が限定されている他者によって作成されたサービス プロファイルで使用できます。

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向上させ、システムリソースの集中管理を可能します。

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、特性が似ている未設定のサーバのプールを作成し、そのプールをサービス プロファイルに含めると、ポリシーを使用して、サービス プロファイルと使用可能な未設定のサーバを関連付けることができます。

MAC アドレスなどの ID 情報をプールすると、特定のアプリケーションをホストするサーバに事前に範囲を割り当てることができます。たとえば、すべてのデータベース サーバに同じ範囲の MAC アドレス、UUID、WWN を設定できます。

ドメイン プール

ドメイン プールは、Cisco UCS ドメイン でローカルに定義され、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 に登録されている場合、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 ブレードおよびラック サーバで設定できる 2 つの OOB 管理インターフェイス アドレスは以下のとおりです。

- 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 web URL から KVM を開始す

るときに、[KVM コンソール（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 準拠の 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 サーバ用のインバンド 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、それらを使用してサーバにアドレスを割り当てることができます。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 CIMC アドレスを Cisco UCS M3 および M4 サーバに割り当てるには、インバンド プロファイルでネットワークおよび IP プール名を設定します。

インバンド管理サポート

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

- KVM
- ISO 準拠の 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、それらを使用してサーバにアドレスを割り当てることができます。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。

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。

帯域幅の使用量

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、直接ピン グループを割り当てるか、ピン グループを vNIC ポリシーに含めてから、サーバに割り当てられているサービス 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

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。変更はできません。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。

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 フレームの扱い方を決定するフロー制御ポリシー

QoS システム クラスに加えられたグローバル QoS の変更によって、すべてのトラフィックにデータプレーンでの中断が短時間発生する可能性があります。このような変更の例を次に示します。

- 有効になっているクラスの MTU サイズの変更
- 有効になっているクラスの パケット ドロップの変更
- 有効になっているクラスの CoS 値の変更

Cisco UCS Mini の Quality of Service に関する注意事項と制限事項

- Cisco UCS Mini はすべてのシステム クラスに共有バッファを使用します。
- ブロンズ クラスは SPAN とバッファを共有します。SPAN またはブロンズ クラスを使用することを推奨します。
- マルチキャスト最適化はサポートされていません。
- いずれかのクラスの QoS パラメータを変更すると、すべてのクラスへのトラフィックが中断されます。
- イーサネットと FC または FCoE トラフィックが混在する場合、帯域幅が均等に分配されません。
- 同じクラスからの複数のトラフィック ストリームが均等に分配されないことがあります。
- FC または FCoE のパフォーマンス問題を回避するために、すべてのドロップなしポリシーに同じ CoS 値を使用します。
- プラチナおよびゴールド クラスのみがドロップなしポリシーをサポートしています。

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 *2*：システム クラス

システム クラス	説明
プラチナ（Platinum） ゴールド（Gold） シルバー（Silver） ブロンズ（Bronze）	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。 Cisco UCS Mini では、プラチナ クラスおよびゴールド クラスでのみパケット ドロップをディセーブルにできます。no drop クラスとして一度に 1 つのプラチナ クラスと 1 つのゴールド クラスだけを設定できます。
ベスト エフォート（Best Effort）	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。
ファイバチャネル（Fibre Channel）	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ライセンス済みです。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。

- ステートレス コンピューティング。この機能で利用されるモバイル サービス プロファイルには、各コンポーネント（サーバ、アダプタなど）がステートレスであるプールとポリシーが含まれています。
- 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の要素が含まれます。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。このサーバでビジネス サービスが不要になった場合は、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、別のサービスプロファイルを関連付け、同じ物理サーバ用に別の ID を作成します。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は、ただちにサービス プロファイルを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 アドレスなど、オリジナルのサーバと同じ ID を新しいサーバに与えるので、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、それらを使用してサーバの 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は、サービス プロファイルを新しいサーバに再割り当てす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 ドメインの大規模な物理インフラストラクチャを、組織と呼ばれる論理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場合、すべての組織は階層的になります。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次のうち 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 の仮想化

仮想化の概要

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（RAM、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や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。仮想化の利点は、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コンピュータ 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および管理されます。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から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 仮想インターフェイス カード（VIC）アダプタと連携して、Cisco Virtual Machine 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仮想化

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 アダプタでの仮想化

Cisco VIC アダプタは、ベア メタルの導入と 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 アダプタに使用される vNICs には、静的と動的の 2 つのタイプがあります。静的な vNIC は、OS またはハイパーバイザから認識されるデバイスです。動的な vNIC は、VM をファブリック インターコネクトの vEth ポートに接続するための VM-FEX に使用されます。

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。

第 3 章

Cisco UCS Manager の概要

この章の内容は、次のとおりです。

Cisco UCS Manager について

Cisco UCS Manager は Cisco UCS ドメイン内のすべてのコンポーネントの管理システムです。Cisco UCS Manager はファブリック インターコネクト内で動作します。この管理サービスで使用できるインターフェイスのいずれかを使用して、ファブリック インターコネクトに接続されたシャーシすべてのネットワークおよびサーバ リソースにアクセスしたり、これらを設定、管理、およびモニタしたりすることができます。

複数の管理インターフェイス

Cisco UCS Manager には、Cisco UCS ドメイン の管理に使用できる次のインターフェイスが含まれています。

- Cisco UCS Manager GUI
- Cisco UCS Manager CLI
- XML API
- KVM
- IPMI

ほとんどすべてのタスクは、これらのインターフェイスのいずれでも実行できます。また、あるインターフェイスで実行されたタスクの結果は、他のタスクにも自動的に表示されます。

ただし、次の操作はできません。

- Cisco UCS Manager GUI を使用して Cisco UCS Manager CLI を呼び出すこと。
- Cisco UCS Manager GUI で Cisco UCS Manager CLI を通じて呼び出されたコマンドの結果を表示すること。
- Cisco UCS Manager GUI から CLI 出力を生成すること。

中央集中型の管理

Cisco UCS Managerはリソースおよびデバイスの管理を一元化し、複数の管理ポイントを使用する必要性をなくします。この中央集中型管理には、Cisco UCS ドメイン における次のデバイスの管理が含まれます。

- ファブリック インターコネクト。
- 仮想サーバ用ソフトウェア スイッチ。
- シャーシおよびサーバにおける電源および環境管理。
- サーバ ネットワーク インターフェイスの設定とファームウェアの更新（イーサネット NIC および統合型ネットワーク アダプタ）。
- サーバに対するファームウェアおよび BIOS 設定。

仮想サーバおよび物理サーバのサポート

Cisco UCS Manager は、サーバの ID、I/O 設定、MAC アドレスおよび World Wide 名、ファームウェアのバージョン、ネットワーク プロファイルなどのサーバ状態情報をサービス プロファイルに要約します。サービス プロファイルをシステム内のサーバ リソースに適用して、VIC アダプタの提供する仮想デバイスに接続されている物理サーバ、仮想サーバ、および仮想マシンに同様の柔軟性とサポートを提供できます。

ロールベースの管理とマルチテナント機能のサポート

Cisco UCS Managerでは、柔軟に定義されたロールがサポートされるため、データセンターでは、個別のサーバ、ストレージ、およびネットワーク管理と同じベスト プラクティスを使用して、Cisco UCS ドメイン を操作できます。データセンターでのユーザの責任を反映した権限を持つユーザ ロールを作成できます。たとえば、次のロールを作成できます。

- サーバ関連設定を制御できるサーバ管理者ロール。
- SAN に関連するタスクを制御するストレージ管理者ロール。
- LAN に関連するタスクを制御するネットワーク管理者ロール。

Cisco UCS はマルチテナント対応で、システムの管理ソフトウェアが API を使用して Cisco UCS リソースへ制御されたアクセスを行えるようにするプリミティブを公開します。マルチテナント環境では、Cisco UCS Manager により、ユーザの範囲を特定の組織に制限できるユーザ ロールのロケールを作成することができます。

Cisco UCS Manager で実行可能なタスク

Cisco UCS Manager を使用して、Cisco UCS ドメイン 内のすべての物理的デバイスおよび仮想デバイスに対する管理タスクを実行できます。

Cisco UCS ハードウェア管理

Cisco UCS Manager を使用して、次を含む Cisco UCS ドメイン 内のすべてのハードウェアを管理できます。

- シャーシ
- サーバ
- ファブリック インターコネクト
- ファン
- ポート
- インターフェイス カード

Cisco UCS リソース管理

Cisco UCS Manager を使用して、次を含む Cisco UCS ドメイン 内のすべてのリソースを作成および管理できます。

- サーバ
- WWN アドレス
- MAC アドレス
- UUID
- 帯域幅

サーバ管理

サーバ管理者は Cisco UCS Manager を使用して、以下のような Cisco UCS ドメイン 内のサーバ管理タスクを実行できます。

- サーバ プール、および資格ポリシーなどこれらのプールに関係するポリシーの作成
- ディスカバリ ポリシー、スクラブ ポリシー、IPMI ポリシーなど、サーバで使用されるポリシーの作成
- サービス プロファイル、および必要に応じてサービス プロファイル テンプレートの作成
- サーバへのサービス プロファイルの適用
- 障害、アラーム、および機器のステータスのモニタ

ネットワーク管理

ネットワーク管理者は Cisco UCS Manager を使用して、以下のような Cisco UCS ドメイン の LAN 設定を作成するのに必要なタスクを実行できます。

- アップリンク ポート、ポート チャネル、および LAN PIN グループの設定
- VLAN の作成
- Quality Of Service クラスおよび定義の設定
- MAC アドレス プール、イーサネット アダプタ プロファイルなど、ネットワーク設定に関連したプールおよびポリシーの作成

ストレージ管理

ストレージ管理者は Cisco UCS Manager を使用して、以下のような Cisco UCS ドメイン の SAN 設定を作成するのに必要なタスクを実行できます。

- ポート、ポート チャネル、および SAN PIN グループの設定
- VSAN の作成
- Quality Of Service クラスおよび定義の設定
- WWN プール、ファイバ チャネル アダプタ プロファイルなど、ネットワーク設定に関連したプールおよびポリシーの作成

Cisco UCS Manager で実行できないタスク

Cisco UCS ドメイン 内のデバイス マネジメントに特に関連していないシステム管理タスクを実行するために Cisco UCS Manager を使用することはできません。

システムを超えた管理はできない

Cisco UCS Manager を使用して、Cisco UCS Manager がある Cisco UCS ドメイン 外部のシステムまたはデバイスを管理することはできません。たとえば、Cisco UCS 以外の x86 システム、SPARC システム、PowerPC システムなどの異機種環境は管理できません。

オペレーティング システムやアプリケーションのプロビジョニングや管理はできない

Cisco UCS Manager はサーバのプロビジョニングを行うため、サーバのオペレーティング システムの下に存在します。したがって、サーバでオペレーティング システムやアプリケーションのプロビジョニングや管理を行うためにこれを使用することはできません。たとえば、次の操作を実行することはできません。

- Windows や Linux などの OS の展開
- OS やアプリケーションなどのソフトウェアに対するパッチの展開

- アンチウイルス ソフトウェア、モニタリング エージェント、バックアップ クライアントなどのベース ソフトウェア コンポーネントのインストール
- データベース、アプリケーション サーバ ソフトウェア、Web サーバなどのソフトウェア アプリケーションのインストール
- Oracle データベースの再起動、プリンタ キューの再起動、または Cisco UCS 以外のユーザ アカウントの処理を含むオペレータ処理の実行
- SAN や NAS ストレージ上の外部ストレージの設定または管理

ハイ アベイラビリティ環境の Cisco UCS Manager

2 つのファブリック インターコネクトを持つハイ アベイラビリティ環境では、それぞれのファブリック インターコネクトで、別々の Cisco UCS Manager インスタンスを実行することができます。プライマリ ファブリック インターコネクトの Cisco UCS Manager はプライマリ管理インスタンスとして動作し、もう 1 つのファブリック インターコネクトの Cisco UCS Manager は従属管理インスタンスとなります。

Cisco UCS Manager の 2 つのインスタンスは、これらのファブリック インターコネクト上の L1 および L2 イーサネット ポートの間にあるプライベート ネットワーク上で通信します。設定およびステータスに関する情報は、このプライベート ネットワーク経由でやりとりされ、すべての管理情報が確実に複製されます。この継続的な通信により、プライマリ ファブリック インターコネクトに不具合が起きた場合でも、Cisco UCS に対する管理情報がそのまま持続されることが保証されます。さらに、プライマリ Cisco UCS Manager 上で実行される「浮動」管理 IP アドレスにより、フェールオーバーが発生したときに、従属ファブリック インターコネクトへのスムーズな移行が確実に行われるようになります。

第 4 章

Cisco UCS Manager CLI の概要

この章の内容は、次のとおりです。

管理対象オブジェクト

Cisco UCS は管理対象オブジェクト モデルを使用します。このモデルでは、管理対象オブジェクトは管理可能な物理エンティティまたは論理エンティティを抽象的に表現したものです。たとえば、サーバ、シャーシ、およびプロセッサは、管理対象オブジェクトとして表現される物理エンティティです。また、リソース プール、ユーザ ロール、サービス プロファイル、およびポリシーは、管理対象オブジェクトとして表現される論理エンティティです。

管理対象オブジェクトには関連付けられている設定可能なプロパティが複数存在する場合があります。

コマンド モード

CLI のコマンド モードは階層構造になっており、EXEC モードがこの階層の最高レベルとなります。上位のモードは下位のモードに分岐しています。上位のモードから 1 つ下位のモードに移動するには **create**、**enter**、**scope** コマンドを使用します。モード階層で 1 つ上位に移動するには **exit** コマンドを使用します。

（注） コマンド モードの大半は管理対象オブジェクトに関連付けられているため、あるオブジェクトと関連付けられているモードにアクセスできるようにするには、まず、そのオブジェクトを作成する必要があります。アクセスするモードに対する管理対象オブジェクトを作成するには、**create** および **enter** コマンドを使用します。**scope** コマンドは管理対象オブジェクトを作成するものではありません。すでに管理対象オブジェクトが存在するモードにアクセスするだけです。

各モードには、モード内で使用できる一連のコマンドがあります。各モードで使用できるコマンドの大部分は、関連する管理対象オブジェクトに関係しています。割り当てられたロールとロケールによっては、そのモードで使用できるコマンドのサブセットだけにしかアクセスできないことがありますが、アクセスできないコマンドは非表示にされます。

各モードの CLI プロンプトには、モード階層における現在のモードのフルパスが表示されます。これにより、コマンド モード階層内での現在位置を容易に判断できます。また、この機能は階層内を移動する際にも非常に役立ちます。

次の表は、主要なコマンド モード、各モードへのアクセスに使用するコマンド、および各モードに関連する CLI プロンプトを示しています。

表 *3*：主要なコマンド モードとプロンプト

モード名	アクセスに使用するコマンド	モード プロンプト
EXEC	任意のモードで **top** コマンド	#
アダプタ	EXEC モードから **scope adapter** コマンド	/adapter #
シャーシ	EXEC モードで **scope chassis** コマンド	/chassis #
イーサネット サーバ	EXEC モードから **scope eth-server** コマンド	/eth-server #
イーサネット アップリンク	EXEC モードで **scope eth-uplink** コマンド	/eth-uplink #

モード名	アクセスに使用するコマンド	モード プロンプト
ファブリック インターコネクト	EXEC モードで **scope fabric-interconnect** コマンド	/fabric-interconnect #
ファイバ チャネル アップリンク	EXEC モードで **scope fc-uplink** コマンド	/fc-uplink #
ファームウェア	EXEC モードで **scope firmware** コマンド	/firmware #
ホスト イーサネット インターフェイス	EXEC モードから **scope host-eth-if** コマンド	/host-eth-if #
ホスト ファイバ チャネル インターフェイス	EXEC モードで **scope host-fc-if** コマンド	/host-fc-if #
モニタリング	EXEC モードで **scope monitoring** コマンド	/monitoring #
組織	EXEC モードで **scope org** コマンド	/org #
セキュリティ	EXEC モードで **scope security** コマンド	/security #
サーバ	EXEC モードで **scope server** コマンド	/server #
サービス プロファイル	EXEC モードから **scope service-profile** コマンド	/service-profile #
システム	EXEC モードで **scope system** コマンド	/system #
仮想 HBA	EXEC モードから **scope vhba** コマンド	/vhba #
仮想 NIC	EXEC モードから **scope vnic** コマンド	/vnic #

オブジェクト コマンド

オブジェクト管理用に 4 つの一般的なコマンドがあります。

- **create** *object*
- **delete** *object*
- **enter** *object*
- **scope** *object*

scope コマンドは、永続的オブジェクトでもユーザ イスタンス化オブジェクトでも、すべての管理対象オブジェクトで使用できます。その他のコマンドを使用して、ユーザ インスタンス化オブジェクトを作成および管理できます。すべての **create** *object* コマンドで、対応する **delete** *object* および **enter** *object* コマンドが存在します。

ユーザ インスタンス化オブジェクトの管理では、次の表に説明するように、これらのコマンドの動作はオブジェクトが存在するかどうかによって異なります。

表 *4*：オブジェクトが存在しない場合のコマンドの動作

コマンド	動作
create *object*	オブジェクトが作成され、該当する場合、そのコンフィギュレーション モードが開始されます。
delete *object*	エラー メッセージが生成されます。
enter *object*	オブジェクトが作成され、該当する場合、そのコンフィギュレーション モードが開始されます。
scope *object*	エラー メッセージが生成されます。

表 *5*：オブジェクトが存在する場合のコマンドの動作

コマンド	動作
create *object*	エラー メッセージが生成されます。
delete *object*	オブジェクトが削除されます。
enter *object*	該当する場合、オブジェクトのコンフィギュレーション モードが開始されます。
scope *object*	オブジェクトのコンフィギュレーション モードが開始されます。

コマンドの実行

任意のモードで Tab キーを使用すると、コマンドを実行できます。コマンド名の一部を入力して Tab を押すと、コマンド全体が表示されるか、または別のキーワードを選択するか引数値を入力する必要があるところまで表示されます。

コマンド履歴

CLI では、現在のセッションで使用したすべてのコマンドが保存されます。上矢印キーまたは下矢印キーを使用すると、これまでに使用したコマンドを 1 つずつ表示できます。上矢印キーを押すと履歴内の直前のコマンドが、下矢印キーを押すと履歴内の次のコマンドが表示されます。履歴の最後に到達すると、下矢印キーを押しても次のコマンドが表示されなくなります。

履歴内のすべてのコマンドは、履歴を 1 つずつ表示し、目的のコマンドを再度呼び出し、Enter キーを押すだけでもう一度実行することができます。このコマンドは手動で入力したように表示されます。また、コマンドを再度呼び出した後、Enter キーを押す前にコマンドを変更することもできます。

保留コマンドのコミット、廃棄、および表示

CLI でコンフィギュレーション コマンドを入力する場合、**commit-buffer** コマンドを入力するまで、そのコマンドは適用されません。コミットされるまで、コンフィギュレーション コマンドは保留状態となり、**discard-buffer** コマンドを入力して廃棄できます。

複数のコマンド モードで保留中の変更を積み重ね、**commit-buffer** コマンド 1 つでまとめて適用できます。任意のコマンド モードで **show configuration pending** コマンドを入力して、保留中のコマンドを表示できます。

（注） 複数のコマンドをまとめてコミットするのは、アトミック操作ではありません。失敗したコマンドがあっても、成功したコマンドは適用されます。失敗したコマンドはエラー メッセージで報告されます。

コマンドが保留中の場合、コマンド プロンプトの前にアスタリスク（*）が表示されます。アスタリスクは、**commit-buffer** コマンドを入力すると消去されます。

次に、プロンプトがコマンド エントリのプロセス中に変わる例を示します。

```
switch-1# scope chassis 1
switch-1 /chassis # enable locator-led
switch-1 /chassis* # show configuration pending
 scope chassis 1
+    enable locator-led
 exit
switch-1 /chassis* # commit-buffer
switch-1 /chassis #
```

CLI に関するオンラインヘルプ

いつでも ? 文字を入力して、その時点のコマンド構文の状態に応じた使用可能なオプションを表示できます。

プロンプトに何も入力せずに ? を入力すると、現在のモードで使用できるコマンドがすべて表示されます。コマンドの一部を入力して ? を入力すると、その時点のコマンド構文内の位置で使用可能なキーワードと引数がすべて表示されます。

CLI セッション制限

Cisco UCS Manager は、同時にアクティブにできる CLI セッションの数を合計で 32 セッションに制限します。この値は設定可能です。

Web セッション制限

Web セッション制限は、ある時点における、システムにアクセス可能な Web セッション（GUI と XML の両方）の数を制限するために Cisco UCS Manager によって使用されます。

デフォルトでは、Cisco UCS Manager が許可する同時 Web セッション数は、最大値の 256 に設定されています。

CLI からの Cisco UCS Manager の Web セッション制限の設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope services**	システム サービス モードを開始します。
ステップ 3	UCS-A /system/services # **scope web-session-limits**	システム サービス Web セッション制限モードを開始します。
ステップ 4	UCS-A /system/services/web-session-limits # **set total** *num-of-logins-total*	システム内のすべてのユーザに許可される HTTP および HTTPS の同時セッションの最大数。 1 ～ 256 の整数を入力します。
ステップ 5	UCS-A /system/services/web-session-limits # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、システムで許可される HTTP および HTTPS セッションの最大数を 200 に設定し、トランザクションをコミットする例を示します。

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # scope web-session-limits
UCS-A /system/services/web-session-limits* # set total 200
UCS-A /system/services/web-session-limits* # commit-buffer
UCS-A /system/services/web-session-limits #
```

ログイン前バナー

ログイン前バナーを使用すると、ユーザが Cisco UCS Manager GUI にログインする場合、Cisco UCS Manager は [ログイン前バナーの作成（Create Pre-Login Banner）] ダイアログボックスにバナー テキストを表示し、ユーザがダイアログボックスを閉じてからユーザ名とパスワードの入力を求めます。ユーザが Cisco UCS Manager CLI にログインする場合、Cisco UCS Manager はダイアログボックスにバナー テキストを表示し、ユーザがダイアログボックスを閉じてからユーザ名とパスワードの入力を求めます。その後は、ユーザに表示するコピーライト ブロックの上にバナー テキストを繰り返します。

ログイン前バナーの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope banner**	バナー セキュリティ モードを開始します。
ステップ 3	UCS-A /security/banner # **create pre-login-banner**	ログイン前バナーを作成します。
ステップ 4	UCS-A /security/banner/pre-login-banner # **set message**	Cisco UCS Manager は、Cisco UCS Manager GUI または CLI 用のログイン プロンプトを表示する前に、ユーザに対してこのメッセージを表示を指定します。 このフィールドには、標準の ASCII 文字を入力できます。 ログイン前バナー メッセージのテキストを入力するためのダイアログを開始します。
ステップ 5	プロンプトで、ログイン前バナー メッセージを入力し、Enter キーを押します。	入力内容の次の行に、「ENDOFBUF」と入力して終了します。

	コマンドまたはアクション	目的
		[set message] ダイアログをキャンセルするには、Ctrl+C キーを押します。
ステップ 6	UCS-A /security/banner/pre-login-banner # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、ログイン前バナーを作成します。

```
UCS-A# scope security
UCS-A /security # scope banner
UCS-A /security/banner # create pre-login-banner
UCS-A /security/banner/pre-login-banner* # set message
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Enter prelogin banner:
>Welcome to UCS System 1
>ENDOFBUF
UCS-A /security/banner/pre-login-banner* # commit-buffer
UCS-A /security/banner/pre-login-banner #
```

ログイン前バナーの変更

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope banner**	バナー セキュリティ モードを開始します。
ステップ 3	UCS-A /security/banner # **scope pre-login-banner**	ログイン前バナーのバナー セキュリティ モードを開始します。
ステップ 4	UCS-A /security/banner/pre-login-banner # **set message**	Cisco UCS Manager は、Cisco UCS Manager GUI または CLI 用のログイン プロンプトを表示する前に、ユーザに対してこのメッセージを表示を指定します。 このフィールドには、標準の ASCII 文字を入力できます。 ログイン前バナー メッセージのテキストを入力するためのダイアログを開始します。
ステップ 5	プロンプトで、ログイン前バナー メッセージを変更し、Enter キーを押します。	入力内容の次の行に、「ENDOFBUF」と入力して終了します。 [set message] ダイアログをキャンセルするには、Ctrl+C キーを押します。

	コマンドまたはアクション	目的
ステップ 6	UCS-A /security/banner/pre-login-banner # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、ログイン前バナーを変更する例を示します。

```
UCS-A# scope security
UCS-A /security # scope banner
UCS-A /security/banner # create pre-login-banner
UCS-A /security/banner/pre-login-banner* # set message
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Enter prelogin banner:
Welcome to UCS System 1
ENDOFBUF
UCS-A /security/banner/pre-login-banner* # commit-buffer
UCS-A /security/banner/pre-login-banner #
```

ログイン前バナーの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope banner**	バナー セキュリティ モードを開始します。
ステップ 3	UCS-A /security/banner # **delete pre-login-banner**	システムからログイン前バナーを削除します。
ステップ 4	UCS-A /security/banner # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、ログイン前バナーを削除する例を示します。

```
UCS-A# scope security
UCS-A /security # scope banner
UCS-A /security/banner # delete pre-login-banner
UCS-A /security/banner* # commit-buffer
UCS-A /security/banner #
```

第 5 章

ファブリック インターコネクトの設定

この章の内容は、次のとおりです。

システムの初期セットアップ

Cisco UCS ドメイン 内のファブリック インターコネクトへの初回アクセス時には、セットアップ ウィザードでシステム設定に必要な次の情報の入力を求められます。

- インストール方法（GUI または CLI）
- セットアップ モード（フル システム バックアップからの復元または初期セットアップ）
- システム設定タイプ（スタンドアロンまたはクラスタ設定）
- システム名

- admin パスワード
- 管理ポートの IPv4 アドレスとサブネット マスク、または IPv6 アドレスとプレフィックス
- デフォルトのゲートウェイの IPv4 アドレスまたは IPv6 アドレス
- DNS サーバの IPv4 アドレスまたは IPv6 アドレス
- デフォルトのドメイン名

セットアップ モード

システム設定を既存のバックアップファイルから復元するか、セットアップ ウィザードを実行してシステムを手動でセットアップするか、選択できます。システムを復元する場合は、バックアップ ファイルが、管理ネットワークから到達可能な場所に存在する必要があります。

システム設定タイプ

スタンドアロン設定で単一のファブリック インターコネクトを使用するように、またはクラスタ設定でファブリック インターコネクトの冗長ペアを使用するように、Cisco UCS ドメイン を設定できます。

クラスタ設定では、ハイアベイラビリティが提供されます。一方のファブリック インターコネクトが使用不可能になっても、もう一方が代わりを務めます。クラスタ設定をサポートするには、管理ポート（Mgmt0）接続が 1 つだけあれば十分です。しかし、リンクレベルの冗長性を実現するには、両方の Mgmt0 ポートを接続する必要があります。

さらに、クラスタ構成では、冗長仮想インターフェイス（VIF）接続のフェールオーバー リカバリ時間が大幅に向上します。アダプタに、あるファブリック インターコネクトへのアクティブな VIF 接続と別の（第 2 の）ファブリック インターコネクトへのスタンバイ VIF 接続が存在する場合、アクティブな VIF の学習済み MAC アドレスは複製されますが、第 2 のファブリック インターコネクトにはインストールされません。アクティブな VIF に障害が発生した場合、第 2 のファブリック インターコネクトは複製された MAC アドレスをインストールし、それを Gratuitous ARP メッセージを介してネットワークにブロードキャストして、切り替え時間を短縮します。

（注） クラスタ構成では、管理プレーンに対してのみ冗長性が提供されます。データの冗長性はユーザの設定に依存するので、データの冗長性をサポートするにはサードパーティ製のツールが必要なこともあります。

クラスタ設定内の両方のファブリック インターコネクトに対して初期セットアップ プロセスを実行する必要があります。クラスタ構成用に設定した 1 番目のファブリック インターコネクトをイネーブルにする必要があります。2 番目のファブリック インターコネクトを設定すると、そのファブリック インターコネクトはクラスタ内のピア ファブリック インターコネクトとして 1 番目のファブリック インターコネクトを検出します。

管理ポートの IP アドレス

スタンドアロン設定では、ファブリック インターコネクトの単一の管理ポートに対して IPv4 アドレス、ゲートウェイ、サブネット マスクを 1 つだけ、または IPv6 アドレス、ゲートウェイ、ネットワーク プレフィックスを 1 つだけ指定する必要があります。管理ポートの IP アドレスには、IPv4 アドレスまたは IPv6 アドレスのいずれかを設定できます。

クラスタ構成では、同一のサブネットに以下の 3 つの IPv4 アドレスを指定するか、プレフィックスが同じ 3 つの IPv6 アドレスを指定する必要があります。

- ファブリック インターコネクト A の管理ポートの IP アドレス
- ファブリック インターコネクト B の管理ポートの IP アドレス
- クラスタの IP アドレス

（注） クラスタ構成では、両方のファブリック インターコネクトの管理ポートに同じアドレス タイプ（IPv4 または IPv6）を設定する必要があります。最初の FI に IPv4 アドレスを設定し、2 番目の FI に IPv6 アドレスを設定すると、その構成は機能しません。

スタンドアロン設定用の初期システムセットアップの実行

はじめる前に

1 ファブリック インターコネクトにおける次の物理接続を確認します。

- コンソール ポートがコンピュータ端末またはコンソール サーバに物理的に接続されている。
- 管理イーサネット ポート（mgmt0）が外部のハブ、スイッチ、またはルータに接続されている。

詳細については、お使いのファブリック インターコネクトに関する『*Cisco UCS Hardware Installation Guide*』を参照してください。

2 コンソール ポートに接続しているコンピュータ端末（またはコンソール サーバ）でコンソール ポート パラメータが次のとおりであることを確認します。

- 9600 ボー
- 8 データ ビット
- パリティなし
- 1 ストップ ビット

3 初期設定で入力する必要がある次の情報を収集します。

- システム名
- admin アカウントのパスワード。Cisco UCS Manager のパスワード ガイドラインに適合する強力なパスワードを選択します。このパスワードは空にできません。
- 管理ポート IPv4 およびサブネット マスク、または IPv6 アドレスとプレフィックス。
- デフォルト ゲートウェイの IPv4 アドレスまたは IPv6 アドレス。
- DNS サーバの IPv4 または IPv6 アドレス（任意）。
- システムのドメイン名（任意）。

手順

ステップ 1 コンソール ポートに接続します。

ステップ 2 ファブリック インターコネクトの電源を入れます。
ファブリック インターコネクトがブートする際、Power On Self-Test のメッセージが表示されます。

ステップ 3 設定されていないシステムがブートすると、使用する設定方法の入力を要求するプロンプトが表示されます。**console** と入力して、コンソール CLI を使用した初期設定を続行します。

ステップ 4 初期システム設定として続行するために、**setup** と入力します。

ステップ 5 初期設定の続行を確定するために、**y** を入力します。

ステップ 6 admin アカウントのパスワードを入力します。

ステップ 7 確認のために、admin アカウントのパスワードを再入力します。

ステップ 8 スタンドアロン設定用の初期設定を続行するために、**no** を入力します。

ステップ 9 システム名を入力します。

ステップ 10 ファブリック インターコネクトの管理ポートの IPv4 または IPv6 アドレスを入力します。
IPv4 アドレスを入力する場合は、IPv4 サブネット マスクを入力するように求められます。IPv6 アドレスを入力する場合は、IPv6 ネットワーク プレフィックスを入力するように求められます。

ステップ 11 各 IPv4 サブネット マスク、または IPv6 ネットワーク プレフィックスを入力し、Enter キーを押します。
ファブリックインターコネクトの管理ポート用に入力したアドレスタイプによって、デフォルト ゲートウェイの IPv4 または IPv6 アドレスを求められます。

ステップ 12 次のいずれかを入力します。

- デフォルト ゲートウェイの IPv4 アドレス
- デフォルト ゲートウェイの IPv6 アドレス

ステップ 13 DNS サーバの IP アドレスを指定する場合は **yes** を入力し、指定しない場合は **no** を入力します。

ステップ 14 （任意） DNS サーバの IPv4 または IPv6 アドレスを入力します。

アドレス タイプはファブリック インターコネクトの管理ポートのアドレス タイプと同じである必要があります。

ステップ 15 デフォルトのドメイン名を指定する場合は **yes** を入力し、指定しない場合は **no** を入力します。

ステップ 16 （任意） デフォルト ドメイン名を入力します。

ステップ 17 集中管理環境（Cisco UCS Central）に加わる場合は **yes** を入力し、加わらない場合は **no** を入力します。

ステップ 18 設定の要約を確認し、**yes** と入力して設定を保存および適用するか、**no** と入力して設定ウィザードを再びやり直し、設定を一部変更します。
設定ウィザードのやり直しを選択した場合は、以前に入力した値が角カッコで囲まれて表示されます。以前に入力した値をそのまま使用する場合は、Enter を押します。

次に、コンソールセットアップ方式とIPv4管理アドレスを使用してスタンドアロン設定をセットアップする例を示します。

```
Enter the installation method (console/gui)?  console
Enter the setup mode (restore from backup or initial setup) [restore/setup]? setup
You have chosen to setup a new switch.  Continue? (y/n): y
Enter the password for "admin": adminpassword%958
Confirm the password for "admin": adminpassword%958
Do you want to create a new cluster on this switch (select 'no' for standalone setup or if
 you want this switch to be added to an existing cluster)? (yes/no) [n]: no
Enter the system name: foo
Mgmt0 address: 192.168.10.10
Mgmt0 IPv4 netmask: 255.255.255.0
IPv4 address of the default gateway: 192.168.10.1
Configure the DNS Server IPv4 address? (yes/no) [n]: yes
  DNS IP address: 20.10.20.10
Configure the default domain name? (yes/no) [n]: yes
  Default domain name: domainname.com
Join centralized management environment (UCS Central)? (yes/no) [n]: no
Following configurations will be applied:
  Switch Fabric=A
  System Name=foo
  Physical Switch Mgmt0 IP Address=192.168.10.10
  Physical Switch Mgmt0 IP Netmask=255.255.255.0
  Default Gateway=192.168.10.1
  DNS Server=20.10.20.10
  Domain Name=domainname.com
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
```

次に、コンソールセットアップ方式とIPv6管理アドレスを使用してスタンドアロン設定をセットアップする例を示します。

```
Enter the installation method (console/gui)?  console
Enter the setup mode (restore from backup or initial setup) [restore/setup]? setup
You have chosen to setup a new switch.  Continue? (y/n): y
Enter the password for "admin": adminpassword%652
Confirm the password for "admin": adminpassword%652
Do you want to create a new cluster on this switch (select 'no' for standalone setup or if
 you want this switch to be added to an existing cluster)? (yes/no) [n]: no
Enter the system name: foo
Mgmt0 address:  2001::107
Mgmt0 IPv6 prefix: 64
IPv6 address of the default gateway: 2001::1
Configure the DNS Server IPv6 address? (yes/no) [n]: yes
  DNS IP address: 2001::101
Configure the default domain name? (yes/no) [n]: yes
  Default domain name: domainname.com
Join centralized management environment (UCS Central)? (yes/no) [n]: no
Following configurations will be applied:
  Switch Fabric=A
```

```
  System Name=foo
  Enforced Strong Password=no
  Physical Switch Mgmt0 IPv6 Address=2001::107
  Physical Switch Mgmt0 IPv6 Prefix=64
  Default Gateway=2001::1
  Ipv6 value=1
  DNS Server=2001::101
  Domain Name=domainname.com
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
```

クラスタ設定の初期システム セットアップ

第 1 ファブリック インターコネクトでの初期システム設定の実行

この手順は、管理ポート、デフォルト ゲートウェイ、および DNS サーバに対し IPv4 または IPv6 アドレスを使用して最初のファブリック インターコネクトをセットアップする方法について説明します。

はじめる前に

1 ファブリック インターコネクトにおける次の物理接続を確認します。

- 第 1 のファブリック インターコネクトのコンソール ポートが、コンピュータ端末またはコンソール サーバに物理的に接続されている。
- 管理イーサネット ポート（mgmt0）が外部のハブ、スイッチ、またはルータに接続されている。

詳細については、お使いのファブリック インターコネクトに関する『*Cisco UCS Hardware Installation Guide*』を参照してください。

2 コンソール ポートに接続しているコンピュータ端末（またはコンソール サーバ）でコンソール ポート パラメータが次のとおりであることを確認します。

- 9600 ボー
- 8 データ ビット
- パリティなし
- 1 ストップ ビット

3 初期設定で入力する必要がある次の情報を収集します。

- システム名。
- admin アカウントのパスワード。Cisco UCS Manager のパスワード ガイドラインに適合する強力なパスワードを選択します。このパスワードは空にできません。
- 3 つのスタティック IPv4 または IPv6 アドレス：両方のファブリック インターコネクトの管理ポートに 2 つ（各ファブリック インターコネクトに 1 つずつ）、および Cisco UCS Manager によって使用されるクラスタ IP アドレスに 1 つ。

- 3 つのスタティック IPv4 アドレスのサブネット マスク、または 3 つのスタティック IPv6 アドレスのネットワーク プレフィックス。
- デフォルト ゲートウェイの IPv4 アドレスまたは IPv6 アドレス。
- DNS サーバの IPv4 または IPv6 アドレス（任意）。
- システムのドメイン名（任意）。

手順

ステップ 1 コンソール ポートに接続します。

ステップ 2 ファブリック インターコネクトの電源を入れます。
ファブリック インターコネクトがブートする際、Power On Self-Test のメッセージが表示されます。

ステップ 3 設定されていないシステムがブートすると、使用する設定方法の入力を要求するプロンプトが表示されます。**console** と入力して、コンソール CLI を使用した初期設定を続行します。

ステップ 4 初期システム設定として続行するために、**setup** と入力します。

ステップ 5 初期設定の続行を確定するために、**y** を入力します。

ステップ 6 admin アカウントのパスワードを入力します。

ステップ 7 確認のために、admin アカウントのパスワードを再入力します。

ステップ 8 クラスタ設定用の初期設定を続行するために、**yes** を入力します。

ステップ 9 ファブリック インターコネクトのファブリックを入力します（**A** または **B**）。

ステップ 10 システム名を入力します。

ステップ 11 ファブリック インターコネクトの管理ポートの IPv4 または IPv6 アドレスを入力します。
IPv4 アドレスを入力する場合は、IPv4 サブネット マスクを入力するように求められます。IPv6 アドレスを入力する場合は、IPv6 ネットワーク プレフィックスを入力するように求められます。

ステップ 12 各 IPv4 サブネット マスク、または IPv6 ネットワーク プレフィックスを入力し、Enter キーを押します。
ファブリック インターコネクトの管理ポート用に入力したアドレス タイプによって、デフォルト ゲートウェイの IPv4 または IPv6 アドレスを求められます。

ステップ 13 次のいずれかを入力します。

- デフォルト ゲートウェイの IPv4 アドレス
- デフォルト ゲートウェイの IPv6 アドレス

ステップ 14 DNS サーバの IP アドレスを指定する場合は **yes** を入力し、指定しない場合は **no** を入力します。

ステップ 15 （任意） DNS サーバの IPv4 または IPv6 アドレスを入力します。

アドレス タイプはファブリック インターコネクトの管理ポートのアドレス タイプと同じである必要があります。

ステップ 16 デフォルトのドメイン名を指定する場合は **yes** を入力し、指定しない場合は **no** を入力します。

ステップ 17 （任意） デフォルト ドメイン名を入力します。

ステップ 18 設定の要約を確認し、**yes** と入力して設定を保存および適用するか、**no** と入力して設定ウィザードを再びやり直し、設定を一部変更します。
設定ウィザードのやり直しを選択した場合は、以前に入力した値が角カッコで囲まれて表示されます。以前に入力した値をそのまま使用する場合は、Enter を押します。

次に、コンソールおよび IPv4 管理アドレスを使用してクラスタ設定の最初のファブリック インターコネクトをセットアップする例を示します。

```
Enter the installation method (console/gui)?  console
Enter the setup mode (restore from backup or initial setup) [restore/setup]? setup
You have chosen to setup a new switch.  Continue? (y/n): y
Enter the password for "admin": adminpassword%958
Confirm the password for "admin": adminpassword%958
Do you want to create a new cluster on this switch (select 'no' for standalone setup or if
 you want this switch to be added to an existing cluster)? (yes/no) [n]: yes
Enter the switch fabric (A/B): A
Enter the system name: foo
Mgmt0 IPv4 address: 192.168.10.10
Mgmt0 IPv4 netmask: 255.255.255.0
IPv4 address of the default gateway: 192.168.10.1
Virtual IPv4 address: 192.168.10.12
Configure the DNS Server IPv4 address? (yes/no) [n]: yes
  DNS IPv4 address: 20.10.20.10
Configure the default domain name? (yes/no) [n]: yes
  Default domain name: domainname.com
Join centralized management environment (UCS Central)? (yes/no) [n]: no
Following configurations will be applied:
  Switch Fabric=A
  System Name=foo
  Management IP Address=192.168.10.10
  Management IP Netmask=255.255.255.0
  Default Gateway=192.168.10.1
  Cluster Enabled=yes
  Virtual Ip Address=192.168.10.12
  DNS Server=20.10.20.10
  Domain Name=domainname.com
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
```

次に、コンソールおよび IPv6 管理アドレスを使用してクラスタ設定の最初のファブリック インターコネクトをセットアップする例を示します。

```
Enter the installation method (console/gui)?  console
Enter the setup mode (restore from backup or initial setup) [restore/setup]? setup
You have chosen to setup a new switch.  Continue? (y/n): y
Enter the password for "admin": adminpassword%652
Confirm the password for "admin": adminpassword%652
Do you want to create a new cluster on this switch (select 'no' for standalone setup or if
 you want this switch to be added to an existing cluster)? (yes/no) [n]: yes
Enter the switch fabric (A/B): A
Enter the system name: foo
Mgmt0 address:  2001::107
Mgmt0 IPv6 prefix: 64
IPv6 address of the default gateway: 2001::1
Configure the DNS Server IPv6 address? (yes/no) [n]: yes
  DNS IP address: 2001::101
Configure the default domain name? (yes/no) [n]: yes
  Default domain name: domainname.com
```

```
Join centralized management environment (UCS Central)? (yes/no) [n]: no
Following configurations will be applied:
  Switch Fabric=A
  System Name=foo
  Enforced Strong Password=no
  Physical Switch Mgmt0 IPv6 Address=2001::107
  Physical Switch Mgmt0 IPv6 Prefix=64
  Default Gateway=2001::1
  Ipv6 value=1
  DNS Server=2001::101
  Domain Name=domainname.com
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
```

第 2 ファブリック インターコネクトでの初期システム設定の実行

この手順は、管理ポートに対しIPv4またはIPv6アドレスを使用して第2のファブリック インターコネクトをセットアップする方法について説明します。

はじめる前に

1 ファブリック インターコネクトにおける次の物理接続を確認します。

- 第 2 のファブリック インターコネクトのコンソール ポートが、コンピュータ端末またはコンソール サーバに物理的に接続されている。
- 管理イーサネット ポート（mgmt0）が外部のハブ、スイッチ、またはルータに接続されている。

詳細については、お使いのファブリック インターコネクトに関する『*Cisco UCS Hardware Installation Guide*』を参照してください。

2 コンソール ポートに接続しているコンピュータ端末（またはコンソール サーバ）でコンソール ポート パラメータが次のとおりであることを確認します。

- 9600 ボー
- 8 データ ビット
- パリティなし
- 1 ストップ ビット

3 初期設定で入力する必要がある次の情報を収集します。

- ピア ファブリック インターコネクトの admin アカウントのパスワード。Cisco UCS Manager のパスワード ガイドラインに適合する強力なパスワードを選択します。このパスワードは空にできません。
- 同じサブネットにある管理ポートの IPv4 アドレス、またはピア ファブリック インターコネクトと同じネットワーク プレフィックスの管理ポート IPv6。

4

手順

ステップ 1 コンソール ポートに接続します。

ステップ 2 ファブリック インターコネクトの電源を入れます。
ファブリック インターコネクトがブートする際、Power On Self-Test のメッセージが表示されます。

ステップ 3 設定されていないシステムがブートすると、使用する設定方法の入力を要求するプロンプトが表示されます。**console** と入力して、コンソール CLI を使用した初期設定を続行します。

（注） ファブリック インターコネクトによって、クラスタ内のピア ファブリック インターコネクトが検出されます。検出されなかった場合は、L1 ポートと L2 ポート間の物理接続を調べ、ピア ファブリック インターコネクトがクラスタ設定でイネーブルになっていることを確認します。

ステップ 4 **y** と入力して、従属ファブリック インターコネクトをクラスタに追加します。

ステップ 5 ピア ファブリック インターコネクトの管理パスワードを入力します。

ステップ 6 従属ファブリック インターコネクト上の管理ポートの IP アドレスを入力します。

ステップ 7 設定の要約を確認し、**yes** と入力して設定を保存および適用するか、**no** と入力して設定ウィザードを再びやり直し、設定を一部変更します。
設定ウィザードのやり直しを選択した場合は、以前に入力した値が角カッコで囲まれて表示されます。以前に入力した値をそのまま使用する場合は、Enter を押します。

次に、ピアのコンソールおよびIPv4アドレスを使用してクラスタ設定の第2のファブリック インターコネクトをセットアップする例を示します。

```
Enter the installation method (console/gui)? console
Installer has detected the presence of a peer Fabric interconnect. This Fabric interconnect
 will be added to the cluster. Continue (y/n) ? y
Enter the admin password of the peer Fabric Interconnect: adminpassword%958
Peer Fabric interconnect Mgmt0 IPv4 Address: 192.168.10.11
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
```

次に、ピアのコンソールおよびIPv6アドレスを使用してクラスタ設定の第2のファブリック インターコネクトをセットアップする例を示します。

```
Enter the installation method (console/gui)? console
Installer has detected the presence of a peer Fabric interconnect. This Fabric interconnect
 will be added to the cluster. Continue (y/n) ? y
Enter the admin password of the peer Fabric Interconnect: adminpassword%958
Peer Fabric interconnect Mgmt0 IPv6 Address: 2001::107
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
```

ファブリックインターコネクトへのアウトオブバンドIPv4アドレスの追加

すべてのファブリック インターコネクトでは、OOB IPv4 アドレス、ネットワーク マスク、およびゲートウェイが必要です。この手順では、スタティック IPv6 アドレスで設定されたファブリック インターコネクトに OOB IPv4 アドレスを設定する方法について説明します。

はじめる前に

ファブリックインターコネクトに割り当てるアウトオブバンド（OOB）IPv4アドレスを収集します。

手順

	コマンドまたはアクション	目的
ステップ1	UCS-A # **scope fabric interconnect a**	ファブリック A のファブリック コンフィギュレーション モードを開始します。
ステップ2	UCS-A/fabric-interconnect # **set out-of-band ip** *ip-addr* **netmask** *ip-addr***gw** *ip-addr*	OOB IPv4 アドレス、ネットワーク マスク、およびゲートウェイ アドレスを設定します。 システムは変更がコミットされると、コンソールセッションの変更が切断される可能性を警告します。
ステップ3	UCS-A/fabric-interconnect # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、ファブリック インターコネクト A の OOB IPv4 アドレスを設定する例を示します。

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect # set out-of-band ip 10.105.214.107 netmask 255.255.255.0 gw
10.105.214.1
Warning: When committed, this change may disconnect the current CLI session
UCS-A /fabric-interconnect* # commit-buffer
```

スタンドアロンファブリックインターコネクトに対するクラスタ設定のイネーブル化

1 つのスタンドアロン ファブリック インターコネクトを使用する既存の Cisco UCS ドメインに、別のファブリックインターコネクトを追加できます。これを行うには、クラスタの仮想IPまたはIPv6アドレスを使用して設定することでスタンドアロンファブリックインターコネクトのクラスタ動作をイネーブルにし、その後、クラスタに 2 番目のファブリック インターコネクトを追加します。

手順

	コマンドまたはアクション	目的
ステップ1	UCS-A# **connect local-mgmt**	ローカル管理モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A(local-mgmt) # **enable cluster** {*virtual-ip-addr*|*virtual-ip6-addr*}	指定の IPv4 または IPv6 アドレスを持つスタンドアロン ファブリック インターコネクトでクラスタ動作をイネーブルにします。このコマンドを入力すると、クラスタ動作をイネーブルにすることを確認するプロンプトが表示されます。確認のために **yes** と入力します。 IP アドレスは、クラスタに追加するファブリック インターコネクトに割り当てられた IP アドレスではなく、クラスタ設定用の仮想 IPv4 または IPv6 アドレスである必要があります。

次に、仮想 IPv4 アドレス 192.168.1.101 を使用して、スタンドアロン ファブリック インターコネクトのクラスタ動作をイネーブルにする例を示します。

```
UCS-A# connect local-mgmt
UCS-A(local-mgmt)# enable cluster 192.168.1.101
This command will enable cluster mode on this setup. You cannot change it
back to stand-alone. Also, any GUI or KVM sessions may be terminated. Are you sure you want
 to continue? (yes/no): yes
UCS-A(local-mgmt)#
```

次に、仮想 IPv6 アドレス 192.168.1.101 を使用して、スタンドアロン ファブリック インターコネクトのクラスタ動作をイネーブルにする例を示します。

```
UCS-A# connect local-mgmt
UCS-A(local-mgmt)# enable cluster ipv6 2001::109
This command will enable IPv6 cluster mode on this setup. You cannot change it
back to stand-alone. Also, any GUI or KVM sessions may be terminated. Are you sure you want
 to continue? (yes/no): yes
UCS-A(local-mgmt)#
```

次の作業

クラスタに第 2 のファブリック インターコネクトを追加します。

システム名の変更

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **set name** *name*	システム名を設定します。
ステップ 3	UCS-A /system # **commit-buffer**	トランザクションをシステム設定にコミットします。

名前は、トランザクションがコミットされた後、30秒ほどの間に両方のファブリック インターコネクトで更新されます。

次の例は、システム名を変更し、トランザクションをコミットします。

```
UCS-A# scope system
UCS-A /system* # set name SanJose5
UCS-A /system* # commit-buffer
UCS-A /system #
```

クラスタの管理サブネットの変更

クラスタ設定の IPv4 管理サブネットを変更する場合は、次の 3 つの IPv4 アドレスを同時に変更する必要があり、3 つのアドレスは同じサブネットに設定する必要があります。

- ファブリック インターコネクト A の管理ポートの IP アドレス
- ファブリック インターコネクト B の管理ポートの IP アドレス
- クラスタ IP（仮想 IP）アドレス

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fabric-interconnect a**	ファブリック A のファブリック インターコネクト モードを開始します。
ステップ 2	UCS-A /fabric-interconnect # **set out-of-band ip** *ip-address* **netmask** *netmask* **gw** *gateway-ip-address*	ファブリック インターコネクトの IP アドレス、ネットワーク マスク、およびゲートウェイ IP アドレスを設定します。
ステップ 3	UCS-A /fabric-interconnect # **scope fabric-interconnect b**	ファブリック B のファブリック インターコネクト モードを開始します。
ステップ 4	UCS-A /fabric-interconnect # **set out-of-band ip** *ip-address* **netmask** *netmask* **gw** *gateway-ip-address*	ファブリック インターコネクトの IP アドレス、ネットマスク、およびゲートウェイ IP アドレスを設定します。
ステップ 5	UCS-A /fabric-interconnect # **scope system**	システム モードを開始します。
ステップ 6	UCS-A /system # **set virtual-ip** *vip-address*	クラスタの仮想IPアドレスを設定します。
ステップ 7	UCS-A /system # **commit-buffer**	トランザクションをシステム設定にコミットします。

トランザクションをコミットすると、管理セッションから切断されます。新しい管理IPアドレスに再接続します。

この例は、両方のファブリック インターコネクトのIPアドレスを変更し、仮想IPアドレスを変更し、トランザクションをコミットして、セッションを切断します。

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect # set out-of-band ip 192.0.2.111 netmask 255.255.255.0 gw 192.0.2.1
UCS-A /fabric-interconnect* # scope fabric-interconnect b
UCS-A /fabric-interconnect* # set out-of-band ip 192.0.2.112 netmask 255.255.255.0 gw
192.0.2.1
UCS-A /fabric-interconnect* # scope system
UCS-A /system* # set virtual-ip 192.0.2.113
UCS-A /system* # commit-buffer
```

クラスタの管理プレフィックスの変更

クラスタ設定のIPv6管理プレフィックスを変更する場合は、次の3つのIPv6アドレスを同時に変更する必要があります。3つのアドレスは同一ネットワーク プレフィックス内に設定する必要があります。

- ファブリック インターコネクトAの管理ポートのIPv6アドレス
- ファブリック インターコネクトBの管理ポートのIPv6アドレス
- クラスタIPv6（仮想IPv6）アドレス

手順

	コマンドまたはアクション	目的
ステップ1	UCS-A# **scope fabric-interconnect a**	ファブリックAのファブリック インターコネクト モードを開始します。
ステップ2	UCS-A fabric-interconnect # **scope ipv6-config**	ファブリックAのIPv6コンフィギュレーション モードを開始します。
ステップ3	UCS-A fabric-interconnect/ ipv6-config # **set out-of-band ipv6** *ipv6-addr* **ipv6-gw** *ipv6-gw-addr* **ipv6-prefix** *prefix*	ファブリックAの管理IPv6アドレス、ゲートウェイIPv6アドレスおよびネットワーク プレフィックスを設定します。
ステップ4	UCS-A fabric-interconnect/ipv6-config # **scope fabric-interconnect b**	ファブリックBのファブリック インターコネクト モードを開始します。
ステップ5	UCS-A fabric-interconnect/ # **scope ipv6-config**	ファブリックBのIPv6コンフィギュレーション モードを開始します。
ステップ6	UCS-A/fabric-interconnect/ipv6-config # **set out-of-band ipv6** *ipv6-addr* **ipv6-gw** *ipv6-gw-addr* **ipv6-prefix** *prefix*	ファブリックBの管理IPv6アドレス、ゲートウェイIPv6アドレスおよびネットワーク プレフィックスを設定します。

	コマンドまたはアクション	目的
ステップ 7	UCS-A/fabric-interconnect/ipv6-config # **scope system**	システム モードを開始します。
ステップ 8	UCS-A/system # **set virtual-ip ipv6** *virtual-ip6-addr*	クラスタの仮想 IPv6 アドレスを設定します。
ステップ 9	UCS-A/system # **commit-buffer**	トランザクションをシステム設定にコミットします。

トランザクションをコミットすると、管理セッションから切断されます。新しい管理IPv6アドレスに再接続します。

次の例では、両方の管理 IPv6 アドレスを変更し、仮想 IPv6 アドレスを変更し、トランザクションをコミットします。

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect # scope ipv6-config
UCS-A /fabric-interconnect/ipv6-config # set out-of-band ipv6 2001:10::157
UCS-A /fabric-interconnect/ipv6-config* # set out-of-band ipv6-gw 2001:10::1
UCS-A /fabric-interconnect/ipv6-config* # set out-of-band ipv6-prefix 64
UCS-A /fabric-interconnect/ipv6-config* # scope fabric-interconnect b
UCS-A /fabric-interconnect* # scope ipv6-config
UCS-A /fabric-interconnect/ipv6-config* # set out-of-band ipv6 2001:10::158
UCS-A /fabric-interconnect/ipv6-config* # set out-of-band ipv6-gw 2001:10::1
UCS-A /fabric-interconnect/ipv6-config* # set out-of-band ipv6-prefix 64
UCS-A /fabric-interconnect/ipv6-config* # scope system
UCS-A /system* # set virtual-ip ipv6 2001:10::156
UCS-A /system* # commit-buffer
UCS-A /system #
```

イーサネット スイッチング モード

イーサネットスイッチングモードにより、サーバとネットワークの間のスイッチング装置としてファブリックインターコネクトがどのように動作するかが決定されます。ファブリックインターコネクトは、次のイーサネット スイッチング モードのいずれかで動作します。

エンドホスト モード

エンドホスト モードでは、ファブリック インターコネクトが、vNIC を介して接続されているすべてのサーバ（ホスト）に代わって、ネットワークに対するエンドホストとして動作できます。この動作は、vNIC をアップリンク ポートにピン接続することにより実現されます（動的なピン接続または固定のピン接続のいずれか）。これにより、ネットワークに対して冗長性が提供され、これらのアップリンク ポートはファブリックの残りの部分に対してサーバポートとなります。エンドホストモードの場合、ファブリックインターコネクトでスパニングツリープロトコル（STP）は実行されません。しかし、ループは、アップリンク ポートがトラフィックを相互に転送するのを拒否すること、および同時に複数のアップリンク ポート上に存在する出力サーバトラフィックを拒否することにより回避されます。エンドホストモードは、デフォルトのイーサネットスイッ

チング モードであり、次のいずれかがアップストリームで使用される場合に使用する必要があります。

- レイヤ 2 集約のための レイヤ 2 スイッチング
- Virtual Switching System（VSS）集約レイヤ

（注） エンドホスト モードを有効にした場合、vNIC がアップリンク ポートに固定ピン接続されていて、このアップリンク ポートがダウンすると、システムはその vNIC をピン接続し直すことはできず、その vNIC はダウンしたままになります。

スイッチ モード

スイッチ モードは従来のイーサネット スイッチング モードです。ループを回避するためにファブリック インターコネクトで STP が実行され、ブロードキャスト パケットとマルチキャスト パケットは従来の方法で処理されます。スイッチモードは、デフォルトのイーサネットスイッチングモードではありません。ファブリックインターコネクトをルータに直接接続する場合、または次のいずれかがアップストリームで使用される場合に限り使用する必要があります。

- レイヤ 3 集約
- ボックス内の VLAN

（注） どちらのイーサネット スイッチング モードの場合でも、サーバ アレイ内のすべてのサーバ間ユニキャスト トラフィックは、ファブリック インターコネクトを介してだけ送信され、アップリンク ポートを介して送信されることはありません。vNIC がアップリンク ポートに固定ピン接続されていたとしても同様です。サーバ間のマルチキャスト トラフィックとブロードキャスト トラフィックは、同じ VLAN 内のすべてのアップリンク ポートを介して送信されます。

イーサネット スイッチング モードの設定

重要 イーサネット スイッチング モードを変更すると、Cisco UCS Manager により自動的にログアウトとファブリック インターコネクトの再起動が実行されます。クラスタ設定では、Cisco UCS Manager により両方のファブリック インターコネクトが再起動されます。2 つめのファブリック インターコネクトでイーサネット スイッチング モードの変更が完了し、システムで使用できるようになるまで数分間かかります。設定は保持されます。

ファブリック インターコネクトがリブートされるときに、すべてのブレード サーバがすべての LAN および SAN 接続を失い、そのためにブレード上のすべてのサーバが完全に停止します。これにより、オペレーティング システムがクラッシュする場合があります。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネットアップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **set mode** {**end-host** | **switch**}	指定したスイッチング モードにファブリック インターコネクトを設定します。
ステップ 3	UCS-A /eth-uplink # **commit-buffer**	トランザクションをシステム設定にコミットします。 Cisco UCS Manager はファブリック インターコネクトを再起動し、ユーザをログアウトし、Cisco UCS Manager CLI との接続を解除します。

次に、ファブリック インターコネクトをエンドホスト モードに設定し、トランザクションをコミットする例を示します。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # set mode end-host
Warning: When committed, this change will cause the switch to reboot
UCS-A /eth-uplink* # commit-buffer
UCS-A /eth-uplink #
```

ファイバ チャネル スイッチング モード

ファイバ チャネル スイッチング モードは、サーバとストレージ デバイス間のスイッチング装置としてファブリック インターコネクトがどのように動作するかを決定します。ファブリック インターコネクトは、次のファイバ チャネル スイッチング モードのいずれかで動作します。

エンドホスト モード

エンドホストを使用すると、ファブリック インターコネクトは、仮想ホスト バス アダプタ（vHBA）を介して接続されているすべてのサーバ（ホスト）に代わって、接続されているファイバ チャネル ネットワークに対するエンド ホストとして動作することができます。この動作は、vHBA をファイバチャネル ポート アダプタにピン接続することにより実現されます（動的なピン接続または固定のピン接続のいずれか）。これにより、ファイバチャネルポートはファブリックの残りの部分に対してサーバ ポート（N ポート）となります。エンドホスト モードの場合、ファブリック インターコネクトは、アップリンク ポートがトラフィックを相互に転送するのを拒否することでループを回避します。

エンドホスト モードは N ポート仮想化（NPV）モードと同義です。このモードは、デフォルトのファイバ チャネル スイッチング モードです。

（注） エンドホスト モードを有効にした場合、vHBA がアップリンク ファイバ チャネル ポートに固定ピン接続されていて、このアップリンク ポートがダウンすると、システムはその vHBA をピン接続し直すことはできず、その vHBA はダウンしたままになります。

スイッチ モード

スイッチ モードは従来のファイバ チャネル スイッチング モードです。スイッチ モードを使用して、ファブリック インターコネクトをストレージデバイスに直接接続することができます。ファイバ チャネル スイッチ モードの有効化は、SAN が存在しない（たとえば、ストレージに直接接続された 1 つの Cisco UCS ドメイン）ポッド モデル、または SAN が存在する（アップストリーム MDS を使用）ポッド モデルで役に立ちます。

スイッチ モードはデフォルトのファイバ チャネル スイッチング モードではありません。

（注） ファイバ チャネル スイッチ モードでは、SAN ピン グループは不適切です。既存の SAN ピン グループはすべて無視されます。

ファイバ チャネル スイッチング モードの設定

（注） ファイバ チャネル スイッチング モードが変更されると、両方の Cisco UCS ファブリック インターコネクトは同時にリロードします。ファブリック インターコネクトをリロードすると、約 10 ～ 15 分のダウンタイムがシステム全体で発生します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **set mode** {**end-host** | **switch**}	指定したスイッチング モードにファブリック インターコネクトを設定します。
ステップ 3	UCS-A /fc-uplink # **commit-buffer**	トランザクションをシステム設定にコミットします。 Cisco UCS Manager はファブリック インターコネクトを再起動し、ユーザをログアウトし、Cisco UCS Manager CLI との接続を解除します。

次の例で、ファブリック インターコネクトを end-host モードに設定し、トランザクションをコミットする方法を示します。

```
UCS-A # scope fc-uplink
UCS-A /fc-uplink # set mode end-host
UCS-A /fc-uplink* # commit-buffer
UCS-A /fc-uplink #
```

第 6 章

ポートおよびポート チャネルの設定

この章の内容は、次のとおりです。

ファブリック インターコネクトのユニファイド ポート

ユニファイド ポートは、イーサネットまたはファイバ チャネル トラフィックを伝送するように設定できるファブリック インターコネクトのポートです。これらのポートは予約されていません。設定するまでは、Cisco UCS ドメイン でこれらのポートを使用できません。

（注） ファブリック インターコネクトのポートを設定すると、管理状態が自動的にイネーブルに設定されます。ポートが他のデバイスに接続されている場合は、これによってトラフィックが中断されることがあります。ポートの設定後に、そのポートを無効にできます。

設定可能なビーコン LED は、選択したポート モードに設定されているユニファイド ポートを示します。

ポート モード

ポート モードは、ファブリック インターコネクト上のユニファイド ポートが、イーサネットまたはファイバ チャネル トラフィックを転送するかどうかを決定します。ファブリック インターコネクトは、自動的にはポート モードを検出しません。ポート モードは Cisco UCS Manager で設定します。

ポート モードを変更すると、既存のポート設定が削除され、新しい論理ポートに置き換えられます。VLAN や VSAN など、そのポートの設定に関連付けられているオブジェクトはすべて削除されます。ユニファイド ポートのポート モードを変更できる回数に制限はありません。

ポート タイプ

ポート タイプは、ユニファイド ポート接続経由で転送されるトラフィックのタイプを定義します。

イーサネット ポート モードに変更されたユニファイド ポートは、デフォルトでアップリンク イーサネット ポート タイプに設定されます。ファイバ チャネル ポート モードに変更されたユニファイド ポートは、ファイブ チャネル アップリンク ポート タイプに設定されます。ファイバ チャネル ポートを設定解除することはできません。

ポート タイプ変更時のリブートは不要です。

イーサネット ポート モード

イーサネットにポート モードを設定するときは、次のポート タイプを設定できます。

- サーバ ポート
- イーサネット アップリンク ポート
- イーサネット ポート チャネル メンバ
- FCoE ポート
- アプライアンス ポート
- アプライアンス ポート チャネル メンバ
- SPAN 宛先ポート
- SPAN 送信元ポート

（注） SPAN 送信元ポートは、ポート タイプのいずれかを設定してから、そのポートを SPAN 送信元として設定します。

ファイバ チャネル ポート モード

ファイバ チャネルにポート モードを設定するときは、次のポート タイプを設定できます。

- ファイバ チャネル アップリンク ポート
- ファイバ チャネル ポート チャネル メンバ
- ファイバ チャネル ストレージ ポート
- FCoE アップリンク ポート
- SPAN 送信元ポート

（注） SPAN 送信元ポートは、ポート タイプのいずれかを設定してから、そのポートを SPAN 送信元として設定します。

Cisco UCS Mini スケーラビリティ ポート

Cisco UCS 6324 ファブリック インターコネクト には 4 つのユニファイド ポートに加えて、1 つのスケーラビリティ ポートがあります。スケーラビリティ ポートは、適切に配線されている場合に、4 つの 1G または 10G SFP+ ポートをサポート可能な 40GB QSFP+ ブレークアウト ポートです。また、スケーラビリティ ポートは、サポートされている Cisco UCS ラック サーバにライセンスされたサーバ ポート、アプライアンス ポート、または FCoE ポートとして使用できます。

Cisco UCS Manager GUI では、スケーラビリティ ポートが [イーサネットポート（Ethernet Ports）] ノードの下の [スケーラビリティポート5（Scalability Port 5）] として表示されます。個別のブレークアウト ポートは、[ポート1（Port 1）] ～ [ポート4（Port 4）] として表示されます。

Cisco UCS Manager CLI では、スケーラビリティ ポートは表示されませんが、個々のブレークアウト ポートは **Br-Eth1/5/1** ～ **Br-Eth1/5/4** として表示されます。

スケーラビリティ ポートの設定

スケーラビリティ ポートにポート、ポート チャネル メンバー、または SPAN メンバーを設定するには、スケーラビリティ ポートに移動してから、標準ユニファイド ポート用の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-server**	イーサネット サーバ モードを開始します。
ステップ 2	UCS-A /eth-server # **scope fabric** {**a** | **b**}	指定したファブリックのイーサネット サーバ ファブリック モードを開始します。
ステップ 3	UCS-A /eth-server/fabric # **scope aggr-interface** *slot-num port-num*	スケーラビリティ ポートのイーサネット サーバファブリック集約インターフェイス モードを開始します。
ステップ 4	UCS-A /eth-server/fabric/aggr-interface # **show interface**	スケーラビリティ ポートのインターフェイスを表示します。
ステップ 5	UCS-A /eth-server/fabric/aggr-interface # **create interface** *slot-num port-num*	指定されたイーサネット サーバ ポートのインターフェイスを作成します。
ステップ 6	UCS-A /eth-server/fabric/aggr-interface # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、ファブリック A スケーラビリティ ポートのイーサネット サーバ ポート 3 にインターフェイスを作成し、トランザクションをコミットする方法を示しています。

```
UCS-A# scope eth-server
UCS-A /eth-server # scope fabric a
UCS-A /eth-server/fabric # scope aggr-interface 1 5
UCS-A /eth-server/fabric/aggr-interface # show interface
Interface:

Slot Id Aggr-Port ID Port Id  Admin State Oper State    State Reason
------- ------------ -------- ----------- ------------- ------------
      1            5        1 Enabled     Up
      1            5        2 Enabled     Up
      1            5        3 Enabled     Admin Down    Administratively Down
      1            5        4 Enabled     Admin Down    Administratively Down

UCS-A /eth-server/fabric/aggr-interface # create interface 1 3
UCS-A /eth-server/fabric/aggr-interface* # commit-buffer
UCS-A /eth-server/fabric/aggr-interface #
```

ユニファイド ポートのビーコン LED

6200 シリーズ ファブリック インターコネクトの各ポートには、対応するビーコン LED があります。ビーコン LED プロパティが設定されている場合、ビーコン LED は点灯し、指定のポート モードでどのポートが設定されたかを表示します。

ビーコン LED プロパティは、どのポートが 1 つのポート モードにグループ化されたかを示すように設定できます。イーサネットまたはファイバ チャネルのいずれかです。デフォルトでは、ビーコン LED プロパティは [オフ（Off）] に設定されます。

（注） 拡張モジュールのユニファイド ポートの場合、ビーコン LED プロパティは拡張モジュール リブートの間デフォルト値の [オフ（Off）] にリセットされます。

ユニファイド ポートの設定に関するガイドライン

ユニファイド ポートを設定する際は、次のガイドラインおよび制約事項を考慮してください。

ポート モードの配置

Cisco UCS Manager GUI インターフェイスはユニファイド ポートのポート モードの設定に、スライダーを使用するため、ポートモードのユニファイドポートへの割り当て方法を制限する次の制約事項が自動的に適用されます。Cisco UCS Manager CLI インターフェイスを使用する場合は、トランザクションをシステム設定にコミットするときに次の制約事項が適用されます。ポート モードの設定が次の制約事項のいずれかに違反している場合、Cisco UCS Manager CLI によってエラーが表示されます。

- イーサネット ポートがブロックにグループ化されていること。
- ファイバ チャネル ポートがブロックにグループ化されていること。
- イーサネット ポートとファイバ チャネル ポートの交替は、サポートされない。

UCS Manager CLI ユーザ向けの特別な考慮事項

Cisco UCS Manager CLI では、システム設定にバッファをコミットするまでポート モードの変更が検証されないため、2 つの以上の新しいインターフェイスを作成する前にバッファのコミットを試みると、グループ化の制約にすぐに違反してしまいます。エラーを回避するために、ポート モードを別のポートモードに変更し、すべてのユニファイドポートに対して新しいインターフェイスを作成してから、システム設定に変更をコミットをすることを推奨します。

複数のインターフェイスを設定する前にバッファをコミットするとエラーが発生しますが、最初からやり直す必要はありません。設定が前述の要件を満たすまでユニファイド ポートの設定を続行できます。

ユニファイドアップリンクポートおよびユニファイドストレージポートの設定に関する注意およびガイドライン

以下は、ユニファイド アップリンク ポートとユニファイド ストレージ ポートを使用する際に従うべき注意事項とガイドラインです。

- ユニファイドアップリンク ポートでは、SPAN 送信元として 1 つのコンポーネントを有効にすると、他のコンポーネントが自動的に SPAN 送信元になります。

（注） イーサネット アップリンク ポートで SPAN 送信元を作成または削除すると、Cisco UCS Manager は自動的に FCoE アップリンク ポートで SPAN 送信元を作成または削除します。FCoE アップリンク ポートで SPAN 送信元を作成する場合も同じことが起こります。

- FCoE およびユニファイド アップリンク ポートでデフォルトでないネイティブ VLAN を設定する必要があります。この VLAN は、トラフィックには使用されません。Cisco UCS Manager はこの目的のために、既存の fcoe-storage-native-vlan を再利用します。この fcoe-storage-native-vlan は、FCoE およびユニファイド アップリンクでネイティブ VLAN として使用されます。
- ユニファイド アップリンク ポートでは、イーサネット アップリンク ポートにデフォルトでない VLAN を設定しないと、fcoe-storage-native-vlan がユニファイド アップリンク ポートのネイティブ VLAN として割り当てられます。イーサネット ポートにネイティブ VLAN として指定されているデフォルトでないネイティブ VLAN がある場合、ユニファイド アップリンク ポートのネイティブ VLAN としてこれが割り当てられます。
- イーサネット ポート チャネル下でメンバ ポートを作成または削除すると、Cisco UCS Manager は FCoE ポート チャネル下で自動的にメンバ ポートを作成または削除します。FCoE ポート チャネルでメンバー ポートを作成または削除する場合も同じことが起こります。
- サーバ ポート、イーサネット アップリンク、FCoE アップリンクまたは FCoE ストレージなどのスタンドアロン ポートとしてイーサネット ポートを設定し、それをイーサネットまたは FCOE ポート チャネルのメンバ ポートにすると、Cisco UCS Manager は自動的にこのポートをイーサネットと FCoE ポート チャネル両方のメンバにします。
- サーバアップリンク、イーサネットアップリンク、FCoE アップリンクまたは FCoE ストレージのメンバからメンバ ポートのメンバーシップを削除すると、Cisco UCS Manager はイーサネット ポート チャネルと FCoE ポート チャネルから対応するメンバ ポートを削除し、新しいスタンドアロン ポートを作成します。
- ユニファイドアップリンク ポートとユニファイドストレージポートの場合、2 つのインターフェイスを作成するときは、1 つだけライセンスがチェックされます。どちらかのインターフェイスが有効な限り、ライセンスはチェックされたままになります。両方のインターフェイスがユニファイド アップリンク ポートまたはユニファイド ストレージ ポートでディセーブルの場合にのみライセンスが解放されます。

ポート モードの変更のデータ トラフィックへの影響

ポート モードの変更は、Cisco UCS ドメイン へのデータ トラフィックの中断を引き起こす場合があります。中断の長さや影響を受けるトラフィックは、ポート モード変更を行ったモジュールおよび Cisco UCS ドメイン の設定に依存します。

ポート モード変更のクラスタ設定の固定モジュールへの影響

クラスタ設定には 2 個のファブリック インターコネクトがあります。固定モジュールへのポート変更を行った後、ファブリックインターコネクトはリブートします。データ トラフィックの影響は、1 つのファブリック インターコネクトに障害が発生したときにもう一方にフェールオーバーするようサーバ vNIC を設定したかどうかに左右されます。

両方のファブリック インターコネクトの固定モジュールのポート モードを同時に変更すると、ファブリック インターコネクトによるすべてのデータ トラフィックが、ファブリック インターコネクトがリブートする約 8 分間中断されます。

ポート モード変更のスタンドアロン設定の固定モジュールへの影響

スタンドアロン設定にはファブリック インターコネクトが 1 つだけあります。固定モジュールへのポート変更を行った後、ファブリックインターコネクトはリブートします。ファブリックインターコネクトを通過するすべてのデータ トラフィックは、ファブリック インターコネクトがリブートする約 8 分間中断されます。

ポート モードの設定

注意 いずれかのモジュールのポート モードを変更すると、データ トラフィックが中断されることがあります。これは、固定モジュールを変更するとファブリック インターコネクトのリブートが必要になり、拡張モジュールを変更するとそのモジュールのリブートが必要になるからです。

Cisco UCS ドメインに、ハイ アベイラビリティ用に設定されたクラスタ構成が存在し、フェールオーバー用に設定されたサービス プロファイルを持つサーバが存在する場合、固定モジュールのポートモードを変更しても、トラフィックは他のファブリックインターコネクトにフェールオーバーし、データ トラフィックは中断されません。

Cisco UCS Manager CLI には、ユニファイド ポートに対応している新規コマンドはありません。代わりに、必要なポート タイプ用のモードにスコープしてから新しいインターフェイスを作成することで、ポート モードを変更します。設定済みのスロット ID およびポート ID に新しいインターフェイスを作成する場合、UCS Manager は、すでに設定されているインターフェイスを削除し、新しく作成します。以前はイーサネット ポート モードで動作していたポートをファイバ チャネル ポート モードに設定するためにポート モードの変更が必要な場合、UCS Manager は変更を確認します。

（注） Cisco UCS Mini では拡張モジュールはサポートされていません。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope** *port-type-mode*	次のいずれかのポート タイプの指定されたポート タイプ モードを開始します。 **eth-server** サーバ ポート設定用。 **eth-storage** イーサネット ストレージ ポートおよびイーサネット ストレージ ポート チャネルの設定用。 **eth-traffic-mon** イーサネット SPAN ポート設定用。 **eth-uplink** イーサネット アップリンク ポート設定用。 **fc-storage** ファイバ チャネル ストレージ ポート設定用。 **fc-traffic-mon** ファイバ チャネル SPAN ポート設定用。 **fc-uplink** ファイバチャネルアップリンク ポートおよびファイバ チャネル アップリンク ポート チャネルの設定用。
ステップ 2	UCS-A /*port-type-mode* # **scope fabric** {**a** | **b**}	指定したファブリックの指定されたポート タイプ モードを開始します。
ステップ 3	UCS-A /*port-type-mode*/fabric # **create interface** *slot-id port-id*	指定されたポートタイプのインターフェイスを作成します。 ポート タイプをイーサネット ポート モードからファイバ チャネル ポート モードに、またはその逆に変更すると、次の警告が表示されます。 警告：この操作では、ポート モードがイーサネットから FC またはその逆に変更されます。（Warning: This operation will

	コマンドまたはアクション	目的
		change the port mode (from Ethernet to FC or vice-versa).）コミットすると、この変更はモジュールの再起動を要求します。（When committed, this change will require the module to restart.）
ステップ 4	イーサネットまたはファイバ チャネル ポート ブロックに属する他のポートの新しいインターフェイスを作成します。	イーサネットおよびファイバ チャネル ポートを固定または拡張モジュールに配置する方法を規定する、いくつかの制約事項があります。他の制約事項の範囲内で、2 つのグループのポートを変更する必要があります。「ユニファイド ポートの設定に関するガイドライン」の項に概説されている制約事項のいずれかに違反すると、エラーが発生します。
ステップ 5	UCS-A /*port-type-mode*/fabric/interface # **commit-buffer**	トランザクションをシステム設定にコミットします。

ポート モードを設定したモジュールに応じて、Cisco UCS ドメイン のデータ トラフィックが次のように中断されます。

- 固定モジュール：ファブリック インターコネクトがリブートします。そのファブリック インターコネクトを経由するすべてのデータ トラフィックが中断されます。ハイ アベイラビリティが提供され、フェールオーバー用に設定された vNIC があるサーバが含まれるクラスタ構成では、トラフィックは他のファブリック インターコネクトにフェールオーバーし、中断は発生しません。両側のポート モードを一度に変更すると、両方のファブリック インターコネクトが同時にリブートし、両方のファブリック インターコネクトが起動するまでトラフィックが完全に失われます。

  固定モジュールがリブートするまで約 8 分かかります。

- 拡張モジュール：モジュールがリブートします。そのモジュールのポートを経由するすべてのデータ トラフィックが中断されます。

  拡張モジュールがリブートするまでに約 1 分かかります。

次の例では、スロット 1 のポート 3 と 4 をイーサネット ポート モードのイーサネット アップリンク ポートからファイバ チャネル ポート モードのアップリンク ファイバ チャネル ポートに変更します。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # create interface 1 3
Warning: This operation will change the port mode (from Ethernet to FC or vice-versa).
When committed, this change will require the fixed module to restart.
UCS-A /fc-uplink/fabric/interface* # up
UCS-A /fc-uplink/fabric* #create interface 1 4
Warning: This operation will change the port mode (from Ethernet to FC or vice-versa).
When committed, this change will require the fixed module to restart.
UCS-A /fc-uplink/fabric/interface* #commit-buffer
```

ユニファイド ポートのビーコン LED の設定

ビーコン LED を設定する各モジュールについて次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fabric-interconnect** {**a** | **b**}	指定したファブリックのファブリック インターコネクト モードを開始します。
ステップ 2	UCS-A /fabric # **scope card** *slot-id*	指定された固定または拡張モジュールのカード モードを開始します。
ステップ 3	UCS-A /fabric/card # **scope beacon-led**	ビーコン LED モードを開始します。
ステップ 4	UCS-A /fabric/card/beacon-led # **set admin-state** {**eth** | **fc** | **off**}	点灯ビーコン LED ライトが表すポート モードを指定します。 **eth** イーサネット モードで設定されたユニファイド ポートすべてが点灯します。 **fc** ファイバチャネル モードで設定されたユニファイド ポートすべてが点灯します。 **off** モジュール上のすべてのポートのビーコン LED ライトが消えます。
ステップ 5	UCS-A /fabric/card/beacon-led # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、イーサネット ポート モードのユニファイド ポートのビーコン ライトすべてを点灯させ、トランザクションをコミットします。

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric # scope card 1
UCS-A /fabric/card # scope beacon-led
UCS-A /fabric/card/beacon-led # set admin-state eth
UCS-A /fabric/card/beacon-led* # commit-buffer
UCS-A /fabric/card/beacon-led #
```

物理ポートとバックプレーン ポート

ASIC から取得した物理ポートの統計情報の表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A /fabric-interconnect # **connect nxos** {**a** | **b**}	ファブリック インターコネクトの NX-OS モードを開始します。
ステップ 2	UCS-A(nxos)# **show interface ethernet** *slot/port*	ASIC から取得した物理ポートの統計情報を表示します。

次の例は、ASIC から取得した物理ポートの統計情報を表示する方法を示しています。

```
UCS-A /fabric-interconnect # connect nxos a
UCS-A(nxos)# show interface ethernet 1/11

Ethernet1/11 is up
 Dedicated Interface
  Hardware: 40000 Ethernet, address: a46c.2ae3.0e1a (bia a46c.2ae3.0e1a)
  Description: S: Server
  MTU 1500 bytes, BW 40000000 Kbit, DLY 10 usec
  reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA
  Port mode is fex-fabric
  full-duplex, 40 Gb/s, media type is 40G
  Beacon is turned off
  Input flow-control is off, output flow-control is off
  Rate mode is dedicated
  Switchport monitor is off
  EtherType is 0x8100
  Last link flapped 01:25:42
  Last clearing of "show interface" counters never
  2 interface resets
  30 seconds input rate 22664 bits/sec, 2833 bytes/sec, 3 packets/sec
  30 seconds output rate 9512 bits/sec, 1189 bytes/sec, 1189 bytes/sec, 4 packets/sec
  Load-Interval #2: 5 minute (300 seconds)
    input rate 33.80 Kbps, 5 pps; output rate 1.23 Mbps, 71 pps
  RX
    126057 unicast packets  1744 multicast packets  12877 broadcast packets
    140693 input packets  28702696 bytes
    3351 jumbo packets  0 storm suppression bytes
    0 runts  0 giants  0 CRC  0 no buffer
    0 input error  0 short frame  0 overrun   0 underrun  0 ignored
    0 watchdog  0 bad etype drop  0 bad proto drop  0 if down drop
    0 input with dribble  184 input discard
    0 Rx pause
  TX
    919778 unicast packets  6991 multicast packets  29 broadcast packets
    926798 output packets  1237109219 bytes
    794275 jumbo packets
    0 output errors  0 collision  0 deferred  0 late collision
    0 lost carrier  0 no carrier  0 babble 0 output discard
    0 Tx pause
```

```
Errors on Peer port (NIF):
RX
  8300 toolong frames  8400 undersize frames  8500 fragment frames
  8600 crcErr_not_stomped frames  8700 crcErr_stomped frames  8800 inRangeErr frames
TX
  8200 frames_with_error
```

BCM の物理ポートに対応するファブリック インターコネクトの物理ポートの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A /fabric-interconnect # **connect nxos** {**a** | **b**}	ファブリック インターコネクトの NX-OS モードを開始します。
ステップ 2	UCS-A(nxos)# **show hardware internal bcm-usd info port-info | grep** *interface_slot_id*	BCM の物理ポートに対応するファブリック インターコネクトの物理ポートを表示します。

次の例は、BCM の物理ポートに対応するファブリック インターコネクトの物理ポートの表示方法を示しています。

```
UCS-A /fabric-interconnect # connect nxos a
UCS-A(nxos)# show hardware internal bcm-usd info port-info | grep Eth 1/11

Eth1/11      0x1a00a000  41 xe-40   57   CR4 sw 4044 0 uta  2240     0 fd dis blk dis dis
ena 40G 40G up
```

バックプレーン ポートのステータス確認

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A /fabric-interconnect # **connect nxos** {**a** | **b**}	ファブリック インターコネクトの NX-OS モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A(nxos)# **show interface br**	バックプレーン ポートの速度やステータスなどを含むインターフェイスの設定を表示します。

次に、ファブリック インターコネクト A のバックプレーン ポートのステータスを確認する例を示します。

```
UCS-A /fabric-interconnect # connect nxos a
UCS-A(nxos)# show interface br


--------------------------------------------------------------------------------
Ethernet      VLAN   Type Mode   Status  Reason                   Speed     Port
Interface                                                                  Ch #
--------------------------------------------------------------------------------
Eth1/1        1       eth  access down    SFP not inserted           40G(D) --
Eth1/2        1       eth  access down    SFP not inserted           40G(D) --
Br-Eth1/3/1   1       eth  access down    Administratively down      10G(D) --
Br-Eth1/3/2   1       eth  access down    Administratively down      10G(D) --
Br-Eth1/3/3   1       eth  access down    Administratively down      10G(D) --
Br-Eth1/3/4   1       eth  access down    Administratively down      10G(D) --
Eth1/4        1       eth  access down    SFP not inserted           40G(D) --
Br-Eth1/5/1   4044    eth  trunk  down    Link not connected         10G(D) --
Br-Eth1/5/2   4044    eth  trunk  down    Link not connected         10G(D) --
Br-Eth1/5/3   4044    eth  trunk  down    Link not connected         10G(D) --
Br-Eth1/5/4   4044    eth  trunk  down    Link not connected         10G(D) --
Eth1/6        1       eth  access down    SFP not inserted           40G(D) --
Eth1/7        1       eth  access down    SFP not inserted           40G(D) --
Eth1/8        1       eth  access down    SFP not inserted           40G(D) --
Eth1/9        1       eth  access down    SFP not inserted           40G(D) --
Eth1/10       1       eth  access down    SFP not inserted           40G(D) --
Eth1/11       1       eth  fabric up      none                       40G(D) --
Eth1/12       1       eth  access down    SFP not inserted           40G(D) --
Eth1/13       1       eth  access down    SFP not inserted           40G(D) --
Eth1/14       1       eth  access down    SFP not inserted           40G(D) --
Eth1/15       1       eth  access down    SFP not inserted           40G(D) --
Eth1/16       1       eth  access down    SFP not inserted           40G(D) --
Eth1/17       1       eth  access down    SFP not inserted           40G(D) --
Eth1/18       1       eth  access down    SFP not inserted           40G(D) --
Eth1/19       1       eth  access down    SFP not inserted           40G(D) --
Eth1/20       1       eth  access down    SFP not inserted           40G(D) --
Br-Eth1/21/1  1       eth  trunk  up      none                       10G(D) --
Br-Eth1/21/2  1       eth  trunk  up      none                       10G(D) --
Br-Eth1/21/3  1       eth  trunk  down    Link not connected         10G(D) --
Br-Eth1/21/4  1       eth  trunk  up      none                       10G(D) --
Eth1/22       1       eth  access down    SFP not inserted           40G(D) --
Eth1/23       1       eth  access down    SFP not inserted           40G(D) --
Eth1/24       1       eth  access down    SFP not inserted           40G(D) --
Eth1/25       1       eth  access down    SFP not inserted           40G(D) --
Eth1/26       1       eth  access down    SFP not inserted           40G(D) --
Eth1/27       1       eth  access down    SFP not inserted           40G(D) --
Eth1/28       1       eth  access down    SFP not inserted           40G(D) --
Eth1/29       1       eth  access down    SFP not inserted           40G(D) --
Eth1/30       1       eth  access down    SFP not inserted           40G(D) --
Eth1/31       1       eth  access down    SFP not inserted           40G(D) --
Eth1/32       1       eth  access down    SFP not inserted           40G(D) --

--------------------------------------------------------------------------------
Port-channel VLAN    Type Mode   Status  Reason                   Speed   Protocol
Interface
--------------------------------------------------------------------------------
Po1285       1       eth  vntag  up      none                     a-10G(D)  none
```

```
Po1286       1       eth  vntag  up      none                          a-10G(D)  none
Po1287       1       eth  vntag  up      none                          a-10G(D)  none
Po1288       1       eth  vntag  up      none                          a-10G(D)  none
Po1289       1       eth  vntag  up      none                          a-10G(D)  none

--------------------------------------------------------------------------------
Port   VRF          Status IP Address                              Speed    MTU
--------------------------------------------------------------------------------
mgmt0  --           down   10.197.157.252                         --       1500

--------------------------------------------------------------------------------
Vethernet     VLAN   Type Mode   Status  Reason                       Speed
--------------------------------------------------------------------------------
Veth691       4047   virt trunk  down    nonParticipating         auto
Veth692       4047   virt trunk  up      none                     auto
Veth693       1      virt trunk  down    nonParticipating         auto
Veth695       1      virt trunk  up      none                     auto
Veth699       1      virt trunk  up      none                     auto

--------------------------------------------------------------------------------
Interface Secondary VLAN(Type)                    Status Reason
--------------------------------------------------------------------------------
Vlan1     --                                      down   Administratively down

--------------------------------------------------------------------------------
Ethernet       VLAN   Type Mode   Status  Reason                   Speed     Port
Interface                                                                    Ch #
--------------------------------------------------------------------------------
Eth1/1/1       1       eth  vntag  up      none                       10G(D) 1286
Eth1/1/2       1       eth  access down    Administratively down      10G(D) --
Eth1/1/3       1       eth  vntag  up      none                       10G(D) 1286
Eth1/1/4       1       eth  access down    Administratively down      10G(D) --
Eth1/1/5       1       eth  vntag  up      none                       10G(D) 1287
Eth1/1/6       1       eth  access down    Administratively down      10G(D) --
Eth1/1/7       1       eth  vntag  up      none                       10G(D) 1287
Eth1/1/8       1       eth  access down    Administratively down      10G(D) --
Eth1/1/9       1       eth  vntag  up      none                       10G(D) 1289
Eth1/1/10      1       eth  access down    Administratively down      10G(D) --
Eth1/1/11      1       eth  vntag  up      none                       10G(D) 1289
Eth1/1/12      1       eth  access down    Administratively down      10G(D) --
Eth1/1/13      1       eth  vntag  up      none                       10G(D) 1285
Eth1/1/14      1       eth  access down    Administratively down      10G(D) --
Eth1/1/15      1       eth  vntag  up      none                       10G(D) 1285
Eth1/1/16      1       eth  access down    Administratively down      10G(D) --
Eth1/1/17      1       eth  access down    Administratively down      10G(D) --
Eth1/1/18      1       eth  vntag  up      none                       10G(D) 1288
Eth1/1/19      1       eth  access down    Administratively down      10G(D) --
Eth1/1/20      1       eth  vntag  up      none                       10G(D) 1288
Eth1/1/21      1       eth  access down    Administratively down      10G(D) --
Eth1/1/22      1       eth  access down    Administratively down      10G(D) --
Eth1/1/23      1       eth  access down    Administratively down      10G(D) --
Eth1/1/24      1       eth  access down    Administratively down      10G(D) --
Eth1/1/25      1       eth  access down    Administratively down      10G(D) --
Eth1/1/26      1       eth  access down    Administratively down      10G(D) --
Eth1/1/27      1       eth  access down    Administratively down      10G(D) --
Eth1/1/28      1       eth  access down    Administratively down      10G(D) --
Eth1/1/29      1       eth  access down    Administratively down      10G(D) --
Eth1/1/30      1       eth  access down    Administratively down      10G(D) --
Eth1/1/31      1       eth  access down    Administratively down      10G(D) --
Eth1/1/32      1       eth  access down    Administratively down      10G(D) --
Eth1/1/33      4044    eth  trunk  up      none                      1000(D) --
```

サーバ ポート

サーバ ポートの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-server**	イーサネット サーバ モードを開始します。
ステップ 2	UCS-A /eth-server # **scope fabric** {**a** | **b**}	指定したファブリックのイーサネット サーバ ファブリック モードを開始します。
ステップ 3	UCS-A /eth-server/fabric # **create interface** *slot-num port-num*	指定されたイーサネット サーバ ポートのインターフェイスを作成します。
ステップ 4	UCS-A /eth-server/fabric # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例で、ファブリック B のスロット 1 にあるイーサネット サーバ ポート 4 のインターフェイスを作成し、トランザクションをコミットする方法を示します。

```
UCS-A# scope eth-server
UCS-A /eth-server # scope fabric b
UCS-A /eth-server/fabric # create interface 1 4
UCS-A /eth-server/fabric* # commit-buffer
UCS-A /eth-server/fabric #
```

サーバ ポートの設定解除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-server**	イーサネット サーバ モードを開始します。
ステップ 2	UCS-A /eth-server # **scope fabric** {**a** | **b**}	指定したファブリックのイーサネット サーバ ファブリック モードを開始します。
ステップ 3	UCS-A /eth-server/fabric # **delete interface** *slot-num port-num*	指定したイーサネット サーバ ポートのインターフェイスを削除します。
ステップ 4	UCS-A /eth-server/fabric # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、ファブリック B のスロット 1 にあるイーサネット サーバ ポート 12 を設定解除し、トランザクションをコミットする例を示します。

```
UCS-A# scope eth-server
UCS-A /eth-server # scope fabric b
UCS-A /eth-server/fabric # delete interface 1 12
UCS-A /eth-server/fabric* # commit-buffer
UCS-A /eth-server/fabric #
```

アップリンクのイーサネット ポート

アップリンク イーサネット ポートの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope fabric** {**a** | **b**}	指定されたファブリックのイーサネットアップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /eth-uplink/fabric # **create interface** *slot-num port-num*	指定されたイーサネット アップリンク ポートのインターフェイスを作成します。
ステップ 4	UCS-A /eth-uplink/fabric # **set speed** {**10gbps** | **1gbps**}	（任意） 指定されたイーサネット アップリンク ポートの速度を設定します。
ステップ 5	UCS-A /eth-uplink/fabric # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例で、ファブリック B のスロット 2 のイーサネット アップリンク ポート 3 にインターフェイスを作成し、10 Gbps の速度を設定し、トランザクションをコミットする方法を示します。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric b
UCS-A /eth-uplink/fabric # create interface 2 3
UCS-A /eth-uplink/fabric # set speed 10gbps
UCS-A /eth-uplink/fabric* # commit-buffer
UCS-A /eth-uplink/fabric #
```

アップリンク イーサネット ポートの設定解除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope fabric** {**a** | **b**}	指定されたファブリックのイーサネットアップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /eth-uplink/fabric # **delete interface** *slot-num port-num*	指定したイーサネット アップリンク ポートのインターフェイスを削除します。
ステップ 4	UCS-A /eth-uplink/fabric # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、ファブリック B のスロット 2 のイーサネット アップリンク ポート 3 を設定解除し、トランザクションをコミットする例を示します。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric b
UCS-A /eth-uplink/fabric # delete interface 2 3
UCS-A /eth-uplink/fabric* # commit-buffer
UCS-A /eth-uplink/fabric #
```

アプライアンス ポート

アプライアンスのポートは、直接接続された NFS ストレージをファブリック インターコネクトに接続するためだけに使用されます。

（注） 新しいアプライアンス VLAN を作成すると、IEEE VLAN ID は LAN クラウドに追加されません。したがって、新しい VLAN に設定されたアプライアンスのポートは、ピン接続障害が原因でデフォルトでダウンしたままになります。これらのアプライアンスのポートを起動するには、同じ IEEE VLAN ID を使用して LAN クラウドで VLAN を設定する必要があります。

Cisco UCS Manager リリース 2.2(4) では、ファブリック インターコネクトあたり最大 4 つのアプライアンス ポートをサポートします。

アプライアンス ポートの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-storage**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A /eth-storage # **scope fabric**{**a** | **b**}	指定したファブリックのイーサネット ストレージモードを開始します。
ステップ 3	UCS-A /eth-storage/fabric # **create interface** *slot-num port-num*	指定されたアプライアンス ポートのインターフェイスを作成します。
ステップ 4	UCS-A /eth-storage/fabric/interface # **set portmode** {**access** | **trunk**}	（任意） ポート モードがアクセスとトランクのどちらであるかを指定します。デフォルトで、モードはトランクに設定されます。 （注） アプリケーション ポートでアップリンク ポートをトラバースする必要がある場合、LANクラウドでこのポートによって使用される各VLANも定義する必要があります。たとえば、ストレージが他のサーバでも使用される場合や、プライマリ ファブリック インターコネクトのストレージ コントローラに障害が発生したときにトラフィックがセカンダリ ファブリック インターコネクトに確実にフェールオーバーされるようにする必要がある場合は、トラフィックでアップリンク ポートをトラバースする必要があります。
ステップ 5	UCS-A /eth-storage/fabric/interface # **set pingroupname** *pin-group name*	（任意） 指定されたファブリックとポート、またはファブリックとポート チャネルへのアプライアンス ピン ターゲットを指定します。
ステップ 6	UCS-A /eth-storage/fabric/interface # **set prio** *sys-class-name*	（任意） アプライアンス ポートにQoSクラスを指定します。デフォルトでは、プライオリティは best-effort に設定されます。 sys-class-name 引数には、次のいずれかのクラス キーワードを指定できます。 • [Fc]：vHBA トラフィックだけを制御するQoSポリシーにこの優先順位を使用します。

	コマンドまたはアクション	目的
		• [プラチナ（Platinum）]：vNIC トラフィックだけを制御する QoS ポリシーにこの優先順位を使用します。 • [ゴールド（Gold）]：vNIC トラフィックだけを制御する QoS ポリシーにこの優先順位を使用します。 • [シルバー（Silver）]：vNIC トラフィックだけを制御する QoS ポリシーにこの優先順位を使用します。 • [ブロンズ（Bronze）]：vNIC トラフィックだけを制御する QoS ポリシーにこの優先順位を使用します。 • [ベストエフォート（Best Effort）]：この優先順位は使用しないでください。 ベーシック イーサネット トラフィック レーンのために予約されています。この優先順位を QoS ポリシーに割り当て、別のシステム クラスを CoS 0 に設定する場合、Cisco UCS Manager はこのシステム クラスのデフォルトには戻りません。当該トラフィックの CoS 0 で優先順位がデフォルトに戻ります。
ステップ 7	UCS-A /eth-storage/fabric/interface # **set adminspeed** {**10gbps** | **1 gbps**}	（任意） インターフェイスの管理速度を指定します。デフォルトでは、管理速度は 10gbps に設定されます。
ステップ 8	UCS-A /eth-storage/fabric/interface # **commit buffer**	トランザクションをシステム設定にコミットします。

次の例は、ファブリック B のスロット 3 のアプライアンス ポート 2 にインターフェイスを作成し、ポート モードを access に設定し、アプライアンス ポートを pingroup1 と呼ばれるピン グループにピン接続し、QoS クラスを fc に設定し、管理速度を 10 Gbps に設定し、トランザクションをコミットします。

```
UCS-A# scope eth-storage
UCS-A /eth-storage # scope fabric b
UCS-A /eth-storage/fabric # create interface 3 2
UCS-A /eth-storage/fabric* # set portmode access
UCS-A /eth-storage/fabric* # set pingroupname pingroup1
UCS-A /eth-storage/fabric* # set prio fc
UCS-A /eth-storage/fabric* # set adminspeed 10gbps
UCS-A /eth-storage/fabric* # commit-buffer
UCS-A /eth-storage/fabric #
```

次の作業

アプライアンス ポートのターゲット MAC アドレスまたは VLAN を割り当てます。

アプライアンス ポートまたはアプライアンス ポート チャネルへの宛先 MAC アドレスの割り当て

次の手順は、アプライアンス ポートに宛先 MAC アドレスを割り当てます。アプライアンス ポート チャネルに宛先 MAC アドレスを割り当てるには、インターフェイスではなくポート チャネルに範囲を設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-storage**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A /eth-storage # **scope fabric** {**a** | **b**}	指定したファブリックのイーサネット ストレージ モードを開始します。
ステップ 3	UCS-A /eth-storage/fabric # **scope interface** *slot-id port-id*	指定したインターフェイスのイーサネット インターフェイス モードを開始します。 （注） アプライアンス ポート チャネルに宛先 MAC アドレスを割り当てるには、**scope interface** の代わりに **scope port-channel** コマンドを使用します。
ステップ 4	UCS-A /eth-storage/fabric/interface # **create eth-target** *eth-target name*	指定された MAC アドレス ターゲットの名前を指定します。
ステップ 5	UCS-A /eth-storage/fabric/interface/eth-target # **set mac-address** *mac-address*	MAC アドレスを nn:nn:nn:nn:nn:nn 形式で指定します。

次の例は、ファブリック B スロット 2 のポート 3 のアプライアンス デバイスに宛先 MAC アドレスを割り当て、トランザクションをコミットします。

```
UCS-A# scope eth-storage
UCS-A /eth-storage* # scope fabric b
UCS-A /eth-storage/fabric* # scope interface 2 3
UCS-A /eth-storage/fabric/interface* # create eth-target macname
UCS-A /eth-storage/fabric/interface* # set mac-address 01:23:45:67:89:ab
UCS-A /eth-storage/fabric/interface* # commit-buffer
UCS-A /eth-storage/fabric #
```

次の例は、ファブリック B のポート チャネル 13 のアプライアンス デバイスに宛先 MAC アドレスを割り当て、トランザクションをコミットします。

```
UCS-A# scope eth-storage
UCS-A /eth-storage* # scope fabric b
UCS-A /eth-storage/fabric* # scope port-channel 13
UCS-A /eth-storage/fabric/port-channel* # create eth-target macname
UCS-A /eth-storage/fabric/port-channel* # set mac-address 01:23:45:67:89:ab
```

```
UCS-A /eth-storage/fabric/port-channel* # commit-buffer
UCS-A /eth-storage/fabric #
```

アプライアンス ポートの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-storage**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A/eth-storage# **create vlan** *vlan-name vlan-id*	ネームドVLANを作成し、VLAN名とVLAN IDを指定し、イーサネット ストレージ VLAN モードを開始します。
ステップ 3	UCS-A/eth-storage/vlan# **set sharing primary**	変更を保存します。
ステップ 4	UCS-A/eth-storage/vlan# **commit buffer**	トランザクションをシステム設定にコミットします。
ステップ 5	UCS-A/eth-storage# **create vlan** *vlan-name vlan-id*	ネームドVLANを作成し、VLAN名とVLAN IDを指定し、イーサネット ストレージ VLAN モードを開始します。
ステップ 6	UCS-A/eth-storage/vlan# **set sharing community**	作成しているセカンダリ VLAN にプライマリ VLAN を関連付けます。
ステップ 7	UCS-A/eth-storage/vlan# **set pubnwname** *primary vlan-name*	このセカンダリ VLAN に関連付けられているプライマリ VLAN を指定します。
ステップ 8	UCS-A/eth-storage/vlan# **commit buffer**	トランザクションをシステム設定にコミットします。

次の例では、アプライアンス ポートを作成します。

```
UCS-A# scope eth-storage
UCS-A/eth-storage# create vlan PRI600 600
UCS-A/eth-storage/vlan* # set sharing primary
UCS-A/eth-storage/vlan* # commit-buffer
UCS-A/eth-storage # create vlan COM602 602
UCS-A/eth-storage/vlan* # set sharing isolated
UCS-A/eth-storage/vlan* # set pubnwname PRI600
UCS-A/eth-storage/vlan* # commit-buffer
```

コミュニティ VLAN へのアプライアンス ポートのマッピング

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-storage**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A/eth-storage# **scope fabric** {*a*|*b*}	指定したファブリック インターコネクトのイーサネット ストレージ ファブリック インターコネクト モードを開始します。
ステップ 3	UCS-A/eth-storage/fabric# **create interface** *slot-num port-num*	指定されたイーサネット サーバ ポートのインターフェイスを作成します。
ステップ 4	UCS-A/eth-storage/fabric/interface# **exit**	インターフェイスを終了します。 （注） VLAN との関連付けの後、トランザクションをコミットすることを確認します。
ステップ 5	UCS-A/eth-storage/fabric# **exit**	ファブリックを終了します。
ステップ 6	UCS-A/eth-storage# **scope vlan** *vlan-name*	指定された VLAN を入力します。 （注） コミュニティ VLAN がアプライアンスのクラウドで作成されていることを確認します。
ステップ 7	UCS-A/eth-storage/vlan# **create member-port** *fabric slot-num port-num*	指定したファブリックのメンバ ポートを作成し、スロット番号、およびポート番号を割り当て、メンバポートの設定を開始します。
ステップ 8	UCS-A/eth-storage/vlan/member-port# **commit**	トランザクションをシステム設定にコミットします。

次の例では、コミュニティ VLAN にアプライアンス ポートをマッピングします。

```
UCS-A# scope eth-storage
UCS-A/eth-storage# scope fabric a
UCS-A/eth-storage/fabric# create interface 1 22
UCS-A/eth-storage/fabric/interface*# exit
UCS-A/eth-storage/fabric*# exit
UCS-A/eth-storage*# scope vlan COM602
UCS-A/eth-storage/vlan*# create member-port a 1 22
UCS-A/eth-storage/vlan/member-port* commit
```

アプライアンス ポートの設定解除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope eth-storage**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A /eth-storage # **scope fabric** {**a** | **b**}	指定したファブリックのイーサネット ストレージ モードを開始します。
ステップ 3	UCS-A /eth-storage/fabric # **delete eth-interface** *slot-num port-num*	指定したアプライアンス ポートのインターフェイスを削除します。
ステップ 4	UCS-A /eth-storage/fabric # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、ファブリック B のスロット 2 のアプライアンス ポート 3 を設定解除し、トランザクションをコミットする例を示します。

```
UCS-A# scope eth-storage
UCS-A /eth-storage # scope fabric b
UCS-A /eth-storage/fabric # delete eth-interface 2 3
UCS-A /eth-storage/fabric* # commit-buffer
UCS-A /eth-storage/fabric #
```

FCoE アップリンク ポート

FCoEアップリンク ポートは、FCoE トラフィックの伝送に使用される、ファブリック インターコネクトとアップストリームイーサネット スイッチ間の物理イーサネットインターフェイスです。このサポートにより、同じ物理イーサネット ポートで、イーサネット トラフィックとファイバ チャネル トラフィックの両方を伝送できます。

FCoEアップリンク ポートはファイバチャネル トラフィック用のFCoEプロトコルを使用してアップストリームイーサネット スイッチに接続します。これにより、ファイバチャネルとイーサネット トラフィックの両方が同じ物理イーサネット リンクに流れることができます。

（注） FCoEアップリンクとユニファイドアップリンクは、ユニファイドファブリックをディストリビューション レイヤ スイッチまで拡張することによりマルチホップ FCoE 機能を有効にします。

次のいずれかと同じイーサネット ポートを設定できます。

- **FCoE アップリンク ポート**：ファイバ チャネル トラフィック専用の FCoE アップリンク ポートとして。
- **アップリンク ポート**：イーサネット トラフィック専用のイーサネット ポートとして。
- **ユニファイド アップリンク ポート**：イーサネットとファイバ チャネル両方のトラフィックを伝送するユニファイド アップリンク ポートとして。

FCoE アップリンク ポートの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	FC アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b**}	特定のファブリックに対して FC - アップリンク モードを開始します。
ステップ 3	UCS-A /fc-uplink/fabric # **create fcoeinterface** *slot-numberport-number*	指定した FCoE アップリンク ポートのインターフェイスを作成します。
ステップ 4	UCS-A /fc-uplink/fabric/fabricinterface # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、ファブリック A のスロット 8 で FCoE アップリンク ポート 1 のインターフェイスを作成し、トランザクションをコミットする例を示します。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # create fcoeinterface 1 8
UCS-A /fc-uplink/fabric/fcoeinterface* # commit-buffer
UCS-A /fc-uplink/fabric/fcoeinterface #
```

FCoE アップリンク ポートの設定解除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	FC アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b**}	特定のファブリックに対して FC - アップリンク モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /fc-uplink/fabric # **delete fcoeinterface** *slot-numberport-number*	指定したインターフェイスを削除します。
ステップ 4	UCS-A /fc-uplink/fabric/fabricinterface # **commit-buffer**	トランザクションをシステム設定にコミットします。

以下に、ファブリック A のスロット 8 のポート 1 上の FCoE アップリンク インターフェイスを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # delete fcoeinterface 1 8
UCS-A /fc-uplink/fabric/fcoeinterface* # commit-buffer
UCS-A /fc-uplink/fabric/fcoeinterface #
```

FCoE アップリンク ポートの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	FC アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b**}	特定のファブリックに対して FC - アップリンク モードを開始します。
ステップ 3	UCS-A /fc-uplink/fabric # **show fcoeinterface**	使用可能なインターフェイスを一覧表示します。

次に、ファブリック A で使用可能な FCoE アップリンク インターフェイスを表示する例を示します。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # show fcoeinterface
FCoE Interface:

Slot Id    Port Id    Admin State Operational State Operational State Reason  Li
c State            Grace Prd
---------- ---------- ----------- ----------------- ------------------------- --
------------------ ----------
         1         26 Enabled     Indeterminate                               Li
cense Ok                   0

Fcoe Member Port:

Port-channel Slot  Port  Oper State      State Reason
------------ ----- ----- --------------- ------------
1                1    10 Sfp Not Present Unknown
1                1     3 Sfp Not Present Unknown
```

```
1                1      4 Sfp Not Present Unknown
1                1      6 Sfp Not Present Unknown
1                1      8 Sfp Not Present Unknown
2                1      7 Sfp Not Present Unknown
UCS-A /fc-uplink/fabric #
```

ユニファイド アップリンク ポート

同じ物理イーサネット ポート上にイーサネット アップリンクと FCoE アップリンクを設定した場合、それらはユニファイド アップリンク ポートと呼ばれます。FCoE またはイーサネット インターフェイスは個別にイネーブルまたはディセーブルにできます。

- FCoE アップリンクをイネーブルまたはディセーブルにすると、対応する VFC がイネーブルまたはディセーブルになります。
- イーサネット アップリンクをイネーブルまたはディセーブルにすると、対応する物理ポートがイネーブルまたはディセーブルになります。

イーサネットアップリンクをディセーブルにすると、ユニファイドアップリンクを構成している物理ポートがディセーブルになります。したがって、FCoE アップリンクもダウンします（FCoE アップリンクがイネーブルになっている場合でも同様です）。しかし、FCoE アップリンクをディセーブルにした場合は、VFC だけがダウンします。イーサネットアップリンクがイネーブルであれば、FCoE アップリンクは引き続きユニファイド アップリンク ポートで正常に動作することができます。

ユニファイド アップリンク ポートの設定

ユニファイドアップリンク ポートを設定するには、ユニファイド ポートとして既存の FCoE アップリンク ポートを変換します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネットアップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope fabric** {**a** | **b**}	指定されたファブリックのイーサネット アップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /eth-uplink/fabric # **create interface** *15*	ユニファイド ポートとして FCoE アップリンク ポートを変換します。
ステップ 4	UCS-A /eth-uplink/fabric/port-channel # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、既存の FCoE ポートでユニファイド アップリンク ポートを作成します。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric b
UCS-A /eth-uplink/fabric # create interface 1 5
UCS-A /eth-uplink/fabric/interface* # commit-buffer
UCS-A /eth-uplink/interface #
```

FCoE およびファイバ チャネル ストレージ ポート

ファイバ チャネル ストレージまたは FCoE ポートの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-storage**	ファイバ チャネル ストレージ モードを開始します。
ステップ 2	UCS-A /fc-storage # **scope fabric** {**a** | **b**}	指定したファブリックのファイバチャネル ストレージ モードを開始します。
ステップ 3	UCS-A /fc-storage/fabric # **create interface** {**fc** | **fcoe**} *slot-num port-num*	指定されたファイバ チャネル ストレージ ポートのインターフェイスを作成します。
ステップ 4	UCS-A /fc-storage/fabric #**commit-buffer**	トランザクションをコミットします。

次の例は、ファブリック A スロット 2 のファイバ チャネル ストレージ ポート 10 のインターフェイスを作成し、トランザクションをコミットします。

```
UCS-A# scope fc-storage
UCS-A /fc-storage # scope fabric a
UCS-A /fc-storage/fabric* # create interface fc 2 10
UCS-A /fc-storage/fabric # commit-buffer
```

次の作業

VSAN を割り当てます。

ファイバ チャネル ストレージまたは FCoE ポートの設定解除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-storage**	ファイバチャネルストレージモードを開始します。
ステップ 2	UCS-A /fc-storage # **scope fabric** {**a** | **b**}	指定したファブリックのファイバ チャネル ストレージ モードを開始します。
ステップ 3	UCS-A /fc-storage/fabric # **delete interface** {**fc** | **fcoe**} *slot-num port-num*	指定したファイバチャネルストレージポートまたはFCoEストレージポートのインターフェイスを削除します。
ステップ 4	UCS-A /fc-storage/fabric #**commit-buffer**	トランザクションをコミットします。

次に、ファブリック A のスロット 2 のファイバ チャネル ストレージ ポート 10 を設定解除し、トランザクションをコミットする例を示します。

```
UCS-A# scope fc-storage
UCS-A /fc-storage # scope fabric a
UCS-A /fc-storage/fabric* # delete interface fc 2 10
UCS-A /fc-storage/fabric # commit-buffer
```

アップリンク ファイバ チャネル ポートへのファイバ チャネル ストレージ ポートの復元

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b**}	指定したファブリックでファイバチャネル アップリンク モードを開始します。
ステップ 3	UCS-A /fc-uplink/fabric # **create interface** *slot-num port-num*	指定したファイバ チャネル アップリンク ポートのインターフェイスを作成します。
ステップ 4	UCS-A /fc-uplink/fabric #**commit-buffer**	トランザクションをコミットします。

次に、ファブリック A のスロット 2 でファイバ チャネル アップリンク ポート 10 のインターフェイスを作成し、トランザクションをコミットする例を示します。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric* # create interface 2 10
UCS-A /fc-uplink/fabric # commit-buffer
```

アップリンク イーサネット ポート チャネル

アップリンク イーサネット ポート チャネルを使用すると、複数の物理アップリンク イーサネット ポートをグループ化して（リンク集約）、1 つの論理イーサネット リンクを作成し、耐障害性と高速接続を実現できます。Cisco UCS Manager で、先にポート チャネルを作成してから、そのポート チャネルにアップリンク イーサネット ポートを追加します。1 つのポート チャネルには、最大で 16 個のアップリンク イーサネット ポートを追加できます。

重要 設定されたポートの状態は、次のシナリオで未設定に変更されます。

- ポートはポート チャネルから削除されるか除去されます。ポート チャネルが、アップリンク、ストレージなど任意のタイプになります。
- ポート チャネルが削除されます。

（注） Cisco UCS では、ポート集約プロトコル（PAgP）ではなく、Link Aggregation Control Protocol（LACP）を使用して、アップリンク イーサネット ポートをポート チャネルにグループ化します。アップストリーム スイッチのポートが LACP に設定されていない場合、ファブリック インターコネクトはアップリンク イーサネット ポート チャネルの全ポートを個別のポートとして扱い、パケットを転送します。

アップリンク イーサネット ポート チャネルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /eth-uplink # **scope fabric** {**a** | **b** }	指定されたファブリックのイーサネット アップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /eth-uplink/fabric # **create port-channel** *port-num*	指定されたイーサネット アップリンク ポートのポート チャネルを作成し、イーサネット アップリンク ファブリック ポート チャネル モードを開始します。
ステップ 4	UCS-A /eth-uplink/fabric/port-channel # {**enable** | **disable**}	（任意） ポート チャネルの管理状態をイネーブルまたはディセーブルにします。ポート チャネルは、デフォルトではディセーブルです。
ステップ 5	UCS-A /eth-uplink/fabric/port-channel # **set name** *port-chan-name*	（任意） ポート チャネルの名前を指定します。
ステップ 6	UCS-A /eth-uplink/fabric/port-channel # **set flow-control-policy** *policy-name*	（任意） 指定されたフロー制御ポリシーをポート チャネルに割り当てます。
ステップ 7	UCS-A /eth-uplink/fabric/port-channel # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、ファブリック A のポート 13 にポート チャネルを作成し、portchan13a に名前を設定し、管理状態をイネーブルにし、ポート チャネルに flow-con-pol432 という名前のフロー制御ポリシーを割り当て、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # create port-channel 13
UCS-A /eth-uplink/fabric/port-channel* # enable
UCS-A /eth-uplink/fabric/port-channel* # set name portchan13a
UCS-A /eth-uplink/fabric/port-channel* # set flow-control-policy flow-con-pol432
UCS-A /eth-uplink/fabric/port-channel* # commit-buffer
UCS-A /eth-uplink/fabric/port-channel #
```

アップリンク イーサネット ポート チャネルの設定解除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope fabric** {**a** | **b** }	指定されたファブリックのイーサネット アップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /eth-uplink/fabric # **delete port-channel** *port-num*	指定したイーサネット アップリンク ポートのポート チャネルを削除します。
ステップ 4	UCS-A /eth-uplink/fabric # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、ファブリック A のポート 13 のポート チャネルを設定解除し、トランザクションをコミットする例を示します。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # delete port-channel 13
UCS-A /eth-uplink/fabric* # commit-buffer
UCS-A /eth-uplink/fabric #
```

アップリンク イーサネット ポート チャネルへのメンバ ポートの追加

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope fabric** {**a** | **b** }	指定されたファブリックのイーサネット アップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /eth-uplink/fabric # **scope port-channel** *port-num*	指定されたポート チャネルのイーサネット アップリンク ファブリック ポート チャネル モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	UCS-A /eth-uplink/fabric/port-channel # **create member-port** *slot-num port-num*	ポート チャネルから指定されたメンバ ポートを作成し、イーサネット アップリンク ファブリック ポート チャネルのメンバ ポート モードを開始します。
ステップ 5	UCS-A /eth-uplink/fabric/port-channel # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、スロット 1、ポート 7 のメンバ ポートをファブリック A のポート 13 のポート チャネルに追加し、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # scope port-channel 13
UCS-A /eth-uplink/fabric/port-channel # create member-port 1 7
UCS-A /eth-uplink/fabric/port-channel* # commit-buffer
UCS-A /eth-uplink/fabric/port-channel #
```

アップリンク イーサネット ポート チャネルからのメンバ ポートの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネットアップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope fabric** {**a** | **b** }	指定されたファブリックのイーサネット アップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /eth-uplink/fabric # **scope port-channel** *port-num*	指定されたポート チャネルのイーサネット アップリンク ファブリック ポート チャネル モードを開始します。
ステップ 4	UCS-A /eth-uplink/fabric/port-channel # **delete member-port** *slot-num port-num*	ポート チャネルから指定されたメンバ ポートを削除します。
ステップ 5	UCS-A /eth-uplink/fabric/port-channel # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、ファブリック A のポート 13 のポート チャネルからメンバ ポートを削除し、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # scope port-channel 13
UCS-A /eth-uplink/fabric/port-channel # delete member-port 1 7
UCS-A /eth-uplink/fabric/port-channel* # commit-buffer
UCS-A /eth-uplink/fabric/port-channel #
```

アプライアンス ポート チャネル

アプライアンス ポート チャネルを使用すると、複数の物理的なアプライアンス ポートをグループ化して 1 つの論理的なイーサネット ストレージ リンクを作成し、耐障害性と高速接続を実現できます。Cisco UCS Manager において、先にポート チャネルを作成してから、そのポート チャネルにアプライアンス ポートを追加します。1 つのポート チャネルには、最大で 8 個のアプライアンス ポートを追加できます。

アプライアンス ポート チャネルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-storage**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A /eth-storage # **scope fabric** {**a** | **b** }	指定したファブリックのイーサネット ストレージ ファブリック モードを開始します。
ステップ 3	UCS-A /eth-storage/fabric # **create port-channel** *port-num*	指定されたイーサネット ストレージ ポートのポート チャネルを作成し、イーサネット ストレージ ファブリック ポート チャネル モードを開始します。
ステップ 4	UCS-A /eth-storage/fabric/port-channel # {**enable** | **disable**}	（任意） ポート チャネルの管理状態をイネーブルまたはディセーブルにします。ポート チャネルは、デフォルトではディセーブルです。
ステップ 5	UCS-A /eth-storage/fabric/port-channel # **set name** *port-chan-name*	（任意） ポート チャネルの名前を指定します。
ステップ 6	UCS-A /eth-storage/fabric/port-channel # **set pingroupname** *pin-group name*	（任意） 指定されたファブリックとポート、またはファブリックとポート チャネルへのアプライアンス ピン ターゲットを指定します。

	コマンドまたはアクション	目的
ステップ 7	UCS-A /eth-storage/fabric/port-channel # **set portmode** {**access** | **trunk**}	（任意） ポート モードがアクセスとトランクのどちらであるかを指定します。デフォルトで、モードはトランクに設定されます。
ステップ 8	UCS-A /eth-storage/fabric/port-channel # **set prio** *sys-class-name*	（任意） アプライアンス ポートに QoS クラスを指定します。デフォルトでは、プライオリティは best-effort に設定されます。 sys-class-name 引数には、次のいずれかのクラス キーワードを指定できます。 • [Fc]：vHBA トラフィックだけを制御する QoS ポリシーにこの優先順位を使用します。 • [プラチナ（Platinum）]：vNIC トラフィックだけを制御する QoS ポリシーにこの優先順位を使用します。 • [ゴールド（Gold）]：vNIC トラフィックだけを制御する QoS ポリシーにこの優先順位を使用します。 • [シルバー（Silver）]：vNIC トラフィックだけを制御する QoS ポリシーにこの優先順位を使用します。 • [ブロンズ（Bronze）]：vNIC トラフィックだけを制御する QoS ポリシーにこの優先順位を使用します。 • [ベストエフォート（Best Effort）]：この優先順位は使用しないでください。ベーシック イーサネット トラフィック レーンのために予約されています。この優先順位を QoS ポリシーに割り当て、別のシステム クラスを CoS 0 に設定する場合、Cisco UCS Manager はこのシステム クラスのデフォルトには戻りません。当該トラフィックの CoS 0 で優先順位がデフォルトに戻ります。
ステップ 9	UCS-A /eth-storage/fabric/port-channel # **set speed** {**1gbps** | **2gbps** | **4gbps** | **8gbps** | **auto**}	（任意） ポート チャネルの速度を指定します。

	コマンドまたはアクション	目的
ステップ 10	UCS-A /eth-storage/fabric/port-channel # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、ファブリック A のポート 13 にポート チャネルを作成し、トランザクションをコミットします。

```
UCS-A# scope eth-storage
UCS-A /eth-storage # scope fabric a
UCS-A /eth-storage/fabric # create port-channel 13
UCS-A /eth-storage/fabric/port-channel* # enable
UCS-A /eth-storage/fabric/port-channel* # set name portchan13a
UCS-A /eth-storage/fabric/port-channel* # set pingroupname pingroup1
UCS-A /eth-storage/fabric/port-channel* # set portmode access
UCS-A /eth-storage/fabric/port-channel* # set prio fc
UCS-A /eth-storage/fabric/port-channel* # set speed 2gbps
UCS-A /eth-storage/fabric/port-channel* # commit-buffer
UCS-A /eth-storage/fabric/port-channel #
```

アプライアンス ポート チャネルの設定解除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-storage**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A /eth-storage # **scope fabric** {**a** | **b** }	指定したファブリックのイーサネット ストレージ ファブリック モードを開始します。
ステップ 3	UCS-A /eth-storage/fabric # **delete port-channel** *port-num*	指定したイーサネット ストレージ ポートからポート チャネルを削除します。
ステップ 4	UCS-A /eth-storage/fabric # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、ファブリック A のポート 13 のポート チャネルを設定解除し、トランザクションをコミットする例を示します。

```
UCS-A# scope eth-storage
UCS-A /eth-storage # scope fabric a
UCS-A /eth-storage/fabric # delete port-channel 13
UCS-A /eth-storage/fabric* # commit-buffer
UCS-A /eth-storage/fabric #
```

アプライアンス ポート チャネルのイネーブル化またはディセーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-storage**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A /eth-storage # **scope fabric** {**a** | **b** }	指定したファブリックのイーサネット ストレージ モードを開始します。
ステップ 3	UCS-A /eth-storage/fabric # **scope port-channel** *port-chan-name*	イーサネット ストレージ ポート チャネル モードを開始します。
ステップ 4	UCS-A /eth-storage/fabric/port-channel # {**enable** | **disable** }	ポート チャネルの管理状態をイネーブルまたはディセーブルにします。ポート チャネルは、デフォルトではディセーブルです。
ステップ 5	UCS-A /eth-storage/fabric/port-channel # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、ファブリック A のポート チャネル 13 をイネーブルにし、トランザクションをコミットする例を示します。

```
UCS-A# scope eth-storage
UCS-A /eth-storage # scope fabric a
UCS-A /eth-storage/fabric # scope port-channel 13
UCS-A /eth-storage/fabric/port-channel* # enable
UCS-A /eth-storage/fabric/port-channel* # commit-buffer
UCS-A /eth-storage/fabric/port-channel #
```

アプライアンス ポート チャネルへのメンバ ポートの追加

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-storage**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A /eth-storage # **scope fabric** {**a** | **b** }	指定したファブリックのイーサネット ストレージ ファブリック モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /eth-storage/fabric # **scope port-channel** *port-num*	指定されたポート チャネルのイーサネット ストレージ ファブリック ポート チャネル モードを開始します。
ステップ 4	UCS-A /eth-storage/fabric/port-channel # **create member-port** *slot-num port-num*	ポート チャネルから指定されたメンバ ポートを作成し、イーサネット ストレージ ファブリック ポート チャネルのメンバ ポート モードを開始します。
ステップ 5	UCS-A /eth-storage/fabric/port-channel # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、スロット 1、ポート 7 のメンバ ポートをファブリック A のポート 13 のポート チャネルに追加し、トランザクションをコミットします。

```
UCS-A# scope eth-storage
UCS-A /eth-storage # scope fabric a
UCS-A /eth-storage/fabric # scope port-channel 13
UCS-A /eth-storage/fabric/port-channel # create member-port 1 7
UCS-A /eth-storage/fabric/port-channel* # commit-buffer
UCS-A /eth-storage/fabric/port-channel #
```

アプライアンス ポート チャネルからのメンバ ポートの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-storage**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A /eth-storage # **scope fabric** {**a** | **b** }	指定したファブリックのイーサネット ストレージ ファブリック モードを開始します。
ステップ 3	UCS-A /eth-storage/fabric # **scope port-channel** *port-num*	指定されたポート チャネルのイーサネット ストレージ ファブリック ポート チャネル モードを開始します。
ステップ 4	UCS-A /eth-storage/fabric/port-channel # **delete member-port** *slot-num port-num*	ポート チャネルから指定されたメンバ ポートを削除します。
ステップ 5	UCS-A /eth-storage/fabric/port-channel # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、ファブリック A のポート 13 のポート チャネルからメンバ ポートを削除し、トランザクションをコミットします。

```
UCS-A# scope eth-storage
UCS-A /eth-storage # scope fabric a
UCS-A /eth-storage/fabric # scope port-channel 13
UCS-A /eth-storage/fabric/port-channel # delete member-port 1 7
UCS-A /eth-storage/fabric/port-channel* # commit-buffer
UCS-A /eth-storage/fabric/port-channel #
```

ファイバ チャネル ポート チャネル

ファイバ チャネル ポート チャネルによって、複数の物理ファイバ チャネル ポートをグループ化して（リンク集約）、1 つの論理ファイバ チャネル リンクを作成し、耐障害性と高速接続性を提供することができます。Cisco UCS Manager で、先にポート チャネルを作成してから、そのポート チャネルにファイバ チャネル ポートを追加します。

各 Cisco UCS ドメイン に最大 4 つのファイバ チャネル ポート チャネルを作成できます。各ファイバ チャネル ポートのチャネルは、最大 16 のアップリンク ファイバ チャネル ポートを含むことができます。

各 Cisco UCS ドメイン に最大 2 つのファイバ チャネル ポート チャネルを作成できます。各ファイバ チャネル ポート チャネルには、最大 4 つのアップリンク ファイバ チャネル ポートを含めることができます。

アップストリーム NPIV スイッチ上のファイバ チャネル ポート チャネルのチャネル モードが**アクティブ**に設定されていることを確認してください。メンバー ポートとピア ポートに同じチャネル モードが設定されていない場合、ポート チャネルはアップ状態になりません。チャネル モードが**アクティブ**に設定されている場合、ピア ポートのチャネル グループ モードに関係なく、メンバー ポートはピア ポートとのポート チャネル プロトコル ネゴシエーションを開始します。チャネル グループで設定されているピア ポートがポート チャネル プロトコルをサポートしていない場合、またはネゴシエーション不可能なステータスを返す場合、デフォルトでオン モードの動作に設定されます。**アクティブ** ポート チャネル モードでは、各端でポート チャネル メンバー ポートを明示的にイネーブルおよびディセーブルに設定することなく自動リカバリが可能です。

この例は、チャネル モードをアクティブに設定する方法を示しています。

```
switch(config)# int po114
switch(config-if)# channel mode active
```

ファイバ チャネル ポート チャネルの設定

（注） 2 つのファイバ チャネル ポート チャネルに接続する場合、両方のポート チャネルの管理速度が、使用するリンクに一致している必要があります。いずれかまたは両方のファイバ チャネル ポート チャネルの管理速度が auto に設定されている場合、Cisco UCS が管理速度を自動的に調整します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b** }	指定したファブリックのファイバ チャネル アップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /fc-uplink/fabric # **create port-channel** *port-num*	指定されたファイバ チャネル アップリンク ポートのポートチャネルを作成し、ファイバ チャネル アップリンク ファブリック ポート チャネル モードを開始します。
ステップ 4	UCS-A /fc-uplink/fabric/port-channel # {**enable** | **disable**}	（任意） ポートチャネルの管理状態をイネーブルまたはディセーブルにします。ポート チャネルは、デフォルトではディセーブルです。
ステップ 5	UCS-A /fc-uplink/fabric/port-channel # **set name** *port-chan-name*	（任意） ポート チャネルの名前を指定します。
ステップ 6	UCS-A /fc-uplink/fabric/port-channel # **set speed** {**1gbps** | **2gbps** | **4gbps** | **8gbps** | **auto**}	（任意） ポート チャネルの速度を指定します。
ステップ 7	UCS-A /fc-uplink/fabric/port-channel # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、ファブリック A にポート チャネル 13 を作成し、名前を portchan13a に設定し、管理状態をイネーブルにし、速度を 2 Gbps の設定し、トランザクションをコミットします。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # create port-channel 13
UCS-A /fc-uplink/fabric/port-channel* # enable
UCS-A /fc-uplink/fabric/port-channel* # set name portchan13a
```

```
UCS-A /fc-uplink/fabric/port-channel* # set speed 2gbps
UCS-A /fc-uplink/fabric/port-channel* # commit-buffer
UCS-A /fc-uplink/fabric/port-channel #
```

ファイバ チャネル ポート チャネルの設定解除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b** }	指定したファブリックのファイバ チャネル アップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /fc-uplink/fabric # **delete port-channel** *port-num*	指定したファイバ チャネル アップリンク ポートのポート チャネルを削除します。
ステップ 4	UCS-A /fc-uplink/fabric # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、ファブリック A のポート チャネル 13 を設定解除し、トランザクションをコミットする例を示します。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # delete port-channel 13
UCS-A /fc-uplink/fabric* # commit-buffer
UCS-A /fc-uplink/fabric #
```

アップストリーム NPIV のファイバ チャネル ポート チャネルへのチャネル モード アクティブの追加

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b** }	指定したファブリックのファイバ チャネル アップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /fc-uplink/fabric # **create port-channel** *port-num*	指定されたファイバ チャネル アップリンク ポートのポート チャネルを作成し、ファイバ チャネル アップリンク ファブリック ポート チャネル モードを開始します。
ステップ 4	UCS-A /fc-uplink/fabric/port-channel # {**enable** | **disable**}	（任意） ポート チャネルの管理状態をイネーブルまたはディセーブルにします。ポート チャネルは、デフォルトではディセーブルです。
ステップ 5	UCS-A /fc-uplink/fabric/port-channel # **set name** *port-chan-name*	（任意） ポート チャネルの名前を指定します。
ステップ 6	UCS-A /fc-uplink/fabric/port-channel # **scope** *port-chan-name*	（任意） ポート チャネルの名前を指定します。
ステップ 7	UCS-A /fc-uplink/fabric/port-channel # **channel mode** {**active**}	（任意） アップストリーム NPIV スイッチのチャネル モードをアクティブに設定します。
ステップ 8	UCS-A /fc-uplink/fabric/port-channel # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、チャネル モードをアクティブにする例を示します。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # create port-channel 13
UCS-A /fc-uplink/fabric/port-channel* # enable
UCS-A /fc-uplink/fabric/port-channel* # set name portchan13a
UCS-A /fc-uplink/fabric/port-channel* # channel mode active
UCS-A /fc-uplink/fabric/port-channel* # commit-buffer
UCS-A /fc-uplink/fabric/port-channel # exit
UCS-A /fc-uplink/fabric/ # show port-channel database

portchan13a
    Administrative channel mode is active
    Operational channel mode is active

UCS-A /fc-uplink/fabric/ #
```

ファイバ チャネル ポート チャネルのイネーブル化またはディセーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b** }	指定したファブリックでファイバ チャネル アップリンク モードを開始します。
ステップ 3	UCS-A /fc-uplink/fabric # **scope port-channel** *port-chan-name*	ファイバ チャネル アップリンク ポート チャネル モードを開始します。
ステップ 4	UCS-A /fc-uplink/fabric/port-channel # {**enable** | **disable** }	ポート チャネルの管理状態をイネーブルまたはディセーブルにします。ポート チャネルは、デフォルトではディセーブルです。

次に、ファブリック A のポート チャネル 13 をイネーブルにし、トランザクションをコミットする例を示します。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # scope port-channel 13
UCS-A /fc-uplink/fabric/port-channel* # enable
UCS-A /fc-uplink/fabric/port-channel* # commit-buffer
UCS-A /fc-uplink/fabric/port-channel #
```

ファイバ チャネル ポート チャネルへのメンバ ポートの追加

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b** }	指定したファブリックのファイバチャネルアップリンク ファブリック モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /fc-uplink/fabric # **scope port-channel** *port-num*	指定されたポート チャネルのファイバ チャネル アップリンク ファブリック ポート チャネル モードを開始します。
ステップ 4	UCS-A /fc-uplink/fabric/port-channel # **create member-port** *slot-num port-num*	ポート チャネルから指定されたメンバ ポートを作成し、ファイバ チャネル アップリンク ファブリック ポート チャネル メンバ ポート モードを開始します。
ステップ 5	UCS-A /fc-uplink/fabric/port-channel # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、スロット 1、ポート 7 のメンバ ポートをファブリック A のポート チャネル 13 に追加し、トランザクションをコミットします。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # scope port-channel 13
UCS-A /fc-uplink/fabric # create member-port 1 7
UCS-A /fc-uplink/fabric/port-channel* # commit-buffer
UCS-A /fc-uplink/fabric/port-channel #
```

ファイバ チャネル ポート チャネルからのメンバ ポートの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b**}	指定したファブリックのファイバ チャネル アップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /fc-uplink/fabric # **scope port-channel** *port-num*	指定されたポート チャネルのファイバ チャネル アップリンク ファブリック ポート チャネル モードを開始します。
ステップ 4	UCS-A /fc-uplink/fabric/port-channel # **delete member-port** *slot-num port-num*	ポート チャネルから指定されたメンバ ポートを削除します。

	コマンドまたはアクション	目的
ステップ 5	UCS-A /fc-uplink/fabric/port-channel # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、ファブリック A ポート チャネル 13 からメンバ ポートを削除し、トランザクションをコミットします。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # scope port-channel 13
UCS-A /fc-uplink/fabric # delete member-port 1 7
UCS-A /fc-uplink/fabric/port-channel* # commit-buffer
UCS-A /fc-uplink/fabric/port-channel #
```

FCoE ポート チャネル数

FCoE ポート チャネルでは、複数の物理 FCoE ポートをグループ化し、1 つの論理的な FCoE ポート チャネルを作成することができます。物理レベルでは、FCoE ポート チャネルは FCoE トラフィックをイーサネットポートチャネル経由で転送します。したがって、一連のメンバから構成される FCoE ポート チャネルは基本的に同じメンバから構成されるイーサネット ポート チャネルです。このイーサネット ポート チャネルは、FCoE トラフィックの物理トランスポートです。

各 FCoE ポート チャネルに対し、Cisco UCS Manager は VFC を内部的に作成し、イーサネットポートチャネルにバインドします。ホストから受信した FCoE トラフィックは、FCoE トラフィックが FC アップリンクに送信されるのと同じ方法で VFC に送信されます。

FCoE ポート チャネルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	FC アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b**}	特定のファブリックに対して FC - アップリンク モードを開始します。
ステップ 3	UCS-A /fc-uplink/fabric # **create fcoe-port-channel** *number*	指定した FCoE アップリンク ポートのポート チャネルを作成します。
ステップ 4	UCS-A /fc-uplink/fabric/fabricinterface # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、ファブリック A のスロット 4 で FCoE アップリンク ポート 1 のインターフェイスを作成し、トランザクションをコミットする例を示します。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # create fcoe-port-channel 4
UCS-A /fc-uplink/fabric/fcoe-port-channel* # commit-buffer
UCS-A /fc-uplink/fabric/fcoe-port-channel #
```

FCoE アップリンク ポート チャネルへのメンバ ポートの追加

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b** }	指定したファブリックのファイバ チャネル アップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /fc-uplink/fabric # **scope fcoe-port-channel** *ID*	指定したポート チャネルの FCoE アップリンク ポート チャネル モードを開始します。
ステップ 4	UCS-A /fc-uplink/fabric/fcoe-port-channel # **create member-port** *slot-num port-num*	ポート チャネルから指定されたメンバ ポートを作成し、FCoE アップリンク ファブリック ポート チャネルのメンバ ポート モードを開始します。 （注） FCoE アップリンク ポート チャネルがユニファイド アップリンク ポート チャネルである場合、次のメッセージが表示されます。 警告：これがユニファイド ポート チャネルの場合、メンバは同じ ID のイーサネット ポート チャネルにも追加されます。（Warning: if this is a unified port channel then member will be added to the ethernet port channel of the same id as well.）
ステップ 5	UCS-A /fc-uplink/fabric/fcoe-port-channel # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、スロット 1、ポート 7 のメンバ ポートをファブリック A の FCoE ポート チャネル 13 に追加し、トランザクションをコミットします。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # scope fcoe-port-channel 13
UCS-A /fc-uplink/fabric # create member-port 1 7
```

```
UCS-A /fc-uplink/fabric/fcoe-port-channel* # commit-buffer
UCS-A /fc-uplink/fabric/fcoe-port-channel #
```

ユニファイド アップリンク ポート チャネル

同じ ID でイーサネット ポート チャネルと FCoE ポート チャネルを作成した場合、それらはユニファイド ポート チャネルと呼ばれます。ユニファイド ポート チャネルが作成されると、指定されたメンバを持つファブリック インターコネクトで物理イーサネット ポート チャネルと VFC が作成されます。物理イーサネット ポート チャネルは、イーサネット トラフィックと FCoE トラフィックの両方を伝送するために使用されます。VFC は、FCoE トラフィックをイーサネット ポート チャネルにバインドします。

次のルールは、ユニファイド アップリンク ポート チャネルのメンバー ポート セットに適用されます。

- ユニファイド ポート チャネルとして設定されている、同じ ID のイーサネット ポート チャネルと FCoE ポート チャネルは、同じメンバー ポートのセットを持つ必要があります。
- イーサネット ポート チャネルにメンバー ポート チャネルを追加すると、Cisco UCS Manager は、FCoE ポート チャネルにも同じポート チャネルを追加します。同様に、FCoE ポート チャネルにメンバを追加すると、イーサネット ポート チャネルにそのメンバ ポートが追加されます。
- ポート チャネルの 1 つからメンバー ポートを削除すると、Cisco UCS Manager は他のポート チャネルから自動的にそのメンバー ポートを削除します。

イーサネット アップリンク ポート チャネルをディセーブルにすると、ユニファイド アップリンク ポート チャネルを構成している物理ポート チャネルがディセーブルになります。したがって、FCoE アップリンク ポート チャネルもダウンします（FCoE アップリンクがイネーブルになっている場合でも同様です）。FCoE アップリンク ポート チャネルをディセーブルにした場合は、VFC のみがダウンします。イーサネット アップリンク ポート チャネルがイネーブルであれば、FCoE アップリンク ポート チャネルは引き続きユニファイド アップリンク ポート チャネルで正常に動作することができます。

ユニファイド アップリンク ポート チャネルの設定

ユニファイド アップリンク ポート チャネルを設定するには、ユニファイド ポート チャネルとして既存の FCoE アップリンク ポート チャネルを変換します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /eth-uplink # **scope fabric** {**a** | **b**}	指定されたファブリックのイーサネットアップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /eth-uplink/fabric # **create port-channel** *ID*	指定したイーサネット アップリンク ポートのポート チャネルを作成します。
ステップ 4	UCS-A /eth-uplink/fabric/port-channel # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、既存の FCoE ポート チャネルでユニファイド アップリンク ポート チャネルを作成します。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric b
UCS-A /eth-uplink/fabric # create port-channel 2
UCS-A /eth-uplink/fabric/port-channel* # commit-buffer
UCS-A /eth-uplink/fabric #
```

イベント検出とアクション

Cisco UCS Manager は、I/O モジュール（IOM）からファブリック インターコネクトに接続されたネットワーク インターフェイス ポートにエラーが発生した場合にアラームを監視およびトリガーする統計情報収集ポリシーを使用します。

ネットワーク インターフェイス ポートのエラー統計情報は NiErrStats と呼ばれ、次のエラーで構成されています。

NiErrStats のエラー名	説明
frameTx	TX_FRM_ERROR のカウンタ値を収集します。
tooLong	RX_TOOLONG のカウンタ値を収集します。
tooShort	RX_UNDERSIZE と RX_FRAGMENT のカウンタ値の合計を収集します。
Crc	RX_CRERR_NOT_STOMPED と RX_CRCERR_STOMPED のカウンタ値の合計を収集します。
inRange	RX_INRANGEERR のカウンタ値を収集します。

（注） ネットワーク インターフェイス ポートの統計情報はアクティブ ポートからのみ収集され、その統計情報は Cisco UCS Manager に送信されます。

ポリシーベースのポート エラー処理

Cisco UCS Manager がアクティブな NI ポートでエラーを検出し、エラー ディセーブル機能がイネーブルの場合、Cisco UCS Manager はエラーが発生した NI ポートに接続されているそれぞれの FI ポートを自動的にディセーブルにします。FI ポートがエラーディセーブルになっているときは事実上シャットダウンし、トラフィックはポートで送受信されません。

エラー ディセーブル機能は、次の 2 つの目的で使用されます。

- どの FI ポートが error-disabled になっているかということと、接続されている NI ポートでエラーが発生したことを通知します。
- このポートが原因で同じシャーシ/FEX に接続された他のポートに障害が発生する可能性を削除します。このような障害は、NI ポートのエラーによって発生する可能性があり、最終的に重大なネットワーク上の問題を引き起こす可能性があります。エラーディセーブル機能は、この状況を回避するのに役立ちます。

しきい値定義の作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope eth-server**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A/eth-server # **scope stats-threshold-policy default**	統計情報しきい値ポリシー モードを開始します。
ステップ 3	UCSA/eth-server/stats-threshold-policy # **create class** *class-name*	指定された統計情報しきい値ポリシー クラスを作成し、組織統計情報しきい値ポリシー クラス モードを開始します。使用可能なクラス名キーワードのリストを表示するには、**create class ?** コマンドを組織しきい値ポリ

	コマンドまたはアクション	目的
		シー モードで入力します。
ステップ 4	UCS-A/eth-server/stats-threshold-policy/class # **create property** *property-name*	指定された統計情報しきい値ポリシー クラス プロパティを作成し、組織統計情報しきい値ポリシー クラス プロパティ モードを開始します。使用可能なプロパティ名キーワードのリストを表示するには、**create property ?** コマンドを組織しきい値ポリシー クラス モードで入力します。
ステップ 5	UCS-A/eth-server/stats-threshold-policy/class/property # **set normal-value** *value*	クラス プロパティに通常値を指定します。*value* の形式は、設定しているクラス プロパティによって異なる場合があります。必要な形式を確認するには、**set normal-value ?** コマンドを組織統計情報しきい値ポリシー クラス プロパティ モードで入力します。
ステップ 6	UCS-A/eth-server/stats-threshold-policy/class/property # **create threshold-value** {*above-normal* | *below-normal*} {*cleared* | *condition* | *critical* | *info* | *major* | *minor* | *warning*}	クラス プロパティに、指定したしきい値を作成し、組織統計情報しきい値ポリシー クラス プロパティ しきい値モードを開始します。
ステップ 7	UCS-A/eth-server/stats-threshold-policy/class/property/threshold-value # **set** {**deescalating** | **escalating**} *value*	降格および昇格のクラス プロパティ しきい値を指定します。*value* の形式は、設定されているクラス プロパティ しきい値によって異なる場合があります。必要な形式を確認するには、**set deescalating ?** または **set escalating ?**

	コマンドまたはアクション	目的
		コマンドを組織統計情報しきい値ポリシー クラス プロパティしきい値モードで入力します。
ステップ 8	UCS-A/eth-server/stats-threshold-policy/class/property/threshold-value # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、しきい値定義を作成する例を示します。

```
UCS-A # scope eth-server
UCS-A /eth-server # scope stats-threshold-policy default
UCS-A /eth-server/stats-threshold-policy # create class ni-ether-error-stats
UCS-A /eth-server/stats-threshold-policy/class* # create property crc-delta
UCS-A /eth-server/stats-threshold-policy/class/property* # set normal-value 0
UCS-A /eth-server/stats-threshold-policy/class/property* # create threshold-value above-normal
 major
UCS-A /eth-server/stats-threshold-policy/class/property/threshold-value* # set escalating
5
UCS-A /eth-server/stats-threshold-policy/class/property/threshold-value* # set deescalating
 3
UCS-A /eth-server/stats-threshold-policy/class/property/threshold-value* # commit-buffer
```

ファブリック インターコネクト ポートにエラー無効を設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope eth-server**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A/eth-server # **scope stats-threshold-policy default**	統計情報しきい値ポリシー モードを開始します。
ステップ 3	UCSA/eth-server/stats-threshold-policy # **scope class** *class-name*	指定した統計情報しきい値ポリシー クラスの組織統計情報しきい値ポリシー クラス モードを開始します。
ステップ 4	UCS-A/eth-server/stats-threshold-policy/class # **scope property** *property-name*	指定した統計情報しきい値ポリシー クラス プロパティの組織統計情報しきい値ポリシー クラス プロパティ モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	UCS-A/eth-server/stats-threshold-policy/class/property # **set error-disable-fi-port** {**yes** | **no**}	クラス プロパティにエラー ディセーブル化ステータスを指定します。 クラス プロパティのエラー ディセーブル化を無効にするには、**no** オプションを使用します。
ステップ 6	UCS-A/eth-server/stats-threshold-policy/class/property* # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、FI ポートでエラー ディセーブル化を有効にする方法を示しています。

```
UCS-A # scope eth-server
UCS-A /eth-server # scope stats-threshold-policy default
UCS-A /eth-server/stats-threshold-policy # scope class ni-ether-error-stats
UCS-A /eth-server/stats-threshold-policy/class # scope property crc-delta
UCS-A /eth-server/stats-threshold-policy/class/property # set error-disable-fi-port yes
UCS-A /eth-server/stats-threshold-policy/class/property* # commit-buffer
```

ファブリック インターコネクト ポートに自動リカバリを設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope eth-server**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A/eth-server # **scope stats-threshold-policy default**	統計情報しきい値ポリシー モードを開始します。
ステップ 3	UCSA/eth-server/stats-threshold-policy # **scope class** *class-name*	指定した統計情報しきい値ポリシー クラスの組織統計情報しきい値ポリシー クラス モードを開始します。
ステップ 4	UCS-A/eth-server/stats-threshold-policy/class # **scope property** *property-name*	指定した統計情報しきい値ポリシー クラス プロパティの組織統計情報しきい値ポリシー クラス プロパティ モードを開始します。
ステップ 5	UCS-A/eth-server/stats-threshold-policy/class/property # **set auto-recovery** {**enabled** | **disabled**}	クラスプロパティに自動リカバリ ステータスを指定します。

	コマンドまたはアクション	目的
		クラスプロパティの自動リカバリをディセーブルにするには、**disabled** オプションを使用します。
ステップ 6	UCS-A/eth-server/stats-threshold-policy/class/property* # **set auto-recovery-time** *time*	ポートが自動的に再びイネーブルになるまでの時間（分単位）を指定します。自動リカバリの時間は、0 ～ 4294967295 分の間で変更できます。
ステップ 7	UCS-A/eth-server/stats-threshold-policy/class/property* # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、FI ポートに自動リカバリを設定する方法を示しています。

```
UCS-A # scope eth-server
UCS-A /eth-server # scope stats-threshold-policy default
UCS-A /eth-server/stats-threshold-policy # scope class ni-ether-error-stats
UCS-A /eth-server/stats-threshold-policy/class # scope property crc-delta
UCS-A /eth-server/stats-threshold-policy/class/property # set auto-recovery enabled
UCS-A /eth-server/stats-threshold-policy/class/property* # set auto-recovery-time 5
UCS-A /eth-server/stats-threshold-policy/class/property* # commit-buffer
```

ネットワーク インターフェイス ポートのエラー カウンタの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope chassis** *chassis-num*	指定したシャーシでシャーシ モードを開始します。
ステップ 2	UCS-A/chassis # **scope iom** {**a** | **b**}	指定した IOM でシャーシ IOM モードを開始します。
ステップ 3	UCS-A/chassis/iom # **scope port-group fabric**	ネットワーク インターフェイス ポートを入力します。
ステップ 4	UCS-A/chassis/iom/port-group # **scope fabric-if** *fabric-if number*	指定されたネットワーク インターフェイスのポート番号を入力します。

	コマンドまたはアクション	目的
ステップ 5	UCS-A/chassis/iom/port-group/fabric-if # **show stats**	ネットワーク インターフェイス ポートのエラー カウンタを表示します。

次の例は、ネットワーク インターフェイス ポートの統計情報を表示する方法を示しています。

```
UCS-A # scope chassis 1
UCS-A/chassis # scope iom a
UCS-A/chassis/iom # scope port-group fabric
UCS-A/chassis/iom/port-group # scope faric-if 1
UCS-A/chassis/iom/port-group/fabric-if # show stats
NI Ether Error Stats:
Time Collected: 2014-08-20T15:37:24:688
Monitored Object: sys/chassis-1/slot-1/fabric/port-1/ni-err-stats
Suspect: Yes
Crc (errors): 5000
Frame Tx (errors): 0
Too Long (errors): 0
Too Short (errors): 0
In Range (errors): 0
Thresholded: 0
```

アダプタ ポート チャネル

アダプタ ポート チャネルは、Cisco UCS 仮想インターフェイス カード（VIC）から I/O モジュールへのすべての物理リンクを 1 つの論理リンクにグループ化します。

アダプタ ポート チャネルは、正しいハードウェアの存在を検出したときに Cisco UCS Manager によって内部的に作成また管理されます。アダプタ ポート チャネルの手動設定はできません。アダプタ ポート チャネルは、Cisco UCS Manager GUI または Cisco UCS Manager CLI を使用して表示できます。

アダプタ ポート チャネルの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope chassis** *chassis-num*	指定したシャーシでシャーシ モードを開始します。
ステップ 2	UCS-A /chassis # **scope iom** {**ab**}	指定した IOM でシャーシ IOM モードを開始します。
ステップ 3	UCS-A /chassis/iom # **scope port group**	指定したポート グループでポート グループ モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	UCS-A /chassis/iom/port group # **show host-port-channel** [**detail** | **expand**]	指定したシャーシのアダプタ ポート チャネルを表示します。

次に、ポート グループ モードでホスト ポート チャネルに関する情報を表示する例を示します。

```
UCS-A # scope chassis 1
UCS-A /chassis # scope iom a
UCS-A /chassis/iom # scope port group
UCS-A /chassis/iom/port group # show host-port-channel

Host Port channel:

  Port Channel Id Fabric ID Oper State       State Reason
    --------------- --------- ---------------- ------------
                1289 B         Up
                1290 B         Up
                1306 B         Up
                1307 B         Up
                1309 B         Up
                1315 B         Up

UCS-A /chassis/iom/port group #
```

第 7 章

ライセンスの管理

この章の内容は、次のとおりです。

ライセンス

各 Cisco UCS ファブリック インターコネクトにはいくつかのポート ライセンスが付属しています。これらはプレインストールされ、ハードウェアとともに出荷されます。ファブリック インターコネクトは、完全ライセンスまたは部分ライセンスで購入できます。また、納入後に追加ライセンスを購入することもできます。

次の 4 つの新しいライセンスは 6300 シリーズ FI 向けに追加され、6332 および 6332-16UP FI でのみ有効です。

- 40G_ETH_PORT_ACTIVATION_PKG：40 GB イーサネット ポート用ライセンス
- 40G_ETH_C_PORT_ACTIVATION_PKG：ラック サーバに直接接続された（C ダイレクト）40 GB イーサネット ポート用ライセンス
- 10G_C_PORT_ACTIVATION_PKG：ラック サーバに直接接続された（C ダイレクト）6332-16UP の最初の 16 個の 10 GB ユニファイド ポート用ライセンス

- 10G_PORT_ACTIVATION_PKG：6332-16UP の最初の 16 個の 10 GB ユニファイド ポート用ライセンス

（注） 10G_PORT_ACTIVATION_PKG および 10G_C_PORT_ACTIVATION_PKG ライセンスは 6332-16UP FI でのみ有効で、それらにだけインストールできます。

各ファブリック インターコネクトは、少なくとも次のカウントされたライセンスがプリインストールされた状態で出荷されます。

ファブリック インターコネクト	デフォルトの基本ライセンス
Cisco UCS 6248（ユニファイド ポート）	拡張モジュールの最初の 12 個の有効なイーサネット ポートおよび任意のファイバ チャネル ポート用。
Cisco UCS 6296（ユニファイド ポート）	拡張モジュールの最初の 18 個の有効なイーサネット ポートおよび任意のファイバ チャネル ポート用。
Cisco UCS 6324	4 個の非ブレークアウト ポート専用。ライセンスを含まない 5 番目のポートは、さらに 4 個の 10 GB ポートに分割されます。
Cisco UCS 6332 16UP	4 個の 40 GB ポートと 8 個の 10 GB ポート用。 （注） 最初の 16 個のポートは 10 GB です。残りは 40 GB です。
Cisco UCS 6332	8 個の 40 GB ポート用。

ポート ライセンスの使用
ポート ライセンスは物理ポートにバインドされません。ライセンスされているポートをディセーブルにすると、そのライセンスは次にイネーブルにされたポートで使用するために保持されます。追加の固定ポートを使用するには、それらのポート用のライセンスを購入し、インストールする必要があります。タイプ（ファイバ、イーサネット）に関係なく、ポートがイネーブルの場合は、すべてのポートがライセンスを使用します。

6332 および 6332-16UP プラットフォームで使用可能なブレークアウト対応ポートの場合は、ポートがブレークアウト ポートで、そのポートが引き続き 40 GB ライセンスを 1 つだけ使用する場合でも、40 GB のライセンスがメイン ポートに適用されたままになります。

（注） ポートの初期設定でそれをイネーブルにし、ライセンスを使用します。

重要　製品の世代間でライセンスを移動させることはできません。6200 シリーズ ファブリック インターコネクト用に購入したライセンスを使用して 6300 シリーズ ファブリック インターコネクトのポートをイネーブルにすることはできません。その逆も同様です。

各 Cisco UCS 6324 ファブリック インターコネクト にはポート ライセンスが付属します。このライセンスは工場でインストールされ、ハードウェアと共に出荷されます。このライセンスは 8 個の 40 GB ユニファイド ポートに対応し、サポートされているあらゆる用途に使用できます。C ダイレクト ポート ライセンスは猶予期間にプレインストールされ、Cisco UCS ラック サーバで使用できます。

猶予期間

ライセンスがインストールされていないポートを使用しようとすると、Cisco UCS は 120 日間の猶予期間を開始します。猶予期間は、最初にライセンスなしでポートを使用した時点から測定され、有効なライセンス ファイルがインストールされると一時停止されます。猶予期間中に使用された時間数はシステムに保存されます。

（注）　各物理ポートには固有の猶予期間があります。1 つのポートで猶予期間を開始しても、すべてのポートの猶予期間が開始するわけではありません。

ライセンスされているポートの設定を解除すると、そのライセンスは、猶予期間内で機能しているポートに移行されます。複数のポートが猶予期間内で動作している場合、ライセンスは猶予期間の終了が最も近いポートに移動されます。

ハイ アベイラビリティ構成

フェールオーバー中の不整合を避けるため、クラスタ内の両方のファブリック インターコネクトに同数のライセンスされたポートを用意することを推奨します。均衡が保たれていない状態でフェールオーバーが発生すると、Cisco UCS は欠けているライセンスを有効化して、フェールオーバー ノードで使用される各ポートに対して猶予期間を開始します。

C ダイレクト ラックのライセンスのサポート

各 Cisco UCS ファブリック インターコネクトは、デフォルトの数のポート ライセンスが工場で付与され、ハードウェアと一緒に出荷されます。C ダイレクト サポートは、ラック サーバに接続されたポートにのみ適用可能です。10G_C_PORT_ACTIVATION_PKG および 40G_ETH_C_PORT_ACTIVATION _PKG は、既存のライセンス機能と同じプロパティがすべて設定された既存のライセンス パッケージに追加されます。[下位数量（Subordinate Quantity）] プロパティは、ラック サーバに接続されたポートを追跡するために、10G_PORT_ACTIVATION_PKG および 40G_ETH_PORT_ACTIVATION_PKG に追加されます。

Cisco UCS Manager GUI の [ライセンス（License）] タブに、新しいライセンスとそのライセンスの [下位数量（Subordinate Quantity）] が表示されます。**scope license** の下で **show feature** コマンド

および **show usage** コマンドを使用して、ライセンス機能、ベンダー バージョン タイプ、各ライセンスの猶予期間を表示することもできます。

ラック サーバに接続されたポートは、ライセンスが使用可能であるか、またはライセンスが使用中でない場合に、既存の 10G_PORT_ACTIVATION_PKG および 40G_ETH_PORT_ACTIVATION_PKG を使用できます。それ以外の場合は、10G_C_PORT_ACTIVATION_PKG および 40G_ETH_C_PORT_ACTIVATION を購入してライセンスの猶予期間を無効にする必要があります。

10 GB ポートでの変更はありません。10G_PORT_ACTIVATION_PKG および 10G_C_PORT_ACTIVATION_PKG ライセンス パッケージには、既存の ETH_PORT_ACTIVATION_PKG および ETH_PORT_C_ACTIVATION_PKG ライセンス機能と同じプロパティがすべて含まれています。

設定と制約事項

- C ダイレクト ラック ライセンス機能は、CIMC ポートではなく、FI に直接接続されたラック サーバ ポートを構成します。10G_C_PORT_ACTIVATION_PKG および 40G_ETH_C_PORT_ACTIVATION_PKG のデフォルトの数量は常に 0 です。
- 40 GB ポートまたは 40 GB ブレークアウト ポート配下のブレークアウト ポートが接続なしで有効な場合、このポートには 40G_ETH_PORT_ACTIVATION_PKG（使用可能な場合）に基づいてライセンスが割り当てられます。このポートがタイム ラグの後にダイレクト コネクト ラック サーバに接続されると、ライセンスの完全な再割り当てがトリガーされ、このポートは、次のライセンス割り当てシナリオのいずれかで処理されます。

  40 GB ブレークアウト ポート配下のブレークアウト ポートがイネーブルで、そのポートがダイレクト コネクト ラック サーバに接続され、40G_C_PORT_ACTIVATION_PKG ライセンス ファイルが FI にインストールされている場合は、次のライセンス割り当てが行われます。

  - ブレークアウト ポート配下の他のポートがイネーブルでない場合は、40G_C_PORT_ACTIVATION_PKG に基づいて親の 40 GB ポートにライセンスが割り当てられ、使用済み数量がこのインスタンスに増分されます。
  - 他のポートが有効で、1 つ以上のポートがダイレクト コネクト ラック サーバに接続されていない場合は、ポートが使用されていない場合でも、40G_ETH_PORT_ACTIVATION_PKG に基づいて親の 40 GB ポートにライセンスが割り当てられ、使用済み数量がこのインスタンスに増分されます。

- 40 GB ブレークアウト ポート配下のブレークアウト ポートがイネーブルで、そのポートがダイレクト コネクト ラック サーバに接続され、40G_C_PORT_ACTIVATION_PKG ライセンス ファイルが FI にインストールされていない場合は、次のライセンス割り当てが行われます。

  - ブレークアウト ポート配下のポートがイネーブルでない場合は、40G_ETH_PORT_ACTIVATION_PKG に基づいて親の 40 GB ポートにライセンスが割り当てられます。ライセンスが 40G_ETH_PORT_ACTIVATION_PKG で使用可能な場合は、下位の数量が増分されます。ライセンスが使用可能でない場合は、この機能の使用済み数量が増分され、ポート全体が猶予期間に入ります。

- 他のポートが有効で、1 つ以上のポートがダイレクト コネクト ラック サーバに接続されていない場合は、ポートが使用されていない場合でも、40G_ETH_PORT_ACTIVATION_PKG に基づいて親の 40 GB ポートにライセンスが割り当てられ、使用済み数量がこのインスタンスに増分されます。

ファブリック インターコネクトのホスト ID の入手

ホスト ID はシリアル番号とも呼ばれます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope license**	ライセンス モードを開始します。
ステップ 2	UCS-A /license # **show server-host-id**	ファブリック インターコネクトのホスト ID またはシリアル番号を入手します。 **ヒント** 等号（=）の後ろに表示されるホスト ID 全体を使用します。

次に、ファブリック インターコネクトのホスト ID を入手する例を示します。

```
UCS-A# scope license
UCS-A /license # show server-host-id
Server host id:
    Scope Host Id
    ----- -------
    A     VDH=SSI12121212
    B     VDH=SSI13131313
UCS-A /license #
```

次の作業

シスコから必要なライセンスを入手します。

ライセンスの取得

（注） このプロセスは、このマニュアルのリリース後に変更される場合があります。このマニュアルの手順が 1 つ以上当てはまらない場合は、シスコの担当者にライセンス ファイルの入手方法をお問い合わせください。

はじめる前に

次を入手します。

- ファブリック インターコネクトのホスト ID またはシリアル番号
- ファブリック インターコネクトの権利証明書またはその他の購入証明書

手順

ステップ 1 権利証明書またはその他の購入証明書から、製品認証キー（PAK）を取得します。

ステップ 2 権利証明書またはその他の購入証明書で Web サイトの URL を確認します。

ステップ 3 ファブリック インターコネクトの Web サイト URL にアクセスし、シリアル番号と PAK を入力します。
シスコからライセンスファイルが電子メールで送信されます。ライセンスファイルは、要求されたファブリック インターコネクトでの使用だけを許可するようにデジタル署名されています。Cisco UCS Manager がライセンス ファイルにアクセスすると、要求された機能もイネーブルになります。

次の作業

ファブリック インターコネクトにライセンスをインストールします。

ライセンスのインストール

（注） クラスタ構成の場合、マッチング ペアの両方のファブリック インターコネクトにライセンスをダウンロードしてインストールすることを推奨します。個々のライセンスは、ダウンロードを開始するために使用するファブリック インターコネクトのみにダウンロードされます。

はじめる前に

シスコから必要なライセンスを入手します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope license**	ライセンス モードを開始します。
ステップ 2	UCS-A /license # **download license** *from-filesystem*	ダウンロード元の場所からライセンスをダウンロードします。*from-filesystem:* 引数には、次のいずれかの構文を使用します。 • **ftp://** *server-ip-addr* • **scp://** *username@server-ip-addr*

	コマンドまたはアクション	目的
		• **sftp:**// *username@server-ip-addr* • **tftp:**// *server-ip-addr***:** *port-num* パス名またはファイル名にスペースを含めることはできません。たとえば、`c:\Path\Folder_Name\License.lic`は有効なパスですが、`c:\Path\Folder Name\License.lic`は「`Folder Name`」内にスペースがあるため無効です。
ステップ 3	UCS-A /license # **install file** *license_filename*	ライセンスをインストールします。

次に、FTP を使用してライセンスをダウンロードし、インストールする例を示します。

```
UCS-A # scope license
UCS-A /license # download license ftp://192.168.10.10/license/port9.lic
UCS-A /license # install file port9.lic
UCS-A /license #
```

ファブリックインターコネクトにインストールされているライセンスの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope license**	ライセンス モードを開始します。
ステップ 2	UCS-A /license # **show file** [*license_filename* | **detail**]	ファブリック インターコネクトにインストールされたライセンスを、コマンドで指定した詳細レベルで表示します。

次に、ファブリック インターコネクトにインストールされたライセンスの全詳細を表示する例を示します。

```
UCS-A# scope license
UCS-A /license # show file detail

License file: UCSFEAT20100928112305377.lic
    Id: 1212121212121212
    Version: 1.0
    Scope: A
    State: Installed
```

```
    Features
    Feature Name: ETH_PORT_ACTIVATION_PKG
    Vendor: cisco
    Version: 1.0
    Quantity: 24
    Lines
        Line Id: 1
        Type: Increment
        Expiry Date: Never
        Pak:
        Quantity: 24
        Signature: B10101010101

License file: UCSFEAT20100928112332175.lic
    Id: 1313131313131313
    Version: 1.0
    Scope: B
    State: Installed
    Features
    Feature Name: ETH_PORT_ACTIVATION_PKG
    Vendor: cisco
    Version: 1.0
    Quantity: 24
    Lines
        Line Id: 1
        Type: Increment
        Expiry Date: Never
        Pak:
        Quantity: 24
        Signature: F302020202020

UCS-A /license #
```

ファブリックインターコネクトのライセンス使用状況の表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope license**	ライセンス モードを開始します。
ステップ 2	UCS-A /license # **show usage**	ファブリック インターコネクトにインストールされたすべてのライセンス ファイルに関するライセンス使用状況テーブルを表示します。 これには以下が含まれます。 • **機能名（Feat Name）** ライセンスを適用する機能の名前。 • **範囲（Scope）** ライセンスに関連付けられたファブリック。

	コマンドまたはアクション	目的
		• **デフォルト（Default）** この Cisco UCS ドメイン に提供されるデフォルトのライセンス数。 • **合計数量（Total Quant）** 使用可能なライセンスの総数。この値は、購入ライセンス数とデフォルト ライセンス数の合計です。 • **使用済み数量（Used Quant）** 現在システムで使用中のライセンスの数。この値が使用可能なライセンスの総数を超えると、一部のポートは関連する猶予期間を経過した後に機能を停止します。 • **下位数量（Subordinate Quant）** 現在システムで使用中の C シリーズ ラック サーバ。 • **状態（State）** ライセンスの動作状態。 • **ピア カウントの比較（Peer Count Comparison）** このファブリック インターコネクトと比較したピア ファブリック インターコネクトのライセンス数。次のいずれかになります。 • [超えています（exceeds）]：ピア ファブリック インターコネクトには、このファブリック インターコネクトよりも多くのライセンスがインストールされています • [不足しています（lacks）]：ピア ファブリック インターコネクトには、このファブリック インターコネクトよりも少ないライセンスがインストールされています • [一致しています（matching）]：両方のファブリック インターコネクトに同数のライセンスがインストールされています

	コマンドまたはアクション	目的
		• **使用された猶予（Grace Used）** 猶予期間に使用された時間（秒単位）。猶予期間が終了すると、新しいライセンスを購入するまで Cisco UCS がアラートメッセージを送信します。

次に、ファブリック インターコネクトにインストールされたライセンスの全詳細を表示する例を示します。

```
UCS-A# scope license
UCS-A /license # show usage
Feat Name                    Scope Default Total Quant Used Quant Subordinate Quant
State                Peer Count Comparison   Grace Used
---------------------------- ----- ------- ----------- ---------- --------------------
-------------------- ---------------------- ----------
ETH_PORT_ACTIVATION_PKG        A     20      48          12                           0
License Ok           Matching                        0
ETH_PORT_C_ACTIVATION_PKG      A     0       0           0                            0
Not Applicable       Matching                        0
ETH_PORT_ACTIVATION_PKG        B     20      48          11                           0
License Ok           Matching                        0
ETH_PORT_C_ACTIVATION_PKG      B     0       0           0                            0
Not Applicable       Matching                        0
UCS-A /license #

UCS-A# scope license
UCS-A /license # show feature

License feature:
    Name                      Vendor Version Type                Grace Period
    ------------------------- ------ ------- ------------------- ------------
    ETH_PORT_ACTIVATION_PKG   cisco  1.0     Counted                     120
    ETH_PORT_C_ACTIVATION_PKG cisco  1.0     Counted                     120
UCS-A /license #
```

ライセンスのアンインストール

（注） 使用中の永続ライセンスはアンインストールできません。未使用の永久ライセンスだけをアンインストールできます。使用中の永久ライセンスの削除を試みると、その要求は Cisco UCS Manager によって拒否され、エラー メッセージが表示されます。

はじめる前に

Cisco UCS Manager の設定をバックアップします。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope license**	ライセンス モードを開始します。
ステップ 2	UCS-A /license # **clear file** *license-filename*	指定したライセンスをアンインストールします。

Cisco UCS Manager はライセンスを非アクティブ化し、ライセンスのリストからそのライセンスを削除し、ファブリック インターコネクトからライセンスを削除します。ポートは、ライセンスなしモードに移行します。クラスタ構成の場合は、他のファブリック インターコネクトからもライセンスをアンインストールする必要があります。

次に、port9.lic をアンインストールする例を示します。

```
UCS-A # scope license
UCS-A /license # clear file port9.lic
Clearing license port9.lic:
SERVER this_host ANY
VENDOR cisco
INCREMENT ETH_PORT_ACTIVATION_PKG cisco 1.0 permanent 1 \
        VENDOR_STRING=<LIC_SOURCE>UCS_SWIFT</LIC_SOURCE><SKU>N10-L001=</SKU> \
        HOSTID=VDH=FLC12360025 \
        NOTICE="<LicFileID>20090519200954833</LicFileID><LicLineID>1</LicLineID> \
        <PAK></PAK>" SIGN=C01FAE4E87FA

Clearing license ........done
UCS-A /license #
```

第 8 章

コミュニケーション サービスの設定

この章の内容は、次のとおりです。

• 通信サービスのディセーブル化，158 ページ

コミュニケーション サービス

以下に定義する通信サービスを使用してサードパーティ アプリケーションを Cisco UCS に接続できます。

Cisco UCS Manager では、次のサービスに対して IPv4 および IPv6 アドレス アクセスをサポートしています。

- CIM XML
- HTTP
- HTTPS
- SNMP
- SSH
- Telnet

Cisco UCS Manager では、Web ブラウザから [Cisco UCS KVM ダイレクト（Cisco UCS KVM Direct）] 起動ページへのアウトオブバンド IPv4 アドレス アクセスをサポートしています。このアクセスを提供するには、次のサービスをイネーブルにする必要があります。

- CIMC Web サービス

通信サービス	説明
CIM XML	Common Information Model（CIM XML）サービスはデフォルトはディセーブルであり、読み取り専用モードでのみ利用できます。デフォルト ポートは 5988 です。 CIM XML は、Distributed Management Task Force によって定義された CIM 情報を交換するための標準ベースのプロトコルです。
CIMC Web サービス	このサービスは、デフォルトでディセーブルになります。 このサービスをイネーブルにすると、ユーザは直接サーバに割り当てられるか、またはサービス プロファイルを介しサーバに関連付けられたアウトオブバンドの管理 IP アドレスの 1 つを使用して直接サーバ CIMC にアクセスできます。 （注） CIMC Web サービスは全体的にイネーブルまたはディセーブルにすることのみが可能です。個別の CIMC IP アドレスに対し KVM ダイレクト アクセスを設定することはできません。

通信サービス	説明
HTTP	デフォルトでは、HTTP はポート 80 でイネーブルになっています。 Cisco UCS Manager GUI は HTTP または HTTPS のブラウザで実行できます。HTTP を選択した場合、すべてのデータはクリア テキスト モードで交換されます。 ブラウザ セッションの安全性の理由により、HTTPS をイネーブルにし、HTTP をディセーブルにすることを推奨します。 デフォルトでは、Cisco UCS では同等の HTTPS にリダイレクトするブラウザ リダイレクトを実装しています。この動作は変更しないことを推奨します。 （注） Cisco UCS バージョン 1.4(1) にアップグレードすると、セキュアなブラウザへのブラウザのリダイレクトはデフォルトでは発生しなくなります。HTTP ブラウザからの同等の HTTPS ブラウザへリダイレクトするには、Cisco UCS Manager で [HTTP を HTTPS にリダイレクト（Redirect HTTP to HTTPS）] をイネーブルにします。
HTTPS	デフォルトでは、HTTPS はポートでイネーブルになっています。 HTTPS を使用すると、すべてのデータはセキュアなサーバを介して暗号化モードで交換されます。 ブラウザ セッションの安全性の理由により、HTTPS だけを使用し、HTTP 通信はディセーブルにするかリダイレクトすることを推奨します。
SMASH CLP	このサービスは読み取り専用アクセスに対してイネーブルになり、**show** コマンドなど、プロトコルの一部のサブセットをサポートします。これをディセーブルにすることはできません。 このシェル サービスは、Distributed Management Task Force によって定義された標準の 1 つです。
SNMP	デフォルトでは、このサービスは無効になっています。イネーブルの場合、デフォルトのポートは 161 です。コミュニティと少なくとも 1 つの SNMP トラップを設定する必要があります。 システムに SNMP サーバとの統合が含まれる場合にだけこのサービスを有効にします。
SSH	このサービスは、ポート 22 でイネーブルになります。これはディセーブルにできず、デフォルトのポートを変更することもできません。 このサービスは Cisco UCS Manager CLI へのアクセスを提供します。

通信サービス	説明
Telnet	デフォルトでは、このサービスは無効になっています。 このサービスは Cisco UCS Manager CLI へのアクセスを提供します。

CIM XML の設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope services**	システム サービス モードを開始します。
ステップ 3	UCS-A /system/services # **enable cimxml**	CIM XLM サービスをイネーブルにします。
ステップ 4	UCS-A /system/services # **set cimxml port** *port-num*	CIM XML 接続のポートを指定します。
ステップ 5	UCS-A /system/services # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、CIM XML をイネーブルにし、ポート番号を 5988 に設定し、トランザクションをコミットする例を示します。

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # enable cimxml
UCS-A /system/services* # set cimxml port 5988
UCS-A /system/services* # commit-buffer
UCS-A /system/services #
```

HTTP の設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /system # **scope services**	システム サービス モードを開始します。
ステップ 3	UCS-A /system/services # **enable http**	HTTP サービスをイネーブルにします。
ステップ 4	UCS-A /system/services # **set http port** *port-num*	HTTP 接続で使用されるポートを指定します。
ステップ 5	UCS-A /system/services # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、HTTP をイネーブルにし、ポート番号を 80 に設定し、トランザクションをコミットします。

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # enable http
UCS-A /system/services* # set http port 80
Warning: When committed, this closes all the web sessions.
UCS-A /system/services* # commit-buffer
UCS-A /system/services #
```

HTTP の設定解除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope services**	システム サービス モードを開始します。
ステップ 3	UCS-A /system/services # **disable http**	HTTP サービスをディセーブルにします。
ステップ 4	UCS-A /system/services # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、HTTP をディセーブルにし、トランザクションをコミットする例を示します。

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # disable http
UCS-A /system/services* # commit-buffer
UCS-A /system/services #
```

HTTPS の設定

証明書、キー リング、トラスト ポイント

HTTPS は、公開キー インフラストラクチャ（PKI）のコンポーネントを使用してクライアントのブラウザと Cisco UCS Manager などの 2 つのデバイス間でセキュアな通信を確立します。

暗号キーとキー リング

各 PKI デバイスは、内部キー リングに非対称の Rivest-Shamir-Adleman（RSA）暗号キーのペア（1 つはプライベート、もう 1 つはパブリック）を保持します。いずれかのキーで暗号化されたメッセージは、もう一方のキーで復号化できます。暗号化されたメッセージを送信する場合、送信者は受信者の公開キーで暗号化し、受信者は独自の秘密キーを使用してメッセージを復号化します。送信者は、独自の秘密キーで既知のメッセージを暗号化（「署名」とも呼ばれます）して公開キーの所有者を証明することもできます。受信者が該当する公開キーを使用してメッセージを正常に復号化できる場合は、送信者が対応する秘密キーを所有していることが証明されます。暗号キーの長さはさまざまであり、通常の長さは 512 ビット ～ 2048 ビットです。一般的に、短いキーよりも長いキーの方がセキュアになります。Cisco UCS Manager では、最初に 1024 ビットのキー ペアを含むデフォルトのキー リングが提供されます。そして、追加のキー リングを作成できます。

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

この操作は、UCS Manager CLI のみで使用できます。

証明書

セキュアな通信を準備するには、まず2つのデバイスがそれぞれのデジタル証明書を交換します。証明書は、デバイスの ID に関する署名済み情報とともにデバイスの公開キーを含むファイルです。暗号化された通信をサポートするために、デバイスは独自のキー ペアと独自の自己署名証明書を生成できます。リモート ユーザが自己署名証明書を提示するデバイスに接続する場合、ユーザはデバイスの ID を簡単に検証することができず、ユーザのブラウザは最初に認証に関する警告を表示します。デフォルトでは、Cisco UCS Manager にはデフォルトのキー リングからの公開キーを含む組み込みの自己署名証明書が含まれます。

トラスト ポイント

Cisco UCS Manager に強力な認証を提供するために、デバイスの ID を証明する信頼できるソース（つまり、トラスト ポイント）からサードパーティ証明書を取得し、インストールできます。サードパーティ証明書は、発行元トラスト ポイント（ルート認証局（CA）、中間 CA、またはルート CA につながるトラスト チェーンの一部となるトラスト アンカーのいずれか）によって署名されます。新しい証明書を取得するには、Cisco UCS Manager で証明書要求を生成し、トラスト ポイントに要求を送信する必要があります。

重要　証明書は、Base64 エンコード X.509（CER）フォーマットである必要があります。

キー リングの作成

Cisco UCS Manager は、デフォルト キー リングを含め、最大 8 個のキー リングをサポートします。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scopesecurity**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **createkeyring** *keyring-name*	キー リングを作成し、名前を指定します。
ステップ 3	UCS-A /security/keyring # **setmodulus** {**mod1024** | **mod1536** | **mod2048** | **mod512**}	SSL キーのビット長を設定します。
ステップ 4	UCS-A /security/keyring # **commit-buffer**	トランザクションをコミットします。

次の例では、1024 ビットのキー サイズのキー リングを作成します。

```
UCS-A# scope security
UCS-A /security # create keyring kr220
UCS-A /security/keyring* # set modulus mod1024
UCS-A /security/keyring* # commit-buffer
UCS-A /security/keyring #
```

次の作業

このキー リングの証明書要求を作成します。

デフォルト キー リングの再生成

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

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scopesecurity**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scopekeyring default**	デフォルト キー リングでキー リング セキュリティ モードを開始します。
ステップ 3	UCS-A /security/keyring # **setregenerate yes**	デフォルトキーリングを再生成します。
ステップ 4	UCS-A /security/keyring # **commit-buffer**	トランザクションをコミットします。

次に、デフォルト キー リングを再生成する例を示します。

```
UCS-A# scope security
UCS-A /security # scope keyring default
UCS-A /security/keyring* # set regenerate yes
UCS-A /security/keyring* # commit-buffer
UCS-A /security/keyring #
```

キー リングの証明書要求の作成

基本オプション付きのキー リングの証明書要求の作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope keyring** *keyring-name*	キー リングのコンフィギュレーション モードに入ります。
ステップ 3	UCS-A /security/keyring # **create certreq** {**ip** [*ipv4-addr* | *ipv6-v6*] |**subject-name** *name*}	指定された IPv4 または IPv6 アドレス、またはファブリック インターコネクトの名前を使用して証明書要求を作成します。証明書要求のパスワードを入力するように求められます。
ステップ 4	UCS-A /security/keyring/certreq # **commit-buffer**	トランザクションをコミットします。
ステップ 5	UCS-A /security/keyring # **show certreq**	コピーしてトラストアンカーまたは認証局に送信可能な証明書要求を表示します。

次の例では、基本オプション付きのキー リングについてIPv4アドレスで証明書要求を作成して表示します。

```
UCS-A# scope security
UCS-A /security # scope keyring kr220
UCS-A /security/keyring # create certreq ip 192.168.200.123 subject-name sjc04
Certificate request password:
Confirm certificate request password:
UCS-A /security/keyring* # commit-buffer
UCS-A /security/keyring # show certreq
Certificate request subject name: sjc04
Certificate request ip address: 192.168.200.123
Certificate request e-mail name:
Certificate request country name:
State, province or county (full name):
Locality (eg, city):
Organization name (eg, company):
Organization Unit name (eg, section):
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIIBfTCB5wIBADARMQ8wDQYDVQQDEwZzYW1jMDQwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALpKn1t8qMZO4UGqILKFXQQc2c8b/vW2rnRF8OPhKbhghLA1YZ1F
JqcYEG5Yl1+vgohLBTd45s0GC8m4RTLJWHo4SwccAUXQ5Zngf45YtX1WsylwUWV4
0re/zgTk/WCd56RfOBvWR2Dtztu2pGA14sd761zLxt29K7R8mzj6CAUVAgMBAAGg
LTArBgkqhkiG9w0BCQ4xHjAcMBoGA1UdEQEB/wQQMA6CBnNhbWMwNIcECsEiXjAN
BgkqhkiG9w0BAQQFAAOBgQCsxN0qUHYGFoQw56RwQueLTNPnrndqUwuZHUO03Teg
nhsyu4satpyiPqVV9viKZ+spvc6x5PWIcTWgHhH8BimOb/0OKuG8kwfIGGsEDlAv
TTYvUP+BZ9OFiPbRIA718S+V8ndXr1HejiQGxlDNqoN+odCXPc5kjoXD0lZTL09H
BA==
-----END CERTIFICATE REQUEST-----

UCS-A /security/keyring #
```

詳細オプション付きのキー リングの証明書要求の作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scopesecurity**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scopekeyring** *keyring-name*	キー リングのコンフィギュレーション モードに入ります。
ステップ 3	UCS-A /security/keyring # **createcertreq**	証明書要求を作成します。
ステップ 4	UCS-A /security/keyring/certreq* # **set country** *country name*	会社が存在している国の国コードを指定します。
ステップ 5	UCS-A /security/keyring/certreq* # **set dns** *DNS Name*	要求に関連付けられたドメイン ネーム サーバ（DNS）アドレスを指定します。
ステップ 6	UCS-A /security/keyring/certreq* # **set e-mail** *E-mail name*	証明書要求に関連付けられた電子メール アドレスを指定します。

	コマンドまたはアクション	目的
ステップ 7	UCS-A /security/keyring/certreq* # **set ip** {*certificate request ip-address*|*certificate request ip6-address* }	ファブリック インターコネクトの IP アドレスを指定します。
ステップ 8	UCS-A /security/keyring/certreq* # **set locality** *locality name (eg, city)*	証明書を要求している会社の本社が存在する市または町を指定します。
ステップ 9	UCS-A /security/keyring/certreq* # **set org-name** *organization name*	証明書を要求している組織を指定します。
ステップ 10	UCS-A /security/keyring/certreq* # **set org-unit-name** *organizational unit name*	組織ユニットを指定します。
ステップ 11	UCS-A /security/keyring/certreq* # **set password** *certificate request password*	証明書要求に関するオプションのパスワードを指定します。
ステップ 12	UCS-A /security/keyring/certreq* # **set state** *state, province or county*	証明書を要求している会社の本社が存在する州または行政区分を指定します。
ステップ 13	UCS-A /security/keyring/certreq* # **set subject-name** *certificate request name*	ファブリック インターコネクトの完全修飾ドメイン名を指定します。
ステップ 14	UCS-A /security/keyring/certreq* # **commit-buffer**	トランザクションをコミットします。
ステップ 15	UCS-A /security/keyring # **showcertreq**	コピーしてトラスト アンカーまたは認証局に送信可能な証明書要求を表示します。

次の例では、詳細オプション付きのキー リングについてIPv4アドレスで証明書要求を作成して表示します。

```
UCS-A# scope security
UCS-A /security # scope keyring kr220
UCS-A /security/keyring # create certreq
UCS-A /security/keyring/certreq* # set ip 192.168.200.123
UCS-A /security/keyring/certreq* #  set subject-name sjc04
UCS-A /security/keyring/certreq* # set country US
UCS-A /security/keyring/certreq* # set dns bg1-samc-15A
UCS-A /security/keyring/certreq* # set email test@cisco.com
UCS-A /security/keyring/certreq* # set locality new york city
UCS-A /security/keyring/certreq* # set org-name "Cisco Systems"
UCS-A /security/keyring/certreq* # set org-unit-name Testing
UCS-A /security/keyring/certreq* # set state new york
UCS-A /security/keyring/certreq* # commit-buffer
UCS-A /security/keyring/certreq # show certreq
Certificate request subject name: sjc04
Certificate request ip address: 192.168.200.123
Certificate request e-mail name: test@cisco.com
Certificate request country name: US
State, province or county (full name): New York
Locality name (eg, city): new york city
Organization name (eg, company): Cisco
Organization Unit name (eg, section): Testing
Request:
```

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBfTCB5wIBADARMQ8wDQYDVQQDEwZzYW1jMDQwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALpKn1t8qMZO4UGqILKFXQQc2c8b/vW2rnRF8OPhKbhghLA1YZ1F
JqcYEG5Yl1+vgohLBTd45s0GC8m4RTLJWHo4SwccAUXQ5Zngf45YtX1WsylwUWV4
0re/zgTk/WCd56RfOBvWR2Dtztu2pGA14sd761zLxt29K7R8mzj6CAUVAgMBAAGg
LTArBgkqhkiG9w0BCQ4xHjAcMBoGA1UdEQEB/wQQMA6CBnNhbWMwNIcECsEiXjAN
BgkqhkiG9w0BAQQFAAOBgQCsxN0qUHYGFoQw56RwQueLTNPnrndqUwuZHUO03Teg
nhsyu4satpyiPqVV9viKZ+spvc6x5PWIcTWgHhH8BimOb/0OKuG8kwfIGGsEDlAv
TTYvUP+BZ9OFiPbRIA718S+V8ndXr1HejiQGxlDNqoN+odCXPc5kjoXD0lZTL09H
BA==
-----END CERTIFICATE REQUEST-----

UCS-A /security/keyring/certreq #
```

次の作業

- 証明書要求のテキストを BEGIN および END 行を含めてコピーし、ファイルに保存します。キー リングの証明書を取得するため、証明書要求を含むファイルをトラスト アンカーまたは認証局に送信します。
- トラスト ポイントを作成し、トラスト アンカーから受け取ったトラストの証明書の証明書チェーンを設定します。

トラスト ポイントの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scopesecurity**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **createtrustpoint** *name*	トラスト ポイントを作成し、その名前を指定します。
ステップ 3	UCS-A /security/trustpoint # **set certchain** [*certchain*]	このトラストポイントの証明書情報を指定します。 コマンドで証明書情報を指定しない場合、ルート認証局（CA）への認証パスを定義するトラスト ポイントのリストまたは証明書を入力するように求められます。入力内容の次の行に、「ENDOFBUF」と入力して終了します。 **重要** 証明書は、Base64 エンコード X.509（CER）フォーマットである必要があります。
ステップ 4	UCS-A /security/trustpoint # **commit-buffer**	トランザクションをコミットします。

次の例は、トラスト ポイントを作成し、トラスト ポイントに証明書を提供します。

```
UCS-A# scope security
UCS-A /security # create trustpoint tPoint10
UCS-A /security/trustpoint* # set certchain
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
```

```
Trustpoint Certificate Chain:
> -----BEGIN CERTIFICATE-----
> MIIDMDCCApmgAwIBAgIBADANBgkqhkiG9w0BAQQFADB0MQswCQYDVQQGEwJVUzEL
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
> jtcEMyZ+f7+3yh421ido3nO4MIGeBgNVHSMEgZYwgZOAFLlNjtcEMyZ+f7+3yh42
> 1ido3nO4oXikdjB0MQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExFDASBgNVBAcT
> C1NhbnRhIENsYXJhMRswGQYDVQQKExJOdW92YSBTeXN0ZW1zIEluYy4xFDASBgNV
> BAsTC0VuZ2luZWVyaW5nMQ8wDQYDVQQDEwZ0ZXN0Q0GCAQAwDAYDVR0TBAUwAwEB
> /zANBgkqhkiG9w0BAQQFAAOBgQAhWaRwXNR6B4g6Lsnr+fptHv+WVhB5fKqGQqXc
> wR4pYiO4z42/j9Ijenh75tCKMhW51az8copP1EBmOcyuhf5C6vasrenn1ddkkYt4
> PR0vxGc40whuiozBolesmsmjBbedUCwQgdFDWhDIZJwK5+N3x/kfa2EHU6id1avt
> 4YL5Jg==
> -----END CERTIFICATE-----
> ENDOFBUF
UCS-A /security/trustpoint* # commit-buffer
UCS-A /security/trustpoint #
```

次の作業

トラスト アンカーまたは認証局からキー リング証明書を取得し、キー リングにインポートします。

キー リングへの証明書のインポート

はじめる前に

- キー リング証明書の証明書チェーンを含むトラスト ポイントを設定します。
- トラスト アンカーまたは認証局からキー リング証明書を取得します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scopesecurity**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scopekeyring** *keyring-name*	証明書を受け取るキー リングでコンフィギュレーション モードを開始します。
ステップ 3	UCS-A /security/keyring # **settrustpoint** *name*	キー リング証明書の取得元のトラスト アンカーまたは認証局に対しトラストポイントを指定します。
ステップ 4	UCS-A /security/keyring # **setcert**	キーリング証明書を入力してアップロードするためのダイアログを起動します。 プロンプトで、トラストアンカーまたは認証局から受け取った証明書のテキストを貼り付けます。証明

	コマンドまたはアクション	目的
		書の後の行に「ENDOFBUF」と入力して、証明書の入力を完了します。 **重要** 証明書は、Base64 エンコード X.509（CER）フォーマットである必要があります。
ステップ 5	UCS-A /security/keyring # **commit-buffer**	トランザクションをコミットします。

次に、トラストポイントを指定し、証明書をキー リングにインポートする例を示します。

```
UCS-A# scope security
UCS-A /security # scope keyring kr220
UCS-A /security/keyring # set trustpoint tPoint10
UCS-A /security/keyring* # set cert
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Keyring certificate:
> -----BEGIN CERTIFICATE-----
> MIIB/zCCAWgCAQAwgZkxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEVMBMGA1UE
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
> mK3Ku+YiORnv6DhxrOoqau8r/hyI/L43l7IPN1HhOi3oha4=
> -----END CERTIFICATE-----
> ENDOFBUF
UCS-A /security/keyring* # commit-buffer
UCS-A /security/keyring #
```

次の作業

キー リングを使用して HTTPS サービスを設定します。

HTTPS の設定

⚠

注意 HTTPS で使用するポートとキー リングの変更を含め、HTTPS の設定を完了した後、トランザクションを保存またはコミットするとすぐに、現在のすべての HTTP および HTTPS セッションは警告なく閉じられます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope services**	システム サービス モードを開始します。
ステップ 3	UCS-A /system/services # **enable https**	HTTPS サービスをイネーブルにします。
ステップ 4	UCS-A /system/services # **set https port** *port-num*	（任意） HTTPS 接続で使用されるポートを指定します。
ステップ 5	UCS-A /system/services # **set https keyring** *keyring-name*	（任意） HTTPS に対して作成したキー リングの名前を指定します。
ステップ 6	UCS-A /system/services # **set https cipher-suite-mode** *cipher-suite-mode*	（任意） Cisco UCS ドメイン で使用される暗号スイート セキュリティのレベル。*cipher-suite-mode* には、次のいずれかのキーワードを指定できます。 • **high-strength** • **medium-strength** • **low-strength** • **custom**：ユーザ定義の暗号スイート仕様の文字列を指定できます。
ステップ 7	UCS-A /system/services # **set https cipher-suite** *cipher-suite-spec-string*	（任意） **cipher-suite-mode** が **custom**. に設定されている場合は、この Cisco UCS ドメイン にカスタム レベルの暗号スイート セキュリティを指定します。 *cipher-suite-spec-string* 最大 256 文字まで使用できますが、OpenSSL 暗号スイート仕様に準拠する必要があります。次を除き、スペースや特殊文字は使用できません。!（感嘆符）、+（プラス記号）、-（ハイフン）、および:（コロン）。詳細については、http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuite を参照してください。. たとえば、Cisco UCS Manager がデフォルトとして使用する中強度仕様の文字列は次のようになります。 ALL:!ADH:!EXPORT56:!LOW:RC4+RSA:+HIGH:+MEDIUM:+EXP:+eNULL

	コマンドまたはアクション	目的
		（注） このオプションは、**cipher-suite-mode** が **custom**以外に設定されている場合は無視されます。
ステップ **8**	UCS-A /system/services # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、HTTPS を有効にし、ポート番号を 443 に設定し、キー リング名を kring7984 に設定し、暗号スイートのセキュリティ レベルを高に設定し、トランザクションをコミットします。

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # enable https
UCS-A /system/services* # set https port 443
Warning: When committed, this closes all the web sessions.
UCS-A /system/services* # set https keyring kring7984
UCS-A /system/services* # set https cipher-suite-mode high
UCS-A /system/services* # commit-buffer
UCS-A /system/services #
```

キーリングの削除

手順

	コマンドまたはアクション	目的
ステップ **1**	UCS-A# **scopesecurity**	セキュリティ モードを開始します。
ステップ **2**	UCS-A /security # **deletekeyring** *name*	名前付きのキー リングを削除します。
ステップ **3**	UCS-A /security # **commit-buffer**	トランザクションをコミットします。

次の例では、キー リングを削除します。

```
UCS-A# scope security
UCS-A /security # delete keyring key10
UCS-A /security* # commit-buffer
UCS-A /security #
```

トラスト ポイントの削除

はじめる前に

トラスト ポイントがキー リングによって使用されていないことを確認してください。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scopesecurity**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **deletetrustpoint** *name*	指定したトラスト ポイントを削除します。
ステップ 3	UCS-A /security # **commit-buffer**	トランザクションをコミットします。

次に、トラスト ポイントを削除する例を示します。

```
UCS-A# scope security
UCS-A /security # delete trustpoint tPoint10
UCS-A /security* # commit-buffer
UCS-A /security #
```

HTTPS の設定解除

はじめる前に

HTTP から HTTPS へのリダイレクションをディセーブルにします。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope services**	システム サービス モードを開始します。
ステップ 3	UCS-A /system/services # **disable https**	HTTPS サービスをディセーブルにします。
ステップ 4	UCS-A /system/services # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、HTTPS を無効にし、トランザクションをコミットする例を示します。

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # disable https
UCS-A /system/services* # commit-buffer
UCS-A /system/services #
```

HTTPS への HTTP リダイレクションの有効化

はじめる前に

HTTP と HTTPS の両方をイネーブルにします。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope services**	システム サービス モードを開始します。
ステップ 3	UCS-A /system/services # **enable http-redirect**	HTTP リダイレクト サービスをイネーブルにします。 イネーブルの場合、HTTP 経由で試行される通信はすべて同等の HTTPS アドレスにリダイレクトされます。 このオプションは、この Cisco UCS ドメインへの HTTP アクセスを実質的にディセーブルにします。
ステップ 4	UCS-A /system/services # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、HTTP から HTTPS へのリダイレクションをイネーブルにし、トランザクションをコミットする例を示します。

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # enable http-redirect
Warning: When committed, this closes all the web sessions.
UCS-A /system/services* # commit-buffer
UCS-A /system/services #
```

SNMP 機能の概要

SNMP フレームワークは 3 つの部分で構成されます。

- SNMP マネージャ：SNMP を使用してネットワーク デバイスのアクティビティを制御し、モニタリングするシステム
- SNMP エージェント：管理対象デバイスである Cisco UCS 内のソフトウェア コンポーネント。Cisco UCS のデータを保守し、必要に応じてそのデータを SNMP マネージャに報告します。Cisco UCS には、エージェントと、MIB のコレクションが組み込まれています。SNMP

エージェントを有効にし、マネージャとエージェント間のリレーションシップを作成するには、Cisco UCS Manager で SNMP を有効にし、設定します。

- 管理情報ベース（MIB）：SNMP エージェント上の管理対象オブジェクトのコレクション。Cisco UCS リリース 1.4(1) 以降では、以前よりも多くの MIB をサポートしています。

Cisco UCS では SNMPv1、SNMPv2c、および SNMPv3 がサポートされます。SNMPv1 および SNMPv2c はどちらも、コミュニティベース形式のセキュリティを使用します。SNMP は次のように定義されています。

- RFC 3410（http://tools.ietf.org/html/rfc3410）
- RFC 3411（http://tools.ietf.org/html/rfc3411）
- RFC 3412（http://tools.ietf.org/html/rfc3412）
- RFC 3413（http://tools.ietf.org/html/rfc3413）
- RFC 3414（http://tools.ietf.org/html/rfc3414）
- RFC 3415（http://tools.ietf.org/html/rfc3415）
- RFC 3416（http://tools.ietf.org/html/rfc3416）
- RFC 3417（http://tools.ietf.org/html/rfc3417）
- RFC 3418（http://tools.ietf.org/html/rfc3418）
- RFC 3584（http://tools.ietf.org/html/rfc3584）

SNMP 通知

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

Cisco UCS Manager は、トラップまたはインフォームとして SNMP 通知を生成します。SNMP マネージャはトラップ受信時に確認応答を送信せず、Cisco UCS Manager はトラップが受信されたかどうかを確認できないため、トラップの信頼性はインフォームよりも低くなります。インフォーム要求を受信する SNMP マネージャは、SNMP 応答プロトコル データ ユニット（PDU）でメッセージの受信を確認応答します。Cisco UCS Manager が PDU を受信しない場合、インフォーム要求を再送できます。

SNMP セキュリティ レベルおよび権限

SNMPv1、SNMPv2c、および SNMPv3 はそれぞれ別のセキュリティ モデルを表します。セキュリティ モデルと選択したセキュリティ レベルの組み合わせにより、SNMP メッセージの処理中に適用されるセキュリティ メカニズムが決まります。

セキュリティ レベルは、SNMP トラップに関連付けられているメッセージを表示するために必要な特権を決定します。権限のレベルによって、メッセージが情報開示の保護を必要とするか、またはメッセージが認証されるかが決定されます。サポートされるセキュリティ レベルは、実装されているセキュリティ モデルによって異なります。SNMP セキュリティ レベルは、次の権限の 1 つ以上をサポートします。

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

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

SNMP セキュリティ モデルとレベルのサポートされている組み合わせ

次の表に、セキュリティ モデルとレベルの組み合わせを示します。

表 *6*：*SNMP* セキュリティ モデルおよびセキュリティ レベル

モデル	水準器	認証	暗号化	結果
v1	noAuthNoPriv	コミュニティ ストリング	なし	コミュニティ ストリングの照合を使用して認証します。
v2c	noAuthNoPriv	コミュニティ ストリング	なし	コミュニティ ストリングの照合を使用して認証します。
v3	noAuthNoPriv	ユーザ名	なし	ユーザ名の照合を使用して認証します。

モデル	水準器	認証	暗号化	結果
v3	authNoPriv	HMAC-MD5 または HMAC-SHA	なし	Hash-Based Message Authentication Code（HMAC）メッセージダイジェスト 5（MD5）アルゴリズムまたは HMAC セキュア ハッシュ アルゴリズム（SHA）アルゴリズムに基づいて認証します。
v3	authPriv	HMAC-MD5 または HMAC-SHA	DES	HMAC-MD5 アルゴリズムまたは HMAC-SHA アルゴリズムに基づいて認証します。データ暗号規格（DES）の 56 ビット暗号化、および暗号ブロック連鎖（CBC）DES（DES-56）標準に基づいた認証を提供します。

SNMPv3 セキュリティ機能

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

- メッセージの完全性：メッセージが不正な方法で変更または破壊されていないこと、データシーケンスが悪意なく起こり得る範囲を超えて変更されていないことを保証します。
- メッセージの発信元の認証：メッセージ送信者の ID を確認できることを保証します。
- メッセージの機密性および暗号化：不正なユーザ、エンティティ、プロセスに対して情報を利用不可にしたり開示しないようにします。

Cisco UCS での SNMP サポート

Cisco UCS は、SNMP に対して以下のサポートを備えています。

MIB のサポート

Cisco UCS は、MIB への読み取り専用アクセスをサポートします。

Cisco UCS で使用可能な特定の MIB およびその入手先については、B シリーズ サーバは http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/mib/b-series/b_UCS_MIBRef.html を、C シリーズは http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/mib/c-series/b_UCS_Standalone_C-Series_MIBRef.html を参照してください。

SNMPv3 ユーザの認証プロトコル

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

- HMAC-MD5-96（MD5）
- HMAC-SHA-96（SHA）

SNMPv3 ユーザの AES プライバシー プロトコル

Cisco UCS は、SNMPv3 メッセージ暗号化用のプライバシー プロトコルの 1 つとして Advanced Encryption Standard（AES）を使用し、RFC 3826 に準拠しています。

プライバシー パスワード（priv オプション）では、SNMP セキュリティ暗号化方式として DES または 128 ビット AES を選択できます。AES-128 設定を有効にし、SNMPv3 ユーザのプライバシー パスワードをインクルードした場合、Cisco UCS Manager はプライバシー パスワードを使用して 128 ビット AES キーを生成します。AES priv パスワードは、8 文字以上にします。パスフレーズをクリア テキストで指定する場合、最大 64 文字を指定できます。

SNMP の有効化および SNMP プロパティの設定

Cisco UCS ドメインからの SNMP メッセージには、システム名ではなくファブリック インターコネクト名が表示されます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニタリング モードを開始します。
ステップ 2	UCS-A /monitoring # **enable snmp**	SNMP をイネーブルにします。
ステップ 3	UCS-A /monitoring # **set snmp community**	snmp コミュニティ モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	UCS-A /monitoring # **Enter a snmp community:** *community-name*	SNMP コミュニティを指定します。パスワードとしてコミュニティ名を使用します。コミュニティ名は、最大 32 文字の英数字で指定できます。
ステップ 5	UCS-A /monitoring # **set snmp syscontact** *system-contact-name*	SNMP 担当者のシステムの連絡先を指定します。システム担当者の連絡先名（電子メールアドレスや、名前と電話番号など）は、最大 255 文字の英数字で指定できます。
ステップ 6	UCS-A /monitoring # **set snmp syslocation** *system-location-name*	SNMP エージェント（サーバ）が実行するホストの場所を指定します。システム ロケーション名は、最大 512 文字の英数字で指定できます。
ステップ 7	UCS-A /monitoring # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、SNMP を有効にし、SnmpCommSystem2 という名前の SNMP コミュニティを設定し、contactperson という名前のシステム連絡先を設定し、systemlocation という名前の連絡先ロケーションを設定し、トランザクションをコミットする例を示します。

```
UCS-A# scope monitoring
UCS-A /monitoring # enable snmp
UCS-A /monitoring* # set snmp community
UCS-A /monitoring* # Enter a snmp community: SnmpCommSystem2
UCS-A /monitoring* # set snmp syscontact contactperson1
UCS-A /monitoring* # set snmp syslocation systemlocation
UCS-A /monitoring* # commit-buffer
UCS-A /monitoring #
```

次の作業

SNMP トラップおよびユーザを作成します。

SNMP トラップの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニタリング モードを開始します。
ステップ 2	UCS-A /monitoring # **enable snmp**	SNMP をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /monitoring # **create snmp-trap** {*hostname* | *ip-addr* | *ip6-addr*}	指定したホスト名、IPv4 アドレス、または IPv6 アドレスで SNMP トラップ ホストを作成します。 ホスト名は IPv4 アドレスの完全修飾ドメイン名にすることができます。
ステップ 4	UCS-A /monitoring/snmp-trap # **set community** *community-name*	SNMP トラップに使用する SNMP コミュニティ名を指定します。
ステップ 5	UCS-A /monitoring/snmp-trap # **set port** *port-num*	SNMP トラップに使用するポートを指定します。
ステップ 6	UCS-A /monitoring/snmp-trap # **set version** {**v1** | **v2c** | **v3**}	トラップに使用する SNMP のバージョンとモデルを指定します。
ステップ 7	UCS-A /monitoring/snmp-trap # **set notification type** {**traps** | **informs**}	（任意） 送信するトラップのタイプ。ここに表示される値は次のとおりです。 • バージョンに [v2c] または [v3] を選択する場合は **traps**。 • バージョンに [v2c] を選択する場合は **informs**。 （注） バージョンとして [v2c] を選択した場合にのみインフォーム通知を送信できます。
ステップ 8	UCS-A /monitoring/snmp-trap # **set v3 privilege** {**auth** | **noauth** | **priv**}	（任意） バージョンとして[v3]を選択した場合に、トラップに関連付ける権限。 ここに表示される値は次のとおりです。 • [auth]：認証あり、暗号化なし • [noauth]：認証なし、暗号化なし • [priv]：認証あり、暗号化あり
ステップ 9	UCS-A /monitoring/snmp-trap # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、SNMP を使用可能にし、IPv4 アドレスを使用して SNMP トラップを作成し、トラップがポート 2 で SnmpCommSystem2 コミュニティを使用するよう指定し、バージョンを v3 に設定し、通知タイプを traps に設定し、v3 権限を priv に設定し、トランザクションを確定します。

```
UCS-A# scope monitoring
UCS-A /monitoring # enable snmp
UCS-A /monitoring* # create snmp-trap 192.168.100.112
UCS-A /monitoring/snmp-trap* # set community SnmpCommSystem2
UCS-A /monitoring/snmp-trap* # set port 2
UCS-A /monitoring/snmp-trap* # set version v3
UCS-A /monitoring/snmp-trap* # set notificationtype traps
UCS-A /monitoring/snmp-trap* # set v3 privilege priv
UCS-A /monitoring/snmp-trap* # commit-buffer
UCS-A /monitoring/snmp-trap #
```

次の例は、SNMP を使用可能にし、IPv6 アドレスを使用して SNMP トラップを作成し、トラップがポート 2 で SnmpCommSystem3 コミュニティを使用するよう指定し、バージョンを v3 に設定し、通知タイプを traps に設定し、v3 権限を priv に設定し、トランザクションを確定します。

```
UCS-A# scope monitoring
UCS-A /monitoring # enable snmp
UCS-A /monitoring* # create snmp-trap  2001::1
UCS-A /monitoring/snmp-trap* # set community SnmpCommSystem3
UCS-A /monitoring/snmp-trap* # set port 2
UCS-A /monitoring/snmp-trap* # set version v3
UCS-A /monitoring/snmp-trap* # set notificationtype traps
UCS-A /monitoring/snmp-trap* # set v3 privilege priv
UCS-A /monitoring/snmp-trap* # commit-buffer
UCS-A /monitoring/snmp-trap #
```

SNMP トラップの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニタリング モードを開始します。
ステップ 2	UCS-A /monitoring # **delete snmp-trap** {*hostname* | *ip-addr*}	指定したホスト名または IP アドレスの指定した SNMP トラップ ホストを削除します。
ステップ 3	UCS-A /monitoring # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、IP アドレス 192.168.100.112 で SNMP トラップを削除し、トランザクションを確定する例を示します。

```
UCS-A# scope monitoring
UCS-A /monitoring # delete snmp-trap 192.168.100.112
UCS-A /monitoring* # commit-buffer
UCS-A /monitoring #
```

SNMPv3 ユーザの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニタリング モードを開始します。
ステップ 2	UCS-A /monitoring # **enable snmp**	SNMP をイネーブルにします。
ステップ 3	UCS-A /monitoring # **create snmp-user** *user-name*	指定された SNMPv3 ユーザを作成します。 SNMP ユーザ名は、ローカル ユーザ名と同じにはできません。ローカル ユーザ名と一致しない SNMP ユーザ名を選択します。
ステップ 4	UCS-A /monitoring/snmp-user # **set aes-128** {**no** | **yes**}	AES-128 暗号化の使用をイネーブルまたはディセーブルにします。
ステップ 5	UCS-A /monitoring/snmp-user # **set auth** {**md5** | **sha**}	MD5 または DHA 認証の使用を指定します。
ステップ 6	UCS-A /monitoring/snmp-user # **set password**	ユーザ パスワードを指定します。**set password** コマンドの入力後、パスワードの入力と確認を求められます。
ステップ 7	UCS-A /monitoring/snmp-user # **set priv-password**	ユーザ プライバシー パスワードを指定します。**set priv-password** コマンドを入力すると、プライバシー パスワードを入力し、確認するように求められます。
ステップ 8	UCS-A /monitoring/snmp-user # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、SNMP をイネーブルにし、snmp-user14 という名前の SNMPv3 ユーザを作成し、AES-128 暗号化をディセーブルにし、MD5 認証の使用を指定し、パスワードおよびプライバシー パスワードを設定し、トランザクションをコミットします。

```
UCS-A# scope monitoring
UCS-A /monitoring # enable snmp
UCS-A /monitoring* # create snmp-user snmp-user14
UCS-A /monitoring/snmp-user* # set aes-128 no
UCS-A /monitoring/snmp-user* # set auth md5
UCS-A /monitoring/snmp-user* # set password
Enter a password:
Confirm the password:
UCS-A /monitoring/snmp-user* # set priv-password
Enter a password:
Confirm the password:
UCS-A /monitoring/snmp-user* # commit-buffer
UCS-A /monitoring/snmp-user #
```

SNMPv3 ユーザの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニタリング モードを開始します。
ステップ 2	UCS-A /monitoring # **delete snmp-user** *user-name*	指定した SNMPv3 ユーザを削除します。
ステップ 3	UCS-A /monitoring # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、snmp-user14 という SNMPv3 ユーザを削除し、トランザクションを確定する例を示します。

```
UCS-A# scope monitoring
UCS-A /monitoring # delete snmp-user snmp-user14
UCS-A /monitoring* # commit-buffer
UCS-A /monitoring #
```

Telnet のイネーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope services**	システム サービス モードを開始します。
ステップ 3	UCS-A /services # **enable telnet-server**	Telnet サービスをイネーブルにします。
ステップ 4	UCS-A /services # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、Telnet を有効にし、トランザクションを確定する例を示します。

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /services # enable telnet-server
UCS-A /services* # commit-buffer
UCS-A /services #
```

CIMC Web サービスのイネーブル化

CIMC Web サービスをイネーブルにするには：

- admin 権限でログインする必要があります。
- CIMC Web サービスは、デフォルトではイネーブルなので、ディセーブルにする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system** /	システム モードを開始します。
ステップ 2	UCS-A /system #**scope services**/	システムのサービス モードを開始します。
ステップ 3	UCS-A/system/services #**enable cimcwebsvc**/	CIMC Web サービスをイネーブルにします。
ステップ 4	UCS-A/system/services *# **commit-buffer**/	トランザクションをシステム設定にコミットします。

次に、CIMC Web サービスをイネーブルにし、トランザクションを保存する例を示します。

```
UCS-A# scope system
UCS-A/system # scope services
UCS-A/system/services # enable cimcwebsvc
UCS-A/system/services *# commit-buffer
UCS-A/system/services # commit-buffer
UCS-A/system/services # show cimcwebsvc
Name: cimcwebservice
    Admin State: Enabled
```

CIMC Web サービスのディセーブル化

CIMC Web サービスをディセーブルにするには：

- admin 権限でログインする必要があります。
- CIMC Web サービスをイネーブルにする必要があります。

（注） CIMC Web サービスはデフォルトでイネーブルとなっています。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system** /	システム モードを開始します。
ステップ 2	UCS-A /system #**scope services**/	システムのサービス モードを開始します。
ステップ 3	UCS-A/system/services #**disable cimcwebsvc**/	CIMC Web サービスをディセーブルにします。
ステップ 4	UCS-A/system/services *# **commit-buffer**/	トランザクションをシステム設定にコミットします。

次に、CIMC Web サービスをディセーブルにし、トランザクションを保存する例を示します。

```
UCS-A# scope system
UCS-A/system # scope services
UCS-A/system/services # disable cimcwebsvc
UCS-A/system/services *# commit-buffer
UCS-A/system/services # commit-buffer
UCS-A/system/services # show cimcwebsvc
Name: cimcwebservice
    Admin State: Disabled
```

通信サービスのディセーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope services**	システム サービス モードを開始します。
ステップ 3	UCS-A /system/services # **disable** *service-name*	指定したサービスを無効にします。ここで *service-name* 引数は次のいずれかのキーワードです。 • *cimxml*：CIM XML サービスを無効にします • **http**：HTTP サービスを無効にします • **https**：HTTPS サービスを無効にします • **telnet-server**：Telnet サービスを無効にします

	コマンドまたはアクション	目的
ステップ 4	UCS-A /system/services # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、CIM XML をディセーブルにし、トランザクションをコミットする例を示します。

```
UCS-A# scope system
UCS-A# scope services
UCS-A /system/services # disable cimxml
UCS-A /system/services* # commit-buffer
UCS-A /system/services #
```

第 9 章

認証の設定

この章の内容は、次のとおりです。

認証サービス

Cisco UCS では、ユーザ ログインを認証するための次の 2 つの方法をサポートしています。

- ローカル ユーザ認証：ローカルの Cisco UCS Manager に存在するユーザ アカウントを使用します。
- リモート ユーザ認証：次のプロトコルのいずれかを使用します。
  - LDAP
  - RADIUS

◦ TACACS+

リモート認証プロバイダーに関する注意事項および推奨事項

システムを、サポートされているリモート認証サービスのいずれかに設定する場合は、そのサービス用のプロバイダーを作成して、Cisco UCS Managerがそのシステムと通信できるようにする必要があります。ユーザ認証に影響する注意事項は次のとおりです。

リモート認証サービスのユーザ アカウント

ユーザ アカウントは、Cisco UCS Manager にローカルに存在するか、またはリモート認証サーバに存在することができます。

リモート認証サービスを介してログインしているユーザの一時的なセッションは、Cisco UCS Manager GUI と Cisco UCS Manager CLI で表示できます。

リモート認証サービスのユーザ ロール

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

リモート認証プロバイダーのユーザ属性

RADIUS および TACACS+ 構成では、ユーザが Cisco UCS Manager へのログインに使用する各リモート認証プロバイダーに Cisco UCS 用のユーザ属性を設定する必要があります。このユーザ属性には、各ユーザに割り当てられたロールとロケールが含まれています。

（注） この手順は、LDAP グループ マッピングを使用してロールとロケールを割り当てる LDAP 設定では必要ありません。

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

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

次の表は、Cisco UCS でサポートしているリモート認証プロバイダーのユーザ属性要件を比較したものです。

表 7: リモート認証プロバイダーによるユーザ属性の比較

認証プロバイダー	カスタム属性	スキーマの拡張	属性 ID 要件
LDAP	グループ マッピング使用時は不要 グループ マッピング不使用時は任意	これはオプションです。次のいずれかを実行するように選択できます。 • LDAP スキーマを拡張せず、要件を満たす既存の未使用の属性を設定します。 • LDAP スキーマを拡張して、CiscoAVPair などの一意の名前でカスタム属性を作成します。	シスコの LDAP の実装では、Unicode タイプの属性が必要です。 CiscoAVPair カスタム属性を作成する場合は、属性 ID として 1.3.6.1.4.1.9.287247.1 を使用します 次の項で、サンプルOIDを示します。
RADIUS	オプション	これはオプションです。次のいずれかを実行するように選択できます。 • RADIUS スキーマを拡張せず、要件を満たす既存の未使用属性を使用します。 • RADIUS スキーマを拡張して、cisco-avpair などの一意の名前でカスタム属性を作成します。	シスコによる RADIUS の実装のベンダー ID は 009 であり、属性のベンダー ID は 001 です。 次の構文例は、cisco-avpair 属性を作成する場合に複数のユーザ ロールとロケールを指定する方法を示しています。`shell:roles="admin,aaa"` `shell:locales="L1,abc"`。複数の値を区切るには、区切り文字としてカンマ「,」を使用します。

認証プロバイダー	カスタム属性	スキーマの拡張	属性 ID 要件
TACACS+	必須	必須作業です。スキーマを拡張し、cisco-av-pair という名前のカスタム属性を作成する必要があります。	cisco-av-pair 名は、TACACS+ プロバイダーの属性 ID を提供する文字列です。 次の構文例は、cisco-av-pair 属性を作成するときに複数のユーザロールとロケールを指定する方法を示しています。 `cisco-av-pair=shell:roles="admin aaa" shell:locales*"L1 abc"`。 cisco-av-pair 属性構文でアスタリスク（*）を使用すると、ロケールがオプションとして指定され、同じ認可プロファイルを使用する他のシスコデバイスで認証の失敗を防ぐことができます。複数の値を区切るには、区切り文字としてスペースを使用します。

LDAP ユーザ属性のサンプル OID

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

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

二要素認証

Cisco UCS Manager では、リモート ユーザのログインに二要素認証を使用して、アカウントのログインのセキュリティ レベルを高めています。二要素認証のログインでは、パスワードフィール

ドでユーザ名、トークン、パスワードの組み合わせが必要です。PIN、証明書、またはトークンを指定できます。

二要素認証では、認証アプリケーションを使用します。このアプリケーションはトークン サーバを保持して、ログイン プロセス中にユーザ用のワンタイム トークンを生成し、パスワードを AAA サーバに保存します。ベンダー固有の属性を取得するために、リクエストがトークン サーバに送信されます。Cisco UCS Manager は、トークン サーバがリクエストを AAA サーバに転送できるように、トークン サーバを AAA サーバと統合することを要求します。パスワードとトークンは、AAA サーバによって同時に検証されます。ユーザは、AAA サーバで設定されているのと同じ順序で、トークンとパスワードを入力する必要があります。

二要素認証は、RADIUS または TACACS+ プロバイダー グループを指定認証ドメインに関連付け、それらのドメインで二要素認証を有効にすることによってサポートされます。二要素認証では IPM をサポートしておらず、また認証レルムが LDAP、local、または none に設定されている場合はサポートされません。

Web セッションの更新および Web セッションのタイムアウト期限

[Web セッションの更新期間（Web Session Refresh Period）] は、Cisco UCS Manager GUI の Web セッションに対する更新要求間隔に許容される最大時間です。[Web セッションのタイムアウト（Web Session Timeout）] は、最後の更新要求後から Cisco UCS Manager GUI の Web セッションが非アクティブになるまでの最大経過時間です。

[Web セッションの更新期間（Web Session Refresh Period）] を 60 秒より長く、最大で 172800 秒まで長くすると、トークンとパスワードを繰り返し生成および再入力する必要があるセッション タイムアウトが頻繁に起きるのを避けることができます。デフォルト値は、二要素認証がイネーブルの場合は 7200 秒、二要素認証がイネーブルでない場合は 600 秒です。

[Web セッションのタイムアウト期間（Web Session Timeout Period）] には 300 から 172800 の間の値を指定できます。デフォルト値は、二要素認証がイネーブルの場合は 8000 秒、二要素認証がイネーブルでない場合は 7200 秒です。

LDAP グループ ルール

LDAP グループ ルールによって、ユーザ ロールおよびロケールをリモート ユーザに割り当てるときに Cisco UCS が LDAP グループを使用するかどうかが決まります。

ネストされた LDAP グループ

LDAP グループを他のグループおよびネスト グループのメンバーとして追加し、メンバー アカウントを統合してトラフィックの重複を減らすことができます。Cisco UCS Manager のリリース 2.1(2) 以降では、LDAP グループ マップで定義された他のグループ内にネストされた LDAP グループを検索できます。

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

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

Cisco UCS Manager のグループ マップでサブグループを常に作成する必要がなくなります。

LDAP プロバイダーの設定

LDAP プロバイダーのプロパティの設定

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

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

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope ldap**	セキュリティ LDAP モードを開始します。
ステップ 3	UCS-A /security/ldap # **set attribute** *attribute*	指定された属性を含むレコードにデータベース検索を限定します。
ステップ 4	UCS-A /security/ldap # **set basedn** *distinguished-name*	指定された識別名を含むレコードにデータベース検索を限定します。
ステップ 5	UCS-A /security/ldap # **set filter** *filter*	指定されたフィルタを含むレコードにデータベース検索を限定します。

	コマンドまたはアクション	目的
ステップ 6	UCS-A /security/ldap # **set timeout** *seconds*	（任意） システムがサーバをダウン状態として通知する前に、LDAP サーバからの応答を待つ時間間隔を設定します。
ステップ 7	UCS-A /security/ldap # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、LDAP 属性を CiscoAvPair に、ベース識別名を「DC=cisco-ucsm-aaa3,DC=qalab,DC=com」に、フィルタを sAMAccountName=$userid、タイムアウト間隔を 5 秒に設定し、トランザクションを確定します。

```
UCS-A# scope security
UCS-A /security # scope ldap
UCS-A /security/ldap # set attribute CiscoAvPair
UCS-A /security/ldap* # set basedn "DC=cisco-ucsm-aaa3,DC=qalab,DC=com"
UCS-A /security/ldap* # set filter sAMAccountName=$userid
UCS-A /security/ldap* # set timeout 5
UCS-A /security/ldap* # commit-buffer
UCS-A /security/ldap #
```

（注） ユーザ ログインは LDAP ユーザの userdn が 255 文字を超えると失敗します。

次の作業

LDAP プロバイダーを作成します。

LDAP プロバイダーの作成

Cisco UCS Manager は、最大 16 の LDAP プロバイダーと最大 128 のグループをサポートします。

はじめる前に

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

- LDAP サーバで、次のいずれかの設定を行います。
  - LDAP グループを設定します。LDAP グループには、ユーザのロールとロケール情報が含まれています。
  - Cisco UCS Manager のユーザ ロールとロケール情報を保持する属性をユーザに対して設定します。この属性について LDAP スキーマを拡張するかどうかを選択できます。スキーマを拡張しない場合は、既存の LDAP 属性を使用して Cisco UCS ユーザ ロールと

ロケールを保持します。スキーマを拡張する場合は、CiscoAVPair 属性などのカスタム属性を作成します。

シスコの LDAP の実装では、Unicode タイプの属性が必要です。

CiscoAVPair カスタム属性を作成する場合は、属性 ID として 1.3.6.1.4.1.9.287247.1 を使用します

- クラスタ設定では、両方のファブリック インターコネクトに対する管理ポートの IPv4 または IPv6 アドレスを追加します。この設定では、1 つめのファブリック インターコネクトで障害が発生し、システムが 2 つめのファブリック インターコネクトにフェールオーバーしても、リモート ユーザは引き続きログインできることが保証されます。ログイン要求はすべて、これらの IP アドレスから送信されます。Cisco UCS Manager により使用されている仮想 IPv4 または IPv6 アドレスではありません。

- セキュアな通信を使用する場合は、LDAP サーバのルート認証局（CA）の証明書が格納されたトラスト ポイントを Cisco UCS Manager で作成します。

- LDAP プロバイダーを変更したり、追加または削除したりする必要がある場合は、ドメイン認証レルムをローカルに変更し、プロバイダーに変更を加えた後、ドメイン認証レルムを LDAP に戻す必要があります。

- Active Directory バインド識別名の属性を定義する際に次の表にある特殊文字を使用する場合、対応する文字の 16 進数値の後にバックスラッシュ（\）を使用して、特殊文字をエスケープ文字で置き換える必要があります。

特殊文字	説明	16 進数値
,	カンマ	0x2C
+	プラス記号	0x2B
"	二重引用符	0x22
\	バックスラッシュ	0x5C
<	左角ブラケット	0x3C
>	右角ブラケット	0x3E
;	セミコロン	0x3B
LF	改行	0x0A
CR	行頭復帰（キャリッジリターン）	0x0D
=	等号	0x3D

特殊文字	説明	16 進数値
/	スラッシュ	0x2F

https://msdn.microsoft.com/en-us/library/aa366101 に特殊文字をエスケープ文字と 16 進数値に置き換える方法についての説明があります。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope ldap**	セキュリティ LDAP モードを開始します。
ステップ 3	UCS-A /security/ldap # **create server** *server-name*	LDAP サーバ インスタンスを作成し、セキュリティ LDAP サーバ モードを開始します。SSL が使用可能の場合、*server-name* は、通常 IP アドレスまたは FQDN となり、LDAP サーバのセキュリティ証明書内の共通名（CN）と正確に一致している必要があります。IP アドレスが指定されているのでない限り、DNS サーバは Cisco UCS Manager で設定する必要があります。
ステップ 4	UCS-A /security/ldap/server # **set attribute** *attr-name*	（任意） ユーザ ロールとロケールの値を保管する LDAP 属性。このプロパティは、常に、名前と値のペアで指定されます。システムは、ユーザ レコードで、この属性名と一致する値を検索します。 LDAP スキーマを拡張しない場合は、既存の使用されていない LDAP 属性を Cisco UCS ロールとスケールに設定できます。あるいは、属性 ID「1.3.6.1.4.1.9.287247.1」を持つ、CiscoAVPair という名前の属性をリモート認証サービスに作成できます。 デフォルトの属性が LDAP の [全般（General）] タブで設定されていない場合は、この値が必要です。
ステップ 5	UCS-A /security/ldap/server # **set basedn** *basedn-name*	（任意） リモート ユーザがログインし、システムがそのユーザ名に基づいてユーザの DN の取得を試みるときに、サーバが検索を開始する LDAP 階層内の特定の識別名。ベース DN の長さは、最大 255 文字から CN=username の長さを引いた長さに設定することができます。username により、LDAP 認証を使用して Cisco UCS Manager にアクセスしようとするリモート ユーザが識別されます。

	コマンドまたはアクション	目的
		デフォルトのベース DN が LDAP の [全般（General）] タブで設定されていない場合は、この値が必要です。
ステップ 6	UCS-A /security/ldap/server # **set binddn** *binddn-name*	（任意） ベース DN のすべてのオブジェクトに対する読み取り権限と検索権限を持つ、LDAP データベース アカウントの識別名（DN）。 サポートされるストリングの最大長は 255 文字（ASCII）です。
ステップ 7	UCS-A /security/ldap/server # **set filter** *filter-value*	（任意） LDAP 検索は、定義したフィルタと一致するユーザ名に制限されます。 デフォルトのフィルタが LDAP の [全般（General）] タブで設定されていない場合は、この値が必要です。
ステップ 8	UCS-A /security/ldap/server # **set password**	[バインド DN（Bind DN）] フィールドで指定した LDAP データベース アカウントのパスワード。標準 ASCII 文字を入力できます。ただし、「§」（セクション記号）、「?」（疑問符）、「=」（等号）は使用できません。 パスワードを設定するには、**set password** コマンドを入力し、プロンプトでキー値を入力してから **Enter** キーを押します。
ステップ 9	UCS-A /security/ldap/server # **set order** *order-num*	（任意） Cisco UCS でユーザの認証にこのプロバイダーを使用する順序。
ステップ 10	UCS-A /security/ldap/server # **set port** *port-num*	（任意） Cisco UCS が LDAP データベースと通信するために使用するポート。標準ポート番号は 389 です。
ステップ 11	UCS-A /security/ldap/server # **set ssl** {**yes no**}	LDAP サーバと通信するときの暗号化の使用を有効または無効にします。オプションは次のとおりです。 • **yes**：暗号化が必要です。暗号化をネゴシエートできない場合は、接続に失敗します。 • **no**：暗号化はディセーブルです。認証情報はクリア テキストとして送信されます。 LDAP では STARTTLS が使用されます。これにより、ポート 389 を使用した暗号化通信が可能になります。

	コマンドまたはアクション	目的
ステップ 12	UCS-A /security/ldap/server # **set timeout** *timeout-num*	LDAP データベースへの問い合わせがタイムアウトするまでの秒数。 1 ～ 60 秒の整数を入力するか、0（ゼロ）を入力して LDAP の [全般（General）] で指定したタイムアウト値を使用します。デフォルトは 30 秒です。
ステップ 13	UCS-A /security/ldap/server # **set vendor** *{ms-ad | openldap}*	LDAP サーバのネストされた LDAP グループ検索機能の使用をイネーブルまたはディセーブルにします。オプションは次のとおりです。 • **ms-ad**：ネストされた LDAP グループ検索は、このオプションでサポートされます。ベンダーを *ms-ad*（Microsoft Active Directory）に設定し、*ldap-group-rule* を有効にして recursive に設定すると、Cisco UCS Manager はネストされた LDAP グループを検索できます。 • **openldap**：ネストされた LDAP グループ検索は、このオプションでサポートされません。ベンダーを *openldap* に設定し、*ldap-group-rule* を有効にして recursive に設定すると、Cisco UCS Manager はネストされた LDAP グループを検索しません。このオプションを選択すると、親グループがグループ マップにすでに設定されていても、Cisco UCS Manager で LDAP グループ マップとして各 LDAP サブグループを作成する必要があります。 （注） Cisco UCS Manager を旧バージョンからリリース 2.1(2) にアップグレードすると、LDAP プロバイダーのベンダー属性は **openldap** にデフォルトで設定され、LDAP 認証が正常に機能し続けます。
ステップ 14	UCS-A /security/ldap/server # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、10.193.169.246 という名前の LDAP サーバインスタンスを作成し、バインド DN、パスワード、順序、ポート、SSL、ベンダー属性を設定し、トランザクションを確定します。

```
UCS-A# scope security
UCS-A /security # scope ldap
UCS-A /security/ldap* # create server 10.193.169.246
UCS-A /security/ldap/server* # set binddn
"cn=Administrator,cn=Users,DC=cisco-ucsm-aaa3,DC=qalab,DC=com"
UCS-A /security/ldap/server* # set password
Enter the password:
Confirm the password:
UCS-A /security/ldap/server* # set order 2
UCS-A /security/ldap/server* # set port 389
```

```
UCS-A /security/ldap/server* # set ssl yes
UCS-A /security/ldap/server* # set timeout 30
UCS-A /security/ldap/server* # set vendor ms-ad
UCS-A /security/ldap/server* # commit-buffer
UCS-A /security/ldap/server #
```

次の例では、12:31:71:1231:45b1:0011:011:900 という名前の LDAP サーバインスタンスを作成し、バインドDN、パスワード、順序、ポート、SSL、ベンダー属性を設定し、トランザクションを確定します。

```
UCS-A# scope security
UCS-A /security # scope ldap
UCS-A /security/ldap* # create server 12:31:71:1231:45b1:0011:011:900
UCS-A /security/ldap/server* # set binddn
"cn=Administrator,cn=Users,DC=cisco-ucsm-aaa3,DC=qalab,DC=com"
UCS-A /security/ldap/server* # set password
Enter the password:
Confirm the password:
UCS-A /security/ldap/server* # set order 1
UCS-A /security/ldap/server* # set port 389
UCS-A /security/ldap/server* # set ssl yes
UCS-A /security/ldap/server* # set timeout 45
UCS-A /security/ldap/server* # set vendor ms-ad
UCS-A /security/ldap/server* # commit-buffer
UCS-A /security/ldap/server #
```

次の作業

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

複数の LDAP データベースが関係する実装の場合は、LDAP プロバイダー グループを設定します。

LDAP プロバイダーの LDAP グループ ルールの変更

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope ldap**	セキュリティ LDAP モードを開始します。
ステップ 3	UCS-A /security/ldap # **scope server** *ldap-provider*	セキュリティ LDAP プロバイダー モードを開始します。
ステップ 4	UCS-A /security/ldap/server # **scope ldap-group-rule**	LDAP グループ ルール モードを開始します。
ステップ 5	UCS-A /security/ldap/server/ldap-group-rule # **set authorization** {**enable** | **disable**}	ユーザ ロールとロケールをリモート ユーザに割り当てるときに、Cisco UCS が LDAP グループを検索するかを指定します。 • [disable]：Cisco UCS はどの LDAP グループにもアクセスしません。

	コマンドまたはアクション	目的
		• [enable]：Cisco UCS は、この Cisco UCS ドメイン 内にマップされている LDAP プロバイダー グループを検索します。リモート ユーザが見つかると、Cisco UCS は関連する LDAP グループ マップでその LDAP グループに対して定義されているユーザ ロールとロケールを割り当てます。 （注） ロールとロケールの割り当ては累積されます。ユーザが複数のグループに含まれる、または LDAP 属性で指定されたロールやロケールがある場合、Cisco UCS はそのユーザに対し、それらのグループや属性のいずれかにマッピングされたすべてのロールとロケールを割り当てます。
ステップ 6	UCS-A /security/ldap/server/ldap-group-rule # **set member-of-attribute** *attr-name*	Cisco UCS が LDAP データベースのグループ メンバーシップを決定するのに使用する属性。 サポートされるストリングの長さは 63 文字です。デフォルトの文字列は「memberOf」です。
ステップ 7	UCS-A /security/ldap/server/ldap-group-rule # **set traversal** {**non-recursive** | **recursive**}	必要に応じて Cisco UCS がグループ メンバの親グループの設定を使用するかどうか指定します。ここに表示される値は次のとおりです。 • [non-recursive]：Cisco UCS はユーザが属するグループだけを検索します。 • [recursive]：Cisco UCS はユーザが属する継承元グループすべてを検索します。
ステップ 8	UCS-A /security/ldap/server/ldap-group-rule # **set use-primary-group** {**yes** | **no**}	プライマリ グループをメンバーシップの検証のために Cisco UCS ドメイン 内の LDAP グループ マップとして設定します。Cisco UCS Manager を有効にして、ユーザのプライマリ グループ メンバーシップをダウンロードして検証することができます。
ステップ 9	UCS-A /security/ldap/server/ldap-group-rule # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、権限をイネーブルにする LDAP グループ ルールを設定し、属性のメンバを memberOf に設定し、traversal を non-recursive に設定し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope ldap
UCS-A /security/ldap # scope server ldapprovider
UCS-A /security/ldap/server # scope ldap-group-rule
UCS-A /security/ldap/server/ldap-group-rule # set authorization enable
UCS-A /security/ldap/server/ldap-group-rule* # set member-of-attribute memberOf
UCS-A /security/ldap/server/ldap-group-rule* # set traversal non-recursive
UCS-A /security/ldap/server/ldap-group-rule* # set use-primary-group yes
UCS-A /security/ldap/server/ldap-group-rule* # commit-buffer
UCS-A /security/ldap/server/ldap-group-rule #
```

LDAP プロバイダーの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope ldap**	セキュリティ LDAP モードを開始します。
ステップ 3	UCS-A /security/ldap # **delete server** *serv-name*	指定したサーバを削除します。
ステップ 4	UCS-A /security/ldap # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、ldap1 という LDAP サーバを削除し、トランザクションを確定する例を示します。

```
UCS-A# scope security
UCS-A /security # scope ldap
UCS-A /security/ldap # delete server ldap1
UCS-A /security/ldap* # commit-buffer
UCS-A /security/ldap #
```

LDAP グループ マッピング

LDAP グループ マッピングにより、LDAP ユーザ オブジェクトのロールまたはロケール情報を定義する必要がなくなります。LDAP データベースへのアクセスを制限する LDAP グループを使用している組織にログインする際、UCSM はグループ メンバーシップ情報を使用してロールとロケールを LDAP ユーザに割り当てます。

ユーザが Cisco UCS Manager にログインする際、LDAP グループ マップはユーザのロールとロケールに関する情報を取り出します。ロールとロケールの基準がポリシー情報と一致する場合は、アクセスが許可されます。

Cisco UCS Manager でローカルに設定したロールとロケール定義に対しては、LDAP ディレクトリに対する変更に基づいた自動更新は行われません。LDAP ディレクトリ内の LDAP グループの削除や名前変更を行う場合は、その変更に合わせて Cisco UCS Manager も更新する必要があります。

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

- ロールのみ
- ロケールのみ
- ロールとロケールの両方

たとえば、特定の場所のサーバ管理者グループを表す LDAP グループがあるとします。LDAP グループ マップには、サーバ プロファイルやサーバ機器などのユーザ ロールが含まれていることもあります。特定の場所のサーバ管理者へのアクセスを制限するために、ロケールに特定のサイト名を設定することができます。

（注） Cisco UCS Manager にはすぐに使用できるユーザ ロールが含まれていますが、ロケールは含まれていません。LDAP プロバイダー グループをロケールにマッピングするには、カスタム ロケールを作成する必要があります。

LDAP グループ マップの作成

はじめる前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope ldap**	セキュリティ LDAP モードを開始します。
ステップ 3	UCS-A /security/ldap # **create ldap-group** *group-dn*	指定した DN 用の LDAP グループ マップを作成します。 グループ DN の最大文字数は 240 です。

	コマンドまたはアクション	目的
		（注） このコマンドに特殊文字を入力する場合は、特殊文字の前にエスケープ文字 \\（バックスラッシュ 2 個）を付ける必要があります。
ステップ 4	UCS-A /security/ldap/ldap-group # **create locale** *locale-name*	指定されたロケールに LDAP グループをマッピングします。
ステップ 5	UCS-A /security/ldap/ldap-group # **create role** *role-name*	指定されたロールに LDAP グループをマッピングします。
ステップ 6	UCS-A /security/ldap/ldap-group # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、DN に LDAP グループをマッピングし、ロケールを pacific に設定し、ロールを admin に設定し、トランザクションをコミットする例を示します。

```
UCS-A# scope security
UCS-A /security # scope ldap
UCS-A /security/ldap # create ldap-group cn=security,cn=users,dc=lab,dc=com
UCS-A /security/ldap/ldap-group* # create locale pacific
UCS-A /security/ldap/ldap-group* # create role admin
UCS-A /security/ldap/ldap-group* # commit-buffer
UCS-A /security/ldap/ldap-group #
```

次の作業

LDAP グループ ルールを設定します。

LDAP グループ マップの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope ldap**	セキュリティ LDAP モードを開始します。
ステップ 3	UCS-A /security/ldap # **delete ldap-group** *group-dn*	指定した DN 用の LDAP グループ マップを削除します。
ステップ 4	UCS-A /security/ldap # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、LDAP グループ マップを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope security
UCS-A /security # scope ldap
UCS-A /security/ldap # delete ldap-group cn=security,cn=users,dc=lab,dc=com
UCS-A /security/ldap* # commit-buffer
UCS-A /security/ldap #
```

RADIUS プロバイダーの設定

RADIUS プロバイダーのプロパティの設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope radius**	セキュリティ RADIUS モードを開始します。
ステップ 3	UCS-A /security/radius # **set retries** *retry-num*	（任意） サーバをダウンとして通知する前に RADIUS サーバとの通信を再試行する回数を設定します。
ステップ 4	UCS-A /security/radius # **set timeout** *seconds*	（任意） システムがサーバをダウン状態として通知する前に、RADIUS サーバからの応答を待つ時間間隔を設定します。
ステップ 5	UCS-A /security/radius # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、RADIUS の再試行回数を 4 に設定し、タイムアウト間隔を 30 秒に設定し、トランザクションを確定します。

```
UCS-A# scope security
UCS-A /security # scope radius
UCS-A /security/radius # set retries 4
UCS-A /security/radius* # set timeout 30
UCS-A /security/radius* # commit-buffer
UCS-A /security/radius #
```

次の作業

RADIUS プロバイダーを作成します。

RADIUS プロバイダーの作成

Cisco UCS Manager では、最大 16 の RADIUS プロバイダーがサポートされます。

はじめる前に

RADIUS サーバで、次の設定を行います。

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

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

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

- クラスタ設定では、両方のファブリック インターコネクトに対する管理ポートの IPv4 またはIPv6アドレスを追加します。この設定では、1つめのファブリック インターコネクトで障害が発生し、システムが 2 つめのファブリック インターコネクトにフェールオーバーしても、リモート ユーザは引き続きログインできることが保証されます。ログイン要求はすべて、これらの IP アドレスから送信されます。Cisco UCS Manager により使用されている仮想 IP アドレスではありません。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope radius**	セキュリティ RADIUS モードを開始します。
ステップ 3	UCS-A /security/radius # **create server** *server-name*	RADIUS サーバ インスタンスを作成し、セキュリティ RADIUS サーバ モードを開始します
ステップ 4	UCS-A /security/radius/server # **set authport** *authport-num*	（任意） RADIUS サーバとの通信に使用するポートを指定します。
ステップ 5	UCS-A /security/radius/server # **set key**	RADIUS サーバ キーを設定します。キー値を設定するには、**set key** コマンドを入力し、プロンプトでキー値を入力してから **Enter** キーを押します。
ステップ 6	UCS-A /security/radius/server # **set order** *order-num*	（任意） このサーバが試行される順序を指定します。

	コマンドまたはアクション	目的
ステップ 7	UCS-A /security/radius/server # **set retries** *retry-num*	（任意） サーバをダウンとして通知する前に RADIUS サーバとの通信を再試行する回数を設定します。
ステップ 8	UCS-A /security/radius/server # **set timeout** *seconds*	（任意） システムがサーバをダウン状態として通知する前に、RADIUS サーバからの応答を待つ時間間隔を設定します。 **ヒント** RADIUS プロバイダーに二要素認証を選択する場合は、より高いタイムアウト値を設定することを推奨します。
ステップ 9	UCS-A /security/radius/server # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、radiusserv7 という名前のサーバインスタンスを作成し、認証ポートを 5858 に設定し、キーを radiuskey321 に設定し、順序を 2 に設定し、再試行回数を 4 回に設定し、タイムアウトを 30 に設定し、二要素認証を有効にし、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope radius
UCS-A /security/radius # create server radiusserv7
UCS-A /security/radius/server* # set authport 5858
UCS-A /security/radius/server* # set key
Enter the key: radiuskey321
Confirm the key: radiuskey321
UCS-A /security/radius/server* # set order 2
UCS-A /security/radius/server* # set retries 4
UCS-A /security/radius/server* # set timeout 30
UCS-A /security/radius/server* # commit-buffer
UCS-A /security/radius/server #
```

次の作業

単一の RADIUS データベースが関係する実装の場合は、RADIUS をプライマリ認証サービスとして選択します。

複数の RADIUS データベースが関係する実装の場合は、RADIUS プロバイダー グループを設定します。

RADIUS プロバイダーの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope RADIUS**	セキュリティ RADIUS モードを開始します。
ステップ 3	UCS-A /security/radius # **delete server** *serv-name*	指定したサーバを削除します。
ステップ 4	UCS-A /security/radius # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、radius1 という RADIUS サーバを削除し、トランザクションを確定する例を示します。

```
UCS-A# scope security
UCS-A /security # scope radius
UCS-A /security/radius # delete server radius1
UCS-A /security/radius* # commit-buffer
UCS-A /security/radius #
```

TACACS+ プロバイダーの設定

TACACS+ プロバイダーのプロパティの設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope tacacs**	セキュリティ TACACS+ モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /security/tacacs # **set timeout** *seconds*	（任意） システムがサーバをダウン状態として通知する前に、TACACS+ サーバからの応答を待つ時間間隔を設定します。
ステップ 4	UCS-A /security/tacacs # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、TACACS+ タイムアウト間隔を 45 秒に設定し、トランザクションを確定する例を示します。

```
UCS-A# scope security
UCS-A /security # scope tacacs
UCS-A /security/tacacs # set timeout 45
UCS-A /security/tacacs* # commit-buffer
UCS-A /security/tacacs #
```

次の作業

TACACS+ プロバイダーを作成します。

TACACS+ プロバイダーの作成

Cisco UCS Manager では、最大 16 の TACACS+ プロバイダーがサポートされます。

はじめる前に

TACACS+ サーバで、次の設定を行います。

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

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

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

- クラスタ設定では、両方のファブリック インターコネクトに対する管理ポートの IPv4 または IPv6 アドレスを追加します。この設定では、1 つめのファブリック インターコネクトで障害が発生し、システムが 2 つめのファブリック インターコネクトにフェールオーバーしても、リモート ユーザは引き続きログインできることが保証されます。ログイン要求はすべて、これらの IP アドレスから送信されます。Cisco UCS Manager により使用されている仮想 IP アドレスではありません。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope tacacs**	セキュリティ TACACS+ モードを開始します。
ステップ 3	UCS-A /security/tacacs # **create server** *server-name*	TACACS+サーバインスタンスを作成し、セキュリティ TACACS+ サーバ モードを開始します
ステップ 4	UCS-A /security/tacacs/server # **set key**	（任意） TACACS+ サーバ キーを設定します。キー値を設定するには、**set key** コマンドを入力し、プロンプトでキー値を入力してから **Enter** キーを押します。
ステップ 5	UCS-A /security/tacacs/server # **set order** *order-num*	（任意） このサーバが試行される順序を指定します。
ステップ 6	UCS-A /security/tacacs/server # **set timeout***seconds*	（任意） システムがサーバをダウン状態として通知する前に、TACACS+ サーバからの応答を待つ時間間隔を設定します。 **ヒント** TACACS+ プロバイダーに二要素認証を選択する場合は、より高いタイムアウト値を設定することを推奨します。
ステップ 7	UCS-A /security/tacacs/server # **set port** *port-num*	TACACS+ サーバとの通信に使用するポートを指定します。
ステップ 8	UCS-A /security/tacacs/server # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、tacacsserv680 という名前のサーバ インスタンスを作成し、キーを tacacskey321 に設定してそのキーを確認し、順序を 4 に設定し、認証ポートを 5859 に設定し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope tacacs
UCS-A /security/tacacs # create server tacacsserv680
UCS-A /security/tacacs/server* # set key
Enter the key: tacacskey321
Confirm the key: tacacskey321
UCS-A /security/tacacs/server* # set order 4
UCS-A /security/tacacs/server* # set port 5859
UCS-A /security/tacacs/server* # commit-buffer
UCS-A /security/tacacs/server #
```

次の作業

単一の TACACS+ データベースが関係する実装の場合は、TACACS+ をプライマリ認証サービスとして選択します。

複数の TACACS+ データベースが関係する実装の場合は、TACACS+ プロバイダー グループを設定します。

TACACS+ プロバイダーの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope tacacs**	セキュリティ TACACS モードを開始します。
ステップ 3	UCS-A /security/tacacs # **delete server** *serv-name*	指定したサーバを削除します。
ステップ 4	UCS-A /security/tacacs # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、tacacs1 という TACACS サーバを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope security
UCS-A /security # scope tacacs
UCS-A /security/tacacs # delete server TACACS1
UCS-A /security/tacacs* # commit-buffer
UCS-A /security/tacacs #
```

マルチ認証システム

マルチ認証サービス

次の機能を実装して、Cisco UCS が複数の認証サービスを使用するよう設定することができます。

- プロバイダー グループ
- 認証ドメイン

プロバイダー グループと認証ドメインが Cisco UCS Manager で設定された後、次の構文を使用してシステムにログインできます。Cisco UCS Manager CLI: **ucs:** *auth-domain\ user-name*

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

（注） SSH ログインでは大文字と小文字が区別されます。

Linux 端末からは以下の SSH を使用します。

- **sshucs-***auth-domain**username*@{*UCSM-ip-address*|*UCMS-ipv6-address*}

```
ssh ucs-example\\jsmith@192.0.20.11
ssh ucs-example\\jsmith@2001::1
```

- **ssh -lucs-***auth-domain**username* {*UCSM-ip-address*| *UCSM-ipv6-address*| *UCSM-host-name*}

```
ssh -l ucs-example\\jsmith 192.0.20.11
ssh -l ucs-example\\jsmith 2001::1
```

- **ssh** {*UCSM-ip-address* | *UCSM-ipv6-address* | *UCSM-host-name*} **-lucs-***auth-domain**username*

```
ssh 192.0.20.11 -l ucs-example\\jsmith
ssh 2001::1 -l ucs-example\\jsmith
```

- **sshucs-***auth-domain**username*@{*UCSM-ip-address*|*UCSM-ipv6-address*}

```
ssh ucs-ldap23\\jsmith@192.0.20.11
ssh ucs-ldap23\\jsmith@2001::1
```

Linux 端末からは以下の Telnet を使用します。

- **telnet ucs-***UCSM-host-name* **ucs-***auth-domain**username*

```
telnet ucs-qa-10
login: ucs-ldap23\blradmin
```

- **telnetucs-**{*UCSM-ip-address*|*UCSM-ipv6-address*}*ucs-auth-domain**username*

```
telnet 10.106.19.12 2052
ucs-qa-10-A login: ucs-ldap23\blradmin
```

Putty クライアントからは、次の手順を実行します。

- **ucs-***auth-domain**username* でログインします。

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

（注） デフォルトの認証がローカルに設定されており、コンソール認証が LDAP に設定されている場合は、ucs-local\admin（admin はローカルアカウントの名前）を使用して Putty クライアントからファブリック インターコネクトにログインできます。

マルチ認証システム

プロバイダー グループ

プロバイダー グループは、認証プロセス中に Cisco UCS がアクセスするプロバイダーのセットです。プロバイダー グループ内のすべてのプロバイダーが、ユーザの認証に Cisco UCS プロバイダーが使用する順にアクセスされます。設定されたすべてのサーバが使用できない場合、または到達不能な場合、Cisco UCS Manager は、ローカル ユーザ名とパスワードを使用して自動的にローカル認証方式にフォールバックします。

Cisco UCS Manager では、グループごとに最大 8 個のプロバイダーが許可された、最大 16 個のプロバイダー グループを作成できます。

LDAP プロバイダー グループの作成

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

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

はじめる前に

1 つ以上の LDAP プロバイダーを作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope ldap**	セキュリティ LDAP モードを開始します。
ステップ 3	UCS-A /security/ldap # **create auth-server-group** *auth-server-group-name*	LDAP プロバイダー グループを作成し、認証サーバ グループの LDAP セキュリティ モードを開始します。
ステップ 4	UCS-A /security/ldap/auth-server-group # **create server-ref** *ldap-provider-name*	指定された LDAP プロバイダーを LDAP プロバイダー グループに追加し、サーバ参照認証サーバ グループの LDAP セキュリティ モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	UCS-A /security/ldap/auth-server-group/server-ref # **set order** *order-num*	Cisco UCS がこのプロバイダーをユーザの認証に使用する順序を指定します。 有効な値には no-value と 0 ～ 16 が含まれ、値が小さいほど優先度が高いことを示します。順序を no-value に指定することは、そのサーバ参照の優先度を最高にするのと同じです。
ステップ 6	UCS-A /security/ldap/auth-server-group/server-ref # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、ldapgroup という名前の LDAP プロバイダー グループを作成し、プロバイダー グループに ldap1 および ldap2 という 2 種類の事前設定されたプロバイダーを追加し、順序を設定し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope ldap
UCS-A /security/ldap # create auth-server-group ldapgroup
UCS-A /security/ldap/auth-server-group* # create server-ref ldap1
UCS-A /security/ldap/auth-server-group/server-ref* # set order 1
UCS-A /security/ldap/auth-server-group/server-ref* # up
UCS-A /security/ldap/auth-server-group* # create server-ref ldap2
UCS-A /security/ldap/auth-server-group/server-ref* # set order 2
UCS-A /security/ldap/auth-server-group/server-ref* # commit-buffer
UCS-A /security/ldap/auth-server-group/server-ref #
```

次の作業

認証ドメインを設定するか、デフォルト認証サービスを選択します。

LDAP プロバイダー グループの削除

はじめる前に

認証設定からプロバイダー グループを削除します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope ldap**	セキュリティ LDAP モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /security/ldap # **delete auth-server-group** *auth-server-group-name*	LDAP プロバイダー グループを削除します。
ステップ 4	UCS-A /security/ldap # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、ldapgroup という名前の LDAP プロバイダー グループを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope security
UCS-A /security # scope ldap
UCS-A /security/ldap # delete auth-server-group ldapgroup
UCS-A /security/ldap* # commit-buffer
UCS-A /security/ldap #
```

RADIUS プロバイダー グループの作成

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

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

はじめる前に

1 つ以上の RADIUS プロバイダーを作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope radius**	セキュリティ RADIUS モードを開始します。
ステップ 3	UCS-A /security/radius # **create auth-server-group** *auth-server-group-name*	RADIUS プロバイダー グループを作成し、認証サーバ グループの RADIUS セキュリティ モードを開始します。
ステップ 4	UCS-A /security/RADIUS/auth-server-group # **create server-ref** *radius-provider-name*	指定された RADIUS プロバイダーを RADIUS プロバイダー グループに追加し、サーバ参照認証サーバ グループの RADIUS セキュリティ モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	UCS-A /security/radius/auth-server-group/server-ref # **set order** *order-num*	Cisco UCS がこのプロバイダーをユーザの認証に使用する順序を指定します。 有効な値には no-value と 0 ～ 16 が含まれ、値が小さいほど優先度が高いことを示します。順序を no-value に指定することは、そのサーバ参照の優先度を最高にするのと同じです。
ステップ 6	UCS-A /security/radius/auth-server-group/server-ref # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、radiusgroup という名前の RADIUS プロバイダー グループを作成し、プロバイダー グループに radius1 と radius2 という 2 種類の事前設定されたプロバイダーを追加し、順序を設定し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope radius
UCS-A /security/radius # create auth-server-group radiusgroup
UCS-A /security/radius/auth-server-group* # create server-ref radius1
UCS-A /security/radius/auth-server-group/server-ref* # set order 1
UCS-A /security/radius/auth-server-group/server-ref* # up
UCS-A /security/radius/auth-server-group* # create server-ref radius2
UCS-A /security/radius/auth-server-group/server-ref* # set order 2
UCS-A /security/radius/auth-server-group/server-ref* # commit-buffer
UCS-A /security/radius/auth-server-group/server-ref #
```

次の作業

認証ドメインを設定するか、デフォルト認証サービスを選択します。

RADIUS プロバイダー グループの削除

認証設定からプロバイダー グループを削除します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope radius**	セキュリティ RADIUS モードを開始します。
ステップ 3	UCS-A /security/radius # **delete auth-server-group** *auth-server-group-name*	RADIUS プロバイダー グループを削除します。

	コマンドまたはアクション	目的
ステップ 4	UCS-A /security/radius # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、radiusgroup という RADIUS プロバイダー グループを削除し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope radius
UCS-A /security/radius # delete auth-server-group radiusgroup
UCS-A /security/radius* # commit-buffer
UCS-A /security/radius #
```

TACACS プロバイダー グループの作成

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

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

はじめる前に

TACACS プロバイダーを作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope tacacs**	セキュリティ TACACS モードを開始します。
ステップ 3	UCS-A /security/tacacs # **create auth-server-group** *auth-server-group-name*	TACACS プロバイダー グループを作成し、認証サーバ グループのセキュリティ TACACS モードを開始します。
ステップ 4	UCS-A /security/tacacs/auth-server-group # **create server-ref** *tacacs-provider-name*	指定した TACACS プロバイダーを TACACS プロバイダー グループに追加し、サーバ参照認証サーバ グループ セキュリティ TACACS モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	UCS-A /security/tacacs/auth-server-group/server-ref # **set order** *order-num*	Cisco UCS がこのプロバイダーをユーザの認証に使用する順序を指定します。 有効な値には no-value と 0 ～ 16 が含まれ、値が小さいほど優先度が高いことを示します。順序を no-value に指定することは、そのサーバ参照の優先度を最高にするのと同じです。
ステップ 6	UCS-A /security/tacacs/auth-server-group/server-ref # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、tacacsgroup という名前の TACACS プロバイダー グループを作成し、プロバイダー グループに tacacs1 と tacacs2 という 2 種類の事前設定されたプロバイダーを追加し、順序を設定し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope tacacs
UCS-A /security/tacacs # create auth-server-group tacacsgroup
UCS-A /security/tacacs/auth-server-group* # create server-ref tacacs1
UCS-A /security/tacacs/auth-server-group/server-ref* # set order 1
UCS-A /security/tacacs/auth-server-group/server-ref* # up
UCS-A /security/tacacs/auth-server-group* # create server-ref tacacs2
UCS-A /security/tacacs/auth-server-group/server-ref* # set order 2
UCS-A /security/tacacs/auth-server-group/server-ref* # commit-buffer
UCS-A /security/tacacs/auth-server-group/server-ref #
```

次の作業

認証ドメインを設定するか、デフォルト認証サービスを選択します。

TACACS プロバイダー グループの削除

認証設定からプロバイダー グループを削除します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope tacacs**	セキュリティ TACACS モードを開始します。
ステップ 3	UCS-A /security/tacacs # **delete auth-server-group** *auth-server-group-name*	TACACS プロバイダー グループを削除します。

	コマンドまたはアクション	目的
ステップ 4	UCS-A /security/tacacs # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、tacacsgroup という TACACS プロバイダー グループを削除し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope tacacs
UCS-A /security/tacacs # delete auth-server-group tacacsgroup
UCS-A /security/tacacs* # commit-buffer
UCS-A /security/tacacs #
```

認証ドメイン

Cisco UCS Manager では、複数の認証システムを活用するために認証ドメインを使用しています。各認証ドメインはログイン時に指定および設定できます。これを行わない場合、Cisco UCS Manager はデフォルトの認証サービス設定を使用します。

最大 8 個の認証ドメインを作成できます。各認証ドメインは、Cisco UCS Manager 内のプロバイダー グループと領域に関連付けられています。プロバイダー グループを指定しないと、Cisco UCS Manager では領域内のすべてのサーバを使用します。

認証ドメインの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **create auth-domain** *domain-name*	認証ドメインを作成し、認証ドメイン モードを開始します。 （注） リモート認証プロトコルを使用するシステムの場合、認証ドメイン名はユーザ名の一部と見なされ、ローカルに作成されたユーザ名に対して 32 文字の制限が適用されます。Cisco UCS はフォーマット用に 5 文字を挿入するため、ドメイン名とユーザ名を組み合わせた合計が 27 文字を超えると、認証は失敗します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /security/auth-domain # **set refresh-period** *seconds*	（任意） Cisco UCS Manager に接続している場合、Web クライアントは、Web セッションをアクティブに保つために、Cisco UCS Manager に更新要求を送信する必要があります。このオプションを使用して、このドメインのユーザに許可する更新要求間隔の最大時間数を指定します。 この時間制限を超えると、Cisco UCS Manager は Web セッションを非アクティブであると見なしますが、セッションの終了は行いません。 60 ～ 172800 の範囲内の整数を指定します。デフォルト値は、二要素認証がイネーブルでない場合は 600 秒、二要素認証がイネーブルの場合は 7200 秒です。 （注） [Web セッションの更新期間（Web Session Refresh Period）] に設定する秒数は、[Web セッションのタイムアウト（Web Session Timeout）] に設定する秒数未満である必要があります。[Web セッションの更新期間（Web Session Refresh Period）] に [Web セッションのタイムアウト（Web Session Timeout）] と同じ値を設定しないでください。
ステップ 4	UCS-A /security/auth-domain # **set session-timeout** *seconds*	（任意） 最後の更新要求から Cisco UCS Manager が Web セッションが非アクティブであると見なすまでの最大経過時間。この時間制限を超えた場合、Cisco UCS Manager は自動的に Web セッションを終了します。 300 ～ 172800 の範囲内の整数を指定します。デフォルト値は、二要素認証がイネーブルでない場合は 7200 秒、二要素認証がイネーブルの場合は 8000 秒です。 （注） RADIUS または TACACS+ レルムに対して二要素認証を設定する場合は、リモートユーザが頻繁に再認証する必要がないよう、セッションの更新時間およびセッションのタイムアウト時間を増やすことを検討してください。
ステップ 5	UCS-A /security/auth-domain # **create default-auth**	（任意） 認証ドメインのデフォルト認証を作成します。

	コマンドまたはアクション	目的
ステップ6	UCS-A /security/auth-domain/default-auth # **set auth-server-group** *auth-serv-group-name*	（任意） 認証ドメインのプロバイダー グループを設定します。
ステップ7	UCS-A /security/auth-domain/default-auth # **set realm** {**ldap** | **local** | **radius** | **tacacs**}	認証ドメインのレルムを設定します。
ステップ8	UCS-A /security/auth-domain/default-auth # **set use-2-factor yes**	（任意） 認証方式をレルムの二要素認証に設定します。 （注） 二要素認証は、RADIUS および TACACS+ レルムにのみ適用されます。
ステップ9	UCS-A /security/auth-domain/default-auth # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、Web の更新時間が 3600 秒（1 時間）およびセッションのタイムアウト時間が 14400 秒（4 時間）の domain1 と呼ばれる認証ドメインを作成します。次に、radius1 でプロバイダーを使用するように domain1 を設定し、レルム タイプを radius に設定し、二要素認証を有効にし、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # create auth-domain domain1
UCS-A /security/auth-domain* # set refresh-period 3600
UCS-A /security/auth-domain* # set session-timeout 14400
UCS-A /security/auth-domain* # create default-auth
UCS-A /security/auth-domain/auth-domain* # set auth-server-group radius1
UCS-A /security/auth-domain/auth-domain* # set realm radius
UCS-A /security/auth-domain/auth-domain* # set user-2-factor yes
UCS-A /security/auth-domain/auth-domain* # commit-buffer
UCS-A /security/auth-domain/auth-domain #
```

プライマリ認証サービスの選択

コンソール認証サービスの選択

はじめる前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope console-auth**	コンソール認証セキュリティ モードを開始します。
ステップ 3	UCS-A /security/console-auth # **set realm** *auth-type*	コンソール認証を指定します。*auth-type* 引数は次のいずれかのキーワードです。 • **ldap**：LDAP 認証を指定します • **local**：ローカル認証を指定します • **none**：ローカル ユーザはパスワードを指定せずにログインできます • **radius**：RADIUS 認証を指定します • **tacacs**：TACACS+ 認証を指定します
ステップ 4	UCS-A /security/console-auth # **set auth-server-group** *auth-serv-group-name*	（任意） 関連付けられたプロバイダー グループ（存在する場合）。
ステップ 5	UCS-A /security/default-auth # **set use-2-factor yes**	（任意） 認証方式をレルムの二要素認証に設定します。 （注） 二要素認証は、RADIUS および TACACS+ レルムにのみ適用されます。
ステップ 6	UCS-A /security/console-auth # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、認証レルムを TACACS+ に設定し、コンソール認証プロバイダー グループを provider1 に設定し、二要素認証を有効にし、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope console-auth
UCS-A /security/console-auth # set realm tacacs
UCS-A /security/console-auth # set auth-server-group provider1
UCS-A /security/console-auth* # set use-2-factor yes
UCS-A /security/console-auth* # commit-buffer
UCS-A /security/console-auth #
```

デフォルト認証サービスの選択

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope default-auth**	デフォルト認証セキュリティ モードを開始します。
ステップ 3	UCS-A /security/default-auth # **set realm** *auth-type*	デフォルト認証を指定します。*auth-type* は次のキーワードのいずれかです。 • **ldap**：LDAP 認証を指定します • **local**：ローカル認証を指定します • **none**：ローカルユーザはパスワードを指定せずにログインできます • **radius**：RADIUS 認証を指定します • **tacacs**：TACACS+ 認証を指定します
ステップ 4	UCS-A /security/default-auth # **set auth-server-group** *auth-serv-group-name*	（任意） 関連付けられたプロバイダー グループ（存在する場合）。
ステップ 5	UCS-A /security/default-auth # **set refresh-period** *seconds*	（任意） Cisco UCS Manager に接続している場合、Web クライアントは、Web セッションをアクティブに保つために、Cisco UCS Manager に更新要求を送信する必要があります。このオプションを使用して、このドメインのユーザに許可する更新要求間隔の最大時間数を指定します。 この時間制限を超えると、Cisco UCS Manager は Web セッションを非アクティブであると見なしますが、セッションの終了は行いません。 60 ～ 172800 の範囲内の整数を指定します。デフォルト値は、二要素認証がイネーブルでない場合は 600 秒、二要素認証がイネーブルの場合は 7200 秒です。
ステップ 6	UCS-A /security/default-auth # **set session-timeout** *seconds*	（任意） 最後の更新要求から Cisco UCS Manager が Web セッションが非アクティブであると見なすまでの最大経過時間。

	コマンドまたはアクション	目的
		この時間制限を超えた場合、Cisco UCS Manager は自動的に Web セッションを終了します。 300 ～ 172800 の範囲内の整数を指定します。デフォルト値は、二要素認証がイネーブルでない場合は 7200 秒、二要素認証がイネーブルの場合は 8000 秒です。 （注） RADIUS または TACACS+ レルムに対して二要素認証を設定する場合は、リモートユーザが頻繁に再認証する必要がないよう、セッションの更新時間およびセッションのタイムアウト時間を増やすことを検討してください。
ステップ 7	UCS-A /security/default-auth # **set use-2-factor yes**	（任意） 認証方式をレルムの二要素認証に設定します。 （注） 二要素認証は、RADIUS および TACACS+ レルムにのみ適用されます。
ステップ 8	UCS-A /security/default-auth # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、デフォルトの認証を RADIUS に設定し、デフォルトの認証プロバイダー グループを provider1 に設定し、二要素認証を有効にし、更新間隔を 7200 秒（2 時間）に設定し、セッションのタイムアウト時間を 28800 秒（8 時間）に設定し、二要素認証を有効にします。その後で、トランザクションを確定します。

```
UCS-A# scope security
UCS-A /security # scope default-auth
UCS-A /security/default-auth # set realm radius
UCS-A /security/default-auth* # set auth-server-group provider1
UCS-A /security/default-auth* # set use-2-factor yes
UCS-A /security/default-auth* # set refresh-period 7200
UCS-A /security/default-auth* # set session-timeout 28800
UCS-A /security/default-auth* # commit-buffer
UCS-A /security/default-auth #
```

リモート ユーザのロール ポリシー

デフォルトでは、Cisco UCS Manager でユーザ ロールが設定されていない場合は、LDAP、RADIUS、または TACACS プロトコルを使用してリモート サーバから Cisco UCS Manager にログインしているすべてのユーザに読み取り専用アクセス権が付与されます。セキュリティ上の理由から、Cisco UCS Manager で確立されたユーザ ロールに一致するユーザにアクセスを制限することが望ましい場合があります。

リモート ユーザのロール ポリシーは、次の方法で設定できます。

assign-default-role

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

これはデフォルトの動作です。

no-login

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

リモート ユーザのロール ポリシーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **set remote-user default-role** {**assign-default-role** | **no-login**}	Cisco UCS Manager へのユーザ アクセスがユーザ ロールに基づいて制限されるかどうかを指定します。
ステップ 3	UCS-A /security # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、リモートユーザのロールポリシーを設定し、トランザクションを確定する例を示します。

```
UCS-A# scope security
UCS-A /security # set remote-user default-role assign-default-role
UCS-A /security* # commit-buffer
UCS-A /security #
```

第 10 章

組織の設定

この章の内容は、次のとおりです。

マルチテナント環境の組織

マルチテナント機能を使用すると、Cisco UCS ドメインの大規模な物理インフラストラクチャを、組織と呼ばれる論理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場合、すべての組織は階層的になります。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次のうち 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

ルート組織は常にトップ レベルの組織です。

マルチテナント環境における階層的な名前解決

マルチテナント環境では、Cisco UCS は組織の階層を使用して、ポリシーおよびリソース プールの名前を解決します。Cisco UCS Manager は、プールに割り当てられているポリシーまたはリソースの詳細を検索する際に、以下の操作を実行します。

1. Cisco UCS Manager は、サービス プロファイルまたはポリシーに割り当てられている組織内で、指定された名前のポリシーとプールの有無をチェックします。
2. ポリシーを検出したか、使用可能なリソースがプール内にある場合、Cisco UCS Manager はそのポリシーまたはリソースを使用します。ローカル レベルで使用可能なリソースがプール内に存在しない場合、Cisco UCS Manager は上位階層の親組織に移動し、同じ名前のプールを検索します。Cisco UCS Manager は、ルートの組織に到達するまでこの手順を繰り返します。
3. ルート組織まで検索し、使用可能なリソースまたはポリシーを検出できない場合、Cisco UCS Manager はローカル組織に戻り、デフォルト プール内でデフォルト ポリシーまたは使用可能なリソースの検出を開始します。
4. デフォルト プール内で適用可能なデフォルト ポリシーまたは使用可能なリソースを検出した場合、Cisco UCS Manager はそのポリシーまたはリソースを使用します。プール内に使用可能なリソースが存在しない場合、Cisco UCS Manager は上位階層の親組織に移動し、デフォルト プールを検索します。Cisco UCS Manager は、ルートの組織に到達するまでこの手順を繰り返します。
5. Cisco UCS Manager は、適用可能なポリシーまたは使用可能なリソースを階層内で検出できない場合、割り当てエラーを返します。

例：単一階層でのサーバ プール名の解決

この例では、すべての組織がルート組織下の同一レベルにあります。たとえば、サービス プロバイダーは、各顧客に対して個別の組織を作成します。この構成では、組織は、自身の組織およびルート組織に割り当てられたポリシーおよびリソースだけにアクセスできます。

この例では、XYZcustomer 組織のサービス プロファイルは、XYZcustomer サーバ プールのサーバを使用するように設定されています。リソースプールとポリシーがサービスプロファイルに割り当てられると、以下の動作が発生します。

1. Cisco UCS Manager は、XYZcustomer サーバ プール内で使用可能なサーバをチェックします。
2. 使用可能なサーバが XYZcustomer サーバ プールに存在する場合、Cisco UCS Manager はこのサーバとサービス プロファイルを関連付け、検索を終了します。プール内に使用可能なサーバが存在しない場合、Cisco UCS Manager はルート組織で同じ名前のサーバ プールをチェックします。
3. ルート組織に XYZcustomer サーバ プールが含まれており、そのプールに使用可能なサーバが存在する場合、Cisco UCS Manager はこのサーバとサービス プロファイルを関連付け、検索を終了します。プール内に使用可能なサーバが存在しない場合、Cisco UCS Manager は XYZcustomer 組織に戻り、デフォルトのサーバ プールを調べます。
4. XYZcustomer 組織内のデフォルト プールに使用可能なサーバが存在する場合、Cisco UCS Manager はこのサーバとサービス プロファイルを関連付け、検索を終了します。デフォルト プールに使用可能なサーバが存在しない場合、Cisco UCS Manager はルート組織内でデフォルト サーバ プールを調べます。
5. ルート組織内のデフォルト サーバ プールに使用可能なサーバが存在する場合、Cisco UCS Manager はこのサーバとサービス プロファイルを関連付け、検索を終了します。デフォルト プールに使用可能なサーバが存在しない場合、Cisco UCS Manager は割り当てエラーを返します。

例：多階層でのサーバ プール名の解決

この例では、各組織に少なくとも 1 つのサブ組織が含まれています。たとえば、企業は、企業内の各主要部門に対しておよびこれらの部門のサブ部門に対して組織を作成できます。この構成では、各組織が、自身のローカル ポリシーとリソース プール、および親階層内のリソース プールにアクセスできます。

この例では、Finance 組織に 2 つのサブ組織（AccountsPayable および AccountsReceivable）が含まれています。AccountsPayable（AP）組織のサービス プロファイルは、AP サーバ プールのサーバを使用するように設定されています。リソース プールとポリシーがサービス プロファイルに割り当てられると、以下の動作が発生します。

1. Cisco UCS Manager は、サービス プロファイルに定義されている AP サーバ プールで使用可能なサーバをチェックします。
2. 使用可能なサーバが AP サーバ プールに存在する場合、Cisco UCS Manager はこのサーバとサービス プロファイルを関連付け、検索を終了します。プールに使用可能なサーバが存在しない場合、Cisco UCS Manager は 1 階層上位に移動し、Finance 組織で同じ名前のプールの有無を調べます。
3. Finance 組織に同じ名前のプールが含まれており、このプールに使用可能なサーバが存在する場合、Cisco UCS Manager はこのサーバとサービス プロファイルを関連付け、検索を終了します。プールに使用可能なサーバが存在しない場合、Cisco UCS Manager は 1 階層上位に移動し、ルート組織で同じ名前のプールの有無を調べます。
4. ルート組織に同じ名前のプールが含まれており、このプールに使用可能なサーバが存在する場合、Cisco UCS Manager はこのサーバとサービス プロファイルを関連付け、検索を終了します。

プールに使用可能なサーバが存在しない場合、Cisco UCS Manager は AccountsPayable 組織に戻り、デフォルトのサーバ プールを調べます。

5 AccountsPayable 組織内のデフォルト プールに使用可能なサーバが存在する場合、Cisco UCS Manager はこのサーバとサービス プロファイルを関連付け、検索を終了します。デフォルト プールに使用可能なサーバが存在しない場合、Cisco UCS Manager は 1 階層上位に移動し、Finance 組織のデフォルト サーバ プールを調べます。

6 Finance 組織内のデフォルト プールに使用可能なサーバが存在する場合、Cisco UCS Manager はこのサーバとサービス プロファイルを関連付け、検索を終了します。デフォルト プールに使用可能なサーバが存在しない場合、Cisco UCS Manager は 1 階層上位に移動し、ルート組織のデフォルト サーバ プールを調べます。

7 ルート組織内のデフォルト サーバ プールに使用可能なサーバが存在する場合、Cisco UCS Manager はこのサーバとサービス プロファイルを関連付け、検索を終了します。デフォルト プールに使用可能なサーバが存在しない場合、Cisco UCS Manager は割り当てエラーを返します。

ルート組織下の組織の設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org /**	ルート組織モードを開始します。
ステップ 2	UCS-A /org # **create org** *org-name*	ルート組織下に選択された組織を作成し、指定した組織で組織モードを開始します。 （注） ある組織モードから別の組織モードに移るとき、コマンド プロンプトは変更されません。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、ルート組織の下に Finance という名前の組織を作成し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # create org Finance
UCS-A /org* # commit-buffer
UCS-A /org #
```

非ルートの組織下の組織の設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org /**	ルート組織モードを開始します。
ステップ 2	UCS-A /org # **scope org** *org-name*	指定した組織の組織モードを開始します。 （注） ある組織モードから別の組織モードに移るとき、コマンドプロンプトは変更されません。
ステップ 3	UCS-A /org # **create org** *org-name*	事前設定された非ルート組織下に選択された組織を作成し、指定した組織で組織モードを開始します。
ステップ 4	UCS-A /org # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、NorthAmerica 組織の下に Finance という名前の組織を作成し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # scope org NorthAmerica
UCS-A /org # create org Finance
UCS-A /org* # commit-buffer
UCS-A /org #
```

組織の削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org /**	ルート組織モードを開始します。
ステップ 2	UCS-A /org # **delete org** *org-name*	指定した組織を削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、Financeという名前のルート組織下の組織を削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # delete org Finance
UCS-A /org* # commit-buffer
UCS-A /org #
```

第 11 章

ロールベース アクセス コントロールの設定

この章の内容は、次のとおりです。

ロールベース アクセス コントロールの概要

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

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

Cisco UCS のユーザ アカウント

ユーザ アカウントを使用してシステムにアクセスします。各 Cisco UCS Manager ドメインに、最大 48 のローカルユーザ アカウントを設定できます。各ユーザ アカウントには、一意のユーザ名とパスワードが必要です。

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

管理者アカウント

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

管理者アカウントは常にアクティブになっており、有効期限がありません。管理者アカウントを非アクティブに設定できません。

ローカル認証されたユーザ アカウント

ローカル認証されたユーザアカウントは、ファブリック インターコネクトのを介して直接認証され、admin または aaa 権限の所有者によって有効または無効にできます。ローカル ユーザ アカウントをディセーブルにすると、そのユーザはログインできなくなります。しかしディセーブルになったローカルユーザアカウントの構成の詳細はデータベースから削除されません。ディセーブルにされたローカルユーザアカウントを再度イネーブルにすると、アカウントはユーザ名とパスワードを含め、既存の構成で再びアクティブになります。

リモート認証されたユーザ アカウント

リモート認証されたユーザ アカウントとは、LDAP、RADIUS、または TACACS+ で認証されたユーザ アカウントです。

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

ユーザ アカウントの有効期限

ユーザ アカウントは、事前に定義した時間に有効期限が切れるように設定できます。有効期限の時間になると、ユーザ アカウントは無効になります。

デフォルトでは、ユーザ アカウントの有効期限はありません。

（注） ユーザ アカウントに有効期限を設定した後、有効期限なしに再設定することはできません。ただし、使用できる最新の有効期限の日付でアカウントを設定することは可能です。

Cisco UCS ユーザ名に関するガイドライン

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

- ログイン ID には、次を含む 1 ～ 32 の文字を含めることができます。
  - 任意の英字
  - 任意の数字
  - _（アンダースコア）
  - -（ダッシュ）
  - .（ドット）
- ログイン ID は Cisco UCS Manager 内で一意である必要があります。
- ログイン ID は、英文字で開始する必要があります。数字やアンダースコアなどの特殊文字から始めることはできません。
- ログイン ID では、大文字と小文字が区別されます。
- すべて数字のログイン ID は作成できません。
- ユーザ アカウントの作成後は、ログイン ID を変更できません。ユーザ アカウントを削除し、新しいユーザ アカウントを作成する必要があります。

予約語：ローカル認証されたユーザ アカウント

次の語は Cisco UCS でローカル ユーザ アカウントを作成するときに使用できません。

- root
- bin
- daemon
- adm
- lp
- sync
- shutdown
- halt
- news
- uucp
- operator
- games

- gopher
- nobody
- nscd
- mailnull
- mail
- rpcuser
- rpc
- mtsuser
- ftpuser
- FTP
- man
- sys
- samdme
- debug

Cisco UCS パスワードに関するガイドライン

それぞれのローカル認証されたユーザ アカウントにはパスワードが必要です。admin または aaa の権限を持つユーザは、Cisco UCS Manager を設定して、ユーザ パスワードのパスワード強度の確認を実行できます。

強いパスワードを使用することをお勧めします。そうしないと、ローカル認証されたユーザに対してパスワード強度の確認をしたときに、Cisco UCS Manager は、次の要件を満たさないパスワードを拒否します。

- 8 ～ 80 文字を含む。
- 次のうち、3 種類以上の文字が含まれていること。
  - 小文字
  - 大文字
  - ディジット
  - 特殊文字
- aaabbb など連続して 3 回を超えて繰り返す文字を含まない。
- ユーザ名と同一、またはユーザ名を逆にしたものではない。
- パスワード ディクショナリ チェックに合格する。たとえば、辞書に記載されている標準的な単語に基づくパスワードを指定することはできません。
- 次の記号を含まない。$（ドル記号）、?（疑問符）、=（等号）。

- ローカル ユーザ アカウントおよび admin アカウントのパスワードは空白にしない。

ユーザ アカウントの Web セッション制限

Cisco UCS Manager では、Web セッション制限を使用して、あるユーザ アカウントに対してある時点で許容される Web セッション数（GUI と XML の両方）を制限します。

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

ユーザ ロール

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

Cisco UCS ドメイン は、デフォルトのユーザ ロールを含めて、最大 48 個のユーザ ロールを持つことができます。最初の 48 のユーザ ロール以降に設定されたユーザ ロールは受け入れられますが、障害が発生すると非アクティブになります。

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

新しい権限を作成したり、既存の権限を変更または削除したり、ロールを削除したりできます。ロールを変更すると、そのロールを持つすべてのユーザに新しい権限が適用されます。権限の割り当ては、デフォルト ロールに定義されている権限に限定されません。つまり、カスタムの権限の組み合わせを使用して、独自のロールを作成できます。たとえば、デフォルトのサーバ管理者ロールとストレージ管理者ロールの権限のセットは異なりますが、両方のロールの権限を組み合わせたサーバおよびストレージ管理者ロールを作成することができます。

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

AAA サーバ（RADIUS または TACACS+）上のユーザ プロファイルを、そのユーザに付与される権限に対応したロールを追加するように変更します。属性にロール情報が保存されます。AAA サーバでは、要求とともにこの属性が返され、それを解析してロールが得られます。LDAP サーバでは、ユーザ プロファイル属性内のロールが返されます。

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

デフォルトのユーザ ロール

システムには、次のデフォルトのユーザ ロールが用意されています。

AAA アドミニストレータ

ユーザ、ロール、および AAA 設定に対する読み取りと書き込みのアクセス権。その他のシステムに対する読み取りアクセス。

管理者

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

ファシリティ マネージャ

power-mgmt 権限による、電源管理操作に対する読み取りと書き込みのアクセス。その他のシステムに対する読み取りアクセス。

ネットワーク管理者

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

操作

システムのログ（syslog サーバを含む）と障害に対する読み取りと書き込みのアクセス権。その他のシステムに対する読み取りアクセス。

読み取り専用

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

サーバ計算

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

サーバ機器アドミニストレータ

物理サーバ関連の操作に対する読み取りと書き込みのアクセス権。その他のシステムに対する読み取りアクセス。

サーバ プロファイル アドミニストレータ

論理サーバ関連の操作に対する読み取りと書き込みのアクセス権。その他のシステムに対する読み取りアクセス。

サーバ セキュリティ アドミニストレータ

サーバ セキュリティ関連の操作に対する読み取りと書き込みのアクセス権。その他のシステムに対する読み取りアクセス。

ストレージ管理者

ストレージ操作に対する読み取りと書き込みのアクセス権。その他のシステムに対する読み取りアクセス。

予約語：ユーザ ロール

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

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

権限

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

ヒント

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

表 *8*：ユーザの権限

権限	説明	デフォルトのロール割り当て
aaa	システム セキュリティおよび AAA	AAA アドミニストレータ
admin	システム管理	管理者
ext-lan-config	外部 LAN 設定	ネットワーク管理者
ext-lan-policy	外部 LAN ポリシー	ネットワーク管理者

権限	説明	デフォルトのロール割り当て
ext-lan-qos	外部 LAN QoS	ネットワーク管理者
ext-lan-security	外部 LAN セキュリティ	ネットワーク管理者
ext-san-config	外部 SAN 設定	ストレージ管理者
ext-san-policy	外部 SAN ポリシー	ストレージ管理者
ext-san-qos	外部 SAN QoS	ストレージ管理者
ext-san-security	外部 SAN セキュリティ	ストレージ管理者
fault	アラームおよびアラーム ポリシー	操作
operations	ログおよび Smart Call Home	操作
org-management	組織管理	操作
pod-config	ポッド設定	ネットワーク管理者
pod-policy	ポッド ポリシー	ネットワーク管理者
pod-qos	ポッド QoS	ネットワーク管理者
pod-security	ポッド セキュリティ	ネットワーク管理者
power-mgmt	電源管理操作に対する読み取りと書き込みのアクセス	ファシリティ マネージャ
read-only	読み取り専用アクセス権 読み取り専用は、権限として選択できません。この権限は、すべてのユーザ ロールに割り当てられます。	読み取り専用
server-equipment	サーバ ハードウェア管理	サーバ機器アドミニストレータ
server-maintenance	サーバ メンテナンス	サーバ機器アドミニストレータ
server-policy	サーバ ポリシー	サーバ機器アドミニストレータ
server-security	サーバ セキュリティ	サーバ セキュリティ アドミニストレータ

権限	説明	デフォルトのロール割り当て
service-profile-compute	サービス プロファイルの計算	サーバ計算アドミニストレータ
service-profile-config	サービス プロファイルの設定	サーバプロファイルアドミニストレータ
service-profile-config-policy	サービスプロファイル設定ポリシー	サーバプロファイルアドミニストレータ
service-profile-ext-access	サービスプロファイルのエンドポイント アクセス	サーバプロファイルアドミニストレータ
service-profile-network	サービス プロファイル ネットワーク	ネットワーク管理者
service-profile-network-policy	サービス プロファイル ネットワーク ポリシー	ネットワーク管理者
service-profile-qos	サービス プロファイル QoS	ネットワーク管理者
service-profile-qos-policy	サービス プロファイル QoS ポリシー	ネットワーク管理者
service-profile-security	サービス プロファイル セキュリティ	サーバセキュリティアドミニストレータ
service-profile-security-policy	サービス プロファイル セキュリティ ポリシー	サーバセキュリティアドミニストレータ
service-profile-server	サービス プロファイル サーバ管理	サーバプロファイルアドミニストレータ
service-profile-server-oper	サービス プロファイル コンシューマ	サーバプロファイルアドミニストレータ
service-profile-server-policy	サービス プロファイル プール ポリシー	サーバセキュリティアドミニストレータ
service-profile-storage	サービスプロファイルストレージ	ストレージ管理者
service-profile-storage-policy	サービスプロファイルストレージ ポリシー	ストレージ管理者

ユーザ ロケール

ユーザは 1 つ以上のロケールに割り当てることができます。各ロケールでは、ユーザがアクセスできる 1 つ以上の組織（ドメイン）を定義します。アクセスはロケールで指定されている組織に限定されますが、例外として組織が指定されていないロケールがあります。この場合はすべての組織内のシステム リソースに無制限にアクセスできます。

Cisco UCS ドメイン は、最大 48 個のユーザ ロケールを持つことができます。最初の 48 のユーザ ロールが許可された後に設定されたユーザ ロケールは、障害が発生して無効になります。

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

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

- aaa
- admin
- fault
- operations

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

ユーザ ロールの設定

ユーザ ロールの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /security # **create role** *name*	ユーザ ロールを作成し、セキュリティ ロール モードを開始します。
ステップ 3	UCS-A /security/role # **add privilege** *privilege-name*	ロールに 1 つ以上の権限を追加します。 （注） 複数の *privilege-name* を同じコマンドラインに指定してロールに複数の権限を追加することもできますし、複数の **add** コマンドを使用して同じロールに複数の権限を追加することもできます。
ステップ 4	UCS-A /security/role #**commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、service-profile-security-admin ロールを作成し、ロールにサービス プロファイル セキュリティおよびサービス プロファイル セキュリティ ポリシー権限を追加し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # create role ls-security-admin
UCS-A /security/role* # add privilege service-profile-security service-profile-security-policy
UCS-A /security/role* # commit-buffer
UCS-A /security/role #
```

ユーザ ロールへの権限の追加

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope role** *name*	指定したロールに対するセキュリティ ロール モードを開始します。
ステップ 3	UCS-A /security/role # **add privilege** *privilege-name*	ユーザ ロールの既存の権限に 1 つ以上の権限を追加します。 （注） 複数の *privilege-name* を同じコマンドラインに指定してロールに複数の権限を追加することもできますし、複数の **add privilege** コマンドを使用して同じロールに複数の権限を追加することもできます。

	コマンドまたはアクション	目的
ステップ 4	UCS-A /security/role #**commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、service-profile-security-admin ロールにサーバ セキュリティ権限とサーバ ポリシー権限を追加し、トランザクションをコミットする方法を示します。

```
UCS-A# scope security
UCS-A /security # scope role service-profile-security-admin
UCS-A /security/role # add privilege server-security server-policy
UCS-A /security/role* # commit-buffer
UCS-A /security/role #
```

ユーザ ロールの権限の置換

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope role** *name*	指定したロールに対するセキュリティ ロール モードを開始します。
ステップ 3	UCS-A /security/role # **set privilege** *privilege-name*	ユーザ ロールの既存の権限を置き換えます。 （注） 同じコマンド ラインで複数の *privilege-name* を指定することで、既存の権限を複数の権限に置換できます。権限を置換した後、**add privilege** コマンドを使用して同じロールに権限を追加できます。
ステップ 4	UCS-A /security/role #**commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、service-profile-security-admin ロール用の既存の権限をサーバ セキュリティおよびサーバ ポリシー権限に置き換え、トランザクションをコミットする方法を示します。

```
UCS-A# scope security
UCS-A /security # scope role service-profile-security-admin
UCS-A /security/role # set privilege server-security server-policy
UCS-A /security/role* # commit-buffer
UCS-A /security/role #
```

ユーザ ロールからの権限の削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope role** *name*	指定したロールに対するセキュリティ ロール モードを開始します。
ステップ 3	UCS-A /security/role # **remove privilege** *privilege-name*	既存のユーザ ロール特権から 1 つ以上の特権を削除します。 （注） 同じコマンド ラインで複数の *privilege-name* を指定することで、複数の特権をロールから削除できます。または、複数の **remove privilege** コマンドを使用することで、同じロールから特権を削除できます。
ステップ 4	UCS-A /security/role #**commit-buffer**	トランザクションをシステム設定にコミットします。

次に、service-profile-security-admin ロールからサーバ セキュリティ特権とサーバ ポリシー特権を削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope security
UCS-A /security # scope role service-profile-security-admin
UCS-A /security/role # remove privilege server-security server-policy
UCS-A /security/role* # commit-buffer
UCS-A /security/role #
```

ユーザ ロールの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **delete role** *name*	ユーザ ロールを削除します。
ステップ 3	UCS-A /security #**commit-buffer**	トランザクションをシステム設定にコミットします。

次に、service-profile-security-admin ロールを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope security
UCS-A /security # delete role service-profile-security-admin
UCS-A /security* # commit-buffer
UCS-A /security #
```

ロケールの設定

ロケールの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **create locale** *locale-name*	ロケールを作成し、セキュリティ ロケール モードを開始します。
ステップ 3	UCS-A /security/locale # **create org-ref** *org-ref-name***orgdn** *orgdn org-root/org-ref-name*	ロケールに組織を参照（バインド）します。*org-ref-name* 引数は組織参照の識別に使用される名前で、*orgdn-name* 引数は参照されている組織の識別名です。
ステップ 4	UCS-A /security/locale #**commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、western ロケールを作成し、そのロケールに財務組織を参照し、参照に finance-ref という名前を指定し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # create locale western
UCS-A /security/locale* # create org-ref finance-ref orgdn org-root/org-finance
UCS-A /security/locale* # commit-buffer
UCS-A /security/locale #
```

ロケールへの組織の割り当て

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A# **scope locale** *locale-name*	セキュリティ ロケール モードを開始します。
ステップ 3	UCS-A /security/locale # **create org-ref** *org-ref-name***orgdn** *org-root/org-ref-name*	ロケールに組織を参照（バインド）します。*org-ref-name* 引数は組織参照の識別に使用される名前で、*orgdn-name* 引数は参照されている組織の識別名です。
ステップ 4	UCS-A /security/locale #**commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、western ロケールに入り、そのロケールに marketing 組織を追加（参照）し、参照に marketing-ref という名前を指定し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope locale western
UCS-A /security/locale* # create org-ref marketing-ref orgdn org-root/org-marketing
UCS-A /security/locale* # commit-buffer
UCS-A /security/locale #
```

ロケールからの組織の削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope locale** *locale-name*	セキュリティ ロケール モードを開始します。
ステップ 3	UCS-A /security/locale # **delete org-ref** *org-ref-name*	ロケールから組織を削除します。
ステップ 4	UCS-A /security/locale #**commit-buffer**	トランザクションをシステム設定にコミットします。

次に、western ロケールから finance 組織を削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope security
UCS-A /security # scope locale western
UCS-A /security/locale # delete org-ref finance-ref
UCS-A /security/locale* # commit-buffer
UCS-A /security/locale #
```

ロケールの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **delete locale** *locale-name*	ロケールを削除します。
ステップ 3	UCS-A /security #**commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、western ロケールを削除し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # delete locale western
UCS-A /security* # commit-buffer
UCS-A /security #
```

ローカル認証されたユーザ アカウントの設定

ユーザ アカウントの作成

少なくとも、次のユーザを作成することを推奨します。

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

はじめる前に

システムに次のいずれかがある場合は、該当するタスクを実行します。

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

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **create local-user** *local-user-name*	指定したローカル ユーザのユーザ アカウントを作成し、セキュリティ ローカル ユーザ モードを開始します。
ステップ 3	UCS-A /security/local-user # **set account-status** {**active**| **inactive**}	ローカル ユーザ アカウントを有効にするか、無効にするかを指定します。 ローカル ユーザ アカウントのアカウント ステータスが非アクティブに設定された場合、ユーザは既存のクレデンシャルを使用してシステムにロギングできません。
ステップ 4	UCS-A /security/local-user # **set password** *password*	ユーザ アカウントのパスワードを設定します
ステップ 5	UCS-A /security/local-user # **set firstname** *first-name*	（任意） ユーザの名を指定します。
ステップ 6	UCS-A /security/local-user # **set lastname** *last-name*	（任意） ユーザの姓を指定します。
ステップ 7	UCS-A /security/local-user # **set expiration** *month day-of-month year*	（任意） ユーザ アカウントが期限切れになる日付を指定します。*month* 引数は、月の英名の最初の 3 文字です。 （注） ユーザ アカウントに有効期限を設定した後、有効期限なしに再設定することはできません。ただし、使用できる最新の有効期限の日付でアカウントを設定することは可能です。
ステップ 8	UCS-A /security/local-user # **set email** *email-addr*	（任意） ユーザの電子メール アドレスを指定します。
ステップ 9	UCS-A /security/local-user # **set phone** *phone-num*	（任意） ユーザの電話番号を指定します。
ステップ 10	UCS-A /security/local-user # **set sshkey** *ssh-key*	（任意） パスワードレス アクセス用の SSH キーを指定します。
ステップ 11	UCS-A security/local-user # **commit-buffer**	トランザクションをコミットします。

次の例は、kikipopo という名前のユーザ アカウントを作成し、ユーザ アカウントをイネーブルにし、foo12345 にパスワードを設定し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # create local-user kikipopo
UCS-A /security/local-user* # set account-status active
UCS-A /security/local-user* # set password
Enter a password:
Confirm the password:
UCS-A /security/local-user* # commit-buffer
UCS-A /security/local-user #
```

次の例は、lincey という名前のユーザアカウントを作成し、ユーザアカウントをイネーブルにし、パスワードレス アクセス用の OpenSSH キーを設定し、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # create local-user lincey
UCS-A /security/local-user* # set account-status active
UCS-A /security/local-user* #  set sshkey "ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAuo9VQ2CmWBI9/S1f30klCWjnV3lgdXMzO0WUl5iPw85lkdQqap+NFuNmHcb4K
iaQB8X/PDdmtlxQQcawclj+k8f4VcOelBxlsGk5luq5ls1ob1VOIEwcKEL/h5lrdbNlI8y3SS9I/gGiBZ9ARlop9LDpD
m8HPh2LOgyH7Ei1MI8="
UCS-A /security/local-user* # commit-buffer
UCS-A /security/local-user #
```

次の例は、jforlenz という名前のユーザ アカウントを作成し、ユーザ アカウントを有効にし、パスワードレス アクセス用のセキュア SSH キーを設定し、トランザクションを確定します。

```
UCS-A# scope security
UCS-A /security # create local-user jforlenz
UCS-A /security/local-user* # set account-status active
UCS-A /security/local-user* #  set sshkey
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
User's SSH key:
> ---- BEGIN SSH2 PUBLIC KEY ----
>AAAAB3NzaC1yc2EAAAABIwAAAIEAuo9VQ2CmWBI9/S1f30klCWjnV3lgdXMzO0WUl5iPw8
>5lkdQqap+NFuNmHcb4KiaQB8X/PDdmtlxQQcawclj+k8f4VcOelBxlsGk5luq5ls1ob1VO
>IEwcKEL/h5lrdbNlI8y3SS9I/gGiBZ9ARlop9LDpDm8HPh2LOgyH7Ei1MI8=
> ---- END SSH2 PUBLIC KEY ----
> ENDOFBUF
UCS-A /security/local-user* # commit-buffer
UCS-A /security/local-user #
```

ローカル認証されたユーザへのパスワード強度チェックのイネーブル化

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

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /security # **enforce-strong-password** {**yes** | **no**}	パスワードの強度チェックを有効にするか、または無効にするかを指定します。

次に、パスワードの強度チェックを有効にする例を示します。

```
UCS-A# scope security
UCS-A /security # set enforce-strong-password yes
UCS-A /security #
```

ユーザ アカウントの Web セッション制限の設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope services**	システム サービス モードを開始します。
ステップ 3	UCS-A /system/services # **scope web-session-limits**	システム サービス Web セッション制限モードを開始します。
ステップ 4	UCS-A /system/services/web-session-limits # **set peruser** *num-of-logins-per-user*	各ユーザに許可する同時 HTTP および HTTPS セッションの最大数を設定します。 1 ～ 256 の整数を入力します。デフォルトでは 32 に設定されます。
ステップ 5	UCS-A /system/services/web-session-limits # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、各ユーザ アカウントに許可する HTTP および HTTPS セッションの最大数を 60 に設定し、トランザクションをコミットする例を示します。

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # scope web-session-limits
UCS-A /system/services/web-session-limits* # set peruser 60
UCS-A /system/services/web-session-limits* # commit-buffer
UCS-A /system/services/web-session-limits #
```

ユーザ アカウントへのロールの割り当て

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

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope local-user** *local-user-name*	指定したローカル ユーザ アカウントに対するセキュリティ ローカル ユーザ モードを開始します。
ステップ 3	UCS-A /security/local-user # **create role** *role-name*	ユーザ アカウントに指定したロールを割り当てます。 （注） **create role** コマンドは、1 つのユーザ アカウントに複数のロールを割り当てるために複数回入力できます。
ステップ 4	UCS-A security/local-user # **commit-buffer**	トランザクションをコミットします。

次の例では、ローカル ユーザ アカウント kikipopo に operations ロールを割り当て、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope local-user kikipopo
UCS-A /security/local-user # create role operations
UCS-A /security/local-user* # commit-buffer
UCS-A /security/local-user #
```

ユーザ アカウントへのロケールの割り当て

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

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope local-user** *local-user-name*	指定したローカル ユーザ アカウントに対するセキュリティ ローカル ユーザ モードを開始します。
ステップ 3	UCS-A /security/local-user # **create locale** *locale-name*	ユーザ アカウントに指定したロケールを割り当てます。 （注） **create locale** コマンドは、1 つのユーザ アカウントに複数のロケールを割り当てるために複数回入力できます。
ステップ 4	UCS-A security/local-user # **commit-buffer**	トランザクションをコミットします。

次の例では、ローカル ユーザ アカウント kikipopo に西洋言語ロケールを割り当て、トランザクションをコミットします。

```
UCS-A# scope security
UCS-A /security # scope local-user kikipopo
UCS-A /security/local-user # create locale western
UCS-A /security/local-user* # commit-buffer
UCS-A /security/local-user #
```

ユーザ アカウントからのロールの削除

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

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope local-user** *local-user-name*	指定したローカル ユーザ アカウントに対するセキュリティ ローカル ユーザ モードを開始します。
ステップ 3	UCS-A /security/local-user # **delete role** *role-name*	ユーザ アカウントから指定したロールを削除します。

	コマンドまたはアクション	目的
		（注） ユーザアカウントから複数のロールを削除するために、**delete role** コマンドを複数回入力できます。
ステップ 4	UCS-A security/local-user # **commit-buffer**	トランザクションをコミットします。

次に、kikipopo というローカル ユーザ アカウントから operations ロールを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope security
UCS-A /security # scope local-user kikipopo
UCS-A /security/local-user # delete role operations
UCS-A /security/local-user* # commit-buffer
UCS-A /security/local-user #
```

ユーザ アカウントからのロケールの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope local-user** *local-user-name*	指定したローカル ユーザ アカウントに対するセキュリティ ローカル ユーザ モードを開始します。
ステップ 3	UCS-A /security/local-user # **delete locale** *locale-name*	ユーザ アカウントから指定したロケールを削除します。 （注） ユーザアカウントから複数のロケールを削除するために、**delete locale** コマンドを複数回入力できます。
ステップ 4	UCS-A security/local-user # **commit-buffer**	トランザクションをコミットします。

次に、kikipopo というローカル ユーザ アカウントから western ロケールを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope security
UCS-A /security # scope local-user kikipopo
UCS-A /security/local-user # delete locale western
UCS-A /security/local-user* # commit-buffer
UCS-A /security/local-user #
```

ユーザ アカウントのイネーブル化またはディセーブル化

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

はじめる前に

ローカル ユーザ アカウントを作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope local-user**	ローカル ユーザ セキュリティ モードを開始します。
ステップ 3	UCS-A /security/local-user # **set account-status** {**active** | **inactive**}	ローカル ユーザ アカウントを有効にするか、無効にするかを指定します。 admin ユーザ アカウントは常にアクティブに設定されます。変更はできません。 （注） アカウント ステータスを非アクティブに設定しても、データベースからコンフィギュレーションは削除されません。

次に、accounting というローカル ユーザ アカウントを有効にする例を示します。

```
UCS-A# scope security
UCS-A /security # scope local-user accounting
UCS-A /security/local-user # set account-status active
```

ローカル認証されたユーザのパスワード履歴のクリア

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope local-user** *user-name*	指定したユーザ アカウントのローカル ユーザ セキュリティ モードに入ります。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /security/local-user # **set clear password-history yes**	指定されたユーザ アカウントのパスワード履歴をクリアします。
ステップ 4	UCS-A /security/local-user # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、パスワード履歴カウントを設定し、トランザクションを確定する例を示します。

```
UCS-A # scope security
UCS-A /security # scope local-user admin
UCS-A /security/local-user # set clear password-history yes
UCS-A /security/local-user* # commit-buffer
UCS-A /security/local-user #
```

ユーザ アカウントの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **delete local-user** *local-user-name*	ローカル ユーザ アカウントを削除します。
ステップ 3	UCS-A /security #**commit-buffer**	トランザクションをシステム設定にコミットします。

次に、foo というユーザ アカウントを削除し、トランザクションを確定する例を示します。

```
UCS-A# scope security
UCS-A /security # delete local-user foo
UCS-A /security* # commit-buffer
UCS-A /security #
```

ローカル認証されたユーザのパスワード プロファイル

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

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

パスワード履歴カウント

パスワード履歴のカウントにより、ローカル認証されたユーザが同じパスワードを再利用しないようにすることができます。パスワード履歴カウントを設定すると、Cisco UCS Manager で以前に使用されたパスワードが最大 15 個保存されます。パスワード履歴カウントでは最も新しいパスワードを先頭に時系列とは逆の順番で保存しているため、履歴カウントがしきい値に到達すると、最も古いパスワードのみが再使用可能になります。

あるパスワードが再使用可能になるまでに、ユーザはパスワード履歴カウントで設定された数のパスワードを作成して使用することができます。たとえば、パスワード履歴カウントを 8 に設定した場合、ユーザは最初のパスワードを 9 番目のパスワードが期限切れになる後まで再使用できません。

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

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

パスワード変更間隔

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

間隔の設定	説明	例
パスワード変更禁止	パスワードの変更後、指定された時間の間は、ローカル認証されたユーザのパスワードを変更することはできません。 1 ～ 745 時間の変更禁止間隔を指定できます。デフォルトでは、変更禁止間隔は 24 時間です。	たとえば、パスワードの変更後、48 時間はパスワードを変更できないようにするには、次のように設定します。 • [間隔中の変更（Change During Interval）] を無効にする • [変更禁止間隔（No Change Interval）] を 48 に設定する

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

変更間隔のパスワード変更の最大数の設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope password-profile**	パスワード プロファイル セキュリティ モードを開始します。
ステップ 3	UCS-A /security/password-profile # **set change-during-interval enable**	ローカル認証されたユーザが指定された時間内に実行できるパスワード変更の回数を制限します。
ステップ 4	UCS-A /security/password-profile # **set change-count** *pass-change-num*	ローカル認証されたユーザが、[変更間隔（Change Interval）] の間に自分のパスワードを変更できる最大回数。 を指定します。 この値は、0 ～ 10 の範囲で自由に設定できます。
ステップ 5	UCS-A /security/password-profile # **set change-interval** *num-of-hours*	フィールドで指定したパスワード変更回数が有効になる時間の最大数。 を指定します。 この値は、1 ～ 745 時間の範囲で自由に設定できます。

	コマンドまたはアクション	目的
		たとえば、このフィールドが 48 に設定され、[変更カウント（Change Count）] フィールドが 2 に設定されている場合、ローカル認証されたユーザは 48 時間以内に 2 回を超えるパスワード変更を実行することはできません。
ステップ 6	UCS-A /security/password-profile # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、[間隔中の変更（Change During Interval）] オプションを有効にし、変更回数を 5 回、変更間隔を 72 時間に設定し、トランザクションを確定する例を示します。

```
UCS-A # scope security
UCS-A /security # scope password-profile
UCS-A /security/password-profile # set change-during-interval enable
UCS-A /security/password-profile* # set change-count 5
UCS-A /security/password-profile* # set change-interval 72
UCS-A /security/password-profile* # commit-buffer
UCS-A /security/password-profile #
```

パスワードの変更禁止間隔の設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope password-profile**	パスワード プロファイル セキュリティ モードを開始します。
ステップ 3	UCS-A /security/password-profile # **set change-during-interval disable**	間隔中の変更機能をディセーブルにします。
ステップ 4	UCS-A /security/password-profile # **set no-change-interval** *min-num-hours*	ローカル認証されたユーザが、新しく作成したパスワードを変更する前に待機する最小時間数。 を指定します。 この値は、1 ～ 745 時間の範囲で自由に設定できます。

	コマンドまたはアクション	目的
		この間隔は、[間隔中の変更（Change During Interval）] プロパティが [無効（Disable）] に設定されていない場合は無視されます。
ステップ 5	UCS-A /security/password-profile # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、間隔中の変更オプションを無効にし、変更禁止間隔を72時間に設定し、トランザクションを確定する例を示します。

```
UCS-A # scope security
UCS-A /security # scope password-profile
UCS-A /security/password-profile # set change-during-interval disable
UCS-A /security/password-profile* # set no-change-interval 72
UCS-A /security/password-profile* # commit-buffer
UCS-A /security/password-profile #
```

パスワード履歴カウントの設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope password-profile**	パスワード プロファイル セキュリティ モードを開始します。
ステップ 3	UCS-A /security/password-profile # **set history-count** *num-of-passwords*	ローカル認証されたユーザが、以前に使用していたパスワードを再利用できるまでに、作成する必要がある一意のパスワードの数を指定します。 この値は、0 ～ 15 の範囲で自由に設定できます。 デフォルトでは、[履歴（History Count）] フィールドは0に設定されます。これにより、履歴カウントが無効になるため、ユーザはいつでも以前に使用していたパスワードを再利用できます。
ステップ 4	UCS-A /security/password-profile # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、パスワード履歴カウントを設定し、トランザクションを確定する例を示します。

```
UCS-A # scope security
UCS-A /security # scope password-profile
UCS-A /security/password-profile # set history-count 5
UCS-A /security/password-profile* # commit-buffer
UCS-A /security/password-profile #
```

CLI からのユーザ セッションのモニタリング

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **show user-session** {**local** | **remote**} [**detail**]	システムにログインしているすべてのユーザのセッション情報を表示します。セッション ID の横のアスタリスク（*）は、現在のログイン セッションを示します。

次に、システムにログインしているすべてのローカル ユーザのリストを表示する例を示します。アスタリスクは、どのセッションが現在のログイン セッションであるかを示します。

```
UCS-A# scope security
UCS-A /security # show user-session local
Session Id      User            Host                  Login Time
--------------- --------------- --------------------- ----------
pts_25_1_31264*  steve           192.168.100.111      2009-05-09T14:06:59
ttyS0_1_3532    jeff            console               2009-05-02T15:11:08
web_25277_A     faye            192.168.100.112       2009-05-15T22:11:25
```

次に、システムにログインしているすべてのローカル ユーザの詳細情報を表示する例を示します。

```
UCS-A# scope security
UCS-A /security # show user-session local detail
Session Id pts_25_1_31264:
    Fabric Id: A
    Term: pts/25
    User: steve
    Host: 64.101.53.93
    Pid: 31264
    Login Time: 2009-05-09T14:06:59

Session Id ttyS0_1_3532:
    Fabric Id: A
    Term: ttyS0
    User: jeff
    Host: console
    Pid: 3532
    Login Time: 2009-05-02T15:11:08

Session Id web_25277_A:
    Fabric Id: A
    Term: web_25277
    User: faye
    Host: 192.168.100.112
    Pid: 3518
```

```
    Login Time: 2009-05-15T22:11:25
```

第 12 章

DNS サーバの設定

この章の内容は、次のとおりです。

Cisco UCS での DNS サーバ

システムがホスト名の名前解決を必要とする場合は、使用する外部 DNS サーバを各 Cisco UCS ドメイン に指定する必要があります。たとえば、DNS サーバを設定していないと、ファブリック インターコネクトに関する設定を行うときに、www.cisco.com などの名前を使用できません。サーバの IP アドレスを使用する必要があります。これには、IPv4 または IPv6 アドレスのいずれかを使用できます。各 Cisco UCS ドメイン に対し最大 4 台の DNS サーバを設定できます。

（注） 複数の DNS サーバを設定する場合、システムによるサーバの検索順はランダムになります。ローカル管理コマンドが DNS サーバの検索を必要とする場合、3 台の DNS サーバのみをランダムに検索します。

DNS サーバの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /system # **scope services**	システム サービス モードを開始します。
ステップ 3	UCS-A /system/services # **create dns** {*ip-addr ip6-addr*}	指定した IPv4 または IPv6 アドレスの DNS サーバを使用するようシステムを設定します。
ステップ 4	UCS-A /system/services # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、IPv4 アドレス 192.168.200.105 の DNS サーバを設定し、トランザクションを確定する例を示します。

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # create dns 192.168.200.105
UCS-A /system/services* # commit-buffer
UCS-A /system/services #
```

次の例では、IPv6 アドレス 2001:db8::22:F376:FF3B:AB3F を持つ DNS サーバを設定し、トランザクションをコミットします。

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # create dns 2001:db8::22:F376:FF3B:AB3F
UCS-A /system/services* # commit-buffer
UCS-A /system/services #
```

DNS サーバの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope services**	システム サービス モードを開始します。
ステップ 3	UCS-A /system/services # **delete dns** *ip-addr*	指定した IP アドレスの NTP サーバを削除します。
ステップ 4	UCS-A /system/services # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、IP アドレス 192.168.200.105 を持つ DNS サーバを削除し、トランザクションを確定する例を示します。

```
UCS-A# scope system
UCS-A /system # scope services
```

```
UCS-A /system/services # delete dns 192.168.200.105
UCS-A /system/services* # commit-buffer
UCS-A /system/services #
```

第 13 章

システム関連ポリシーの設定

この章の内容は、次のとおりです。

ラック サーバ ディスカバリ ポリシーの設定

ラック サーバ ディスカバリ ポリシー

ラック サーバ ディスカバリ ポリシーは、新しいラックマウント サーバを追加したときのシステムの対処方法を決定します。Cisco UCS Manager は、ラック サーバ ディスカバリ ポリシー内の設定を使用して、ハード ディスク上のデータがスクラビングされたかどうか、およびサーバ検出を直ちに実行する必要があるかユーザの明示的な承認を待機する必要があるかを決定します。

Cisco UCS Manager は、ファブリック インターコネクトに適切にケーブル接続されていないラックマウント サーバを検出できません。サポート対象の Cisco UCS ラックマウント サーバを Cisco UCS Manager に統合する方法については、適切な『rack-mount server integration guide』を参照してください。

ラック サーバ ディスカバリ ポリシーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org /**	ルート組織モードを開始します。

	コマンドまたはアクション	目的
		（注） ラック サーバ ディスカバリ ポリシーは、ルート組織からだけアクセスできます。
ステップ 2	UCS-A /org # **scope rackserver-disc-policy**	組織ラック サーバ ディスカバリ ポリシー モードを開始します。
ステップ 3	UCS-A /org/rackserver-disc-policy # **set action** {**immediate** | **user-acknowledged**}	新しいラック サーバの追加にシステムが対応する方法を指定します。
ステップ 4	UCS-A /org/rackserver-disc-policy #**set descr** *description*	（任意） ラック サーバディスカバリ ポリシーに説明を加えます。 （注） 説明にスペース、特殊文字、または句読点が含まれている場合は、説明を引用符で括る必要があります。引用符は、**show** コマンド出力の説明フィールドには表示されません。
ステップ 5	UCS-A /org/rackserver-disc-policy # **set scrub-policy** *scrub-pol-name*	新しく検出されたラック サーバ上で実行する必要があるスクラブ ポリシーを指定します。
ステップ 6	UCS-A /org/rackserver-disc-policy # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、デフォルト ラック サーバ ディスカバリ ポリシーに範囲を設定し、すぐに新しいラック サーバを検出するよう設定し、ポリシーの説明を記入し、scrubpol1 というスクラブ ポリシーを指定して、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # scope rackserver-disc-policy
UCS-A /org/rackserver-disc-policy* # set action immediate
UCS-A /org/rackserver-disc-policy* # set descr "This is an example rackserver discovery
policy."
UCS-A /org/rackserver-disc-policy* # set scrub-policy scrubpol1
UCS-A /org/rackserver-disc-policy* # commit-buffer
UCS-A /org/rackserver-disc-policy #
```

MAC アドレス テーブルのエージング タイムの設定

MAC アドレス テーブルのエージング タイム

ポート間でパケットを効率的に切り替えるために、ファブリック インターコネクトは MAC アドレス テーブルを保持しています。ファブリック インターコネクトは、受信したパケットの MAC

ソース アドレスと、パケットが読み取られた関連ポートを使用して、MAC アドレス テーブルを動的に構築します。ファブリック インターコネクトは、設定可能なエージング タイマーで定義されたエージング メカニズムを使用して、エントリが MAC アドレス テーブル内にとどまる期間を判断します。アドレスの非アクティブ状態が所定の秒数続くと、そのアドレスは MAC アドレス テーブルから削除されます。

MAC アドレス エントリ（MAC アドレスとその関連ポート）が MAC アドレス テーブルにとどまる時間（エージ）はユーザが設定できます。

MAC アドレス テーブルのエージング タイムの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **set mac-aging** {*dd hh mm ss* | **mode-default** | **never**}	MAC アドレス テーブルのエージング タイムを指定します。設定済みのイーサネット スイッチング モードに依存するデフォルト値にエージング タイムを設定するには、**mode-default** キーワードを使用します。アイドルのまま経過した時間にかかわらず MAC アドレスがテーブルから削除されないようにするには、**never** キーワードを使用します。
ステップ 3	UCS-A /eth-uplink # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、MAC アドレス テーブルに 1 日と 12 時間のエージング タイムを設定し、トランザクションをコミットする例を示します。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # set mac-aging 01 12 00 00
UCS-A /eth-uplink* # commit-buffer
UCS-A /eth-uplink #
```

第 14 章

仮想インターフェイスの管理

この章の内容は、次のとおりです。

仮想インターフェイス

ブレード サーバ環境では、サービス プロファイルに対して設定可能な vNIC と vHBA の数は、アダプタの機能と、アダプタで利用できる仮想インターフェイス（VIF）の名前空間の量で決まります。Cisco UCS では、VIF 名前空間の各部分は VIF という固まりで割り当てられます。ハードウェアによっては、VIF の最大数が定義済みのポート単位で割り当てられます。
VIF の最大数は、ハードウェア機能とポート接続によって異なります。設定された各 vNIC または vHBA には、1 つまたは 2 つの VIF が割り当てられます。スタンドアロン vNIC および vHBA は 1 つの VIF を使用し、フェールオーバー vNIC および vHBA は 2 つを使用します。

次の変数はブレード サーバで利用可能な VIF の数に影響するため、サービス プロファイルに設定可能な vNIC と vHBA の数にも影響します。

- ファブリック インターコネクトでサポートされる VIF の最大数
- ファブリック インターコネクトがどのように接続されているか
- ファブリック インターコネクトと IOM がファブリック ポート チャネル モードで設定されているかどうか

ご使用のハードウェア設定でサポートされる VIF の最大数について詳しくは、該当するソフトウェア リリースの『*Cisco UCS Configuration Limits for Cisco UCS Manager*』を参照してください。

仮想インターフェイスの予約管理とエラー処理

ポートチャネルでグループ化されたファブリック インターコネクトの場合、I/O モジュールへのファブリック インターコネクトの接続方法を変更すると、ブレードサーバで使用可能な VIF の数が大幅に変化します。変更の影響を追跡できるように、Cisco UCS Manager には次のメトリックが保持されます。

- ハードウェアがサポートする VIF の最大数
- 接続タイプ

ブレードで使用可能な VIF の数を削減するように設定を変更すると、UCS Manager は警告を表示し、続行するかどうか確認を求めます。これには、接続の追加または変更によって VIF の数を削減する場合など、いくつかの状況があります。

第 15 章

Cisco UCS Central へ Cisco UCS ドメインを登録

この章の内容は、次のとおりです。

Cisco UCS ドメインの登録

データセンター内の Cisco UCS ドメイン の一部またはすべてを Cisco UCS Central が管理するよう設定できます。

Cisco UCS Central に Cisco UCS ドメイン を管理させる場合、そのドメインを登録する必要があります。登録するときに、Cisco UCS Central と Cisco UCS Manager でそれぞれ管理するポリシー タイプやその他の設定（バックアップやファームウェアなど）を選択する必要があります。Cisco UCS Central によって、登録されたすべての Cisco UCS ドメイン で同じタイプのポリシーおよび設定を管理するか、または登録された各 Cisco UCS ドメイン に異なる設定を行うこともできます。

Cisco UCS Central に Cisco UCS ドメイン を登録する前に、以下を実行します。

- Cisco UCS Manager と Cisco UCS Central が同期されるようにするには、双方に NTP サーバと正しいタイム ゾーンを設定します。Cisco UCS ドメインと Cisco UCS Central の日時が同期していなければ、登録が失敗する可能性があります。
- Cisco UCS Central のホスト名または IP アドレスを取得します。
- Cisco UCS Central を展開したときに設定した共有シークレットを取得します。

（注） Cisco UCS Central に登録されているドメイン内で Cisco UCS Manager が使用する IP アドレスを変更または交換することはできません。IPアドレスを変更または交換しなければならない場合は、まず Cisco UCS Central からドメインを登録解除する必要があります。IP アドレスを変更または交換した後で、Cisco UCS ドメイン を再登録できます。

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

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

これらのポリシーおよび設定を解決するには、次のオプションを使用します。

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

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

名前	説明
インフラストラクチャおよびカタログ ファームウェア（Infrastructure & Catalog Firmware）	機能カタログとインフラストラクチャ ファームウェア ポリシーが、Cisco UCS Manager でローカルに定義されるかまたは Cisco UCS Central から取得されるかを決定します。
タイム ゾーン管理（Time Zone Management）	タイム ゾーンと NTP サーバの設定が Cisco UCS Manager でローカルに定義されるか、Cisco UCS Central から取得されるかを決定します。
コミュニケーション サービス（Communication Services）	HTTP、CIM XML、Telnet、SNMP、Web セッション制限、管理インターフェイス モニタリング ポリシー設定を、Cisco UCS Manager でローカルに定義するか、または Cisco UCS Central で定義するかを決定します。
グローバル障害ポリシー（Global Fault Policy）	グローバル障害ポリシーが Cisco UCS Manager でローカルに定義されるか、または Cisco UCS Central で定義されるかを決定します。

名前	説明
ユーザ管理（User Management）	認証およびネイティブ ドメイン、LDAP、RADIUS、TACACS+、トラスト ポイント、ロケールおよびユーザ ロールを Cisco UCS Manager でローカルに定義するか、または Cisco UCS Central で定義するかを決定します。
DNS 管理（DNS Management）	DNS サーバが Cisco UCS Manager でローカルに定義されるか、または Cisco UCS Central で定義されるかを決定します。
バックアップおよびエクスポート ポリシー（Backup & Export Policies）	フルステートバックアップ ポリシーおよびすべての構成のエクスポート ポリシーが、Cisco UCS Manager でローカルに定義されるか、または Cisco UCS Central で定義されるかを決定します。
モニタリング（Monitoring）	Call Home、Syslog、TFTP Core Exporter 設定が、Cisco UCS Manager でローカルに定義されるか、または Cisco UCS Central で定義されるかを決定します。
SEL ポリシー（SEL Policy）	SEL ポリシーが Cisco UCS Manager でローカルに定義されるか、または Cisco UCS Central で定義されるかを決定します。
電力割り当てポリシー（Power Allocation Policy）	電力割り当てポリシーが Cisco UCS Manager でローカルに定義されるか、または Cisco UCS Central で定義されるかを決定します。
Power Policy（電源ポリシー）	電源ポリシーが Cisco UCS Manager でローカルに定義されるか、または Cisco UCS Central で定義されるかを決定します。
機器ポリシー（Equipment Policy）	機器ポリシーが Cisco UCS Manager でローカルに定義されるか、または Cisco UCS Central で定義されるかを決定します。
ポート設定（Port Configuration）	ポート設定が Cisco UCS Manager でローカルに定義されるか、または Cisco UCS Central で定義されるかを決定します。

を使用した Cisco UCS Central への Cisco UCS ドメイン の登録

（注） Cisco UCS Central に登録されているドメイン内で Cisco UCS Manager が使用する IP アドレスを変更または交換することはできません。IP アドレスを変更または交換しなければならない場合は、まず Cisco UCS Central からドメインを登録解除する必要があります。IP アドレスを変更または交換した後で、Cisco UCS ドメイン を再登録できます。

はじめる前に

Cisco UCS Manager と Cisco UCS Central が同期されるようにするには、双方に NTP サーバと正しいタイム ゾーンを設定します。Cisco UCS ドメインと Cisco UCS Central の日時が同期していなければ、登録が失敗する可能性があります。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A/system # **create control-ep policy** *ucs-central*	Cisco UCS ドメイン を Cisco UCS Central に登録するために必要なポリシーを作成します。 *ucs-central* には Cisco UCS Central が導入されている仮想マシンのホスト名または IP アドレス。 を使用できます。 （注） IPv4 や IPv6 アドレスではなくホスト名を使用する場合、DNS サーバを設定する必要があります。Cisco UCS ドメイン が Cisco UCS Central に登録されていないか、または DNS 管理が [ローカル（local）] に設定されている場合は、Cisco UCS Manager で DNS サーバを設定します。Cisco UCS ドメイン Cisco UCS Central に登録されていないか、DNS 管理が [グローバル（global）] に設定されている場合は、Cisco UCS Central で DNS サーバを設定します。
ステップ 3	登録に使用する共有秘密：*shared-secret*	Cisco UCS Central を導入したときに設定した共有秘密（またはパスワード）を入力します。
ステップ 4	UCS-A/system/control-ep # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、IP アドレス 209.165.200.233 で Cisco UCS ドメイン を Cisco UCS Central システムに登録し、トランザクションをコミットする例を示します。

```
UCS-A# scope system
UCS-A /system # create control-ep policy 209.165.200.233
Shared Secret for Registration: S3cretW0rd!
UCS-A /system/control-ep* # commit-buffer
UCS-A /system/control-ep #
```

次の作業

Cisco UCS Manager と Cisco UCS Central の間にポリシー解決を設定します。

を使用した Cisco UCS Manager と Cisco UCS Central の間のポリシー解決の設定

はじめる前に

ポリシー解決を設定するには、最初に Cisco UCS ドメイン を Cisco UCS Central に登録する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A/system # **scope control-ep policy**	control-ep ポリシー モードを開始します。
ステップ 3	UCS-A/system/control-ep # **set backup-policy-ctrl source** {**local** | **global**}	フルステートバックアップ ポリシーおよびすべての構成のエクスポート ポリシーが、ローカルまたは Cisco UCS Central のどちらで定義されるかを決定します。
ステップ 4	UCS-A/system/control-ep # **set communication-policy-ctrl source** {**local** | **global**}	HTTP、CIM XML、Telnet、SNMP、Web セッション制限、管理インターフェイス モニタリング ポリシー設定を、ローカルまたは Cisco UCS Central のどちらで定義するかを決定します。
ステップ 5	UCS-A/system/control-ep # **set datetime-policy-ctrl source** {**local** | **global**}	日付と時刻がローカルで定義されるかまたは Cisco UCS Central から取得されるかを決定します。
ステップ 6	UCS-A/system/control-ep # **set dns-policy-ctrl source** {**local** | **global**}	DNS サーバがローカルまたは Cisco UCS Central のどちらで定義されるかを決定します。

	コマンドまたはアクション	目的
ステップ 7	UCS-A/system/control-ep # **set fault-policy-ctrl source** {**local** | **global**}	グローバル障害ポリシーがローカルまたは Cisco UCS Central のどちらで定義されるかを決定します。
ステップ 8	UCS-A/system/control-ep # **set infra-pack-ctrl source** {**local** | **global**}	機能カタログとインフラストラクチャ ファームウェア ポリシーが、ローカルで定義されるかまたは Cisco UCS Central から取得されるかを決定します。
ステップ 9	UCS-A/system/control-ep # **set mep-policy-ctrl source** {**local** | **global**}	管理対象エンドポイントがローカルまたは Cisco UCS Central のどちらで定義されるかを決定します。
ステップ 10	UCS-A/system/control-ep # **set monitoring-policy-ctrl source** {**local** | **global**}	Call Home、Syslog、TFTP Core Exporter 設定が、ローカルまたは Cisco UCS Central のどちらで定義されるかを決定します。
ステップ 11	UCS-A/system/control-ep # **set powermgmt-policy-ctrl source** {**local** | **global**}	電源管理がローカルまたは Cisco UCS Central のどちらで定義されるかを決定します。
ステップ 12	UCS-A/system/control-ep # **set psu-policy-ctrl source** {**local** | **global**}	電源装置がローカルまたは Cisco UCS Central のどちらで定義されるかを決定します。
ステップ 13	UCS-A/system/control-ep # **set security-policy-ctrl source** {**local** | **global**}	認証およびネイティブ ドメイン、LDAP、RADIUS、TACACS+、トラスト ポイント、ロケールおよびユーザ ロールをローカルまたは Cisco UCS Central のどちらで定義するかを決定します。
ステップ 14	UCS-A/system/control-ep # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、Cisco UCS Central に登録された Cisco UCS ドメイン にポリシー解決を設定し、トランザクションをコミットする例を示します。

```
UCS-A# scope system
UCS-A /system # scope control-ep policy
UCS-A /system/control-ep* # set backup-policy-ctrl source global
UCS-A /system/control-ep* # set communication-policy-ctrl source local
UCS-A /system/control-ep* # set datetime-policy-ctrl source global
UCS-A /system/control-ep* # set dns-policy-ctrl source global
UCS-A /system/control-ep* # set fault-policy-ctrl source global
UCS-A /system/control-ep* # set infra-pack-ctrl source global
UCS-A /system/control-ep* # set mep-policy-ctrl source global
UCS-A /system/control-ep* # set monitoring-policy-ctrl source global
UCS-A /system/control-ep* # set powermgmt-policy-ctrl source global
UCS-A /system/control-ep* # set psu-policy-ctrl source local
UCS-A /system/control-ep* # set security-policy-ctrl source global
```

```
UCS-A /system/control-ep* # commit-buffer
UCS-A /system/control-ep #
```

Cisco UCS Manager での Cisco UCS Central 登録プロパティの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope control-ep policy**	登録ポリシーを入力します。
ステップ 3	UCS-A /system/control-ep # **set cleanupmode** { | }	次のいずれかになります。 • [グローバルにローカライズする（Localize Global）]：Cisco UCS ドメイン が登録解除されると、Cisco UCS ドメイン 内のすべてのグローバル ポリシーが Cisco UCS Manager にローカライズされます。ポリシーは Cisco UCS ドメイン 内に残り、ポリシーの所有権がローカルで Cisco UCS Manager になり、Cisco UCS Manager の管理者ユーザが変更を行うことができます。 （注） Cisco UCS ドメイン を Cisco UCS Central に再登録すると、Cisco UCS Central と Cisco UCS Manager の両方にポリシーが存在するため、ポリシーの競合が起こる可能性があります。グローバル サービス プロファイルを作成して関連付ける前に、ローカル ポリシーを削除するか、ローカル ポリシーをグローバルに設定します。 • [グローバル ディープ削除（Deep Remove Global）]：このオプションは、慎重に検討してから使用してください。Cisco UCS ドメイン が登録解除されると、Cisco UCS ドメイン のすべてのグローバル ポリシーが削除されます。グローバル サービス プロファイルが存在する場合、それらのプロファイルは Cisco UCS Manager のローカル デフォルト ポリシーを参照するようになり、次のいずれかの状況になります。 ◦ ローカル デフォルト ポリシーが存在する場合、サーバは再起動します。

	コマンドまたはアクション	目的
		◦ローカル デフォルト ポリシーがない場合、サービス プロファイル関連付けは設定エラーで失敗します。 （注） グローバル ディープ削除のクリーンアップ モードでは、Cisco UCS Central からの登録解除時にグローバル VSAN および VLAN は削除されません。したがって、必要に応じて手動で削除する必要があります。
ステップ 4	UCS-A /system/control-ep # **set suspendstate on**	一時停止状態を設定します。自動的に設定されると、Cisco UCS ドメイン が Cisco UCS Central から一時的に削除され、すべてのグローバル ポリシーはローカルの同等のものに戻ります。すべてのサービス プロファイルは、現在の ID を維持します。ただし、グローバル プールは表示されなくなり、新しいサービス プロファイルからはアクセスできません。一時停止状態をオフにするには、状況を認識する必要があります。
ステップ 5	UCS-A /system/control-ep # **set ackstate acked**	Cisco UCS Manager と Cisco UCS Central の間に不一致が存在し、引き続き Cisco UCS ドメイン を Cisco UCS Central に再接続する意思があることを確認します。これは自動的に一次停止状態をオフにします。
ステップ 6	UCS-A /system/control-ep # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、Cisco UCS Central 登録クリーンアップ モードを deep-remove-global に変更して、トランザクションをコミットする方法を示しています。

```
UCS-A# scope system
UCS-A /system # scope control-ep policy
UCS-A /system/control-ep* # set cleanupmode deep-remove-global
UCS-A /system/control-ep* # commit-buffer
UCS-A /system/control-ep #
```

を使用した Cisco UCS Central からの Cisco UCS ドメインの登録解除

Cisco UCS ドメイン から Cisco UCS Central を登録解除すると、それ以降、Cisco UCS Manager はグローバル ポリシーの更新を受信しなくなります。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A/system # **delete control-ep policy**	ポリシーを削除し、Cisco UCS ドメイン を Cisco UCS Central から登録解除します。
ステップ 3	UCS-A/system # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、Cisco UCS ドメイン を Cisco UCS Central から登録解除し、トランザクションをコミットします。

```
UCS-A# scope system
UCS-A /system # delete control-ep policy
UCS-A /system* # commit-buffer
UCS-A /system #
```

第 16 章

VLAN

ネームド VLAN

ネームド VLAN は、所定の外部 LAN への接続を作成します。VLAN は、ブロードキャスト トラフィックを含む、その外部 LAN へのトラフィックを切り離します。

VLAN ID に名前を割り当てると、抽象レイヤが追加されます。これにより、ネームド VLAN を使用するサービス プロファイルに関連付けられたすべてのサーバをグローバルにアップデートすることができます。外部 LAN との通信を維持するために、サーバを個別に再設定する必要はありません。

同じ VLAN ID を使用して、複数のネームド VLAN を作成できます。たとえば、HR および Finance のビジネス サービスをホストするサーバが同一の外部 LAN にアクセスする必要がある場合、同じ VLAN ID を使用して HR と Finance という名前の VLAN を作成できます。その後でネットワークが再設定され、Finance が別の LAN に割り当てられた場合、変更する必要があるのは Finance のネームド VLAN の VLAN ID だけです。

クラスタ設定では、ネームド VLAN が 1 つのファブリック インターコネクトだけにアクセスできるようにすることも、両方のファブリック インターコネクトにアクセスできるように設定することも可能です。

VLAN ID のガイドライン

重要

ID が 4030 ～ 4047 の VLAN は作成できません。この範囲の VLAN ID は予約されています。

指定する VLAN ID は、使用しているスイッチでもサポートされている必要があります。たとえば Cisco Nexus 5000 シリーズ スイッチでは、VLAN ID 3968 ～ 4029 は予約されています。Cisco UCS Manager で VLAN ID を指定する前に、スイッチで同じ VLAN ID を使用できることを確認してください。

LAN クラウドの VLAN と SAN クラウドの FCoE VLAN の ID が同じであってはなりません。VSAN 内の VLAN と FCoE VLAN で同じ ID を使用すると、その VLAN を使用しているすべての vNIC とアップリンク ポートで重大な障害が発生し、トラフィックが中断されます。FCoE VLAN ID と重なる ID が設定されたすべての VLAN 上でイーサネット トラフィックがドロップされます。

VLAN 4048 はユーザが設定可能です。ただし、Cisco UCS Manager では、VLAN 4048 が次のデフォルト値に使用されます。4048 を VLAN に割り当てる場合は、これらの値を再設定する必要があります。

- Cisco UCS リリース 2.0 へのアップグレード後：FCoE ストレージ ポートのネイティブ VLAN は、デフォルトで VLAN 4048 を使用します。デフォルト FCoE VSAN が、アップグレード前に VLAN 1 を使用するように設定されていた場合は、使用または予約されていない VLAN ID に変更する必要があります。たとえば、デフォルトを 4049 に変更することを検討します（その VLAN ID が使用されていない場合）。
- Cisco UCS リリース 2.0 の新規インストール後：デフォルト VSAN 用の FCoE VLAN は、デフォルトで VLAN 4048 を使用します。FCoE ストレージ ポート ネイティブ VLAN は VLAN 4049 を使用します。

VLAN 名の大文字と小文字は区別されます。

プライベート VLAN

プライベート VLAN（PVLAN）は、VLAN のイーサネット ブロードキャスト ドメインをサブドメインに分割する機能で、これを使用して一部のポートを分離することができます。PVLAN の各サブドメインには、1 つのプライマリ VLAN と 1 つ以上のセカンダリ VLAN が含まれます。PVLAN のすべてのセカンダリ VLAN は、同じプライマリ VLAN を共有する必要があります。セカンダリ VLAN ID は、各サブドメインの区別に使用されます。

独立 VLAN とコミュニティ VLAN

Cisco UCS ドメイン 内のすべてのセカンダリ VLAN は、独立 VLAN またはコミュニティ VLAN になることができます。

（注） 独立 VLAN を標準 VLAN と共に使用するよう設定することはできません。

独立 VLAN のポート

独立 VLAN の通信では、プライマリ VLAN 内の関連するポートだけを使用できます。これらのポートは独立ポートであり、Cisco UCS Manager では設定できません。プライマリ VLAN には 1 つの独立 VLAN しか存在できませんが、同じ独立 VLAN 上に複数の独立ポートが存在することは可能です。これらの独立ポートは相互に通信できません。独立ポートは、独立 VLAN を許可している標準トランク ポートまたは無差別ポートとのみ通信できます。

独立ポートは、独立セカンダリ VLAN に属しているホスト ポートです。このポートは、同じプライベート VLAN ドメイン内の他のポートから完全に独立しています。PVLAN は、無差別ポートからのトラフィックを除き、独立ポート宛のトラフィックをすべてブロックします。独立ポートから受信されたトラフィックは、無差別ポートにだけ転送されます。指定した独立 VLAN には、複数の独立ポートを含めることができます。各ポートは、独立 VLAN にある他のすべてのポートから、完全に隔離されています。

アップリンク ポートに関するガイドライン

PVLAN を作成する場合は、次のガイドラインに従ってください。

- アップリンク イーサネット ポート チャネルを無差別モードにすることはできません。
- 各プライマリ VLAN には、独立 VLAN が 1 つだけ存在できます。
- VNTAG アダプタの VIF には、独立 VLAN が 1 つだけ存在できます。

VLAN ID のガイドライン

重要 ID が 4030 ～ 4047 の VLAN は作成できません。この範囲の VLAN ID は予約されています。

指定する VLAN ID は、使用しているスイッチでもサポートされている必要があります。たとえば Cisco Nexus 5000 シリーズ スイッチでは、VLAN ID 3968 ～ 4029 は予約されています。Cisco UCS Manager で VLAN ID を指定する前に、スイッチで同じ VLAN ID を使用できることを確認してください。

LAN クラウドの VLAN と SAN クラウドの FCoE VLAN の ID が同じであってはなりません。VSAN 内の VLAN と FCoE VLAN で同じ ID を使用すると、その VLAN を使用しているすべての vNIC とアップリンク ポートで重大な障害が発生し、トラフィックが中断されます。FCoE VLAN ID と重なる ID が設定されたすべての VLAN 上でイーサネット トラフィックがドロップされます。

VLAN 4048 はユーザが設定可能です。ただし、Cisco UCS Manager では、VLAN 4048 が次のデフォルト値に使用されます。4048 を VLAN に割り当てる場合は、これらの値を再設定する必要があります。

- Cisco UCS リリース 2.0 へのアップグレード後：FCoE ストレージ ポートのネイティブ VLAN は、デフォルトで VLAN 4048 を使用します。デフォルト FCoE VSAN が、アップグレード前に VLAN 1 を使用するように設定されていた場合は、使用または予約されていない VLAN ID に変更する必要があります。たとえば、デフォルトを 4049 に変更することを検討します（その VLAN ID が使用されていない場合）。
- Cisco UCS リリース 2.0 の新規インストール後：デフォルト VSAN 用の FCoE VLAN は、デフォルトで VLAN 4048 を使用します。FCoE ストレージ ポート ネイティブ VLAN は VLAN 4049 を使用します。

VLAN 名の大文字と小文字は区別されます。

VLAN ポートの制限

Cisco UCS Manager では、1 つのファブリック インターコネクト上の境界ドメインとサーバ ドメインで設定可能な VLAN ポート インスタンスの数は制限されます。

VLAN ポート数に含まれるポートのタイプ

次のタイプのポートが VLAN ポートの計算でカウントされます。

- ボーダー アップリンク イーサネット ポート
- ボーダー アップリンク イーサチャネル メンバー ポート
- SAN クラウドの FCoE ポート
- NAS クラウドのイーサネット ポート
- サービス プロファイルによって作成されたスタティックおよびダイナミック vNIC
- ハイパーバイザ ドメイン内のハイパーバイザのポート プロファイルの一部として作成された VM vNIC

これらのポートに設定されている VLAN の数に基づいて、Cisco UCS Manager は VLAN ポート インスタンスの累積数を追跡し、検証中に VLAN ポート制限を実行します。Cisco UCS Manager は、制御トラフィック用に事前定義されたいくつかの VLAN ポート リソースを予約します。これには、HIF および NIF ポートに設定された管理 VLAN が含まれます。

VLAN ポートの制限の実行

Cisco UCS Manager は、次の操作中に VLAN ポートのアベイラビリティを検証します。

- 境界ポートおよび境界ポート チャネルの設定および設定解除
- クラウドへの VLAN の追加またはクラウドからの VLAN の削除

- SAN または NAS ポートの設定または設定解除
- 設定の変更を含むサービス プロファイルの関連付けまたは関連付け解除
- vNIC または vHBA での VLAN の設定または設定解除
- VMWare vNIC からおよび ESX ハイパーバイザから作成通知または削除通知を受け取ったとき

（注） これは Cisco UCS Manager の制御の範囲外です。

- ファブリック インターコネクトのリブート
- Cisco UCS Manager のアップグレードまたはダウングレード

Cisco UCS Manager は、サービス プロファイルの動作に対し、厳密に VLAN ポート制限を実施します。VLAN ポート制限を超過したことを Cisco UCS Manager が検出した場合、サービス プロファイル設定は展開時に失敗します。

境界ドメインでの VLAN ポート数の超過は、それほど混乱をもたらしません。境界ドメインで VLAN ポート数が超過すると、Cisco UCS Manager は割り当てステータスを [超過（Exceeded）] に変更します。ステータスを [使用可能（Available）] に戻すには、次のいずれかのアクションを実行します。

- 1 つ以上の境界ポートを設定解除する
- LAN クラウドから VLAN を削除する
- 1 つ以上の vNIC または vHBA を設定解除する

ネームド VLAN の設定

両方のファブリックインターコネクトにアクセス可能なネームドVLANの作成（アップリンク イーサネット モード）

重要

ID が 4030 ～ 4047 の VLAN は作成できません。この範囲の VLAN ID は予約されています。

指定する VLAN ID は、使用しているスイッチでもサポートされている必要があります。たとえば Cisco Nexus 5000 シリーズ スイッチでは、VLAN ID 3968 ～ 4029 は予約されています。Cisco UCS Manager で VLAN ID を指定する前に、スイッチで同じ VLAN ID を使用できることを確認してください。

LAN クラウドの VLAN と SAN クラウドの FCoE VLAN の ID が同じであってはなりません。VSAN 内の VLAN と FCoE VLAN で同じ ID を使用すると、その VLAN を使用しているすべての vNIC とアップリンク ポートで重大な障害が発生し、トラフィックが中断されます。FCoE VLAN ID と重なる ID が設定されたすべての VLAN 上でイーサネット トラフィックがドロップされます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **create vlan** *vlan-name vlan-id*	ネームド VLAN を作成し、VLAN 名と VLAN ID を指定し、イーサネットアップリンク VLANモードを開始します。 VLAN 名の大文字と小文字は区別されます。
ステップ 3	UCS-A /eth-uplink/fabric/vlan # **set sharing** {**isolated** | **none** | **primary**}	指定した VLAN の共有を設定します。 次のいずれかになります。 • **isolated**：これはプライマリ VLAN に関連付けられたセカンダリ VLAN です。この VLAN はプライベートです。 • **none**：この VLAN にセカンダリまたはプライベート VLAN はありません。 • **primary**：この VLAN には、1 つ以上のセカンダリ VLAN を設定できます。

	コマンドまたはアクション	目的
ステップ 4	UCS-A /eth-uplink/vlan # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、両方のファブリック インターコネクト用にネームド VLAN を作成し、VLAN に accounting という名前を付け、VLAN ID 2112 を割り当て、共有を none に設定し、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # create vlan accounting 2112
UCS-A /eth-uplink/vlan* # set sharing none
UCS-A /eth-uplink/vlan* # commit-buffer
UCS-A /eth-uplink/vlan #
```

両方のファブリックインターコネクトにアクセス可能なネームド VLAN の作成（イーサネット ストレージ モード）

重要 ID が 4030 ～ 4047 の VLAN は作成できません。この範囲の VLAN ID は予約されています。

指定する VLAN ID は、使用しているスイッチでもサポートされている必要があります。たとえば Cisco Nexus 5000 シリーズ スイッチでは、VLAN ID 3968 ～ 4029 は予約されています。Cisco UCS Manager で VLAN ID を指定する前に、スイッチで同じ VLAN ID を使用できることを確認してください。

LAN クラウドの VLAN と SAN クラウドの FCoE VLAN の ID が同じであってはなりません。VSAN 内の VLAN と FCoE VLAN で同じ ID を使用すると、その VLAN を使用しているすべての vNIC とアップリンク ポートで重大な障害が発生し、トラフィックが中断されます。FCoE VLAN ID と重なる ID が設定されたすべての VLAN 上でイーサネット トラフィックがドロップされます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-storage**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A /eth-storage # **create vlan** *vlan-name vlan-id*	ネームド VLAN を作成し、VLAN 名と VLAN ID を指定し、イーサネット ストレージ VLAN モードを開始します。 VLAN 名の大文字と小文字は区別されます。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /eth-storage/vlan # **create member-port** {**a** | **b**} *slot-id port-id*	指定したファブリック上に指定したVLANのメンバ ポートを作成します。
ステップ 4	UCS-A /eth-storage/vlan/member-port # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、両方のファブリック インターコネクト用にネームド VLAN を作成し、VLAN に accouonting という名前を付け、VLAN ID 2112 を割り当て、スロット 2、ポート 20 にメンバ ポートを作成し、トランザクションをコミットします。

```
UCS-A# scope eth-storage
UCS-A /eth-storage # create vlan accounting 2112
UCS-A /eth-storage/vlan* # create member-port a 2 20
UCS-A /eth-storage/vlan/member-port* # commit-buffer
UCS-A /eth-storage/vlan/member-port #
```

1つのファブリックインターコネクトにアクセス可能なネームドVLANの作成（アップリンク イーサネット モード）

重要 ID が 4030 ～ 4047 の VLAN は作成できません。この範囲の VLAN ID は予約されています。

指定する VLAN ID は、使用しているスイッチでもサポートされている必要があります。たとえば Cisco Nexus 5000 シリーズ スイッチでは、VLAN ID 3968 ～ 4029 は予約されています。Cisco UCS Manager で VLAN ID を指定する前に、スイッチで同じ VLAN ID を使用できることを確認してください。

LAN クラウドの VLAN と SAN クラウドの FCoE VLAN の ID が同じであってはなりません。VSAN 内の VLAN と FCoE VLAN で同じ ID を使用すると、その VLAN を使用しているすべての vNIC とアップリンク ポートで重大な障害が発生し、トラフィックが中断されます。FCoE VLAN ID と重なる ID が設定されたすべての VLAN 上でイーサネット トラフィックがドロップされます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope fabric** {**a** | **b**}	指定したファブリック インターコネクト（A または B）のイーサネット アップリンク ファブリック インターコネクト モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /eth-uplink/fabric # **create vlan** *vlan-name vlan-id*	ネームド VLAN を作成し、VLAN 名と VLAN ID を指定し、イーサネットアップリンク ファブリック インターコネクト VLAN モードを開始します。 VLAN 名の大文字と小文字は区別されます。
ステップ 4	UCS-A /eth-uplink/fabric/vlan # **set sharing** {**isolated** | **none** | **primary**}	指定した VLAN の共有を設定します。 次のいずれかになります。 • **isolated**：これはプライマリ VLAN に関連付けられたセカンダリ VLAN です。この VLAN はプライベートです。 • **none**：この VLAN にセカンダリまたはプライベート VLAN はありません。 • **primary**：この VLAN には、1 つ以上のセカンダリ VLAN を設定できます。
ステップ 5	UCS-A /eth-uplink/fabric/vlan # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、ファブリック インターコネクト A のネームド VLAN を作成し、VLAN に finance という名前を付け、VLAN ID 3955 を割り当て、共有を none に設定し、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # create vlan finance 3955
UCS-A /eth-uplink/fabric/vlan* # set sharing none
UCS-A /eth-uplink/fabric/vlan* # commit-buffer
UCS-A /eth-uplink/fabric/vlan #
```

1つのファブリックインターコネクトにアクセス可能なネームドVLANの作成（イーサネット ストレージ モード）

重要 ID が 4030 ～ 4047 の VLAN は作成できません。この範囲の VLAN ID は予約されています。

指定する VLAN ID は、使用しているスイッチでもサポートされている必要があります。たとえば Cisco Nexus 5000 シリーズ スイッチでは、VLAN ID 3968 ～ 4029 は予約されています。Cisco UCS Manager で VLAN ID を指定する前に、スイッチで同じ VLAN ID を使用できることを確認してください。

LAN クラウドの VLAN と SAN クラウドの FCoE VLAN の ID が同じであってはなりません。VSAN 内の VLAN と FCoE VLAN で同じ ID を使用すると、その VLAN を使用しているすべての vNIC とアップリンク ポートで重大な障害が発生し、トラフィックが中断されます。FCoE VLAN ID と重なる ID が設定されたすべての VLAN 上でイーサネット トラフィックがドロップされます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-storage**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A /eth-storage # **scope fabric** {**a** | **b**}	指定したファブリック インターコネクトのイーサネット ストレージ ファブリック インターコネクト モードを開始します。
ステップ 3	UCS-A /eth-storage/fabric # **create vlan** *vlan-name vlan-id*	ネームド VLAN を作成し、VLAN 名と VLAN ID を指定し、イーサネット ストレージ ファブリック インターコネクト VLAN モードを開始します。 VLAN 名の大文字と小文字は区別されます。
ステップ 4	UCS-A /eth-storage/vlan # **create member-port** {**a** | **b**} *slot-id port-id*	指定したファブリック上に指定した VLAN のメンバ ポートを作成します。
ステップ 5	UCS-A /eth-storage/fabric/vlan/member-port # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、ファブリック インターコネクト A のネームド VLAN を作成し、VLAN に finance という名前を付け、VLAN ID 3955 を割り当て、スロット 2、ポート 20 にメンバ ポートを作成し、トランザクションをコミットします。

```
UCS-A# scope eth-storage
UCS-A /eth-storage # scope fabric a
```

```
UCS-A /eth-storage/fabric # create vlan finance 3955
UCS-A /eth-storage/fabric/vlan* # create member-port a 2 20
UCS-A /eth-storage/fabric/vlan/member-port* # commit-buffer
UCS-A /eth-storage/fabric/vlan/member-port #
```

ネームド VLAN の削除

Cisco UCS Manager に、削除する VLAN と同じ VLAN ID を持つネームド VLAN が含まれている場合、この ID を持つネームド VLAN がすべて削除されるまで、この VLAN はファブリック インターコネクト設定から削除されません。

プライベート プライマリ VLAN を削除する場合は、必ずセカンダリ VLAN を動作している別のプライマリ VLAN にセカンダリ VLAN を再割り当てします。

はじめる前に

ファブリック インターコネクトから VLAN を削除する前に、その VLAN がすべての vNIC と vNIC テンプレートから削除されていることを確認します。

（注） vNIC または vNIC テンプレートに割り当てられている VLAN を削除すると、vNIC によって VLAN がフラップする場合があります。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope fabric**{**a** | **b**}	（任意） イーサネット アップリンク ファブリック モードを開始します。指定されたファブリック（a または b）からだけネームド VLAN 削除するには、このコマンドを使用します。
ステップ 3	UCS-A /eth-uplink # **delete vlan** *vlan-name*	指定されたネームド VLAN を削除します。
ステップ 4	UCS-A /eth-uplink # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、両方のファブリック インターコネクトにアクセス可能なネームド VLAN を削除し、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # delete vlan accounting
UCS-A /eth-uplink* # commit-buffer
```

```
UCS-A /eth-uplink #
```

次の例は、1 つのファブリック インターコネクトにアクセス可能なネームド VLAN を削除し、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # delete vlan finance
UCS-A /eth-uplink/fabric* # commit-buffer
UCS-A /eth-uplink/fabric #
```

プライベート VLAN の設定

プライベート VLAN 用プライマリ VLAN の作成（両方のファブリック インターコネクトにアクセス可能）

重要

ID が 4030 ～ 4047 の VLAN は作成できません。この範囲の VLAN ID は予約されています。

指定する VLAN ID は、使用しているスイッチでもサポートされている必要があります。たとえば Cisco Nexus 5000 シリーズ スイッチでは、VLAN ID 3968 ～ 4029 は予約されています。Cisco UCS Manager で VLAN ID を指定する前に、スイッチで同じ VLAN ID を使用できることを確認してください。

LAN クラウドの VLAN と SAN クラウドの FCoE VLAN の ID が同じであってはなりません。VSAN 内の VLAN と FCoE VLAN で同じ ID を使用すると、その VLAN を使用しているすべての vNIC とアップリンク ポートで重大な障害が発生し、トラフィックが中断されます。FCoE VLAN ID と重なる ID が設定されたすべての VLAN 上でイーサネット トラフィックがドロップされます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **create vlan** *vlan-name vlan-id*	ネームド VLAN を作成し、VLAN 名と VLAN ID を指定し、イーサネット アップリンク VLAN モードを開始します。 VLAN 名の大文字と小文字は区別されます。
ステップ 3	UCS-A /eth-uplink/vlan # **set sharing primary**	VLAN をプライマリ VLAN として設定します。

	コマンドまたはアクション	目的
ステップ 4	UCS-A /eth-uplink/vlan # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、両方のファブリック インターコネクト用にネームド VLAN を作成し、VLAN に accounting という名前を付け、VLAN ID 2112 を割り当て、この VLAN をプライマリ VLAN にし、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # create vlan accounting 2112
UCS-A /eth-uplink/vlan* # set sharing primary
UCS-A /eth-uplink/vlan* # commit-buffer
UCS-A /eth-uplink/vlan #
```

プライベート VLAN 用プライマリ VLAN の作成（1 つのファブリック インターコネクトにアクセス可能）

重要 ID が 4030 ～ 4047 の VLAN は作成できません。この範囲の VLAN ID は予約されています。

指定する VLAN ID は、使用しているスイッチでもサポートされている必要があります。たとえば Cisco Nexus 5000 シリーズ スイッチでは、VLAN ID 3968 ～ 4029 は予約されています。Cisco UCS Manager で VLAN ID を指定する前に、スイッチで同じ VLAN ID を使用できることを確認してください。

LAN クラウドの VLAN と SAN クラウドの FCoE VLAN の ID が同じであってはなりません。VSAN 内の VLAN と FCoE VLAN で同じ ID を使用すると、その VLAN を使用しているすべての vNIC とアップリンク ポートで重大な障害が発生し、トラフィックが中断されます。FCoE VLAN ID と重なる ID が設定されたすべての VLAN 上でイーサネット トラフィックがドロップされます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope fabric** {**a** | **b**}	指定したファブリック インターコネクトのイーサネット アップリンク ファブリック インターコネクト モードを開始します。
ステップ 3	UCS-A /eth-uplink/fabric # **create vlan** *vlan-name vlan-id*	ネームド VLAN を作成し、VLAN 名と VLAN ID を指定し、イーサネット アップリンク ファ

	コマンドまたはアクション	目的
		ブリック インターコネクト VLAN モードを開始します。 VLAN 名の大文字と小文字は区別されます。
ステップ 4	UCS-A /eth-uplink/fabric/vlan # **set sharing primary**	VLAN をプライマリ VLAN として設定します。
ステップ 5	UCS-A /eth-uplink/fabric/vlan # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、ファブリック インターコネクト A 用にネームド VLAN を作成し、VLAN に finance という名前を付け、VLAN ID 3955 を割り当て、この VLAN をプライマリ VLAN にし、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # create vlan finance 3955
UCS-A /eth-uplink/fabric/vlan* # set sharing primary
UCS-A /eth-uplink/fabric/vlan* # commit-buffer
UCS-A /eth-uplink/fabric/vlan #
```

プライベート VLAN 用セカンダリ VLAN の作成（両方のファブリック インターコネクトにアクセス可能）

重要 ID が 4030 ～ 4047 の VLAN は作成できません。この範囲の VLAN ID は予約されています。

指定する VLAN ID は、使用しているスイッチでもサポートされている必要があります。たとえば Cisco Nexus 5000 シリーズ スイッチでは、VLAN ID 3968 ～ 4029 は予約されています。Cisco UCS Manager で VLAN ID を指定する前に、スイッチで同じ VLAN ID を使用できることを確認してください。

LAN クラウドの VLAN と SAN クラウドの FCoE VLAN の ID が同じであってはなりません。VSAN 内の VLAN と FCoE VLAN で同じ ID を使用すると、その VLAN を使用しているすべての vNIC とアップリンク ポートで重大な障害が発生し、トラフィックが中断されます。FCoE VLAN ID と重なる ID が設定されたすべての VLAN 上でイーサネット トラフィックがドロップされます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **create vlan** *vlan-name vlan-id*	ネームド VLAN を作成し、VLAN 名と VLAN ID を指定し、イーサネット アップリンク VLAN モードを開始します。 VLAN 名の大文字と小文字は区別されます。
ステップ 3	UCS-A /eth-uplink/vlan # **set sharing isolated**	VLAN をセカンダリ VLAN として設定します。
ステップ 4	UCS-A /eth-uplink/vlan # **set pubnwname** *primary-vlan-name*	このセカンダリ VLAN に関連付けられているプライマリ VLAN を指定します。
ステップ 5	UCS-A /eth-uplink/vlan # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、両方のファブリック インターコネクト用のネームド VLAN を作成し、VLAN に accounting という名前を付け、VLAN ID 2112 を割り当て、この VLAN をセカンダリ VLAN として、セカンダリ VLAN をプライマリ VLAN と関連付け、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # create vlan accounting 2112
UCS-A /eth-uplink/vlan* # set sharing isolated
UCS-A /eth-uplink/vlan* # set pubnwname pvlan1000
UCS-A /eth-uplink/vlan* # commit-buffer
UCS-A /eth-uplink/vlan #
```

プライベート VLAN 用セカンダリ VLAN の作成（1 つのファブリック インターコネクトにアクセス可能）

重要 ID が 4030 ～ 4047 の VLAN は作成できません。この範囲の VLAN ID は予約されています。

指定する VLAN ID は、使用しているスイッチでもサポートされている必要があります。たとえば Cisco Nexus 5000 シリーズ スイッチでは、VLAN ID 3968 ～ 4029 は予約されています。Cisco UCS Manager で VLAN ID を指定する前に、スイッチで同じ VLAN ID を使用できることを確認してください。

LAN クラウドの VLAN と SAN クラウドの FCoE VLAN の ID が同じであってはなりません。VSAN 内の VLAN と FCoE VLAN で同じ ID を使用すると、その VLAN を使用しているすべての vNIC とアップリンク ポートで重大な障害が発生し、トラフィックが中断されます。FCoE VLAN ID と重なる ID が設定されたすべての VLAN 上でイーサネット トラフィックがドロップされます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope fabric** {**a** | **b**}	指定したファブリック インターコネクト（A または B）のイーサネット アップリンク ファブリック インターコネクト モードを開始します。
ステップ 3	UCS-A /eth-uplink/fabric # **create vlan** *vlan-name vlan-id*	ネームド VLAN を作成し、VLAN 名と VLAN ID を指定し、イーサネット アップリンク ファブリック インターコネクト VLAN モードを開始します。 VLAN 名の大文字と小文字は区別されます。
ステップ 4	UCS-A /eth-uplink/vlan # **set sharing isolated**	VLAN をセカンダリ VLAN として設定します。
ステップ 5	UCS-A /eth-uplink/vlan # **set pubnwname** *primary-vlan-name*	このセカンダリ VLAN に関連付けられているプライマリ VLAN を指定します。
ステップ 6	UCS-A /eth-uplink/fabric/vlan/member-port # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、ファブリック インターコネクト A 用のネームド VLAN を作成し、VLAN に finance という名前を付け、VLAN ID 3955 を割り当て、この VLAN をセカンダリ VLAN として、セカンダリ VLAN をプライマリ VLAN と関連付け、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # create vlan finance 3955
UCS-A /eth-uplink/fabric/vlan* # set sharing isolated
UCS-A /eth-uplink/fabric/vlan* # set pubnwname pvlan1000
UCS-A /eth-uplink/fabric/vlan* # commit-buffer
UCS-A /eth-uplink/fabric/vlan #
```

コミュニティ VLAN

Cisco UCS Manager は、UCS ファブリック インターコネクトのコミュニティ VLAN をサポートします。コミュニティ ポートは、コミュニティ ポート同士、および無差別ポートと通信します。コミュニティ ポートは、他のコミュニティの他のすべてのポート、または PVLAN 内の独立ポートからレイヤ 2 分離されています。ブロードキャストは PVLAN だけに関連付けられたコミュニティ ポートと他の無差別ポート間で送信されます。無差別ポートは、PVLAN 内の独立ポート、コミュニティ ポートなどのすべてのインターフェイスと通信できます。

コミュニティ VLAN の作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**.	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A# /eth-uplink/ # **create vlan** *ID*.	指定した VLAN ID を持つ VLAN を作成します。
ステップ 3	UCS-A# /eth-uplink/ vlan # **set sharing** *Type*.	VLAN タイプを指定します。
ステップ 4	UCS-A# /eth-uplink/ vlan # **set pubnwname** *Name*.	プライマリ VLAN の関連付けを指定します。
ステップ 5	UCS-A# /eth-uplink/ vlan # **commit-buffer**.	トランザクションをシステム設定にコミットします。

次の例は、コミュニティ VLAN の作成方法を示しています。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # create vlan vlan203 203
UCS-A /eth-uplink/vlan* # set sharing community
UCS-A /eth-uplink/vlan* # set pubname vlan200
UCS-A /eth-uplink/vlan* # commit-buffer
```

```
UCS-A /eth-uplink/vlan* # exit
UCS-A /vlan-group #
```

vNIC でのコミュニティ VLAN の許可

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルート組織モードを開始するには、/ を *org-name* として入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	トランザクションをシステム設定にコミットします。
ステップ 3	UCS-A /org/service-profile # **scope vnic** *vnic-name*	指定された vNIC のコマンド モードを開始します。
ステップ 4	UCS-A /org/service-profile/vnic # **create eth-if** *community-vlan-name*	コミュニティ VLAN が指定の vNIC へアクセスすることを可能にします。
ステップ 5	UCS-A /org/service-profile/vnic # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、コミュニティ VLAN cVLAN101 を vNIC vnic_1 を割り当て、トランザクションをコミットする方法の例を示します。

```
UCS-A# scope org /
UCS-A /org # scope service-profile GSP1
UCS-A /org/service-profile # scope vnic vnic_1
UCS-A /org/service-profile/vnic # create eth-if cVLAN101
UCS-A /org/service-profile/vnic* # commit-buffer
```

無差別アクセス ポートまたはトランク ポートでの PVLAN の許可

無差別アクセス ポートでは、隔離された VLAN とコミュニティ VLAN は同じプライマリ VLAN に関連付ける必要があります。

無差別トランク ポートでは、異なるプライマリ VLAN に属する隔離 VLAN やコミュニティ VLAN が、普通の VLAN 同様に許容されます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope eth-storage**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A /eth-storage # **scope vlan** *iso-vlan-name*	指定された隔離 VLAN を入力します。
ステップ 3	UCS-A /eth-storage/vlan # **create member-port** *fabric slot- num port-num*	指定したファブリックのメンバポートを作成し、スロット番号、およびポート番号を割り当て、メンバポートの設定範囲に入ります。
ステップ 4	UCS-A /eth-storage/vlan/member-port # **exit**	VLAN モードに戻ります。
ステップ 5	UCS-A /eth-storage/vlan # **exit**	イーサネット ストレージ モードに戻ります。
ステップ 6	UCS-A /eth-storage # **scope vlan** *comm-vlan-name*	指定されたコミュニティ VLAN を入力します。
ステップ 7	UCS-A /eth-storage/vlan # **create member-port** *fabric slot- num port-num*	指定したファブリックのメンバポートを作成し、スロット番号、およびポート番号を割り当て、メンバポートの設定範囲に入ります。
ステップ 8	UCS-A /eth-storage/vlan/member-port # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、同じプライマリ VLAN に関連付けられた隔離 VLAN とコミュニティ VLAN を同じアプライアンス ポートに割り当て、トランザクションをコミットする方法の例を示します。

```
UCS-A# scope eth-storage
UCS-A /eth-storage # scope vlan isovlan501
UCS-A /eth-storage/vlan # create member-port a 1 2
UCS-A /eth-storage/vlan/member-port* # exit
UCS-A /eth-storage/vlan* # exit
UCS-A /eth-storage* # scope vlan cvlan502
UCS-A /eth-storage/vlan* # create member-port a 1 2
UCS-A /eth-storage/vlan/member-port* # commit-buffer
UCS-A /eth-storage/vlan/member-port #
```

コミュニティ VLAN の削除

Cisco UCS Manager に、削除する VLAN と同じ VLAN ID を持つネームド VLAN が含まれている場合、この ID を持つネームド VLAN がすべて削除されるまで、この VLAN はファブリック インターコネクト設定から削除されません。

プライベート プライマリ VLAN を削除する場合は、必ずセカンダリ VLAN を動作している別のプライマリ VLAN にセカンダリ VLAN を再割り当てします。

はじめる前に

ファブリック インターコネクトから VLAN を削除する前に、その VLAN がすべての vNIC と vNIC テンプレートから削除されていることを確認します。

（注） vNIC または vNIC テンプレートに割り当てられている VLAN を削除すると、vNIC によって VLAN がフラップする場合があります。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope fabric**{**a** | **b**}	（任意） イーサネット アップリンク ファブリック モードを開始します。指定されたファブリック（a または b）からだけネームド VLAN 削除するには、このコマンドを使用します。
ステップ 3	UCS-A /eth-uplink # **delete community vlan** *vlan-name*	指定されたコミュニティ VLAN を削除します。
ステップ 4	UCS-A /eth-uplink # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、コミュニティ VLAN を削除し、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # delete commnity vlan vlan203
UCS-A /eth-uplink* # commit-buffer
UCS-A /eth-uplink #
```

VLAN ポート数の表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fabric-interconnect** {**a** | **b**}	指定したファブリック インターコネクトのファブリック インターコネクト モードを開始します。
ステップ 2	UCS-A /fabric-interconnect # **show vlan-port-count**	VLAN ポート数を表示します。

次に、ファブリック インターコネクト A の VLAN ポート数を表示する例を示します。

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect # show vlan-port-count

VLAN-Port Count:
VLAN-Port Limit     Access VLAN-Port Count     Border VLAN-Port Count     Alloc Status
----------          ----------------           ----------------           ----------
6000                        3                          0                      Available
```

VLAN ポート数の最適化

VLAN ポート数の最適化を使用すると、複数の VLAN の状態を単一の内部状態にマッピングできます。VLAN ポート数の最適化を有効にすると、Cisco UCS Manager は、ポート VLAN メンバーシップに基づいて VLAN を論理的にグループ化します。このグループ化により、ポート VLAN 数の制限が増加します。VLAN ポート数の最適化によりさらに VLAN 状態が圧縮され、ファブリック インターコネクトの CPU の負荷が減少します。この CPU 負荷の減少により、より多くの VLAN をより多くの vNIC に展開できるようになります。VLAN のポート数を最適化しても、vNIC 上の既存の VLAN 設定は変更されません。

VLAN ポート数の最適化は、デフォルトで無効になっています。このオプションは、必要に応じて有効または無効にできます。

重要

- VLAN ポート数の最適化を有効にすると、使用可能な VLAN ポートの数が増加します。最適化されていない状態でポート VLAN 数が VLAN の最大数を超えた場合、VLAN ポート数の最適化を無効にすることはできません。
- VLAN ポート数の最適化は、Cisco UCS 6100 シリーズ ファブリック インターコネクトではサポートされていません。

ポート VLAN 数の最適化のイネーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネットアップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink# **set vlan-port-count-optimization enable**	VLAN ポート数の最適化に対し vlan をイネーブルにします。
ステップ 3	UCS-A /eth-uplink* # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、VLAN ポート数の最適化をイネーブルにする方法を示します。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # set vlan-port-count-optimization enable
UCS-A /eth-uplink* # commit-buffer
UCS-A /eth-uplink#
```

ポート VLAN 数最適化のディセーブル化

ポート VLAN 数が最適化されていない状態で使用可能な上限数よりも多くのポート VLAN がある場合、最適化をディセーブルにできません。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink# **set vlan-port-count-optimization disable**	ポート VLAN 数の最適化をディセーブルにします。
ステップ 3	UCS-A /eth-uplink # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、ポート VLAN 数の最適化をディセーブルにする方法を示します。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # set vlan-port-count-optimization disable
UCS-A /eth-uplink* # commit-buffer
UCS-A /eth-uplink#
```

ポート VLAN 数最適化グループの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink# **show vlan-port-count-optimization group**	ポート VLAN 数最適化グループの VLAN を表示します。

次の例では、ファブリック a および b のポート VLAN 数最適化グループを表示します。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # show vlan-port-count-optimization group
VLAN Port Count Optimization Group:
    Fabric ID  Group ID   VLAN ID
    ---------  --------   -------
    A          5          6
    A          5          7
    A          5          8
    B          10         100
    B          10         101
```

VLAN グループ

VLAN グループを使用すると、イーサネット アップリンク ポート上の VLAN を機能別または特定のネットワークに属する VLAN 別にグループ化することができます。VLAN メンバーシップを定義し、そのメンバーシップをファブリック インターコネクト上の複数のイーサネット アップリンク ポートに適用することができます。

（注） Cisco UCS Manager では、最大 200 個の VLAN グループをサポートします。200 を超える VLAN グループを作成していると Cisco UCS Manager で判別すると、VLAN の圧縮をディセーブルにします。

インバンドおよびアウトオブバンド（OOB）VLAN グループを設定し、それを使用してブレードおよびラック サーバの Cisco Integrated Management Interface（CIMC）にアクセスすることができます。Cisco UCS Manager は、アップリンク インターフェイスまたはアップリンク ポート チャネルでの OOB IPv4 およびインバンド IPv4/IPv6 VLAN グループの使用をサポートします。

VLAN を VLAN グループに割り当てた後、VLAN グループに対する変更は VLAN グループで設定されたすべてのイーサネット アップリンク ポートに適用されます。また、VLAN グループによって、分離 VLAN 間での VLAN の重複を識別することができます。

VLAN グループ下にアップリンク ポートを設定できます。VLAN グループ用のアップリンク ポートを設定すると、そのアップリンク ポートはそのグループ内のすべての VLAN のみをサポートします。

LAN クラウドまたは LAN アップリンク マネージャから VLAN グループを作成できます。

VLAN グループの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**.	イーサネット アップリンク モードを開始します。 VLAN グループ名では、大文字と小文字が区別されます。
ステップ 2	UCS-A# /eth-uplink/ #**create vlan-group***Name*.	指定された名前で VLAN グループを作成します。 この名前には、1 ～ 32 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
ステップ 3	UCS-A# /eth-uplink/ vlan-group#**create member-vlan***ID*.	作成された VLAN グループに指定した VLAN を追加します。
ステップ 4	UCS-A# /eth-uplink/vlan-group #**create member-port** [member-port-channel] .	VLAN グループにアップリンク イーサネット ポートを割り当てます。
ステップ 5	UCS-A#/vlan-group* # **commit-buffer**.	トランザクションをシステム設定にコミットします。

次に、VLAN グループを作成する例を示します。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # create vlan-group eng
UCS-A /eth-uplink/vlan-group* # create member-vlan 3
UCS-A /eth-uplink/vlan-group* # commit-buffer
UCS-A /vlan-group #
```

インバンド VLAN グループの作成

インバンド VLAN グループを設定し、リモート ユーザにインバンド サービス プロファイルを介したアクセスを提供します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth uplink**	イーサネット アップリンク コンフィギュレーション モードを開始します。
ステップ 2	UCS-A /eth-uplink # **create vlan-group** *inband-vlan-name*	VLAN グループを指定された名前で作成し、VLAN グループ コンフィギュレーション モードを開始します。
ステップ 3	UCS-A /eth-uplink/vlan-group # **create member-vlan***inband-vlan-nameinband-vlan-id*	指定した VLAN を VLAN グループに追加し、VLAN グループ メンバ コンフィギュレーション モードを開始します。
ステップ 4	UCS-A /eth-uplink/vlan-group/member-vlan # **exit**	VLAN グループ メンバ コンフィギュレーション モードを終了します。
ステップ 5	UCS-A /eth-uplink/vlan-group # **create member-port***fabricslot-numport-num*	指定したファブリックのメンバ ポートを作成し、スロット番号、およびポート番号を割り当て、メンバ ポートの設定を開始します。
ステップ 6	UCS-A /eth-uplink/vlan-group/member-port # **commit-buffer**	トランザクションをコミットします。

次の例では、inband-vlan-group という名前の VLAN グループを作成し、Inband_VLAN という名前のグループ メンバを作成し、VLAN ID 888 を割り当て、ファブリック A とファブリック B のメンバ ポートを作成し、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # create vlan-group inband-vlan-group
UCS-A /eth-uplink/vlan-group* # create member-vlan Inband_VLAN 888
UCS-A /eth-uplink/vlan-group/member-vlan* # exit
UCS-A /eth-uplink/vlan-group* # create member-port a 1 23
UCS-A /eth-uplink/vlan-group/member-port* # exit
UCS-A /eth-uplink/vlan-group* # create member-port b 1 23
UCS-A /eth-uplink/vlan-group/member-port* # commit-buffer
UCS-A /eth-uplink/vlan-group/member-port # exit
UCS-A /eth-uplink/vlan-group # exit
```

次の作業

インバンド サービス プロファイルにインバンド VLAN グループを割り当てます。

VLAN グループの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**.	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A# /eth-uplink/ #**delete vlan-group***Name*.	指定したVLANグループを削除します。
ステップ 3	UCS-A#/eth-uplink* # **commit-buffer**.	トランザクションをシステム設定にコミットします。

次に、VLAN グループを削除する例を示します。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # delete vlan-group eng
UCS-A /eth-uplink* # commit-buffer
UCS-A /eth-uplink #
```

VLAN グループの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org**	Cisco UCS Manager 組織を入力します。
ステップ 2	UCS-A /org # **show vlan-group**	組織に使用可能なグループを表示します。

次の例では、ルート組織で使用可能な VLAN グループを表示します。

```
UCS-A# scope org
UCS-A# /org/# show vlan-group
VLAN Group:
    Name
    ----
    eng
    hr
    finance
```

VLAN 権限

VLAN 権限は、指定した組織および VLAN が属するサービス プロファイル組織に基づいて VLAN へのアクセスを制限します。VLAN 権限により、サービス プロファイルの vNIC に割り当てることができる VLAN のセットも制限されます。VLAN 権限はオプションの機能であり、デフォルトでは無効になっています。この機能は、要件に応じて有効または無効にできます。この機能を無効にすると、すべての VLAN にすべての組織からグローバルでアクセスできるようになります。

（注） [LAN] > [LAN クラウド（LAN Cloud）] > [グローバル ポリシー（Global Policies）] > [組織の権限（Org Permissions）] の順で組織権限を有効にすると、VLAN の作成時に、[VLAN の作成（Create VLANs）] ダイアログボックスに [VLAN に許可された組織（Permitted Orgs for VLAN(s)）] オプションが表示されます。[組織の権限（Org Permissions）] を有効にしない場合、[VLAN に許可された組織（Permitted Orgs for VLAN(s)）] オプションは表示されません。

組織の権限を有効にすると、VLAN の組織を指定できます。組織を指定すると、その VLAN は特定の組織とその構造下にあるすべてのサブ組織で利用可能になります。他の組織のユーザは、この VLAN にアクセスできません。また、VLAN アクセス要件の変更に基づいて VLAN の権限を随時変更できます。

注意 VLAN の組織権限をルート レベルで組織に割り当てると、すべてのサブ組織が VLAN にアクセスできるようになります。ルート レベルで組織権限を割り当てた後で、サブ組織に属する VLAN の権限を変更した場合は、その VLAN はルート レベルの組織で使用できなくなります。

VLAN 権限の作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org**.	Cisco UCS Manager VLAN 組織を入力します。
ステップ 2	UCS-A# /org/ #**create vlan-permit***VLAN permission name*.	指定された VLAN 権限を作成し、その組織に VLAN アクセス権限を割り当てます。
ステップ 3	UCS-A#/org* # **commit-buffer**.	トランザクションをシステム設定にコミットします。

次の例では、組織用の VLAN 権限を作成する方法を示します。

```
UCS-A# scope org
UCS-A /org # create vlan-permit dev
UCS-A /org* # commit-buffer
UCS-A /org #
```

VLAN 権限の削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org**.	Cisco UCS Manager VLAN 組織を入力します。
ステップ 2	UCS-A# /org/ #**delete vlan-permit***VLAN permission name*.	VLAN へのアクセス権を削除します。
ステップ 3	UCS-A#/org* # **commit-buffer**.	トランザクションをシステム設定にコミットします。

次に、組織から VLAN 権限を削除する例を示します。

```
UCS-A# scope org
UCS-A /org # delete vlan-permit dev
UCS-A /org* # commit-buffer
UCS-A /org #
```

VLAN 権限の表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org**	Cisco UCS Manager 組織を入力します。
ステップ 2	UCS-A /org # **show vlan-permit**	組織で使用可能な権限を表示します。

次の例では、この VLAN にアクセスするための権限を持つ VLAN グループを表示します。

```
UCS-A# scope org
UCS-A# /org/# show vlan-permit
VLAN Group:
    Name
    ----
    eng
    hr
    finance
```

第 17 章

LAN ピン グループの設定

この章の内容は、次のとおりです。

LAN ピン グループ

Cisco UCS は LAN ピン グループを使用して、サーバ上の vNIC から、ファブリック インターコネクトのアップリンク イーサネット ポートまたはポート チャネルに、イーサネット トラフィックをピン接続します。このピン接続を使用して、サーバからのトラフィックの分散を管理できます。

サーバにピン接続を設定するには、LAN ピン グループを vNIC ポリシーにインクルードする必要があります。その後、この vNIC ポリシーは、このサーバに割り当てられたサービス プロファイルに含められます。vNIC からのすべてのトラフィックは、I/O モジュールを経由して所定のアップリンク イーサネット ポートに進みます。

（注） vNIC ポリシーを使用してピン グループがサーバ インターフェイスに割り当てられていない場合、Cisco UCS Manager はそのサーバ インターフェイスからのトラフィックに対するアップリンク イーサネット ポートまたはポート チャネルを動的に選択します。この選択は永続的ではありません。インターフェイス フラップまたはサーバのリブートの後は、そのサーバ インターフェイスからのトラフィックに対して別のアップリンク イーサネット ポートまたはポート チャネルが使用される可能性があります。

アップリンクが LAN ピン グループに属している場合、そのアップリンクは所属グループ専用に予約されているわけではありません。LAN ピン グループを指定していない他の vNIC ポリシーは、動的なアップリンクとしてそのアップリンクを使用できます。

LAN ピン グループの設定

LAN ピン グループの設定

2 つのファブリック インターコネクトを持つシステムでピン グループとの関連付けができるのはのは、1 つのファブリック インターコネクト、または両方のファブリック インターコネクトだけです。

はじめる前に

ピン グループの設定に使用するポートおよびポート チャネルを設定します。使用できるのは、LAN ピン グループでアップリンク ポートとして設定されているポートおよびポート チャネルだけです。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネットアップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **create pin-group** *pin-group-name*	イーサネット（LAN）ピン グループを指定された名前で作成し、イーサネット アップリンクのピン グループ モードを開始します。
ステップ 3	UCS-A /eth-uplink/pin-group # **set descr** *description*	（任意） ピン グループに説明を加えます。 （注） 説明にスペース、特殊文字、または句読点が含まれている場合は、説明を引用符で括る必要があります。引用符は、**show** コマンド出力の説明フィールドには表示されません。
ステップ 4	UCS-A /eth-uplink/pin-group # **set target** {**a** | **b** | **dual**} {**port** *slot-num*/ *port-num* | **port-channel** *port-num*}	（任意） 指定されたファブリックとポート、またはファブリックとポート チャネルへのイーサネット ピン ターゲットを設定します。
ステップ 5	UCS-A /eth-uplink/pin-group # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、ファブリック A に pingroup54 という名前の LAN ピン グループを作成し、ピン グループに説明を加え、ポート チャネル 28 にピン グループのターゲットを設定し、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # create pin-group pingroup54
UCS-A /eth-uplink/pin-group* # set descr "This is my pin group #54"
UCS-A /eth-uplink/pin-group* # set target a port-channel 28
UCS-A /eth-uplink/pin-group* # commit-buffer
UCS-A /eth-uplink/pin-group #
```

次の作業

ピン グループを vNIC テンプレートに含めます。

LAN ピン グループの設定

第 18 章

MAC プールの設定

この章の内容は、次のとおりです。

MAC プール

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

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

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

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

MAC プールの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルート組織モードを開始するには、*/* を *org-name* として入力します。
ステップ 2	UCS-A /org # **create mac-pool** *mac-pool-name*	指定された名前で MAC プールを作成し、組織 MAC プール モードを開始します。 この名前には、1 ～ 32 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
ステップ 3	UCS-A /org/mac-pool # **set descr** *description*	（任意） MAC プールの説明を記入します。 （注） 説明にスペース、特殊文字、または句読点が含まれている場合は、説明を引用符で括る必要があります。引用符は、**show** コマンド出力の説明フィールドには表示されません。
ステップ 4	UCS-A /org/mac-pool # **set assignmentorder** {**default** | **sequential**}	次のいずれかになります。 • **default**：Cisco UCS Manager はプールからランダムな ID を選択します。 • **sequential**：Cisco UCS Manager はプールから最も小さい使用可能 ID を選択します。
ステップ 5	UCS-A /org/mac-pool # **create block** *first-mac-addr last-mac-addr*	MAC アドレス ブロック（範囲）を作成し、組織 MAC プール ブロック モードを開始します。アドレス範囲内の最初と最後の MAC アドレスを *nn*:*nn*:*nn*:*nn*:*nn*:*nn* 形式を使用して指定する必要があります。アドレス間はスペースで区切ります。 （注） MAC プールには、複数の MAC アドレス ブロックを含めることができます。複数の MAC アドレス ブロックを作成するには、組織 MAC プール モードから複数の **create block** コマンドを入力します。

	コマンドまたはアクション	目的
ステップ 6	UCS-A /org/mac-pool # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、pool37 という名前の MAC プールを作成し、プールに説明を加え、ブロックの最初および最後の MAC アドレスを指定して MAC アドレス ブロックを定義し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org # create mac-pool pool37
UCS-A /org/mac-pool* # set descr "This is my MAC pool"
UCS-A /org/mac-pool* # create block 00:A0:D7:42:00:01 00:A0:D7:42:01:00
UCS-A /org/mac-pool/block* # commit-buffer
UCS-A /org/mac-pool/block #
```

次の作業

MAC プールを vNIC テンプレートに含めます。

MAC プールの削除

プールを削除した場合、Cisco UCS Manager は、 でプールの vNIC または vHBA に割り当てられたアドレスを再割り当てしません。削除されたプールのすべての割り当て済みブロックは、次のいずれかが起きるまで、割り当てられた vNIC または vHBA に残ります。

- 関連付けられたサービス プロファイルが削除された場合。
- アドレスが割り当てられた vNIC または vHBA が削除された場合。
- vNIC または vHBA が異なるプールに割り当てられた場合。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルート組織モードを開始するには、/ を *org-name* として入力します。
ステップ 2	UCS-A /org # **delete mac-pool** *pool-name*	指定された MAC プールを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、pool4 という名前の MAC プールを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # delete mac-pool pool4
UCS-A /org* # commit-buffer
UCS-A /org #
```

第 19 章

Quality of Service の設定

この章の内容は、次のとおりです。

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

QoS システム クラスに加えられたグローバル QoS の変更によって、すべてのトラフィックにデータプレーンでの中断が短時間発生する可能性があります。このような変更の例を次に示します。

- 有効になっているクラスの MTU サイズの変更
- 有効になっているクラスの パケット ドロップの変更
- 有効になっているクラスの CoS 値の変更

Cisco UCS Mini の Quality of Service に関する注意事項と制限事項

- Cisco UCS Mini はすべてのシステム クラスに共有バッファを使用します。

- ブロンズ クラスは SPAN とバッファを共有します。SPAN またはブロンズ クラスを使用することを推奨します。
- マルチキャスト最適化はサポートされていません。
- いずれかのクラスの QoS パラメータを変更すると、すべてのクラスへのトラフィックが中断されます。
- イーサネットと FC または FCoE トラフィックが混在する場合、帯域幅が均等に分配されません。
- 同じクラスからの複数のトラフィック ストリームが均等に分配されないことがあります。
- FC または FCoE のパフォーマンス問題を回避するために、すべてのドロップなしポリシーに同じ CoS 値を使用します。
- プラチナおよびゴールド クラスのみがドロップなしポリシーをサポートしています。

システム クラスの設定

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 *9*：システム クラス

システム クラス	説明
プラチナ（Platinum） ゴールド（Gold） シルバー（Silver） ブロンズ（Bronze）	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。 Cisco UCS Mini では、プラチナ クラスおよびゴールド クラスでのみパケット ドロップをディセーブルにできます。no drop クラスとして一度に 1 つのプラチナ クラスと 1 つのゴールド クラスだけを設定できます。
ベスト エフォート（Best Effort）	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。
ファイバチャネル（Fibre Channel）	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。

システム クラスの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-server**	イーサネット サーバ モードを開始します。
ステップ 2	UCS-A /eth-server # **scope qos**	イーサネット サーバ QoS モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /eth-server/qos # **scope eth-classified** {**bronze** | **gold** | **platinum** | **silver**}	指定されたシステム クラスに対し、イーサネット サーバQoSイーサネット機密モードを開始します。
ステップ 4	UCS-A /eth-server/qos/eth-classified # **enable**	指定されたシステムクラスをイネーブルにします。
ステップ 5	UCS-A /eth-server/qos/eth-classified # **set cos** *cos-value*	指定されたシステム クラスにサービス クラスを指定します。有効なサービス クラスの値は 0 ～ 6 です。 **重要** すべての非ドロップ ポリシーに対して、UCS と N5K で同じ CoS 値を使用します。エンドツーエンドPFCが正常に動作することを保証するには、すべての中間スイッチで同じ QoS ポリシーを設定します。
ステップ 6	UCS-A /eth-server/qos/eth-classified # **set drop** {**drop** | **no-drop**}	チャネルでパケットをドロップできるかどうか指定します。Cisco UCS Mini では、プラチナ クラスおよびゴールドクラスでのみパケット ドロップをディセーブルにできます。
ステップ 7	UCS-A /eth-server/qos/eth-classified # **set mtu** {*mtu-value* | **fc** | **normal**}	最大伝送単位（使用されるパケットサイズ）。MTU の最大値は 9216 です。 （注） vNIC に対応する QoS ポリシーがある場合、ここで指定した MTU は、関連付けられたQoSシステム クラスで指定されたMTUと同等以下でなければなりません。この MTU 値が QoS システム クラスのMTU値を超えている場合、データ転送中にパケットがドロップされる可能性があります。
ステップ 8	UCS-A /eth-server/qos/eth-classified # **set weight** {*weight-value* | **best-effort** | **none**}	指定されたシステム クラスに対して相対的な重み値を指定します。有効な重み値は 0 ～ 10 です。
ステップ 9	UCS-A /eth-server/qos/eth-classified # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、プラチナシステム クラスをイネーブルにして、チャネルによるパケットのドロップを許可し、サービス クラスを 6 に設定して、MTU を標準に設定し、相対重みを 5 に設定して、トランザクションをコミットする方法を示しています。

```
UCS-A# scope eth-server
UCS-A /eth-server # scope qos
UCS-A /eth-server/qos # scope eth-classified platinum
UCS-A /eth-server/qos/eth-classified # enable
UCS-A /eth-server/qos/eth-classified* # set drop drop
UCS-A /eth-server/qos/eth-classified* # set cos 6
UCS-A /eth-server/qos/eth-classified* # set mtu normal
UCS-A /eth-server/qos/eth-classified* # set weight 5
UCS-A /eth-server/qos/eth-classified* # commit-buffer
UCS-A /eth-server/qos/eth-classified #
```

システム クラスのディセーブル化

QoS ポリシーで使用されるシステム クラスを無効にすると、Cisco UCS Manager は QoS ポリシーが設定されているサーバのトラフィックに対して CoS 0 のシステム クラスを設定します。CoS 0 に設定されているシステム クラスがない場合、ベスト エフォート システム クラスが使用されます。ベスト エフォート システム クラスやファイバ チャネル システム クラスは無効にできません。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-server**	イーサネット サーバ モードを開始します。
ステップ 2	UCS-A /eth-server # **scope qos**	イーサネット サーバ QoS モードを開始します。
ステップ 3	UCS-A /eth-server/qos # **scope eth-classified** {**bronze** | **gold** | **platinum** | **silver**}	指定されたシステム クラスに対し、イーサネット サーバ QoS イーサネット機密モードを開始します。
ステップ 4	UCS-A /eth-server/qos/eth-classified # **disable**	指定したシステム クラスをディセーブルにします。
ステップ 5	UCS-A /eth-server/qos/eth-classified # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、platinum システム クラスをディセーブルにし、トランザクションをコミットする例を示します。

```
UCS-A# scope eth-server
UCS-A /eth-server # scope qos
UCS-A /eth-server/qos # scope eth-classified platinum
UCS-A /eth-server/qos/eth-classified # disable
UCS-A /eth-server/qos/eth-classified* # commit-buffer
UCS-A /eth-server/qos/eth-classified #
```

Quality of Service ポリシーの設定

Quality of Service ポリシー

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

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

QoS ポリシーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	Switch-A# **scope org** *org-name*	指定した組織で組織モードを開始します。デフォルト組織モードを開始するには、*/* を *org-name* として入力します。
ステップ 2	Switch-A /org # **create qos-policy** *policy-name*	指定した QoS ポリシーを作成し、組織 QoS ポリシー モードを開始します。
ステップ 3	Switch-A /org/qos-policy # **create egress-policy**	QoS ポリシーが使用する出力ポリシー（vNIC および vHBA の両方）を作成し、組織 QoS ポリシーの出力ポリシー モードを開始します。
ステップ 4	Switch-A /org/qos-policy/egress-policy # **set host-cos-control** {**full** | **none**}	（任意）ホストと Cisco UCS Manager のどちらが vNIC に対するサービス クラス（CoS）を制御するかを指定します。この設定は、vHBA には影響しません。 ホストに CoS を制御させるには、**full** キーワードを使用します。パケットに有効な CoS 値がある場合、ホストはその値を使用します。それ以外の場合、指定されたクラス プライオリティに関連付けられた CoS 値を使用します。指定したプライオリティに関連付けられている CoS 値を Cisco UCS Manager に使用させるには、**none** キーワードを使用します。
ステップ 5	Switch-A /org/qos-policy/egress-policy # **set prio** *sys-class-name*	出力ポリシーで使用されるシステム クラスを指定します。*sys-class-name* 引数には、次のいずれかのクラス キーワードを指定できます。

	コマンドまたはアクション	目的
		• [Fc]：vHBA トラフィックだけを制御する QoS ポリシーにこの優先順位を使用します。 • [プラチナ（Platinum）]：vNIC トラフィックだけを制御する QoS ポリシーにこの優先順位を使用します。 • [ゴールド（Gold）]：vNIC トラフィックだけを制御する QoS ポリシーにこの優先順位を使用します。 • [シルバー（Silver）]：vNIC トラフィックだけを制御する QoS ポリシーにこの優先順位を使用します。 • [ブロンズ（Bronze）]：vNIC トラフィックだけを制御する QoS ポリシーにこの優先順位を使用します。 • [ベストエフォート（Best Effort）]：この優先順位は使用しないでください。 ベーシック イーサネット トラフィック レーンのために予約されています。この優先順位を QoS ポリシーに割り当て、別のシステム クラスを CoS 0 に設定する場合、Cisco UCS Manager はこのシステム クラスのデフォルトには戻りません。当該トラフィックの CoS 0 で優先順位がデフォルトに戻ります。
ステップ 6	Switch-A /org/qos-policy/egress-policy # **set rate** {**line-rate** | *kbps*} **burst** *bytes*	想定されるトラフィックの平均レートを指定します。このレートを下回るトラフィックは、常に適用されます。デフォルトは **line-rate** で、値 10,000,000 に等しい値です。最小値は 8 で、最大値は 40,000,000 です。 レート制限は、Cisco UCS VIC-1240 仮想インターフェイス カード および Cisco UCS VIC-1280 仮想インターフェイス カード の vNIC でのみサポートされています。Cisco UCS M81KR 仮想インターフェイス カード は、vNIC および vHBA の両方に対しレート制限をサポートしています。
ステップ 7	Switch-A /org/qos-policy/egress-policy # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、vNIC トラフィックの QoS ポリシーを作成し、プラチナ システム クラスを割り当てて出力ポリシーのレート制限（トラフィック レートとバーストサイズ）を設定し、トランザクションをコミットします。

```
Switch-A# scope org /
Switch-A /org # create qos-policy VnicPolicy34
Switch-A /org/qos-policy* # create egress-policy
```

```
Switch-A /org/qos-policy/egress-policy* # set prio platinum
Switch-A /org/qos-policy/egress-policy* # set rate 5000000 burst 65000
Switch-A /org/qos-policy/egress-policy* # commit-buffer
Switch-A /org/qos-policy/egress-policy #
```

次の例は、vHBA トラフィックの QoS ポリシーを作成し、fc（ファイバ チャネル）システム クラスを割り当てて出力ポリシーのレート制限（トラフィック レートとバーストサイズ）を設定し、トランザクションをコミットします。

```
Switch-A# scope org /
Switch-A /org # create qos-policy VhbaPolicy12
Switch-A /org/qos-policy* # create egress-policy
Switch-A /org/qos-policy/egress-policy* # set prio fc
Switch-A /org/qos-policy/egress-policy* # set rate 5000000 burst 65000
Switch-A /org/qos-policy/egress-policy* # commit-buffer
Switch-A /org/qos-policy/egress-policy #
```

次の作業

QoS ポリシーを vNIC または vHBA テンプレートに含めます。

QoS ポリシーの削除

使用中の QoS ポリシーを削除した場合、または QoS ポリシーで使用されているシステム クラスを無効にした場合、この QoS ポリシーを使用している vNIC と vHBA はすべて、ベスト エフォート システム クラスまたは CoS が 0 のシステム クラスに割り当てられます。マルチテナント機能を実装しているシステムでは、Cisco UCS Manager はまず、組織階層から一致する QoS ポリシーを見つけようとします。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / と入力します。
ステップ 2	UCS-A /org # **delete qos-policy** *policy-name*	指定された QoS ポリシーを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、QosPolicy34 という名前の QoS ポリシーを削除し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # delete qos-policy QosPolicy34
UCS-A /org* # commit-buffer
UCS-A /org #
```

フロー制御ポリシーの設定

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。

フロー制御ポリシーの設定

はじめる前に

必要なフロー制御に対応する設定を使用して、ネットワーク ポートを設定します。たとえば、ポリシーのフロー制御ポーズ フレームに対する送信設定を有効にした場合は、ネットワーク ポートの受信パラメータを [オン（on）] または [指定（desired）] に必ず設定してください。Cisco UCS ポートでフロー制御フレームを受信する場合は、ネットワーク ポートの送信パラメータが [オン（on）] または [指定（desired）] に設定されていることを確認します。フロー制御を使用する必要がない場合は、ネットワーク ポートの受信パラメータと送信パラメータを off に設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope flow-control**	イーサネット アップリンク フロー制御モードを開始します。
ステップ 3	UCS-A /eth-uplink/flow-control # **create policy** *policy-name*	指定されたフロー制御ポリシーを作成します。

	コマンドまたはアクション	目的
ステップ 4	UCS-A /eth-uplink/flow-control/policy # **set prio** *prio-option*	次のフロー制御プライオリティ オプションのいずれかを指定します。 • **auto**：PPP がこのファブリック インターコネクトで使用されるかどうか、Cisco UCS システムとネットワークがネゴシエートします。 • **on**：このファブリック インターコネクト上で PPP が有効にされます。
ステップ 5	UCS-A /eth-uplink/flow-control/policy # **set receive** *receive-option*	次のフロー制御受信オプションのいずれかを指定します。 • **off**：ネットワークからのポーズ要求は無視され、トラフィック フローは通常どおり継続します。 • **on**：ポーズ要求に従い、そのアップリンク ポート上のすべてのトラフィックは、ネットワークでポーズ要求が取り消されるまで停止されます。
ステップ 6	UCS-A /eth-uplink/flow-control/policy # **set send** *send-option*	次のフロー制御送信オプションのいずれかを指定します。 • **off**：パケット負荷に関係なくポート上のトラフィックが通常どおり流れます。 • **on**：着信パケット レートが非常に高くなる場合に、Cisco UCS システムがポーズ要求をネットワークに送信します。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。
ステップ 7	UCS-A /eth-uplink/flow-control/policy # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、フロー制御ポリシーを設定し、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope flow-control
UCS-A /eth-uplink/flow-control # create policy FlowControlPolicy23
UCS-A /eth-uplink/flow-control/policy* # set prio auto
UCS-A /eth-uplink/flow-control/policy* # set receive on
UCS-A /eth-uplink/flow-control/policy* # set send on
UCS-A /eth-uplink/flow-control/policy* # commit-buffer
UCS-A /eth-uplink/flow-control/policy #
```

次の作業

フロー制御ポリシーと、アップリンク イーサネット ポート、またはポート チャネルを関連付けます。

フロー制御ポリシーの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネットアップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope flow-control**	イーサネット アップリンク フロー制御モードを開始します。
ステップ 3	UCS-A /eth-uplink/flow-control # **delete policy** *policy-name*	指定されたフロー制御ポリシーを削除します。
ステップ 4	UCS-A /eth-uplink/flow-control # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、FlowControlPolicy23 という名前のフロー制御ポリシーを削除し、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope flow-control
UCS-A /eth-uplink/flow-control # delete policy FlowControlPolicy23
UCS-A /eth-uplink/flow-control* # commit-buffer
UCS-A /eth-uplink/flow-control #
```

第 20 章

ネットワーク関連ポリシーの設定

この章の内容は、次のとおりです。

vNIC テンプレートの設定

vNIC テンプレート

このポリシーは、サーバ上の vNIC が LAN に接続する方法を定義します。このポリシーは、vNIC LAN 接続ポリシーとも呼ばれます。

Cisco UCS Manager は、vNIC テンプレートを作成する際に正しい設定で VM-FEX ポート プロファイル自動的には作成しません。VM-FEX ポート プロファイルを作成するには、vNIC テンプレートのターゲットを VM として設定する必要があります。

このポリシーを有効にするには、このポリシーをサービス プロファイルに含める必要があります。

（注） サーバに 2 つの Emulex NIC または QLogic NIC（Cisco UCS CNA M71KR-E または Cisco UCS CNA M71KR-Q）がある場合は、両方の NIC にユーザ定義の MAC アドレスが取得されるように、サービス プロファイルで両方のアダプタの vNIC ポリシーを設定する必要があります。両方の NIC のポリシーを設定しない場合でも、Windows は PCI バスで両方の NIC を引き続き検出します。ただし、2 番目のイーサネット インターフェイスがサービス プロファイルに含まれていないため、Windows はそれにハードウェア MAC アドレスを割り当てます。その後でサービス プロファイルを異なるサーバに移動すると、Windows によって追加の NIC が検出されますが、これは 1 つの NIC でユーザ定義の MAC アドレスが取得されなかったためです。

vNIC テンプレートの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルート組織モードを開始するには、*/* を *org-name* として入力します。
ステップ 2	UCS-A /org # **create vnic-templ** *vnic-templ-name* [**eth-if** *vlan-name*] [**fabric** {**a** | **b**}] [**target** [**adapter** | **vm**]]	vNIC テンプレートを作成し、組織 vNIC テンプレート モードを開始します。 選択したターゲットによって、Cisco UCS Manager が、vNIC テンプレートの適切な設定を使用して、自動的に VM-FEX ポート プロファイルを作成するかどうかが決まります。次のいずれかになります。 • [アダプタ（Adapter）]：vNIC はすべてのアダプタに適用されます。このオプションを選択した場合、VM-FEX ポート プロファイルが作成されません。 • [VM]：vNIC はすべての仮想マシンに適用されます。このオプションを選択した場合、VM-FEX ポート プロファイルが作成されます。
ステップ 3	UCS-A /org/vnic-templ # **set descr** *description*	（任意） vNIC テンプレートに説明を加えます。
ステップ 4	UCS-A /org/vnic-templ # **set fabric** {**a** | **a-b** | **b** | **b-a**}	（任意） vNIC に使用するファブリックを指定します。vNIC テンプレートを作成するときにステップ 2 でファブリックを指定しなかった場合は、このコマンドで指定するオプションがあります。

	コマンドまたはアクション	目的
		デフォルトのファブリック インターコネクトが使用できない場合に、この vNIC が第 2 のファブリック インターコネクトにアクセスできるようにするには、**a-b**（A がプライマリ）または **b-a**（B がプライマリ）を選択します。 （注） 次の状況下では、vNIC のファブリック フェールオーバーを有効にしないでください。 • Cisco UCS ドメイン がイーサネット スイッチ モードで動作している場合。vNIC ファブリック フェールオーバーはこのモードではサポートされません。1 つのファブリック インターコネクト上のすべてのイーサネット アップリンクが障害になった場合、vNIC は他のイーサネット アップリンクにフェールオーバーしません。 • ファブリック フェールオーバーをサポートしていないアダプタ（Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter など）を搭載しているサーバに、この vNIC を関連付けることを計画している場合。これを行った場合、Cisco UCS Manager により、サービス プロファイルとサーバを関連付けたときに設定エラーが生成されます。
ステップ 5	UCS-A /org/vnic-templ # **set mac-pool** *mac-pool-name*	この vNIC テンプレートから作成された vNIC によって使用される MAC アドレス プール。
ステップ 6	UCS-A /org/vnic-templ # **set mtu** *mtu-value*	この vNIC テンプレートから作成された vNIC によって使用される最大伝送単位、つまりパケット サイズ。 1500 ～ 9000 の整数を入力します。 （注） vNIC テンプレートに QoS ポリシーが関連付けられている場合、ここで指定された MTU は、関連付けられている QoS システム クラスで指定された MTU 以下であることが必要です。この MTU 値が QoS システム クラスの MTU 値を超えている場合、データ転送中にパケットがドロップされる可能性があります。
ステップ 7	UCS-A /org/vnic-templ # **set nw-control-policy** *policy-name*	この vNIC テンプレートから作成された vNIC によって使用されるネットワーク制御ポリシー。

	コマンドまたはアクション	目的
ステップ 8	UCS-A /org/vnic-templ # **set pin-group** *group-name*	この vNIC テンプレートから作成された vNIC によって使用される LAN ピン グループ。
ステップ 9	UCS-A /org/vnic-templ # **set qos-policy** *policy-name*	この vNIC テンプレートから作成された vNIC によって使用されるサービス ポリシーの品質。
ステップ 10	UCS-A /org/vnic-templ # **set stats-policy** *policy-name*	この vNIC テンプレートから作成された vNIC によって使用される統計情報収集ポリシー。
ステップ 11	UCS-A /org/vnic-templ # **set type** {**initial-template** | **updating-template**}	vNIC テンプレートの更新タイプを指定します。テンプレートのアップデート時にこのテンプレートから作成された vNIC インスタンスが自動的にアップデートされないようにする場合は、**initial-template** キーワードを使用します。それ以外の場合は、vNIC テンプレートのアップデート時にすべての vNIC インスタンスがアップデートされるようにするために **updating-template** キーワードを使用します。
ステップ 12	UCS-A /org/vnic-templ # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、vNIC テンプレートを設定し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org* # create vnic template VnicTempFoo
UCS-A /org/vnic-templ* # set descr "This is a vNIC template example."
UCS-A /org/vnic-templ* # set fabric a
UCS-A /org/vnic-templ* # set mac-pool pool137
UCS-A /org/vnic-templ* # set mtu 8900
UCS-A /org/vnic-templ* # set nw-control-policy ncp5
UCS-A /org/vnic-templ* # set pin-group PinGroup54
UCS-A /org/vnic-templ* # set qos-policy QosPol5
UCS-A /org/vnic-templ* # set stats-policy ServStatsPolicy
UCS-A /org/vnic-templ* # set type updating-template
UCS-A /org/vnic-templ* # commit-buffer
UCS-A /org/vnic-templ #
```

vNIC テンプレートの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルート組織モードを開始するには、/ を *org-name* として入力します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /org # **delete vnic-templ** *vnic-templ-name*	指定した vNIC テンプレートを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、VnicTemp42 という名前の vNIC テンプレートを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # delete vnic template VnicTemp42
UCS-A /org* # commit-buffer
UCS-A /org #
```

イーサネット アダプタ ポリシーの設定

イーサネットおよびファイバ チャネル アダプタ ポリシー

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

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

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

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

オペレーティング システム固有のアダプタ ポリシー

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

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

ただし、（デフォルトの Windows のアダプタ ポリシーを使用する代わりに）Windows OS のイーサネット アダプタ ポリシーを作成する場合は、次の式を使用して Windows で動作する値を計算します。

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

たとえば、送信キューが 1 で受信キューが 8 の場合、

完了キュー = 1 + 8 = 9
割り込み回数 = (9 + 2) 以上の 2 のべき乗の最小値 = 16

Accelerated Receive Flow Steering

Accelerated Receive Flow Steering（ARFS）は、ハードウェアによる受信フロー ステアリングで、CPUデータ キャッシュ ヒット率を向上させることができます。これは、カーネル レベルのパケット処理を、そのパケットを消費するアプリケーション スレッドが動作しているCPUに誘導することによって行います。

ARFS を使用すると、CPU 効率の向上とトラフィック遅延の短縮が可能になります。CPU の各受信キューには、割り込みが関連付けられています。割り込みサービス ルーチン（ISR）は、CPU で実行するよう設定できます。ISR により、パケットは受信キューから現在のいずれかの CPU のバックログに移動されます。パケットは、ここで後から処理されます。アプリケーションがこの CPU で実行されていない場合、CPU はローカル以外のメモリにパケットをコピーする必要があり、これにより遅延が増加します。ARFS では、この特定の流れをアプリケーションが実行されている CPU の受信キューに移動することによって、この遅延を短縮できます。

ARFS はデフォルトでは無効であり、Cisco UCS Manager を使用して有効にできます。ARFS を設定するには、次の手順を実行します。

1. ARFS を有効にしたアダプタ ポリシーを作成します。
2. アダプタ ポリシーをサービス プロファイルと関連付けます。
3. ホスト上で ARFS を有効にします。
    1. Interrupt Request Queue（IRQ）のバランスをオフにします。
    2. IRQ を別の CPU と関連付けます。
    3. ethtool を使用して ntuple を有効にします。

Accelerated Receive Flow Steering のガイドラインと制約事項

- ARFS では vNIC ごとに 64 フィルタをサポート
- ARFS は次のアダプタでサポートされています。
    - Cisco UCS VIC 1280、1240、1340、および 1380
    - Cisco UCS VIC 1225、1225T、1285、1223、1227T、1385、1387
- ARFS は次のオペレーティング システムでサポートされています。
    - Red Hat Enterprise Linux 6.5 および 6.6
    - Red Hat Enterprise Linux 7.0 以上のバージョン
    - SUSE Linux Enterprise Server 11 SP2 および SP3
    - SUSE Linux Enterprise Server 12 以上のバージョン
    - Ubuntu 14.04.2

割り込み調停

アダプタは、通常、ホストCPUが処理する必要のある割り込みを大量に生成します。割り込み調停は、ホストCPUで処理される割り込みの数を削減します。これは、設定可能な調停間隔に同じイベントが複数発生した場合にホストの中断を1回だけにすることで実現されます。

受信動作の割り込み調停を有効にした場合、アダプタは引き続きパケットを受信しますが、ホストCPUは各パケットの割り込みをすぐには受信しません。調停タイマーは、アダプタが最初のパケットを受信すると開始します。設定された調停間隔がタイムアウトすると、アダプタはその間隔の中で受信した複数のパケットで1つの割り込みを生成します。ホストのNICドライバは、受信した複数のパケットを処理します。生成される割り込み数が削減されるため、コンテキストスイッチのホストCPUが消費する時間が短縮されます。つまり、CPUでパケットを処理する時間が増加することになり、結果としてスループットと遅延が改善されます。

適応型割り込み調停

調停間隔が原因で、受信パケットの処理によって遅延が増加します。パケット レートの低い小さなパケットの場合は、この遅延が増加します。遅延のこの増加を避けるため、ドライバは通過するトラフィックのパターンに適応し、サーバからの応答が向上するよう割り込み調停間隔を調整することができます。

適応型割り込み調停（AIC）は、電子メール サーバ、データベース サーバ、LDAP サーバなど、コネクション型の低リンク使用率のシナリオで最も効果的です。ラインレート トラフィックには適しません。

適応型割り込み調停のガイドラインと制約事項

- リンク使用率が80％を超えている場合、適応型割り込み調停（AIC）による遅延の低減効果はありません。
- AIC を有効化すると静的調停は無効になります。
- AIC がサポートされるのは、次のオペレーティング システムだけです。
  - Red Hat Enterprise Linux 6.4 以上のバージョン
  - Red Hat Enterprise Linux 7.0 以上のバージョン
  - SUSE Linux Enterprise Server 11 SP2 および SP3
  - SUSE Linux Enterprise Server 12
  - XenServer 6.5
  - Ubuntu 14.04.2

SMB ダイレクト用 RDMA Over Converged Ethernet

RDMA Over Converged Ethernet（RoCE）は、イーサネット ネットワーク越しのダイレクト メモリ アクセスを実現します。RoCEはリンク層プロトコルであるため、同じイーサネットブロードキャスト ドメインにある任意の 2 ホスト間の通信を可能にします。RoCE は、低遅延、低 CPU 使用率、およびネットワーク帯域幅使用率の高さによって、従来のネットワーク ソケット実装と比較して優れたパフォーマンスを提供します。Windows 2012 以降のバージョンでは、SMB ファイル共有とライブ マイグレーションのパフォーマンスを高速化し、向上させるため RDMA を使用します。

Cisco UCS Manager Release 2.2(4) では、Microsoft SMB ダイレクト用に RoCE をサポートしています。イーサネットアダプタ ポリシーを作成または変更しながら追加の設定情報がアダプタに送信されます。

RoCE を搭載した SMB ダイレクトのガイドラインと制約事項

- RoCE を搭載した Microsoft SMB ダイレクトは Windows 2012 R2 でのみサポートされています。
- RoCE を搭載した Microsoft SMB ダイレクトは Cisco UCS VIC 1340 および 1380 アダプタでのみサポートされています。
- Cisco UCS Manager では、RoCE 対応 vNIC をアダプタごとに 4 つまでしかサポートしません。
- Cisco UCS Manager では、NVGRE、VXLAN、NetFlow、VMQ、usNIC での RoCE をサポートしません。
- アダプタごとのキュー ペアの最大数は 8192 個です。
- アダプタごとのメモリ領域の最大数は 524288 個です。
- リリース 2.2(4) から Cisco UCS Manager をダウングレードする前に RoCE をディセーブルにしないと、ダウングレードは失敗します。

イーサネット アダプタ ポリシーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /org # **create eth-policy** *policy-name*	指定されたイーサネットアダプタポリシーを作成し、組織イーサネットポリシーモードを開始します。
ステップ 3	UCS-A /org/eth-policy # **set arfs accelaratedrfs** {**enabled** | **disabled**}	（任意） Accelerated RFS を設定します。
ステップ 4	UCS-A /org/eth-policy # **set comp-queue count** *count*	（任意） イーサネットの完了キューを設定します。
ステップ 5	UCS-A /org/eth-policy # **set descr** *description*	（任意） ポリシーの説明を記します。 （注） 説明にスペース、特殊文字、または句読点が含まれている場合は、説明を引用符で括る必要があります。引用符は、**show** コマンド出力の説明フィールドには表示されません。
ステップ 6	UCS-A /org/eth-policy # **set failovertimeout** *timeout-sec*	（任意） イーサネットのフェールオーバーを設定します。
ステップ 7	UCS-A /org/eth-policy # **set interrupt** {**coalescing-time** *sec* | **coalescing-type** {**idle** | **min**} | **count** *count* | **mode** {**intx** | **msi** | **msi-x**}}	（任意） イーサネットの割り込みを設定します。
ステップ 8	UCS-A /org/eth-policy # **set nvgre adminstate** {**disabled** | **enabled**}	（任意） NVGRE を設定します。
ステップ 9	UCS-A /org/eth-policy # **set offload** {**large-receive** | **tcp-rx-checksum** | **tcp-segment** | **tcp-tx-checksum**} {**disabled** | **enabled**}	（任意） イーサネットのオフロードを設定します。
ステップ 10	UCS-A /org/eth-policy # **set policy-owner** {**local** | **pending**}	（任意） イーサネットアダプタポリシーのオーナーを指定します。
ステップ 11	UCS-A /org/eth-policy # **set recv-queue** {**count** *count* | **ring-size** *size-num*}	（任意） イーサネットの受信キューを設定します。
ステップ 12	UCS-A /org/eth-policy # **set roceadminstate** {**disabled** | **enabled**} | **memoryregions** *number-of-memory-regions* | **queuepairs** *number-of-queue-pairs* |	（任意） 次のオプションを使用して、RDMA over converged Ethernet（RoCE）を設定します。 • [adminstate]：RoCE を有効または無効にします。

	コマンドまたはアクション	目的
	resourcegroups *number-of-resource-groups*	• [memoryregions]：アダプタごとに使用するメモリ領域の数を設定します。 値の範囲は 1 ～ 524288 のメモリ領域で、最も近い 2 の乗数を整数として指定する必要があります。 • [queuepairs]：アダプタごとに使用するキューペアの数を設定します。値の範囲は 1 ～ 8192 のキュー ペアで、最も近い 2 の乗数を整数として指定する必要があります。 • [resourcegroups]：使用するリソース グループの数を設定します。値の範囲は 1 ～ 128 のリソース グループです。最適なパフォーマンスを得るためには、システムの CPU コアの数以上の整数値を、最も近い 2 の乗数として指定する必要があります。
ステップ 13	UCS-A /org/eth-policy # **set rss receivesidescaling** {**disabled** | **enabled**}	（任意） RSS を設定します。
ステップ 14	UCS-A /org/eth-policy # **set trans-queue** {**count** *count* | **ring-size** *size-num*}	（任意） イーサネットの送信キューを設定します。
ステップ 15	UCS-A /org/eth-policy # **set vxlan adminstate** {**disabled** | **enabled**}	（任意） VXLAN を設定します。
ステップ 16	UCS-A /org/eth-policy # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、イーサネット アダプタ ポリシーを設定し、トランザクションをコミットします。

```
UCS-A# scope org
UCS-A /org* # create eth-policy EthPolicy19
UCS-A /org/eth-policy* # set comp-queue count 16
UCS-A /org/eth-policy* # set descr "This is an Ethernet adapter policy example."
UCS-A /org/eth-policy* # set failover timeout 300
UCS-A /org/eth-policy* # set interrupt count 64
UCS-A /org/eth-policy* # set offload large-receive disabled
UCS-A /org/eth-policy* # set recv-queue count 32
UCS-A /org/eth-policy* # set rss receivesidescaling enabled
UCS-A /org/eth-policy* # set trans-queue
UCS-A /org/eth-policy* # commit-buffer
UCS-A /org/eth-policy #
```

次の例は、RoCEを使用してイーサネットアダプタポリシーを設定し、トランザクションをコミットします。

```
UCS-A# scope org
UCS-A /org* # create eth-policy EthPolicy20
UCS-A /org/eth-policy* # set roce adminstate enable
UCS-A /org/eth-policy* # set roce memoryregions 131072
UCS-A /org/eth-policy* # set roce queuepairs 256
UCS-A /org/eth-policy* # set roce resourcegroups 32
UCS-A /org/eth-policy # commit buffer
UCS-A /org # show eth-policy EthPolicy20 detail expand

Eth Adapter Policy:
    Name: EthPolicy20
    Description:
    Policy Owner: Local

    ARFS:
        Accelarated Receive Flow Steering: Disabled

    Ethernet Completion Queue:
        Count: 2

    Ethernet Failback:
        Timeout (sec): 5

    Ethernet Interrupt:
        Coalescing Time (us): 125
        Coalescing Type: Min
        Count: 4
        Driver Interrupt Mode: MSI-X

    NVGRE:
        NVGRE: Disabled

    Ethernet Offload:
        Large Receive: Enabled
        TCP Segment: Enabled
        TCP Rx Checksum: Enabled
        TCP Tx Checksum: Enabled

    Ethernet Receive Queue:
        Count: 1
        Ring Size: 512

    ROCE:
        RoCE: Enabled
        Resource Groups: 32
        Memory Regions: 131072
        Queue Pairs: 256

    VXLAN:
        VXLAN: Disabled

    Ethernet Transmit Queue:
        Count: 1
        Ring Size: 256

    RSS:
        Receive Side Scaling: Disabled
```

Linux オペレーティング システムで MRQS 用の eNIC サポートをイネーブル化するためのイーサネット アダプタ ポリシーの設定

Cisco UCS Manager には、Red Hat Enterprise Linux バージョン 6.x および SUSE Linux Enterprise Server バージョン 11.x での Multiple Receive Queue Support（MRQS）機能向けの eNIC サポートが含まれます。

手順

ステップ 1 イーサネット アダプタ ポリシーを作成します。
イーサネット アダプタ ポリシーを作成する場合は、次のパラメータを使用します。

- 送信キュー = 1
- 受信キュー = n（最大 8）
- 完了キュー = 送信キューの数 + 受信キューの数
- 割り込み = 完了キューの数 + 2
- Receive Side Scaling（RSS）= [有効（Enabled）]
- 割り込みモード = Msi-X

イーサネット アダプタ ポリシーの設定, （311 ページ） を参照してください。

ステップ 2 eNIC ドライバ バージョン 2.1.1.35 以降をインストールします。
『Cisco UCS Virtual Interface Card Drivers for Linux Installation Guide』を参照してください。

ステップ 3 サーバをリブートします。

イーサネット アダプタ ポリシーの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **delete eth-policy** *policy-name*	指定したイーサネット アダプタ ポリシーを削除します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、EthPolicy19 という名前のイーサネット アダプタ ポリシーを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # delete eth-policy EthPolicy19
UCS-A /org* # commit-buffer
UCS-A /org #
```

デフォルトの vNIC 動作ポリシーの設定

デフォルトの vNIC 動作ポリシー

デフォルトの vNIC 動作ポリシーにより、サービス プロファイルに対する vNIC の作成方法を設定できます。vNICS を手動で作成することもできますし、自動的に作成することもできます。

デフォルトの vNIC 動作ポリシーを設定して、vNIC の作成方法を定義することができます。次のいずれかになります。

- [なし（None）]：サービス プロファイルに Cisco UCS Manager はデフォルトの vNIC を作成しません。すべての vNIC を明示的に作成する必要があります。
- [HW 継承（HW Inherit）]：サービス プロファイルが vNIC を必要とし、何も明示的に定義されていない場合、Cisco UCS Manager はサービス プロファイルに関連付けられたサーバにインストールされたアダプタに基づいて必要な vNIC を作成します。

（注） vNIC のデフォルトの動作ポリシーを指定しない場合、[HW 継承（HW Inherit）] がデフォルトで使用されます。

デフォルトの vNIC 動作ポリシーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org /**	ルート組織モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A/org # **scope vnic-beh-policy**	デフォルトの vNIC 動作ポリシーモードを開始します。
ステップ 3	UCS-A/org/vnic-beh-policy # **set action** {**hw-inherit** [**template_name** *name*] | **none**}	デフォルトの vNIC 動作ポリシーを指定します。次のいずれかになります。 • **hw-inherit**：サービス プロファイルが vNIC を必要とし、何も明示的に定義されていない場合、Cisco UCS Manager はサービス プロファイルに関連付けられたサーバにインストールされたアダプタに基づいて必要な vNIC を作成します。 **hw-inherit** を指定した場合は、vNIC テンプレートを指定して vNIC を作成することもできます。 • **none**：Cisco UCS Manager はサービス プロファイルにデフォルトの vNIC を作成しません。すべての vNIC を明示的に作成する必要があります。
ステップ 4	UCS-A/org/vnic-beh-policy # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、デフォルトの vNIC 動作ポリシーを **hw-inherit** に設定する方法を示します。

```
UCS-A # scope org /
UCS-A/org # scope vnic-beh-policy
UCS-A/org/vnic-beh-policy # set action hw-inherit
UCS-A/org/vnic-beh-policy* # commit-buffer
UCS-A/org/vnic-beh-policy #
```

LAN 接続ポリシーの設定

LAN および SAN 接続ポリシーについて

接続ポリシーは、ネットワーク上のサーバと LAN または SAN 間の接続およびネットワーク通信リソースを決定します。これらのポリシーは、プールを使用してサーバに MAC アドレス、WWN、および WWPN を割り当て、サーバがネットワークとの通信に使用する vNIC および vHBA を識別します。

（注） これらの接続ポリシーは、サービス プロファイルおよびサービス プロファイル テンプレートに含まれ、複数のサーバを設定するために使用できるので、静的 ID を接続ポリシーで使用することはお勧めしません。

LAN および SAN の接続ポリシーに必要な権限

接続ポリシーにより、ネットワークまたはストレージ権限のないユーザがネットワークおよびストレージ接続をしているサービス プロファイルおよびサービス プロファイル テンプレートを作成および変更することが可能になります。ただし、ユーザは接続ポリシーを作成するための適切なネットワークおよびストレージの権限が必要です。

接続ポリシーの作成に必要な権限

接続ポリシーは、他のネットワークおよびストレージ構成と同じ権限を必要とします。たとえば、接続ポリシーを作成するには、次の権限の少なくとも 1 つを有している必要があります。

- admin：LAN および SAN 接続ポリシーを作成できます
- ls-server：LAN および SAN 接続ポリシーを作成できます
- ls-network：LAN 接続ポリシーを作成できます
- ls-storage：SAN 接続ポリシーを作成できます

接続ポリシーをサービス プロファイルに追加するために必要な権限

接続ポリシーの作成後、ls-compute 権限を持つユーザは、そのポリシーをサービス プロファイルまたはサービス プロファイル テンプレートに組み込むことができます。ただし、ls-compute 権限しかないユーザは接続ポリシーを作成できません。

サービス プロファイルと接続ポリシー間の相互作用

次のいずれかの方法により、サービス プロファイルに LAN および SAN の接続を設定できます。

- サービス プロファイルで参照される LAN および SAN 接続ポリシー
- サービス プロファイルで作成されるローカル vNIC および vHBA
- ローカル vNIC および SAN 接続ポリシー
- ローカル vHBA および LAN 接続ポリシー

Cisco UCS では、サービス プロファイルのローカル vNIC および vHBA 設定と接続ポリシー間の相互排他性が維持されます。接続ポリシーとローカルに作成した vNIC または vHBA を組み合わせて使用することはできません。サービス プロファイルに LAN 接続ポリシーを含めると、既存の vNIC 設定がすべて消去されます。SAN 接続ポリシーを含めた場合は、そのサービス プロファイル内の既存の vHBA 設定がすべて消去されます。

LAN 接続ポリシーの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルート組織モードを開始するには、*/* を *org-name* として入力します。
ステップ 2	UCS-A /org # **create lan-connectivity-policy** *policy-name*	指定された LAN 接続ポリシーを作成し、組織 LAN 接続ポリシー モードを開始します。 この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
ステップ 3	UCS-A /org/lan-connectivity-policy # **set descr** *policy-name*	（任意） ポリシーに説明を追加します。どこでどのようにポリシーが使用されるかについての情報を含めることを推奨します。 256 文字以内で入力します。次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
ステップ 4	UCS-A /org/lan-connectivity-policy # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、LanConnect42 という名前の LAN 接続ポリシーを作成し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org* # create lan-connectivity-policy LanConnect42
UCS-A /org/lan-connectivity-policy* # set descr "LAN connectivity policy"
UCS-A /org/lan-connectivity-policy* # commit-buffer
UCS-A /org/lan-connectivity-policy #
```

次の作業

この LAN 接続ポリシーに 1 つ以上の vNIC および（または）iSCSI vNIC を追加します。

LAN 接続ポリシー用の vNIC の作成

LAN 接続ポリシーの作成, （319 ページ） から続行した場合、ステップ 3 でこの手順を開始します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルート組織モードを開始するには、*/* を *org-name* として入力します。
ステップ 2	UCS-A /org # **scope lan-connectivity-policy** *policy-name*	指定した LAN 接続ポリシーの LAN 接続ポリシー モードを開始します。
ステップ 3	UCS-A /org/lan-connectivity-policy # **create vnic** *vnic-name* [**eth-if** *eth-if-name*] [**fabric** {**a** | **b**}]	指定された LAN 接続ポリシー用の vNIC を作成します。 この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
ステップ 4	UCS-A /org/lan-connectivity-policy/vnic # **set fabric** {**a** | **a-b** | **b** | **b-a**}	vNIC に使用するファブリックを指定します。ステップ 3 で vNIC を作成したときにファブリックを指定しなかった場合は、このコマンドで指定するオプションがあります。 デフォルトのファブリック インターコネクトが使用できない場合に、この vNIC が第 2 のファブリック インターコネクトにアクセスできるようにするには、**a-b**（A がプライマリ）または **b-a**（B がプライマリ）を選択します。

	コマンドまたはアクション	目的
		（注） 次の状況下では、vNIC のファブリック フェールオーバーを有効にしないでください。 • Cisco UCS ドメイン がイーサネット スイッチ モードで動作している場合。vNIC ファブリック フェールオーバーはこのモードではサポートされません。1 つのファブリック インターコネクト上のすべてのイーサネットアップリンクが障害になった場合、vNIC は他のイーサネットアップリンクにフェールオーバーしません。 • ファブリック フェールオーバーをサポートしていないアダプタ（Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter など）を搭載しているサーバに、この vNIC を関連付けることを計画している場合。これを行った場合、Cisco UCS Manager により、サービス プロファイルとサーバを関連付けたときに設定エラーが生成されます。
ステップ 5	UCS-A /org/lan-connectivity-policy/vnic # **set adapter-policy** *policy-name*	vNIC に使用するアダプタ ポリシーを指定します。
ステップ 6	UCS-A /org/lan-connectivity-policy/vnic # **set identity** {**dynamic-mac** {*mac-addr* | **derived**} | **mac-pool** *mac-pool-name*}	vNIC の ID（MAC アドレス）を指定します。次のいずれかのオプションを使用して識別を設定できます。 • 一意の MAC アドレスを *nn*:*nn*:*nn*:*nn*:*nn*:*nn* の形式で作成します。 • 製造時にハードウェアに焼き付けられた MAC アドレスを取得する。 • MAC プールから MAC アドレスを割り当てる。
ステップ 7	UCS-A /org/lan-connectivity-policy/vnic # **set mtu** *size-num*	この vNIC で受け入れられる最大伝送単位、つまりパケット サイズ。 を指定します。 1500 ～ 9216 の整数を入力します。

	コマンドまたはアクション	目的
		（注） vNIC に対応する QoS ポリシーがある場合、ここで指定した MTU は、関連付けられた QoS システム クラスで指定された MTU と同等以下でなければなりません。この MTU 値が QoS システム クラスの MTU 値を超えている場合、データ転送中にパケットがドロップされる可能性があります。
ステップ 8	UCS-A /org/lan-connectivity-policy/vnic # **set nw-control-policy** *policy-name*	vNIC によって使用されるネットワーク制御ポリシーを指定します。
ステップ 9	UCS-A /org/lan-connectivity-policy/vnic # **set order** {*order-num* | **unspecified**}	vNIC に相対順序を指定します。
ステップ 10	UCS-A /org/lan-connectivity-policy/vnic # **set pin-group** *group-name*	vNIC によって使用される LAN ピン グループを指定します。
ステップ 11	UCS-A /org/lan-connectivity-policy/vnic # **set qos-policy** *policy-name*	vNIC によって使用されるサービス ポリシーの品質を指定します。
ステップ 12	UCS-A /org/lan-connectivity-policy/vnic # **set stats-policy** *policy-name*	vNIC によって使用される統計情報収集ポリシーを指定します。
ステップ 13	UCS-A /org/lan-connectivity-policy/vnic # **set template-name** *policy-name*	ダイナミック vNIC 接続ポリシーを vNIC に使用するように指定します。
ステップ 14	UCS-A /org/lan-connectivity-policy/vnic # **set vcon** {**1** | **2** | **3** | **4** | **any**}	指定された vCon に vNIC を割り当てます。Cisco UCS Manager が自動的に vNIC を割り当てるようにするには、**any** キーワードを使用します。
ステップ 15	UCS-A /org/lan-connectivity-policy/vnic # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、LanConnect42 という名前の LAN 接続ポリシー用の vNIC を設定し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org # scope lan-connectivity-policy LanConnect42
UCS-A /org/lan-connectivity-policy* # create vnic vnic3 fabric a
UCS-A /org/lan-connectivity-policy/vnic* # set fabric a-b
UCS-A /org/lan-connectivity-policy/vnic* # set adapter-policy AdaptPol2
UCS-A /org/lan-connectivity-policy/vnic* # set identity mac-pool MacPool3
```

```
UCS-A /org/lan-connectivity-policy/vnic* # set mtu 8900
UCS-A /org/lan-connectivity-policy/vnic* # set nw-control-policy ncp5
UCS-A /org/lan-connectivity-policy/vnic* # set order 0
UCS-A /org/lan-connectivity-policy/vnic* # set pin-group EthPinGroup12
UCS-A /org/lan-connectivity-policy/vnic* # set qos-policy QosPol5
UCS-A /org/lan-connectivity-policy/vnic* # set stats-policy StatsPol2
UCS-A /org/lan-connectivity-policy/vnic* # set template-name VnicConnPol3
UCS-A /org/lan-connectivity-policy/vnic* # set vcon any
UCS-A /org/lan-connectivity-policy/vnic* # commit-buffer
UCS-A /org/lan-connectivity-policy/vnic #
```

次の作業

必要に応じて、LAN 接続ポリシーに別の NIC または iSCSI vNIC を追加します。そうでない場合は、サービス プロファイルまたはサービス プロファイル テンプレートにポリシーをインクルードします。

LAN 接続ポリシーからの vNIC の削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルート組織モードを開始するには、/ を *org-name* として入力します。
ステップ 2	UCS-A /org # **scope lan-connectivity-policy** *policy-name*	指定した LAN 接続ポリシーの LAN 接続ポリシー モードを開始します。
ステップ 3	UCS-A /org/lan-connectivity-policy # **delete vnic** *vnic-name*	LAN 接続ポリシーから指定された vNIC を削除します。
ステップ 4	UCS-A /org/lan-connectivity-policy # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、vnic3 という名前の vNIC を LanConnect42 という名前の LAN 接続ポリシーから削除し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org # scope lan-connectivity-policy LanConnect42
UCS-A /org/lan-connectivity-policy # delete vnic vnic3
UCS-A /org/lan-connectivity-policy* # commit-buffer
UCS-A /org/lan-connectivity-policy #
```

LAN 接続ポリシー用の iSCSI vNIC の作成

LAN 接続ポリシーの作成 から続行した場合、ステップ 3 でこの手順を開始します。

はじめる前に

LAN 接続ポリシーは、iSCSI デバイス用のオーバーレイ vNIC として使用できるイーサネット vNIC を含める必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルート組織モードを開始するには、*/* を *org-name* として入力します。
ステップ 2	UCS-A /org # **scope lan-connectivity-policy** *policy-name*	指定した LAN 接続ポリシーの LAN 接続ポリシーモードを開始します。
ステップ 3	UCS-A /org/lan-connectivity-policy # **create vnic-iscsi** *iscsi-vnic-name*.	指定された LAN 接続ポリシーの iSCSI vNIC を作成します。 この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
ステップ 4	UCS-A /org/lan-connectivity-policy/vnic-iscsi # **set iscsi-adaptor-policy** *iscsi-adaptor-name*	（任意） この iSCSI vNIC 用に作成した iSCSI アダプタ ポリシーを指定します。
ステップ 5	UCS-A /org/lan-connectivity-policy/vnic-iscsi # **set auth-name** *authentication-profile-name*	（任意） iSCSI vNIC によって使用される認証プロファイルを設定します。設定する認証プロファイルがすでに存在している必要があります。詳細については、認証プロファイルの作成を参照してください。
ステップ 6	UCS-A /org/lan-connectivity-policy/vnic-iscsi # **set identity** { **dynamic-mac** {*dynamic-mac-address* | **derived** } | **mac-pool** *mac-pool-name* }	iSCSI vNIC の MAC アドレスを指定します。 （注） MAC アドレスは、Cisco UCS NIC M51KR-B アダプタ専用に設定されます。
ステップ 7	UCS-A /org/lan-connectivity-policy/vnic-iscsi # **set iscsi-identity** {**initiator-name** *initiator-name* | **initiator-pool-name** *iqn-pool-name*}	iSCSI イニシエータの名前、または iSCSI イニシエータの名前の指定に使用される IQN プールの名前を指定します。iSCSI イニシエータ名には最大 223 文字を使用できます。

	コマンドまたはアクション	目的
ステップ 8	UCS-A /org/lan-connectivity-policy/vnic-iscsi # **set overlay-vnic-name** *overlay-vnic-name*	オーバーレイ vNIC として iSCSI デバイスで使用される、イーサネット vNIC を指定します。詳細については、サービス プロファイルの vNIC の設定を参照してください。
ステップ 9	UCS-A /org/lan-connectivity-policy/vnic-iscsi # **create eth-if**	iSCSI vNIC に割り当てられた VLAN のイーサネット インターフェイスを作成します。
ステップ 10	UCS-A /org/ex/vnic-iscsi/eth-if # **set vlanname** *vlan-name*	VLAN 名を指定します。デフォルトの VLAN は、default です。Cisco UCS M81KR 仮想インターフェイス カードおよび Cisco UCS VIC-1240 仮想インターフェイス カードの場合、指定する VLAN はオーバーレイ vNIC のネイティブ VLAN と同じである必要があります。Cisco UCS M51KR-B Broadcom BCM57711 アダプタの場合、指定した VLAN は、オーバーレイ vNIC に割り当てられたどの VLAN でも設定できます。
ステップ 11	UCS-A /org/lan-connectivity-policy/vnic-iscsi # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、LanConnect42 という名前の LAN 接続ポリシー用の iSCSI vNIC を設定し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org # scope lan-connectivity-policy LanConnect42
UCS-A /org/lan-connectivity-policy # create vnic-iscsi iSCSI1
UCS-A /org/lan-connectivity-policy/vnic-iscsi* # set iscsi-adaptor-policy iscsiboot
UCS-A /org/lan-connectivity-policy/vnic-iscsi* # set auth-name initauth
UCS-A /org/lan-connectivity-policy/vnic-iscsi* # set identity dynamic-mac derived
UCS-A /org/lan-connectivity-policy/vnic-iscsi* # set iscsi-identity initiator-name iSCSI1
UCS-A /org/lan-connectivity-policy/vnic-iscsi* # set overlay-vnic-name eth1
UCS-A /org/lan-connectivity-policy/vnic-iscsi* # create eth-if
UCS-A /org/lan-connectivity-policy/vnic-iscsi/eth-if* # set vlanname default
UCS-A /org/lan-connectivity-policy/vnic-iscsi/eth-if* # commit buffer
UCS-A /org/lan-connectivity-policy/vnic-iscsi/eth-if
```

次の作業

必要に応じて、LAN 接続ポリシーに別の iSCI vNIC または vNIC を追加します。そうでない場合は、サービス プロファイルまたはサービス プロファイル テンプレートにポリシーをインクルードします。

LAN 接続ポリシーからの iSCSI vNIC の削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルート組織モードを開始するには、/ を *org-name* として入力します。
ステップ 2	UCS-A /org # **scope lan-connectivity-policy** *policy-name*	指定した LAN 接続ポリシーの LAN 接続ポリシー モードを開始します。
ステップ 3	UCS-A /org/lan-connectivity-policy # **delete vnic-iscsi** *iscsi-vnic-name*	LAN 接続ポリシーから指定された iSCSI vNIC を削除します。
ステップ 4	UCS-A /org/lan-connectivity-policy # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、iscsivnic3 という名前の iSCSI vNIC を LanConnect42 という名前の LAN 接続ポリシーから削除し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org # scope lan-connectivity-policy LanConnect42
UCS-A /org/lan-connectivity-policy # delete vnic-iscsi iscsivnic3
UCS-A /org/lan-connectivity-policy* # commit-buffer
UCS-A /org/lan-connectivity-policy #
```

LAN 接続ポリシーの削除

サービス プロファイルに含まれる LAN 接続ポリシーを削除する場合、すべての vNIC と iSCSI vNIC もそのサービス プロファイルから削除し、そのサービス プロファイルに関連付けられているサーバの LAN データ トラフィックを中断します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルート組織モードを開始するには、/ を *org-name* として入力します。
ステップ 2	UCS-A /org # **delete lan-connectivity-policy** *policy-name*	指定されたLAN接続ポリシーを削除します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、LanConnectiSCSI42 という名前の LAN 接続ポリシーをルート組織から削除し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org # delete lan-connectivity-policy LanConnectiSCSI42
UCS-A /org* # commit-buffer
UCS-A /org #
```

ネットワーク制御ポリシーの設定

ネットワーク制御ポリシー

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

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

[アップリンクのアクションに失敗しました（Action on Uplink Fail）] プロパティ

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

オでは、リモートイーサネットインターフェイスにバインドされているvFibreチャネルインターフェイスもダウンします。

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

MAC 登録モード

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

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

ネットワーク制御ポリシーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルート組織モードを開始するには、*/* を *org-name* として入力します。
ステップ 2	UCS-A /org # **create nw-ctrl-policy** *policy-name*	指定されたネットワーク制御ポリシーを作成し、組織ネットワーク制御ポリシーモードを開始します。
ステップ 3	UCS-A /org/nw-ctrl-policy # {**disable** | **enable**} **cdp**	Cisco Discovery Protocol（CDP）をディセーブルまたはイネーブルにします。
ステップ 4	UCS-A /org/nw-ctrl-policy # **set uplink-fail-action** {**link-down** | **warning**}	エンドホスト モードで使用可能なアップリンク ポートがない場合に実行するアクションを指定します。 **link-down** キーワードを使用すると、ファブリック インターコネクトでアップリンク接続が失われた場合にvNICの動作ステータスがdownに変更さ

	コマンドまたはアクション	目的
		れ、vNIC のファブリック フェールオーバーが容易になります。**warning** キーワードを使用すると、アップリンク ポートを使用できない場合でもサーバ間の接続が維持され、ファブリック インターコネクトでアップリンク接続が失われた場合にファブリック フェールオーバーがディセーブルになります。デフォルトのアップリンク障害処理は link-down ダウンです。
ステップ 5	UCS-A /org/nw-ctrl-policy # **set mac-registration-mode**{**all-host-vlans** | **only-native-vlan**	アダプタ登録済みの MAC アドレスを、インターフェイスに関連付けられているネイティブ VLAN にのみ追加するか、インターフェイスに関連付けられているすべての VLAN に追加するか。次のいずれかになります。 • [ネイティブ VLAN のみ（Only Native Vlan）]：MAC アドレスはネイティブ VLAN にのみ追加されます。デフォルトではこのオプションが設定され、port+VLAN のカウントが最大になります。 • [すべてのホスト VLAN（All Host Vlans）]：関連付けられているすべての VLAN に MAC アドレスが追加されます。トランキングを使用するよう設定されているが、無差別モードで実行されていない VLAN の場合、このオプションを選択します。
ステップ 6	UCS-A /org/nw-ctrl-policy # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、ncp5 というネットワーク制御ポリシーを作成して、CDP をイネーブルにし、アップリンク フェール アクションを link-down に設定して、トランザクションをコミットする方法を示しています。

```
UCS-A# scope org /
UCS-A /org # create nw-ctrl-policy ncp5
UCS-A /org/nw-ctrl-policy* # enable cdp
UCS-A /org/nw-ctrl-policy* # set uplink-fail-action link-down
UCS-A /org/nw-ctrl-policy* # commit-buffer
UCS-A /org/nw-ctrl-policy #
```

ネットワーク制御ポリシーの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org /**	ルート組織モードを開始します。
ステップ 2	UCS-A /org # **delete nwctrl-policy** *policy-name*	指定されたネットワーク制御ポリシーを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、ncp5 という名前のネットワーク制御ポリシーを削除し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # delete nwctrl-policy ncp5
UCS-A /org* # commit-buffer
UCS-A /org #
```

マルチキャスト ポリシーの設定

マルチキャスト ポリシー

このポリシーは、インターネット グループ管理プロトコル（IGMP）のスヌーピングおよびIGMP クエリアの設定に使用されます。IGMP スヌーピングは、特定のマルチキャスト伝送に含まれるべき VLAN のホストを動的に決定します。1 つ以上の VLAN に関連付けることができるマルチキャストポリシーを作成、変更、削除できます。マルチキャストポリシーが変更されると、そのマルチキャスト ポリシーに関連付けられたすべての VLAN が再処理され変更が適用されます。デフォルトでは、IGMP スヌーピングが有効になり、IGMP クエリアが無効になります。プライベート VLAN の場合、プライマリ VLAN にはマルチキャスト ポリシーを設定できますが、Cisco NX-OS 転送の実装により、プライマリ VLAN に関連付けられている独立 VLAN には設定できません。

マルチキャスト ポリシーには、次の制限事項およびガイドラインが適用されます。

- 6200 シリーズ ファブリック インターコネクトでは、ユーザ定義のマルチキャスト ポリシーをデフォルトのマルチキャスト ポリシーとともに割り当てることができます。
- グローバル VLAN で許可されるのは、デフォルトのマルチキャスト ポリシーだけです。
- Cisco UCS ドメイン に 6300 シリーズと 6200 シリーズのファブリック インターコネクトが含まれている場合は、どのマルチキャスト ポリシーでも割り当てることができます。

- ファブリック インターコネクトおよび関連付けられた LAN スイッチで同じ IGMP スヌーピング状態を使用することを強くお勧めします。たとえば、ファブリック インターコネクトで IGMP スヌーピングが無効にされている場合は、関連付けられているすべての LAN スイッチでも無効にする必要があります。

マルチキャスト ポリシーの作成

マルチキャスト ポリシーは、ルート組織でのみ作成でき、サブ組織では作成できません。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org**	指定した組織の組織モードを開始します。
ステップ 2	UCS-A /org # **create mcast-policy** *policy-name*	マルチキャスト ポリシーを指定されたポリシー名で作成し、組織マルチキャスト ポリシー モードを開始します。
ステップ 3	UCS-A /org/mcast-policy* # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、policy1 という名前のマルチキャスト ポリシーを作成する方法を示します。

```
UCS-A# scope org /
UCS-A /org # create mcast-policy policy1
UCS-A /org/mcast-policy* # commit-buffer
UCS-A /org/mcast-policy #
```

IGMP スヌーピング パラメータの設定

マルチキャスト ポリシーに対して IGMP スヌーピングをイネーブルまたはディセーブルにできます。デフォルトでは、IGMP スヌーピング状態はマルチキャスト ポリシーに対しイネーブルになっています。また、マルチキャスト ポリシーに対し IGMP スヌーピング クエリアの状態と IPv4 アドレスを設定することもできます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org**	指定した組織の組織モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /org # **create mcast-policy** *policy-name*	新しいマルチキャスト ポリシーを指定されたポリシー名で作成し、組織マルチキャスト ポリシー モードを開始します。
ステップ 3	UCS-A /org/mcast-policy* # **set querier**{**enabled** | **disabled**}	IGMP スヌーピング クエリアをイネーブルまたはディセーブルにします。デフォルトでは、IGMP スヌーピング クエリアは、マルチキャスト ポリシーに対しディセーブルになっています。
ステップ 4	UCS-A /org/mcast-policy* # **set querierip** *IGMP snooping querier IPv4 address*	IGMP スヌーピング クエリアの IPv4 アドレスを指定します。
ステップ 5	UCS-A /org/mcast-policy* # **set snooping**{**enabled** | **disabled**}	IGMP スヌーピングをイネーブルまたはディセーブルにします。デフォルトでは、IGMP スヌーピングは、マルチキャスト ポリシーに対しイネーブルになっています。
ステップ 6	UCS-A /org/mcast-policy* # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、policy1 という名前のマルチキャスト ポリシーを作成および開始する方法を示します。

```
UCS-A# scope org /
UCS-A /org # create mcast-policy policy1
UCS-A /org/mcast-policy* # set querier enabled
UCS-A /org/mcast-policy* # set querierip 1.2.3.4
UCS-A /org/mcast-policy* # set snooping enabled
UCS-A /org/mcast-policy* # commit-buffer
UCS-A /org/mcast-policy #
```

マルチキャスト ポリシー パラメータの変更

既存のマルチキャスト ポリシーを変更して、IGMP スヌーピングまたは IGMP スヌーピング クエリアの状態を変更することができます。マルチキャスト ポリシーが変更されると、そのマルチキャスト ポリシーに関連付けられたすべての VLAN が再処理され変更が適用されます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org**	指定した組織の組織モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /org # **scope mcast-policy** *policy-name*	組織マルチキャスト ポリシー モードを開始します。
ステップ 3	UCS-A /org/mcast-policy* # **set querier**{**enabled** | **disabled**}	IGMP スヌーピング クエリアをイネーブルまたはディセーブルにします。デフォルトでは、IGMP スヌーピング クエリアは、マルチキャスト ポリシーに対しディセーブルになっています。
ステップ 4	UCS-A /org/mcast-policy* # **set querierip** *IGMP snooping querier IPv4 address*	IGMP スヌーピング クエリアの IPv4 アドレスを指定します。
ステップ 5	UCS-A /org/mcast-policy* # **set snooping**{**enabled** | **disabled**}	IGMP スヌーピングをイネーブルまたはディセーブルにします。デフォルトでは、IGMP スヌーピングは、マルチキャスト ポリシーに対しイネーブルになっています。
ステップ 6	UCS-A /org/mcast-policy* # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、policy1 という名前のマルチキャスト ポリシーを作成する方法を示します。

```
UCS-A# scope org /
UCS-A /org # scope mcast-policy policy1
UCS-A /org/mcast-policy* # set querier enabled
UCS-A /org/mcast-policy* # set querierip 1.2.3.4
UCS-A /org/mcast-policy* # set snooping enabled
UCS-A /org/mcast-policy* # commit-buffer
UCS-A /org/mcast-policy #
```

VLAN マルチキャスト ポリシーの割り当て

VLAN のマルチキャスト ポリシーをイーサネット アップリンク ファブリック モードに設定できます。独立 VLAN のマルチキャスト ポリシーは設定できません。

はじめる前に

VLAN を作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネットアップリンク モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /eth-uplink # **scope fabric**{**a** | **b**}	指定したファブリック インターコネクトのイーサネット アップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /eth-uplink/fabric # **scope vlan** *vlan-name*	イーサネット アップリンク ファブリック VLAN モードを開始します。
ステップ 4	UCS-A /eth-uplink/fabric/vlan # **set mcastpolicy** *policy-name*	VLAN のマルチキャスト ポリシーを割り当てます。
ステップ 5	UCS-A /eth-uplink/fabric/vlan # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、1 つのファブリック インターコネクトにアクセス可能なネームド VLAN を設定し、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # scope vlan vlan1
UCS-A /eth-uplink/fabric/vlan # set mcastpolicy policy1
UCS-A /eth-uplink/fabric/vlan* # commit-buffer
UCS-A /eth-uplink/fabric/vlan #
```

マルチキャスト ポリシーの削除

（注） VLAN にデフォルト以外の（ユーザ定義）マルチキャスト ポリシーを割り当て、そのマルチキャスト ポリシーを削除すると、関連付けられた VLAN は削除済みポリシーが再作成されるまで、デフォルトのマルチキャストポリシーからマルチキャストポリシー設定を継承します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org**	指定した組織の組織モードを開始します。
ステップ 2	UCS-A /org # **delete mcast-policy** *policy-name*	指定されたポリシー名を持つマルチキャスト ポリシーを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、policy1 という名前のマルチキャスト ポリシーを削除する方法を示します。

```
UCS-A# scope org /
UCS-A /org # delete mcast-policy policy1
UCS-A /org* # commit-buffer
UCS-A /org #
```

LACP ポリシーの設定

LACP ポリシー

リンク集約は、複数のネットワーク接続を並列に組み合わせて、スループットを向上させ、冗長性を実現します。Link Aggregation Control Protocol（LACP）は、それらのリンク集約グループにさらに利点をもたらします。Cisco UCS Manager では、LACP ポリシーを使用して LACP のプロパティを設定することができます。

LACP ポリシーには以下を設定できます。

- **個別一時停止**：LACP でアップストリーム スイッチのポートを設定しない場合、ファブリック インターコネクトは、すべてのポートをアップリンク イーサネット ポートとして扱い、パケットを転送します。ループを回避するために、LACP ポートを一時停止状態にすることができます。LACP を使用してポートチャネルに個別一時停止を設定すると、そのポートチャネルの一部であるポートがピア ポートから PDU を受信しない場合、そのポートは一時停止状態になります。
- **タイマー値**：rate-fast または rate-normal を設定できます。rate-fast 設定では、ポートはピア ポートから 1 秒ごとに 1 PDU を受信します。このタイムアウトは 3 秒です。rate-normal 設定では、ポートは 30 秒ごとに 1 PDU を受信します。このタイムアウトは 90 秒です。

システムの起動時に、デフォルトの LACP ポリシーが作成されます。このポリシーを変更したり、新規のポリシーを作成できます。また、複数のポートチャネルに 1 つの LACP ポリシーを適用することもできます。

LACP ポリシーの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org**	ルート組織モードを開始します。
ステップ 2	UCS-A /org # **create lacppolicy***policy nam*.	指定された lacp ポリシーを作成します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、LACP ポリシーを作成し、トランザクションをコミットします。

```
UCS-A# scope org
UCS-A /org # create lacppolicy lacp1
UCS-A /org* # commit-buffer
UCS-A /org #
```

LACP ポリシーの編集

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org**	ルート組織モードを開始します。
ステップ 2	UCS-A /org # **scope lacppolicy** *policy-name*.	指定された lacp ポリシーを開始します。
ステップ 3	UCS-A /org/lacp policy/ policy-name # **set suspend-individual** *true*.	ポリシーに個々の一時停止を設定します。
ステップ 4	UCS-A /org/lacp policy/ policy-name # **set lacp-rate** *fast*.	ポリシーの LACP レートを設定します。
ステップ 5	UCS-A /org/lacp policy/ policy-name # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、lacp ポリシーを変更し、トランザクションをコミットする例を示します。

```
UCS-A# scope org
UCS-A/org # scope lacppolicy policy-name
UCS-A /org/lacp policy policy-name# set suspend-individual true
UCS-A/prg/policy policy-name# set lacp-rate fast
UCS-A /org* # commit-buffer
UCS-A /org #
```

LACP ポリシーのポート チャネルへの割り当て

デフォルトの lacp ポリシーは、ポートチャネルにデフォルトで割り当てられます。ポートチャネルに別の lacp ポリシーを割り当てることができます。割り当てられたポリシーが存在しない場合は、システムによりエラーが生成されます。エラーを取り除くために同じポリシーを作成できます。

（注） ポート チャネル、FCoE ポート チャネルおよびイーサネット ストレージのポート チャネルに lacp ポリシーを割り当てることができます。この手順では、ポート チャネルに lacp ポリシーを割り当てる方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope fabric**	ファブリック モードを開始します。
ステップ 3	UCS-A /eth-uplink/fabric # **scope port-channel**	ポート チャネル モードを開始します。
ステップ 4	UCS-A /eth-uplink/fabric/port-channel # **set lacp-policy-name***policy-name*	このポート チャネルに lacp ポリシーを指定します。
ステップ 5	UCS-A /eth-uplink/ fabric/port-channel **commit-buffer**	トランザクションをシステムにコミットします。

次に、ポート チャネルに lacp ポリシーを割り当てる例を示します。

```
UCS-A# scope eth-uplink
UCS-A UCS-A/eth-uplink # scope fabric
UCS-A UCS-A/eth-uplink/facric # scope port-channel
UCS-A UCS-A/eth-uplink/port-channel# set lacp-policy-name
UCS-A UCS-A/eth-uplink/port-channel# commit-buffer
```

UDLD リンク ポリシーの設定

UDLD の概要

UniDirectional Link Detection（UDLD）は、光ファイバまたはツイストペア イーサネット ケーブルを通して接続されたデバイスからケーブルの物理設定をモニタリングしたり、単一方向リンクの存在を検出できるようにするためのレイヤ 2 プロトコルです。このプロトコルが単一方向リンクを正常に識別してディセーブルにするには、接続されたすべてのデバイスで UDLD プロトコルがサポートされている必要があります。UDLD は、単一方向リンクを検出するとそのリンクを単方向としてマークします。単一方向リンクは、スパニングツリー トポロジループをはじめ、さまざまな問題を引き起こす可能性があります。

UDLD は、レイヤ 1 メカニズムと連動してリンクの物理ステータスを判断します。レイヤ 1 では、物理的シグナリングおよび障害検出は、自動ネゴシエーションによって処理されます。UDLD は、ネイバーの ID の検知、誤って接続されたインターフェイスのシャットダウンなど、自動ネゴシ

エーションでは実行不可能な処理を実行します。自動ネゴシエーションと UDLD の両方をイネーブルにすると、レイヤ 1 と 2 の検出機能が連動し、物理的および論理的な単一方向接続、および他のプロトコルの誤動作を防止します。

ローカル デバイスが送信したトラフィックをネイバーが受信するにもかかわらず、ネイバーから送信されたトラフィックをローカル デバイスが受信しない場合に、単一方向リンクが発生します。

動作モード

UDLD は、2 つの動作モードをサポートしています。通常（デフォルト）とアグレッシブです。通常モードの UDLD は、光ファイバ接続におけるインターフェイスの誤接続に起因する単一方向リンクを検出します。アグレッシブ モードの UDLD は、光ファイバ リンクやツイストペア リンク上の片方向トラフィックに起因する単一方向リンク、および光ファイバ リンク上のインターフェイスの誤接続に起因する単一方向リンクも検出できます。

通常モードの UDLD は、光ファイバインターフェイスの光ファイバが誤接続されている場合に単一方向リンクを検出しますが、レイヤ1メカニズムは、この誤接続を検出しません。インターフェイスが正しく接続されていてもトラフィックが片方向である場合は、単一方向リンクを検出するはずのレイヤ 1 メカニズムがこの状況を検出できないため、UDLD は単一方向リンクを検出できません。その場合、論理リンクは不明となり、UDLD はインターフェイスをディセーブルにしません。UDLD が通常モードのときに、ペアの一方の光ファイバが切断されており、自動ネゴシエーションがアクティブであると、レイヤ 1 メカニズムはリンクの物理的な問題を検出しないため、リンクは稼働状態でなくなります。この場合は、UDLD は何のアクションも行わず、論理リンクは不確定と見なされます。

デフォルトでは、UDLD アグレッシブ モードはディセーブルになっています。UDLD アグレッシブモードは、そのモードをサポートするネットワーク デバイス間のポイントツーポイントのリンク上に限って設定してください。UDLD アグレッシブ モードが有効になっている場合、UDLD ネイバー関係が確立されている双方向リンク上のポートが UDLD パケットを受信しなくなると、UDLD はネイバーとの接続の再確立を試み、影響を受けたポートを管理シャットダウンします。アグレッシブ モードの UDLD は、2 つのデバイス間の障害発生が許されないポイントツーポイント リンクの単一方向リンクも検出できます。また、次のいずれかの問題が発生している場合に、単一方向リンクも検出できます。

- 光ファイバまたはツイストペア リンクのインターフェイスの片方で、トラフィックの送受信ができない場合。
- 光ファイバまたはツイストペア リンクのインターフェイスの片方がダウン状態で、もう片方がアップ状態の場合。
- ケーブルのうち 1 本の光ファイバが切断されている。

単一方向リンクの検出方法

UDLD は 2 つのメカニズムを使用して動作します。

- ネイバー データベース メンテナンス

UDLD は、すべてのアクティブ インターフェイスで Hello パケット（別名アドバタイズメントまたはプローブ）を定期的に送信して、他のUDLD対応ネイバーについて学習し、各デバイスがネイバーに関しての最新情報を維持できるようにします。スイッチが hello メッセージを受信すると、エージング タイム（ホールド タイムまたは存続可能時間）が経過するまで、情報をキャッシュします。古いキャッシュ エントリの期限が切れる前に、スイッチが新しい hello メッセージを受信すると、古いエントリが新しいエントリで置き換えられます。

インターフェイスがディセーブルになりUDLDが実行中の場合、インターフェイスでUDLDがディセーブルになった場合、またはスイッチがリセットされた場合、UDLD は、設定変更によって影響を受けるインターフェイスの既存のキャッシュ エントリをすべてクリアします。UDLD は、ステータス変更の影響を受けるキャッシュの一部をフラッシュするようにネイバーに通知するメッセージを 1 つまたは複数送信します。このメッセージは、キャッシュを継続的に同期するためのものです。

- イベント駆動の検出およびエコー

  UDLD は検出メカニズムとしてエコーを利用します。UDLD デバイスが新しいネイバーを学習するか、または同期していないネイバーから再同期要求を受信すると、接続のUDLDデバイス側の検出ウィンドウを再起動して、エコー メッセージを返送します。この動作はすべてのUDLDネイバーに対して同様に行われるため、エコー送信側では返信エコーを受信するように待機します。

  検出ウィンドウが終了し、有効な応答メッセージが受信されなかった場合、リンクは、UDLD モードに応じてシャットダウンされることがあります。UDLD が通常モードにある場合、リンクは不確定と見なされ、シャットダウンされない場合があります。UDLD がアグレッシブ モードのときは、リンクは単一方向であると見なされ、インターフェイスはシャットダウンされます。

通常モードにある UDLD が、アドバタイズまたは検出段階にあり、すべてのネイバーのキャッシュ エントリが期限切れになると、UDLD はリンク起動シーケンスを再起動し、未同期の可能性のあるネイバーとの再同期を行います。

アグレッシブ モードをイネーブルにしていて、ポートのすべてのネイバーがアドバタイズまたは検出段階で期限切れになると、UDLD はリンク起動シーケンスを再起動し、未同期の可能性のあるネイバーとの再同期を行います。高速な一連のメッセージの送受信後に、リンク ステートが不確定のままの場合、UDLD はポートをシャットダウンします。

UDLD 設定時の注意事項

次のガイドラインと推奨事項は、UDLD を設定する場合に該当します。

- UDLD対応インターフェイスを別のスイッチのUDLD非対応ポートに接続すると、そのUDLD対応インターフェイスも単方向リンクを検出できなくなります。
- モード（通常またはアグレッシブ）を設定する場合、リンクの両側に同じモードを設定します。
- UDLD は、UDLD 対応デバイスに接続されているインターフェイスでのみ有効にする必要があります。次のインターフェイス タイプがサポートされます。

- イーサネット アップリンク
- FCoE アップリンク
- イーサネット アップリンク ポート チャネル メンバ
- FCoE アップリンク ポート チャネル メンバ

リンク プロファイルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** /	ルート組織モードを開始します。
ステップ 2	UCS-A /org # **create eth-link-profile** *link-profile-name*	指定された名前でリンク プロファイルを作成し、リンク プロファイル モードを開始します。
ステップ 3	UCS-A /org/eth-link-profile # **commit-buffer**	トランザクションをシステム設定にコミットします。
ステップ 4	UCS-A /org/eth-link-profile # **exit**	前のモードに戻ります。
ステップ 5	UCS-A /org # **scope eth-link-profile** *link-profile-name*	指定したリンク プロファイルのリンク プロファイル モードを開始します。
ステップ 6	UCS-A /org/eth-link-profile # **set udld-link-policy** *link-policy-name*	リンク プロファイルに指定した UDLD のリンク ポリシーを割り当てます。
ステップ 7	UCS-A /org/eth-link-profile # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、LinkProfile1 と呼ばれるリンク プロファイルを作成し、デフォルトの UDLD リンク ポリシーを割り当てる方法を示します。

```
UCS-A# scope org /
UCS-A /chassis/org # create eth-link-profile LinkProfile1
UCS-A /chassis/org/eth-link-profile* # commit-buffer
UCS-A /chassis/org/eth-link-profile # exit
UCS-A /chassis/org # scope eth-link-profile LinkProfile1
UCS-A /chassis/org/eth-link-profile # set udld-link-policy default
UCS-A /chassis/org/eth-link-profile* # commit-buffer
```

UDLD リンク ポリシーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** /	ルート組織モードを開始します。
ステップ 2	UCS-A /org # **create udld-link-policy** *link-policy-name*	UDLD リンク ポリシーを指定された名前で作成し、UDLD リンク ポリシー モードを開始します。
ステップ 3	UCS-A /org/udld-link-policy # **commit-buffer**	トランザクションをシステム設定にコミットします。
ステップ 4	UCS-A /org/udld-link-policy # **exit**	前のモードに戻ります。
ステップ 5	UCS-A /org # **scope udld-link-policy** *link-policy-name*	指定した UDLD リンク ポリシーの UDLD リンク ポリシー モードを開始します。
ステップ 6	UCS-A /org/udld-link-policy # **set mode** {**aggressive** | **normal**}	UDLD リンク ポリシーのモードを指定します。
ステップ 7	UCS-A /org/udld-link-policy # **set admin-state** {**disabled** | **enabled**}	インターフェイスの UDLD をディセーブルまたはイネーブルにします。
ステップ 8	UCS-A /org/udld-link-policy # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、UDLDPol1 と呼ばれるリンク プロファイルを作成し、モードをアグレッシブに設定し、インターフェイスの UDLD をイネーブルにする方法を示します。

```
UCS-A# scope org /
UCS-A /chassis/org # create udld-link-policy UDLDPol1
UCS-A /chassis/org/udld-link-policy* # commit-buffer
UCS-A /chassis/org/udld-link-policy # exit
UCS-A /chassis/org # scope udld-link-policy UDLDPol1
UCS-A /chassis/org/udld-link-policy # set mode aggressive
UCS-A /chassis/org/udld-link-policy* # set admin-state enabled
UCS-A /chassis/org/udld-link-policy* # commit-buffer
UCS-A /chassis/org/udld-link-policy #
```

UDLD システム設定の変更

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** /	ルート組織モードを開始します。
ステップ 2	UCS-A /org # **show udld-policy**	現在の UDLD のシステム設定を表示します。
ステップ 3	UCS-A /org # **scope udld-policy default**	グローバル UDLD ポリシーの UDLD ポリシーモードを開始します。
ステップ 4	UCS-A /org/udld-policy # **set message-interval** *seconds*	アドバタイズメントモードになっているポートで UDLD プローブ メッセージの時間間隔を秒単位で指定します。7 ～ 60 の整数を入力します。デフォルトは 15 秒です。
ステップ 5	UCS-A /org/udld-policy # **set recovery-action** [**reset** | **none**]	UDLD アグレッシブ モードがイネーブルのときにディセーブルになっているポート上で実行するアクションを指定します。デフォルトは none です。
ステップ 6	UCS-A /org/udld-policy # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、デフォルトの UDLD システム設定を 30 秒間隔で更新する例を示します。

```
UCS-A# scope org /
UCS-A /chassis/org # show udld-policy

UDLD system settings:
    Name       Message interval (sec) Recovery action
    ---------- ---------------------- ---------------
    default    15                     None

UCS-A /chassis/org # scope udld-policy default
UCS-A /chassis/org/udld-policy # set message-interval 30
UCS-A /chassis/org/udld-policy* # commit-buffer
UCS-A /chassis/org/udld-policy #
```

リンク プロファイルのポート チャネル イーサネット インターフェイスへの割り当て

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope fabric** {**a** | **b**}	指定されたファブリックのイーサネット アップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /eth-uplink/fabric # **scope port-channel** *port-chan-id*	指定されたポートチャネルのイーサネット アップリンク ファブリック ポート チャネル モードを開始します。
ステップ 4	UCS-A /eth-uplink/fabric/port-channel # **scope member-port** *slot-id port-id*	指定したメンバーポートでイーサネット サーバファブリック、ファブリック ポート チャネル モードを開始します。
ステップ 5	UCS-A /eth-uplink/fabric/port-channel/member-port # **set eth-link-profile** *link-profile-name*	指定したリンクのプロファイルを割り当てます。
ステップ 6	UCS-A /eth-uplink/fabric/port-channel/member-port # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、リンク プロファイル LinkProfile1 をポート チャネル イーサネット インターフェイスに割り当てる方法を示します。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # scope port-channel 88
UCS-A /eth-uplink/fabric/port-channel # scope member-port 1 31
UCS-A /eth-uplink/fabric/port-channel/member-port # set eth-link-profile LinkProfile1
UCS-A /eth-uplink/fabric/port-channel/member-port* # commit-buffer
UCS-A /eth-uplink/fabric/port-channel/member-port #
```

リンク プロファイルのポート チャネル FCoE インターフェイスへの割り当て

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b**}	指定したファブリックのファイバ チャネルアップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /fc-uplink/fabric # **scope fcoe-port-channel** *port-chan-id*	指定されたポート チャネルのファイバチャネルアップリンク ファブリック ポート チャネル モードを開始します。
ステップ 4	UCS-A /fc-uplink/fabric/fcoe-port-channel # **scope fcoe-member-port** *slot-id port-id*	指定したメンバ ポートのファイバ チャネル サーバ ファブリック、ファブリック ポート チャネル モードを開始します。
ステップ 5	UCS-A /fc-uplink/fabric/fcoe-port-channel/fcoe-member-port # **set eth-link-profile** *link-profile-name*	指定したリンクのプロファイルを割り当てます。
ステップ 6	UCS-A /fc-uplink/fabric/fcoe-port-channel/fcoe-member-port # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、リンク プロファイル LinkProfile1 をポート チャネル FCoE インターフェイスに割り当てる方法を示します。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # scope fcoe-port-channel 192
UCS-A /fc-uplink/fabric/fcoe-port-channel # scope fcoe-member-port 1 20
UCS-A /fc-uplink/fabric/fcoe-port-channel/fcoe-member-port # set eth-link-profile LinkProfile1
UCS-A /fc-uplink/fabric/fcoe-port-channel/fcoe-member-port* # commit-buffer
UCS-A /fc-uplink/fabric/fcoe-port-channel/fcoe-member-port #
```

リンク プロファイルのアップリンク イーサネット インターフェイスへの割り当て

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope fabric** {**a** | **b**}	指定されたファブリックのイーサネット アップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /eth-uplink/fabric # **scope interface** *slot-num port num*	指定されたアップリンク ポートのインターフェイス コマンド モードを開始します。
ステップ 4	UCS-A /eth-uplink/fabric/interface # **set eth-link-profile** *link-profile-name*	指定したリンクのプロファイルを割り当てます。
ステップ 5	UCS-A /eth-uplink/fabric/interface # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、リンク プロファイル LinkProfile1 をアップリンク イーサネット インターフェイスに割り当てる方法を示します。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # scope interface 2 2
UCS-A /eth-uplink/fabric/interface # set eth-link-profile LinkProfile1
UCS-A /eth-uplink/fabric/interface* # commit-buffer
UCS-A /eth-uplink/fabric/interface #
```

リンク プロファイルのアップリンク FCoE インターフェイスへの割り当て

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b**}	指定したファブリックのファイバチャネル アップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /fc-uplink/fabric # **scope fcoeinterface** *slot-num port num*	指定されたアップリンク ポートのファイバ チャネル インターフェイス コマンド モードを開始します。
ステップ 4	UCS-A /fc-uplink/fabric/fcoeinterface # **set eth-link-profile** *link-profile-name*	指定したリンクのプロファイルを割り当てます。
ステップ 5	UCS-A /fc-uplink/fabric/fcoeinterface # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、リンク プロファイル LinkProfile1 をアップリンク FCoE インターフェイスに割り当てる方法を示します。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # scope fcoeinterface 2 2
UCS-A /fc-uplink/fabric/fcoeinterface # set eth-link-profile LinkProfile1
UCS-A /fc-uplink/fabric/fcoeinterface* # commit-buffer
UCS-A /fc-uplink/fabric/fcoeinterface #
```

VMQ 接続ポリシーの設定

VMQ 接続ポリシー

Cisco UCS Manager では、vNIC に対し VMQ 接続ポリシーを設定することができます。VMQ により、管理オペレーティング システム全体のネットワーク パフォーマンスが向上します。VMQ vNIC 接続ポリシーを設定するには、次の作業を実行します。

- VMQ 接続ポリシーの作成
- サービス プロファイルでのスタティック vNIC の作成
- vNIC への VMQ 接続ポリシーの適用

サーバのサービス プロファイルで VMQ vNIC を設定する場合は、サーバ内の少なくとも 1 つのアダプタが VMQ をサポートしている必要があります。以下のアダプタのうち少なくとも 1 つがサーバにインストールされていることを確認してください。

- UCS-VIC-M82-8P
- UCSB-MLOM-40G-01
- UCSC-PCIE-CSC-02

以下は VMQ でサポートされるオペレーティング システムです。

- Windows 2012
- Windows 2012R2

サービス プロファイルで 1 度に適用できる vNIC 接続ポリシーは 1 つだけです。vNIC に対して 3 つのオプション（ダイナミック、usNIC、VMQ 接続ポリシー）のいずれか 1 つを選択してください。サービスプロファイルで VMQ vNIC が設定されている場合は、次のように設定されていることを確認してください。

- BIOS ポリシーで [SRIOV] を選択する。
- アダプタ ポリシーで [Windows] を選択する。

VMQ 接続ポリシーの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に **/** を入力します。
ステップ 2	UCS-A /org # **create vmq-conn-policy** *policy-name*	この VMQ 接続ポリシーの名前を指定します。
ステップ 3	UCS-A /org/vmq-conn-policy* # **set queue-count***queue count*	VMQ 接続ポリシーのキュー カウントを指定します。
ステップ 4	UCS-A /org/vmq-conn-policy* # **set interrupt-count***interrupt count*	VMQ 接続ポリシーの割り込み回数を指定します。
ステップ 5	UCS-A /org/vmq-conn-policy* # **commit-buffer**	トランザクションをシステムにコミットします。

次の例では、VMQ 接続ポリシーを作成します。

```
UCS-A# scope org
UCS-A /org # create vmq-conn-policy policy name
UCS-A /org/vmq-conn-policy* # set queue-count queue count (number)
UCS-A /org/vmq-conn-policy* # set interrupt-count queue count (number)
UCS-A /org/vmq-conn-policy* # commit-buffer
```

NetQueue

NetQueue について

NetQueueは、ネットワーク アダプタに複数の受信キューを提供することによってトラフィックのパフォーマンスを向上します。これらのキューにより、グループ化される個々の仮想マシンに関連付けられたデータ割り込み処理が可能になります。

（注） NetQueue は、VMware ESXi オペレーティング システムを実行しているサーバでサポートされます。

NetQueue の設定

手順

ステップ 1 仮想マシン キュー（VMQ）接続ポリシーを作成します。

ステップ 2 VMQ 接続ポリシーを選択することにより、サービス プロファイルに NetQueue を設定します。NetQueue を設定する場合は、次の事項を参考にしてください。

- デフォルトのリング サイズは受信 512、送信 256
- 各 VNIC の割り込み回数は VMQ 数 X 2 + 2

  （注） 割り込みの数は有効化されている NetQueue の数によって決まります。

- ドライバは標準フレーム構成の場合、ポートあたり最大 16 個の NetQueue をサポートします。

  （注） VMware は標準フレーム構成の場合、ポートあたり最大 8 個の NetQueue を使用することを推奨しています。

- NetQueue を有効にする必要があるのは MSIX システムでのみです。
- 1 GB NIC では NetQueue を無効にする必要があります。

ステップ 3 NetQueue のアダプタ ポリシーで MSIX モードを有効にします。

ステップ 4 サービス プロファイルをサーバに関連付けます。

第 21 章

アップストリーム分離レイヤ 2 ネットワークの設定

この章の内容は、次のとおりです。

アップストリーム分離レイヤ 2 ネットワーク

接続はしないものの、同一の Cisco UCS ドメイン 内に存在するサーバや仮想マシンがアクセスする必要がある 2 つ以上のイーサネット「クラウド」がある場合、レイヤ 2 ネットワークのアップストリーム分離（分離L2ネットワーク）が必要です。たとえば、次のいずれかが必要な場合、分離 L2 ネットワークを設定できます。

- パブリック ネットワークおよびバックアップ ネットワークにアクセスするサーバまたは仮想マシン
- マルチテナント システムでは、複数のカスタマー用のサーバまたは仮想マシンは同一の Cisco UCS ドメイン に存在し、両方のカスタマーのために L2 ネットワークにアクセスする必要があります。

（注） デフォルトでは、Cisco UCS 内のデータ トラフィックは相互包含の原則で動作します。VLAN およびアップストリーム ネットワークへのトラフィックはすべて、すべてのアップリンク ポートとポート チャネルで伝送されます。アップストリーム分離レイヤ 2 ネットワークをサポートしていないリリースからアップグレードする場合は、VLAN に適切なアップリンク インターフェイスを割り当てる必要があります。これを行わないと、VLAN へのトラフィックがすべてのアップリンク ポートとポート チャネルに流れ続けます。

分離 L2 ネットワークのコンフィギュレーションは、選択的排除の原則で動作します。分離ネットワークの一部として指定された VLAN へのトラフィックは、その VLAN に特別に割り当てられたポート チャネルまたはアップリンク イーサネット ポートだけを移動でき、他のすべてのアップリンク ポートおよびポート チャネルから選択的に除外されます。ただし、アップリンク イーサネット ポートまたはポート チャネルに特別に割り当てられていない VLAN へのトラフィックは、分離 L2 ネットワークへのトラフィックを伝送するものを含め、すべてのアップリンク ポートまたはポート チャネルを引き続き移動できます。

Cisco UCS では、VLAN がアップストリームの分離 L2 ネットワークを表します。分離 L2 ネットワーク向けのネットワーク トポロジを設計する際は、アップリンク インターフェイスを VLAN に割り当て、逆にならないようにする必要があります。

サポートされているアップストリーム分離 L2 ネットワークの最大数については、『*Cisco UCS Configuration Limits for Cisco UCS Manager Guide*』を参照してください。

アップストリーム分離L2ネットワークの設定に関するガイドライン

アップストリーム分離 L2 ネットワークの設定を計画する際は、次の事項を考慮してください。

イーサネット スイッチング モードはエンドホスト モードでなければならない

Cisco UCS は、ファブリック インターコネクトのイーサネット スイッチング モードがエンドホスト モードに設定された場合にのみ、分離 L2 ネットワークをサポートします。ファブリック インターコネクトのイーサネット スイッチング モードがスイッチ モードの場合、分離 L2 ネットワークに接続できません。

ハイ アベイラビリティのために対称構成を推奨

Cisco UCS ドメインが 2 個のファブリック インターコネクトでハイ アベイラビリティ用に設定されている場合、ファブリック インターコネクトの両方を同じ VLAN セットに設定することを推奨します。

VLAN の有効基準はアップリンク イーサネット ポートとポート チャネルで同一

分離 L2 ネットワークで使用する VLAN は、アップリンク イーサネット ポートまたはアップリンク イーサネット ポート チャネル向けに設定して、割り当てる必要があります。ポートまたはポー

トチャネルに VLAN が含まれていない場合、Cisco UCS Manager は VLAN が無効であると見なし、次の作業を行います。

- サーバの [ステータスの詳細（Status Details）] 領域に設定に関する警告を表示します。
- ポートまたはポートチャネルの設定を無視し、その VLAN のすべてのトラフィックをドロップします。

（注） 有効基準はアップリンク イーサネット ポートとアップリンク イーサネット ポート チャネルで同一です。Cisco UCS Manager はこの 2 つを区別しません。

重複 VLAN はサポート対象外

Cisco UCS は、分離 L2 ネットワーク内の重複 VLAN をサポートしません。各 VLAN が 1 つのアップストリーム分離 L2 ドメインだけに接続するようにする必要があります。

各 vNIC は 1 つの分離 L2 ネットワークとのみ通信できる

1 つの vNIC は 1 つの分離 L2 ネットワークとのみ通信できます。サーバが複数の分離 L2 ネットワークと通信する必要がある場合は、それらのネットワークにそれぞれ vNIC を設定する必要があります。

複数の分離 L2 ネットワークと通信するには、2 つ以上の vNIC をサポートする Cisco VIC アダプタをサーバに搭載する必要があります。

アプライアンス ポートにはアップリンク イーサネット ポートまたはポート チャネルと同じ VLAN を設定する必要がある

分離 L2 ネットワークと通信するアプライアンス ポートの場合は、最低 1 つのアップリンク イーサネット ポートまたはポートチャネルが同じネットワーク内にあり、それがアプライアンス ポートで使用される VLAN に割り当てられていることを確認する必要があります。Cisco UCS Manager がアプライアンス ポートのトラフィックを伝送するすべての VLAN を含むアップリンク イーサネット ポートまたはポート チャネルを識別できない場合、アプライアンス ポートにはピン接続障害が発生し、ダウン状態になります。

たとえば、Cisco UCS ドメイン には、ID が 500、名前が vlan500 のグローバル VLAN が含まれています。vlan500 はアップリンク イーサネット ポートでグローバル VLAN として作成されます。ただし、Cisco UCS Manager はアプライアンス ポートにこの VLAN を伝播しません。vlan500 をアプライアンス ポートに設定するには、ID が 500 で vlan500 という名前を持つ別の VLAN をアプライアンス ポートに作成する必要があります。この重複 VLAN は、Cisco UCS Manager GUI の [LAN] タブの [アプライアンス（Appliances）] ノードで、または Cisco UCS Manager CLI の **eth-storage** 範囲で作成できます。VLAN の重複チェックを求めるプロンプトが表示されたら、重複を受け入れると、Cisco UCS Manager はアプライアンス ポートの重複 VLAN を作成します。

デフォルトの VLAN 1 はアップリンク イーサネット ポートまたはポート チャネルで明示的に設定できない

Cisco UCS Manager は、暗黙的にすべてのアップリンク ポートおよびポート チャネルにデフォルト VLAN 1 を割り当てます。他の VLAN を設定しない場合でも、Cisco UCS はデフォルトの VLAN 1 を使用してすべてのアップリンク ポートおよびポート チャネルへのデータ トラフィックを扱います。

（注） Cisco UCS ドメイン の VLAN の設定後、デフォルト VLAN 1 はすべてのアップリンク ポートとポート チャネルとして暗黙的に残ります。デフォルトの VLAN 1 は、アップリンク ポートやポート チャネルに明示的に割り当てることができず、それらから削除することもできません。

特定のポートまたはポート チャネルにデフォルト VLAN 1 を割り当てようとすると、Cisco UCS Manager は [更新に失敗しました（Update Failed）] という障害を生成します。

したがって、Cisco UCS ドメインに分離 L2 ネットワークを設定する場合、そのサーバへのすべてのデータ トラフィックをすべてのアップリンク イーサネット ポートおよびポートチャネルで伝送させ、すべてのアップストリーム ネットワークに送信するのでない限り、どの vNIC にもデフォルト VLAN 1 を設定しないでください。

両方の FI の VLAN を同時に割り当てる必要がある

グローバル VLAN にポートを割り当てると、両方のファブリック インターコネクトの VLAN に明示的に割り当てられていないすべてのポートから VLAN が削除されます。両方の FI のポートを同時に設定する必要があります。1 番目の FI にのみポートを設定すると、2 番目の FI のトラフィックが中断されます。

アップストリーム分離L2ネットワークのピン接続に関する考慮事項

アップストリーム分離 L2 ネットワークと通信するには、ピン接続を適切に設定する必要があります。ソフト ピン接続とハード ピン接続のどちらを実装しているかにかかわらず、VLAN メンバーシップの不一致によって、1 つ以上の VLAN のトラフィックがドロップされることになります。

ソフト ピン接続

ソフト ピン接続は Cisco UCS のデフォルト動作です。ソフト ピン接続の実装を計画する場合は、LAN ピン グループを作成して vNIC のピン ターゲットを指定する必要はありません。代わりに、Cisco UCS Manager は VLAN メンバーシップ条件に応じて vNIC をアップリンク イーサネット ポートまたはポート チャネルにピン接続します。

ソフト ピン接続を使用すると、Cisco UCS Manager は vNIC からすべてのアップリンク イーサネット ポートおよびポート チャネルの VLAN メンバーシップに向けたデータ トラフィックを検証します。分離 L2 ネットワークを設定してある場合、Cisco UCS Manager は vNIC 上のすべての VLAN

に割り当てられたアップリンク イーサネット ポートまたはポート チャネルを検出できる必要があります。アップリンク イーサネット ポートまたはポート チャネルが vNIC のすべての VLAN で設定されていない場合、Cisco UCS Manager は次の動作を実行します。

- リンクをダウンさせます。
- vNIC のすべての VLAN のトラフィックをドロップします。
- 次のエラーを発生させます。
  - リンクダウン
  - VIF ダウン

Cisco UCS Manager は、VLAN 設定についてのエラーや警告は発生させません。

たとえば、サーバ上の vNIC に VLAN 101、102、103 が設定されているとします。インターフェイス 1/3 が VLAN 102 にだけ割り当てられています。インターフェイス 1/1 および 1/2 は VLAN に明示的に割り当てられていないため、VLAN 101 と 103 のトラフィックで利用できます。この設定の結果として、Cisco UCS ドメイン は vNIC が設定された 3 つの VLAN すべてへのトラフィックを伝送可能な境界ポート インターフェイスを含みません。その結果、Cisco UCS Manager は vNIC をダウンさせ、vNIC の 3 つの VLAN すべてのトラフィックをドロップし、リンク ダウンおよび VIF ダウン エラーを発生させます。

ハード ピン接続

ハード ピン接続は、LAN ピン グループを使用して、分離 L2 ネットワーク用のトラフィックにピン接続ターゲットを指定すると発生します。また、ピン接続ターゲットであるアップリンク イーサネット ポートやポート チャネルが、適切な分離 L2 ネットワークと通信できるように設定されている必要があります。

ハード ピン接続を使用すると、Cisco UCS Manager は vNIC からすべてのアップリンク イーサネット ポートおよびポート チャネルの VLAN メンバーシップに向けたデータ トラフィックを検証し、LAN ピン グループ設定に VLAN とアップリンク イーサネット ポートまたはポート チャネルが含まれているかどうかを検証します。検証がいずれかの時点で失敗した場合、Cisco UCS Manager は次の動作を実行します。

- 重大度が「警告」のピン接続 VLAN 不一致エラーを発生させます。
- VLAN へのトラフィックをドロップします。
- 他の VLAN へのトラフィックが継続して流れるようにするため、リンクはダウンさせません。

たとえば、VLAN 177 を使用するアップストリーム分離 L2 ネットワークにハード ピン接続を設定する場合は、次の手順を実行します。

- 分離 L2 ネットワークへのトラフィックを伝送するアップリンク イーサネット ポートまたはポート チャネルを持つ LAN ピン グループを作成します。
- サービス プロファイルで、VLAN 177 と LAN ピン グループを持つ少なくとも 1 つの vNIC を設定します。

- LAN ピン グループに含まれるアップリンク イーサネット ポートまたはポート チャネルに VLAN 177 を割り当てます

この設定が前述の 3 つのポイントのいずれかで失敗した場合、Cisco UCS Manager は VLAN 177 への VLAN 不一致について警告し、その VLAN へのトラフィックだけをドロップします。

（注） ソフト ピン接続の設定が変更され、その結果、vNIC VLAN が分離 L2 アップリンクで解決されなくなった場合は、警告ダイアログボックスが表示されます。警告ダイアログボックスでは、設定の続行または取り消しを選択できます。不適切な設定を続行すると、サーバのトラフィック パフォーマンスが低下します。

アップストリーム分離L2ネットワークに関するCiscoUCSの設定

アップストリーム分離 L2 ネットワークと接続する Cisco UCS ドメイン を設定する場合、次のすべてのステップを完了する必要があります。

はじめる前に

この設定を開始する前に、分離 L2 ネットワーク設定をサポートするために、ファブリック インターコネクトのポートが適切にケーブル接続されていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	イーサネット エンドホスト モードの両方のファブリック インターコネクトに対しイーサネット スイッチング モードを設定します。	Cisco UCS がアップストリーム分離 L2 ネットワークと通信できるようにするために、イーサネット スイッチング モードはエンドホスト モードである必要があります。
ステップ 2	分離 L2 ネットワークのトラフィックを伝送するために必要なポートおよびポート チャネルを設定します。	ポートおよびポート チャネルの設定, （65 ページ）を参照してください。
ステップ 3	該当するアップリンク イーサネット ポートまたはポート チャネルのトラフィックをピン接続するために必要な LAN ピン グループを設定します。	（任意） LAN ピン グループの設定, （283 ページ）を参照してください。
ステップ 4	1 つ以上の VLAN を作成します。	クラスタ設定では、 VLAN を作成することを推奨します。また、それらの VLAN がアップリンク イーサネット モードで両方のファブリック インターコネクトにアクセスできるよ

	コマンドまたはアクション	目的
		うにするために、共通/グローバル コンフィギュレーションを使用することを推奨します。 VLAN, （255 ページ）を参照してください。
ステップ 5	分離 L2 ネットワークの VLAN に目的のポートまたはポート チャネルを割り当てます。	このステップが完了した場合、それらの VLAN のトラフィックは、割り当てられたポート、ポート チャネル、またはその両方のトランクを介してのみ送信できます。 VLAN へのポートおよびポート チャネルの割り当て, （355 ページ）
ステップ 6	vNIC が適切な VLAN にトラフィックを送信できるようにするために、分離 L2 ネットワークと通信する必要があるすべてのサーバのサービス プロファイルに、正しい LAN 接続設定を含める必要があります。	1 つ以上の vNIC テンプレートを使用して、またはサービス プロファイルのネットワーク オプションを設定するときに、この設定を完了できます。 サービス プロファイル, （655 ページ）を参照してください。

VLAN へのポートおよびポート チャネルの割り当て

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope vlan** *vlan-name*	指定した VLAN でイーサネット アップリンク VLAN モードを開始します。
ステップ 3	UCS-A /eth-uplink/vlan # **create member-port** *fabric-interconnect slot-id port-id*	指定されたアップリンク イーサネット ポートに指定した VLAN を割り当てます。
ステップ 4	UCS-A /eth-uplink/vlan # **create member-port-channel** *fabric-interconnect member-port-chan-id*	指定されたアップリンク イーサネット ポート チャネルに指定された VLAN を割り当てます。
ステップ 5	UCS-A /eth-uplink/vlan # **commit-buffer**	トランザクションをシステム設定にコミットします。

	コマンドまたはアクション	目的
		ポートまたはポート チャネルを 1 つ以上の VLAN に割り当てると、他のすべての VLAN から削除されます。

次の例は、ファブリック インターコネクト A の VLAN100 というネームド VLAN にアップリンク イーサネット ポートを割り当て、トランザクションをコミットします。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope vlan VLAN100
UCS-A /eth-uplink/vlan # create member-port a 2
UCS-A /eth-uplink/vlan # create member-port a 4
UCS-A /eth-uplink/vlan* # commit-buffer
UCS-A /eth-uplink/vlan #
```

VLAN からのポートおよびポート チャネルの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope vlan** *vlan-name*	指定した VLAN でイーサネット アップリンク VLAN モードを開始します。
ステップ 3	UCS-A /eth-uplink/vlan # **delete member-port** *fabric-interconnect slot-id port-id*	指定したアップリンク イーサネット メンバー ポート割り当てを VLAN から削除します。
ステップ 4	UCS-A /eth-uplink/vlan # **delete member-port-channel** *fabric-interconnect member-port-chan-id*	指定したアップリンク イーサネット ポート チャネル割り当てを VLAN から削除します。
ステップ 5	UCS-A /eth-uplink/vlan # **commit-buffer**	トランザクションをシステム設定にコミットします。

	コマンドまたはアクション	目的
		重要 すべてのポートまたはポート チャネル インターフェイスを VLAN から削除すると、VLAN はデフォルトの動作に戻り、その VLAN 上のデータ トラフィックはすべてのアップリンク ポートとポート チャネル上で伝送されます。Cisco UCS ドメイン での設定によっては、このデフォルト動作により Cisco UCS Manager がその VLAN のトラフィックをドロップすることがあります。これを避けるには、少なくとも 1 つのインターフェイスを VLAN に割り当てるか、VLAN を削除することを推奨します。

次に、ファブリック インターコネクト A のアップリンク イーサネット ポート 2 と MyVLAN という名前の VLAN の間のアソシエーションを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope vlan MyVLAN
UCS-A /eth-uplink/vlan # delete member-port a 2
UCS-A /eth-uplink/vlan* # commit-buffer
UCS-A /eth-uplink/vlan #
```

VLAN に割り当てられたポートおよびポート チャネルの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope vlan** *vlan-name*	指定した VLAN でイーサネット アップリンク VLAN モードを開始します。
ステップ 3	UCS-A /eth-uplink/vlan # **show member-port** [**detail** | **expand**]	指定した VLAN に割り当てられているメンバー ポートを示します。
ステップ 4	UCS-A /eth-uplink/vlan # **show member-port-channel** [**detail** | **expand**]	指定した VLAN に割り当てられているメンバー ポート チャネルを表示します。

	コマンドまたはアクション	目的
ステップ 5	UCS-A /eth-uplink/vlan # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、MyVLAN という名前の VLAN に割り当てられているアップリンク イーサネット ポートの詳細を表示する例を示します。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope vlan MyVLAN
UCS-A /eth-uplink/vlan # show member-port detail
Member Port:
    Fabric ID: A
    Slot ID: 1
    Port ID: 2
    Mark Native Vlan: No
UCS-A /eth-uplink/vlan #
```

第 22 章

ネームド VSAN の設定

この章の内容は、次のとおりです。

ネームド VSAN

ネームド VSAN は、所定の外部 SAN への接続を作成します。VSAN は、その外部 SAN へのトラフィックを切り離しますが、これにはブロードキャスト トラフィックも含まれます。1 つのネームド VSAN のトラフィックは、別のネームド VSAN にトラフィックが存在していることを認識しますが、そのトラフィックの読み取りまたはアクセスはできません。

ネームドVLANと同様、VSAN IDに名前を割り当てると、抽象レイヤが追加されます。これにより、ネームドVSANを使用するサービスプロファイルに関連付けられたすべてのサーバをグローバルにアップデートすることができます。外部SANとの通信を維持するために、サーバを個別に再設定する必要はありません。同じ VSAN ID を使用して、複数のネームド VSAN を作成できます。

クラスタ設定内のネームド VSAN

クラスタ構成では、1つのファブリックインターコネクトのファイバチャネルアップリンク ポート、または両方のファブリック インターコネクトのファイバ チャネル アップリンク ポートにアクセスできるように、ネームド VSAN を設定できます。

ネームド VSAN と FCoE VLAN ID

それぞれのネームド VSAN に FCoE VLAN ID を設定する必要があります。このプロパティは、VSAN およびそのファイバ チャネル パケットの送信に、どの VLAN が使用されるかを決定します。

Cisco UCS CNA M72KR-Q や Cisco UCS CNA M72KR-E などの FIP 対応統合型ネットワーク アダプタの場合は、FCoE VLAN ID のネイティブ VLAN ではないネームド VLAN を使ってネームド VSAN を設定する必要があります。この設定により、FCoE トラフィックがこれらのアダプタを通過できることが保証されます。

次のサンプルの設定では、ファブリック A にマッピングされる vNIC および vHBA を含むサービス プロファイルが、FIP 対応の統合型ネットワーク アダプタを搭載したサーバに関連付けられます。

- vNIC は、VLAN 10 を使用するように設定されます。
- VLAN 10 は、vNIC 用のネイティブ VLAN としても指定されます。
- vHBA は、VSAN 2 を使用するように設定されます。
- そのため、VLAN 10 を FCoE VLAN ID として、VSAN 2 を設定することはできません。VSAN 2 は、ファブリック A 上で設定された他のどの VLAN にもマッピングもできます。

ネームド VSAN のファイバチャネル アップリンク トランキング

各ファブリック インターコネクトのネームド VSAN にファイバ チャネル アップリンク トランキングを設定できます。ファブリック インターコネクトのトランキングをイネーブルにすると、そのファブリック インターコネクトのすべてのファイバ チャネル アップリンク ポートで、Cisco UCS ドメイン のすべてのネームド VSAN が許可されます。

VSAN に関するガイドラインおよび推奨事項

次のガイドラインと推奨事項は、ストレージ VSAN を含め、すべてのネームド VSAN に適用されます。

VSAN 4079 は予約済み VSAN ID です。

VSAN を 4079 に設定しないでください。この VSAN は予約されており、FC スイッチ モードや FC エンドホスト モードでは使用できません。

ID 4079 でネームド VSAN を作成すると、Cisco UCS Manager はその VSAN をエラーと見なし、障害を生成します。

FC スイッチ モードのネームド VSAN 用に予約された VSAN 範囲

Cisco UCS ドメイン FC スイッチ モードを使用する予定の場合は、ID が 3040 ～ 4078 の範囲にある VSAN を設定しないでください。

ファブリック インターコネクトが FC スイッチ モードで動作するように設定されている場合、その範囲内の VSAN は動作しません。Cisco UCS Manager はその VSAN をエラーと見なし、障害を生成します。

FC エンドホスト モードのネームド VSAN 用に予約された VSAN 範囲

Cisco UCS ドメイン FC エンドホスト モードを使用する予定の場合は、ID が 3840 ～ 4079 の範囲にある VSAN を設定しないでください。

Cisco UCS ドメイン 内に次の状況が存在する場合、その範囲内の VSAN は動作しません。

- ファブリック インターコネクトが FC エンドホスト モードで動作するように設定されている。
- Cisco UCS ドメイン にファイバ チャネル トランキングまたは SAN ポート チャネルが設定されている。

これらの設定が存在する場合、Cisco UCS Manager は次の操作を実行します。

1. 3840 ～ 4079 の ID を持つすべての VSAN を使用不能にします。
2. 動作しない VSAN に対して障害を生成します。
3. デフォルトの VSAN にすべての非動作 VSAN を転送します。
4. 非動作 VSAN に関連付けられたすべての vHBA をデフォルトの VSAN に転送します。

ファイバ チャネル トランキングを無効にして、既存の SAN ポート チャネルのいずれかを削除すると、Cisco UCS Manager は 3840 ～ 4078 の範囲のすべての VSAN を動作状態に戻し、関連付けられている vHBA をそれらの VSAN に復元します。

FC スイッチ モードのネームド VSAN ID の範囲に関する制約事項

Cisco UCS ドメイン で FC スイッチ モードの使用を計画している場合は、3040 ～ 4078 の範囲に VSAN を設定しないでください。

FC スイッチ モードで動作するファブリック インターコネクトがアップストリーム スイッチとして MDS に接続されている場合、Cisco UCS Manager で 3040 ～ 4078 の範囲に設定され、ポート VSAN として割り当てられた VSAN は、MDS で作成できません。この設定では、ポート VSAN の不一致が発生する可能性があります。

FCoE VLAN ID に関するガイドライン

（注） SAN クラウドの FCoE VLAN と LAN クラウドの VLAN の ID が同じであってはなりません。VSAN 内の FCoE VLAN と VLAN で同じ ID を使用すると、その FCoE VLAN を使用しているすべての vNIC とアップリンク ポートで重大な障害が発生し、トラフィックが中断されます。FCoE VLAN ID と重なる ID が設定されたすべての VLAN 上でイーサネット トラフィックがドロップされます。

VLAN 4048 はユーザが設定可能です。ただし、Cisco UCS Manager では、VLAN 4048 が次のデフォルト値に使用されます。4048 を VLAN に割り当てる場合は、これらの値を再設定する必要があります。

- Cisco UCS リリース 2.0 へのアップグレード後：FCoE ストレージ ポートのネイティブ VLAN は、デフォルトで VLAN 4048 を使用します。デフォルト FCoE VSAN が、アップグレード前に VLAN 1 を使用するように設定されていた場合は、使用または予約されていない VLAN ID に変更する必要があります。たとえば、デフォルトを 4049 に変更することを検討します（その VLAN ID が使用されていない場合）。
- Cisco UCS リリース 2.0 の新規インストール後：デフォルト VSAN 用の FCoE VLAN は、デフォルトで VLAN 4048 を使用します。FCoE ストレージ ポート ネイティブ VLAN は VLAN 4049 を使用します。

両方のファブリックインターコネクトにアクセス可能なネームド VSAN の作成（ファイバ チャネル アップリンク モード）

（注） SAN クラウドの FCoE VLAN と LAN クラウドの VLAN の ID が同じであってはなりません。VSAN 内の FCoE VLAN と VLAN で同じ ID を使用すると、その FCoE VLAN を使用しているすべての vNIC とアップリンク ポートで重大な障害が発生し、トラフィックが中断されます。FCoE VLAN ID と重なる ID が設定されたすべての VLAN 上でイーサネット トラフィックがドロップされます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **create vsan** *vsan-name vsan-id fcoe-id*	指定されたネームド VSAN を作成し、VSAN の名前、VSAN ID および FCoE VLAN ID を指定し、ファイバ チャネル アップリンク VSAN モードを開始します。 • Cisco UCS リリース 2.0 へのアップグレード後：FCoE ストレージ ポートのネイティブ VLAN は、デフォルトで VLAN 4048 を使用します。デフォルト FCoE VSAN が、アップグレード前に VLAN 1 を使用するように設定されていた場合は、使用または予約されていない VLAN ID に変更する必要があります。たとえば、デフォルトを 4049 に変更することを検討します（その VLAN ID が使用されていない場合）。 • Cisco UCS リリース 2.0 の新規インストール後：デフォルト VSAN 用の FCoE VLAN は、デフォルトで VLAN 4048 を使用します。FCoE ストレージ ポート ネイティブ VLAN は VLAN 4049 を使用します。
ステップ 3	UCS-A /fc-uplink/vsan # **set fc-zoning** {**disabled** | **enabled**}	次のように、VSAN に対するファイバ チャネル ゾーン分割を設定します。 • [disabled]：アップストリーム スイッチがファイバ チャネルゾーン分割を設定および制御します。または、ファイバ チャネル ゾーン分割がこの VSAN で実行されません。

	コマンドまたはアクション	目的
		• [enabled]：Cisco UCS Manager がファイバ チャネル ゾーン分割を設定し、制御します。
ステップ 4	UCS-A /fc-uplink/vsan # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、両方のファブリック インターコネクト用のネームド VSAN を作成し、VSAN に accounting という名前を付け、VSAN ID 2112 を割り当て、FCoE VLAN ID 4021 を割り当て、Cisco UCS Manager ベースのファイバ チャネル ゾーン分割について VSAN をイネーブルにし、トランザクションをコミットします。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink* # create vsan accounting 2112 4021
UCS-A /fc-uplink/vsan # set fc-zoning enabled
UCS-A /fc-uplink/vsan* # commit-buffer
UCS-A /fc-uplink/vsan #
```

両方のファブリックインターコネクトにアクセス可能なネームド VSAN の作成（ファイバ チャネル ストレージ モード）

（注） SAN クラウドの FCoE VLAN と LAN クラウドの VLAN の ID が同じであってはなりません。VSAN 内の FCoE VLAN と VLAN で同じ ID を使用すると、その FCoE VLAN を使用しているすべての vNIC とアップリンク ポートで重大な障害が発生し、トラフィックが中断されます。FCoE VLAN ID と重なる ID が設定されたすべての VLAN 上でイーサネット トラフィックがドロップされます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-storage**	ファイバ チャネル ストレージ モードを開始します。
ステップ 2	UCS-A /fc-storage # **create vsan** *vsan-name vsan-id fcoe-id*	指定されたネームド VSAN を作成し、VSAN の名前、VSAN ID および FCoE VLAN ID を指定し、ファイバ チャネル ストレージ VSAN モードを開始します。

	コマンドまたはアクション	目的
		• Cisco UCS リリース 2.0 へのアップグレード後：FCoE ストレージ ポートのネイティブ VLAN は、デフォルトで VLAN 4048 を使用します。デフォルト FCoE VSAN が、アップグレード前に VLAN 1 を使用するように設定されていた場合は、使用または予約されていない VLAN ID に変更する必要があります。たとえば、デフォルトを 4049 に変更することを検討します（その VLAN ID が使用されていない場合）。 • Cisco UCS リリース 2.0 の新規インストール後：デフォルト VSAN 用の FCoE VLAN は、デフォルトで VLAN 4048 を使用します。FCoE ストレージ ポート ネイティブ VLAN は VLAN 4049 を使用します。
ステップ 3	UCS-A /fc-storage/vsan # **create member-port** {**fc** | **fcoe**} {**a** | **b**} *slot-id port-id*	メンバ ポートを作成し、ポート タイプ、ファブリック、スロット ID およびポート ID かを指定します。
ステップ 4	UCS-A /fc-storage/vsan # **set fc-zoning** {**disabled** | **enabled**}	次のように、VSAN に対するファイバ チャネル ゾーン分割を設定します。 • [disabled]：アップストリーム スイッチがファイバ チャネル ゾーン分割を設定および制御します。または、ファイバ チャネル ゾーン分割がこの VSAN で実行されません。 • [enabled]：Cisco UCS Manager がファイバ チャネル ゾーン分割を設定し、制御します。
ステップ 5	UCS-A /fc-storage/vsan # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、ネームド VSAN を作成し、VSAN に finance という名前を付け、VSAN ID 3955 を割り当て、FCoE VLAN ID 4021 を割り当て、メンバ ポートを作成してメンバ ポート A、スロット 1 ポート 40 に割り当て、Cisco UCS Manager ベースのファイバ チャネル ゾーン分割について VSAN をイネーブルにし、トランザクションをコミットします。

```
UCS-A# scope fc-storage
UCS-A /fc-storage/ # create VSAN finance 3955 4021
UCS-A /fc-storage/vsan # create member-port fcoe a 1 40
UCS-A /fc-storage/vsan # set fc-zoning enabled
UCS-A /fc-storage/vsan/member-port* # commit-buffer
UCS-A /fc-storage/vsan/member-port #
```

1 つのファブリック インターコネクトにアクセス可能なネームド VSAN の作成（ファイバ チャネル アップリンク モード）

（注） SAN クラウドの FCoE VLAN と LAN クラウドの VLAN の ID が同じであってはなりません。VSAN 内の FCoE VLAN と VLAN で同じ ID を使用すると、その FCoE VLAN を使用しているすべての vNIC とアップリンク ポートで重大な障害が発生し、トラフィックが中断されます。FCoE VLAN ID と重なる ID が設定されたすべての VLAN 上でイーサネット トラフィックがドロップされます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b**}	指定したファブリック インターコネクト（A または B）のファイバ チャネル アップリンク ファブリック インターコネクト モードを開始します。
ステップ 3	UCS-A /fc-uplink/fabric # **create vsan** *vsan-name vsan-id fcoe-id*	指定されたネームド VSAN を作成し、VSAN の名前、VSAN ID および FCoE VLAN ID を指定し、ファイバ チャネル アップリンク VSAN モードを開始します。 • Cisco UCS リリース 2.0 へのアップグレード後：FCoE ストレージ ポートのネイティブ VLAN は、デフォルトで VLAN 4048 を使用します。デフォルト FCoE VSAN が、アップグレード前に VLAN 1 を使用するように設定されていた場合は、使用または予約されていない VLAN ID に変更する必要があります。たとえば、デフォルトを 4049 に変更することを検討します（その VLAN ID が使用されていない場合）。 • Cisco UCS リリース 2.0 の新規インストール後：デフォルト VSAN 用の FCoE VLAN は、デフォルトで VLAN 4048 を使用します。FCoE ストレージ ポート ネイティブ VLAN は VLAN 4049 を使用します。
ステップ 4	UCS-A /fc-uplink/vsan # **set fc-zoning** {**disabled** | **enabled**}	次のように、VSAN に対するファイバ チャネル ゾーン分割を設定します。

	コマンドまたはアクション	目的
		• [disabled]：アップストリーム スイッチがファイバ チャネル ゾーン分割を設定および制御します。または、ファイバ チャネル ゾーン分割がこの VSAN で実行されません。 • [enabled]：Cisco UCS Manager がファイバ チャネル ゾーン分割を設定し、制御します。
ステップ 5	UCS-A /fc-uplink/fabric/vsan # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、ファブリック インターコネクト A 用のネームド VSAN を作成し、VSAN に finance という名前を付け、VSAN ID 3955 を割り当て、FCoE VLAN ID 2221 を割り当て、Cisco UCS Manager ベースのファイバ チャネル ゾーン分割について VSAN をイネーブルにし、トランザクションをコミットします。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # create vsan finance 3955 2221
UCS-A /fc-uplink/vsan # set fc-zoning enabled
UCS-A /fc-uplink/fabric/vsan* # commit-buffer
UCS-A /fc-uplink/fabric/vsan #
```

1 つのファブリック インターコネクトにアクセス可能なネームド VSAN の作成（ファイバ チャネル ストレージ モード）

（注） SAN クラウドの FCoE VLAN と LAN クラウドの VLAN の ID が同じであってはなりません。VSAN 内の FCoE VLAN と VLAN で同じ ID を使用すると、その FCoE VLAN を使用しているすべての vNIC とアップリンク ポートで重大な障害が発生し、トラフィックが中断されます。FCoE VLAN ID と重なる ID が設定されたすべての VLAN 上でイーサネット トラフィックがドロップされます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-storage**	ファイバ チャネル ストレージ モードを開始します。
ステップ 2	UCS-A /fc-storage #**scope fabric** {**a** | **b**}	指定したファブリック インターコネクトのファイバチャネル ストレージ モードを開始します。
ステップ 3	UCS-A /fc-storage/fabric #**create vsan** *vsan-name vsan-id fcoe-id*	指定されたネームド VSAN を作成し、VSAN の名前、VSAN ID および FCoE VLAN ID を指定し、ファイバ チャネル ストレージ VSAN モードを開始します。 • Cisco UCS リリース 2.0 へのアップグレード後：FCoE ストレージ ポートのネイティブ VLAN は、デフォルトで VLAN 4048 を使用します。デフォルト FCoE VSAN が、アップグレード前に VLAN 1 を使用するように設定されていた場合は、使用または予約されていない VLAN ID に変更する必要があります。たとえば、デフォルトを 4049 に変更することを検討します（その VLAN ID が使用されていない場合）。 • Cisco UCS リリース 2.0 の新規インストール後：デフォルト VSAN 用の FCoE VLAN は、デフォルトで VLAN 4048 を使用します。FCoE ストレージ ポート ネイティブ VLAN は VLAN 4049 を使用します。
ステップ 4	UCS-A /fc-storage/fabric/vsan #**create member-port** {**fc** | **fcoe**} {**a** | **b**} *slot-id port-id*	指定された VSAN のメンバ ポートを作成します。
ステップ 5	UCS-A /fc-storage/vsan # **set fc-zoning** {**disabled** | **enabled**}	次のように、VSAN に対するファイバチャネルゾーン分割を設定します。 • [disabled]：アップストリーム スイッチがファイバ チャネルゾーン分割を設定および制御します。または、ファイバ チャネル ゾーン分割がこの VSAN で実行されません。 • [enabled]：Cisco UCS Manager がファイバ チャネル ゾーン分割を設定し、制御します。
ステップ 6	UCS-A /fc-storage/fabric/vsan #**commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、ファブリック A にネームド VSAN を作成し、VSAN に finance という名前を付け、VSAN ID 3955 を割り当て、FCoE VLAN ID 2221 を割り当て、メンバポートを作成してメンバポート A、スロット 1 ポート 40 に割り当て、トランザクションをコミットします。

```
UCS-A# scope fc-storage
UCS-A /fc-storage/ # scope fabric a
UCS-A /fc-storage/fabric # create VSAN finance 3955 2221
UCS-A /fc-storage/fabric/vsan # create member-port a 1 40
UCS-A /fc-storage/fabric/vsan # set fc-zoning enabled
UCS-A /fc-storage/fabric/vsan/member-port* # commit-buffer
UCS-A /fc-storage/fabric/vsan/member-port #
```

ネームド VSAN の削除

Cisco UCS Manager に、削除する VSAN と同じ VSAN ID を持つネームド VLAN が含まれている場合、この ID を持つネームド VSAN がすべて削除されるまで、この VSAN はファブリック インターコネクト設定から削除されません。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバチャネルアップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **delete vsan** *vsan-name*	指定されたネームド VSAN を削除します。
ステップ 3	UCS-A /fc-uplink # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、ネームド VSAN を削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # delete vsan finance
UCS-A /fc-uplink* # commit-buffer
UCS-A /fc-uplink #
```

ネームド VSAN の FCoE ネイティブ VLAN の VLAN ID の変更

（注） SAN クラウドの FCoE VLAN と LAN クラウドの VLAN の ID が同じであってはなりません。VSAN 内の FCoE VLAN と VLAN で同じ ID を使用すると、その FCoE VLAN を使用しているすべての vNIC とアップリンク ポートで重大な障害が発生し、トラフィックが中断されます。FCoE VLAN ID と重なる ID が設定されたすべての VLAN 上でイーサネット トラフィックがドロップされます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバチャネルアップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope vsan** *vsan-name*	指定されたネームド VSAN の VSAN モードが開始されます。
ステップ 3	UCS-A /fc-uplink/vsan # **set fcoe-vlan** *fcoe-vlan-id*	ファイバ チャネル接続に使用される VLAN に割り当てられた固有識別情報を設定します。
ステップ 4	UCS-A /fc-uplink/vsan # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、finance というネームド VSAN の FCoE ネイティブ VLAN の VLAN ID を 4000 に変更し、トランザクションをコミットします。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope vsan finance
UCS-A /fc-uplink/vsan # set fcoe-vlan 4000
UCS-A /fc-uplink/vsan* # commit-buffer
UCS-A /fc-uplink/vsan #
```

ストレージ VSAN の FCoE ネイティブ VLAN の VLAN ID の変更

（注） SAN クラウドの FCoE VLAN と LAN クラウドの VLAN の ID が同じであってはなりません。VSAN 内の FCoE VLAN と VLAN で同じ ID を使用すると、その FCoE VLAN を使用しているすべての vNIC とアップリンク ポートで重大な障害が発生し、トラフィックが中断されます。FCoE VLAN ID と重なる ID が設定されたすべての VLAN 上でイーサネット トラフィックがドロップされます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-storage**	ファイバチャネル ストレージ モードを開始します。
ステップ 2	UCS-A /fc-storage #**set fcoe-storage-native-vlan** *fcoe-id*	ファイバ チャネル接続に使用される VLAN に割り当てられた固有識別情報を設定します。
ステップ 3	UCS-A /fc-storage #**commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、finance というストレージ VSAN の FCoE ネイティブ VLAN の VLAN ID を 4000 に変更し、トランザクションをコミットします。

```
UCS-A# scope fc-storage
UCS-A /fc-storage # set fcoe-storage-native-vlan 4000
UCS-A /fc-storage* # commit-buffer
UCS-A /fc-storage #
```

ファイバチャネルアップリンクのトランキングのイネーブル化またはディセーブル化

（注） ファブリック インターコネクトがファイバ チャネル エンドホスト モードに設定されている場合、ファイバ チャネル アップリンク トランキングを有効にすると、ID が 3840 ～ 4079 の範囲にあるすべての VSAN が動作不能になります。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b** }	指定したファブリックでファイバチャネル アップリンク モードを開始します。
ステップ 3	UCS-A /fc-uplink/fabric # **set uplink-trunking** {**enabled** | **disabled** }	アップリンクのトランキングをイネーブルまたはディセーブルにします。
ステップ 4	UCS-A /fc-uplink/fabric # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、ファブリック A のファイバ チャネル アップリンクのトランキングをイネーブルにし、トランザクションをコミットする例を示します。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # set uplink-trunking enabled
UCS-A /fc-uplink/fabric* # commit-buffer
UCS-A /fc-uplink/fabric #
```

第 23 章

SAN ピン グループの設定

この章の内容は、次のとおりです。

SAN ピン グループ

Cisco UCS では、SAN ピン グループを使用して、サーバ上の vHBA からのファイバ チャネル トラフィックがファブリック インターコネクト上のアップリンク ファイバ チャネル ポートへピン接続されます。このピン接続を使用して、サーバからのトラフィックの分散を管理できます。

（注） ファイバ チャネル スイッチ モードでは、SAN ピン グループは不適切です。既存の SAN ピン グループはすべて無視されます。

ピン接続をサーバに設定するには、SAN ピン グループを vHBA ポリシーに含める必要があります。その後、vHBA ポリシーは、そのサーバに割り当てられたサービス プロファイルに取り込まれます。vHBA からのすべてのトラフィックは、I/O モジュールを経由して、指定されたアップリンク ファイバ チャネル ポートへ移動します。

同じピン グループを複数の vHBA ポリシーに割り当てられます。したがって、vHBA ごとに手動でトラフィックをピン接続する必要はありません。

重要 既存の SAN ピン グループのターゲット インターフェイスを変更すると、そのピン グループを使用するすべての vHBA のトラフィックが中断されます。ファイバ チャネル プロトコルでトラフィックを再びピン接続するために、ファブリック インターコネクトからログインとログアウトが実行されます。

SAN ピン グループの設定

2 つのファブリック インターコネクトを持つシステムでピン グループとの関連付けができるのはのは、1 つのファブリック インターコネクト、または両方のファブリック インターコネクトだけです。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **create pin-group** *pin-group-name*	ファイバ チャネル（SAN）のピン グループを指定された名前で作成し、ファイバ チャネル アップリンクのピン グループ モードを開始します。
ステップ 3	UCS-A /fc-uplink/pin-group # **set descr** *description*	（任意） ピン グループに説明を加えます。 （注） 説明にスペース、特殊文字、または句読点が含まれている場合は、説明を引用符で括る必要があります。引用符は、**show** コマンド出力の説明フィールドには表示されません。
ステップ 4	UCS-A /fc-uplink/pin-group # **set target** {**a** | **b** | **dual**} **port** *slot-num*/ *port-num*	（任意） 指定したファブリックとポートにファイバ チャネル ピン ターゲットを設定します。
ステップ 5	UCS-A /fc-uplink/pin-group # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、fcpingroup12 という名前の SAN ピン グループを作成し、ピン グループに説明を加え、スロット 2 のポート 1 にピン グループのターゲットを設定し、トランザクションをコミットします。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # create pin-group fcpingroup12
UCS-A /fc-uplink/pin-group* # set descr "This is my pin group #12"
UCS-A /fc-uplink/pin-group* # set target a port 2/1
UCS-A /fc-uplink/pin-group* # commit-buffer
UCS-A /fc-uplink/pin-group #
```

次の作業

ピン グループを vHBA テンプレートに含めます。

FCoE ピン グループの設定

FCoE ピン グループを作成して、ピン グループ ターゲットとして FCoE アップリンク ポートを指定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	FC アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **create pin-group fcoepingroup**	FCoE ピン グループを指定された名前で作成し、FCoE アップリンクのピン グループ モードを開始します。
ステップ 3	UCS-A /fc-uplink/pin-group # **set target a fcoe-port 1/8**	このピン グループのターゲット ポートとして FCoE ポート 1/8 を設定します。
ステップ 4	UCS-A /fc-uplink/pin-group # **commit-buffer**	トランザクションをシステム設定にコミットします。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # create pin-group fcoepingroup
UCS-A /fc-uplink/pin-group* #set target a fcoe-port 1/8
UCS-A /fc-uplink/pin-group* # commit-buffer
UCS-A /fc-uplink/pin-group #
```

第 24 章

WWN プールの設定

この章の内容は、次のとおりです。

WWN プール

ワールド ワイド名（WWN）のプールは、Cisco UCS ドメイン 内のファイバ チャネル vHBA で使用される WWN のコレクションです。次の独立したプールを作成します。

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

重要

WWN プールは、20:00:00:00:00:00:00:00 ～ 20:FF:FF:FF:FF:FF:FF:FF、または 50:00:00:00:00:00:00:00 ～ 5F:FF:FF:FF:FF:FF:FF:FF の範囲内の WWNN または WWPN だけを含めることができます。その他の WWN 範囲はすべて予約されています。SAN ファブリックで Cisco UCS WWNN と WWPN の一意性を確保するには、プール内のすべてのブロックに WWN プレフィックスとして 20:00:00:25:B5:XX:XX:XX を使用することをお勧めします。

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

WWN をブロック単位でプールに割り当てます。

WWNN プール

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

WWPN プール

WWPN プールは、WW ポート名だけを含む WWN プールです。サービス プロファイルに WWPN のプールを含めると、関連付けられたサーバの各 vHBA 上のポートは、そのプールから WWPN を割り当てられます。

WWxN プール

WWXN プールは、WW ノード名および WW ポート名の両方を含む WWN プールです。ノードごとに WWxN プールで作成されるポート数を指定できます。プール サイズは、*ports-per-node*+1 の倍数である必要があります。たとえば、ノードごとに 7 つのポートを指定する場合、プール サイズは 8 の倍数である必要があります。ノードごとに 63 のポートを指定する場合、プール サイズは 64 の倍数である必要があります。

WWNN または WWPN プールを選択するたびに WWxN プールを使用できます。WWxN プールを割り当てるには、その前に WWxN プールを作成する必要があります。

- WWNN プールの場合、WWxN プールは [WWNN の割り当て（WWNN Assignment）] ドロップダウン リストにオプションとして表示されます。
- WWPN プールの場合は、[WWPN の割り当て（WWPN Assignment）] ドロップダウン リストから [派生（Derived）] を選択します。

WWN プールの作成

重要 WWN プールは、20:00:00:00:00:00:00:00 ～ 20:FF:FF:FF:FF:FF:FF:FF、または 50:00:00:00:00:00:00:00 ～ 5F:FF:FF:FF:FF:FF:FF:FF の範囲内の WWNN または WWPN だけを含めることができます。その他の WWN 範囲はすべて予約されています。SAN ファブリックで Cisco UCS WWNN と WWPN の一意性を確保するには、プール内のすべてのブロックに WWN プレフィックスとして 20:00:00:25:B5:XX:XX:XX を使用することをお勧めします。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルート組織モードを開始するには、*/* を *org-name* として入力します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /org # **create wwn-pool** *wwn-pool-name* {**node-and-port-wwn-assignment** | **node-wwn-assignment** | **port-wwn-assignment**}	指定された名前と目的でWWNプールを作成し、組織WWNプールモードを開始します。次のいずれかになります。 • **node-and-port-wwn-assignment**：ワールドワイドノード名（WWNN）およびワールドワイドポート名（WWPN）の両方を含むWWxNプールを作成します。 • **node-wwn-assignment**：WWNN のみを含む WWNN プールを作成します。 • **port-wwn-assignment**：WWPN のみを含む WWPN プールを作成します。 この名前には、1～32 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
ステップ 3	UCS-A /org/wwn-pool # **set descr** *description*	（任意） WWN プールの説明を記入します。 （注） 説明にスペース、特殊文字、または句読点が含まれている場合は、説明を引用符で括る必要があります。引用符は、**show** コマンド出力の説明フィールドには表示されません。
ステップ 4	UCS-A /org/wwn-pool # **set assignmentorder** {**default** | **sequential**}	次のいずれかになります。 • **default**：Cisco UCS Manager はプールからランダムな ID を選択します。 • **sequential**：Cisco UCS Manager はプールから最も小さい使用可能 ID を選択します。
ステップ 5	UCS-A /org/wwn-pool # **set max-ports-per-node** {**15-ports-per-node** | **3-ports-per-node** |	WWxN プールの場合、このプール内の各ノード名に割り当てることができるポートの最大数。デフォルト値は **3-ports-per-node** です。

	コマンドまたはアクション	目的
	31-ports-per-node | **63-ports-per-node** | **7-ports-per-node**}	（注） WWxNプールのプールサイズは、ノードごとのポートに 1 を加えた数の倍数である必要があります。たとえば、**7-ports-per-node** を指定する場合、プール サイズは 8 の倍数である必要があります。**63-ports-per-node** を指定する場合、プール サイズは 64 の倍数である必要があります。
ステップ 6	UCS-A /org/wwn-pool # **create block** *first-wwn last-wwn*	WWNブロック（範囲）を作成し、組織 WWN プール ブロック モードを開始します。ブロックの最初と最後の WWN を *nn*:*nn*:*nn*:*nn*:*nn*:*nn*:*nn*:*nn* 形式で指定する必要があります。WWN 間はスペースで区切ります。 （注） WWN プールには、複数の WWN ブロックを含めることができます。複数の WWN ブロックを作成するには、組織 MAC プール モードから複数の **create block** コマンドを入力します。
ステップ 7	UCS-A /org/wwn-pool/block # **exit**	組織 WWN プール ブロック モードを終了します。
ステップ 8	UCS-A /org/wwn-pool # **create initiator** *wwn wwn*	WWNN または WWPN プール用の単一イニシエータを作成し、組織 WWN プール イニシエータ モードを開始します。イニシエータは *nn*:*nn*:*nn*:*nn*:*nn*:*nn*:*nn*:*nn* の形式で指定する必要があります。 （注） WWNN または WWPN プールは複数のイニシエータを含むことができます。複数のイニシエータを作成するには、組織MACプール モードから複数の **create initiator** コマンドを入力します。
ステップ 9	UCS-A /org/wwn-pool/initiator # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、sanpool という名前の WWNN プールを作成し、プールの説明を記入し、プールに使用される WWN とイニシエータのブロックを指定し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # create wwn-pool sanpool node-wwn-assignment
UCS-A /org/wwn-pool* # set descr "This is my WWNN pool"
UCS-A /org/wwn-pool* # create block 20:00:00:25:B5:00:00:00 20:00:00:25:B5:00:00:01
UCS-A /org/wwn-pool/block* # exit
UCS-A /org/wwn-pool* # create initiator 23:00:00:05:AD:1E:02:00
UCS-A /org/wwn-pool/initiator* # commit-buffer
UCS-A /org/wwn-pool/initiator #
```

次に、sanpool という名前の WWxN プールを作成し、プールの説明を記入し、ノードあたりのポート数を 7 を指定し、プールに使用される 8 個の WWN からなるブロックを指定し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # create wwn-pool sanpool node-and-port-wwn-assignment
UCS-A /org/wwn-pool* # set descr "This is my WWxN pool"
UCS-A /org/wwn-pool* # set max-ports-per-node 7-ports-per-node
UCS-A /org/wwn-pool* # create block 20:00:00:25:B5:00:00:00 20:00:00:25:B5:00:00:08
UCS-A /org/wwn-pool/block* # commit-buffer
UCS-A /org/wwn-pool/block #
```

次の作業

- WWPN プールを vHBA テンプレートに含めます。
- WWNN プールをサービス プロファイルとテンプレートに含めます。
- WWxN プールをサービス プロファイルとテンプレートに含めます。

WWN プールの削除

プールを削除した場合、Cisco UCS Manager は、 でプールの vNIC または vHBA に割り当てられたアドレスを再割り当てしません。削除されたプールのすべての割り当て済みブロックは、次のいずれかが起きるまで、割り当てられた vNIC または vHBA に残ります。

- 関連付けられたサービス プロファイルが削除された場合。
- アドレスが割り当てられた vNIC または vHBA が削除された場合。
- vNIC または vHBA が異なるプールに割り当てられた場合。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルート組織モードを開始するには、/ を *org-name* として入力します。
ステップ 2	UCS-A /org # **delete wwn-pool** *pool-name*	指定された WWN プールを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、pool4 という名前の WWN プールを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # delete wwn-pool pool4
```

```
UCS-A /org* # commit-buffer
UCS-A /org #
```

第 25 章

ストレージ関連ポリシーの設定

この章の内容は、次のとおりです。

vHBA テンプレートの設定

vHBA テンプレート

このテンプレートは、サーバ上の vHBA と SAN の接続方法を定義するポリシーです。これは、vHBA SAN 接続テンプレートとも呼ばれます。

このポリシーを有効にするには、このポリシーをサービス プロファイルに含める必要があります。

vHBA テンプレートの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /org # **create vhba-templ** *vhba-templ-name* [**fabric** {**a** | **b**}] [**fc-if** *vsan-name*]	vHBA テンプレートを作成し、組織 vHBA テンプレート モードを開始します。
ステップ 3	UCS-A /org/vhba-templ # **set descr** *description*	（任意） vHBA テンプレートの説明を指定します。
ステップ 4	UCS-A /org/vhba-templ # **set fabric** {**a** | **b**}	（任意） vHBA に使用するファブリックを指定します。ステップ 2 で vHBA テンプレートを作成したときにファイブリックを指定しなかった場合、このコマンドでファブリックを指定するオプションを使用できます。
ステップ 5	UCS-A /org/vhba-templ # **set fc-if** *vsan-name*	（任意） vHBA テンプレートに使用する（VSAN という名前の）ファイバ チャネル インターフェイスを指定します。ステップ 2 で vHBA テンプレートを作成したときにファイバ チャネル インターフェイスを指定しなかった場合、このコマンドでファイバ チャネル インターフェイスを指定するオプションを使用できます。
ステップ 6	UCS-A /org/vhba-templ # **set max-field-size** *size-num*	vHBA がサポートするファイバ チャネル フレーム ペイロードの最大サイズ（バイト数）を指定します。
ステップ 7	UCS-A /org/vhba-templ # **set pin-group** *group-name*	vHBA テンプレートに対し使用するピン グループを指定します。
ステップ 8	UCS-A /org/vhba-templ # **set qos-policy** *mac-pool-name*	vHBA テンプレートに対し使用する QoS ポリシーを指定します。
ステップ 9	UCS-A /org/vhba-templ # **set stats-policy** *policy-name*	vHBA テンプレートに対し使用するサーバおよびサーバ コンポーネント統計情報しきい値ポリシーを指定します。
ステップ 10	UCS-A /org/vhba-templ # **set type** {**initial-template** | **updating-template**}	vHBA テンプレートのアップデート タイプを指定します。テンプレートのアップデート時にこのテンプレートから作成された vHBA インスタンスが自動的にアップデートされないようにする場合は、**initial-template** キーワードを使用します。それ以外の場合は、vHBA テンプレートのアップデート時にすべての vHBA インスタンスがアップデートされる

	コマンドまたはアクション	目的
		ようにするために **updating-template** キーワードを使用します。
ステップ 11	UCS-A /org/vhba-templ # **set wwpn-pool** *pool-name*	vHBA テンプレートに対し使用する WWPN プールを指定します。
ステップ 12	UCS-A /org/vhba-templ # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、vHBA テンプレートを設定し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org* # create vhba template VhbaTempFoo
UCS-A /org/vhba-templ* # set descr "This is a vHBA template example."
UCS-A /org/vhba-templ* # set fabric a
UCS-A /org/vhba-templ* # set fc-if accounting
UCS-A /org/vhba-templ* # set max-field-size 2112
UCS-A /org/vhba-templ* # set pin-group FcPinGroup12
UCS-A /org/vhba-templ* # set qos-policy policy34foo
UCS-A /org/vhba-templ* # set stats-policy ServStatsPolicy
UCS-A /org/vhba-templ* # set type updating-template
UCS-A /org/vhba-templ* # set wwpn-pool SanPool7
UCS-A /org/vhba-templ* # commit-buffer
UCS-A /org/vhba-templ #
```

vHBA テンプレートの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **delete vhba-templ** *vhba-templ-name*	指定した vHBA テンプレートを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、VhbaTempFoo という名前の vHBA テンプレートを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # delete vhba template VhbaTempFoo
UCS-A /org* # commit-buffer
UCS-A /org #
```

ファイバ チャネル アダプタ ポリシーの設定

イーサネットおよびファイバ チャネル アダプタ ポリシー

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

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

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

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

オペレーティング システム固有のアダプタ ポリシー

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

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

ただし、（デフォルトの Windows のアダプタ ポリシーを使用する代わりに）Windows OS のイーサネット アダプタ ポリシーを作成する場合は、次の式を使用して Windows で動作する値を計算します。

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

たとえば、送信キューが 1 で受信キューが 8 の場合、

完了キュー = 1 + 8 = 9
割り込み回数 = (9 + 2) 以上の 2 のべき乗の最小値 = 16

ファイバ チャネル アダプタ ポリシーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **create fc-policy** *policy-name*	指定されたファイバ チャネル アダプタ ポリシーを作成し、組織ファイバ チャネル ポリシー モードを開始します。
ステップ 3	UCS-A /org/fc-policy # **set descr** *description*	（任意） ポリシーの説明を記します。 （注） 説明にスペース、特殊文字、または句読点が含まれている場合は、説明を引用符で括る必要があります。引用符は、**show** コマンド出力の説明フィールドには表示されません。
ステップ 4	UCS-A /org/fc-policy # **set error-recovery** {**fcp-error-recovery** {**disabled** | **enabled**} | **link-down-timeout** *timeout-msec* |	（任意） ファイバ チャネル エラー回復を設定します。

	コマンドまたはアクション	目的
	port-down-io-retry-count *retry-count* | **port-down-timeout** *timeout-msec*}	
ステップ 5	UCS-A /org/fc-policy # **set interrupt mode** {**intx** | **msi** | **msi-x**}}	（任意） ドライバ割り込みモードを設定します。
ステップ 6	UCS-A /org/fc-policy # **set port** {**io-throttle-count** *throttle-count* | **max-luns** *max-num*}	（任意） ファイバ チャネル ポートを設定します。
ステップ 7	UCS-A /org/fc-policy # **set port-f-logi** {**retries** *retry-count* | **timeout** *timeout-msec*}	（任意） ファイバ チャネル ポートのファブリック ログイン（FLOGI）を設定します。
ステップ 8	UCS-A /org/fc-policy # **set port-p-logi** {**retries** *retry-count* | **timeout** *timeout-msec*}	（任意） ファイバ チャネルのポートツーポート ログイン（PLOGI）を設定します。
ステップ 9	UCS-A /org/fc-policy # **set recv-queue** {**count** *count* | **ring-size** *size-num*}	（任意） ファイバチャネルの受信キューを設定します。
ステップ 10	UCS-A /org/fc-policy # **set scsi-io** {**count** *count* | **ring-size** *size-num*}	（任意） ファイバ チャネルの SCSI I/O を設定します。
ステップ 11	UCS-A /org/fc-policy # **set trans-queue ring-size** *size-num*}	（任意） ファイバチャネルの送信キューを設定します。
ステップ 12	UCS-A /org/fc-policy # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、ファイバ チャネル アダプタ ポリシーを設定し、トランザクションをコミットます。

```
UCS-A# scope org /
UCS-A /org* # create fc-policy FcPolicy42
UCS-A /org/fc-policy* # set descr "This is a Fibre Channel adapter policy example."
UCS-A /org/fc-policy* # set error-recovery error-detect-timeout 2500
UCS-A /org/fc-policy* # set port max-luns 4
UCS-A /org/fc-policy* # set port-f-logi retries 250
UCS-A /org/fc-policy* # set port-p-logi timeout 5000
UCS-A /org/fc-policy* # set recv-queue count 1
UCS-A /org/fc-policy* # set scsi-io ring-size 256
UCS-A /org/fc-policy* # set trans-queue ring-size 256
UCS-A /org/fc-policy* # commit-buffer
UCS-A /org/fc-policy #
```

ファイバ チャネル アダプタ ポリシーの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **delete fc-policy** *policy-name*	指定されたファイバ チャネル アダプタ ポリシーを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、FcPolicy42 という名前のファイバ チャネル アダプタ ポリシーを削除し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # delete fc-policy FcPolicy42
UCS-A /org* # commit-buffer
UCS-A /org #
```

デフォルトの vHBA 動作ポリシーの設定

デフォルトの vHBA 動作ポリシー

デフォルトの vHBA 動作ポリシーにより、サービス プロファイルに対する vHBA の作成方法を設定できます。vHBA を手動で作成するか、自動的に作成されるようにするかを選択できます。

デフォルトの vHBA 動作ポリシーを設定して、vHBA の作成方法を定義することができます。次のいずれかになります。

- [なし（None）]：Cisco UCS Manager はサービス プロファイルにデフォルトの vHBA を作成しません。すべての vHBA を明示的に作成する必要があります。
- [HW 継承（HW Inherit）]：サービス プロファイルが vHBA を必要とし、何も明示的に定義されていない場合、Cisco UCS Manager はサービス プロファイルに関連付けられたサーバにインストールされたアダプタに基づいて必要な vHBA を作成します。

（注） vHBA のデフォルト動作ポリシーを指定しない場合、[none] がデフォルトで使用されます。

デフォルトの vHBA 動作ポリシーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org /**	ルート組織モードを開始します。
ステップ 2	UCS-A/org # **scope vhba-beh-policy**	デフォルトの vHBA 動作ポリシー モードを開始します。
ステップ 3	UCS-A/org/vhba-beh-policy # **set action** {**hw-inherit** [**template_name** *name*] | **none**}	デフォルトの vHBA 動作ポリシーを指定します。次のいずれかになります。 • **hw-inherit**：サービス プロファイルが vHBA を必要とし、何も明示的に定義されていない場合、Cisco UCS Manager はサービス プロファイルに関連付けられたサーバにインストールされたアダプタに基づいて必要な vHBA を作成します。 **hw-inherit** を指定した場合は、vHBA テンプレートを指定して vHBA を作成することもできます。 • **none**：Cisco UCS Manager はサービス プロファイルにデフォルトの vHBA を作成しません。すべての vHBA を明示的に作成する必要があります。
ステップ 4	UCS-A/org/vhba-beh-policy # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、デフォルトの vHBA 動作ポリシーを **hw-inherit** に設定する方法を示します。

```
UCS-A # scope org /
UCS-A/org # scope vhba-beh-policy
UCS-A/org/vhba-beh-policy # set action hw-inherit
UCS-A/org/vhba-beh-policy* # commit-buffer
UCS-A/org/vhba-beh-policy #
```

SAN 接続ポリシーの設定

LAN および SAN 接続ポリシーについて

接続ポリシーは、ネットワーク上のサーバと LAN または SAN 間の接続およびネットワーク通信リソースを決定します。これらのポリシーは、プールを使用してサーバにMACアドレス、WWN、

および WWPN を割り当て、サーバがネットワークとの通信に使用する vNIC および vHBA を識別します。

（注） これらの接続ポリシーは、サービス プロファイルおよびサービス プロファイル テンプレートに含まれ、複数のサーバを設定するために使用できるので、静的 ID を接続ポリシーで使用することはお勧めしません。

LAN および SAN の接続ポリシーに必要な権限

接続ポリシーにより、ネットワークまたはストレージ権限のないユーザがネットワークおよびストレージ接続をしているサービス プロファイルおよびサービス プロファイル テンプレートを作成および変更することが可能になります。ただし、ユーザは接続ポリシーを作成するための適切なネットワークおよびストレージの権限が必要です。

接続ポリシーの作成に必要な権限

接続ポリシーは、他のネットワークおよびストレージ構成と同じ権限を必要とします。たとえば、接続ポリシーを作成するには、次の権限の少なくとも 1 つを有している必要があります。

- admin：LAN および SAN 接続ポリシーを作成できます
- ls-server：LAN および SAN 接続ポリシーを作成できます
- ls-network：LAN 接続ポリシーを作成できます
- ls-storage：SAN 接続ポリシーを作成できます

接続ポリシーをサービス プロファイルに追加するために必要な権限

接続ポリシーの作成後、ls-compute 権限を持つユーザは、そのポリシーをサービス プロファイルまたはサービス プロファイル テンプレートに組み込むことができます。ただし、ls-compute 権限しかないユーザは接続ポリシーを作成できません。

サービス プロファイルと接続ポリシー間の相互作用

次のいずれかの方法により、サービス プロファイルに LAN および SAN の接続を設定できます。

- サービス プロファイルで参照される LAN および SAN 接続ポリシー
- サービス プロファイルで作成されるローカル vNIC および vHBA
- ローカル vNIC および SAN 接続ポリシー
- ローカル vHBA および LAN 接続ポリシー

Cisco UCS では、サービス プロファイルのローカル vNIC および vHBA 設定と接続ポリシー間の相互排他性が維持されます。接続ポリシーとローカルに作成した vNIC または vHBA を組み合わせて使用することはできません。サービス プロファイルに LAN 接続ポリシーを含めると、既存の vNIC 設定がすべて消去されます。SAN 接続ポリシーを含めた場合は、そのサービス プロファイル内の既存の vHBA 設定がすべて消去されます。

SAN 接続ポリシーの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルート組織モードを開始するには、*/* を *org-name* として入力します。
ステップ 2	UCS-A /org # **create san-connectivity-policy** *policy-name*	指定されたSAN接続ポリシーを作成を作成し、組織ネットワーク制御ポリシー モードを開始します。 この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
ステップ 3	UCS-A /org/lan-connectivity-policy # **set descr** *policy-name*	（任意） ポリシーに説明を追加します。どこでどのようにポリシーが使用されるかについての情報を含めることを推奨します。 256 文字以内で入力します。次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
ステップ 4	UCS-A /org/service-profile # **set identity** {**dynamic-uuid** {*uuid* | **derived**} | **dynamic-wwnn** {*wwnn* | **derived**} | **uuid-pool** *pool-name* | **wwnn-pool** *pool-name*}	サーバが UUID または WWNN を取得する方法を指定します。次のいずれかを実行できます。 • 一意の UUID を *nnnnnnnn-nnnn-nnnn-nnnnnnnnnnnn* 形式で作成する • 製造時にハードウェアに焼き付けられたUUIDを取得する • UUID プールを使用する

	コマンドまたはアクション	目的
		• 一意の WWNN を *hh* : *hh* : *hh* : *hh* : *hh* : *hh* : *hh* : *hh* 形式で作成する • 製造時にハードウェアに焼き付けられた WWNN を取得する • WWNN プールを使用する
ステップ 5	UCS-A /org/lan-connectivity-policy # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、SanConnect242 という名前の SAN 接続ポリシーを作成し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org* # create san-connectivity-policy SanConnect242
UCS-A /org/san-connectivity-policy* # set descr "SAN connectivity policy"
UCS-A /org/san-connectivity-policy* # set identity wwnn-pool SanPool7
UCS-A /org/san-connectivity-policy* # commit-buffer
UCS-A /org/san-connectivity-policy #
```

次の作業

この SAN 接続ポリシーに 1 つ以上の vHBA および（または）イニシエータ グループを追加します。

SAN 接続ポリシー用の vHBA の作成

SAN 接続ポリシーの作成, （392 ページ） から続行した場合、ステップ 3 でこの手順を開始します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルート組織モードを開始するには、*/* を *org-name* として入力します。
ステップ 2	UCS-A /org # **scope san-connectivity-policy** *policy-name*	指定した SAN 接続ポリシーの SAN 接続ポリシーモードを開始します。
ステップ 3	UCS-A /org/san-connectivity-policy # **create vhba** *vhba-name* [**fabric** {**a** | **b**}] [**fc-if** *fc-if-name*]	指定した SAN 接続ポリシー用の vHBA を作成し、vHBA モードを開始します。

	コマンドまたはアクション	目的
		この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
ステップ 4	UCS-A /org/san-connectivity-policy/vhba # **set adapter-policy** *policy-name*	vHBA に対し使用するアダプタ ポリシーを指定します。
ステップ 5	UCS-A /org/san-connectivity-policy/vhba # **set identity** {**dynamic-wwpn** {*wwpn* | **derived**} | **wwpn-pool** *wwn-pool-name*}	vHBA の WWPN を指定します。 次のいずれかのオプションを使用してストレージ ID を設定できます。 • 一意の WWPN を *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh* 形式で作成します。 WWPN は、20:00:00:00:00:00:00:00 ～ 20:FF:FF:FF:FF:FF:FF:FF または 50:00:00:00:00:00:00:00 ～ 5F:FF:FF:FF:FF:FF:FF:FF の範囲内で指定できます。 WWPN に Cisco MDS ファイバ チャネル スイッチと互換性を持たせる場合は、WWPN テンプレート 20:00:00:25:B5:XX:XX:XX を使用します。 • 製造時にハードウェアに焼き付けられた WWPN から WWPN 取得する。 • WWN プールから WWPN を割り当てる。
ステップ 6	UCS-A /org/san-connectivity-policy/vhba # **set max-field-size** *size-num*	vHBA がサポートするファイバ チャネル フレーム ペイロードの最大サイズ（バイト数）を指定します。 256 ～ 2112 の整数を入力します。デフォルトは 2048 です。
ステップ 7	UCS-A /org/san-connectivity-policy/vhba # **set order** {*order-num* | **unspecified**}	vHBA の PCI スキャン順序を指定します。

	コマンドまたはアクション	目的
ステップ 8	UCS-A /org/san-connectivity-policy/vhba # **set pers-bind** {**disabled** | **enabled**}	ファイバ チャネル ターゲットに対する永続的なバインディングをディセーブルまたはイネーブルにします。
ステップ 9	UCS-A /org/san-connectivity-policy/vhba # **set pin-group** *group-name*	vHBA に使用する SAN ピン グループを指定します。
ステップ 10	UCS-A /org/san-connectivity-policy/vhba # **set qos-policy** *policy-name*	vHBA に対し使用する QoS ポリシーを指定します。
ステップ 11	UCS-A /org/san-connectivity-policy/vhba # **set stats-policy** *policy-name*	vHBAに使用する統計情報しきい値ポリシーを指定します。
ステップ 12	UCS-A /org/san-connectivity-policy/vhba # **set template-name** *policy-name*	vHBA に使用する vHBA テンプレートを指定します。vHBA に vHBA テンプレートを使用する場合は、ステップ 4、7、および 8 などの vHBA テンプレートに含まれていないすべての設定を完了する必要があります。
ステップ 13	UCS-A /org/san-connectivity-policy/vhba # **set vcon** {**1** | **2** | **3** | **4** | **any**}	vHBA を 1 つまたはすべての仮想ネットワーク インターフェイス接続に割り当てます。
ステップ 14	UCS-A /org/san-connectivity-policy/vhba # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、SanConnect242 という名前の SAN 接続ポリシー用の vHBA を設定し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org* # scope san-connectivity-policy SanConnect242
UCS-A /org/san-connectivity-policy* # create vhba vhba3 fabric a
UCS-A /org/san-connectivity-policy/vhba* # set adapter-policy AdaptPol2
UCS-A /org/san-connectivity-policy/vhba* # set identity wwpn-pool SanPool7
UCS-A /org/san-connectivity-policy/vhba* # set max-field-size 2112
UCS-A /org/san-connectivity-policy/vhba* # set order 0
UCS-A /org/san-connectivity-policy/vhba* # set pers-bind enabled
UCS-A /org/san-connectivity-policy/vhba* # set pin-group FcPinGroup12
UCS-A /org/san-connectivity-policy/vhba* # set qos-policy QosPol5
UCS-A /org/san-connectivity-policy/vhba* # set stats-policy StatsPol2
UCS-A /org/san-connectivity-policy/vhba* # set template-name SanConnPol3
UCS-A /org/san-connectivity-policy/vhba* # set vcon any
UCS-A /org/san-connectivity-policy/vhba* # commit-buffer
UCS-A /org/san-connectivity-policy/vhba #
```

次の作業

必要に応じて、SAN接続ポリシーに別のvHBAまたはイニシエータ グループを追加します。そうでない場合は、サービス プロファイルまたはサービス プロファイル テンプレートにポリシーをインクルードします。

SAN 接続ポリシーからの vHBA の削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルート組織モードを開始するには、/ を *org-name* として入力します。
ステップ 2	UCS-A /org # **scope san-connectivity-policy** *policy-name*	指定した SAN 接続ポリシーの SAN 接続ポリシー モードを開始します。
ステップ 3	UCS-A /org/san-connectivity-policy # **delete vHBA** *vhba-name*	SAN 接続ポリシーから指定された vHBA を削除します。
ステップ 4	UCS-A /org/san-connectivity-policy # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、vHBA3 という名前の vHBA を SanConnect242 という名前の SAN 接続ポリシーから削除し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org # scope san-connectivity-policy SanConnect242
UCS-A /org/san-connectivity-policy # delete vHBA vHBA3
UCS-A /org/san-connectivity-policy* # commit-buffer
UCS-A /org/san-connectivity-policy #
```

SAN 接続ポリシー用のイニシエータ グループの作成

SAN 接続ポリシーの作成, （392 ページ） から続行した場合、ステップ 3 でこの手順を開始します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルー

	コマンドまたはアクション	目的
		ト組織モードを開始するには、/ を *org-name* として入力します。
ステップ 2	UCS-A /org # **scope san-connectivity-policy** *policy-name*	指定した SAN 接続ポリシーの SAN 接続ポリシー モードを開始します。
ステップ 3	UCS-A /org/san-connectivity-policy # **create initiator-group** *group-name***fc**	ファイバ チャネル ゾーン分割の指定イニシエータ グループを作成し、イニシエータ グループ モードを開始します。 この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
ステップ 4	UCS-A /org/san-connectivity-policy/initiator-group # **create initiator** *vhba-name*	イニシエータ グループの指定 vHBA イニシエータを作成します。

	コマンドまたはアクション	目的
		必要に応じて、この手順を繰り返しグループに2番目の vHBA を追加します。
ステップ 5	UCS-A /org/san-connectivity-policy/initiator-group # **set storage-connection-policy** *policy-name*	SAN 接続ポリシーに指定したストレージ接続ポリシーを関連付けます。

	コマンドまたはアクション	目的
		（注） この手順は、SAN 接続ポリシーに関連付ける既存のストレージ接続ポリシーを関連付けると仮定しています。行うには、ステップ 10 に進みます。代わりに、このポリシーのローカル ストレージ定義を作成する場合は、ステップ 6 に進みます。
ステップ 6	UCS-A /org/san-connectivity-policy/initiator-group/storage-connection-def # **create storage-target** *wwpn*	指定された WWPN を持つストレージ ターゲット エンドポ

	コマンドまたはアクション	目的
		イントを作成し、ストレージ ターゲット モードを開始します。
ステップ 7	UCS-A /org/san-connectivity-policy/initiator-group/storage-connection-def/storage-target # **set target-path** {**a** | **b**}	ターゲット エンドポイントとの通信に使用するファブリック インターコネクトを指定します。
ステップ 8	UCS-A /org/san-connectivity-policy/initiator-group/storage-connection-def/storage-target # **set target-vsan** *vsan*	ターゲット エンドポイントとの通信に使用するVSANを指定します。
ステップ 9	UCS-A /org/san-connectivity-policy/initiator-group # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、SanConnect242 という名前の SAN 接続ポリシーに対し 2 つのイニシエータを持つ initGroupZone1 という名前のイニシエータ グループを設定し、scPolicyZone1 という名前のローカル ストレージ接続ポリシー定義を設定し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org* # scope san-connectivity-policy SanConnect242
UCS-A /org/san-connectivity-policy # create initiator-group initGroupZone1 fc
UCS-A /org/san-connectivity-policy/initiator-group* # set zoning-type sist
UCS-A /org/san-connectivity-policy/initiator-group* # create initiator vhba1
UCS-A /org/san-connectivity-policy/initiator-group* # create initiator vhba2
UCS-A /org/san-connectivity-policy/initiator-group* # create storage-connection-def
scPolicyZone1
UCS-A /org/san-connectivity-policy/initiator-group/storage-connection-def* # create
storage-target
20:10:20:30:40:50:60:70
UCS-A /org/san-connectivity-policy/initiator-group/storage-connection-def/storage-target*
# set
target-path a
UCS-A /org/san-connectivity-policy/initiator-group/storage-connection-def/storage-target*
# set
target-vsan default
UCS-A /org/san-connectivity-policy/initiator-group* # commit-buffer
UCS-A /org/san-connectivity-policy/initiator-group #
```

次の作業

必要に応じて、SAN接続ポリシーに他のイニシエータ グループまたはvHBAを追加します。そうでない場合は、サービス プロファイルまたはサービス プロファイル テンプレートにポリシーをインクルードします。

SAN 接続ポリシーからのイニシエータ グループの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルート組織モードを開始するには、**/** を *org-name* として入力します。
ステップ 2	UCS-A /org # **scope san-connectivity-policy** *policy-name*	指定した SAN 接続ポリシーの SAN 接続ポリシー モードを開始します。
ステップ 3	UCS-A /org/san-connectivity-policy # **delete initiator-group** *group-name*	SAN接続ポリシーから指定されたイニシエータ グループを削除します。
ステップ 4	UCS-A /org/san-connectivity-policy # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、initGroup3 という名前のイニシエータ グループを SanConnect242 という名前の SAN 接続ポリシーから削除し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org # scope san-connectivity-policy SanConnect242
UCS-A /org/san-connectivity-policy # delete initiator-group initGroup3
UCS-A /org/san-connectivity-policy* # commit-buffer
UCS-A /org/san-connectivity-policy #
```

SAN 接続ポリシーの削除

サービスプロファイルに含まれるSAN接続ポリシーを削除する場合、すべてのvHBAもそのサービス プロファイルから削除し、そのサービス プロファイルに関連付けられているサーバの SAN データ トラフィックを中断します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルート組織モードを開始するには、/ を *org-name* として入力します。
ステップ 2	UCS-A /org # **delete san-connectivity-policy** *policy-name*	指定されたSAN接続ポリシーを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、SanConnect52という名前のSAN接続ポリシーをルート組織から削除し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org # delete san-connectivity-policy SanConnect52
UCS-A /org* # commit-buffer
UCS-A /org #
```

第 26 章

ファイバ チャネル ゾーン分割の設定

この章の内容は、次のとおりです。

ファイバ チャネル ゾーン分割に関する情報

ファイバ チャネル ゾーン分割によって、ファイバ チャネル ファブリックを 1 つ以上のゾーンに区切ることができます。各ゾーンでは、VSAN で相互通信できるファイバ チャネル イニシエータとファイバチャネル ターゲットのセットが定義されます。ゾーン分割により、ホストとストレージ デバイスまたはユーザ グループ間のアクセス制御を設定することができます。

ゾーン分割がもたらすアクセス制御とデータ トラフィック制御によって以下が可能になります。

- SAN ネットワーク セキュリティの強化
- データの損失や破損の防止
- パフォーマンス問題の軽減

ゾーンに関する情報

ゾーンは複数のゾーン メンバから構成されており、次のような特性を備えています。

- ゾーンのメンバ同士はアクセスできますが、異なるゾーンのメンバ同士はアクセスできません。
- ゾーンのサイズを変更できます。
- デバイスは複数のゾーンに所属できます。
- 1 つの物理ファブリックに最大 8,000 ゾーンを収容できます。

ゾーン セットに関する情報

各ゾーン セットは、1 つまたは複数のゾーンから構成されます。ゾーン セットを使用して、ファイバ チャネル ファブリック内でアクセス制御を実行することができます。また、ゾーン セットには次のような利点があります。

- アクティブにできるのは、常に 1 つのゾーン セットだけです。
- ゾーン セット内のすべてのゾーンは、ファブリック内のスイッチ全体で単一のエンティティとしてアクティブまたは非アクティブにできます。
- 1 つのゾーンを複数のゾーン セットのメンバにできます。
- ゾーン内の各スイッチは最大 500 のゾーン セットを持つことができます。

Cisco UCS Manager でのファイバ チャネル ゾーン分割のサポート

Cisco UCS Manager は、スイッチベースのファイバ チャネル ゾーン分割と Cisco UCS Manager ベースのファイバ チャネル ゾーン分割をサポートしています。同じ Cisco UCS ドメイン 内ではゾーン分割タイプを組み合わせて設定できません。次のゾーン分割タイプのいずれかを使って Cisco UCS ドメイン を設定できます。

- Cisco UCS Manager ベースのファイバ チャネル ゾーン分割：この設定は、直接接続ストレージとローカル ゾーン分割の組み合わせです。ファイバ チャネルまたは FCoE のストレージはファブリック インターコネクトに直接接続され、ゾーン分割は、Cisco UCS ローカル ゾーン分割を使用して Cisco UCS Manager で実行されます。既存のファイバ チャネルまたは FCoE のアップリンク接続を無効にする必要があります。現時点では、Cisco UCS は、UCS ローカル ゾーン分割機能の利用において、アクティブなファイバ チャネルまたは FCoE アップリンク接続の共存をサポートしていません。
- スイッチベースのファイバ チャネル ゾーン分割：この設定は、直接接続ストレージとアップリンク ゾーン分割の組み合わせです。ファイバ チャネルまたは FCoE のストレージはファ

ブリック インターコネクトに直接接続され、ゾーン分割は、MDS または Nexus 5000 スイッチを介して Cisco UCS ドメイン の外部から実行されます。この設定は、Cisco UCS ドメインでのローカル ゾーン分割をサポートしません。

（注） ゾーン分割は、VSAN 単位で設定します。ファブリック レベルでゾーン分割を有効にすることはできません。

Cisco UCS Manager ベースのファイバ チャネル ゾーン分割

Cisco UCS Manager ベースのゾーン分割により、Cisco UCS Manager は、このタイプのゾーン分割で設定されたすべての VSAN のゾーンの作成やアクティブ化など、Cisco UCS ドメイン のファイバチャネル ゾーン分割の設定を制御します。このタイプのゾーン分割は、ローカル ゾーン分割、または直接接続ストレージとローカル ゾーン分割の組み合わせとも呼ばれます。

（注） VSAN も上流に位置するスイッチの VSAN と通信するよう設定されており、ファイバ チャネル ポートまたは FCoE アップリンク ポートを含んでいる場合は、Cisco UCS Manager ベースのゾーン分割を実行できません。

サポートされているファイバ チャネル ゾーン分割モード

Cisco UCS Manager ベースのゾーン分割は、次のタイプのゾーン分割をサポートしています。

- 単一のイニシエータと単一のターゲット：Cisco UCS Manager は、vHBA とストレージ ポートの組み合わせごとに 1 つのゾーンを自動作成します。各ゾーンには 2 つのメンバがあります。ゾーンの数がサポートされる最大数を超えると予想されない限り、このタイプのゾーン分割を設定することをお勧めします。
- 単一のイニシエータと複数のターゲット：Cisco UCS Manager は、vHBA ごとに 1 つゾーンを自動作成します。ゾーンの数がサポートされる最大数に達するか、それを超えると予想される場合は、このタイプのゾーン分割を設定することをお勧めします。

vHBA イニシエータ グループ

vHBA イニシエータ グループによって、サービス プロファイル内のすべての vHBA のファイバ チャネル ゾーン分割設定を決定します。Cisco UCS Manager にはデフォルトの vHBA イニシエータ グループが含まれていません。ゾーン内のサーバに割り当てるサービス プロファイルで vHBA イニシエータ グループを作成する必要があります。

vHBA イニシエータ グループでの設定により、以下が決定されます。

- イニシエータ グループに含める vHBA（vHBA イニシエータとも呼ばれる）。

- ファイバ チャネル ストレージ接続ポリシー。これには、関連する VSAN およびストレージ アレイ上のファイバ チャネル ターゲット ポートが含まれます。
- グループに含める vHBA に対して設定するファイバ チャネル ゾーン分割のタイプ。

ファイバ チャネル ストレージ接続ポリシー

ファイバ チャネル ストレージ接続ポリシーには、Cisco UCS Manager ベースのファイバ チャネル ゾーン分割の設定に使用される、ストレージ アレイ上の一連のターゲット ストレージ ポートが含まれています。このポリシーは、組織またはイニシエータ グループの下に作成できます。

これらのゾーン内のストレージアレイは、ファブリック インターコネクトに直接接続される必要があります。ファイバチャネルストレージ接続ポリシーに組み込むこれらのアレイのターゲット ストレージ ポートには、ファイバ チャネル ストレージ ポートまたは FCoE ストレージ ポートを使用できます。ポートの WWN を使用して、ポートをポリシーに追加し、ファイバ チャネル ゾーンのポートを識別します。

（注） Cisco UCS Manager は、デフォルトのファイバ チャネル ストレージを作成しません。

ファイバ チャネル アクティブ ゾーン セット設定

ファイバ チャネル ゾーン分割が有効になっている各 VSAN では、Cisco UCS Manager は自動的に 1 つのゾーン セットと複数のゾーンを設定します。ゾーン メンバーシップは、相互通信が許可されたイニシエータとターゲットのセットを指定します。Cisco UCS Manager は自動的にそのゾーン セットをアクティブにします。

Cisco UCS Manager は、ユーザ設定の vHBA イニシエータ グループとそれらの関連したファイバ チャネル ストレージ接続ポリシーを処理し、ファイバ チャネル イニシエータとターゲット間の必要な接続を決定します。Cisco UCS Manager は、次の情報を使用し、イニシエータとターゲット間のペアワイズ ゾーン メンバーシップを構築します。

- vHBA イニシエータのポート WWN は、vHBA イニシエータ グループから作成されます。
- ストレージ アレイのポート WWN は、ストレージ接続ポリシーから作成されます。

スイッチベースのファイバ チャネル ゾーン分割

スイッチベースのゾーン分割の場合、Cisco UCS ドメイン はアップストリーム スイッチからゾーン分割設定を継承します。Cisco UCS Manager では、ゾーン分割の設定に関する情報を設定したり表示したりできません。VSAN に対してスイッチベースのゾーン分割を適用するには、Cisco UCS Manager でその VSAN のゾーン分割を無効にする必要があります。

Cisco UCS Manager ベースのファイバ チャネル ゾーン分割に関するガイドラインおよび推奨事項

ファイバチャネルゾーン分割の設定を計画する際は、次のガイドラインおよび推奨事項を考慮してください。

ファイバ チャネル スイッチング モードは Cisco UCS Manager 設定用のスイッチ モードでなければならない

Cisco UCS Manager にファイバ チャネル ゾーン分割を処理させる場合は、ファブリック インターコネクトがファイバチャネルスイッチモードである必要があります。エンドホストモードでは、ファイバ チャネルのゾーン分割を設定できません。

ハイ アベイラビリティのために対称構成を推奨

Cisco UCS ドメイン が 2 個のファブリック インターコネクトでハイ アベイラビリティ用に設定されている場合、ファブリック インターコネクトが両方の VSAN セットに設定されることを推奨します。

Cisco UCS Manager ファイバ チャネル ゾーン分割の設定

（注） この手順は、Cisco UCS Manager によって制御されるファイバ チャネル ゾーン分割に対し Cisco UCS ドメイン を設定するのに必要な手順の概要を示します。次のすべてのステップを完了する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	まだ完了してない場合は、Cisco UCS ドメイン内のファブリック インターコネクトの接続を、外付けファイバ チャネル スイッチ（MDS など）から切り離してください。	
ステップ 2	Cisco UCS ドメイン にまだ外部ファイバ チャネル スイッチによって管理されたゾーンが含まれる場合は、これらのゾーンを削除するために、影響を受けたすべての VSAN で **clear-unmanaged-fc-zone-all** コマンドを実行します。	この機能は現在、Cisco UCS Manager GUI では使用できません。このステップは、Cisco UCS Manager CLI で実行する必要があります。

	コマンドまたはアクション	目的
ステップ 3	両方のファブリック インターコネクトに、ファイバチャネルスイッチング モードを設定します。	エンドホスト モードでは、ファイバ チャネルのゾーン分割を設定できません。 ファイバ チャネル スイッチング モードの設定, （62 ページ）を参照してください。
ステップ 4	ファイバ チャネル ゾーンのトラフィック転送に必要なファイバチャネルとFCoE ストレージ ポートを設定します。	ポートおよびポート チャネルの設定, （65 ページ）を参照してください。
ステップ 5	1 つ以上の VSAN を作成し、ファイバチャネル ゾーンのトラフィック転送に必要なすべてのVSANで、ファイバチャネルのゾーン分割を有効にします。	クラスタ設定では、ファイバチャネル ゾーンに含める VSAN を ファイバ チャネル ストレージ モードで作成し、両方のファブリック インターコネクトにアクセスできるようにすることを推奨します。 ネームドVSANの設定, （359ページ）を参照してください。
ステップ 6	1 つ以上のファイバ チャネル ストレージ接続ポリシーを作成します。	必要に応じて、この手順を実行してサービス プロファイルにファイバ チャネル ゾーン分割を設定することができます。 ファイバチャネル ストレージ接続ポリシーの作成, （411 ページ）を参照してください。
ステップ 7	ファイバ チャネル ゾーン経由で通信する必要があるサーバに対してサービス プロファイルまたはサービス プロファイル テンプレートにゾーン分割を設定します。	この設定を完了するには、次の手順を完了します。 • VHBA に割り当てられた VSAN（複数の場合あり）のゾーン分割を有効にします。 • 1 つ以上の vHBA イニシエータ グループを設定します。 サービス プロファイル, （655ページ）を参照してください。

両方のファブリックインターコネクトにアクセス可能な VSAN からの管理対象外ゾーンの削除

外部ファイバ チャネル スイッチを切断した後、そのスイッチによって管理されていたファイバ チャネル ゾーンが Cisco UCS ドメイン からクリアされていない場合があります。この手順では、Cisco UCS ドメイン の各 VSAN からこれらのゾーンを削除して、ファイバ チャネル ゾーン分割を Cisco UCS に設定できます。

はじめる前に

まだ完了してない場合は、Cisco UCS ドメイン内のファブリック インターコネクトの接続を、外付けファイバ チャネル スイッチ（MDS など）から切り離してください。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink #**scope fabric** {**a** | **b**}	指定したファブリック インターコネクトのファイバ チャネル アップリンク モードを開始します。
ステップ 3	UCS-A /fc-uplink/fabric # **scope vsan** *vsan-name*	指定されたネームド VSAN の VSAN モードが開始されます。
ステップ 4	UCS-A /fc-uplink/fabric/vsan # **clear-unmanaged-fc-zones-all**	指定されたネームド VSAN からすべての管理対象外ファイバ チャネル ゾーンをクリアします。 必要に応じて、ステップ 2 から 4 を繰り返し、バッファをコミットする前に、指定したファブリック インターコネクトにアクセス可能なすべての VSAN から管理対象外のゾーンを削除することができます。
ステップ 5	UCS-A /fc-uplink/fabric/vsan # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、管理対象外のゾーンをファブリック インターコネクト A にアクセス可能なネームド VSAN から削除し、トランザクションをコミットする方法を示します。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # scope vsan finance
UCS-A /fc-uplink/fabric/vsan # clear-unmanaged-fc-zones-all
UCS-A /fc-uplink/fabric/vsan* # commit-buffer
UCS-A /fc-uplink #
```

1 つのファブリック インターコネクトにアクセス可能な VSAN からの管理対象外ゾーンの削除

外部ファイバ チャネル スイッチを切断した後、そのスイッチによって管理されていたファイバ チャネル ゾーンが Cisco UCS ドメイン からクリアされていない場合があります。この手順では、Cisco UCS ドメイン の各 VSAN からこれらのゾーンを削除して、ファイバ チャネル ゾーン分割を Cisco UCS に設定できます。

はじめる前に

まだ完了してない場合は、Cisco UCS ドメイン内のファブリック インターコネクトの接続を、外付けファイバ チャネル スイッチ（MDS など）から切り離してください。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバチャネルアップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope vsan** *vsan-name*	指定されたネームド VSAN の VSAN モードが開始されます。
ステップ 3	UCS-A /fc-uplink/vsan # **clear-unmanaged-fc-zones-all**	指定されたネームド VSAN からすべての管理対象外ファイバ チャネル ゾーンをクリアします。 必要に応じて、ステップ 2 と 3 を繰り返し、バッファをコミットする前に、両方のファブリック インターコネクトにアクセス可能なすべての VSAN から管理対象外のゾーンを削除することができます。
ステップ 4	UCS-A /fc-uplink/vsan # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、管理対象外のゾーンをネームド VSAN から削除し、トランザクションをコミットする方法を示します。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope vsan finance
UCS-A /fc-uplink/vsan # clear-unmanaged-fc-zones-all
UCS-A /fc-uplink/vsan* # commit-buffer
UCS-A /fc-uplink #
```

ファイバ チャネル ストレージ接続ポリシーの設定

ファイバ チャネル ストレージ接続ポリシーの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルート組織モードを開始するには、*/* を *org-name* として入力します。
ステップ 2	UCS-A /org # **create storage-connection-policy** *policy-name*	ストレージ接続ポリシーを指定されたポリシー名で作成し、組織ストレージ接続ポリシー モードを開始します。
ステップ 3	UCS-A /org # **set zoning-type** {**none** | **simt** | **sist**}	• [なし（None）]：Cisco UCS Manager はファイバチャネル ゾーン分割を設定しません。 • [単一イニシエータの単一ターゲット（Single Initiator Single Target）]：Cisco UCS Manager は、vHBA とストレージ ポートの組み合わせごとに 1 つのゾーンを自動作成します。各ゾーンには 2 つのメンバがあります。ゾーンの数がサポートされる最大数を超えると予想されない限り、このタイプのゾーン分割を設定することをお勧めします。 • [単一イニシエータの複数ターゲット（Single Initiator Multiple Targets）]：Cisco UCS Manager は、vHBA ごとに 1 つゾーンを自動作成します。ゾーンの数がサポートされる最大数に達するか、それを超えると予想される場合は、このタイプのゾーン分割を設定することをお勧めします。
ステップ 4	UCS-A /org/storage-connection-policy # **create storage-target** *wwpn*	指定された WWPN を持つストレージ ターゲット エンドポイントを作成し、ストレージ ターゲット モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	UCS-A /org/storage-connection-policy/storage-target # **set target-path** {**a** | **b**}	ターゲット エンドポイントとの通信に使用するファブリック インターコネクトを指定します。
ステップ 6	UCS-A /org/storage-connection-policy/storage-target # **set target-vsan** *vsan*	ターゲット エンドポイントとの通信に使用する VSAN を指定します。
ステップ 7	UCS-A /org/storage-connection-policy # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、ファブリック インターコネクト A とデフォルト VSAN を使用して scPolicyZone1 という名前のルート組織でファイバチャネルストレージ接続ポリシーを設定し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org* # create storage-connection-policy scPolicyZone1
UCS-A /org/storage-connection-policy* set zoning-type sist
UCS-A /org/storage-connection-policy* # create storage-target 20:10:20:30:40:50:60:70
UCS-A /org/storage-connection-policy/storage-target* # set target-path a
UCS-A /org/storage-connection-policy/storage-target* # set target-vsan default
UCS-A /org/storage-connection-policy* # commit-buffer
UCS-A /org/storage-connection-policy #
```

ファイバ チャネル ストレージ接続ポリシーの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルート組織モードを開始するには、/ を *org-name* として入力します。
ステップ 2	UCS-A /org # **delete storage-connection-policy** *policy-name*	指定されたストレージ接続ポリシーを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、ルート組織から scPolicyZone1 という名前のストレージ接続ポリシーを削除し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # delete san-connectivity-policy scPolicyZone1
```

```
UCS-A /org* # commit-buffer
UCS-A /org #
```

第 27 章

サーバ関連プールの設定

この章の内容は、次のとおりです。

サーバ プールの設定

サーバ プール

サーバ プールは複数のサーバで構成されています。これらのサーバは通常、同じ特性を持っています。これらの特性は、シャーシ内の位置であったり、サーバタイプ、メモリ容量、ローカル ストレージ、CPU のタイプ、ローカル ドライブ設定などの属性だったりします。サーバを手動でサーバ プールに割り当てることも、サーバ プール ポリシーとサーバ プール ポリシー資格情報を使用して割り当てを自動化することもできます。

システムが組織を通じて、マルチテナント機能を実装している場合、特定の組織で使用されるサーバ プールを 1 つ以上、指定できます。たとえば、CPU を 2 個搭載したサーバをすべて含むプールをマーケティング組織に割り当て、メモリのサイズが 64GB のサーバをすべて、財務組織に割り当てることができます。

サーバ プールには、システム内のどのシャーシにあるサーバでも入れることができます。1 つのサーバは複数のサーバ プールに属することができます。

サーバ プールの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **create server-pool** *server-pool-name*	指定した名前のサーバプールを作成し、組織サーバ プール モードを開始します。
ステップ 3	UCS-A /org/server-pool # **create server** *chassis-num*/*slot-num*	サーバ プールのサーバを作成します。 （注） サーバ プールには複数のサーバを含めることができます。プールに複数のサーバを作成するには、組織サーバ プール モードで複数の **create server** コマンドを入力する必要があります。
ステップ 4	UCS-A /org/server-pool # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例に、ServPool2 という名前のサーバ プールを作成し、そのサーバ プール用に 2 つのサーバを作成して、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org # create server-pool ServPool2
UCS-A /org/server-pool* # create server 1/1
UCS-A /org/server-pool* # create server 1/4
UCS-A /org/server-pool* # commit-buffer
UCS-A /org/server-pool #
```

サーバ プールの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **delete server-pool** *server-pool-name*	指定されたサーバ プールを削除します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、ServPool2 という名前のサーバプールを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # delete server-pool ServPool2
UCS-A /org* # commit-buffer
UCS-A /org #
```

UUID 接尾辞プール設定

UUID サフィックス プール

UUID サフィックス プールは、サーバへの割り当てに使用できる SMBIOS UUID の集まりです。UUID の接頭辞を構成する先頭の桁の数字は固定されています。残りの桁で構成される UUID 接尾辞は変数です。サービス プロファイルで特定の UUID サフィックス プールを使用すると、そのプロファイルに関連付けられているサーバの変数値が一意のものになり、競合を避けることができます。

サービス プロファイルで UUID サフィックス プールを使用する場合は、サービス プロファイルに関連付けられているサーバの UUID を手動で設定する必要はありません。

UUID サフィックス プールの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルート組織モードを開始するには、*/* を *org-name* として入力します。
ステップ 2	UCS-A /org # **create uuid-suffix-pool** *pool-name*	指定されたプール名で UUID 接尾辞プールを作成し、組織の UUID 接尾辞プール モードを開始します。 この名前には、1 ～ 32 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /org/uuid-suffix-pool #**set descr** *description*	（任意） UUID サフィックス プールの説明を記入します。 （注） 説明にスペース、特殊文字、または句読点が含まれている場合は、説明を引用符で括る必要があります。引用符は、**show** コマンド出力の説明フィールドには表示されません。
ステップ 4	UCS-A /org/uuid-suffix-pool # **set assignmentorder** {**default** | **sequential**}	次のいずれかになります。 • **default**：Cisco UCS Manager はプールからランダムな ID を選択します。 • **sequential**：Cisco UCS Manager はプールから最も小さい使用可能 ID を選択します。
ステップ 5	UCS-A /org/uuid-suffix-pool # **create block** *first-uuid last-uuid*	UUIDサフィックスブロック（範囲）を作成し、組織UUIDサフィックス プール ブロック モードを開始します。 *nnnn-nnnnnnnnnnnn* 形式を使用してブロック内の最初と最後のUUIDサフィックスを指定する必要があります。UUIDサフィックス間はスペースで区切ります。 （注） UUID サフィックス プールには、複数の UUID サフィックス ブロックを含めることができます。複数のブロックを作成するには、組織UUID接尾辞プール モードから複数の **create block** コマンドを入力する必要があります。
ステップ 6	UCS-A /org/uuid-suffix-pool/block # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、pool4 という名前の UUID サフィックス プールを作成し、プールの説明を記入し、プールに使用される UUID サフィックス ブロックを指定し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # create uuid-suffix-pool pool4
UCS-A /org/uuid-suffix-pool* # set descr "This is UUID suffix pool 4"
UCS-A /org/uuid-suffix-pool* # create block 1000-000000000001 1000-000000000010
UCS-A /org/uuid-suffix-pool/block* # commit-buffer
UCS-A /org/uuid-suffix-pool/block #
```

次の作業

UUID サフィックス プールをサービス プロファイルとテンプレートのうち一方、または両方に含めます。

UUID 接尾辞プールの削除

プールを削除した場合、Cisco UCS Manager は、 でプールの vNIC または vHBA に割り当てられたアドレスを再割り当てしません。削除されたプールのすべての割り当て済みブロックは、次のいずれかが起きるまで、割り当てられた vNIC または vHBA に残ります。

- 関連付けられたサービス プロファイルが削除された場合。
- アドレスが割り当てられた vNIC または vHBA が削除された場合。
- vNIC または vHBA が異なるプールに割り当てられた場合。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルート組織モードを開始するには、*/* を *org-name* として入力します。
ステップ 2	UCS-A /org # **delete uuid-suffix-pool** *pool-name*	指定された UUID サフィックス プールを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、pool4 という名前の UUID サフィックス プールを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # delete uuid-suffix-pool pool4
UCS-A /org* # commit-buffer
UCS-A /org #
```

IP プール設定

IP プール

IP プールは、用途が初期設定されていない IP アドレスの集合です。Cisco UCS Manager で IPv4 または IPv6 アドレス プールを作成して以下を行うことができます。

-
- サービス プロファイルが関連付けられているサーバのデフォルトの管理 IP プール ext-mgmt の置き換え。Cisco UCS Manager は、サーバ上の Cisco Integrated Management Controller（CIMC）で終端する外部アクセス用に、IP プールの各 IP アドレス ブロックを予約します。サービス

プロファイルが関連付けられていない場合は、CIMC 用の ext-mgmt IP プールを使用して IP アドレスを取得する必要があります。

- CIMC 用の管理インバンドまたはアウトオブバンド IP アドレスの置き換え。

（注） Cisco UCS Manager では iSCSI ブート IPv6 プールを作成できません。

Cisco UCS Manager で IPv4 アドレス プールを作成して以下を行うことができます。

- デフォルトの iSCSI ブート IP プール iscsi-initiator-pool の置き換え。Cisco UCS Manager は、指定された IP プールの各 IP アドレス ブロックを予約します。
- 管理 IP アドレスと iSCSI ブート IP アドレス両方の置き換え。

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

インバンド IP プールの作成

IPv4 および IPv6 アドレスのブロックを持つインバンド IP プールを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルート組織モードを開始するには、*/* を *org-name* として入力します。
ステップ 2	UCS-A /org # **create ip-pool** *pool-name*	指定された名前で IP プールを作成し、組織 IP プール モードを開始します。 この名前には、1～32 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
ステップ 3	UCS-A /org/ip-pool # **set descr** *description*	（任意） IP プールの説明を記入します。

	コマンドまたはアクション	目的
		（注） 説明にスペース、特殊文字、または句読点が含まれている場合は、説明を引用符で括る必要があります。引用符は、**show** コマンド出力の説明フィールドには表示されません。
ステップ 4	UCS-A /org/ip-pool # **create block** *first-ip-addr last-ip-addr gateway-ip-addr subnet-mask*	IP アドレス ブロック（範囲）を作成し、組織 IP プール ブロック モードを開始します。アドレス範囲の最初と最後の IP アドレス、ゲートウェイ IP アドレス、およびサブネットマスクを指定する必要があります。
ステップ 5	UCS-A /org/ip-pool/block # **commit-buffer**	トランザクションをシステム設定にコミットします。
ステップ 6	UCS-A /org/ip-pool/block # **exit**	組織 IP プール ブロック モードを終了します。
ステップ 7	UCS-A /org/ip-pool # **create ip6block** *first-ip6-addr last-ip6-addr gateway-ip6-addr prefix*	IPv6 アドレス ブロックを作成し、組織 IPv6 プール ブロック モードを開始します。アドレス範囲の最初と最後の IPv6 アドレス、ゲートウェイ IPv6 アドレス、およびネットワーク プレフィックスを指定する必要があります。
ステップ 8	UCS-A /org/ip-pool/ ipv6-block # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、inband-default という名前のインバンド IP プールを作成し、IPv4 アドレスのブロックを作成し、IPv6 アドレスのブロックを作成し、トランザクションをコミットします。

```
UCS-A# scope org
UCS-A /org # create ip-pool inband_default
UCS-A /org/ip-pool* # create block 192.168.100.10 192.168.100.100 192.168.100.1 255.255.255.0
UCS-A /org/ip-pool/block* # commit-buffer
UCS-A /org/ip-pool/block # exit
UCS-A /org/ip-pool # create ipv6-block 2001:888::10 2001:888::100 2001:888::1 64
UCS-A /org/ip-pool/ipv6-block* # commit-buffer
UCS-A /org/ip-pool/ipv6-block #
```

次の作業

IP プールをサービス プロファイルとテンプレートに含めます。

IP プールへのブロックの追加

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルート組織モードを開始するには、*/* を *org-name* として入力します。
ステップ 2	UCS-A /org # **scope ip-pool** *pool-name*	指定したプールの組織 IP プール モードを開始します。
ステップ 3	UCS-A /org/ip-pool # **create** *block first-ip-addr last-ip-addr gateway-ip-addr subnet-mask*	IP アドレス ブロック（範囲）を作成し、組織 IP プール ブロック モードを開始します。アドレス範囲の最初と最後の IP アドレス、ゲートウェイ IP アドレス、およびサブネットマスクを指定する必要があります。 （注） IP プールには、複数の IP ブロックを含めることができます。複数のブロックを作成するには、組織 IP プール モードから複数の **create block** コマンドを入力します。
ステップ 4	UCS-A /org/ip-pool/block # **commit-buffer**	トランザクションをコミットします。
ステップ 5	UCS-A /org/ip-pool/block # **exit**	IPv4 ブロック コンフィギュレーション モードを終了します。
ステップ 6	UCS-A /org/ip-pool # **create ipv6-block** *first-ip6-addr last-ip6-addr gateway-ip6-addr prefix*	IPv6 アドレスのブロック（範囲）を作成し、組織 IP プール IPv6 ブロック モードを開始します。アドレス範囲の最初と最後の IPv6 アドレス、ゲートウェイ IPv6 アドレス、およびネットワーク プレフィックスを指定する必要があります。 （注） IP プールには、複数の IPv6 ブロックを含めることができます。複数の IPv6 ブロックを作成するには、組織 IP プール モードから複数の **create ipv6-block** コマンドを入力します。
ステップ 7	UCS-A /org/ip-pool/ ipv6-block # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、IPv4 および IPv6 アドレスのブロックを pool4 という名前の IP プールに追加し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org # scope ip-pool pool4
```

```
UCS-A /org/ip-pool # create block 192.168.100.1 192.168.100.200 192.168.100.10 255.255.255.0
UCS-A /org/ip-pool/block* # commit-buffer
UCS-A /org/ip-pool/block #exit
UCS-A /org/ip-pool* # create ipv6-block 2001:888::10 2001:888::100 2001:888::1 64
UCS-A /org/ip-pool/ipv6-block* commit-buffer
```

IP プールからのブロックの削除

プールからアドレスブロックを削除した場合、Cisco UCS Manager では、そのブロック内から vNIC または vHBA に割り当てられていたアドレスは再割り当てされません。削除されたブロックのすべての割り当て済みブロックは、次のいずれかが起きるまで、割り当てられた vNIC または vHBA に残ります。

- 関連付けられたサービス プロファイルが削除された場合。
- アドレスが割り当てられた vNIC または vHBA が削除された場合。
- vNIC または vHBA が異なるプールに割り当てられた場合。

（注） IPv6 アドレス ブロックは、vNIC または vHBA には適用できません。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルート組織モードを開始するには、/ を *org-name* として入力します。
ステップ 2	UCS-A /org # **scope ip-pool***pool-name*	指定したプールの組織 IP プール モードを開始します。
ステップ 3	UCS-A /org/ip-pool # **delete** {*ip-block*|*ipv6-block*} {*first-ip-addr*|*first-ip6-addr*} {*last-ip-addr*|*last-ip6-addr*}	IPv4 または IPv6 アドレスの指定されたブロック（範囲）を削除します。
ステップ 4	UCS-A /org/ip-pool # **commit-buffer**	トランザクションをシステム設定にコミットします。

この例では、pool4 という名前の IP プールから IP アドレス ブロックを削除し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org # scope ip-pool pool4
UCS-A /org/ip-pool # delete block 192.168.100.1 192.168.100.200
UCS-A /org/ip-pool* # commit-buffer
UCS-A /org/ip-pool #
```

この例では、pool4 という名前の IP プールから IPv6 アドレス ブロックを削除し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org # scope ip-pool pool4
UCS-A /org/ip-pool # delete ipv6-block 2001::1 2001::10
UCS-A /org/ip-pool* # commit-buffer
UCS-A /org/ip-pool #
```

IP プールの削除

プールを削除した場合、Cisco UCS Manager は、 でプールの vNIC または vHBA に割り当てられたアドレスを再割り当てしません。削除されたプールのすべての割り当て済みブロックは、次のいずれかが起きるまで、割り当てられた vNIC または vHBA に残ります。

- 関連付けられたサービス プロファイルが削除された場合。
- アドレスが割り当てられた vNIC または vHBA が削除された場合。
- vNIC または vHBA が異なるプールに割り当てられた場合。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルート組織モードを開始するには、/ を *org-name* として入力します。
ステップ 2	UCS-A /org # **delete ip-pool** *pool-name*	指定された IP プールを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、pool4 という名前の IP プールを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # delete ip-pool pool4
UCS-A /org* # commit-buffer
UCS-A /org #
```

第 28 章

管理 IP アドレスの設定

この章の内容は、次のとおりです。

管理 IP アドレス

Cisco UCS ドメイン の各サーバには 1 つ以上の管理 IP アドレスが必要です。これらの IP アドレスは、Cisco Integrated Management Controller（CIMC）に割り当てられたり、サーバに関連付けられたサービス プロファイルに割り当てられます。Cisco UCS Manager は CIMC で終端する外部アクセスのためにこの IP アドレスを使用します。この外部アクセスは、次のいずれかのサービスを経由することが可能です。

- KVM コンソール
- Serial over LAN
- IPMI ツール

サーバの CIMC にアクセスするための管理 IP アドレスとして、アウトオブバンド（OOB）アドレス（このアドレスから管理ポート経由で、トラフィックがファブリック インターコネクトを通過）、またはインバンドアドレス（このアドレスからファブリック アップリンク ポート経由で、トラフィックがファブリック インターコネクトを通過）を使用できます。サーバの CIMC にアクセスする最大 6 つの IP アドレスを設定できます（2 つはアウトオブバンド（OOB）アドレス、他の 4 つはインバンド アドレス）。

以下の管理 IP アドレスを設定できます。

- サーバに直接割り当てられるスタティック OOB IPv4 アドレス
- グローバル ext-mgmt プールからサーバに割り当てられる OOB IPv4 アドレス
- 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
- 管理 IP プールから取り込まれ、サービス プロファイルまたはサービス プロファイル テンプレートに割り当てられるインバンド IPv4 アドレス
- サーバに直接割り当てられるスタティック インバンド IPv6 アドレス
- 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

サーバの各 CIMC およびサーバに関連付けられたサービス プロファイルに、複数の管理 IP アドレスを割り当てることができます。その場合は、それぞれ異なる IP アドレスを使用する必要があります。

サービス プロファイルに割り当てられた管理 IP アドレスはそのサービス プロファイルとともに移動します。別のサーバにサービス プロファイルを移行するときに KVM または SoL セッションがアクティブな場合、Cisco UCS Manager はセッションを終了させ、移行完了後もそのセッションを再開しません。この IP アドレスは、サービスプロファイルを作成または変更するときに設定します。

（注） Cisco UCS ドメイン 内のサーバまたはサービス プロファイルにすでにスタティック IP アドレスが割り当てられている場合、サーバまたはサービス プロファイルにそのスタティック IP アドレスを割り当てることはできません。そのような設定を試みると、Cisco UCS Manager は IP アドレスがすでに使用中であることを警告し、設定を拒否します。

ブレード サーバの管理 IP アドレスの設定

ブレード サーバにスタティック IP アドレスを使用させる設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *chassis-id/blade-id*	指定サーバのシャーシ サーバ モードを開始します。
ステップ 2	UCS-A /chassis/server # **scope cimc**	シャーシ サーバ CIMC モードを開始します。
ステップ 3	UCS-A /chassis/server/cimc # **create ext-static-ip**	指定されたサーバのスタティック管理 IP アドレスを作成します。

	コマンドまたはアクション	目的
ステップ 4	UCS-A /chassis/server/cimc/ext-static-ip # **set addr** *ip-addr*	サーバに割り当てられるスタティック IPv4 アドレスを指定します。
ステップ 5	UCS-A /chassis/server/cimc/ext-static-ip # **set default-gw** *ip-addr*	IP アドレスが使用するデフォルト ゲートウェイを指定します。
ステップ 6	UCS-A /chassis/server/cimc/ext-static-ip # **set subnet** *ip-addr*	IP アドレスのサブネット マスクを指定します。
ステップ 7	UCS-A /chassis/server/cimc/ext-static-ip # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、シャーシ 1 のサーバ 1 にスタティック管理 IP アドレスを設定し、スタティック IPv4 アドレスを設定し、デフォルト ゲートウェイを設定し、サブネット マスクを設定し、トランザクションをコミットします。

```
UCS-A# scope server 1/1
UCS-A /chassis/server # scope cimc
UCS-A /chassis/server/cimc # create ext-static-ip
UCS-A /chassis/server/cimc/ext-static-ip* # set addr 192.168.10.10
UCS-A /chassis/server/cimc/ext-static-ip* # set default-gw 192.168.10.1
UCS-A /chassis/server/cimc/ext-static-ip* # set subnet 255.255.255.0
UCS-A /chassis/server/cimc/ext-static-ip* # commit-buffer
UCS-A /chassis/server/cimc/ext-static-ip #
```

ブレード サーバにスタティック IPv6 アドレスを使用させる設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *chassis-id/blade-id*	指定サーバのシャーシ サーバ モードを開始します。
ステップ 2	UCS-A /chassis/server # **scope cimc**	シャーシ サーバ CIMC モードを開始します。
ステップ 3	UCS-A /chassis/server/cimc # **create ext-static-ip6**	指定されたサーバのスタティック管理 IPv6 アドレスを作成します。
ステップ 4	UCS-A /chassis/server/cimc/ext-static-ip6 # **set addr ipv6-addr**	サーバに割り当てられるスタティック IPv6 アドレスを指定します。
ステップ 5	UCS-A /chassis/server/cimc/ext-static-ip6 # **set default-gw ip6-addr**	IPv6 アドレスが使用するデフォルト ゲートウェイを指定します。

	コマンドまたはアクション	目的
ステップ 6	UCS-A /chassis/server/cimc/ext-static-ip6 # **set prefix ip6-addr**	IPv6 アドレスのネットワーク プレフィックスを指定します。
ステップ 7	UCS-A /chassis/server/cimc/ext-static-ip6 # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、シャーシ 1 のサーバ 1 にスタティック管理 IPv6 アドレスを設定し、スタティック IPv6 アドレスを設定し、デフォルト ゲートウェイを設定し、ネットワーク プレフィックスを設定し、トランザクションをコミットします。

```
UCS-A# scope server 1/1
UCS-A /chassis/server # scope cimc
UCS-A /chassis/server/cimc # create ext-static-ip6
UCS-A /chassis/server/cimc/ext-static-ip* # set addr 2001:888::10
UCS-A /chassis/server/cimc/ext-static-ip* # set default-gw 2001:888::100
UCS-A /chassis/server/cimc/ext-static-ip* # set prefix 64
UCS-A /chassis/server/cimc/ext-static-ip* # commit-buffer
UCS-A /chassis/server/cimc/ext-static-ip #
```

ブレード サーバで管理 IP プールを使用するための設定

スタティック管理 IP アドレスを削除すると、指定サーバを管理 IP プールに戻します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *chassis-id/blade-id*	指定サーバのシャーシ サーバ モードを開始します。
ステップ 2	UCS-A /chassis/server # **scope cimc**	シャーシ サーバ CIMC モードを開始します。
ステップ 3	UCS-A /chassis/server/cimc # **delete** {*ext-static-ip* | *ext-static-ip6*}	外部スタティック IPv4 または IPv6 アドレスを削除し、管理 IP プールにブレード サーバを戻します。
ステップ 4	UCS-A /chassis/server/cimc/ # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、シャーシ 1 のサーバ 1 のスタティック管理 IP アドレスを削除し、トランザクションをコミットします。

```
UCS-A# scope server 1/1
UCS-A /chassis/server # scope cimc
```

```
UCS-A /chassis/server/cimc # delete ext-static-ip
UCS-A /chassis/server/cimc* # commit-buffer
UCS-A /chassis/server/cimc/ #
```

次の例は、シャーシ 1 のサーバ 1 のスタティック管理 IPv6 アドレスを削除し、トランザクションをコミットします。

```
UCS-A# scope server 1/1
UCS-A /chassis/server # scope cimc
UCS-A /chassis/server/cimc # delete ext-static-ip6
UCS-A /chassis/server/cimc* # commit-buffer
UCS-A /chassis/server/cimc/ #
```

ラック サーバの管理 IP アドレスの設定

ラック サーバでスタティック IP アドレスを使用するための設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *blade-id*	指定したサーバのサーバ モードを開始します。
ステップ 2	UCS-A /server # **scope cimc**	サーバ CIMC モードを開始します。
ステップ 3	UCS-A /server/cimc # **create ext-static-ip**	指定されたサーバのスタティック管理 IP アドレスを作成します。
ステップ 4	UCS-A /server/cimc/ext-static-ip # **set addr** *ip-addr*	サーバに割り当てられるスタティック IPv4 アドレスを指定します。
ステップ 5	UCS-A /server/cimc/ext-static-ip # **set default-gw** *ip-addr*	IP アドレスが使用するデフォルト ゲートウェイを指定します。
ステップ 6	UCS-A /server/cimc/ext-static-ip # **set subnet** *ip-addr*	IP アドレスのサブネット マスクを指定します。
ステップ 7	UCS-A /server/cimc/ext-static-ip # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、ラック サーバ 1 にスタティック管理 IP アドレスを設定し、スタティック IPv4 アドレスを設定し、デフォルトゲートウェイを設定し、サブネットマスクを設定し、トランザクションをコミットします。

```
UCS-A# scope server 1
UCS-A /server # scope cimc
UCS-A /server/cimc # create ext-static-ip
UCS-A /server/cimc/ext-static-ip* # set addr 192.168.10.10
UCS-A /server/cimc/ext-static-ip* # set default-gw 192.168.10.1
UCS-A /server/cimc/ext-static-ip* # set subnet 255.255.255.0
```

```
UCS-A /server/cimc/ext-static-ip* # commit-buffer
UCS-A /server/cimc/ext-static-ip #
```

ラック サーバにスタティック IPv6 アドレスを使用させる設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *blade-id*	指定したサーバのサーバ モードを開始します。
ステップ 2	UCS-A /server # **scope cimc**	サーバ CIMC モードを開始します。
ステップ 3	UCS-A /server/cimc # **create ext-static-ip6**	指定されたサーバのスタティック管理 IPv6 アドレスを作成します。
ステップ 4	UCS-A /server/cimc/ext-static-ip6 # **set addr** *ip6-addr*	サーバに割り当てられるスタティック IPv6 アドレスを指定します。
ステップ 5	UCS-A /server/cimc/ext-static-ip6 # **set default-gw** *ip6-addr*	IP アドレスが使用するデフォルト ゲートウェイを指定します。
ステップ 6	UCS-A /server/cimc/ext-static-ip6 # **set prefix** *ip6-addr*	IPv6 アドレスのネットワーク プレフィックスを指定します。
ステップ 7	UCS-A /server/cimc/ext-static-ip # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、ラック サーバ 1 にスタティック管理 IPv6 アドレスを設定し、スタティック IPv4 アドレスを設定し、デフォルト ゲートウェイを設定し、ネットワーク プレフィックスを設定し、トランザクションをコミットします。

```
UCS-A# scope server 1
UCS-A /server # scope cimc
UCS-A /server/cimc # create ext-static-ip6
UCS-A /server/cimc/ext-static-ip6* # set addr 2001::8999
UCS-A /server/cimc/ext-static-ip6* # set default-gw 2001::1
UCS-A /server/cimc/ext-static-ip6* # set prefix 64
UCS-A /server/cimc/ext-static-ip6* # commit-buffer
UCS-A /server/cimc/ext-static-ip #
```

ラック サーバで管理 IP プールを使用するための設定

スタティック管理 IP アドレスを削除すると、指定サーバを管理 IP プールに戻します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *blade-id*	指定したサーバのサーバモードを開始します。
ステップ 2	UCS-A /server # **scope cimc**	サーバ CIMC モードに入ります。
ステップ 3	UCS-A /server/cimc # **delete** {*ext-static-ip* | *ext-static-ip6*}	外部スタティック IPv4 または IPv6 アドレスを削除し、管理 IP プールにラック サーバを戻します。
ステップ 4	UCS-A /server/cimc/ # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、ラック サーバ 1 のスタティック管理 IP アドレスを削除し、トランザクションをコミットします。

```
UCS-A# scope server 1
UCS-A /server # scope cimc
UCS-A /server/cimc # delete ext-static-ip
UCS-A /server/cimc* # commit-buffer
UCS-A /server/cimc/ #
```

次の例は、ラック サーバ 1 のスタティック管理 IPv6 アドレスを削除し、トランザクションをコミットします。

```
UCS-A# scope server 1
UCS-A /server # scope cimc
UCS-A /server/cimc # delete ext-static-ip6
UCS-A /server/cimc* # commit-buffer
UCS-A /server/cimc/ #
```

サービス プロファイルまたはサービス プロファイル テンプレートでの管理 IP アドレスの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。 ルート組織モードを開始するには、org-name に / と入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	指定したサービスで組織サービス プロファイル モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /org/service-profile # **set ext-mgmt-ip-state** {*none* | *ext-pooled-ip* | *ext-pooled-ip6*|*ext-static-ip*|*ext-static-ip6*}	管理 IPv4 または IPv6 アドレスをサービス プロファイルに割り当てる方法を指定します。 次のオプションを使用して管理 IP アドレス ポリシーを設定できます。 • [なし（None）]：サービス プロファイルには IP アドレスが割り当てられません。 • [プール済み（Pooled）]：サービスプロファイルに管理 IPv4 または IPv6 プールから IP アドレスが割り当てられます。 • [スタティック（Static）]：サービス プロファイルに設定済みのスタティック IPv4 または IPv6 アドレスが割り当てられます。 （注） サービス プロファイル テンプレートでは ext-management-ip-state を static に設定することはサポートされておらず、設定するとエラーが発生します。
ステップ 4	UCS-A /org/service-profile # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、accounting というサービス プロファイルの管理 IP アドレス ポリシーを static IPv4 に設定し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # scope service-profile accounting
UCS-A /org/service-profile # set ext-mgmt-ip-state ext-static-ip
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile #
```

次の作業

管理 IP アドレスを static に設定する場合、スタティック IP アドレスを使用するようにサーバを設定します。

管理 IP プールの設定

管理 IP プール

デフォルトの管理 IP プール ext-mgmt は、外部の IPv4 および IPv6 アドレスの集合です。Cisco UCS Manager は、サーバの CIMC で終端する外部アクセスのために、管理 IP プールに IP アドレスの各ブロックを予約しています。

個別のアウトオブバンド IPv4 アドレス プール、およびインバンド IPv4 または IPv6 アドレス プールを設定できます。IPv4 と IPv6 アドレス ブロックの両方を含むインバンド プールを設定できます。

ヒント　サーバ CIMC に IPv4 アドレスのみを含む IP プールをインバンド IPv6 ポリシーとして割り当てたり、IPv6 アドレスのみ含む IP プールをインバンド IPv4 ポリシーとして割り当てることを回避するために、それぞれが IPv4 または IPv6 アドレスのみを持つ個別のインバンド アドレス プールを設定することを推奨します。

管理 IP プールの IP アドレスを使用するようにサービス プロファイルとサービス プロファイル テンプレートを設定できます。管理 IP プールを使用するようサーバを設定することはできません。

管理 IP プール内のすべての IP アドレスは、同じ IPv4 サブネットに含まれるか、ファブリック インターコネクトの IP アドレスと同じ IPv6 ネットワーク プレフィックスが付けられている必要があります。

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

管理 IP プールの IP アドレス ブロックの設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org /**	ルート組織モードを開始します。
ステップ 2	UCS-A /org # **scope ip-pool ext-mgmt**	組織 IP プール モードを開始します。

	コマンドまたはアクション	目的
		（注） 管理 IP プールの作成（または削除）はできません。既存のデフォルト プールに入る（範囲を設定する）ことだけが可能です。
ステップ 3	UCS-A /org/ip-pool # **set descr** *description*	（任意） 管理 IP プールに説明を記入します。この説明は管理 IP プールのすべてのアドレス ブロックに適用されます。 （注） 説明にスペース、特殊文字、または句読点が含まれている場合は、説明を引用符で括る必要があります。引用符は、**show** コマンド出力の説明フィールドには表示されません。
ステップ 4	UCS-A /org/ip-pool # **set assignmentorder** {**default** | **sequential**}	次のいずれかになります。 • **default**：Cisco UCS Manager はプールからランダムな ID を選択します。 • **sequential**：Cisco UCS Manager はプールから最も小さい使用可能 ID を選択します。
ステップ 5	UCS-A /org/ip-pool # **create block** *first-ip-addr last-ip-addr gateway-ip-addr subnet-mask*	IP アドレス ブロック（範囲）を作成し、組織 IP プール ブロック モードを開始します。アドレス範囲の最初と最後の IP アドレス、ゲートウェイ IP アドレス、およびサブネット マスクを指定する必要があります。 （注） IP プールには、複数の IP ブロックを含めることができます。複数のブロックを作成するには、組織 IP プール モードから複数の **create block** コマンドを入力します。
ステップ 6	UCS-A /org/ip-pool/block # **set primary-dns** *ip-addrress* |**secondary-dns** *ip-address*	プライマリ DNS とセカンダリ DNS の IP アドレスを指定します。
ステップ 7	UCS-A /org/ip-pool/ ipv6-block # **commit-buffer**	トランザクションをシステム設定にコミットします。
ステップ 8	UCS-A /org/ip-pool/block # **exit**	IPv4 ブロック コンフィギュレーション モードを終了します。
ステップ 9	UCS-A /org/ip-pool # **create ipv6-block** *first-ip6-addr last-ip6-addr gateway-ip6-addr prefix*	IPv6 アドレスのブロック（範囲）を作成し、組織 IP プール IPv6 ブロック モードを開始します。アドレス範囲の最初と最後の IPv6 アドレス、ゲートウェイ

	コマンドまたはアクション	目的
		IPv6アドレス、およびネットワーク プレフィックスを指定する必要があります。 （注） IP プールには、複数の IPv6 ブロックを含めることができます。複数の IPv6 ブロックを作成するには、組織 IP プール モードから複数の **create ipv6-block** コマンドを入力します。
ステップ 10	UCS-A /org/ip-pool/ipv6-block # **set primary-dns** *ip6-address* **secondary-dns** *ip6-address*	プライマリ DNS とセカンダリ DNS の IPv6 アドレスを指定します。
ステップ 11	UCS-A /org/ip-pool/ipv6-block # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、管理 IP プールの IPv4 アドレス ブロックを設定し、プライマリおよびセカンダリ IPv4アドレスを指定し、IPv6ブロックを作成し、プライマリおよびセカンダリ IPv6アドレスを指定し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # scope ip-pool ext-mgmt-ip
UCS-A /org/ip-pool* # set descr "This is a management ip pool example."
UCS-A /org/ip-pool* # create block 192.168.100.1 192.168.100.200 192.168.100.10 255.255.255.0
UCS-A /org/ip-pool/block* # set primary-dns 192.168.100.1 secondary-dns 192.168.100.20
UCS-A /org/ip-pool/block* commit-buffer
UCS-A /org/ip-pool/block exit
UCS-A /org/ip-pool* # create ipv6-block 2001:888::10 2001:888::100 2001:888::1 64
UCS-A /org/ip-pool/ipv6- block* set primary-dns 2001:888::11 secondary-dns 2001:888::12
UCS-A /org/ip-pool/ipv6- block* commit-buffer
UCS-A /org/ip-pool/ipv6- block #UCS-A /org/ip-pool/block* # commit-buffer
UCS-A /org/ip-pool/block #
```

次の例では、管理 IP プールの IPv6 アドレス ブロックを設定し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org #scope ip-pool ext-mgmt-ip
UCS-A /org/ip-pool* # set descr "This is a management IPv6 pool example."
UCS-A /org/ip-pool* # create ipv6-block 2001:888::10 2001:888::100 2001:888::1 64
UCS-A /org/ip-pool/ipv6-block* # commit-buffer
UCS-A /org/ip-pool/ipv6-block* #
```

次の作業

1 つ以上のサービス プロファイルまたはサービス プロファイル テンプレートを設定し、管理 IP プールから CIMC IP アドレスを取得します。

管理 IP プールからの IP アドレス ブロックの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **scope ip-pool ext-mgmt**	管理 IP プールを入力します。
ステップ 3	UCS-A /org/ip-pool # **delete** {*ip-block*|*ipv6-block*} {*first-ip-addr*|*first-ip6-addr*} {*last-ip-addr*|*last-ip6-addr*}	IPv4 または IPv6 アドレスの指定されたブロック（範囲）を削除します。
ステップ 4	UCS-A /org/ip-pool # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、管理 IP プールから IP アドレス ブロックを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # scope ip-pool ext-mgmt
UCS-A /org/ip-pool # delete block 192.168.100.1 192.168.100.200
UCS-A /org/ip-pool* # commit-buffer
UCS-A /org/ip-pool #
```

次に、管理 IP プールから IPv6 アドレス ブロックを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # scope ip-pool pool4
UCS-A /org/ip-pool # delete ipv6-block 2001::1 2001::10
UCS-A /org/ip-pool* # commit-buffer
UCS-A /org/ip-pool #
```

第 29 章

サーバ関連ポリシーの設定

この章の内容は、次のとおりです。

BIOS の設定

サーバ BIOS 設定

Cisco UCS では、Cisco UCS ドメイン内のサーバの BIOS 設定をグローバルに変更する 2 種類の方法が用意されています。サーバまたはサーバの集合のニーズに合う特定の BIOS 設定グループを含む BIOS ポリシーを 1 つ以上作成するか、特定のサーバ プラットフォームに対するデフォルトの BIOS 設定を使用できます。

BIOS ポリシーおよびサーバ プラットフォームのデフォルトの BIOS 設定のいずれを使用しても、Cisco UCS Manager によって管理されているサーバの BIOS 設定を微調整できます。

データセンターのニーズに応じて、同じ Cisco UCS ドメイン内の一部のサービス プロファイルに BIOS ポリシーを設定して、他のサービス プロファイルにデフォルトの BIOS 設定を使用するか、そのいずれかのみを使用することができます。また、Cisco UCS Manager を使用して、サーバの実際の BIOS 設定を表示し、それらが現在のニーズを満たしているかどうかを確認できます。

（注） Cisco UCS Manager は、BIOS ポリシーまたはデフォルトの BIOS 設定による BIOS 設定の変更を Cisco Integrated Management Controller（CIMC）バッファにプッシュします。これらの変更はバッファ内にとどまり、サーバがリブートされるまでは有効になりません。

設定するサーバで BIOS 設定のサポートを確認することをお勧めします。RAS メモリのミラーリング モードなどの一部の設定は、すべての Cisco UCS サーバでサポートされているわけではありません。

メイン BIOS 設定

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

名前	説明
[BIOS 設定変更時のリブート（Reboot on BIOS Settings Change）] **set reboot-on-update**	1 つ以上の BIOS 設定を変更した後、サーバをリブートするタイミング。 **yes**：この設定を有効にした場合、サーバはそのサービス プロファイルのメンテナンス ポリシーに従ってリブートされます。たとえば、メンテナンス ポリシーでユーザの確認応答が必要な場合、サーバはリブートされず、ユーザが保留中のアクティビティを確認するまで BIOS の変更は適用されません。 **no**：この設定を有効にしない場合は、他のサーバ設定の変更によるリブートであろうと、手動によるリブートであろうと、BIOS の変更は次回サーバがリブートされるまで適用されません。

名前	説明
[Quiet Boot] **set quiet-boot-config quiet-boot**	BIOS が Power On Self-Test（POST）中に表示する内容。次のいずれかになります。 • [無効（Disabled）]：BIOS はブート中にすべてのメッセージとオプション ROM 情報を表示します。 • [有効（Enabled）]：BIOS はロゴ画面を表示しますが、ブート中にメッセージやオプション ROM 情報を表示しません。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[Post エラー一時停止（Post Error Pause）] **set post-error-pause-config post-error-pause**	POST 中にサーバで重大なエラーが発生した場合の処理。次のいずれかになります。 • [無効（Disabled）]：BIOS はサーバのブートを続行します。 • [有効（Enabled）]：POST 中に重大なエラーが発生した場合、BIOS はサーバのブートを一時停止し、Error Manager を開きます。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[停電時に AC を再開（Resume Ac On Power Loss）] **set resume-ac-on-power-loss-config resume-action**	予期しない電力損失後に電力が復帰したときにサーバがどのように動作するかを決定します。次のいずれかになります。 • [オフのまま（stay-off）]：手動で電源をオンにするまでサーバの電源がオフになります。 • [最後の状態（last-state）]：サーバの電源がオンになり、システムが最後の状態を復元しようとします。 • [リセット（reset）]：サーバの電源がオンになり、自動的にリセットされます。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[前面パネルのロックアウト（Front Panel Lockout）] **set front-panel-lockout-config front-panel-lockout**	前面パネルの電源ボタンとリセット ボタンがサーバによって無視されるかどうかを決定します。次のいずれかになります。 • [無効（Disabled）]：前面パネルの電源ボタンとリセットボタンはアクティブであり、サーバに影響を与えるために使用できます。 • [有効（Enabled）]：電源ボタンとリセットボタンはロックアウトされます。サーバをリセットしたり、電源をオンにしたりできるのは、CIMC GUI からだけです。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[一貫したデバイスの命名（Consistent Device Naming）] **set consistent-device-name-control cdn-name**	一貫したデバイスの命名によって、一貫した方法でイーサネットインターフェイスに名前を付けることができます。これによりイーサネット インターフェイスの名前は、より統一され、識別しやすくなり、アダプタや他の設定に変更が加えられても永続的に保持されます。 一貫したデバイスの命名を有効にするかどうか。次のいずれかになります。 • [無効（Disabled）]：一貫したデバイスの命名はBIOSポリシーで無効になっています。 • [有効（Enabled）]：一貫したデバイスの命名がBIOSポリシーで有効になります。これにより、イーサネットインターフェイスに一貫した方法で命名できます。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

プロセッサの BIOS 設定

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

[名前（Name）]	説明
[ターボ ブースト（Turbo Boost）] **set intel-turbo-boost-config turbo-boost**	プロセッサで Intel Turbo Boost Technology を使用するかどうか。このテクノロジーでは、仕様よりも低い電力、温度、または電圧でプロセッサが動作していると、自動的にそのプロセッサの周波数が上がります。次のいずれかになります。 • [無効（Disabled）]：プロセッサの周波数は自動的には上がりません。 • [有効（Enabled）]：必要に応じてプロセッサで Turbo Boost Technology が利用されます。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[Enhanced Intel Speedstep] **set enhanced-intel-speedstep-config speed-step**	プロセッサで Enhanced Intel SpeedStep Technology を使用するかどうか。このテクノロジーでは、プロセッサの電圧やコア周波数をシステムが動的に調整できます。このテクノロジーにより、平均電力消費量と平均熱発生量が減少する可能性があります。次のいずれかになります。 • [無効（Disabled）]：プロセッサの電圧または周波数を動的に調整しません。 • [有効（Enabled）]：プロセッサで Enhanced Intel SpeedStep Technology が使用され、サポートされているすべてのスリープ状態でさらに電力を節約することが可能になります。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。 オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせることを推奨します。

[名前（Name）]	説明
[ハイパー スレッディング（Hyper Threading）] **set hyper-threading-config hyper-threading**	プロセッサで Intel Hyper-Threading Technology を使用するかどうか。このテクノロジーでは、マルチスレッドソフトウェアアプリケーションのスレッドを各プロセッサ内で並列に実行できます。次のいずれかになります。 • [無効（Disabled）]：プロセッサでのハイパースレッディングを禁止します。 • [有効（Enabled）]：プロセッサでの複数スレッドの並列実行を許可します。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。 オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせることを推奨します。
[コア多重処理（Core Multi Processing）] **set core-multi-processing-config multi-processing**	CPU あたりのパッケージの論理プロセッサ コアの状態を設定します。この設定を無効にすると、Intel Hyper Threading テクノロジーも無効になります。次のいずれかになります。 • [すべて（all）]：すべての論理プロセッサ コアの多重処理を有効にします。 • [1 ～ *n]*：サーバで実行可能な CPU あたりの論理プロセッサ コアの数を指定します。多重処理を無効にして、サーバで実行される CPU あたりの論理プロセッサ コアを 1 個のみにするには、[1] を選択します。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。 オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせることを推奨します。

[名前（Name）]	説明
[無効ビットの実行（Execute Disabled Bit）] **set execute-disable bit**	サーバのメモリ領域を分類し、アプリケーション コードを実行可能な場所を指定します。この分類の結果、悪意のあるワームがバッファにコードを挿入しようとした場合、プロセッサでコードの実行を無効にします。この設定は、損害、ワームの増殖、および特定クラスの悪意のあるバッファ オーバーフロー攻撃を防止するのに役立ちます。次のいずれかになります。 • [無効（Disabled）]：プロセッサでメモリ領域を分類しません。 • [有効（Enabled）]：プロセッサでメモリ領域を分類します。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。 オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせることを推奨します。
[仮想化テクノロジー（VT）（Virtualization Technology (VT)）] **set intel-vt-config vt**	プロセッサで Intel Virtualization Technology を使用するかどうか。このテクノロジーでは、1 つのプラットフォームで、複数のオペレーティング システムとアプリケーションをそれぞれ独立したパーティション内で実行できます。次のいずれかになります。 • [無効（Disabled）]：プロセッサでの仮想化を禁止します。 • [有効（Enabled）]：プロセッサで、複数のオペレーティングシステムをそれぞれ独立したパーティション内で実行できます。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。 （注） このオプションを変更した場合は、設定を有効にするためにサーバの電源を再投入する必要があります。

[名前（Name）]	説明
[ハードウェア プリフェッチャ（Hardware Pre-fetcher）] **set processor-prefetch-config hardware-prefetch**	プロセッサで、インテル ハードウェア プリフェッチャが必要に応じてデータおよび命令ストリームをメモリから取得し、統合 2 次キャッシュに入れることを許可するかどうか。次のいずれかになります。 • [無効（Disabled）]：ハードウェア プリフェッチャは使用しません。 • [有効（Enabled）]：プロセッサで、キャッシュの問題が検出されたときにプリフェッチャを使用します。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。 （注） この値を指定するには、[CPUPerformance] を [カスタム（Custom）]に設定する必要があります。[カスタム（Custom）]以外の値の場合は、このオプションよりも、選択された CPU パフォーマンス プロファイルの設定が優先されます。
[隣接キャッシュラインプリフェッチャ（Adjacent Cache Line Pre-fetcher）] **set processor-prefetch-config adjacent-cache-line-prefetch**	プロセッサで必要な行のみを取得するのではなく、偶数または奇数のペアのキャッシュ行を取得するかどうか。次のいずれかになります。 • [無効（Disabled）]：プロセッサで必要な行のみを取得します。 • [有効（Enabled）]：プロセッサで必要な行およびペアの行の両方を取得します。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。 （注） この値を指定するには、[CPUPerformance] を [カスタム（Custom）]に設定する必要があります。[カスタム（Custom）]以外の値の場合は、このオプションよりも、選択された CPU パフォーマンス プロファイルの設定が優先されます。

[名前（Name）]	説明
[DCU ストリーマー プリフェッチ（DCU Streamer Pre-fetch）] **set processor-prefetch-config dcu-streamer-prefetch**	プロセッサで DCU IP Prefetch メカニズムを使用して履歴キャッシュ アクセス パターンを分析し、L1 キャッシュ内で最も関連性の高い行をプリロードします。次のいずれかになります。 • [無効（Disabled）]：プロセッサはキャッシュ読み取り要求を予測しようとせず、明示的に要求された行のみを取得します。 • [有効（Enabled）]：DCU Prefetcher でキャッシュ読み取りパターンを分析し、必要と判断した場合にキャッシュ内の次の行を事前に取得します。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[DCU IP プリフェッチ（DCU IP Pre-fetcher）] **set processor-prefetch-config dcu-ip-prefetch**	プロセッサで DCU IP Prefetch メカニズムを使用して履歴キャッシュ アクセス パターンを分析し、L1 キャッシュ内で最も関連性の高い行をプリロードします。次のいずれかになります。 • [無効（Disabled）]：プロセッサでキャッシュ データをプリロードしません。 • [有効（Enabled）]：DCU IP Prefetcher で最も関連性が高いと判断されたデータを含む L1 キャッシュをプリロードします。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

[名前（Name）]	説明
[Direct Cache Access] **set direct-cache-access-config access**	プロセッサで、データを I/O デバイスから直接プロセッサ キャッシュに入れることにより、I/O パフォーマンスを向上させることができます。この設定はキャッシュ ミスを減らすのに役立ちます。次のいずれかになります。 • [無効（Disabled）]：データは I/O デバイスから直接プロセッサ キャッシュには入れられません。 • [有効（Enabled）]：データは I/O デバイスから直接プロセッサ キャッシュに入れられます。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[プロセッサ C ステート（Processor C State）] **set processor-c-state-config c-state**	アイドル期間中にシステムが省電力モードに入ることができるかどうか。次のいずれかになります。 • [無効（Disabled）]：システムは、アイドル時にも高パフォーマンス状態を維持します。 • [有効（Enabled）]：システムは DIMM や CPU などのシステム コンポーネントへの電力を低減できます。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。 オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせることを推奨します。

[名前（Name）]	説明
[プロセッサ C1E（Processor C1E）] **set processor-c1e-config c1e**	C1 に入ってプロセッサが最低周波数に遷移できるようにします。この設定は、サーバをリブートするまで有効になりません。次のいずれかになります。 • [無効（Disabled）]：CPU は C1 状態でも引き続き最大周波数で動作します。 • [有効（Enabled）]：CPU は最小周波数に移行します。このオプションでは、C1 状態での最大電力量が削減されます。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[プロセッサ C3 レポート（Processor C3 Report）] ドロップダウンリスト **set processor-c3-report-config processor-c3-report**	プロセッサからオペレーティング システムに C3 レポートを送信するかどうか。次のいずれかになります。 • [無効（Disabled）]：プロセッサから C3 レポートを送信しません。 • [acpi-c2]：プロセッサは Advanced Configuration and Power Interface（ACPI）C2 フォーマットを使用して C3 レポートを送信します。 • [acpi-c3]：ACPI C3 フォーマットを使用してプロセッサから C3 レポートを送信します。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。 Cisco UCS B440 Server の場合、[BIOS 設定（BIOS Setup）] メニューでこれらのオプションに対して [有効（Enabled）] と [無効（disabled）] が使用されます。[acpi-c2] または [acpi-c2] を指定すると、このサーバではそのオプションの BIOS 値に [有効（Enabled）] が設定されます。

[名前（Name）]	説明
[プロセッサ C6 レポート（Processor C6 Report）] **set processor-c6-report-config processor-c6-report**	プロセッサからオペレーティング システムに C6 レポートを送信するかどうか。次のいずれかになります。 • [無効（Disabled）]：プロセッサから C6 レポートを送信しません。 • [有効（Enabled）]：プロセッサから C6 レポートを送信します。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
Processor C7 Report **set processor-c7-report-config processor-c7-report**	プロセッサからオペレーティング システムに C7 レポートを送信するかどうか。次のいずれかになります。 • [無効（Disabled）]：プロセッサから C7 レポートを送信しません。 • [有効（Enabled）]：プロセッサから C7 レポートを送信します。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[CPU パフォーマンス（CPU Performance）] **set cpu-performance-config cpu-performance**	サーバの CPU パフォーマンス プロファイルを設定します。次のいずれかになります。 • [エンタープライズ（Enterprise）]：M3 サーバに対して、すべてのプリフェッチャとデータの再利用が有効になります。M1 および M2 サーバについては、データの再利用と DCU IP プリフェッチャは有効になり、他のすべてのプリフェッチャは無効になります。 • [高スループット（high-throughput）]：データの再利用と DCU IP プリフェッチャは有効になり、他のすべてのプリフェッチャは無効になります。 • [hpc]：プリフェッチャはすべて有効になり、データの再利用は無効になります。 この設定はハイ パフォーマンス コンピューティングとも呼ばれます。

[名前（Name）]	説明
[最大 MTRR 変数の設定（Max Variable MTRR Setting）] **set max-variable-mtrr-setting-config processor-mtrr**	平均修復時間（MTRR）変数の数を選択できます。次のいずれかになります。 • [自動最大（auto-max）]：BIOS はプロセッサのデフォルト値を使用します。 • [8]：BIOS は MTRR 変数に指定された数を使用します。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[ローカル X2 APIC（Local X2 APIC）] **set local-x2-apic-config**	Application Policy Infrastructure Controller（APIC）アーキテクチャ タイプを設定できます。次のいずれかになります。 • [xapic]：標準の xAPIC アーキテクチャを使用します。 • [x2apic]：拡張 x2APIC アーキテクチャを使用してプロセッサの 32 ビット アドレス指定能力をサポートします。 • [自動（auto）]：検出された xAPIC アーキテクチャを自動的に使用します。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

[名前（Name）]	説明
[電源技術（Power Technology）] **set processor-energy-config cpu-power-management**	次のオプションの CPU 電源管理設定を指定できます。 • Enhanced Intel Speedstep Technology • Intel Turbo Boost Technology • Processor Power State C6 [Power Technology] は次のいずれかになります。 • [無効（Disabled）]：サーバで CPU 電源管理は実行されず、前述の BIOS パラメータの設定が無視されます。 • [Energy_Efficient]：前述の BIOS パラメータに最適な設定が決定され、これらのパラメータの個々の設定は無視されます。 • [パフォーマンス（Performance）]：サーバは前述の BIOS パラメータのパフォーマンスを自動的に最適化します。 • [カスタム（Custom）]：前述の BIOS パラメータの個々の設定が使用されます。これらの BIOS パラメータのいずれかを変更する場合は、このオプションを選択する必要があります。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

[名前（Name）]	説明
[エネルギー パフォーマンス（Energy Performance）] **set processor-energy-config energy-performance**	システム パフォーマンスまたはエネルギー効率がこのサーバで重要かどうかを判断できます。次のいずれかになります。 • パフォーマンス • balanced-performance • balanced-energy • energy-efficient • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。 （注） [CPUPowerManagement] を [カスタム（Custom）]に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。
[周波数フロア オーバーライド（Frequency Floor Override）] **set frequency-floor-override-config cpu-frequency**	アイドル時に、CPUがターボを除く最大周波数よりも低い周波数にできるようにするかどうか。次のいずれかになります。 • [無効（Disabled）]：アイドル中に CPU をターボを除く最大周波数よりも低くできます。このオプションでは電力消費が低下しますが、システムパフォーマンスが低下する可能性があります。 • [有効（Enabled）]：アイドル中に CPU をターボを除く最大周波数よりも低くできません。このオプションではシステム パフォーマンスが向上しますが、消費電力が増加することがあります。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

[名前（Name）]	説明
[P-STATE 調整（P-STATE Coordination）] **set p-state-coordination-config p-state**	BIOS がオペレーティング システムに P-state サポート モデルを通信する方法を定義できます。Advanced Configuration and Power Interface（ACPI）仕様で定義される 3 つのモデルがあります。 • [HW_ALL]：プロセッサ ハードウェアが、依存性のある論理プロセッサ（パッケージ内のすべての論理プロセッサ）間の P-state を調整します。 • [SW_ALL]：OS Power Manager（OSPM）が、依存性のある論理プロセッサ（物理パッケージ内のすべての論理プロセッサ）間の P-state を調整します。すべての論理プロセッサで遷移を開始する必要があります。 • [SW_ANY]：OS Power Manager（OSPM）が、依存性のある論理プロセッサ（パッケージ内のすべての論理プロセッサ）間の P-state を調整します。ドメイン内の任意の論理プロセッサで遷移を開始する場合があります。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。 （注） [CPUPowerManagement] を [カスタム（Custom）] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。

[名前（Name）]	説明
[DRAM クロック スロットリング（DRAM Clock Throttling）] **set dram-clock-throttling-config dram-clock-throttling**	メモリ帯域幅と消費電力に関してシステム設定を調整できます。次のいずれかになります。 • [バランス（Balanced）]：DRAM クロック スロットリングを低下させ、パフォーマンスと電力のバランスをとります。 • [パフォーマンス（Performance）]：DRAM クロック スロットリングは無効です。追加の電力をかけてメモリ帯域幅を増やします。 • [Energy_Efficient]：DRAM のクロック スロットリングを上げてエネルギー効率を向上させます。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[チャネル インターリーブ（Channel Interleaving）] **set interleave-config channel-interleave**	CPUがメモリ ブロックを分割して、データの隣接部分をインターリーブされたチャネル間に分散し、同時読み取り動作を有効にするかどうか。次のいずれかになります。 • [自動（Auto）]：実行するインターリーブを、CPU が決定します。 • [1-way]：何らかのチャネル インターリーブが使用されます。 • [2-way] • [3-way] • [4-way]：最大量のチャネル インターリーブが使用されます。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

[名前（Name）]	説明
[ランク インターリーブ（Rank Interleaving）] **set interleave-config rank-interleave**	1 つのランクを更新中に別のランクにアクセスできるよう、CPUがメモリの物理ランクをインターリーブするかどうか。次のいずれかになります。 • [自動（Auto）]：実行するインターリーブを、CPUが決定します。 • [1-way]：何らかのランク インターリーブが使用されます。 • [2-way] • [4-way] • [8-way]：最大量のランク インターリーブが使用されます。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[デマンド スクラブ（Demand Scrub）] **set set scrub-policies config demand-scrub**	CPU または I/O が読み取りを要求した場合に検出された 1 ビットのメモリ エラーを、システムが修正するかどうか。次のいずれかになります。 • [無効（Disabled）]：1 ビット メモリ エラーは修正されません。 • [有効（Enabled）]：1 ビット メモリ エラーがメモリ内部で修正され、修正されたデータが、読み取り要求に対する応答に設定されます。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

[名前（Name）]	説明
[パトロール スクラブ（Patrol Scrub）] **set scrub-policies config patrol-scrub**	システムがサーバ上のメモリの未使用部分でも単一ビット メモリ エラーをアクティブに探して訂正するかどうか。次のいずれかになります。 • [無効（Disabled）]：CPU がメモリ アドレスの読み取りまたは書き込みを行うときのみ、システムはメモリの ECC エラーをチェックします。 • [有効（Enabled）]：システムは定期的にメモリを読み書きして ECC エラーを探します。エラーが見つかると、システムは修正を試みます。このオプションにより、単一ビット エラーは複数ビット エラーになる前に修正される場合がありますが、パトロール スクラブの実行時にパフォーマンスが低下する場合もあります。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[高度（Altitude）] **set altitude altitude-config**	物理サーバが設置されているおおよその海抜（m）。次のいずれかになります。 • [自動（Auto）]：物理的な高度を CPU によって判別します。 • [300_M]：サーバは、海抜約 300 m です。 • [900_M]：サーバは、海抜約 900 m です。 • [1500_M]：サーバは、海抜約 1500 m です。 • [3000_M]：サーバは海抜約 3000 メートルの位置にあります。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

[名前（Name）]	説明
[パッケージの C ステートの制限（Package C State Limit）] ドロップダウンリスト **set package-c-state-limit-config package-c-state-limit**	

[名前（Name）]	説明
	アイドル時にサーバ コンポーネントが使用できる電力量。次のいずれかになります。 • [no-limit]：サーバは、使用可能な任意の C ステートに入ることがあります。 • [c0]：サーバはすべてのサーバ コンポーネントに常にフルパワーを提供します。このオプションでは、最高レベルのパフォーマンスが維持され、最大量の電力が必要となります。 • [C1]：CPU のアイドル時に、システムは電力消費を少し減らします。このオプションでは、必要な電力が C0 よりも少なく、サーバはすばやくハイ パフォーマンス モードに戻ることができます。 • [C3]：CPU のアイドル時に、システムは C1 オプションの場合よりもさらに電力消費を減らします。この場合、必要な電力は C1 または C0 よりも少なくなりますが、サーバがハイ パフォーマンス モードに戻るのに要する時間が少し長くなります。 • [C6]：CPU のアイドル時に、システムは C3 オプションの場合よりもさらに電力消費を減らします。このオプションを使用すると、C0、C1、または C3 よりも電力量が節約されますが、サーバがフルパワーに戻るまでにパフォーマンス上の問題が発生する可能性があります。 • [C3]：CPU のアイドル時に、システムは C1 オプションの場合よりもさらに電力消費を減らします。この場合、必要な電力は C1 または C0 よりも少なくなりますが、サーバがハイ パフォーマンス モードに戻るのに要する時間が少し長くなります。 • [C7]：CPU のアイドル時に、サーバはコンポーネントが使用できる電力量を最小にします。このオプションでは、節約される電力量が最大になりますが、サーバがハイ パフォーマンス モードに戻るのに要する時間も最も長くなります。 • [C7s]：CPU のアイドル時に、サーバはコンポーネントが使用できる電力量を最小にします。このオプションでは、C7 よりも多い電力を節約できますが、サーバがハイ パフォーマンス モードに戻るのに要する時間も最も長くなります。 • [プラットフォームのデフォルト（Platform

[名前（Name）]	説明
	Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
CPU Hardware Power Management **set cpu-hardware-power-management-config cpu-hardware-power-management**	プロセッサの Hardware Power Management（HWPM）を有効にします。次のいずれかになります。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。 • [disabled]：HWPM が無効になります。 • [hwpm-native-mode]：HWPM ネイティブ モードが有効になります。 • [hwpm-oob-mode]：HWPM アウトオブボックス モードが有効になります。

Intel Directed I/O BIOS 設定

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

名前	説明
[ダイレクト IO 向け VT（VT for Directed IO）] **set intel-vt-directed-io-config vtd**	Intel Virtualization Technology for Directed I/O（VT-d）をプロセッサで使用するかどうか。次のいずれかになります。 • [無効（Disabled）]：プロセッサで仮想化テクノロジーを使用しません。 • [有効（Enabled）]：プロセッサで仮想化テクノロジーを使用します。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。 （注） 他の Intel Directed I/O BIOS 設定を変更する場合は、このオプションを有効にする必要があります。

名前	説明
[Interrupt Remap] **set intel-vt-directed-io-config interrupt-remapping**	プロセッサで Intel VT-d Interrupt Remapping をサポートするかどうか。次のいずれかになります。 • [無効（Disabled）]：プロセッサでリマッピングをサポートしません。 • [有効（Enabled）]：プロセッサで VT-d Interrupt Remapping を必要に応じて使用します。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[Coherency Support] **set intel-vt-directed-io-config coherency-support**	プロセッサで Intel VT-d Coherency をサポートするかどうか。次のいずれかになります。 • [無効（Disabled）]：プロセッサでコヒーレンシをサポートしません。 • [有効（Enabled）]：プロセッサで VT-d Coherency を必要に応じて使用します。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[ATS Support] **set intel-vt-directed-io-config ats-support**	プロセッサで Intel VT-d Address Translation Services（ATS）をサポートするかどうか。次のいずれかになります。 • [無効（Disabled）]：プロセッサで ATS をサポートしません。 • [有効（Enabled）]：プロセッサで VT-d ATS を必要に応じて使用します。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[パススルー DMA サポート（Pass Through DMA Support）] **set intel-vt-directed-io-config passthrough-dma**	プロセッサで Intel VT-d Pass-through DMA をサポートするかどうか。次のいずれかになります。 • [無効（Disabled）]：プロセッサでパススルー DMA をサポートしません。 • [有効（Enabled）]：プロセッサで VT-d Pass-through DMA を必要に応じて使用します。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

RAS メモリの BIOS 設定

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

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

名前	説明
[NUMA] **set numa-config numa-optimization**	BIOS で NUMA をサポートするかどうか。次のいずれかになります。 • [無効（Disabled）]：BIOS で NUMA をサポートしません。 • [有効（Enabled）]：NUMA に対応したオペレーティング システムに必要な ACPI テーブルを BIOS に含めます。このオプションを有効にした場合は、一部のプラットフォームでシステムのソケット間メモリ インターリーブを無効にする必要があります。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[ミラーリング モード（Mirroring Mode）] **set memory-mirroring-mode mirroring-mode**	メモリ ミラーリングは、メモリに 2 個の同じデータ イメージを保存することにより、システムの信頼性を向上します。 このオプションは、[メモリ RAS 設定（Memory RAS Config）] で [ミラーリング（mirroring）] オプションを選択したときのみ使用可能です。次のいずれかを設定できます。 • [ソケット間（inter-socket）]：メモリは、CPU ソケットをまたいで 2 台の Integrated Memory Controller（IMC）間でミラーリングされます。 • [ソケット内（intra-socket）]：1 台の IMC が同じソケットの別の IMC とミラーリングされます。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[スペアリング モード（Sparing Mode）] **set memory-sparing-mode sparing-mode**	スペアリングはメモリを予備に保持することで信頼性を最適化し、別のDIMMの障害発生時に使用できるようにします。このオプションは、メモリの冗長性を実現しますが、ミラーリングほどの冗長性は提供されません。使用可能なスペアリングのモードは、現在のメモリの数によって異なります。 このオプションは、[メモリ RAS 設定（Memory RAS Config）]で[スペアリング（sparing）]オプションを選択したときのみ使用可能です。次のいずれかを設定できます。 • [dimm スペアリング（dimm-sparing）]：1 枚の DIMM が予備に保持されます。DIMM に障害が発生すると、その DIMM の内容はスペア DIMM に移されます。 • [ランク スペアリング（rank-sparing）]：DIMM のスペア ランクが予備に保持されます。あるランクの DIMMに障害が発生した場合、そのランクの内容がスペア ランクに移されます。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[LV DDR モード（LV DDR Mode）] **set lv-dimm-support-config lv-ddr-mode**	低電圧と高周波数のどちらのメモリ動作をシステムで優先するか。次のいずれかになります。 • [省電力モード（power-saving-mode）]：低電圧のメモリ動作が高周波数のメモリ動作よりも優先されます。 このモードでは、電圧を低く維持するために、メモリの周波数が低下する可能性があります。 • [パフォーマンス モード（performance-mode）]：高周波数の動作が低電圧の動作よりも優先されます。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[DRAM リフレッシュ レート（DRAM Refresh Rate）]	内部メモリ用の更新間隔レート。次のいずれかになります。 • 1x • 2x • 3x • 4x • auto • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[DDR3 電圧選択（DDR3 Voltage Selection）] **set Ddr3VoltageSelection**	デュアル電圧 RAM に使用される電圧。次のいずれかになります。 • DDR3-1500mv • DDR3-1350mv • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

シリアル ポートの BIOS 設定

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

名前	説明
[シリアル ポート A（Serial Port A）] **set serial-port-a-config serial-port-a**	シリアル ポート A が有効か無効か。次のいずれかになります。 • [無効（disabled）]：シリアル ポートは無効になります。 • [有効（enabled）]：シリアル ポートが有効になります。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

USB の BIOS 設定

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

名前	説明
[デバイスをブート不能にする（Make Device Non Bootable）] **set usb-boot-config make-device-non-bootable**	サーバがUSBデバイスからブートできるかどうか。次のいずれかになります。 • [無効（disabled）]：サーバはUSBデバイスからブートできます。 • [有効（enabled）]：サーバはUSBデバイスからブートできません。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[レガシー USB サポート（Legacy USB Support）] **set LegacyUSBSupport**	システムでレガシーUSBデバイスをサポートするかどうか。次のいずれかになります。 • [無効（disabled）]：USB デバイスは、EFI アプリケーションでのみ使用できます。 • [有効（enabled）]：レガシーUSBのサポートは常に使用できます。 • [自動（auto）]：USB デバイスが接続されていない場合、レガシー USB のサポートを無効にします。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[システム アイドル時の USB 電力最適化設定（USB System Idle Power Optimizing Setting）] **set usb-system-idle-power-optimizing-setting-config usb-idle-power-optimizing**	USB EHCI のアイドル時電力消費を減らすために USB システムにアイドル時電力最適化設定を使用するかどうか。この設定で選択した値によって、パフォーマンスが影響を受けることがあります。次のいずれかになります。 • [高パフォーマンス（high-performance）]：最適なパフォーマンスを電力節約より優先するため、USB システムのアイドル時電力最適化設定は無効化されます。 このオプションを選択すると、パフォーマンスが大幅に向上します。サイトにサーバの電源制限がない場合はこのオプションを選択することを推奨します。 • [アイドル時低消費電力（lower-idle-power）]：電力節約を最適なパフォーマンスより優先するため、USB システムのアイドル時電力最適化設定は有効化されます。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[フロントパネルのUSBアクセスロック（USB Front Panel Access Lock）] **set usb-front-panel-access-lock-config usb-front-panel-lock**	USB 前面パネル ロックは、USB ポートへの前面パネル アクセスを有効または無効にするために設定されます。次のいずれかになります。 • 無効 • 有効（enabled） • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[Port 60/64 エミュレーション（Port 60/64 Emulation）] **set UsbEmul6064**	完全な USB キーボード レガシー サポートのために 60h/64h エミュレーションをシステムでサポートするかどうか。次のいずれかになります。 • [無効（Disabled）]：60h/64 エミュレーションはサポートされません。 • [有効（Enabled）]：60h/64 エミュレーションはサポートされます。 サーバで USB 非対応オペレーティング システムを使用する場合は、このオプションを選択する必要があります。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[USB ポート：前面（USB Port:Front）] **set UsbPortFront**	前面パネルの USB デバイスが有効か無効か。次のいずれかになります。 • [無効（Disabled）]：前面パネルの USB ポートを無効にします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されません。 • [有効（Enabled）]：前面パネルの USB ポートを有効にします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されます。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[USB ポート：内部（USB Port:Internal）] **set UsbPortInt**	内部 USB デバイスが有効か無効か。次のいずれかになります。 • [無効（Disabled）]：内部 USB ポートを無効にします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されません。 • [有効（Enabled）]：内部 USB ポートを有効にします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されます。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[USB ポート：KVM（USB Port:KVM）] **set UsbPortKVM**	KVM ポートが有効か無効か。次のいずれかになります。 • [無効（Disabled）]：KVM キーボードおよびマウス デバイスを無効にします。キーボードとマウスは KVM ウィンドウで機能しなくなります。 • [有効（Enabled）]：KVM キーボードおよびマウス デバイスを有効にします。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[USB ポート：背面（USB Port:Rear）] **set UsbPortRear**	背面パネルの USB デバイスが有効か無効か。次のいずれかになります。 • [無効（Disabled）]：背面パネルの USB ポートを無効にします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されません。 • [有効（Enabled）]：背面パネルの USB ポートを有効にします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されます。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[USB ポート：SD カード（USB Port:SD Card）] **set UsbPortSdCard**	SD カード ドライブが有効か無効か。次のいずれかになります。 • [無効（Disabled）]：SD カード ドライブを無効にします。SD カード ドライブは、BIOS およびオペレーティング システムによって検出されません。 • [有効（Enabled）]：SD カード ドライブを有効にします。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[USB ポート：VMedia（USB Port:VMedia）] **set UsbPortVMedia**	仮想メディアデバイスが有効か無効か。次のいずれかになります。 • [無効（Disabled）]：vMedia デバイスを無効にします。 • [有効（Enabled）]：vMedia デバイスを有効にします。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[すべての USB デバイス（All USB Devices）] **set AllUsbDevices**	すべての物理および仮想USBデバイスが有効であるか、無効であるか。次のいずれかになります。 • [無効（Disabled）]：すべての USB デバイスが無効になります。 • [有効（Enabled）]：すべての USB デバイスが有効です。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

PCI 設定の BIOS 設定

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

名前	説明
[4GB 以下でメモリの最大化（Max Memory Below 4G）] **set max-memory-below-4gb-config max-memory**	PAE サポートなしで動作しているオペレーティング システムのメモリ使用率を、BIOS がシステム設定に応じて 4GB 以下で最大化するかどうか。次のいずれかになります。 • [無効（Disabled）]：メモリ使用率を最大化しません。 PAE をサポートするオペレーティング システムすべてにこのオプションを選択します。 • [有効（Enabled）]：PAE をサポートしないオペレーティング システムについて 4GB 以下でメモリ使用率を最大化します。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[4 GB を超えるメモリ マップド IO 構成（Memory Mapped IO Above 4Gb Config）] **set memory-mapped-io-above-4gb-config memory-mapped-io**	64 ビット PCI デバイスの 4 GB 以上のアドレス空間に対するメモリ マップド I/O を有効にするか、無効にするか。レガシーなオプション ROM は 4 GB を超えるアドレスにアクセスできません。PCI デバイスが 64 ビット対応でも、レガシーなオプション ROM を使用する場合は、この設定を有効にしても正しく機能しない場合があります。次のいずれかになります。 • [無効（Disabled）]：64 ビット PCI デバイスを 4 GB 以上のアドレス空間にマッピングしません。 • [有効（Enabled）]：64 ビット PCI デバイスを 4 GB 以上のアドレス空間にマッピングします。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[VGA Priority] **set VGAPriority**	システムに複数の VGA デバイスがある場合は、VGA グラフィックス デバイスのプライオリティを設定できます。次のいずれかになります。 • [オンボード（Onboard）] : プライオリティがオンボード VGA デバイスに与えられます。BIOS ポスト画面および OS ブートはオンボード VGA ポート経由で駆動されます。 • [オフボード（Offboard）] : プライオリティが PCIE グラフィックス アダプタに与えられます。BIOS ポスト画面および OS ブートは外部グラフィックス アダプタ ポート経由で駆動されます。 • [オンボード VGA を無効（onboard-vga-disabled）] : PCIE グラフィックス アダプタにプライオリティが与えられ、オンボード VGA デバイスは無効になります。 （注） オンボード VGA が無効の場合、vKVM は機能しません。 • [プラットフォームのデフォルト（Platform Default）][platform-default] : BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。 （注） Cisco UCS B シリーズ サーバでは、オンボード VGA デバイスのみがサポートされます。
[ASPM サポート（ASPM Support）] **set ASPMSupport**	BIOS での ASPM（アクティブ電源状態管理）サポートのレベルを設定できます。次のいずれかになります。 • [無効（Disabled）] : ASPM サポートは、BIOS で無効です。 • [自動（auto）] : 電力状態を CPU によって判別します。 • [l0 の強制（force l0）] : すべてのリンクを強制的に L0 スタンバイ（L0s）状態にします。 • [プラットフォームのデフォルト（Platform Default）][platform-default] : BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

QPI の BIOS 設定

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

名前	説明
[QPI リンク周波数（QPI Link Frequency）] **set qpi-link-frequency-select-config qpi-link-freqency-mt-per-sec**	メガトランスファー/秒（MT/s）単位での Intel QuickPath Interconnect（QPI）リンク周波数。次のいずれかになります。 • 6400 • 7200 • 8000 • [自動（Auto）]：QPI リンク周波数は CPU によって決定されます。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[QPI スヌープ モード（QPI Snoop Mode）] **set vfqpisnoopmode vpqpisnoopmode**	次のいずれかになります。 • [home-snoop]：スヌープは、常に、メモリ コントローラのホーム エージェント（集中型リング停止）によって起動されます。このモードは、早期スヌープよりローカル遅延が多いですが、未処理トランザクションが増えた場合に予備のリソースを使用できます。 • [cluster-on-die]：このモードは、コアが 10 以上のプロセッサでのみ使用できます。高度に NUMA 最適化されたワークロードに最適なモードです。 • [early-snoop]：分散キャッシュ リング停止で、別のキャッシング エージェントにスヌープ プローブまたは要求を直接送信できます。このモードは、遅延が少なく、スレッド全体でデータセットを共有しているためにキャッシュ間転送からメリットが得られるワークロードや NUMA 最適化されていないワークロードに最適です。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

LOM および PCIe スロットの BIOS 設定

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

名前	説明
[PCIe スロット：SAS OptionROM（PCIe Slot:SAS OptionROM）] **set slot-option-rom-enable-config pcie-sas**	オプション ROM が SAS ポートで使用できるかどうか。次のいずれかになります。 • [無効（Disabled）]：拡張スロットを使用できません。 • [有効（Enabled）]：拡張スロットを使用できます。 • [UEFI のみ（UEFI-Only）][UEFI のみ（UEFI_Only）]：UEFIでのみ拡張スロットを使用できます。 • [レガシーのみ（Legacy-Only）][レガシーのみ（Legacy_Only）]：レガシーでのみ拡張スロットを使用できます。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[PCIe スロット：n リンク速度（PCIe Slot:*n* Link Speed）] **set slot-link-speed config pcie-slot*n*-link-speed**	このオプションを使用すると、PCIe スロット *n* に装着されているアダプタ カードの最大速度を制限できます。次のいずれかになります。 • [gen1]：最大 2.5GT/s（ギガトランスファー/秒）までの速度が許可されます。 • [gen2]：最大 5GT/s までの速度が許可されます。 • [gen3]：最大 8GT/s までの速度が許可されます。 • [auto]：最高速度は自動的に設定されます。 • [disabled]：最大速度は制限されません。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[PCIe スロット：n OptionROM（PCIe Slot:*n* OptionROM）] **set slot-option-rom-enable-configslot*n*-option-rom-enable**	オプション ROM がポートで使用できるかどうか。次のいずれかになります。 • [無効（Disabled）]：スロットは使用できません。 • [有効（Enabled）]：スロットは使用できます。 • [UEFIのみ（UEFI-Only）][UEFI のみ（UEFI_Only）]：スロットは UEFI にのみ使用できます。 • [レガシーのみ（Legacy-Only）][レガシーのみ（Legacy_Only）]：スロットはレガシーにのみ使用できます。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[PCIe スロット：HBA OptionROM（PCIe Slot:HBA OptionROM）] ドロップダウンリスト **set slot-option-rom-enable-config pcie-hba**	オプション ROM が HBA ポートで使用できるかどうか。次のいずれかになります。 • [無効（Disabled）]：拡張スロットを使用できません。 • [有効（Enabled）]：拡張スロットを使用できます。 • [UEFI のみ（UEFI-Only）][UEFI のみ（UEFI_Only）]：UEFIでのみ拡張スロットを使用できます。 • [レガシーのみ（Legacy-Only）][レガシーのみ（Legacy_Only）]：レガシーでのみ拡張スロットを使用できます。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[PCIe スロット：MLOM OptionROM（PCIe Slot:MLOM OptionROM）] ドロップダウンリスト **set slot-option-rom-enable-config mlom**	オプション ROM が MLOM ポートで使用できるかどうか。次のいずれかになります。 • [無効（Disabled）]：拡張スロットを使用できません。 • [有効（Enabled）]：拡張スロットを使用できます。 • [UEFI のみ（UEFI-Only）][UEFI のみ（UEFI_Only）]：UEFIでのみ拡張スロットを使用できます。 • [レガシーのみ（Legacy-Only）][レガシーのみ（Legacy_Only）]：レガシーでのみ拡張スロットを使用できます。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[PCIe スロット N1 OptionROM：（PCIe Slot:N1 OptionROM）] ドロップダウンリスト **set slot-option-rom-enable-config n1**	オプション ROM がポートで使用できるかどうか。次のいずれかになります。 • [無効（Disabled）]：拡張スロットを使用できません。 • [有効（Enabled）]：拡張スロットを使用できます。 • [UEFI のみ（UEFI-Only）][UEFI のみ（UEFI_Only）]：UEFIでのみ拡張スロットを使用できます。 • [レガシーのみ（Legacy-Only）][レガシーのみ（Legacy_Only）]：レガシーでのみ拡張スロットを使用できます。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[PCIe スロット N2 OptionROM：（PCIe Slot:N2 OptionROM）] ドロップダウンリスト **set slot-option-rom-enable-config n2**	オプション ROM がポートで使用できるかどうか。次のいずれかになります。 • [無効（Disabled）]：拡張スロットを使用できません。 • [有効（Enabled）]：拡張スロットを使用できます。 • [UEFI のみ（UEFI-Only）][UEFI のみ（UEFI_Only）]：UEFIでのみ拡張スロットを使用できます。 • [レガシーのみ（Legacy-Only）][レガシーのみ（Legacy_Only）]：レガシーでのみ拡張スロットを使用できます。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[PCIe OptionROM（PCIe OptionROMs）] ドロップダウンリスト **set option-rom-enable-config option-rom-enable**	オプション ROM がすべての拡張ポートで使用できるかどうか。次のいずれかになります。 • [無効（Disabled）]：拡張スロットは使用できません。 • [有効（Enabled）]：拡張スロットを使用できます。 • [UEFI_Only]：UEFI でのみ拡張スロットを使用できます。 • [レガシーのみ（Legacy-Only）][レガシーのみ（Legacy_Only）]：レガシーでのみ拡張スロットを使用できます。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[PCIe Mezz OptionRom] **set slot-option-rom-enable-config mezz-slot-option-rom-enable**	すべてのメザニン PCIe ポートを有効にするか、または無効にするか。次のいずれかになります。 • [無効（Disabled）]：すべての LOM ポートが無効になります。 • [有効（Enabled）]：すべての LOM ポートが有効です。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[すべての PCI オンボード LOM ポート（All PCI Onboard LOM Ports）] **set lom-ports-config all-lom-ports**	すべてのLOMポートが有効であるか、無効であるか。次のいずれかになります。 • [無効（Disabled）]：すべての LOM ポートが無効になります。 • [有効（Enabled）]：すべての LOM ポートが有効です。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[PCIe 1G LOM 1 リンク（PCIe 1G LOM 1 Link）] **set pcie-lom1-link**	オプション ROM が 1G LOM ポートで使用できるかどうか。次のいずれかになります。 • [無効（Disabled）]：拡張スロットを使用できません。 • [有効（Enabled）]：拡張スロットを使用できます。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[PCIe 10G LOM 2 リンク（PCIe 10G LOM 2 Link）] **set pcie-lom2-link**	オプション ROM を 10G LOM ポートで使用できるかどうか。次のいずれかになります。 • [無効（Disabled）]：拡張スロットを使用できません。 • [有効（Enabled）]：拡張スロットを使用できます。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

グラフィックス構成の BIOS 設定

次の表は、BIOS ポリシーまたはデフォルトの BIOS 設定を介して実行できるグラフィックス構成の BIOS 設定を示しています。

名前	説明
統合グラフィックス（Integrated Graphics） **set integrated-graphics-config integrated-graphics**	統合グラフィックスを有効にします。次のいずれかになります。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。 • [enabled]：統合グラフィックスが有効になります。 • [disabled]：統合グラフィックスが無効になります。
開口サイズ（Aperture Size） **set integrated-graphics-aperture-config integrated-graphics-aperture**	統合グラフィックス コントローラのマッピング メモリのサイズを設定できます。次のいずれかになります。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。 • 128mb • 256mb • 512mb • 1024mb • 2048mb • 4096mb
オンボード グラフィックス（Onboard Graphics） **set onboard-graphics-config onboard-graphics**	オンボード グラフィックス（KVM）を有効にします。次のいずれかになります。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。 • [enabled]：オンボード グラフィックスが有効になります。 • [disabled]：オンボード グラフィックスが無効になります。

ブート オプションの BIOS 設定

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

名前	説明
[ブート オプションの再試行（Boot Option Retry）] **set boot-option-retry-config retry**	BIOS でユーザ入力を待機せずに非 EFI ベースのブート オプションを再試行するかどうか。次のいずれかになります。 • [無効（Disabled）]：ユーザ入力を待機してから非 EFI ベースのブート オプションを再試行します。 • [有効（Enabled）]：ユーザ入力を待機せずに非 EFI ベースのブート オプションを継続的に再試行します。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[Intel Entry SAS RAID] **set intel-entry-sas-raid-config sas-raid**	Intel SAS Entry RAID モジュールが有効かどうか。次のいずれかになります。 • [無効（Disabled）]：Intel SAS Entry RAID モジュールは無効です。 • [有効（Enabled）]：Intel SAS Entry RAID モジュールが有効になります。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[Intel Entry SAS RAID モジュール（Intel Entry SAS RAID Module）] **set intel-entry-sas-raid-config sas-raid-module**	Intel SAS Entry RAID モジュールがどのように設定されるか。次のいずれかになります。 • [it-ir-raid]：Intel IT/IR RAID を使用するよう RAID モジュールを設定します。 • [intel-esrtii]：Intel Embedded Server RAID Technology II を使用するよう RAID モジュールを設定します。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[オンボード SCU ストレージ サポート（Onboard SCU Storage Support）] **set onboard-sas-storage-config onboard-sas-ctrl**	オンボード ソフトウェア RAID コントローラをサーバで使用できるかどうか。次のいずれかになります。 • [無効（Disabled）]：ソフトウェア RAID コントローラを使用できません。 • [有効（Enabled）]：ソフトウェア RAID コントローラを使用できます。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

サーバ管理 BIOS 設定

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

全般設定

[名前（Name）]	説明
[SERR 時の NMI の挿入（Assert Nmi on Serr）] **set assert-nmi-on-serr-config assertion**	システムエラー（SERR）の発生時に、BIOS がマスク不能割り込み（NMI）を生成し、エラーをログに記録するかどうか。次のいずれかになります。 • [無効（disabled）]：SERR の発生時に、BIOS は NMI を生成することもエラーをログに記録することもしません。 • [有効（enabled）]：BIOS は PERR が発生すると NMI を生成し、エラーを記録します。[PERR 時の NMI の挿入（Assert Nmi on Perr）] を有効にするには、この設定を有効にする必要があります。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[PERR 時の NMI の挿入（Assert Nmi on Perr）] **set assert-nmi-on-perr-config assertion**	プロセッサ バス パリティ エラー（PERR）の発生時に、BIOS がマスク不能割り込み（NMI）を生成し、エラーをログに記録するかどうか。次のいずれかになります。 • [無効（disabled）]：PERR の発生時に、BIOS は NMI を生成することもエラーをログに記録することもしません。 • [有効（enabled）]：BIOS は PERR が発生すると NMI を生成し、エラーを記録します。この設定を使用するには、[SERR 時の NMI の挿入（Assert Nmi on Serr）] を有効にする必要があります。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

[名前（Name）]	説明
[OS ブート ウォッチドッグ タイマー（OS Boot Watchdog Timer）] **set os-boot-watchdog-timer-config os-boot-watchdog-timer**	BIOS が定義済みのタイム アウト値を持つウォッチドッグ タイマーをプログラムするかどうか。タイマーが切れる前にオペレーティング システムのブートを完了しない場合、CIMC はシステムをリセットし、エラーがログに記録されます。次のいずれかになります。 • [無効（disabled）]：サーバのブートにかかる時間をトラッキングするためにウォッチドッグ タイマーは使用されません。 • [有効（enabled）]：サーバ ブートにかかる時間をウォッチドッグ タイマーで追跡します。サーバが事前に定義した時間内にブートしない場合、CIMC はシステムをリセットし、エラーを記録します。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。 この機能には、オペレーティング システムのサポートまたは Intel 管理ソフトウェアが必要です。
[OS ブート ウォッチドッグ タイマー タイムアウト ポリシー（OS Boot Watchdog Timer Timeout Policy）] **set os-boot-watchdog-timer-policy-config os-boot-watchdog-timer-policy**	ウォッチドッグ タイマーが切れた場合にシステムで実行されるアクション。次のいずれかになります。 • [電源オフ（power-off）]：OS ブート中にウォッチドッグ タイマーが期限切れになった場合、サーバは電源オフになります。 • [リセット（reset）]：OS のブート中にウォッチドッグ タイマーが切れた場合、サーバはリセットされます。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。 このオプションは、[OS ブート ウォッチドッグ タイマー（OS Boot Watchdog Timer）] を有効にした場合にだけ利用できます。

[名前（Name）]	説明
[OS ブート ウォッチドッグ タイマー タイムアウト（OS Boot Watchdog Timer Timeout）] ドロップダウンリスト **set os-boot-watchdog-timer-timeout-config os-boot-watchdog-timer-timeout**	BIOS でウォッチドッグ タイマーの設定に使用されるタイムアウト値。次のいずれかになります。 • [5 分（5-minutes）]：ウォッチドッグ タイマーは OS ブート開始から 5 分後に期限切れになります。 • [10 分（10-minutes）]：ウォッチドッグ タイマーは OS ブート開始から 10 分後に期限切れになります。 • [15 分（15-minutes）]：ウォッチドッグ タイマーは OS ブート開始から 15 分後に期限切れになります。 • [20 分（20-minutes）]：ウォッチドッグ タイマーは OS ブート開始から 20 分後に期限切れになります。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。 このオプションは、[OS ブート ウォッチドッグ タイマー（OS Boot Watchdog Timer）] を有効にした場合にだけ利用できます。
[FRB-2 タイマー（FRB-2 Timer）] **set FRB-2**	POST 中にシステムがハングした場合に、システムを回復するために FRB-2 タイマーが使用されるかどうか。次のいずれかになります。 • [無効（disabled）]：FRB-2 タイマーは使用されません。 • [有効（Enabled）]：POST 中に FRB-2 タイマーが開始され、必要に応じてシステムの回復に使用されます。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

コンソール リダイレクション設定

[名前（Name）]	説明
[コンソール リダイレクション（Console Redirection）] **set console-redir-config console-redir**	POST および BIOS のブート中に、シリアル ポートをコンソール リダイレクションに使用できるようにします。BIOS のブートが完了し、オペレーティング システムがサーバを担当すると、コンソール リダイレクションは関連がなくなり、無効になります。次のいずれかになります。 • [無効（disabled）]：POST 中にコンソール リダイレクションは発生しません。 • [シリアル ポート A（serial-port-a）]：POST 中のコンソール リダイレクションのためシリアル ポート A を有効にします。このオプションはブレードサーバおよびラックマウントサーバに対して有効です。 • [シリアル ポート B（serial-port-b）]：POST 中のコンソール リダイレクションのためシリアル ポート B を有効にし、サーバ管理タスク実行を許可します。このオプションは、ラックマウントサーバでのみ有効です。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。 （注） このオプションを有効にする場合は、POST 中に表示される Quiet Boot のロゴ画面も無効にします。

[名前（Name）]	説明
[フロー制御（Flow Control）] **set console-redir-config flow-control**	フロー制御にハンドシェイク プロトコルを使用するかどうか。送信要求/クリア ツー センド（RTS/CTS）を使用すると、隠れた端末問題が原因で発生する可能性があるフレーム コリジョンを減らすことができます。次のいずれかになります。 • [なし（none）]：フロー制御は使用されません。 • [rts-cts]：フロー制御に RTS/CTS が使用されます。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。 （注） この設定は、リモート ターミナル アプリケーション上の設定と一致している必要があります。
[ボー レート（BAUD Rate）] **set console-redir-config baud-rate**	シリアル ポートの伝送速度として使用されるボー レート。[コンソール リダイレクション（Console Redirection）]を無効にした場合は、このオプションを使用できません。次のいずれかになります。 • [9600]：9600 ボー レートが使用されます。 • [19200]：19200 ボー レートが使用されます。 • [38400]：38400 ボー レートが使用されます。 • [57600]：57600 ボー レートが使用されます。 • [115200]：115200 ボー レートが使用されます。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。 （注） この設定は、リモート ターミナル アプリケーション上の設定と一致している必要があります。

[名前（Name）]	説明
[ターミナル タイプ（Terminal Type）] ドロップダウンリスト **set console-redir-config terminal-type**	コンソール リダイレクションに使用される文字フォーマットのタイプ。次のいずれかになります。 • [pc-ansi]：PC-ANSI 端末フォントが使用されます。 • [vt100]：サポートされている vt100 ビデオ端末とその文字セットが使用されます。 • [vt100-plus]：サポートされている vt100-plus ビデオ端末とその文字セットが使用されます。 • [VT-UTF8]：UTF-8 文字セットのビデオ端末が使用されます。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。 （注） この設定は、リモート ターミナル アプリケーション上の設定と一致している必要があります。
[レガシー OS リダイレクション（Legacy OS Redirect）] **set console-redir-config legacy-os-redir**	シリアル ポートでレガシーなオペレーティング システム（DOS など）からのリダイレクションを有効にするかどうか。次のいずれかになります。 • [無効（disabled）]：コンソール リダイレクションが有効になっているシリアル ポートは、レガシーなオペレーティング システムから認識されません。 • [有効（enabled）]：コンソール リダイレクションが有効になっているシリアル ポートは、レガシーなオペレーティング システムから認識できます。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

[名前（Name）]	説明
[Putty キーパッド（Putty KeyPad）] **set PuttyFunctionKeyPad**	PuTTY ファンクション キーおよびテンキーの最上段のキーのアクションを変更できます。次のいずれかになります。 • [VT100]：ファンクション キーが ESC OP ～ ESC O[を生成します。 • [LINUX]：Linux 仮想コンソールを模倣します。ファンクション キー F6 ～ F12 はデフォルト モードと同様に動作しますが、F1 ～ F5 は ESC [[A ～ ESC [[E を生成します。 • [XTERMR6]：ファンクション キー F5 ～ F12 がデフォルト モードと同様に動作します。ファンクション キー F1 ～ F4 が ESC OP ～ ESC OS を生成します。これはデジタル端末のキーパッドの上段によって生成されるシーケンスです。 • [SCO]：ファンクション キー F1 ～ F12 が ESC [M ～ ESC [X を生成します。ファンクションおよび Shift キーが ESC [Y ～ ESC [j を生成します。Ctrl およびファンクション キーが ESC [k ～ ESC [v を生成します。Shift、Ctrl およびファンクション キーが ESC [w ～ ESC [{ を生成します。 • [ESCN]：デフォルト モードです。ファンクション キーはデジタル端末の一般的な動作と一致します。ファンクション キーが ESC [11~ や ESC [12~ などのシーケンスを生成します。 • [VT400]：ファンクション キーがデフォルト モードと同様に動作します。テンキーの最上段のキーが ESC OP ～ ESC OS を生成します。 • [プラットフォームのデフォルト（Platform Default）][platform-default]：BIOSは、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

BIOS ポリシー

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

BIOS ポリシーを使用するには、次の手順を実行します。

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

サービス プロファイルを関連付けるときに、Cisco UCS Manager は BIOS ポリシーの設定と一致するようにサーバの BIOS 設定を変更します。BIOS ポリシーを作成せず、BIOS ポリシーをサービス プロファイルに割り当てていない場合は、サーバの BIOS 設定にそのサーバ プラットフォームのデフォルトが使用されます。

デフォルトの BIOS 設定

Cisco UCS Manager には、Cisco UCS がサポートするサーバの各タイプのための 1 セットのデフォルト BIOS 設定が含まれています。デフォルトの BIOS 設定は、ルート組織でのみ使用できるグローバル設定です。Cisco UCS でサポートされている各サーバ プラットフォームには、一組のデフォルトの BIOS 設定のみを適用できます。デフォルトの BIOS 設定は変更可能ですが、追加のセットは作成できません。

デフォルト BIOS 設定の各セットは、サポートされている特定タイプのサーバ用にそれぞれ設計されており、その特定タイプに属し、サービス プロファイルに BIOS ポリシーが含まれていないサーバすべてに適用されます。

Cisco UCS 実装にサーバ特定の設定によって満たされない特定の要件がある場合を除き、Cisco UCS ドメイン 内のサーバの各タイプ用に設計されたデフォルト BIOS 設定を使用することを推奨します。

Cisco UCS Manager では、これらのサーバ プラットフォーム固有の BIOS 設定は次のように適用されます。

- サーバに関連付けられるサービス プロファイルには、BIOS ポリシーが含まれません。
- BIOS ポリシーには、特定の設定に応じたプラットフォーム デフォルトのオプションが設定されます。

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

BIOS ポリシーの作成

（注） Cisco UCS Manager は、BIOS ポリシーまたはデフォルトの BIOS 設定による BIOS 設定の変更を Cisco Integrated Management Controller（CIMC）バッファにプッシュします。これらの変更はバッファ内にとどまり、サーバがリブートされるまでは有効になりません。

設定するサーバで BIOS 設定のサポートを確認することをお勧めします。RAS メモリのミラーリング モードなどの一部の設定は、すべての Cisco UCS サーバでサポートされているわけではありません。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織で組織モードを開始します。デフォルト組織モードを開始するには、*/* を *org-name* として入力します。
ステップ 2	UCS-A /org # **create bios-policy** *policy-name*	BIOS ポリシーを指定されたポリシー名で作成し、組織 BIOS ポリシー モードを開始します。
ステップ 3	BIOS 設定を設定します。	CLI コマンドに関する各 BIOS 設定のオプションの詳細については、次のトピックを参照してください。 • [メイン（Main）] ページ： メイン BIOS 設定, （438 ページ） • [プロセッサ（Processor）] ページ： プロセッサの BIOS 設定, （440 ページ） • [Intel Directed IO] ページ： Intel Directed I/O BIOS 設定, （458 ページ） • [RAS メモリ（RAS Memory）] ページ： RAS メモリの BIOS 設定, （460 ページ） • [シリアル ポート（Serial Port）] ページ： シリアル ポートの BIOS 設定, （463 ページ） • [USB] ページ： USB の BIOS 設定, （464 ページ） • [PCI 設定（PCI Configuration）] ページ： PCI 設定の BIOS 設定, （469 ページ） • [ブート オプション（Boot Options）] ページ： ブート オプションの BIOS 設定, （480 ページ）

	コマンドまたはアクション	目的
		• [サーバ管理（Server Management）] ページ： サーバ管理 BIOS 設定, （481 ページ）
ステップ 4	UCS-A /org/bios-policy # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、ルート組織下で BIOS ポリシーを作成し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # create bios-policy biosPolicy3
UCS-A /org/bios-policy* # set numa-config numa-optimization enabled
UCS-A /org/bios-policy* # commit-buffer
UCS-A /org/bios-policy #
```

BIOS デフォルトの変更

設定するサーバで BIOS 設定のサポートを確認することをお勧めします。RAS メモリのミラーリング モードなどの一部の設定は、すべての Cisco UCS サーバでサポートされているわけではありません。

Cisco UCS 実装にサーバ特定の設定によって満たされない特定の要件がある場合を除き、Cisco UCS ドメイン 内のサーバの各タイプ用に設計されたデフォルト BIOS 設定を使用することを推奨します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope server-defaults**	サーバ デフォルト モードを開始します。
ステップ 3	UCS-A /system/server-defaults # **show platform**	（任意）すべてのサーバのプラットフォームの説明を表示します。
ステップ 4	UCS-A /system/server-defaults # **scope platform** *platform-description*	指定したサーバでサーバ デフォルト モードを開始します。*platform-description* 引数に、次のフォーマットを使用して **show platform** コマンドによって表示されるサーバの説明を入力します："*vendor*" *model revision*。

	コマンドまたはアクション	目的
		ヒント　ベンダーは、すべての句読点を含む **show platform** コマンドで表示されるとおり正確に入力する必要があります。
ステップ 5	UCS-A /system/server-defaults/platform # **scope bios-settings**	サーバでサーバ デフォルト BIOS 設定モードを開始します。
ステップ 6	BIOS 設定を再設定します。	CLI コマンドに関する各 BIOS 設定のオプションの詳細については、次のトピックを参照してください。 • [メイン（Main）] ページ： メイン BIOS 設定, （438 ページ） • [プロセッサ（Processor）] ページ： プロセッサの BIOS 設定, （440 ページ） • [Intel Directed IO] ページ： Intel Directed I/O BIOS 設定, （458 ページ） • [RAS メモリ（RAS Memory）] ページ： RAS メモリの BIOS 設定, （460 ページ） • [シリアル ポート（Serial Port）] ページ： シリアル ポートの BIOS 設定, （463 ページ） • [USB] ページ： USB の BIOS 設定, （464 ページ） • [PCI 設定（PCI Configuration）] ページ： PCI 設定の BIOS 設定, （469 ページ） • [ブート オプション（Boot Options）] ページ： ブート オプションの BIOS 設定, （480 ページ） • [サーバ管理（Server Management）] ページ： サーバ管理 BIOS 設定, （481 ページ）
ステップ 7	UCS-A /system/server-defaults/platform/bios-settings # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、プラットフォームの NUMA デフォルト BIOS 設定を変更し、トランザクションをコミットする例を示します。

```
UCS-A# scope system
UCS-A /system # scope server-defaults
UCS-A /system/server-defaults # show platform

Platform:
    Product Name Vendor     Model      Revision
    ------------ ---------- ---------- --------
    Cisco B200-M1
                 Cisco Systems, Inc.
                            N20-B6620-1
                                       0

UCS-A /system/server-defaults # scope platform "Cisco Systems, Inc." N20-B6620-1 0
UCS-A /system/server-defaults/platform # scope bios-settings
UCS-A /system/server-defaults/platform/bios-settings # set numa-config numa-optimization
disabled
UCS-A /system/server-defaults/platform/bios-settings* # commit-buffer
UCS-A /system/server-defaults/platform/bios-settings #
```

サーバの実際の BIOS 設定の表示

サーバの実際の BIOS 設定を表示するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *chassis-id/ server-id*	指定サーバのシャーシ サーバ モードを開始します。
ステップ 2	UCS-A /chassis/server # **scope bios**	指定したサーバで BIOS モードを開始します。
ステップ 3	UCS-A /chassis/server/bios # **scope bios-settings**	指定したサーバで BIOS 設定モードを開始します。
ステップ 4	UCS-A /chassis/server/bios/bios-settings # **show** *setting*	BIOS 設定を表示します。**show ?** と入力して、*setting* で使用可能な値のリストを表示します。

次に、シャーシ 1 のブレード 3 の BIOS 設定を表示する例を示します。

```
UCS-A# scope server 1/3
UCS-A /chassis/server # scope bios
UCS-A /chassis/server/bios # scope  bios-settings
UCS-A /chassis/server/bios/bios-settings # show intel-vt-config

Intel Vt Config:
    Vt
    --
    Enabled

UCS-A /chassis/server/bios/bios-settings #
```

トラステッド プラットフォーム モジュールの設定

トラステッド プラットフォーム モジュール

トラステッドプラットフォームモジュール（TPM）は、サーバの認証に使用するアーティファクトを安全に保存できるコンポーネントです。これらのアーティファクトには、パスワード、証明書、または暗号キーを収録できます。プラットフォームが信頼性を維持していることを確認するうえで効果的なプラットフォームの尺度の保存でも、TPM を使用できます。すべての環境で安全なコンピューティングを実現するうえで、認証（プラットフォームがその表明どおりのものであることを証明すること）および立証（プラットフォームが信頼でき、セキュリティを維持していることを証明するプロセス）は必須の手順です。これは Intel Trusted Execution Technology（TXT）セキュリティ機能の要件であり、TPM を搭載したサーバの BIOS 設定でイネーブルにする必要があります。Cisco UCS M4 ブレードおよびラックマウント サーバは、TPM をサポートします。 デフォルトでは、TPM はこれらのサーバで有効になっています。

重要

- Cisco UCS Manager をリリース 2.2(4) にアップグレードする場合は、TPM が有効になります。
- TPM が有効な状態で Cisco UCS Manager をリリース 2.2(4) からダウングレードすると、TPM が無効になります。

Intel Trusted Execution Technology

Intel Trusted Execution Technology（TXT）を使用すると、ビジネス サーバ上で使用および保管される情報の保護機能が強化されます。この保護の主要な特徴は、隔離された実行環境および付随メモリ領域の提供にあり、機密データに対する操作をシステムの他の部分から見えない状態で実行することが可能になります。Intel TXT は、暗号キーなどの機密データを保管できる封印されたストレージ領域を提供し、悪意のあるコードからの攻撃時に機密データが漏洩するのを防ぐために利用できます。Cisco UCS M4 ブレードおよびラックマウント サーバは、TXT をサポートしています。デフォルトでは、TXT はこれらのサーバで無効になっています。

TXT は TPM、Intel Virtualization Technology（VT）、および Intel Virtualization Technology for Directed I/O（VT-d）が有効になっている場合にだけ、有効にできます。TXT だけを有効にすると、暗黙的に TPM、VT、および VT-d も有効になります。

信頼できるプラットフォーム

Cisco UCSME-2814 コンピュート カートリッジのモジュラ サーバには、TPM および TXT のサポートが含まれています。Cisco UCS M4 ブレードおよびラックマウント サーバは、TPM および TXT をサポートします。 UCS Manager リリース 2.5(2)UCS Manager リリース 2.2(4) では、TPM および TXT で次の操作を実行できます。

- TPM の有効化または無効化
- TXT の有効化または無効化
- ブレード サーバの TPM のクリア または ラックマウント サーバの TPM のクリア
- モジュラ サーバの TPM のクリア
- TPM のプロパティの表示

（注） Cisco UCS M3 ブレード サーバの場合は、F2 を押して BIOS セットアップ メニューを表示し、設定を変更します。

TPM の有効化または無効化

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルート組織モードを開始するには、/ を *org-name* として入力します。
ステップ 2	UCS-A /org # **create bios-policy** *policy-name*	BIOS ポリシーを指定されたポリシー名で作成し、組織 BIOS ポリシー モードを開始します。
ステップ 3	UCS-A /org/bios-policy* # **set trusted-platform-module-config tpm-support** {**enabled** | **disabled** | **platform-default**}	TPM を**有効**にするか、**無効**にするかを指定します。**Platform-default** では、TPM は有効になっています。
ステップ 4	UCS-A /org/bios-policy* # **commit-buffer**	トランザクションをシステム設定にコミットします。
ステップ 5	UCS-A /org # **create service-profile** *sp-name*}	指定されたサービスプロファイルを作成し、サービス プロファイルのコンフィギュレーション モードを開始します。
ステップ 6	UCS-A /org/service-profile* # **set bios-policy** *policy-name*	指定された BIOS ポリシーをサービス プロファイルに関連付けます。
ステップ 7	UCS-A /org/service-profile* # **commit-buffer**	トランザクションをシステム設定にコミットします。

	コマンドまたはアクション	目的
ステップ 8	UCS-A /org/service-profile # **associate server** *chassis-id / slot-id*	サービス プロファイルを 1 つのサーバに関連付けます。

次に、TPM を有効にする例を示します。

```
UCS-A # scope org
UCS-A /org # create bios-policy bp1
UCS-A /org/bios-policy* # set trusted-platform-module-config tpm-support enabled
UCS-A /org/bios-policy* # commit-buffer
UCS-A /org # create service-profile sp1
UCS-A /org/service-profile* # set bios-policy bp1
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile # associate server 1/2
```

TXT の有効化または無効化

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルート組織モードを開始するには、/ を *org-name* として入力します。
ステップ 2	UCS-A /org # **create bios-policy** *policy-name*	BIOS ポリシーを指定されたポリシー名で作成し、組織 BIOS ポリシー モードを開始します。
ステップ 3	UCS-A /org/bios-policy* # **set intel-trusted-execution-technology-config txt-support** {**enabled** | **disabled** | **platform-default**}	TXT を**有効**にするか、**無効**にするかを指定します。**Platform-default** では、TXT は有効になっています。
ステップ 4	UCS-A /org/bios-policy* # **commit-buffer**	トランザクションをシステム設定にコミットします。
ステップ 5	UCS-A /org # **create service-profile** *sp-name*}	指定されたサービス プロファイルを作成し、サービス プロファイルのコンフィギュレーション モードを開始します。
ステップ 6	UCS-A /org/service-profile* # **set bios-policy** *policy-name*	指定された BIOS ポリシーをサービス プロファイルに関連付けます。

	コマンドまたはアクション	目的
ステップ 7	UCS-A /org/service-profile* # **commit-buffer**	トランザクションをシステム設定にコミットします。
ステップ 8	UCS-A /org/service-profile # **associate server** *chassis-id / slot-id*	サービス プロファイルを 1 つのサーバに関連付けます。

次に、TXT を有効にする例を示します。

```
UCS-A # scope org
UCS-A /org # create bios-policy bp1
UCS-A /org/bios-policy* # set intel-trusted-execution-technology-config txt-support enabled
UCS-A /org/bios-policy* # commit-buffer
UCS-A /org # create service-profile sp1
UCS-A /org/service-profile* # set bios-policy bp1
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile # associate server 1/2
```

一貫したデバイスの命名

オペレーティングシステムが一貫した方法でイーサネットインターフェイスに命名できるメカニズムがない場合は、サーバの構成が変更されたネットワーク接続の管理は困難になります。Cisco UCS Manager リリース 2.2(4) で導入された一貫したデバイスの命名（CDN）を使用すると、イーサネット インターフェイスに一貫した方法で名前を付けることができます。これにより、アダプタまたは他の設定が変更された場合でも、イーサネット インターフェイスの名前がより永続的になります。

vNIC の CDN を設定するには、次の手順を実行します。

- BIOS ポリシーで一貫したデバイスの命名を有効にします。
- BIOS ポリシーとサービス プロファイルを関連付けます。
- vNIC の一貫した命名を設定します。

一貫したデバイスの命名の注意事項と制約事項

- 一貫したデバイスの命名（CDN）は Windows 2012 R2 でのみサポートされます。その他のオペレーティング システムではサポートされません。
- CDN は、M3 以降のすべてのブレードサーバとラックマウント サーバでサポートされます。
- CDN をサポートするには、BIOS とアダプタ ファームウェアがリリース 2.2(4) バンドルに組み込まれている必要があります。
- Cisco UCS Manager リリース 2.2(4) では、CDN は次のアダプタでのみサポートされます。

- Cisco UCS VIC 1225（UCSC-PCIE-CSC-02）
- Cisco UCS MLOM 1227（UCSC-MLOM-CSC-02）
- Cisco UCS VIC 1225T（UCSC-PCIE-C10T-02）
- Cisco UCS MLOM 1227T（UCSC-MLOM-C10T-02）
- Cisco UCS VIC 1240（UCSB-MLOM-40G-01）
- Cisco UCS VIC 1280（UCS-VIC-M82-8P）
- Cisco UCS VIC 1340（UCSB-MLOM-40G-03）
- Cisco UCS VIC 1380（UCSB-VIC-M83-8P）

- CDN は vNIC テンプレートおよびダイナミック vNIC ではサポートされません。
- 同じサービス プロファイル内の複数の vNIC に同じ CDN 名を指定することはできません。
- CDN 名が vNIC に指定されていない場合は、vNIC 名が CDN 名として使用されます。
- vNIC に設定する CDN 名は [管理者 CDN 名（Admin CDN Name）] として表示されます。vNIC に最後に適用された CDN 名は、[オペレータ CDN 名（Oper CDN Name）] として表示されます。たとえば、「vnic0」という名前の vNIC の [管理者 CDN 名（Admin CDN Name）] が cdn0 の場合、この vNIC の [オペレータ CDN 名（Oper CDN Name）] は cdn0 になりますが、同じ vNIC でも [管理者 CDN 名（Admin CDN Name）] が指定されていない場合は [オペレータ CDN 名（Oper CDN Name）] は vnic0 になります。
- Cisco UCS Manager リリース 2.2(4) では、CDN が関連付けられたサーバに割り当てられた BIOS ポリシーで有効な場合、Cisco UCS Manager のダウングレードは禁止されています。
- Cisco UCS Manager リリース 2.2(4) では、CDN 対応 BIOS ポリシーがサーバに割り当てられている場合は、BIOS ファームウェアのダウングレードは禁止されています。
- Cisco UCS Manager リリース 2.2(4) では、CDN 対応 BIOS ポリシーがサーバに割り当てられている場合は、アダプタ ファームウェアのダウングレードは禁止されています。
- 適用された BIOS ポリシーが CDN 非対応から CDN 対応に、または CDN 対応から CDN 非対応に変更された場合は、BIOS 更新プログラムのリブートが有効かどうかに関係なく、警告が表示されホストがリブートします。
- Windows オペレーティング システムをインストールする前に、BIOS ポリシーで CDN を有効にし、vNIC に CDN 名を追加しておくことを推奨します。
- Windows オペレーティング システムがすでにサーバにインストールされ、CDN が BIOS ポリシーで有効な場合は、次の手順を実行します。

  1. ネットワーク ドライバをアンインストールします。
  2. システムで非表示のデバイスをスキャンし、それらをアンインストールします。
  3. システムで新しいハードウェアを再スキャンし、ネットワーク ドライバを再インストールします。

これを行わないと、vNIC が設定された CDN 名で認識されません。

- サービス プロファイルで、適用された BIOS ポリシーが CDN 非対応から CDN 対応に、または CDN 対応から CDN 非対応に変更された場合は、次の手順を実行します。

  1 ネットワーク ドライバをアンインストールします。

  2 システムで非表示のデバイスをスキャンし、それらを削除します。

  3 システムで新しいハードウェアを再スキャンし、ネットワーク ドライバを再インストールします。

  

  （注） BIOS ポリシーが CDN 対応から CDN 非対応に変更された場合は、CDN 名がシステム上のすべての vNIC から削除されたことを確認します。

- vNIC に変更が加えられた場合、システム上のすべてのデバイスの BDF も変更されます。次に、システムに存在するすべての vNIC の BDF の変更をトリガーするいくつかのシナリオを示します。

  ◦ vNIC が追加または削除された場合

  ◦ vNIC がシステム上のあるアダプタからシステム上の別のアダプタに移動された場合

  これらの変更がシステムに加えられた場合は、次の手順を実行します。

  1 存在するすべてのネットワーク インターフェイスからネットワーク ドライバをアンインストールします。

  2 システムで非表示のデバイスをスキャンし、それらをアンインストールします。

  3 システムで新しいハードウェアを再スキャンし、ネットワーク コントローラにネットワーク ドライバを再インストールします。

  非表示のデバイスが削除されないと、ネットワーク アダプタの CDN 名は Cisco UCS Manager に設定されたとおりに表示されません。

各種アダプタが混在する場合の CDN

CDN 名が CDN がサポートされているアダプタと CDN がサポートされていないアダプタが混在するシステム内の vNIC に設定されると、システム配置において、CDN が設定された vNIC が CDN をサポートするアダプタに配置されない場合があります。

CDN が BIOS ポリシーで有効であり、システム配置によって、CDN が設定された vNIC（管理者 CDN 設定済み）が CDN をサポートしていないアダプタに配置された場合は、情報エラーが発生しますが、サービス プロファイルの設定問題は無視されます。

CDN が BIOS ポリシーで有効であり、システム配置によって、vNIC（管理者 CDN 未設定）が CDN をサポートしていないアダプタに配置された場合は、情報エラーが発生しますが、サービス

プロファイルの設定問題は無視されます。この場合、[オペレータ CDN 名（Oper CDN Name）] は空になり、vNIC 名から派生されません。

CDN 名をサーバのホスト ネットワーク インターフェイス名として展開する場合は、サポートされるアダプタに手動で vNIC を配置する必要があります。

BIOS ポリシーでの一貫したデバイスの命名の有効化

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルート組織モードを開始するには、*/* を *org-name* として入力します。
ステップ 2	UCS-A /org # **create bios-policy** *policy-name*	BIOS ポリシーを指定されたポリシー名で作成し、組織 BIOS ポリシー モードを開始します。
ステップ 3	UCS-A /org/bios-policy* # **set consistent-device-name-control cdn-name** {**enabled** | **disabled** | **platform-default**}	一貫したデバイスの命名（CDN）を**有効**にするか**無効**にするかを指定します。
ステップ 4	UCS-A /org/bios-policy* # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、BIOS ポリシーでの CDN を有効にする方法を示しています。

```
UCS-A # scope org
UCS-A /org # create bios-policy cdn-bios-policy
UCS-A /org/bios-policy* # set consistent-device-name-control cdn-name enabled
UCS-A /org/bios-policy* # commit-buffer
```

BIOS ポリシーとサービス プロファイルの関連付け

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルート組織モードを開始するには、*/* を *org-name* として入力します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /org # **scope service-profile** *sp-name*}	指定したサービス プロファイルのサービス プロファイル コンフィギュレーション モードを開始します。
ステップ 3	UCS-A /org/service-profile # **set bios-policy** *policy-name*	指定された BIOS ポリシーをサービス プロファイルに関連付けます。
ステップ 4	UCS-A /org/service-profile* # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、CDN が有効の BIOS ポリシーをサービス プロファイルに関連付ける方法を示します。

```
UCS-A # scope org
UCS-A /org # scope service-profile sp1
UCS-A /org/service-profile # set bios-policy cdn-bios-policy
UCS-A /org/service-profile* # commit-buffer
```

vNIC の一貫したデバイスの命名の設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルート組織モードを開始するには、*/* を *org-name* として入力します。
ステップ 2	UCS-A /org # **scope service-profile** *sp-name*	指定したサービス プロファイルのサービス プロファイル コンフィギュレーション モードを開始します。
ステップ 3	UCS-A /org/service-profile # **scope vnic** *vnic-name*	指定した vNIC の vNIC コンフィギュレーション モードを開始します。
ステップ 4	UCS-A /org/service-profile/vnic # **set cdn-name** *cdn-name*	vNIC に CDN 名を指定します。
ステップ 5	UCS-A /org/service-profile/vnic* # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、vNIC に CDN を設定する例を示します。

```
UCS-A # scope org
```

```
UCS-A /org # scope service-profile sp1
UCS-A /org/service-profile # scope vnic vn1
UCS-A /org/service-profile/vnic # set cdn-name eth0
UCS-A /org/service-profile/vnic* # commit-buffer
```

vNIC の CDN 名の表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *server-num*	指定したサーバのサーバ モードを開始します。
ステップ 2	UCS-A /server # **scope adapter** *adapter-id*	指定されたアダプタのアダプタ モードを開始します。
ステップ 3	UCS-A /server/adapter # **show host-eth-if** [**detail**] [**expand**]	指定されたアダプタのホスト イーサネット インターフェイスの詳細を表示します。

次に、vNIC の CDN 名を表示する例を示します。

```
UCS-A # scope server 3
UCS-A /server # scope adapter 1
UCS-A /server/adapter # show host-eth-if detail expand

Eth Interface:
    ID: 1
    Dynamic MAC Address: 00:25:B5:00:00:99
    Burned-In MAC Address: 00:00:00:00:00:00
    Model: UCSC-PCIE-CSC-02
    Name: vnic1
    Cdn Name: cdn0
    Admin State: Enabled
    Operability: Operable
    Order: 1
```

vNIC のステータスの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルート組織モードを開始するには、*/* を *org-name* として入力します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /org # **scope service-profile** *sp-name*	指定したサービス プロファイルのサービス プロファイル コンフィギュレーション モードを開始します。
ステップ 3	UCS-A /org/service-profile # **show vnic** [**detail**] [**expand**]	指定されたサービス プロファイルの vNIC の詳細を表示します。

次に、vNIC のステータスを表示する例を示します。

（注） vNIC に設定する CDN 名は、[管理者 CDN 名（Admin CDN Name）] として表示されます。BIOS ポリシーに最後に適用された CDN 名前は、[オペレータ CDN 名（Oper CDN Name）] として表示されます。

```
UCS-A# scope org
UCS-A /org # scope service-profile sp1
UCS-A /org/service-profile # show vnic detail expand

vNIC:
    Name: vnic1
    Fabric ID: B
    Dynamic MAC Addr: 00:25:B5:17:47:01
    Desired Order: Unspecified
    Actual Order: 1
    Desired VCon Placement: 2
    Actual VCon Placement: 2
    Desired Host Port: ANY
    Actual Host Port: NONE
    Equipment: sys/chassis-2/blade-5/adaptor-3/host-eth-2
    Host Interface Ethernet MTU: 1500
    Ethernet Interface Admin CDN Name:cdn0
    Ethernet Interface Oper CDN Name:cdn0
    Template Name:
```

CIMC セキュリティ ポリシー

Cisco UCS Manager は、セキュリティを強化するために次のポリシーを提供しています。

- KVM 管理ポリシー
- IPMI アクセス プロファイル

IPMI アクセス プロファイル

このポリシーでは、IP アドレスを使用して、IPMI コマンドを直接サーバに送信できるかどうかを決定することができます。たとえば、CIMC からセンサー データを取得するためのコマンドを送

信することができます。このポリシーによって、サーバでローカルに認証可能なユーザ名とパスワードを含む IPMI アクセスを定義し、さらにアクセスが読み取り専用であるか読み取り/書き込みであるかを定義します。

また、IPMI アクセス プロファイルで IPMI over LAN をディセーブルまたはイネーブルにして、リモート接続を制限することもできます。IPMI over LAN はデフォルトで、関連付けられていないサーバすべて、および IPMI アクセス ポリシーのないサーバすべてでディセーブルになります。IPMI アクセス ポリシーを作成すると、IPMI over LAN はデフォルトでイネーブルに設定されます。値を変更してディセーブルにしない場合、IPMI over LAN は関連するサーバすべてでイネーブルになります。

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

IPMI アクセス プロファイルの設定

はじめる前に

次を入手します。

- 適切な権限があり、サーバのオペレーティング システムによる認証が可能なユーザ名
- このユーザ名のパスワード
- ユーザ名と関連付けられている権限

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に */* を入力します。
ステップ 2	UCS-A /org # **create ipmi-access-profile** *profile-name*	指定された IPMI アクセス プロファイルを作成し、組織 IPMI アクセス プロファイル モードを開始します。
ステップ 3	UCS-A /org/ipmi-access-profile # **set ipmi-over-lan** {**disable** | **enable**}	リモート接続を確立できるかどうかを決定します。 （注） IPMI over LAN はデフォルトで、関連付けられていないサーバすべて、および IPMI アクセス ポリシーのないサーバすべてでディセーブルになります。IPMI アクセス ポリシーを作成すると、IPMI over LAN はデフォルトでイネーブルに設定されます。値を変更してディセーブルにしない場合、IPMI over LAN は関連するサーバすべてでイネーブルになります。

	コマンドまたはアクション	目的
ステップ 4	UCS-A /org/ipmi-access-profile # **create ipmi-user** *ipmi-user-name*	指定されたエンドポイントユーザを作成して、組織 IPMI アクセス プロファイル エンドポイント ユーザ モードを開始します。 （注） IPMI アクセス プロファイル内には、それぞれが独自のパスワードと権限を持つエンドポイントユーザを複数作成できます。
ステップ 5	UCS-A /org/ipmi-access-profile/ipmi-user #**set password**	エンドポイントユーザのパスワードを設定します。 **set password** コマンドの入力後、パスワードの入力と確認を求められます。セキュリティ上の理由から、入力したパスワードは CLI には表示されません。
ステップ 6	UCS-A /org/ipmi-access-profile/ipmi-user # **set privilege** {**admin** | **readonly**}	エンドポイントユーザが管理権限と読み取り専用権限のいずれを持つかを指定します。
ステップ 7	UCS-A /org/ipmi-access-profile/ipmi-user # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、ReadOnly という名前の IPMI アクセス プロファイルを作成し、bob という名前のエンドポイント ユーザを作成し、bob のパスワードと権限を設定し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # create ipmi-access-profile ReadOnly
UCS-A /org/ipmi-access-profile* # create ipmi-user bob
UCS-A /org/ipmi-access-profile/ipmi-user* # set password
Enter a password:
Confirm the password:
UCS-A /org/ipmi-access-profile/ipmi-user* # set privilege readonly
UCS-A /org/ipmi-access-profile/ipmi-user* # commit-buffer
UCS-A /org/ipmi-access-profile/ipmi-user #
```

次の作業

IPMI プロファイルをサービス プロファイルとテンプレートのうち一方、または両方に含めます。

IPMI アクセス プロファイルの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / と入力します。
ステップ 2	UCS-A /org # **delete ipmi-access-profile** *profile-name*	指定した IPMI アクセス プロファイルを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、ReadOnly という名前の IPMI アクセス プロファイルを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # delete ipmi-access-profile ReadOnly
UCS-A /org* # commit-buffer
UCS-A /org #
```

IPMI アクセス プロファイルへのエンドポイント ユーザの追加

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **scope ipmi-access-profile** *profile-name*	指定した IPMI アクセス プロファイルの組織 IPMI アクセス プロファイル モードを開始します。
ステップ 3	UCS-A /org/ipmi-access-profile # **create ipmi-user** *ipmi-user-name*	指定されたエンドポイント ユーザを作成して、組織 IPMI アクセス プロファイル エンドポイント ユーザ モードを開始します。 （注） IPMI アクセス プロファイル内には、それぞれが独自のパスワードと権限を持つエンドポイントユーザを複数作成できます。

	コマンドまたはアクション	目的
ステップ 4	UCS-A /org/ipmi-access-profile/ipmi-user #**set password**	エンドポイント ユーザのパスワードを設定します。 **set password** コマンドの入力後、パスワードの入力と確認を求められます。セキュリティ上の理由から、入力したパスワードは CLI には表示されません。
ステップ 5	UCS-A /org/ipmi-access-profile/ipmi-user # **set privilege** {**admin** | **readonly**}	エンドポイント ユーザが管理権限と読み取り専用権限のいずれを持つかを指定します。
ステップ 6	UCS-A /org/ipmi-access-profile/ipmi-user # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、ReadOnly という名前の IPMI アクセス プロファイルに alice という名前のエンドポイント ユーザを追加し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org* # scope ipmi-access-profile ReadOnly
UCS-A /org/ipmi-access-profile* # create ipmi-user alice
UCS-A /org/ipmi-access-profile/ipmi-user* # set password
Enter a password:
Confirm the password:
UCS-A /org/ipmi-access-profile/ipmi-user* # set privilege readonly
UCS-A /org/ipmi-access-profile/ipmi-user* # commit-buffer
UCS-A /org/ipmi-access-profile/ipmi-user #
```

IPMI アクセス プロファイルからのエンドポイント ユーザの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に **/** と入力します。
ステップ 2	UCS-A /org # **scope ipmi-access-profile** *profile-name*	指定した IPMI アクセス プロファイルの組織 IPMI アクセス プロファイル モードを開始します。
ステップ 3	UCS-A /org/ipmi-access-profile # **delete ipmi-user** *epuser-name*	IPMI アクセス プロファイルから指定したエンドポイント ユーザを削除します。

	コマンドまたはアクション	目的
ステップ 4	UCS-A /org/ipmi-access-profile # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、ReadOnly という名前の IPMI アクセス プロファイルから alice という名前のエンドポイント ユーザを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # scope ipmi-access-profile ReadOnly
UCS-A /org/ipmi-access-profile # delete ipmi-user alice
UCS-A /org/ipmi-access-profile* # commit-buffer
UCS-A /org/ipmi-access-profile #
```

KVM 管理ポリシー

KVM管理ポリシーを使用して、KVM経由でサーバにアクセスするときに仮想メディア（vMedia）暗号化を有効にするかどうかを指定できます。

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

（注） KVM 仮想メディア（vMedia）セッションがマッピングされた後、KVM 管理ポリシーを変更すると、仮想メディア（vMedia）セッションは失われます。KVM仮想メディア（vMedia）セッションを再度マッピングする必要があります。

KVM 管理ポリシーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **create kvm-mgmt-policy** *policy-name*	指定された KVM 管理ポリシーを作成し、組織 KVM 管理ポリシー モードを開始します。
ステップ 3	UCS-A /org/kvm-mgmt-policy # **set descr** *description*	（任意） ポリシーの説明を記します。

	コマンドまたはアクション	目的
ステップ 4	UCS-A /org/kvm-mgmt-policy # **set vmedia-encryption** {**disable** | **enable**}	vMedia の暗号化を有効にするか無効にするかを指定します。
ステップ 5	UCS-A /org/ipmi-access-profile/ipmi-user # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、KVM_Policy1 という名前の KVM 管理ポリシーを作成し、vMedia の暗号化を有効にし、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # create kvm-mgmt-policy KVM_Policy1
UCS-A /org/kvm-mgmt-policy* # set vmedia-encryption enable
UCS-A /org/kvm-mgmt-policy* # commit-buffer
UCS-A /org/kvm-mgmt-policy #
```

ローカル ディスク設定ポリシーの設定

ローカル ディスク設定ポリシー

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

ローカル ディスク モードには次のものがあります。

- [ローカルストレージなし（No Local Storage）]：ディスクレス サーバまたは SAN 専用の設定で使用します。このオプションを選択する場合、このポリシーを使用する任意のサービス プロファイルを、ローカル ディスクを持つサーバに関連付けることができません。
- [RAID 0がストライプ済み（RAID 0 Striped）]：データはアレイのすべてのディスクにストライプ化され、高速スループットを提供します。 データの冗長性はなく、いずれかのディスクで障害が発生すると、すべてのデータが失われます。
- [RAID 1がミラー済み（RAID 1 Mirrored）]：データが 2 つのディスクに書き込まれ、1 つのディスクで障害が発生した場合でも完全なデータ冗長性を提供します。最大アレイ サイズは、2 つのドライブの小さい方の空き容量に等しくなります。
- [任意の設定（Any Configuration）]：変更なしのローカル ディスク設定を転送するサーバ設定で使用します。
- [RAIDなし（No RAID）]：RAID を削除し、ディスク MBR およびペイロードを変更しない状態のままにするサーバ設定で使用します。

[RAIDなし（No RAID）] を選択し、このポリシーをすでに RAID ストレージが設定されているオペレーティング システムを使用するサーバに適用した場合、ディスクの内容は削除されません。そのため、[RAIDなし（No RAID）] モードの適用後にサーバでの違いがわからないことがあります。よって、ポリシーの RAID 設定と、サーバの [インベントリ（Inventory）] > [ストレージ（Storage）] タブに表示される実際のディスク設定とが一致しない場合があります。

以前のすべての RAID 設定情報をディスクから削除するには、[RAIDなし（No RAID）] コンフィギュレーション モードの適用後にすべてのディスク情報を削除するスクラブ ポリシーを適用します。

- [RAID 5が部分的にストライプ済み（RAID 5 Striped Parity）]：データはアレイのすべてのディスクにストライプ化されます。 各ディスクの容量の一部に、ディスクの障害発生時にデータの再構築に使用できるパリティ情報が格納されます。RAID 5 は、高い読み取り要求レートで、アプリケーションに適切なデータ スループットを提供します。
- [RAID 6が部分的にデュアルストライプ済み（RAID 6 Striped Dual Parity）]：データはアレイのすべてのディスクにストライプ化され、2 つのパリティ ディスクを使用して、最大 2 つの物理ディスクの障害に対する保護を提供します。データ ブロックの各行に、2 セットのパリティ データが格納されます。
- [RAID 10がミラーおよびストライプ済み（RAID 10 Mirrored and Striped）]：RAID 10 はミラー化されたディスクのペアを使用して、完全なデータ冗長性と高いスループット レートを提供します。
- [RAID 50が部分的にストライプおよびストライプ済み]：データが複数のストライプ化されたパリティ ディスク セットにストライプ化され、高いスループットと複数のディスク故障耐性を提供します。
- [RAID 60部分的にストライプおよびストライプ済み]：データが複数のストライプ化されたパリティ ディスク セットにストライプ化され、高いスループットと優れたディスク故障耐性を提供します。

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

（注） 組み込みオンボード RAID コントローラを搭載した Cisco UCS Manager と統合された Cisco UCS C シリーズ サーバの場合、ローカル ディスク モードは常に [任意の設定（Any Configuration）] でなければならず、RAID はコントローラ上で直接設定する必要があります。

すべてのローカル ディスク設定ポリシーに関するガイドライン

ローカル ディスク設定ポリシーを作成する前に、次のガイドラインを考慮してください。

HDD と SSD を混合しない

1 台のサーバや RAID 設定に、HDD と SSD を使用しないでください。

B200 M1 または M2 のデフォルト ローカル ディスク設定ポリシーを使用して、B200 M3 にサービス プロファイルを割り当てない

B200 M1 および M2 サーバと B200 M3 サーバのストレージ コントローラで提供される RAID/JBOD サポートは異なっているため、B200M1 または M2 サーバのデフォルト ローカル ディスク設定ポリシーを含むサービス プロファイルを B200 M3 サーバに割り当てたり、再割り当てを行ったりすることはできません。デフォルトのローカル ディスク設定ポリシーには、[任意の設定（Any Configuration）] モードまたは JBOD 設定が含まれます。

JBOD モードのサポート

B200 M3 サーバでは、ローカル ディスクの JBOD モードがサポートされています。

（注） ローカル ディスクの JBOD モードをサポートしているのは、B200 M1、B200 M2、B200 M3、B250 M1、B250 M2、B22 M3 ブレード サーバのみです。

RAID 用に設定されているローカル ディスク設定ポリシーに関するガイドライン

MegaRAID ストレージ コントローラを搭載したサーバ用のローカル ディスク設定ポリシーに RAID 設定を設定する

ブレード サーバまたは統合されたラックマウント サーバに MegaRAID コントローラが搭載されている場合、そのサーバのサービスプロファイルに含まれるローカルディスク設定ポリシーでドライブの RAID 設定を設定する必要があります。これを実行するには、そのサーバに定義されている RAID モードのいずれかを使用して、サービス プロファイルのローカル ディスク設定ポリシーを設定するか、[任意の設定（Any Configuration）] モードと LSI ユーティリティ ツールセットを使用して、RAID ボリュームを作成します。

OS をインストールする前に RAID LUN を設定していないと、インストール時にディスク検出エラーが発生し、「No Device Found」といったエラー メッセージが表示される可能性があります。

サーバ プロファイルで [任意の設定（Any Configuration）] モードが指定されている場合、RAID 1 クラスタ移行後にサーバが起動しない

RAID 1 クラスタの移行後、サービス プロファイルをサーバに関連付ける必要があります。サービス プロファイル内のローカル ディスク設定ポリシーに [RAID 1] ではなく [任意の設定（Any Configuration）] モードが設定されていると、RAID LUN は、関連付け中およびその後も「非アクティブ」状態のままになります。その結果、サーバは起動できなくなります。

この問題を回避するには、サーバに関連付けるサービス プロファイルに、移行前の元のサービス プロファイルとまったく同じローカル ディスク設定ポリシーが含まれるようにし、[任意の設定（Any Configuration）] モードは含まれないようにします。

MegaRAID ストレージ コントローラを搭載したサーバ上で JBOD モードを使用しない

MegaRAIDストレージコントローラが搭載されたブレードサーバまたは統合ラックマウントサーバ上で JBOD モードまたは JBOD 操作を設定または使用しないでください。JBOD モードと操作は、このサーバで完全に機能するよう設計されていません。

統合されたラックマウント サーバ内の RAID ボリュームと RAID コントローラはそれぞれ 1 つまで

Cisco UCS Manager と統合されているラックマウント サーバは、Cisco UCS Centralサーバ上に存在するハード ドライブの数とは関係なく、RAID ボリュームを 1 つまでしか設定できません。

統合されたラックマウント サーバ内のローカル ハード ドライブは、1 つの RAID コントローラのみにすべて接続される必要があります。Cisco UCS Manager との統合では、ローカル ハード ドライブが単一のラックマウント サーバ内の複数の RAID コントローラに接続することはサポートされていません。そのため、Cisco UCS Manager と統合されるラックマウント サーバを発注する際は、単一の RAID コントローラ構成を要求することを推奨します。

また、サードパーティ製のツールを使用して、ラックマウント サーバ上に複数の RAID LUN を作成しないでください。Cisco UCS Manager では、そのような設定はサポートされていません。

ブレード サーバ内の RAID ボリュームと RAID コントローラはそれぞれ 1 つまで

ブレード サーバは、サーバ内に存在するドライブの数とは関係なく、RAID ボリュームを 1 つまでしか設定できません。ローカル ハード ドライブは、1 つの RAID コントローラのみにすべて接続される必要があります。たとえば、B200 M3 に LSI コントローラと Intel Patsburg コントローラが搭載されていても、LSI コントローラだけが RAID コントローラして使用できます。

また、サードパーティ製のツールを使用して、ブレード サーバ上に複数の RAID LUN を作成しないでください。Cisco UCS Manager では、そのような設定はサポートされていません。

ミラー RAID で選択されるディスクの数は 2 つまでにする

ミラー RAID で選択されたディスクの数が 2 つを超えると、RAID 1 は RAID 10 LUN として作成されます。この問題は、Cisco UCS B440 M1 サーバと B440 M2 サーバで発生する可能性があります。

一部のサーバの特定の RAID 設定オプションでは、ライセンスが必要

一部の Cisco UCS サーバには、特定の RAID 設定オプションのライセンスが必要です。Cisco UCS Manager で、このローカル ディスク ポリシーを含むサービス プロファイルとサーバを関連付けると、Cisco UCS Manager によって選択された RAID オプションに適切なライセンスが備わっているかが確認されます。問題がある場合は、サービス プロファイルを関連付ける際に、Cisco UCS Manager に設定エラーが表示されます。

特定の Cisco UCS サーバの RAID ライセンス情報については、そのサーバの『*Hardware Installation Guide*』を参照してください。

B420 M3 サーバでは全コンフィギュレーション モードはサポートされていない

B420 M3 サーバでは、ローカル ディスク設定ポリシーで、次のような設定オプションはサポートされていません。

- RAID なし
- RAID 6 ストライプ化デュアルパリティ

また、B420 M3 では JBOD モードや操作はサポートされていません。

シングル ディスク RAID 0 設定は、一部のブレード サーバではサポートされていない

シングル ディスク RAID 0 設定は、次のブレード サーバではサポートされていません。

- Cisco UCS B200 M1
- Cisco UCS B200 M2
- Cisco UCS B250 M1
- Cisco UCS B250 M2

ローカル ディスク設定ポリシーの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に **/** を入力します。
ステップ 2	UCS-A /org # **create local-disk-config-policy** *policy-name*	ローカル ディスク設定ポリシーを作成し、ローカル ディスク設定ポリシー モードを開始します。
ステップ 3	UCS-A /org/local-disk-config-policy # **set descr** *description*	（任意） ローカルディスク設定ポリシーに説明を記入します。
ステップ 4	UCS-A /org/local-disk-config-policy # **set mode** {**any-configuration** | **no-local-storage** | **no-raid** | **raid-0-striped** | **raid-1-mirrored** | **raid-5-striped-parity** | **raid-6-striped-dual-parity** | **raid-10-mirrored-and-striped**}	ローカル ディスク設定ポリシーのモードを指定します。
ステップ 5	UCS-A /org/local-disk-config-policy # **set protect** {**yes** | **no**}	サーバは、サービス プロファイルとの関連付けが解除されても、ローカル ディスク設定ポリシー内の設定を保持するかどうかを指定します。

	コマンドまたはアクション	目的
		注意 サーバ内の 1 つ以上のディスクに障害が発生すると、[設定の保護（Protect Configuration）] は機能しなくなります。 サービス プロファイルがサーバから関連付けを解除され、新しいサービス プロファイルが関連付けられると、新しいサービス プロファイルの Protect Configuration プロパティの設定が優先され、前のサービス プロファイルの設定が上書きされます。 このオプションが有効になっていると、サーバが稼働停止して再稼働された後でもディスク上のデータは保護されます。従って、サーバとサービス プロファイルとの再アソシエーションは失敗します。 （注） このオプションが有効な状態でサーバとサービスプロファイルの関連付けを解除した後、そのサーバに新しいサービス プロファイルを関連付け、そのサービス プロファイル内のローカル ディスク設定ポリシーに前とは異なるプロパティが含まれていると、サーバから設定不一致のエラーが返され、関連付けは失敗します。
ステップ 6	UCS-A /org/local-disk-config-policy # **set flexflash-state** {**enable** | **disable**}	FlexFlash SD カードのサポートをイネーブルにするかを指定します。
ステップ 7	UCS-A /org/local-disk-config-policy # **set flexflash-raid-reporting-state** {**enable** | **disable**}	FlexFlash RAID レポートのサポートをイネーブルにするかを指定します。 （注） インストールされている SD カードが 1 つだけの場合、FlexFlash インベントリに RAID 状態が [無効（Disabled）]、RAID ヘルスが [適用しない（NA）] と表示されます。
ステップ 8	UCS-A /org/local-disk-config-policy # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、ローカル ディスク設定ポリシーを設定し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # create local-disk-config-policy DiskPolicy7
UCS-A /org/local-disk-config-policy* # set mode raid-1-mirrored
UCS-A /org/local-disk-config-policy* # set protect yes
UCS-A /org/local-disk-config-policy* # commit-buffer
UCS-A /org/local-disk-config-policy #
```

ローカル ディスク設定ポリシーの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **show local-disk-config-policy** *policy-name*	ローカル ディスク ポリシーを表示します。ローカル ディスク ポリシーを設定していない場合は、（create local-disk-config コマンドで作成された）ローカルディスク設定が表示されます。 （create local-disk-config コマンドで設定された）ローカル ディスク定義を表示します。Serial over LAN 定義が設定されていない場合、およびポリシーが（set local-disk-config-policy コマンドを使用して）設定されている場合、ポリシーが表示されます。

次に、DiskPolicy7 というローカル ディスク設定ポリシーのローカル ディスク ポリシー情報を表示する例を示します。

```
UCS-A# scope org /
UCS-A /org # show local-disk-config-policy DiskPolicy7

Local Disk Config Policy:
Name: DiskPolicy7
Mode: Raid 1 Mirrored
Description:
Protect Configuration: Yes
```

ローカル ディスク設定ポリシーの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / と入力します。
ステップ 2	UCS-A /org # **delete local-disk-config-policy** *policy-name*	指定したローカルディスク設定ポリシーを削除します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、DiskPolicy7 という名前のローカルディスク設定ポリシーを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # delete local-disk-config-policy DiskPolicy7
UCS-A /org* # commit-buffer
UCS-A /org #
```

FlexFlash のサポート

概要

Cisco UCS B シリーズおよび C シリーズ M3 および M4 サーバは、内蔵のセキュア デジタル（SD）メモリ カードをサポートします。SD カードは、Cisco Flexible Flash ストレージ コントローラ（SD カード用スロットが 2 つある PCI ベースのコントローラ）によってホストされます。カードには、HV と呼ばれる単一のパーティションが含まれています。FlexFlash が有効な場合、Cisco UCS Manager には、BIOS とホスト オペレーティング システムの両方に対する USB ドライブとして HV パーティションが表示されます。

FlexFlash はデフォルトでディセーブルになっています。サービス プロファイルで使用されるローカル ディスク ポリシーで FlexFlash をイネーブルにできます。FlexFlash がローカル ディスク ポリシーでイネーブルと定義され、サーバが SD カードをサポートしている場合、FlexFlash コントローラはサービス プロファイルを関連付ける際にイネーブルになります。サーバが SD カードをサポートしていない場合や CIMC バージョンが古い場合は、構成エラー メッセージが表示されます。

サポートされるサーバの FlexFlash を無効にすると、ハイパーバイザまたは HV パーティションはホストからすぐに切断されます。FlexFlash コントローラは、関連サービス プロファイルの関連付け解除の一環としてもディセーブルになります。

FlexFlash コントローラはデュアル SD カード用の RAID-1 をサポートします。FlexFlash スクラブ ポリシーを作成しサーバを再認識することで RAID ペアに新しい SD カードを設定できます。FlexFlash スクラブ ポリシーは、両方のカードの HV パーティションを削除し、そのカードを正常な RAID 状態にすることができます。

（注） ペアリングが完了したらすぐにスクラブ ポリシーをディセーブルにします。

HV パーティションから起動するには、SD カードがサービス プロファイルで使用されるブート ポリシーで定義されている必要があります。

FlexFlash ファームウェア管理

FlexFlash コントローラ ファームウェアは、CIMC イメージの一部としてバンドルされます。CIMC をアップグレードする際に、最新のファームウェア バージョンが FlexFlash コントローラで使用可能な場合、コントローラは管理されなくなり、FlexFlash インベントリには、[コントローラ状態（Controller State）] が [ユーザ アクションを待機（Waiting For User Action）] として、[コントローラ状況（Controller Health）] が [古いファームウェアを実行中（Old Firmware Running）] として表示されます。FlexFlash コントローラのファームウェアをアップグレードするには、ボード コントローラの更新を行う必要があります。詳細については、該当する『*Cisco UCS B-Series Firmware Management Guide*』を参照してください。次の URL で入手できます。http://www.cisco.com/en/US/products/ps10281/products_installation_and_configuration_guides_list.html

Cisco Flexible Flash ストレージ コントローラの制約事項：

- Cisco Flexible Flash ストレージ コントローラは 16 GB、32 GB および 64 GB の SD カードのみをサポートしています。

（注） 16 GB および 32 GB カードは B200-M3 ブレード サーバでのみサポートされ、64 GB SD カードは B200-M4 ブレード サーバでのみサポートされます。

- ラック サーバの SD カードをブレード サーバで使用したり、ブレード サーバの SD カードをラック サーバで使用することは推奨されません。サーバ タイプ間での SD カードの交換は SD カードのデータ損失につながる可能性があります。
- 一部の Cisco UCS C シリーズ ラックマウント サーバには、4 つのパーティション（HV、HUU、SCU、ドライバ）を持つ SD カードが搭載されています。Cisco UCS Manager では HV パーティションのみが表示されます。FlexFlash スクラブ ポリシーを使用して、4 つのパーティションを持つ SD カードを単一 HV パーティション カードに移行できます。
- FlexFlash コントローラは RAID-1 同期（ミラー再構築）をサポートしません。SD カードが RAID の低下状態である場合、あるいはメタデータ エラーがコントローラによって報告された場合は、FlexFlash スクラブ ポリシーを実行して RAID のためのカードを組み合わせる必要があります。FlexFlash スクラブ ポリシーの詳細については、スクラブ ポリシーの設定, （523 ページ） を参照してください。次の条件によって RAID の低下やメタデータ エラーが引き起こされる可能性があります。
  - サーバの 2 番目のスロットに SD カードがすでに存在する状態で、新規または使用済み SD カードを 1 つのスロットへ挿入する。
  - 異なるサーバの 2 つの SD カードを挿入する。
- サーバのファームウェア バージョンは、2.2(1a) 以上が必要です。

FlexFlash FX3S のサポート

リリース 2.2(3) 以降、Cisco UCS Manager では FX3S コントローラによる追加の FlexFlash サポートが可能になりました。FX3S コントローラは次のサーバ上に存在します。

- Cisco UCS B200 M4 ブレード サーバ
- Cisco UCS C220 M4 ラック サーバ
- Cisco UCS C240 M4 ラック サーバ

FX3S 制御を使用した FlexFlash 操作は、Cisco Flexible Flash ストレージ コントローラでの操作と同じです。FlexFlash はデフォルトでは無効で、ローカルディスク ポリシーを使用して有効化されます。また、コントローラをリセットし、SD カードをフォーマットして、一対の SD カードを自動同期させることもできます。

FX3S コントローラの SD カードには、ハイパーバイザと呼ばれる単一のパーティションが含まれています。

Cisco FX3S コントローラの制約事項：

- FX3S コントローラは、32 GB および 64 GB の SD カードのみをサポートします。16 GB のカードはサポートされません。
- ラック サーバの SD カードをブレード サーバで使用したり、ブレード サーバの SD カードをラック サーバで使用することは推奨されません。サーバ タイプ間での SD カードの交換は SD カードのデータ損失につながる可能性があります。
- サーバのファームウェア バージョンは、2.2(3a) 以上が必要です。

FlexFlash SD カードのサポートのイネーブル化またはディセーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **scope local-disk-config-policy** *policy-name*	指定したローカル ディスク設定ポリシー モードを開始します。
ステップ 3	UCS-A /org/local-disk-config-policy # **set flexflash-state** {**enable** | **disable**}	FlexFlash SD カードのサポートをイネーブルにするかを指定します。
ステップ 4	UCS-A /org/local-disk-config-policy # **set flexflash-raid-reporting-state** {**enable** | **disable**}	FlexFlash RAID レポートのサポートをイネーブルにするかを指定します。 （注） インストールされている SD カードが 1 つだけの場合、FlexFlash インベントリに RAID 状態が [無効（Disabled）]、RAID ヘルスが [適用しない（NA）] と表示されます。

	コマンドまたはアクション	目的
ステップ 5	UCS-A /org/local-disk-config-policy # **commit-buffer**	トランザクションをシステムにコミットします。

次の例では、ローカル ディスク設定ポリシー デフォルトの FlexFlash SD カードのサポートおよび FlexFlash RAID レポート ステートをイネーブルにし、システムへのトランザクションをコミットする方法を示します。

```
UCS-A# scope org/
UCS-A /org # scope local-disk-config-policy default
UCS-A /org/local-disk-config-policy #set flexflash-state enable
UCS-A /org/local-disk-config-policy# #set flexflash-raid-reporting-state enable
UCS-A /org/local-disk-config-policy* # commit-buffer
UCS-A /org/local-disk-config-policy #
```

自動同期のイネーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope chassis** *chassis-num*	指定したシャーシでシャーシ モードを開始します。
ステップ 2	UCS-A /chassis # **scope server** *server-num*	サーバ シャーシ モードを開始します。
ステップ 3	UCS-A /chassis/server # **scope flexflash-controller** *controller-id*	FlexFlash コントローラ サーバ シャーシ モードを開始します。
ステップ 4	UCS-A /chassis/server/flexflash-controller # **pair** *primary_slot_number*	同期していない場合は、選択されたスロット番号のカードをプライマリとして使用して SD カードを再同期します。次のいずれかになります。 • 1：スロット 1 の SD カードがプライマリとして使用されます。 • 2：スロット 2 の SD カードがプライマリとして使用されます。
ステップ 5	UCS-A /chassis/server/flexflash-controller # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、スロット2のSDカードをプライマリとして使用して再同期する方法を示しています。

```
UCS-A# scope chassis 1
UCS-A /chassis # scope server 1
UCS-A /chassis/server # scope flexflash-controller 1
UCS-A /chassis/server/flexflash-controller # pair 2
UCS-A /chassis/server/flexflash-controller* # commit-buffer
UCS-A /chassis/server/flexflash-controller #
```

FlexFlash カードのフォーマット

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope chassis** *chassis-num*	指定したシャーシでシャーシ モードを開始します。
ステップ 2	UCS-A /chassis # **scope server** *server-num*	サーバ シャーシ モードを開始します。
ステップ 3	UCS-A /chassis/server # **scope flexflash-controller** *controller-id*	FlexFlash コントローラ サーバ シャーシ モードを開始します。
ステップ 4	UCS-A /chassis/server/flexflash-controller # **format**	SD カードをフォーマットします。
ステップ 5	UCS-A /chassis/server/flexflash-controller # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、FlexFlash コントローラをフォーマットする例を示します。

```
UCS-A# scope chassis 1
UCS-A /chassis # scope server 1
UCS-A /chassis/server # scope flexflash-controller 1
UCS-A /chassis/server/flexflash-controller # format
Warning: When commited, UCSM will format the SD Cards.
This will completely erase the data on the SD Cards!!

UCS-A /chassis/server/flexflash-controller* # commit-buffer
UCS-A /chassis/server/flexflash-controller #
```

FlexFlash コントローラのリセット

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope chassis** *chassis-num*	指定したシャーシでシャーシ モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /chassis # **scope server** *server-num*	サーバ シャーシ モードを開始します。
ステップ 3	UCS-A /chassis/server # **scope flexflash-controller** *controller-id*	FlexFlash コントローラ サーバ シャーシ モードを開始します。
ステップ 4	UCS-A /chassis/server/flexflash-controller # **reset**	指定された FlexFlash コントローラをリセットします。
ステップ 5	UCS-A /chassis/server/flexflash-controller # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、FlexFlash コントローラをリセットする方法を示します。

```
UCS-A# scope chassis 1
UCS-A /chassis # scope server 1
UCS-A /chassis/server # scope flexflash-controller 1
UCS-A /chassis/server/flexflash-controller # reset
Warning: When commited, UCSM will reset the FlexFlash Controller.
This will cause the host OS to lose connectivity to the SD Cards.

UCS-A /chassis/server/flexflash-controller* # commit-buffer
UCS-A /chassis/server/flexflash-controller #
```

FlexFlash コントローラのステータスの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope chassis** *chassis-num*	指定したシャーシでシャーシ モードを開始します。
ステップ 2	UCS-A /chassis # **scope server** *server-num*	サーバ シャーシ モードを開始します。
ステップ 3	UCS-A /chassis/server # **scope flexflash-controller** *controller-id*	FlexFlash コントローラ サーバ シャーシ モードを開始します。
ステップ 4	UCS-A /chassis/server/flexflash-controller # **show detail expand**	詳細な FlexFlash コントローラのプロパティを表示します。

次の例は、FlexFlash コントローラと SD カードのステータスを示しています。

```
UCS-A# scope chassis 1
UCS-A /chassis # scope server 1
UCS-A /chassis/server # scope flexflash-controller 1
UCS-A /chassis/server/flexflash-controller # show detail expand
```

```
FlexFlash Controller:
    ID: 1
    Type: SD
    FlexFlash Type: FX3S
    Vendor: Cypress
    Model: FX3S
    Serial: NA
    Firmware Version: 1.3.2 build 158
    Controller State: Connected Partition Over USB To Host
    Controller Health: Old Firmware Running
    RAID State: Enabled Paired
    RAID Health: OK
    Physical Drive Count: 2
    Virtual Drive Count: 1
    RAID Sync Support: Supported
    Operability: Operable
    Oper Qualifier Reason:
    Presence: Equipped
    Current Task:

    FlexFlash Card:
        Controller Index: 1
        Slot Number: 1
        Vendor: SE32G
        Model: SE32G
        HW Rev: 8.0
        Serial: 0xa2140794
        Manufacturer ID: 3
        OEM ID: SD
        Manufacturer Date: 2/14
        Size (MB): 30436
        Block Size: 512
        Card Type: FX3S configured
        Write Enabled: Not Write Protected
        Card Health: OK
        Card Mode: Secondary Active
        Operation State: Raid Partition
        Card State: Active
        Write IO Error Count: 0
        Read IO Error Count: 0
        Operability: Operable
        Oper Qualifier Reason:
        Presence: Equipped

        FlexFlash Card Drive:
            Name: Hypervisor
            Size (MB): 30432
            Removable: Yes
            Operability: Operable
            Operation State: Raid Partition

        Controller Index: 1
        Slot Number: 2
        Vendor: SE32G
        Model: SE32G
        HW Rev: 8.0
        Serial: 0xa2140742
        Manufacturer ID: 3
        OEM ID: SD
        Manufacturer Date: 2/14
        Size (MB): 30436
        Block Size: 512
        Card Type: FX3S configured
        Write Enabled: Not Write Protected
        Card Health: OK
        Card Mode: Primary
        Operation State: Raid Partition
        Card State: Active
        Write IO Error Count: 0
        Read IO Error Count: 0
        Operability: Operable
        Oper Qualifier Reason:
```

```
        Presence: Equipped

        FlexFlash Card Drive:
            Name: Hypervisor
            Size (MB): 30432
            Removable: Yes
            Operability: Operable
            Operation State: Raid Partition

    Local Disk Config Definition:
        Mode: Any Configuration
        Description:
        Protect Configuration: Yes

UCS-A /chassis/server/flexflash-controller #
```

スクラブ ポリシーの設定

スクラブ ポリシーの設定

このポリシーは、ディスカバリ プロセス中にサーバのローカル データおよびBIOS設定に何が起こるか、サーバがいつ再認識されるか、またはサーバとサービス プロファイルの関連付けがいつ解除されるかを決定します。

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

スクラブ ポリシーの設定に応じて、以下の処理が行われます。

ディスク スクラブ

関連付けが解除された場合は、すべてのローカル ドライブのデータに対して次のいずれかの処理が実行されます。

- 有効になっている場合、ローカル ドライブ上のすべてのデータが破棄されます。
- 無効になっている場合、ローカル ドライブ上のすべてのデータが保持されます（ローカル ストレージ設定を含む）。

BIOS 設定スクラブ

スクラブ ポリシーを含むサービス プロファイルとサーバとの関連付けが解除された場合は、BIOS設定に対して次のいずれかの処理が実行されます。

- 有効になっている場合は、サーバのすべてのBIOS設定が消去され、サーバ タイプとベンダーに応じたBIOSのデフォルトにリセットされます。
- 無効になっている場合は、サーバの既存のBIOS設定が保持されます。

FlexFlash スクラブ

FlexFlash スクラブにより、新規またはデグレードした SD カードの組み合わせ、FlexFlash メタデータの設定エラーの解決、および 4 パーティションの旧式 SD カードから単一パーティションの SD カードへの移行を実行できます。スクラブ ポリシーを含むサービス プロファイルとサーバとの関連付けが解除された場合、またはサーバが再認識された場合は、SD カードに対して次のいずれかの処理が実行されます。

- 有効になっている場合は、PNUOS フォーマット ユーティリティにより SD カードの HV パーティションがフォーマットされます。SD カードが 2 枚ある場合、それらカードは RAID-1 ペアになっており、両方のカードの HV パーティションが有効と見なされます。スロット 1 のカードはプライマリ、スロット 2 のカードはセカンダリと見なされます。
- 無効になっている場合は、既存の SD カード設定が保持されます。

（注）

- FlexFlash スクラブを行うと SD カードの HV パーティションが消去されるため、FlexFlash スクラブを実行する前に、適切なホスト オペレーティング システム ユーティリティを使用して SD カードの完全バックアップを行うことを推奨します。
- サービス プロファイルのメタデータ設定の不具合を解決するには、FlexFlash スクラブを実行する前にローカル ディスク設定ポリシーの FlexFlash を無効にして、サーバが再認識された後に FlexFlash を有効にする必要があります。
- ペアリングが完了するか、またはメタデータの不具合が解決したら、ただちにスクラブ ポリシーを無効にしてください。

スクラブ ポリシーの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に **/** を入力します。
ステップ 2	UCS-A /org # **create scrub-policy** *policy-name*	スクラブ ポリシーを指定されたポリシー名で作成し、組織スクラブ ポリシー モードを開始します。
ステップ 3	UCS-A /org/scrub-policy # **set descr** *description*	（任意） スクラブ ポリシーの説明を記入します。

	コマンドまたはアクション	目的
		（注） 説明にスペース、特殊文字、または句読点が含まれている場合は、説明を引用符で括る必要があります。引用符は、**show** コマンド出力の説明フィールドには表示されません。
ステップ 4	UCS-A /org/scrub-policy # **set disk-scrub** {**no** | **yes**}	次のように、このスクラブ ポリシーを使用するサーバでのディスク スクラブをイネーブル化またはディセーブル化します。 • 有効になっている場合、ローカル ドライブ上のすべてのデータが破棄されます。 • 無効になっている場合、ローカル ドライブ上のすべてのデータが保持されます（ローカル ストレージ設定を含む）。
ステップ 5	UCS-A /org/scrub-policy # **set bios-settings-scrub** {**no** | **yes**}	次のように、このスクラブ ポリシーを使用するサーバでのBIOS 設定スクラブをイネーブル化またはディセーブル化します。 • 有効になっている場合は、サーバのすべての BIOS 設定が消去され、サーバタイプとベンダーに応じたBIOSのデフォルトにリセットされます。 • 無効になっている場合は、サーバの既存の BIOS 設定が保持されます。
ステップ 6	UCS-A /org/scrub-policy # **set flexflash-scrub** {**no** | **yes**}	次のように、このスクラブ ポリシーを使用するサーバでのflexflash スクラブをイネーブル化またはディセーブル化します。 • 有効になっている場合は、PNUOS フォーマット ユーティリティにより SD カードの HV パーティションがフォーマットされます。SD カードが 2 枚ある場合、それらカードは RAID-1 ペアになっており、両方のカードのHVパーティションが有効と見なされます。スロット 1 のカードはプライマリ、スロット 2 のカードはセカンダリと見なされます。 • 無効になっている場合は、既存の SD カード設定が保持されます。
ステップ 7	UCS-A /org/scrub-policy # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、ScrubPolicy2 という名前のスクラブ ポリシーを作成し、スクラブ ポリシーを使用するサーバでディスクのスクラブをイネーブルにし、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # create scrub-policy ScrubPolicy2
UCS-A /org/scrub-policy* # set descr "Scrub disk but not BIOS."
UCS-A /org/scrub-policy* # set disk-scrub yes
UCS-A /org/scrub-policy* # set bios-settings-scrub no
UCS-A /org/scrub-policy* # set flexflash-scrub no
UCS-A /org/scrub-policy* # commit-buffer
UCS-A /org/scrub-policy #
```

スクラブ ポリシーの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / と入力します。
ステップ 2	UCS-A /org # **delete scrub-policy** *policy-name*	指定したスクラブ ポリシーを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、ScrubPolicy2 という名前のスクラブ ポリシーを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # delete scrub-policy ScrubPolicy2
UCS-A /org* # commit-buffer
UCS-A /org #
```

DIMM エラー管理の設定

DIMM の修正可能なエラー処理

Cisco UCS Manager では、DIMM が事前定義されたウィンドウにおいて修正可能な重大エラーに遭遇した場合、ステータスが [低下（Degraded）] と表され、機能しないデバイスと見なされます。

DIMM の修正可能なエラー処理機能により、サーバ内のすべての DIMM に関する修正可能および修正不可能なメモリ エラーをすべてリセットできます。エラー設定をリセットすると、当該DIMM

のエラー数はクリアされ、ステータスは操作可能に変わり、該当 DIMM のセンサー状態がリセットされます。

メモリ エラーのリセット

Cisco UCS Manager とベースボード管理コントローラ（BMC）で発生したすべての修正可能および修正不可能なメモリ エラーをリセットするには、この手順を使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope chassis** *chassis-num*	指定したシャーシでシャーシ モードを開始します。
ステップ 2	UCS-A/chassis # **scope server** *server-num*	指定したサーバのサーバ モードを開始します。
ステップ 3	UCS-A/chassis/server # **reset-all-memory-errors**	サーバ内のすべての DIMM で発生した修正可能および修正不可能なエラーをリセットします。
ステップ 4	UCS-A /chassis/server* # **commit-buffer**	保留中のすべてのトランザクションをコミットします。

次に、選択されたメモリ ユニットのメモリ エラーをリセットする例を示します。

```
UCS-A# scope chassis 1
UCS-A/chassis # scope server 1
UCS-A/chassis/server # reset-all-memory-errors
UCS-A/chassis/server* # commit-buffer
UCS-A/chassis/server #
```

DIMM のブラックリスト化

Cisco UCS Manager で、デュアル インライン メモリ モジュール（DIMM）の状態は、SEL イベント レコードに基づいています。メモリ テストの実行中に BIOS で修正不可能なメモリ エラーに遭遇した場合、DIMM は不良としてマークされます。不良な DIMM は機能しないデバイスと見なされます。

DIMM のブラックリスト化を有効にすると、Cisco UCS Manager はメモリ テスト実行メッセージをモニタし、DIMM SPD データ内でメモリ エラーに遭遇した DIMM をブラックリストに載せます。これにより、ホストは修正不可能な ECC エラーに遭遇した DIMM をマップから外すことができます。

DIMM のブラックリストのイネーブル化

メモリ ポリシーは、Cisco UCS ドメイン の既存のサーバ、およびメモリ ポリシーを設定した後で追加されたサーバに適用できるグローバル ポリシーです。

（注）

- この機能は、Cisco UCS B シリーズ ブレード サーバおよび UCS C シリーズ ラック サーバの両方でサポートされています。

  （注） Cisco UCS C シリーズ 420 M3 ラック サーバはこの機能をサポートしていません。

- このグローバル ポリシーをサービス プロファイルに追加することはできません。

はじめる前に

- Cisco B シリーズ ブレード サーバの場合、サーバ ファームウェアはリリース 2.2(1) 以降のリリースである必要があります。
- シスコ C シリーズ ラック サーバの場合、サーバ ファームウェアはリリース 2.2(3) である必要があります。
- 次の権限のいずれかでログインする必要があります。
  - Admin
  - サーバ ポリシー
  - サーバ プロファイルのサーバ ポリシー

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** /	ルート組織モードを開始します。
ステップ 2	UCS-A /org # **memory-config-policy default**	グローバル メモリ ポリシーのメモリ ポリシー モードを開始します。
ステップ 3	UCS-A /org/memory-config-policy # **set blacklisting enabled**	DIMM のブラックリストは、ドメイン レベル ポリシーで有効化され、これらの変更は、その特定のドメイン内のすべてのサーバに適用されます。 （注） サーバの Cisco IMC が DIMM のブラックリストをサポートしない場合、情報レベルのエラーが生成されます。

	コマンドまたはアクション	目的
ステップ 4	UCS-A /org/memory-config-policy* # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、DIMM のブラックリストをイネーブルにする例を示します。

```
UCS-A# scope org /
UCS-A /chassis/org # scope memory-config-policy default
UCS-A /chassis/org/memory-config-policy # set blacklisting enabled
UCS-A /chassis/org/memory-config-policy* # commit-buffer
UCS-A /chassis/org/memory-config-policy #
UCS-A /chassis/org/memory-config-policy # show detail

Memory Config Policy:
    Blacklisting: enabled
```

Serial over LAN ポリシーの設定

Serial over LAN ポリシーの概要

このポリシーは、このポリシーを使用するサービス プロファイルと関連付けられているすべてのサーバに対する Serial over LAN 接続の設定を行います。デフォルトでは、Serial over LAN 接続は無効になります。

Serial over LAN ポリシーを実装する場合は、IPMI プロファイルも作成することをお勧めします。

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

Serial over LAN ポリシーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **create sol-policy** *policy-name*	Serial over LAN ポリシーを作成し、組織 Serial over LAN ポリシー モードを開始します。
ステップ 3	UCS-A /org/sol-policy # **set descr** *description*	（任意） ポリシーの説明を記します。

	コマンドまたはアクション	目的
		（注） 説明にスペース、特殊文字、または句読点が含まれている場合は、説明を引用符で括る必要があります。引用符は、**show** コマンド出力の説明フィールドには表示されません。
ステップ 4	UCS-A /org/sol-policy # **set speed** {**115200** | **19200** | **38400** | **57600** | **9600**}	シリアル ボー レートを指定します。
ステップ 5	UCS-A /org/sol-policy # {**disable** | **enable**}	Serial over LAN ポリシーをディセーブルまたはイネーブルにします。デフォルトでは、Serial over LAN ポリシーはディセーブルです。ポリシーを適用する前にイネーブルにする必要があります。
ステップ 6	UCS-A /org/sol-policy # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、Sol9600 という名前の Serial over LAN ポリシーを作成し、ポリシーの説明を指定し、速度を 9,600 ボーに設定し、ポリシーをイネーブルにし、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org* # create sol-policy Sol9600
UCS-A /org/sol-policy* # set descr "Sets serial over LAN policy to 9600 baud."
UCS-A /org/sol-policy* # set speed 9600
UCS-A /org/sol-policy* # enable
UCS-A /org/sol-policy* # commit-buffer
UCS-A /org/sol-policy #
```

Serial over LAN ポリシーの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **show sol-policy** *policy-name*	（create sol-config コマンドで設定された）Serial over LAN 定義を表示します。Serial over LAN 定義が設定されていない場合、およびポリシーが（set sol-policy コマンドを使用して）設定されている場合、ポリシーが表示されます。

次に、Sol9600 という Serial over LAN ポリシーの Serial over LAN 情報を表示する例を示します。

```
UCS-A# scope org /
UCS-A /org # show sol-policy Sol9600

SOL Policy:
Full Name: Sol9600
SOL State: Enable
Speed: 9600
Description:
```

Serial over LAN ポリシーの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **delete sol-policy** *policy-name*	指定された Serial over LAN ポリシーを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、Sol9600 という名前の Serial over LAN ポリシーを削除し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org* # delete sol-policy Sol9600
UCS-A /org* # commit-buffer
UCS-A /org #
```

サーバ自動構成ポリシーの設定

サーバ自動構成ポリシーの概要

Cisco UCS Manager では、このポリシーを使用して、新しいサーバの設定方法を決定します。サーバ自動構成ポリシーを作成すると、新しいサーバの起動時に次の処理が行われます。

1. サーバに対してサーバ自動構成ポリシーの資格認定が実行されます。
2. 必要な資格を満たしている場合、サーバは、サーバ自動構成ポリシーで設定された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と関連付けられます。そのサービス プロファイルの名前は、Cisco UCS Manager によって付与されるサーバの名前に基づきます。

3 サービス プロファイルは、サーバ自動構成ポリシーで設定された組織に割り当てられます。

サーバ自動構成ポリシーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **create server-autoconfig-policy** *policy-name*	サーバ自動構成ポリシーを指定されたポリシー名で作成し、組織サーバ自動構成ポリシー モードを開始します。
ステップ 3	UCS-A /org/server-autoconfig-policy # **set descr** *description*	（任意） ポリシーの説明を記します。 （注） 説明にスペース、特殊文字、または句読点が含まれている場合は、説明を引用符で括る必要があります。引用符は、**show** コマンド出力の説明フィールドには表示されません。
ステップ 4	UCS-A /org/server-autoconfig-policy # **set destination org** *org-name*	（任意） サーバを使用する組織を指定します。
ステップ 5	UCS-A /org/server-autoconfig-policy # **set qualifier** *server-qual-name*	（任意） サーバの資格認定にサーバプール ポリシー資格情報を使用するように指定します。
ステップ 6	UCS-A /org/server-autoconfig-policy # **set template** *profile-name*	（任意） サーバのサービス プロファイル インスタンスを作成するために使用するサービス プロファイル テンプレートを指定します。
ステップ 7	UCS-A /org/server-autoconfig-policy # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、AutoConfigFinance というサーバ自動構成ポリシーを作成し、ポリシーに説明を加え、宛先組織として finance を、サーバ プール ポリシー資格情報として ServPoolQual22 を、サービス プロファイル テンプレートとして ServTemp2 を指定し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org* # create server-autoconfig-policy AutoConfigFinance
```

```
UCS-A /org/server-autoconfig-policy* # set descr "Server Autoconfiguration Policy for
Finance"
UCS-A /org/server-autoconfig-policy* # set destination org finance
UCS-A /org/server-autoconfig-policy* # set qualifier ServPoolQual22
UCS-A /org/server-autoconfig-policy* # set template ServTemp2
UCS-A /org/server-autoconfig-policy* # commit-buffer
UCS-A /org/server-autoconfig-policy #
```

サーバ自動構成ポリシーの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **delete server-autoconfig-policy** *policy-name*	指定されたサーバ自動構成ポリシーを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、AutoConfigFinance という名前のサーバ自動構成ポリシーを削除し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org* # delete server-autoconfig-policy AutoConfigFinance
UCS-A /org* # commit-buffer
UCS-A /org #
```

サーバ ディスカバリ ポリシーの設定

サーバ ディスカバリ ポリシーの概要

サーバディスカバリ ポリシーは、新しいUCSブレードサーバ、UCS Mini、またはUCS Mシリーズ モジュラ サーバを追加したときにUCS Managerがどのように対応するかを決定します。サーバディスカバリ ポリシーを作成する場合、サーバがシャーシに追加されたときに、システムにより詳細なディスカバリを行うのか、または、ユーザがまず新しいサーバを確認する必要があるのかどうかを制御できます。デフォルトでは、システムにより完全なディスカバリが実行されます。

サーバディスカバリ ポリシーを作成した場合は、新しいサーバを起動すると次の処理が行われます。

1 サーバに対してサーバ ディスカバリ ポリシーの資格認定が行われます。

2 サーバが必要な資格情報と一致する場合、Cisco UCS Manager はサーバに次の処理を適用します。

- この処理に関して選択されたオプションに応じて、UCS Manager が新しいサーバをただちに検出するか、または新しいサーバに対するユーザの確認応答を待機する
- サーバにスクラブ ポリシーを適用する

重要 Cisco UCS Manager リリース 2.2(4) では、ブロック サイズが 4K のドライブはブレード サーバではサポートされませんが、ラックマウント サーバではサポートされます。ブロック サイズが 4 K のドライブがブレード サーバに挿入された場合、検出は失敗し、次のエラー メッセージが表示されます。

システムから SCSI デバイス情報を取得できません（Unable to get Scsi Device Information from the system）
このエラーが発生した場合は、次の手順を実行します。

1 4 K のドライブを取り外します。

2 サーバを再認識します。

注：サーバを再認識すると、サーバはリブートし、その結果、サービスは失われます。

サーバ ディスカバリ ポリシーの設定

はじめる前に

このポリシーとサーバ プールを関連付ける予定がある場合は、サーバ プール ポリシー資格情報を作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org /**	ルート組織モードを開始します。 （注） シャーシディスカバリ ポリシーは、ルート組織からしかアクセスできません。
ステップ 2	UCS-A /org # **create server-disc-policy** *policy-name*	サーバ ディスカバリ ポリシーを指定されたポリシー名で作成し、組織サーバ ディスカバリ ポリシー モードを開始します。
ステップ 3	UCS-A /org/server-disc-policy # **set action** {**diag** | **immediate** | **user-acknowledged**}	システムが新しいサーバの検出を試みるタイミングを指定します。

	コマンドまたはアクション	目的
ステップ 4	UCS-A /org/chassis-disc-policy #**set descr** *description*	（任意） サーバ ディスカバリ ポリシーに説明を加えます。 （注） 説明にスペース、特殊文字、または句読点が含まれている場合は、説明を引用符で括る必要があります。引用符は、**show** コマンド出力の説明フィールドには表示されません。
ステップ 5	UCS-A /org/server-disc-policy # **set qualifier** *qualifier*	（任意） 指定されたサーバ プール ポリシー資格情報をこのポリシーとサーバ プールを関連付けるために使用します。
ステップ 6	UCS-A /org/server-disc-policy # **set scrub-policy**	このポリシーが使用するスクラブ ポリシーを指定します。スクラブ ポリシーは、検出時にサーバのディスク ドライブをきれいにスクラブするかどうかを定義します。
ステップ 7	UCS-A /org/server-disc-policy # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、ServDiscPolExample という名前のサーバ ディスカバリ ポリシーを作成し、すぐに新しいサーバを検出するように設定し、ポリシーについて説明を加え、サーバプール ポリシー資格情報とスクラブ ポリシーを指定し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # create server-disc-policy ServDiscPolExample
UCS-A /org/server-disc-policy* # set action immediate
UCS-A /org/server-disc-policy* # set descr "This is an example server discovery policy."
UCS-A /org/server-disc-policy* # set qualifier ExampleQual
UCS-A /org/server-disc-policy* # set scrub-policy NoScrub
UCS-A /org/server-disc-policy # commit-buffer
```

次の作業

サーバ ディスカバリ ポリシーをサービス プロファイルとテンプレートのうち一方、または両方に含めます。

サーバ ディスカバリ ポリシーの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / と入力します。
ステップ 2	UCS-A /org # **Delete server-disc-policy** *policy-name*	指定したサーバ ディスカバリ ポリシーを削除します。
ステップ 3	UCS-A /org/server-disc-policy # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、ServDiscPolExample という名前のサーバ ディスカバリ ポリシーを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # delete server-disc-policy ServDiscPolExample
UCS-A /org* # commit-buffer
UCS-A /org #
```

サーバ継承ポリシーの設定

サーバ継承ポリシーの概要

このポリシーは、サーバ用のサービス プロファイルを作成するために、サーバ ディスカバリ プロセス中に呼び出されます。このポリシーから作成されたサービス プロファイルはすべて、製造元でブレードに設定された値を使用します。このポリシーは次の機能を実行します。

- サーバのインベントリの分析
- 選択された組織へのサーバの割り当て（設定されている場合）
- 製造元でサーバに設定された ID を使って、このサーバのサービス プロファイルを作成

このポリシーを使って作成したサービス プロファイルは他のサーバに移行できません。

サーバ継承ポリシーの設定

VIC アダプタが搭載されたブレード サーバまたはラックマウント サーバ（Cisco UCS M81KR 仮想インターフェイス カードなど）、サーバのアイデンティティ値が製造時にサーバ ハードウェア

に書き込まれていません。その結果、アダプタのアイデンティティは、デフォルト プールから取得する必要があります。デフォルト プールに、サーバに割り当てるのに十分なエントリが格納されていない場合、サービス プロファイルの関連付けが設定エラーで失敗します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **create server-inherit-policy** *policy-name*	サーバ継承ポリシーを指定されたポリシー名で作成し、組織サーバ継承ポリシーモードを開始します。
ステップ 3	UCS-A /org/server-inherit-policy # **set descr** *description*	（任意） ポリシーの説明を記します。 （注） 説明にスペース、特殊文字、または句読点が含まれている場合は、説明を引用符で括る必要があります。引用符は、**show** コマンド出力の説明フィールドには表示されません。
ステップ 4	UCS-A /org/server-inherit-policy # **set destination org** *org-name*	（任意） サーバを使用する組織を指定します。
ステップ 5	UCS-A /org/server-inherit-policy # **set qualifier** *server-qual-name*	（任意） サーバの資格認定にサーバ プール ポリシー資格情報を使用するように指定します。
ステップ 6	UCS-A /org/server-inherit-policy # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、InheritEngineering という名前のサーバ継承ポリシーを作成し、ポリシーに説明を加え、宛先組織として engineering を、サーバ プール ポリシー資格情報として ServPoolQual22 を指定し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org* # create server-inherit-policy InheritEngineering
UCS-A /org/server-inherit-policy* # set descr "Server Inheritance Policy for Engineering"
UCS-A /org/server-inherit-policy* # set destination org engineering
UCS-A /org/server-inherit-policy* # set qualifier ServPoolQual22
UCS-A /org/server-inherit-policy* # commit-buffer
UCS-A /org/server-inherit-policy #
```

サーバ継承ポリシーの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **delete server-inherit-policy** *policy-name*	指定されたサーバ継承ポリシーを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、InheritEngineering という名前のサーバ継承ポリシーを削除し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org* # delete server-inherit-policy InheritEngineering
UCS-A /org* # commit-buffer
UCS-A /org #
```

サーバ プール ポリシーの設定

サーバ プール ポリシーの概要

このポリシーはサーバ ディスカバリ プロセス中に呼び出されます。これは、サーバ プール ポリシー資格情報により、サーバと、ポリシーで指定されたターゲット プールが一致した場合にどのような処理が行われるかを定義します。

サーバが複数のプールに適合したときに、これらのプールにサーバ プール ポリシーがあった場合、このサーバはこれらすべてのプールに追加されます。

サーバ プール ポリシーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **create pooling-policy** *policy-name*	サーバ プール ポリシーを指定された名前で作成し、組織プール ポリシー モードを開始します。
ステップ 3	UCS-A /org/pooling-policy # **set descr** *description*	（任意） サーバ プール ポリシーに説明を加えます。 （注） 説明にスペース、特殊文字、または句読点が含まれている場合は、説明を引用符で括る必要があります。引用符は、**show** コマンド出力の説明フィールドには表示されません。
ステップ 4	UCS-A /org/pooling-policy # **set pool** *pool-distinguished-name*	サーバ プール ポリシーで使用するサーバ プールを指定します。プールの完全識別名を指定する必要があります。
ステップ 5	UCS-A /org/pooling-policy # **set qualifier** *qualifier-name*	サーバ プール ポリシーで使用するサーバ プール修飾子を指定します。
ステップ 6	UCS-A /org/pooling-policy # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、ServerPoolPolicy4 という名前のサーバ プール ポリシーを作成し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # create pooling-policy ServerPoolPolicy4
UCS-A /org/pooling-policy* # set pool org-root/compute-pool-pool3
UCS-A /org/pooling-policy* # set qualifier ServPoolQual8
UCS-A /org/pooling-policy* # commit-buffer
UCS-A /org/pooling-policy #
```

サーバ プール ポリシーの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / と入力します。
ステップ 2	UCS-A /org # **delete pooling-policy** *policy-name*	指定したサーバ プール ポリシーを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、ServerPoolPolicy4 という名前のサーバ プール ポリシーを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # delete pooling-policy ServerPoolPolicy4
UCS-A /org/pooling-policy* # commit-buffer
UCS-A /org/pooling-policy #
```

サーバ プール ポリシーの資格情報の設定

サーバ プール ポリシー資格情報の概要

このポリシーは、ディスカバリ プロセス中に実行されたサーバのインベントリに基づいて、サーバを資格認定します。資格情報は、サーバが選択基準を満たすかどうかを判断するために、ポリシーで設定されたルールです。たとえば、データセンター プールのサーバの最小メモリ容量を指定するルールを作成できます。

資格情報は、サーバプールポリシーだけではなく、その他のポリシーでも、サーバを配置するために使用されます。たとえば、サーバがある資格ポリシーの基準を満たしている場合、このサーバを 1 つ以上のサーバ プールに追加したり、自動的にサービス プロファイルと関連付けたりできます。

サーバ プール ポリシー資格情報を使用すると、次の基準に従ってサーバを資格認定できます。

- アダプタのタイプ
- シャーシの場所
- メモリのタイプと設定

- 電源グループ
- CPU のコア数、タイプ、および設定
- ストレージの設定と容量
- サーバのモデル

実装によっては、サーバプールポリシー資格情報を使用して、次を含む複数のポリシーを設定する必要があります。

- 自動構成ポリシー
- シャーシ ディスカバリ ポリシー
- サーバ ディスカバリ ポリシー
- サーバ継承ポリシー
- サーバ プール ポリシー

サーバ プール ポリシー資格情報の作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に **/** を入力します。
ステップ 2	UCS-A /org # **create server-qual** *server-qual-name*	サーバ プール資格情報を指定された名前で作成し、組織サーバ資格情報モードを開始します。
ステップ 3	UCS-A /org/server-qual # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、ServPoolQual22 という名前のサーバ プール資格情報を作成し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org* # create server-qual ServPoolQual22
UCS-A /org/server-qual* # commit-buffer
UCS-A /org/server-qual #
```

次の作業

次のサーバ コンポーネントの 1 つ以上の資格情報を設定します。

- アダプタ資格情報

- シャーシ資格情報
- メモリ資格情報
- 電源グループ資格情報
- プロセッサ資格情報
- ストレージ資格情報

サーバ プール ポリシーの資格情報の削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **delete server-qual** *server-qual-name*	指定されたサーバ プール資格情報を削除します。
ステップ 3	UCS-A /org/server-qual # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、ServPoolQual22 という名前のサーバ プール資格情報を削除し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org* # delete server-qual ServPoolQual22
UCS-A /org* # commit-buffer
UCS-A /org #
```

アダプタ資格情報の作成

はじめる前に

サーバ プール ポリシー資格情報を作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **scope server-qual** *server-qual-name*	指定したサーバ プール ポリシー資格情報で組織サーバ資格情報モードを開始します。
ステップ 3	UCS-A /org/server-qual # **create adapter**	アダプタ資格情報を作成し、組織サーバ資格情報アダプタ モードを開始します。
ステップ 4	UCS-A /org/server-qual/adapter # **create cap-qual** *adapter-type*	指定されたアダプタ タイプのアダプタ容量資格を作成して、組織サーバ資格アダプタ容量資格情報モードを開始します。*adapter-type* 引数には、次の任意の値を設定できます。 • **fcoe**：Fibre Channel over Ethernet • **non-virtualized-eth-if**：非仮想化イーサネット インターフェイス • **non-virtualized-fc-if**：非仮想化ファイバ チャネル インターフェイス • **path-encap-consolidated**：パス カプセル化統合 • **path-encap-virtual**：パス カプセル化仮想 • **protected-eth-if**：保護されたイーサネット インターフェイス • **protected-fc-if**：保護されたファイバ チャネル インターフェイス • **protected-fcoe**：保護された Fibre Channel over Ethernet • **virtualized-eth-if**：仮想化イーサネット インターフェイス • **virtualized-fc-if**：仮想化ファイバ チャネル インターフェイス • **virtualized-scsi-if**：仮想化 SCSI インターフェイス
ステップ 5	UCS-A /org/server-qual/adapter/cap-qual	選択したアダプタ タイプの最大容量を指定します。

	コマンドまたはアクション	目的
	# **set maximum** {*max-cap* | **unspecified**}	
ステップ 6	UCS-A /org/server-qual/adapter/cap-qual # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、非仮想化イーサネット インターフェイスのアダプタ資格情報を作成して設定し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # scope server-qual ServPoolQual22
UCS-A /org/server-qual # create adapter
UCS-A /org/server-qual/adapter* # create cap-qual non-virtualized-eth-if
UCS-A /org/server-qual/adapter/cap-qual* # set maximum 2500000000
UCS-A /org/server-qual/adapter/cap-qual* # commit-buffer
UCS-A /org/server-qual/adapter/cap-qual #
```

アダプタ資格情報の削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **scope server-qual** *server-qual-name*	指定したサーバ プール ポリシー資格情報で組織サーバ資格情報モードを開始します。
ステップ 3	UCS-A /org/server-qual # **delete adapter**	サーバ プール ポリシー資格情報からアダプタ資格情報を削除します。
ステップ 4	UCS-A /org/server-qual # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、ServPoolQual22 という名前のサーバ プール ポリシー資格情報からアダプタ資格情報を削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # scope server-qual ServPoolQual22
UCS-A /org/server-qual # delete adapter
UCS-A /org/server-qual* # commit-buffer
UCS-A /org/server-qual #
```

シャーシ資格情報の設定

はじめる前に

サーバ プール ポリシー資格情報を作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に **/** を入力します。
ステップ 2	UCS-A /org # **scope server-qual** *server-qual-name*	指定したサーバ プール ポリシー資格情報で組織サーバ資格情報モードを開始します。
ステップ 3	UCS-A /org/server-qual # **create chassis** *min-chassis-num max-chassis-num*	指定されたシャーシ範囲のシャーシ資格情報を作成し、組織サーバ資格情報シャーシ モードを開始します。
ステップ 4	UCS-A /org/server-qual/chassis # **create slot** *min-slot-num max-slot-num*	指定されたスロット範囲のシャーシ スロット資格情報を作成し、組織サーバ資格情報シャーシ スロット モードを開始します。
ステップ 5	UCS-A /org/server-qual/chassis/slot # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、シャーシ 1 および 2 のスロット 1 ～ 4 にシャーシ資格情報を設定し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org* # scope server-qual ServPoolQual22
UCS-A /org/server-qual* # create chassis 1 2
UCS-A /org/server-qual/chassis* # create slot 1 4
UCS-A /org/server-qual/chassis/slot* # commit-buffer
UCS-A /org/server-qual/chassis/slot #
```

シャーシ資格情報の削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に **/** を入力します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /org # **scope server-qual** *server-qual-name*	指定したサーバ プール ポリシー資格情報で組織サーバ資格情報モードを開始します。
ステップ 3	UCS-A /org/server-qual # **delete chassis** *min-chassis-num max-chassis-num*	指定されたシャーシ範囲のシャーシ資格情報を削除します。
ステップ 4	UCS-A /org/server-qual # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、シャーシ 1 および 2 のシャーシ資格情報を削除し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # scope server-qual ServPoolQual22
UCS-A /org/server-qual # delete chassis 1 2
UCS-A /org/server-qual* # commit-buffer
UCS-A /org/server-qual #
```

CPU 資格情報の作成

はじめる前に

サーバ プール ポリシー資格情報を作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **scope server-qual** *server-qual-name*	指定したサーバプールポリシー資格情報で組織サーバ資格情報モードを開始します。
ステップ 3	UCS-A /org/server-qual # **create cpu**	CPU 資格情報を作成し、組織サーバ資格情報プロセッサ モードを開始します。
ステップ 4	UCS-A /org/server-qual/cpu # **set arch** {**any** | **dual-core-opteron** | **intel-p4-c** | **opteron** | **pentium-4** | **turion-64** | **xeon** | **xeon-mp**}	プロセッサのアーキテクチャ タイプを指定します。

	コマンドまたはアクション	目的
ステップ 5	UCS-A /org/server-qual/cpu # **set maxcores** {*max-core-num* | **unspecified**}	プロセッサの最大コア数を指定します。
ステップ 6	UCS-A /org/server-qual/cpu # **set mincores** {*min-core-num* | **unspecified**}	プロセッサの最小コア数を指定します。
ステップ 7	UCS-A /org/server-qual/cpu # **set maxprocs** {*max-proc-num* | **unspecified**}	プロセッサの最大数を指定します。
ステップ 8	UCS-A /org/server-qual/cpu # **set minprocs** {*min-proc-num* | **unspecified**}	プロセッサの最小数を指定します。
ステップ 9	UCS-A /org/server-qual/cpu # **set maxthreads** {*max-thread-num* | **unspecified**}	スレッドの最大数を指定します。
ステップ 10	UCS-A /org/server-qual/cpu # **set minthreads** {*min-thread-num* | **unspecified**}	スレッドの最小数を指定します。
ステップ 11	UCS-A /org/server-qual/cpu # **set stepping** {*step-num* | **unspecified**}	プロセッサのステッピング番号を指定します。
ステップ 12	UCS-A /org/server-qual/cpu # **set model-regex** *regex*	プロセッサ名が一致する必要のある正規表現を指定します。
ステップ 13	UCS-A /org/server-qual/cpu # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、CPU 資格情報を設定し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # scope server-qual ServPoolQual22
UCS-A /org/server-qual # create processor
UCS-A /org/server-qual/cpu* # set arch xeon
UCS-A /org/server-qual/cpu* # set maxcores 8
UCS-A /org/server-qual/cpu* # set mincores 4
UCS-A /org/server-qual/cpu* # set maxprocs 2
UCS-A /org/server-qual/cpu* # set minprocs 1
UCS-A /org/server-qual/cpu* # set maxthreads 16
UCS-A /org/server-qual/cpu* # set minthreads 8
UCS-A /org/server-qual/cpu* # set stepping 5
UCS-A /org/server-qual/cpu* # commit-buffer
UCS-A /org/server-qual/cpu #
```

CPU 資格情報の削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **scope server-qual** *server-qual-name*	指定したサーバ プール ポリシー資格情報で組織サーバ資格情報モードを開始します。
ステップ 3	UCS-A /org/server-qual # **delete cpu**	プロセッサ資格情報を削除します。
ステップ 4	UCS-A /org/server-qual # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、プロセッサの資格情報を削除し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # scope server-qual ServPoolQual22
UCS-A /org/server-qual # delete cpu
UCS-A /org/server-qual* # commit-buffer
UCS-A /org/server-qual #
```

電源グループ資格情報の作成

はじめる前に

サーバ プール ポリシー資格情報を作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **scope server-qual** *server-qual-name*	指定したサーバ プール ポリシー資格情報で組織サーバ資格情報モードを開始します。
ステップ 3	UCS-A /org/server-qual # **create power-group** *power-group-name*	指定された電源グループ名の電源グループ資格情報を作成します。

	コマンドまたはアクション	目的
ステップ 4	UCS-A /org/server-qual # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、powergroup1 という電源グループの電源グループ資格情報を設定し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # scope server-qual ServPoolQual22
UCS-A /org/server-qual # create power-group powergroup1
UCS-A /org/server-qual* # commit-buffer
UCS-A /org/server-qual #
```

電源グループ資格情報の削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **scope server-qual** *server-qual-name*	指定したサーバ プール ポリシー資格情報で組織サーバ資格情報モードを開始します。
ステップ 3	UCS-A /org/server-qual # **delete power-group** *power-group-name*	指定された電源グループ資格情報を削除します。
ステップ 4	UCS-A /org/server-qual # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、powergroup1 という電源グループの電源グループ資格情報を削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # scope server-qual ServPoolQual22
UCS-A /org/server-qual # delete power-group powergroup1
UCS-A /org/server-qual* # commit-buffer
UCS-A /org/server-qual #
```

メモリ資格情報の作成

はじめる前に

サーバ プール ポリシー資格情報を作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **scope server-qual** *server-qual-name*	指定したサーバプール ポリシー資格情報で組織サーバ資格情報モードを開始します。
ステップ 3	UCS-A /org/server-qual # **create memory**	メモリ資格情報を作成し、組織サーバ資格情報メモリ モードを開始します。
ステップ 4	UCS-A /org/server-qual/memory # **set clock** {*clock-num* | **unspec**}	メモリのクロック速度を指定します。
ステップ 5	UCS-A /org/server-qual/memory # **set maxcap** {*max-cap-num* | **unspec**}	メモリ アレイの最大容量を指定します。
ステップ 6	UCS-A /org/server-qual/memory # **set mincap** {*min-cap-num* | **unspec**}	メモリ アレイの最小容量を指定します。
ステップ 7	UCS-A /org/server-qual/memory # **set speed** {*speed-num* | **unspec**}	メモリ データ レートを指定します。
ステップ 8	UCS-A /org/server-qual/memory # **set units** {*unit-num* | **unspec**}	メモリ ユニット（メモリ基板にマウントされているDRAMチップ）の数を指定します。
ステップ 9	UCS-A /org/server-qual/memory # **set width** {*width-num* | **unspec**}	データ バスのビット幅を指定します。
ステップ 10	UCS-A /org/server-qual/memory # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、メモリ資格情報を作成して設定し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # scope server-qual ServPoolQual22
UCS-A /org/server-qual # create memory
UCS-A /org/server-qual/memory* # set clock 1067
UCS-A /org/server-qual/memory* # set maxcap 4096
UCS-A /org/server-qual/memory* # set mincap 2048
UCS-A /org/server-qual/memory* # set speed unspec
```

```
UCS-A /org/server-qual/memory* # set units 16
UCS-A /org/server-qual/memory* # set width 64
UCS-A /org/server-qual/memory* # commit-buffer
UCS-A /org/server-qual/memory #
```

メモリ資格情報の削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **scope server-qual** *server-qual-name*	指定したサーバ プール ポリシー資格情報で組織サーバ資格情報モードを開始します。
ステップ 3	UCS-A /org/server-qual # **delete memory**	メモリ資格情報を削除します。
ステップ 4	UCS-A /org/server-qual # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、メモリの資格情報を削除し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # scope server-qual ServPoolQual22
UCS-A /org/server-qual # delete memory
UCS-A /org/server-qual* # commit-buffer
UCS-A /org/server-qual #
```

物理的な資格情報の作成

はじめる前に

サーバ プール ポリシー資格情報を作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /org # **scope server-qual** *server-qual-name*	指定したサーバ プール ポリシー資格情報で組織サーバ資格情報モードを開始します。
ステップ 3	UCS-A /org/server-qual # **create physical-qual**	物理的な資格情報を作成し、組織サーバ資格情報物理モードを開始します。
ステップ 4	UCS-A /org/server-qual/physical-qual # **set model-regex** *regex*	モデル名が一致する必要のある正規表現を指定します。
ステップ 5	UCS-A /org/server-qual/physical-qual # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、物理的な資格情報を作成して設定し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # scope server-qual ServPoolQual22
UCS-A /org/server-qual # create physical-qual
UCS-A /org/server-qual/physical-qual* # set model-regex
UCS-A /org/server-qual/physical-qual* # commit-buffer
UCS-A /org/server-qual/physical-qual #
```

物理的な資格情報の削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **scope server-qual** *server-qual-name*	指定したサーバ プール ポリシー資格情報で組織サーバ資格情報モードを開始します。
ステップ 3	UCS-A /org/server-qual # **delete physical-qual**	物理的な資格情報を削除します。
ステップ 4	UCS-A /org/server-qual # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、物理的な資格情報を削除し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # scope server-qual ServPoolQual22
UCS-A /org/server-qual # delete physical-qual
UCS-A /org/server-qual* # commit-buffer
UCS-A /org/server-qual #
```

ストレージ資格情報の作成

はじめる前に

サーバ プール ポリシー資格情報を作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **scope server-qual** *server-qual-name*	指定したサーバ プール ポリシー資格情報で組織サーバ資格情報モードを開始します。
ステップ 3	UCS-A /org/server-qual # **create storage**	ストレージ資格情報を作成し、組織サーバ資格情報ストレージモードを開始します。
ステップ 4	UCS-A /org/server-qual/storage # **set blocksize** {*block-size-num* | **unknown**}	ストレージブロック サイズを指定します。
ステップ 5	UCS-A /org/server-qual/storage # **set diskless** {**no** | **unspecified** | **yes** }	使用できるストレージがディスクレスである必要があるかどうかを指定します。
ステップ 6	UCS-A /org/server-qual/storage # **set disktype** {**hdd** | **ssd** | **unspecified**}	使用できるディスクのタイプを指定します。次のオプションがあります。 • [未指定（Unspecified）]：どのディスク タイプも受け入れ可能です。 • [HDD]：ディスクは HDD にする必要があります。 • [SSD]：ディスクは SSD（SATA または SAS）にする必要があります。
ステップ 7	UCS-A /org/server-qual/storage # **set flexflash-num-cards** {*ff_card-num* | **unknown**}	FlexFlash カードの数を指定します。
ステップ 8	UCS-A /org/server-qual/storage # **set maxcap** {*max-cap-num* | **unknown**}	ストレージ アレイの最大容量を指定します。
ステップ 9	UCS-A /org/server-qual/storage # **set mincap** {*min-cap-num* | **unknown**}	ストレージ アレイの最小容量を指定します。

	コマンドまたはアクション	目的
ステップ 10	UCS-A /org/server-qual/storage # **set numberofblocks** {*block-num* | **unknown**}	ブロック数を指定します。
ステップ 11	UCS-A /org/server-qual/storage # **set perdiskcap** {*disk-cap-num* | **unknown**}	ディスク単位の容量を指定します。
ステップ 12	UCS-A /org/server-qual/storage # **set units** {*unit-num* | **unspecified**}	ストレージ デバイス数を指定します。
ステップ 13	UCS-A /org/server-qual/storage # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、ストレージ資格情報を作成および設定し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org # scope server-qual ServPoolQual22
UCS-A /org/server-qual # create storage
UCS-A /org/server-qual/storage* # set blocksize 512
UCS-A /org/server-qual/storage* # set disktype hdd
UCS-A /org/server-qual/storage* # set maxcap 420000
UCS-A /org/server-qual/storage* # set mincap 140000
UCS-A /org/server-qual/storage* # set numberofblocks 287277984
UCS-A /org/server-qual/storage* # set perdiskcap 140000
UCS-A /org/server-qual/storage* # set units 1
UCS-A /org/server-qual/storage* # set flexflash-num-cards 2
UCS-A /org/server-qual/storage* # commit-buffer
UCS-A /org/server-qual/storage #
```

ストレージ資格情報の削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **scope server-qual** *server-qual-name*	指定したサーバ プール ポリシー資格情報で組織サーバ資格情報モードを開始します。
ステップ 3	UCS-A /org/server-qual # **delete storage**	ストレージ資格情報を削除します。
ステップ 4	UCS-A /org/server-qual/ # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、ストレージの資格情報を削除し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # scope server-qual ServPoolQual22
UCS-A /org/server-qual # delete storage
UCS-A /org/server-qual* # commit-buffer
UCS-A /org/server-qual #
```

vNIC/vHBA 配置ポリシーの設定

vNIC/vHBA 配置ポリシー

vNIC/vHBA 配置ポリシーは、次のことを決定するために使用されます。

- 仮想ネットワーク インターフェイス接続（vCon）をサーバ上の物理アダプタにマッピングする方法。
- 各 vCon に割り当てることのできる vNIC または vHBA のタイプ。

各 vNIC/vHBA 配置ポリシーには、物理アダプタの仮想表現である vCon が含まれます。vNIC/vHBA 配置ポリシーがサービス プロファイルに割り当てられ、サービス プロファイルがサーバに関連付けられると、vNIC/vHBA 配置ポリシー内の vCon が物理アダプタに割り当てられ、vNIC および vHBA がそれらの vCon に割り当てられます。

1 つのアダプタを持つブレード サーバやラック サーバの場合は、Cisco UCS がすべての vCon をそのアダプタに割り当てます。4 つのアダプタを持つサーバの場合は、Cisco UCS が vCon1 をアダプタ 1 に、vCon2 をアダプタ 2 に、vCon3 をアダプタ 3 に、vCon4 をアダプタ 4 に割り当てます。

2 つまたは 3 つのアダプタを搭載したブレード サーバまたはラック サーバの場合、Cisco UCS は、サーバのタイプと選択された仮想スロット マッピング スキーム（[ラウンドロビン] または [線形順序]）に基づいて vCon を割り当てます。使用可能なマッピング スキームの詳細については、vCon のアダプタへの配置, （556 ページ）を参照してください。

Cisco UCS は、vCon の割り当て後、vNIC と vHBA を各 vCon の [選択プリファレンス（Selection Preference）] に基づいて割り当てます。これは、次のいずれかになります。

- [すべて（All）]**all**：設定されたすべてのvNIC と vHBA は、明示的な割り当て、割り当て解除、動的のいずれかで vCon に割り当てられます。これがデフォルトです。
- [割り当てのみ（AssignedOnly）]**assigned-only**：vNICs と vHBA を vCon に明示的に割り当てる必要があります。サービス プロファイルや vNIC または vHBA のプロパティにより、明示的に割り当てることができます。
- [動的を除く（ExcludeDynamic）]**exclude-dynamic**：動的な vNIC や vHBA を vCon に割り当てることはできません。vCon は静的な vNIC と vHBA に使用可能で、割り当て解除または明示的な割り当てを行います。
- [割り当て解除を除く（ExcludeUnassigned）]**exclude-unassigned**：割り当て解除された vNIC や vHBA を vCon に割り当てることはできません。vCon は動的な vNIC や vHBA の他、明示的に割り当てられた静的な vNIC や vHBA に使用できます。

- [usNICを除く（Exclude usNIC）]**exclude-usnic**：Cisco usNIC を vCon に割り当てることはできません。vCon は、設定されているその他のすべての vNIC と vHBA に対しては使用可能です。これらの vNIC と vHBA が明示的に割り当てられているか、割り当て解除されているか、または動的かどうかは関係ありません。

（注） [usNICを除く（Exclude usNIC）]**exclude-usnic** に設定されている vCon に明示的に割り当てられている SRIOV usNIC は、引き続きその vCon に割り当てられたままになります。

vNIC/vHBA 配置ポリシーをサービス プロファイルに含めない場合、Cisco UCS Manager はデフォルトで、vCon マッピング スキームを [ラウンド ロビン（Round Robin）]、vNIC/vHBA 選択プリファレンスを [すべて（All）] に設定し、各アダプタの機能と相対的な処理能力に基づいて vNIC と vHBA をアダプタ間に配分します。

vCon のアダプタへの配置

Cisco UCS は、サービス プロファイル内のすべての vCon をサーバ上の物理アダプタにマッピングします。マッピングの実行方法、およびサーバ内の特定のアダプタへの vCon の割り当て方法は、次の条件によって決まります。

- サーバのタイプ。2 つのアダプタ カードを搭載した N20-B6620-2 および N20-B6625-2 ブレード サーバは、他のサポートされるラック サーバまたはブレード サーバとは異なるマッピング スキームを使用します。
- サーバ内のアダプタの数。
- vNIC/vHBA 配置ポリシー内の仮想スロット マッピング スキームの設定（該当する場合）。

vNIC および vHBA を vCon に割り当てるための vNIC/vHBA 選択環境設定を設定するときは、この配置を検討する必要があります。

（注） vCon のアダプタへの配置は、アダプタの PCIE スロット番号とは関係ありません。vCon の配置のために使用されるアダプタ番号は、アダプタの PCIE スロット番号ではなく、サーバ検出中にそれらに割り当てられる ID です。

N20-B6620-2 および N20-B6625-2 ブレード サーバでの vCon のアダプタへの配置

N20-B6620-2 および N20-B6625-2 ブレード サーバの場合は、2 つのアダプタを左から右に、vCon を右から左に数えます。これらのブレード サーバの 1 台が 1 つのアダプタを持つ場合は、Cisco UCS がすべての vCon をそのアダプタに割り当てます。サーバが 2 つのアダプタを持つ場合は、vCon の割り当ては仮想スロット マッピング スキームに基づいて行われます。

- [ラウンドロビン（Round Robin）]**round-robin**：Cisco UCS は vCon2 と vCon4 をアダプタ 1 に、vCon1 と vCon3 をアダプタ 2 に割り当てます。これがデフォルトです。
- [線形順序（LinearOrdered）]**linear-ordered**：Cisco UCS は vCon3 と vCon4 をアダプタ 1 に、vCon1 と vCon2 をアダプタ 2 に割り当てます。

vCon のアダプタへの配置（他のすべてのサポート対象サーバの場合）

N20-B6620-2 および N20-B6625-2 ブレード サーバに加え、Cisco UCS によりサポートされるその他すべてのサーバでは、vCon の割り当ては、サーバに搭載されるアダプタ数と仮想スロット マッピング スキームに応じて異なります。

1 つのアダプタを持つブレード サーバやラック サーバの場合は、Cisco UCS がすべての vCon をそのアダプタに割り当てます。4 つのアダプタを持つサーバの場合は、Cisco UCS が vCon1 をアダプタ 1 に、vCon2 をアダプタ 2 に、vCon3 をアダプタ 3 に、vCon4 をアダプタ 4 に割り当てます。

2 つまたは 3 つのアダプタを搭載したブレード サーバまたはラック サーバの場合、Cisco UCS は、選択した仮想スロット マッピング スキーム（[ラウンドロビン] または [線形順序]）に基づいて vCons を割り当てます。

表 *10*：ラウンドロビン マッピング スキームを使用した *vCon* のアダプタへの配置

アダプタの数	vCon1 の割り当て	vCon2 の割り当て	vCon3 の割り当て	vCon4 の割り当て
1	アダプタ1	アダプタ1	アダプタ1	アダプタ1
2	アダプタ1	アダプタ2	アダプタ1	アダプタ2
3	アダプタ1	アダプタ2	アダプタ3	アダプタ2
4	アダプタ1	アダプタ2	アダプタ3	アダプタ4

[ラウンドロビン（Round Robin）] はデフォルトのマッピング スキームです。

表 *11*：線形順序マッピング スキームを使用した *vCon* のアダプタへの配置

アダプタの数	vCon1 の割り当て	vCon2 の割り当て	vCon3 の割り当て	vCon4 の割り当て
1	アダプタ1	アダプタ1	アダプタ1	アダプタ1
2	アダプタ1	アダプタ1	アダプタ2	アダプタ2
3	アダプタ1	アダプタ2	アダプタ3	アダプタ3
4	アダプタ1	アダプタ2	アダプタ3	アダプタ4

（注） Cisco UCS B440 M2 ブレード サーバに搭載された 2 つのアダプタで vCon ポリシーを使用している場合は、次のマッピングに注意してください。

- 最初に vCon 2 からアダプタ 1 へのマッピング
- 2 番目に vCon 1 からアダプタ 2 へのマッピング

vNIC/vHBA の vCon への割り当て

Cisco UCS Manager には、vNIC/vHBA 配置ポリシーを使用して vNIC および vHBA を vCon に割り当てるオプションが 2 つあります。つまり、明示的割り当てと暗黙的割り当てです。

vNIC および vHBA の明示的割り当て

明示的割り当てでは、vCon を指定してから、vNIC または vHBA を割り当てるアダプタを指定します。この割り当てオプションは、サーバ上のアダプタ間への vNIC および vHBA の配布方法を決定する必要がある場合に使用します。

明示的割り当ての場合に、vCon と関連付けられる vNIC および vHBA を設定するには、次の手順を実行します。

- vCon 設定を任意の使用可能なオプションに設定します。vCon は、vNIC/vHBA 配置ポリシーを使用して設定するか、サーバに関連付けられているサービス プロファイルで設定できます。vCon で [すべて（All）] が設定されている場合でも、vNIC または vHBA をその vCon に明示的に割り当てることができます。
- vNIC および vHBA を vCon に割り当てます。この割り当ては、vNIC または vHBA の仮想ホストインターフェイス配置プロパティを使用して行うか、またはサーバに関連付けられているサービス プロファイルで設定できます

vNIC や vHBA をそれらのタイプに設定されていない vCon に割り当てようとすると、Cisco UCS Manager によって設定エラーが発生したことを示すメッセージが表示されます。

サービス プロファイルの関連付け中に、Cisco UCS Manager は、設定済みの vNIC および vHBA の割り当てを、サーバ内の物理的なアダプタ数および機能と比較して検証し、その後でポリシー内の設定に従って vNIC および vHBA を割り当てます。負荷分散は、このポリシー内で設定された vCon およびアダプタへの明示的な割り当てを元にして実行されます。

1 つ以上の vNIC または vHBA の割り当てがアダプタでサポートされない場合、Cisco UCS Manager は、サービス プロファイルに対する障害を発生させます。

vNIC および vHBA の暗黙的割り当て

暗黙的割り当てでは、Cisco UCS Manager は vCon を決定した後で、アダプタの機能とそれらの相対的な処理能力に基づいて vNIC または vHBA を割り当てるアダプタを決定します。この割り当

てオプションは、vNICまたはvHBAが割り当てられるアダプタがシステム設定で重要ではない場合に使用します。

暗黙的割り当ての場合に vCon を設定するには、次の手順を実行します。

- vCon 設定を [すべて（All）]、[動的を除く（Exclude Dynamic）]、または [未割り当てを除く（Exclude Unassigned）] に設定します。vCon は、vNIC/vHBA 配置ポリシーを使用して設定するか、サーバに関連付けられているサービス プロファイルで設定できます。
- vCon 設定を [割当済みのみ（Assigned Only）] にしないでください。この設定を使用して暗黙的割り当てを実行することはできません。
- vNIC または vHBA を vCon に割り当てないでください。

サービス プロファイルの関連付け中に、Cisco UCS Manager は、サーバ内の物理的なアダプタ数および機能を検証し、必要に応じて vNIC および vHBA を割り当てます。負荷分散はアダプタの機能に基づいて実行され、vNICおよびvHBAの配置は、システムで決定された実際の順序に従って実行されます。たとえば、1つのアダプタが他のアダプタより多くの vNIC を処理できる場合、そのアダプタにより多くの vNIC が割り当てられます。

サーバに設定されている数の vNIC および vHBA をアダプタでサポートできない場合、Cisco UCS Manager は、サービス プロファイルに対する障害を発生させます。

デュアル アダプタ環境での vNIC の暗黙的割り当て

各スロットにアダプタ カードが搭載されたデュアル スロット サーバで暗黙的な vNIC 割り当てを使用する場合、Cisco UCS Manager は通常 vNIC/vHBA を次のように割り当てます。

- サーバの両方のスロットに同じアダプタがある場合、Cisco UCS Manager は、各アダプタに vNIC と vHBA を半分ずつ割り当てます。
- サーバに 1 つの 非 VIC アダプタと 1 つの VIC アダプタがある場合、Cisco UCS Manager は、2 つの vNIC と 2 つの vHBA を非 VIC アダプタに割り当て、残りの vNIC と vHBA を VIC アダプタに割り当てます。
- サーバに 2 つの異なる VIC アダプタがある場合、Cisco UCS Manager は、2 つのアダプタの相対的な処理能力に基づいて、vNIC と vHBA を比例的に割り当てます。

次の例は、サポートされるアダプタ カードのさまざまな組み合わせに対して、Cisco UCS Manager が vNIC と vHBA をどのように割り当てるのか、その一般的な方法を示しています。

- 4 つ の vNIC と、2 つの Cisco UCS M51KR-B Broadcom BCM57711アダプタ（それぞれ 2 つの vNIC）を搭載したサーバを設定する場合、Cisco UCS Manager は 2 つの vNIC を各アダプタに割り当てます。
- 50 の vNIC と、Cisco UCS CNA M72KR-Eアダプタ（2 つの vNIC）および Cisco UCS M81KR 仮想インターフェイス カードアダプタ（128 の vNIC）を搭載したサーバを設定する場合、Cisco UCS Manager は、2 つの vNIC を Cisco UCS CNA M72KR-Eアダプタに割り当て、48 の vNIC を Cisco UCS M81KR 仮想インターフェイス カードアダプタに割り当てます。
- 150 の vNIC と、Cisco UCS M81KR 仮想インターフェイス カードアダプタ（128 の vNIC）および Cisco UCS VIC-1240 仮想インターフェイス カードアダプタ（256 の vNIC）を搭載した

サーバを設定する場合、Cisco UCS Manager は、50 の vNIC を Cisco UCS M81KR 仮想インターフェイス カードアダプタに割り当て、100 の vNIC を Cisco UCS VIC-1240 仮想インターフェイス カードアダプタに割り当てます。

（注） ファブリック フェールオーバー用の vNIC を設定した場合と、サーバ用に動的 vNIC を設定した場合は、この暗黙的割り当ての例外が発生します。

vNIC ファブリックのフェールオーバーが含まれる設定で、1 つのアダプタが vNIC のフェールオーバーをサポートしない場合、Cisco UCS Manager は、ファブリックのフェールオーバーが有効になっているすべての vNIC を、それらをサポートするアダプタに割り当てます。ファブリックのフェールオーバー用に設定された vNIC のみが設定に含まれる場合、それらをサポートしないアダプタに割り当てられる vNIC はありません。ファブリックのフェールオーバー用に設定された vNIC と設定されていない vNIC がある場合、Cisco UCS Manager は、すべてのフェールオーバー vNIC を、それらをサポートするアダプタに割り当て、上記の比率に従って、少なくとも 1 つの非フェールオーバー vNIC を、それらをサポートしないアダプタに割り当てます。

動的 vNIC が含まれる設定の場合、同じ暗黙的割り当てが実行されます。Cisco UCS Manager は、すべての動的 vNIC を、それらをサポートするアダプタに割り当てます。ただし、動的 vNIC と静的 vNIC の組み合わせを使用する場合は、少なくとも 1 つの静的 vNIC が動的 vNIC をサポートしないアダプタに割り当てられます。

vNIC/vHBA 配置ポリシーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **create vcon-policy** *policy-name*	指定された vNIC/vHBA 配置プロファイルを作成し、組織 vCon ポリシー モードを開始します。
ステップ 3	UCS-A /org/vcon-policy # **set descr** *description*	（任意） vNIC/vHBA 配置プロファイルの説明を提供します。 256 文字以内で入力します。次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。

	コマンドまたはアクション	目的
		（注） 説明にスペース、特殊文字、または句読点が含まれている場合は、説明を引用符で括る必要があります。引用符は、**show** コマンド出力の説明フィールドには表示されません。
ステップ 4	UCS-A /org/vcon-policy # **set mapping-scheme** {**round-robin** | **linear-ordered**}	（任意） 1 つのアダプタを持つブレード サーバやラック サーバの場合は、Cisco UCS がすべての vCon をそのアダプタに割り当てます。4 つのアダプタを持つサーバの場合は、Cisco UCS が vCon1 をアダプタ 1 に、vCon2 をアダプタ 2 に、vCon3 をアダプタ 3 に、vCon4 をアダプタ 4 に割り当てます。 2 つまたは 3 つのアダプタを持つブレード サーバやラック サーバの場合は、Cisco UCS が選択された仮想スロット マッピング スキームに基づいて、vCon を割り当てます。次のいずれかになります。 • [ラウンドロビン（Round Robin）]**round-robin**：2 つのアダプタ カードを持つサーバの場合は、Cisco UCS は vCon1 と vCon3 をアダプタ 1 に、vCon2 と vCon4 をアダプタ 2 に割り当てます。 3 つのアダプタ カードを持つサーバの場合は、Cisco UCS が vCon1 をアダプタ 1 に、vCon2 と vCon4 をアダプタ 2 に、vCon3 をアダプタ 3 に割り当てます。 これがデフォルトのスキームです。 • [線形順序（LinearOrdered）]**linear-ordered**：2 つのアダプタ カードを持つサーバの場合は、Cisco UCS は vCon1 と vCon2 をアダプタ 1 に、vCon3 と vCon4 をアダプタ 2 に割り当てます。 3 つのアダプタ カードを持つサーバの場合は、Cisco UCS が vCon1 をアダプタ 1 に、vCon2 をアダプタ 2 に割り当て、vCon3 と vCon4 をアダプタ 3 に割り当てます。 N20-B6620-2 および N20-B6625-2 ブレード サーバの場合は、2 つのアダプタを左から右に、vCon を右から左に数えます。これらのブレード サーバの 1 台が 1 つのアダプタを持つ場合は、Cisco UCS がすべての vCon をそのアダプタに割り当てます。サーバが 2 つのアダプタを持つ場合は、vCon の割り当ては仮想スロット マッピング スキームに基づいて行われます。 • [ラウンドロビン（Round Robin）]**round-robin**：Cisco UCS は vCon2 と vCon4 をアダプタ 1 に、vCon1 と vCon3 をアダプタ 2 に割り当てます。これがデフォルトです。

	コマンドまたはアクション	目的
		• [線形順序（LinearOrdered）]**linear-ordered**：Cisco UCS は vCon3 と vCon4 をアダプタ 1 に、vCon1 と vCon2 をアダプタ 2 に割り当てます。
ステップ 5	UCS-A /org/vcon-policy # **set vcon** {**1** | **2** | **3** | **4**} **selection** {**all** | **assigned-only** | **exclude-dynamic** | **exclude-unassigned**}	指定された vCon に選択プリファレンスを指定します。次のオプションがあります。 • [すべて（All）]**all**：設定されたすべてのvNIC と vHBA は、明示的な割り当て、割り当て解除、動的のいずれかで vCon に割り当てられます。これがデフォルトです。 • [割り当てのみ（AssignedOnly）]**assigned-only**：vNICs と vHBA を vCon に明示的に割り当てる必要があります。サービス プロファイルや vNIC または vHBA のプロパティにより、明示的に割り当てることができます。 • [動的を除く（ExcludeDynamic）]**exclude-dynamic**：動的な vNIC や vHBA を vCon に割り当てることはできません。vCon は静的な vNIC と vHBA に使用可能で、割り当て解除または明示的な割り当てを行います。 • [割り当て解除を除く（ExcludeUnassigned）]**exclude-unassigned**：割り当て解除された vNIC や vHBA を vCon に割り当てることはできません。vCon は動的な vNIC や vHBA の他、明示的に割り当てられた静的な vNIC や vHBA に使用できます。 • [usNICを除く（Exclude usNIC）]**exclude-usnic**：Cisco usNIC を vCon に割り当てることはできません。vCon は、設定されているその他のすべての vNIC と vHBA に対しては使用可能です。これらの vNIC と vHBA が明示的に割り当てられているか、割り当て解除されているか、または動的かどうかは関係ありません。 （注） [usNICを除く（Exclude usNIC）]**exclude-usnic** に設定されている vCon に明示的に割り当てられている SRIOV usNIC は、引き続きその vCon に割り当てられたままになります。
ステップ 6	UCS-A /org/vcon-policy # **commit-buffer**	トランザクションをコミットします。

次の例では、Adapter1All という名前の vNIC/vHBA 配置ポリシーを作成し、vCons マッピング方式を [線形順序（Linear Ordered）] に設定し、割り当てられた vNIC および vHBA のみがアダプタ 1 に配置できるよう指定し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # create vcon-policy Adapter1
UCS-A /org/vcon-policy* # set descr "This profile places all vNICs and vHBAs on adapter 1."
UCS-A /org/vcon-policy* # set mapping-scheme linear-ordered
UCS-A /org/vcon-policy* # set vcon 1 selection assigned-only
UCS-A /org/vcon-policy* # commit-buffer
UCS-A /org/vcon-policy* #
UCS-A /org #
```

vNIC/vHBA 配置ポリシーの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **delete vcon-policy** *policy-name*	指定した vNIC/vHBA 配置プロファイルを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをコミットします。

次に、Adapter1All という名前の vNIC/vHBA 配置プロファイルを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # delete vcon-policy Adapter1All
UCS-A /org* # commit-buffer
UCS-A /org #
```

vCon への vNIC の明示的割り当て

はじめる前に

vNIC/vHBA 配置ポリシーまたはサービス プロファイルで次のいずれかの値を使用して、vCon を設定します。

- [割り当て済みのみ（Assigned Only）]
- [ダイナミックを除外（Exclude Dynamic）]
- [未割り当てを除外（Exclude Unassigned）]

vCon で [すべて（All）] が設定されている場合、vNIC または vHBA をその vCon に明示的に割り当てることができます。しかし、この設定ではほとんど制御ができません。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	vCon に明示的に割り当てる vNIC があるサービス プロファイルを含む組織で組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	指定したサービスで組織サービス プロファイル モードを開始します。
ステップ 3	UCS-A /org/service-profile # **scope vnic** *vnic-name*	指定した vNIC で組織サービス プロファイル モードを開始します。
ステップ 4	UCS-A /org/service-profile/vnic # **set vcon** {**1** | **2** | **3** | **4** | **any**}	指定した vNIC の vCon（仮想ネットワーク インターフェイス接続）の配置を設定します。 いずれかの値を入力すると、Cisco UCS Manager は vNIC の割り当て先の vCon を判別できます。
ステップ 5	UCS-A /org/service-profile/vnic # **set order** {*order-num* | **unspecified**}	vNIC の目的の PCI 順序を指定します。 有効な値は 0 ～ 128 および未指定です。
ステップ 6	UCS-A /org/service-profile/vnic # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、vnic3 という vNIC の vCon 配置を 2 に設定し、目的の順序を 10 に設定し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # scope service-profile accounting
UCS-A /org/service-profile # scope vnic vnic3
UCS-A /org/service-profile/vnic # set vcon 2
UCS-A /org/service-profile/vnic* # set order 10
UCS-A /org/service-profile/vnic* # commit-buffer
UCS-A /org/service-profile/vnic #
```

vCon への vHBA の明示的割り当て

はじめる前に

vNIC/vHBA 配置ポリシーまたはサービス プロファイルで次のいずれかの値を使用して、vCon を設定します。

- [割り当て済みのみ（Assigned Only）]

- [ダイナミックを除外（Exclude Dynamic）]
- [未割り当てを除外（Exclude Unassigned）]

vCon で [すべて（All）] が設定されている場合、vNIC または vHBA をその vCon に明示的に割り当てることができます。しかし、この設定ではほとんど制御ができません。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	vCon に明示的に割り当てる vHBA があるサービス プロファイルを含む組織で組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	指定したサービスで組織サービス プロファイル モードを開始します。
ステップ 3	UCS-A /org/service-profile # **scope vhba** *vhba-name*	指定した vHBA で組織サービス プロファイル モードを開始します。
ステップ 4	UCS-A /org/service-profile/vhba # **set vcon** {**1** | **2** | **3** | **4** | **any**}	指定した vHBA の vCon（仮想ネットワーク インターフェイス接続）の配置を設定します。 いずれかの値を入力すると、Cisco UCS Manager は vHBA の割り当て先の vCon を判別できます。
ステップ 5	UCS-A /org/service-profile/vhba # **set order** {*order-num* | **unspecified**}	vHBA の目的の PCI 順序を指定します。 有効な順序番号値は 0 ～ 128 および未指定です。
ステップ 6	UCS-A /org/service-profile/vhba # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、vhba3 という vHBA の vCon 配置を 2 に設定し、目的の順序を 10 に設定し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # scope service-profile accounting
UCS-A /org/service-profile # scope vhba vhba3
UCS-A /org/service-profile/vhba # set vcon 2
UCS-A /org/service-profile/vhba* # set order 10
UCS-A /org/service-profile/vhba* # commit-buffer
UCS-A /org/service-profile/vhba #
```

ダイナミック vNIC の前にスタティック vNIC を配置

最適なパフォーマンスを得るために、スタティック vNIC とスタティック vHBA は、PCIe バス上のダイナミック vNIC の前に配置する必要があります。スタティック vNIC は、スタティック vNIC

および vHBA の両方を参照します。Cisco UCS Manager リリース 2.1 は、スタティックおよびダイナミック vNIC の順序に関する次の機能を備えています。

- Cisco UCS Manager リリース 2.1 にアップグレードした後、既存のサービス プロファイル（Cisco UCS Manager リリース 2.1 以前のリリースで定義されたプロファイル）に変更がない場合は、vNIC の順序は変更されません。
- Cisco UCS Manager リリース 2.1 へのアップグレード後、vNIC 関連の変更によって vNIC マップの順序が変更されます。その結果、すべてのダイナミック vNIC がスタティック vNIC の後に配置されます。
- Cisco UCS Manager リリース 2.1 で新しく作成されたサービス プロファイルでは、スタティック vNIC が常にダイナミック vNIC の前に順序付けられます。
- 上記の動作は、スタティック vNIC またはダイナミック vNIC の作成または削除の順番に依存しません。
- SRIOV 対応のサービス プロファイルの場合は、UCSM によって対応する仮想関数（VF）の前に vNIC 物理関数（PF）が挿入されます。この方式では、VF が PCIe バスおよび BDF 上の親 PF vNIC の近くに配置され、VF の継続的な増分順序になることが保証されます。

例

Cisco UCS Manager リリース 2.0 での当初のデバイス順序

```
dyn-vNIC-1 1
dyn-vNIC-2 2
```

Cisco UCS Manager リリース 2.0 での新たなデバイス順序（2 つのスタティック vNIC を追加）

```
dyn-vNIC-1 1
dyn-vNIC-2 2
eth-vNIC-1 3
eth-vNIC-2 4
```

Cisco UCS Manager リリース 2.1 へのアップグレード後（vNIC 関連の変更がサービス プロファイルで行われる前）

```
dyn-vNIC-1 1
dyn-vNIC-2 2
eth-vNIC-1 3
eth-vNIC-2 4
```

Cisco UCS Manager リリース 2.1 での新たなデバイス順序（ポリシー数を 2 から 4 に変更することによって 2 つのダイナミック vNIC を追加）

```
dyn-vNIC-1 3
dyn-vNIC-2 4
eth-vNIC-1 1
eth-vNIC-2 2
dyn-vNIC-3 5
dyn-vNIC-4 6
```

多機能 PCIe デバイスとしてのダイナミック vNIC

Cisco UCS Manager バージョン 2.1 は、0 機能デバイス（すべてのスタティック vNIC に対応する新しい BUS）としてスタティック vNIC をプロビジョニングします。多機能ダイナミック vNIC は、新しいバス スロットから最後のスタティック vNIC/vHBA の後に配置されます。

（注） Cisco UCS Manager バージョン 2.1 は、新しい StaticZero モードをサポートしています。

表 *12*：バージョンの互換性

Cisco UCS Manager		
Version 1.4 **方式：ZeroFunction**	**Version 2.0** **方式：ZeroFunction/MultiFunction**	**Version 2.1** **方式：ZeroFunction/MultiFunction/StaticZero**
スタティックおよびダイナミック vNIC はすべて、バス [0-57]、関数 [0] 上にあります。 < ZeroFunction モード >	スタティック vNIC およびダイナミック vNIC は、バス [0-57]、関数 [0-7] 上にあります。バス 0、関数 0 バス 0、関数 7 バス 1、関数 0 < MultiFunction モード >	スタティック vNIC または PF は、バス [0-57]、関数 [0] 上にあります。SRIOV：対応する VF が同一バスおよび関数 [1-255] 上にあります。 No-SRIOV：ダイナミック vNIC は、バス [0-57]、関数 [0-7] 上にあります。 < StaticZero モード>
	Balboa からのアップグレードでは、バスが <= 57 になるまで BDF の番号の付け直しは行われません（ZeroFunction モードのまま）。 デバイスが 58 台を超えると、MultiFunction モードに切り替わります。	Balboa からのアップグレードでは、バスが <= 57 になるまで BDF の番号の付け直しは行われません（ZeroFunction モードのまま）。デバイスが 58 台またはプラットフォーム固有の最大 PCIe バス数を超えるか、SRIOV 設定に変更されると、StaticZero モードに切り替わります。
		Cisco UCS Manager バージョン 2.0 からのアップグレードでは、BDF の番号の付け直しは行われません（ZeroFunction/MultiFunction モードのまま）。デバイスが 58 台またはプラットフォーム固有の最大 PCIe バス数を超えるか、SRIOV 設定に変更されると、StaticZero モードに切り替わります。

vNIC/vHBA ホスト ポートの配置

vNIC/vHBA を vCon に割り当てた後、それを特定のアダプタのホスト ポートのいずれかに配置できます。配置先のホスト ポートは明示的に指定するか、または Cisco UCS Manager により自動的にホスト ポートに vNICs/vHBA を割り当てることができます。

（注） Cisco UCS VIC 1340 および VIC 1380 アダプタをサポートするサーバへの vNIC/vHBA ホスト ポート配置を実行できます。

vNIC/vHBA のホスト ポート配置により、アダプタの vNIC/vHBA の順序が決まります。最初のホスト ポートに配置された vNIC/vHBA は最初に列挙され、2 番目のホスト ポートの vNIC/vHBA がそれに続きます。

ホスト ポート配置の設定

Cisco UCS VIC 1340 および VIC 1380 アダプタをサポートするサーバへの vNIC のホスト ポート配置を実行できます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルート組織モードを開始するには、*/* を *org-name* として入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	サービス プロファイルのサービス プロファイル組織モードを開始します。
ステップ 3	UCS-A /org/service-profile # **scope vnic** *vnic-name*	指定した vNIC で組織サービス プロファイル モードを開始します。
ステップ 4	UCS-A /org/service-profile/vnic # **set host-port** {1 | 2 | any}	指定した vNIC のホスト ポートを設定します。 **any** を入力すると、Cisco UCS Manager は vNIC の割り当て先のホスト ポートを判別できます。 ホスト ポートの配置をサポートしないアダプタ上で vNIC のホスト ポートを設定すると、[実際のホスト ポート（Actual Host Port）] パラメータは [なし（None）] を表示します。
ステップ 5	UCS-A /org/service-profile/vnic* # **commit-buffer**	トランザクションをシステム設定にコミットします。

	コマンドまたはアクション	目的
ステップ 6	UCS-A /org/service-profile/vnic # **show detail**	指定した vNIC に関する詳細を表示します。

次の例は、vnic3 という名前の vNIC をホスト ポート 2 に配置し、トランザクションをコミットし、ホスト ポートの情報を表示します。

```
UCS-A# scope org
UCS-A /org # scope service-profile SP-2
UCS-A /org/service-profile # scope vnic vnic3
UCS-A /org/service-profile/vnic # set host-port 2
UCS-A /org/service-profile/vnic* # commit-buffer
UCS-A /org/service-profile/vnic # show detail
vNIC:
    Name: vnic3
    Fabric ID: A
    Dynamic MAC Addr: 00:25:B5:13:13:11
    Desired Order: 2
    Actual Order: 3
    Desired VCon Placement: 1
    Actual VCon Placement: 1
    Desired Host Port: 2
    Actual Host Port: 2
...

UCS-A /org/service-profile/vnic #
```

CIMC マウント vMedia

スクリプト可能な vMedia の使用

Cisco UCS Manager では、リモート UCS サーバの vMedia デバイス ISO イメージをプロビジョニングできます。スクリプト可能な vMedia を使用して、リモート サーバに IMG または ISO イメージをマウントするようにプログラミングできます。CIMC マウント vMedia を使用すると、メディア接続を追加することなく、データセンター内の他のマウント メディア間で通信できるようになります。スクリプト可能な vMedia を使用すると、ブラウザを使用せずに仮想メディア デバイスを制御して、手動で各 UCS サーバを個別にマッピングできます。

スクリプト可能な vMedia は、NFS、CIFS、HTTP、および HTTPS の共有など、複数の共有タイプをサポートします。**スクリプト可能な vMedia** は、BIOS 設定により有効化し、Web GUI や CLI インターフェイスを介して設定します。

Cisco UCS Manager のスクリプト可能な vMedia は次の機能をサポートしています。

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

（注） Cisco UCS Manager によるスクリプト可能な vMedia のサポートは、CIMC にマッピングされているデバイスにのみ適用されます。既存の KVM ベースの vMedia デバイスはサポートされません。

次の条件に合致する場合、vMedia のマウントは失敗します。

1. vMedia ポリシー内のリモート vMedia イメージ ファイル名が [Service-Profile-Name] に設定されている。
2. サービス プロファイルの名前が変更されている。

これは、サービスプロファイルの名前を変更しても、vMediaポリシー内のリモートvMediaイメージ ファイル名は変更されないためです。イメージ ファイル名は引き続き、リモート デバイス上の古いイメージをポイントするため、検出できません。

CIMC vMedia ポリシーの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **create vmedia-policy** *policy-name*	指定されたポリシー名で vMedia ポリシーを作成します。
ステップ 3	UCS-A /org/vmedia-policy* # **create vmedia-mapping** *mapping -name*	指定されたマッピング名で vMedia ポリシーのサブディレクトリを作成します。
ステップ 4	UCS-A /org/vmedia-policy/vmedia-mapping # **set descr** *description*	（任意） vMedia ポリシーの説明を記入します。 （注） 説明にスペース、特殊文字、または句読点が含まれている場合は、説明を引用符で括る必要があります。引用符は、**show** コマンド出力の説明フィールドには表示されません。
ステップ 5	UCS-A /org/vmedia-policy/vmedia-mapping* # **set device type** *device-type*	マウントするリモート vMedia イメージ タイプを指定します。オプションは次のとおりです。 • **CDD** • **HDD**

	コマンドまたはアクション	目的
ステップ 6	UCS-A /org/vmedia-policy/vmedia-mapping* # **set image-file** *image-file-name*	リモート vMedia のイメージ ファイル名のタイプを指定します。
ステップ 7	UCS-A /org/vmedia-policy/vmedia-mapping* # **set image-path** *image-path*	リモート vMedia のイメージ パスを指定します。
ステップ 8	UCS-A /org/vmedia-policy/vmedia-mapping* # **set image-variable-name** {**none** | **service-profile-name**}	イメージに使用される名前を指定します。オプションは次のとおりです。 • [none]：手動でファイル名を入力します。 • [service-profile-name]：ポリシーが関連付けられたサービス プロファイルの名前を自動的に使用します。 （注） [image-variable-name] を [service-profile-name] として指定する場合、サービス プロファイルの名前を変更しないでください。サービス プロファイルの名前を変更すると、仮想メディア（vMedia）のマウントが失敗することがあります。
ステップ 9	UCS-A /org/vmedia-policy/vmedia-mapping* # **set mount-protocol** *mount-protocol*	リモート vMedia のマウント プロトコルを指定します。オプションは次のとおりです。 • **[CIFS]** • **NFS** • **HTTP** • **HTTPS**
ステップ 10	UCS-A /org/vmedia-policy/vmedia-mapping* # **set auth-option** { **default** | **none** | **ntlm** | **ntlmi** | **ntlmssp** | **ntlmsspi** | **ntlmv2** | **ntlmv2i**}	CIFS 認証オプションを指定します。このコマンドは、リモート vMedia マウント プロトコルとして CIFS を指定する場合にのみ使用できます。他のリモート vMedia マウント プロトコルを選択する場合は使用できません。CIFS 認証オプションは次のとおりです。 • [default]：NT LAN Manager のセキュリティ サポート プロバイダー（NTLMSSP）プロトコル。このオプションは、Windows 2008 R2 および Windows 2012 R2 でのみ使用します。

	コマンドまたはアクション	目的
		• [none]：認証は使用されません。 • [ntlm]：NT LAN Manager（NTLM）セキュリティ プロトコル。このオプションは、Windows 2008 R2 および Windows 2012 R2 でのみ使用します。 • [ntlmi]：NTLMi のセキュリティプロトコル。このオプションは、CIFS Windows サーバでデジタル署名が有効な場合にのみ使用します。 • [ntlmssp]：NT LAN Manager のセキュリティ サポート プロバイダー（NTLMSSP）プロトコル。このオプションは、Windows 2008 R2 および Windows 2012 R2 でのみ使用します。 • [ntlmsspi]：このオプションは、CIFS Windows サーバでデジタル署名が有効な場合のみ使用します。 • [ntlmv2]：NTLMv2 セキュリティ プロトコル。このオプションは、Samba Linux でのみ使用します。 • [ntlmv2i]：NTLMv2i のセキュリティ プロトコル。このオプションは、Samba Linux でのみ使用します。
ステップ 11	UCS-A /org/vmedia-policy/vmedia-mapping* # **set password**	リモート vMedia のイメージ パスワードを指定します。
ステップ 12	UCS-A /org/vmedia-policy/vmedia-mapping* # **set remote-ip** *remote-ip*	リモート vMedia のイメージ IP アドレスを指定します。
ステップ 13	UCS-A /org/vmedia-policy/vmedia-mapping* # **set user-id** *user-id*	vMedia デバイスをマウントするためのユーザ ID を指定します。
ステップ 14	UCS-A /org/vmedia-policy/vmedia-mapping* # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、vMediaPolicy2 という名前の vMedia ポリシーを作成し、リモート vMedia のデバイス タイプ、マウント プロトコル、イメージの場所を選択し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # create vmedia-policy vmediapolicy2
UCS-A /org/vmedia-policy* # create vmedia-mapping map1
UCS-A /org/vmedia-policy/vmedia-mapping* # set descr vmedia-map
UCS-A /org/vmedia-policy/vmedia-mapping* # set device-type cdd
UCS-A /org/vmedia-policy/vmedia-mapping* # set image-file-name win2011.iso
UCS-A /org/vmedia-policy/vmedia-mapping* # set image-path cifs
UCS-A /org/vmedia-policy/vmedia-mapping* # set image-variable-name service-profile-name
UCS-A /org/vmedia-policy/vmedia-mapping* # set mount-protocol cifs
UCS-A /org/vmedia-policy/vmedia-mapping* # set auth-option default
UCS-A /org/vmedia-policy/vmedia-mapping* # set password Password:
UCS-A /org/vmedia-policy/vmedia-mapping* # set remote-ip 172.41.1.158
UCS-A /org/vmedia-policy/vmedia-mapping* # set user-id Adminstrator
UCS-A /org/vmedia-policy/vmedia-mapping* # commit-buffer
```

（注） vMedia ポリシーが作成されると、[マウント時の再試行の失敗（Retry on Mount Fail）] オプションが [はい（Yes）] に設定されます。次に、[マウント時の再試行の失敗（Retry on Mount Fail）] オプションを [いいえ（No）] に変更する例を示します。

```
UCS-A# scope org /
UCS-A /org # create vmedia-policy vmediapolicy2
UCS-A /org/vmedia-policy* # set retry-on-mount-fail No
UCS-A /org/vmedia-policy* # commit-buffer
```

警告 [マウント時の再試行の失敗（Retry on Mount Fail）] オプションを [いいえ（No）] に設定すると、「**これにより、vMedia のマウントに失敗した場合のマウントの自動再試行が無効になります（This will disable automatic retry of mount in case of any vMedia mount failure）**」という警告メッセージが表示されます。

第 30 章

サーバ ブートの設定

この章の内容は、次のとおりです。

ブート ポリシー

Cisco UCS Manager を使用して、ブレード サーバ、ラック サーバ、およびモジュラ サーバのブート ポリシーを作成することができます。

Cisco UCS Manager ブート ポリシーは、BIOS 設定メニューのブート順序をオーバーライドし、次のことを決定します。

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

たとえば、関連するサーバをローカル ディスクや CD-ROM（VMedia）などのローカル デバイスから起動したり、SAN ブートや LAN（PXE）ブートを選択することができます。

1 つ以上のサービス プロファイルに関連付ける名前付きブート ポリシーを作成するか、または特定のサービス プロファイルに対するブート ポリシーを作成できます。ブート ポリシーを有効にするには、ブート ポリシーをサービス プロファイルに含め、このサービス プロファイルをサーバに関連付ける必要があります。サービス プロファイルにブート ポリシーを含めない場合、Cisco UCS Manager によってデフォルトのブート ポリシーが適用されます。

（注） ブート ポリシーに対する変更は、そのブート ポリシーを含んでいる、更新中のサービス プロファイル テンプレートを使って作成されたすべてのサーバに伝播されます。BIOS にブート順序情報を再書き込みするためのサービス プロファイルとサーバとの再関連付けは自動的にトリガーされます。

また、ブート ポリシーに次の内容を指定することもできます。

- ローカル LUN の名前。指定された名前は、展開される名前ではなく、ストレージ プロファイル内の論理名です。モジュラ サーバの場合、プライマリ名とセカンダリ名の両方を指定できます。他のサーバの場合は、プライマリ名のみを指定します。セカンダリ名を指定すると、設定エラーが発生します。
- JBOD ディスクからブートするための特定の JBOD ディスク番号。これは、モジュラ サーバではサポートされません。
- 下位互換性のための任意の LUN。ただし、これは非推奨です。その他のデバイスを正常にブートさせるには、ブート可能なイメージを保持していない必要があります。

UEFI ブート モード

Unified Extensible Firmware Interface（UEFI）は、オペレーティング システムとプラットフォーム ファームウェア間のソフトウェア インターフェイスを定義する仕様です。Cisco UCS Manager は、UEFI を使用して BIOS ファームウェア インターフェイスを置換します。これにより、BIOS は UEFI モードで動作すると同時に、レガシーもサポートできます。

ブート ポリシーを作成する場合、レガシー ブート モードまたは UEFI ブート モードのいずれかを選択できます。レガシー ブート モードはすべての Cisco UCS サーバでサポートされています。UEFI ブート モードは M3 および M4 サーバでのみサポートされており、UEFI セキュア ブート モードをイネーブルにします。

次の制限は、UEFI ブート モードに適用されます。

- UEFI ブート モードは Cisco UCS B シリーズ M3 および M4 ブレード サーバ、ならびに、Cisco UCS C シリーズ M3 および M4 ラック サーバでのみサポートされています。
- UEFI ブート モードは、次の組み合わせではサポートされません。

- Cisco UCS Manager と統合された Cisco UCS ブレード サーバおよびラック サーバ上の Gen-3 Emulex アダプタおよび QLogic アダプタ。
- Cisco UCS Manager と統合された Cisco UCS ラック サーバ上のすべてのアダプタに対する PXE ブート。
- Cisco UCS Manager と統合された Cisco UCS ラック サーバ上のすべてのアダプタに対する iSCSI ブート。

- 2 つの iSCSI LUN を使用して UEFI ブート モードを使用する場合は、Cisco UCS Manager による IQN サフィックス プールからの名前の選択を許可するのではなく、共通の iSCSI イニシエータ名を基盤となっている iSCSI eNIC の両方に適用されるサービス プロファイルに手動で指定する必要があります。共通の名前を指定しなかった場合は、Cisco UCS Manager は 2 番目の iSCSI LUN を検出できません。
- 同じサーバで UEFI とレガシー ブート モードを混在させることはできません。
- ブート ポリシーに設定されたブート デバイスにインストール済みの UEFI 対応オペレーティング システムがある場合にのみ、サーバは UEFI モードで正しく起動します。互換性のある OS が存在しない場合、ブート デバイスは [ブート順序の詳細（Boot Order Details）] 領域の [実際のブート順序（Actual Boot Order）] タブに表示されません。
- 一部の特殊なケースでは、UEFI ブート マネージャ エントリが BIOS NVRAM に正しく保存されなかったことが原因で、UEFI ブートが失敗することがあります。UEFI シェルを使用して UEFI ブート マネージャ エントリを手動で入力できます。この状況は、以下の場合に発生する可能性があります。
  - UEFI ブート モードがイネーブルになっているブレード サーバとサービス プロファイルの関連付けが解除されており、[機器（Equipment）] タブまたは前面パネルを使用してブレードの電源が手動で投入されている場合。
  - UEFI ブート モードがイネーブルになっているブレード サーバとサービス プロファイルの関連付けが解除されており、ダイレクト VIC ファームウェア アップグレードが試行された場合。
  - UEFI ブート モードがイネーブルになっているブレード サーバまたはラック サーバが SAN LUN でブートオフされ、サービス プロファイルが移行された場合。

UEFI セキュア ブート

Cisco UCS Manager は、Cisco UCS B シリーズ M3 および M4 ブレード サーバと Cisco UCS C シリーズ M3 および M4 ラック サーバ上での UEFI セキュア ブートをサポートしています。UEFI セキュア ブートがイネーブルの場合、すべての実行可能ファイル（ブート ローダ、アダプタ ドライバなど）はロードされる前に BIOS によって認証されます。認証されるには、イメージが Cisco 認証局（CA）または Microsoft CA によって署名される必要があります。

次の制限は、UEFI セキュア ブートに適用されます。

- UEFI ブート モードは、ブート ポリシーでイネーブルにする必要があります。
- Cisco UCS Manager ソフトウェアと BIOS ファームウェアは、リリース 2.2 以上である必要があります。

（注） UEFI ブート モードは、リリース 2.2(3a) 以降の Cisco UCS C シリーズ ラック サーバでサポートされます。

- ユーザ生成された暗号キーはサポートされません。
- UEFI セキュア ブートは、Cisco UCS Manager でのみ制御することができます。
- サーバがセキュア ブート モードである場合に Cisco UCS Manager の以前のバージョンにダウングレードする場合で、セキュア ブート モードのシステムがある場合は、ダウングレード前に、サーバの関連付けを解除してから、再度関連付けする必要があります。これを行わないと、サーバは検出されません。

CIMC セキュア ブート

CIMC セキュア ブートでは、署名済みのシスコ ファームウェア イメージのみをサーバにインストールし、実行できます。CIMC が更新されると、イメージは、ファームウェアがフラッシュされる前に認証されます。認証に失敗すると、ファームウェアはフラッシュされません。これにより、CIMC ファームウェアへの不正アクセスを防止します。

CIMC セキュア ブートの注意事項と制約事項

- CIMC セキュア ブートは、Cisco UCS M3 ラック サーバでサポートされています。

（注） CIMC セキュア ブートは Cisco UCS C220 M4 および C240 M4 ラック サーバで、デフォルトでイネーブルになっており、Cisco UCS C460 M4 ラック サーバでは、CIMC ファームウェア リリース 2.2(3) 以降にアップグレードした後に自動的にイネーブルになります。

- CIMC セキュア ブートがイネーブルになると、それをディセーブルにすることはできません。
- CIMC セキュア ブートがサーバ上でイネーブルになると、2.1(3) より前の CIMC ファームウェア イメージにダウングレードすることはできません。

CIMC セキュア ブートのステータスの判別

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *server-num*	指定したサーバのサーバ モードを開始します。
ステップ 2	UCS-A /chassis/server # **scope cimc**	サーバ CIMC モードを開始します。
ステップ 3	UCS-A /server/cimc # **show secure-boot**	指定されたサーバの CIMC セキュア ブートのステータスが表示されます。次のいずれかになります。 • [サポート対象外（Unsupported）] : CIMC セキュア ブートはサーバでサポートされていません。 • [無効（Disabled）] : CIMC セキュア ブートはサーバでサポートされていますが、ディセーブルになっています。 • [有効化（Enabling）] : CIMC セキュア ブートは有効化され、操作は進行中です。 • [有効（Enabled）] : CIMC セキュア ブートはサーバでイネーブルになっています。

次に、CIMC セキュア ブートのステータスを表示する例を示します。

```
UCS-A# scope server 1
UCS-A /chassis/server # scope cimc
UCS-A /chassis/server/cimc # show secure-boot
Secure Boot: Disabled
UCS-A /chassis/server/cimc #
```

CIMC セキュア ブートの有効化

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *server-num*	指定したサーバのサーバ モードを開始します。
ステップ 2	UCS-A /chassis/server # **scope cimc**	サーバ CIMC モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /server/cimc # **enable secure-boot**	指定されたサーバの CIMC セキュア ブートのステータスを有効化します。CIMC セキュア ブートは、Cisco UCS M3 ラック サーバでのみサポートされています。 （注） 一度有効化すると、CIMC セキュア ブートを無効化できません。
ステップ 4	UCS-A /server/cimc # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、CIMC セキュアブートを有効化し、トランザクションをコミットする方法を示しています。

```
UCS-A# scope server 1
UCS-A /chassis/server # scope cimc
UCS-A /chassis/server/cimc # enable secure-boot
Warning: When committed, CIMC Secure Boot and Installation Feature will be enabled for the
 server.
This is an irreversible operation!!

UCS-A /chassis/server/cimc* # commit-buffer
UCS-A /chassis/server/cimc #
```

ブート ポリシーの作成

サービス プロファイルまたはサービス プロファイル テンプレートに制限されたローカル ブート ポリシーを作成することもできます。しかし、複数のサービスプロファイルまたはサービスプロファイル テンプレートに含むことのできるグローバルなブート ポリシーの作成を推奨します。

はじめる前に

SAN LUN からサーバをブートするブート ポリシーを作成し、安定した SAN ブート操作が必要な場合は、ブートポリシーを含むサービスプロファイルに関連付けられたサーバからすべてのローカル ディスクを最初に削除する必要があります。

（注） これは、Cisco UCS M3 および M4 サーバには適用されません。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **create boot-policy** *policy-name* [**purpose** {**operational** | **utility**}]	ブート ポリシーを指定されたポリシー名で作成し、組織ブート ポリシー モードを開始します。 ブート ポリシーを作成する場合、**operational** オプションを指定します。これにより、サーバは、サーバにインストールされているオペレーティング システムからブートするようにします。**utility** オプションは予約されており、シスコの担当者が指示した場合にのみ使用するようにします。
ステップ 3	UCS-A /org/boot-policy # **set descr** *description*	（任意） ブート ポリシーの説明を記入します。 （注） 説明にスペース、特殊文字、または句読点が含まれている場合は、説明を引用符で括る必要があります。引用符は、**show** コマンド出力の説明フィールドには表示されません。
ステップ 4	UCS-A /org/boot-policy # **set reboot-on-update** {**no** | **yes**}	このブート ポリシーを使用するサーバが、ブート順序の変更後に自動的に再起動されるかどうかを指定します。
ステップ 5	UCS-A /org/boot-policy # **set enforce-vnic-name** {**no** | **yes**}	[yes] を選択すると、Cisco UCS Manager は設定エラーを表示し、[ブート順序（Boot Order）] テーブルにリストされた 1 つ以上の vNIC、vHBA、または iSCSI vNIC がサービス プロファイル内のサーバ設定に一致するかどうかをレポートします。 [no] を選択すると、Cisco UCS Manager はサービス プロファイルから vNIC、vHBA、または iSCSI vNIC（ブート オプションに適切なもの）を使用します。
ステップ 6	UCS-A /org/boot-policy # **set boot-mode** {**legacy** | **uefi**}	このブート ポリシーを使用するサーバが UEFI またはレガシー ブート モードを使用するかどうかを指定します。
ステップ 7	UCS-A /org/boot-policy # **commit-buffer**	トランザクションをシステム設定にコミットします。

	コマンドまたはアクション	目的
ステップ 8	UCS-A /org/boot-policy # **create boot-security**	指定したブート ポリシーでブート セキュリティ モードを開始します。
ステップ 9	UCS-A /org/boot-policy/boot-security # **set secure-boot** {**no** | **yes**}	セキュア ブートがブート ポリシーに対してイネーブルにするかを指定します。
ステップ 10	UCS-A /org/boot-policy/boot-security # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、boot-policy-LAN という名前のブート ポリシーを作成し、このポリシーを使用するサーバがブート順序が変更されたときに自動的にリブートされないよう指定し、UEFI ブート モードを設定し、UEFI ブート セキュリティを有効にし、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org* # create boot-policy boot-policy-LAN purpose operational
UCS-A /org/boot-policy* # set descr "Boot policy that boots from the LAN."
UCS-A /org/boot-policy* # set reboot-on-update no
UCS-A /org/boot-policy* # set boot-mode uefi
UCS-A /org/boot-policy* # commit-buffer
UCS-A /org/boot-policy # create boot-security
UCS-A /org/boot-policy/boot-security* # set secure-boot yes
UCS-A /org/boot-policy/boot-security* # commit-buffer
UCS-A /org/boot-policy/boot-security #
```

次の作業

次の 1 つ以上のオプションをブート ポリシーに設定し、ブート順序を設定します。

- **LAN Boot**：中央集中型プロビジョニング サーバからブートします。これは、このサーバから、別のサーバ上にオペレーティング システムをインストールするためによく使用されます。

  [LAN ブート（LAN Boot）] オプションを選択した場合は、ブート ポリシー用 LAN ブートの設定, （624 ページ） に進みます。

- **SAN Boot**：SAN 上のオペレーティング システム イメージからブートします。プライマリおよびセカンダリ SAN ブートを指定できます。プライマリ ブートが失敗した場合、サーバはセカンダリからのブートを試行します。

  システムに最高のサービス プロファイル モビリティを提供する SAN ブート ポリシーの使用を推奨します。SAN からブートした場合、あるサーバから別のサーバにサービス プロファイルを移動すると、移動後のサーバは、まったく同じオペレーティング システム イメージからブートします。したがって、ネットワークからは、この新しいサーバはまったく同じサーバと認識されます。

  [SAN ブート（SAN Boot）] オプションを選択した場合は、ブート ポリシー用 SAN ブート ポリシー設定, （584 ページ） に進みます。

- **Virtual Media Boot**：サーバへの物理 CD の挿入を模倣します。これは通常、サーバ上にオペレーティング システムを手動でインストールする場合に使用されます。

  [仮想メディア ブート（Virtual Media Boot）] オプションを選択した場合は、ブート ポリシー用仮想メディア ブートの設定, （630 ページ） に進みます。

ヒント

ローカル ディスクと SAN LUN の両方がブート順序のストレージ タイプに設定されていて、オペレーティング システムまたは論理ボリューム マネージャ（LVM）の設定が誤っている場合、サーバが SAN LUN ではなくローカル ディスクからブートする場合があります。

たとえば、Red Hat Linux がインストールされているサーバで、LVM にデフォルトの LVM が設定されていて、ブート順序に SAN LUN とローカル ディスクが設定されている場合、Linux は同じ名前の LV が 2 つあるという通知を生成し、SCSI ID の値が最も小さい LV（ローカル ディスクの可能性があります）からブートします。

ブート ポリシーをサービス プロファイルとテンプレートに含めます。

SAN ブート

SAN 上のオペレーティング システム イメージから 1 つ以上のサーバがブートするように、ブート ポリシーを設定できます。ブート ポリシーにはプライマリとセカンダリの SAN ブート含めることができます。プライマリ ブートが失敗した場合、サーバはセカンダリからのブートを試行します。

システムに最高のサービス プロファイル モビリティを提供する SAN ブートの使用を推奨します。SAN からブートした場合、サービス プロファイルを別のサーバに移動しても、そのサーバは同じオペレーティング システム イメージからブートします。したがって、ネットワークからは、新しいサーバが同じサーバとして認識されます。

SAN ブートを使用するには、次の項目が設定されていることを確認してください。

- Cisco UCS ドメインが、オペレーティング システム イメージをホストしている SAN ストレージ デバイスと通信できること。
- オペレーティング システム イメージが置かれているデバイス上のブート ターゲット LUN（論理ユニット番号）。

（注）

SAN ブートは、Cisco UCS ブレード サーバおよびラック サーバ上の Gen-3 Emulex アダプタではサポートされていません。

ブート ポリシー用 SAN ブート ポリシー設定

ヒント　ローカル ディスクと SAN LUN の両方がブート順序のストレージ タイプに設定されていて、オペレーティング システムまたは論理ボリューム マネージャ（LVM）の設定が誤っている場合、サーバが SAN LUN ではなくローカル ディスクからブートする場合があります。

たとえば、Red Hat Linux がインストールされているサーバで、LVM にデフォルトの LVM が設定されていて、ブート順序に SAN LUN とローカル ディスクが設定されている場合、Linux は同じ名前の LV が 2 つあるという通知を生成し、SCSI ID の値が最も小さい LV（ローカル ディスクの可能性があります）からブートします。

この手順は、ブート ポリシーの作成, （580 ページ） から直接続いています。

はじめる前に

SAN ブート設定を含めるブート ポリシーを作成します。

（注）

リリース 2.2 以降では、すべての SAN ブート関連 CLI コマンドが SAN スコープに移動されています。**org/boot-policy/san** または **org/service-profile/boot-definition/san** の代わりにストレージ範囲で SAN ブートを使用する以前のリリースからの既存のスクリプトは更新する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **scope boot-policy** *policy-name*	指定されたブート ポリシーの組織ブート ポリシー モードを開始します。
ステップ 3	UCS-A /org/boot-policy #**create san**	ブート ポリシーの SAN ブートを作成し、組織ブート ポリシー ストレージ モードを開始します。
ステップ 4	UCS-A /org/boot-policy/san # **set order** *order_number*	SAN ブートのブート順序を設定します。1 ～ 16 の整数を入力します。
ステップ 5	UCS-A /org/boot-policy/san # **create san-image** {**primary** | **secondary**}	SAN イメージの場所を作成し、san-image オプションが指定されている場合は、組織ブート ポリシーのストレージ SAN イメージ モードを開始します。 Cisco UCS サーバで拡張ブート順序を使用する場合は、定義したブート順序が使用されます。用語

	コマンドまたはアクション	目的
		「プライマリ」または「セカンダリ」を使用した標準のブートモードは、ブート順序を示唆するものではありません。同じデバイス クラス内での実際のブート順序は、PCIeバス スキャン順序により決定されます。
ステップ 6	UCS-A /org/boot-policy/ssn/san-image # **set vhba** *vhba-name*	SAN ブートに使用される vHBA を指定します。
ステップ 7	UCS-A /org/boot-policy/san/san-image # **create path** {**primary** | **secondary**}	プライマリまたはセカンダリ SAN ブート パスを作成し、組織ブート ポリシーの SAN パス モードを開始します。 Cisco UCS サーバで拡張ブート順序を使用する場合は、定義したブート順序が使用されます。用語「プライマリ」または「セカンダリ」を使用した標準のブートモードは、ブート順序を示唆するものではありません。同じデバイス クラス内での実際のブート順序は、PCIeバス スキャン順序により決定されます。
ステップ 8	UCS-A /org/boot-policy/san/san-image/path # **set** {**lun** *lun-id* | **wwn** *wwn-num*}	ブート イメージへの SAN パスに使用される LUN または WWN を指定します。
ステップ 9	UCS-A /org/boot-policy/san/san-image/path # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例で、lab1-boot-policy という名前のブート ポリシーに入り、ポリシーの SAN ブートを作成し、ブート順序を 1 に設定し、プライマリ SAN イメージを作成し、vHBA2 という名前の vHBA を使用し、LUN 0 を使用してプライマリ パスを作成し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org* # scope boot-policy lab1-boot-policy
UCS-A /org/boot-policy # create san
UCS-A /org/boot-policy/san* # set order 1
UCS-A /org/boot-policy/san* # create san-image primary
UCS-A /org/boot-policy/san/san-image* # set vhba vHBA2
UCS-A /org/boot-policy/san/san-image* # create path primary
UCS-A /org/boot-policy/san/san-image/path* # set lun 0
UCS-A /org/boot-policy/san/san-image/path* # commit-buffer
UCS-A /org/boot-policy/san/san-image/path #
```

次の例で、サービス プロファイル SP_lab1 用の SAN ブートを作成し、ブート順序を 1 に設定し、プライマリ SAN イメージを作成し、vHBA2 という名前の vHBA を使用し、LUN 0 を使用してプライマリ パスを作成し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org* # scope service-profile SP_lab1
UCS-A /org/service-profile # create boot-definition
UCS-A /org/service-profile/boot-definition* # create san
UCS-A /org/service-profile/boot-definition/san* # create san-image primary
UCS-A /org/service-profile/boot-definition/san/san-image* # set vhba vHBA2
UCS-A /org/service-profile/boot-definition/san/san-image* # create path primary
UCS-A /org/service-profile/boot-definition/san/san-image/path* # set lun 0
UCS-A /org/service-profile/boot-definition/san/san-image/path* # commit-buffer
UCS-A /org/service-profile/boot-definition/san/san-image/path #
```

次の作業

ブート ポリシーをサービス プロファイルとテンプレートに含めます。

iSCSI ブート

iSCSI ブートは、サーバがネットワークにリモートに配置されている iSCSI ターゲット マシンからオペレーティング システムを起動できるようにします。

iSCSI ブートは次の Cisco UCS ハードウェアでサポートされます。

- Cisco UCS M51KR-B Broadcom BCM57711 ネットワーク アダプタを持ち、Broadcom から提供されるデフォルトの MAC アドレスを使用する、Cisco UCS ブレード サーバ。
- Cisco UCS M81KR 仮想インターフェイス カード
- Cisco UCS VIC-1240 仮想インターフェイス カード
- Cisco UCS VIC-1280 仮想インターフェイス カード
- Cisco UCS M61KR-B Broadcom BCM57712 のネットワーク アダプタを持つ Cisco UCS ラック サーバ。
- Cisco UCS P81E 仮想インターフェイス カード
- Cisco UCS ラック サーバ上の Cisco UCS VIC 1225 仮想インターフェイス カード

iSCSIブートを設定する前に満たさなければならない前提条件があります。これらの前提条件のリストについては、iSCSI ブートのガイドラインと前提条件, （587 ページ） を参照してください。

iSCSI ブートを実装するための高度な手順については、iSCSI ブートの設定, （590 ページ） を参照してください。

iSCSI ブート プロセス

Cisco UCS Manager は、サーバにあるアダプタをプログラムするための関連付けプロセスでサービス プロファイル用に作成された iSCSI vNIC と iSCSI のブート情報を使用します。アダプタのプログラミング後に、サーバは最新のサービスプロファイル値で再起動します。電源投入時セルフテ

スト（POST）の後、アダプタは、次のサービスプロファイル値を使用して初期化を試みます。アダプタが値を使用して指定されたターゲットにログインできる場合、アダプタはiSCSI Boot Firmware Table（iBFT）を初期化してホスト メモリに、有効なブート可能 LUN をシステム BIOS にポストします。ホスト メモリにポストされる iBFT には、プライマリ iSCSI VNIC にプログラミングされた、イニシエータとターゲットの設定が含まれています。

（注） 以前は、ホストは LUN 検出が最初に終了したパスに応じて、設定されたブート パスのうち 1 つだけを参照し、そのパスから起動していました。現在は、設定された iSCSI ブート vNIC が 2つある場合、ホストは両方のブートパスを参照するようになりました。そのため、マルチパス構成では、両方のブート vNIC に単一の IQN を設定する必要があります。ホスト上のブート vNIC に設定された異なる IQN が存在する場合、ホストは PCI 順序が低いブート vNIC に設定された IQN を使用して起動します。

次の手順であるオペレーティング システム（OS）のインストールでは、iBFT 対応の OS が必要です。OS のインストール時に、OS インストーラは iBFT テーブルのホストのメモリをスキャンし、iBFT テーブルの情報を使用してブート デバイスの検出とターゲット LUN への iSCSI パス作成を行います。OS によっては、このパスを完了するために NIC ドライバが必要です。このステップが成功した場合、OS インストーラが OS をインストールする iSCSI ターゲット LUN を検出します。

（注） iBFT は OS インストールのソフトウェア レベルで動作し、HBA モード（別名 TCP オフロード）では動作しない場合があります。iBFT が HBA モードで動作するかどうかは、インストール中の OS の機能によって異なります。また、Cisco UCS M51KR-B Broadcom BCM57711 アダプタを含むサーバについては、iBFT は MTU ジャンボ設定に関係なく、最大伝送単位（MTU）サイズ 1500 で正常に動作します。OS が HBA モードをサポートする場合、iSCSI インストール プロセスの後に HBA モード、デュアル ファブリックのサポートおよびジャンボ MTU サイズの設定が必要な場合があります。

iSCSI ブートのガイドラインと前提条件

iSCSI ブートを設定する前に、これらのガイドラインと前提条件を満たす必要があります。

- iSCSI ブート ポリシーの作成後、ls-compute 権限を持つユーザは、そのポリシーをサービス プロファイルまたはサービス プロファイル テンプレートに組み込むことができます。ただし、ls-compute 権限しかないユーザは iSCSI ブート ポリシーを作成できません。
- セカンド vNIC（フェールオーバー vNIC）が iSCSI LUN から起動する必要がある Windows 2008 サーバからの iSCSI ブートを設定するには、Microsoft Knowledge Base Article 976042 を参照してください。Microsoft には、ネットワーキング ハードウェアが変更されたときに、Windows が iSCSI ドライブからの起動に失敗するか、bugcheck エラーが発生する可能性がある、という既知の問題があります。この問題を回避するには、Microsoft が推奨する解決方法に従ってください。

- ストレージ アレイは、iSCSI ブートのライセンスが付与され、アレイ サイド LUN マスキングが正しく設定されている必要があります。
- 各 iSCSI イニシエータに 1 つずつ、2 つの IP アドレスを決定する必要があります。可能であれば、IP アドレスは、ストレージ アレイと同じサブネット上にある必要があります。IP アドレスは、Dynamic Host Configuration Protocol（DHCP）を使用してスタティックまたはダイナミックに割り当てられます。
- グローバル ブート ポリシーのブート パラメータは設定できません。代わりに、ブート パラメータを設定した後、ブート ポリシーを適切なサービス プロファイルに含めます。
- オペレーティング システム（OS）は iSCSI Boot Firmware Table（iBFT）と互換性がある必要があります。
- Cisco UCS M51KR-B Broadcom BCM57711 ネットワーク アダプタの場合：
  - iSCSI ブートを使用するサーバは、Cisco UCS M51KR-B Broadcom BCM57711 ネットワーク アダプタを含んでいる必要があります。アダプタ カードを取り付けまたは交換する方法については、『*Cisco UCS B250 Extended Memory Blade Server Installation and Service Note*』を参照してください。サービス ノートは、http://www.cisco.com/go/unifiedcomputing/b-series-doc の『*Cisco UCS B-Series Servers Documentation Roadmap*』からアクセスできます。
  - iSCSI デバイスの MAC アドレスを設定します。
  - DHCP Vendor ID（オプション 43）を使用している場合は、iSCSI デバイスの MAC アドレスを /etc/dhcpd.conf に設定します。
  - HBA モード（別名 TCP オフロード）およびターゲットへのブート設定がサポートされます。ただし、インストール中の HBA モードは Windows OS だけがサポートします。
  - OS をインストールする前に、iSCSI のアダプタ ポリシーでターゲットへのブート設定を無効にし、OS をインストールした後で、ターゲットへのブート設定を再度有効にします。

    （注） アダプタ ポリシーの設定を変更するたびに、アダプタはリブートして新しい設定を適用します。

  - OS を iSCSI ターゲットにインストールする場合、iSCSI ターゲットは OS イメージが存在するデバイスの前の順番にしておく必要があります。たとえば、CD から iSCSI ターゲットに OS をインストールする場合、ブート順序は最初に iSCSI ターゲット、その後 CD とする必要があります。
  - サーバが iSCSI ブートされた後は、イニシエータ名、ターゲット名、LUN、iSCSI デバイス IP、ネットマスクやゲートウェイを Broadcom ツールを使用して変更しないでください。
  - POST（電源投入時自己診断テスト）プロセスを中断しないでください。中断すると、Cisco UCS M51KR-B Broadcom BCM57711 ネットワーク アダプタは初期化に失敗します。

- Cisco UCS M81KR 仮想インターフェイス カードおよびCisco UCS VIC-1240 仮想インターフェイス カード の場合：

  Cisco UCS VIC-1240 仮想インターフェイス カード の場合：

  - iSCSI デバイスの MAC アドレスを設定しないでください。
  - HBA モードおよびターゲットへのブート設定はサポートされていません。
  - OS を iSCSI ターゲットにインストールする場合、iSCSI ターゲットは OS イメージが存在するデバイスより後の順番にしておく必要があります。たとえば、CD から iSCSI ターゲットに OS をインストールする場合、ブート順序は最初に CD、その後 iSCSI ターゲットとする必要があります。
  - DHCP Vendor ID（オプション 43）を使用している場合、オーバーレイ vNIC の MAC アドレスを /etc/dhcpd.conf に設定する必要があります。
  - サーバの iSCSI ブート後は、オーバーレイ vNIC の IP 詳細を変更しないでください。

- VMware ESX/ESXi オペレーティング システムは、iSCSI ブート ターゲット LUN へのコア ダンプ ファイルの保存をサポートしていません。ダンプ ファイルはローカル ディスクに書き込む必要があります。

イニシエータ IQN の設定

Cisco UCS は、サービス プロファイルが物理サーバに関連付けられた時点で、以下のルールを使用してアダプタ iSCSI vNIC のイニシエータ IQN を決定します。

- サービス プロファイル レベルのイニシエータ IQN と iSCSI vNIC レベルのイニシエータ IQN を、1 つのサービス プロファイルで一緒に使用することはできません。
- イニシエータ IQN をサービス プロファイル レベルで指定すると、DHCP オプション 43 の場合（イニシエータ IQN はアダプタ iSCSI vNIC で空に設定される）を除き、すべてのアダプタ iSCSI vNIC が同じイニシエータ IQN を使用するように設定されます。
- イニシエータ IQN を iSCSI vNIC レベルで設定すると、サービス プロファイル レベルのイニシエータ IQN は削除されます（存在する場合）。
- サービス プロファイルに 2 つの iSCSI vNIC があり、一方にだけイニシエータ IQN が設定されている場合、もう一方にはデフォルトの IQN プールが設定されます。この設定は後で変更できます。唯一の例外は、DHCP オプション 43 が設定されている場合です。その場合、もう一方の iSCSI vNIC のイニシエータ IQN は、サービス プロファイルを関連付けるときに削除されます。

（注） ベンダー ID を設定して、DHCP オプション 43 を使用するように iSCSI vNIC を変更した場合、サービス プロファイル レベルで設定したイニシエータ IQN は削除されません。サービス プロファイル レベルのイニシエータ IQN は、DHCP オプション 43 を使用しない別の iSCSI vNIC で使用できます。

Windows での MPIO のイネーブル化

ストレージ アレイで接続を最適化するには、MPIO をイネーブルにします。

（注） ネットワーク ハードウェアを変更すると、Windows が iSCSI ドライブからの起動に失敗する場合があります。詳細については、『Microsoft support Article ID: 976042』を参照してください。

はじめる前に

Microsoft Multipath I/O（MPIO）をイネーブル化するサーバには、Cisco VIC ドライバが必要です。

ブート LUN に設定されたパスが複数ある場合、LUN がインストールされるときにイネーブルにするパスは 1 つのみです。

手順

ステップ 1 サーバに関連付けられたサービス プロファイルで、プライマリ iSCSI vNIC を設定します。
詳細については、サービス プロファイルでの iSCSI vNIC の作成を参照してください。

ステップ 2 プライマリ iSCSI vNIC を使用して、iSCSI ターゲット LUN に Windows オペレーティング システムをインストールします。

ステップ 3 Windows のインストールが完了したら、ホスト上で MPIO をイネーブルにします。

ステップ 4 サーバに関連付けられたサービス プロファイルで、ブート ポリシーにセカンダリ iSCSI vNIC を追加します。
詳細については、iSCSI ブート ポリシーの作成を参照してください。

iSCSI ブートの設定

LUN ターゲットから iSCSI ブートするよう Cisco UCS でアダプタまたはブレードを設定する場合、次のすべてのステップを完了します。

手順

	コマンドまたはアクション	目的
ステップ 1	iSCSI ブートのアダプタ ポリシーを設定します。	（任意） 詳細については、次を参照してください。 iSCSI アダプタ ポリシーの作成
ステップ 2	イニシエータとターゲットの認証プロファイルを設定します。	（任意） 詳細については、次を参照してください。 認証プロファイルの作成
ステップ 3	IP アドレス プールの IP アドレスを使用するよう iSCSI イニシエータを設定するには、iSCSI イニシエータ プールに IP アドレスのブロックを追加します。	（任意） 詳細については、次を参照してください。 イニシエータ プールへの IP アドレスのブロックの追加
ステップ 4	すべてのサービス プロファイルで使用できるブート ポリシーを作成します。または、特定のサービス ポリシーに対してのみローカル ブート ポリシーを作成できます。ただし、複数のサービス プロファイルと共有できるブート ポリシーを作成することを推奨します。	すべてのサービス プロファイルで使用できるブート ポリシーの作成の詳細については、iSCSI ブート ポリシーの作成 を参照してください。
ステップ 5	すべてのサービス プロファイルで使用できるブート ポリシーを作成した場合は、それをサービス プロファイルに割り当てます。それ以外の場合は、次のステップに進みます。	詳細については、サービス プロファイル テンプレートの作成を参照してください。
ステップ 6	サービス プロファイルでイーサネット vNIC を設定します。	イーサネット vNIC は、iSCSI デバイスのオーバーレイ vNIC として使用されます。詳細については、サービス プロファイルの vNIC の設定を参照してください。
ステップ 7	サービス プロファイルで iSCSI vNIC を作成します。	詳細については、次を参照してください。 サービス プロファイルでの iSCSI vNIC の作成
ステップ 8	スタティック IP アドレス、IP プールの IP アドレス、または DHCP を使用して iSCSI イニシエータがブートするように設定します。	スタティック IP アドレスを使用してブートする iSCSI イニシエータの作成、IP プールからの IP アドレスを使用してブートする iSCSI イニシエータの作成、または DHCP を使用してブートする iSCSI イニシエータの作成 を参照してください。

	コマンドまたはアクション	目的
ステップ 9	iSCSI スタティックまたは自動ターゲットを作成します。	詳細については、iSCSI スタティック ターゲットの作成 または iSCSI 自動ターゲットの作成 を参照してください。
ステップ 10	サービス プロファイルをサーバと関連付けます。	詳細については、サービス プロファイルとブレードサーバまたはサーバプールの関連付けを参照してください。
ステップ 11	iSCSI ブート動作を確認します。	詳細については、次を参照してください。 iSCSI ブートの確認
ステップ 12	サーバに OS をインストールします。	詳細については、次のいずれかのドキュメントを参照してください。 • *Cisco UCS B-Series Blade Servers VMware Installation Guide* • *Cisco UCS B-Series Blade Servers Linux Installation Guide* • *Cisco UCS B-Series Blade Servers Windows Installation Guide*
ステップ 13	サーバをブートします。	

iSCSI アダプタ ポリシーの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **create iscsi-policy** *policy-name*	iSCSI アダプタ ポリシーを作成します。
ステップ 3	UCS-A /org/iscsi-policy # **set descr** *description*	（任意） iSCSI アダプタ ポリシーに説明を記入します。
ステップ 4	UCS-A /org/iscsi-policy # **set iscsi-protocol-item connection-timeout** *timeout-secs*	最初のログインに失敗し、iSCSI アダプタが使用できないと Cisco UCS が判断するまで待機する秒数。

	コマンドまたはアクション	目的
		0 ～ 255 の整数を入力します。0 を入力すると、Cisco UCS はアダプタ ファームウェアに設定された値（デフォルト：15 秒）を使用します。
ステップ 5	UCS-A /org/iscsi-policy # **set iscsi-protocol-item dhcp-timeout** *timeout-secs*	イニシエータが DHCP サーバが使用できないと判断するまでに待機する秒数。 60 ～ 300 の整数を入力します（デフォルトは 60 秒です）。
ステップ 6	UCS-A /org/iscsi-policy # **set iscsi-protocol-item lun-busy-retry-count** *num*	iSCSI LUN 検出中にエラーが発生した場合に接続を再試行する回数。 0 ～ 60 の整数を入力します。0 を入力すると、Cisco UCS はアダプタ ファームウェアに設定された値（デフォルト：15 秒）を使用します。
ステップ 7	UCS-A /org/iscsi-policy # **set iscsi-protocol-item tcp-time-stamp** {**no** | **yes**}	TCP タイムスタンプを適用するかどうかを指定します。この設定を使用すると、転送されるパケットにパケット送信時のタイムスタンプが付けられるので、必要なときにパケットのラウンドトリップ時間を計算することができます。この設定は Cisco UCS M51KR-B Broadcom BCM57711 アダプタにだけ適用されます。
ステップ 8	UCS-A /org/iscsi-policy # **set iscsi-protocol-item hbamode** {**no** | **yes**}	HBA モードをイネーブルにするかどうかを指定します。 このオプションは、Windows オペレーティング システムを実行する Cisco UCS NIC M51KR-B のアダプタを備えるサーバに対してのみ有効にする必要があります。
ステップ 9	UCS-A /org/iscsi-policy # **set iscsi-protocol-item boottotarget** {**no** | **yes**}	iSCSI ターゲットからブートするかどうかを指定します。 このオプションは Cisco UCS NIC M51KR-B のアダプタを備えたサーバにのみ適用されます。このオプションは、サーバにオペレーティング システムをインストールするまで無効にしておく必要があります。
ステップ 10	UCS-A /org/iscsi-policy # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例に、iscsiboot という iSCSI アダプタ ポリシーを作成し、接続タイムアウト、DHCP タイムアウト、LUN ビジー再試行カウントを設定し、TCP タイムスタンプを適用して、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org # create iscsi-policy iscsiboot
UCS-A /org/iscsi-policy* # set iscsi-protocol-item connection-timeout 60
UCS-A /org/iscsi-policy* # set iscsi-protocol-item dhcp-timeout 200
UCS-A /org/iscsi-policy* # set iscsi-protocol-item lun-busy-retry-count 5
UCS-A /org/iscsi-policy* # set iscsi-protocol-item tcp-time-stamp yes
UCS-A /org/iscsi-policy* # set iscsi-protocol-item hbamode yes
UCS-A /org/iscsi-policy* # set iscsi-protocol-item boottotarget yes
UCS-A /org/iscsi-policy* # commit-buffer
UCS-A /org/iscsi-policy #
```

次の作業

アダプタ ポリシーをサービス プロファイルとテンプレートに含めます。

iSCSI アダプタ ポリシーの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / と入力します。
ステップ 2	UCS-A /org # **delete iscsi-policy** *policy-name*	iSCSI アダプタ ポリシーを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、iscsi-adapter-pol という名前の iSCSI アダプタ ポリシーを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # delete iscsi-policy iscsi-adapter-pol
UCS-A /org* # commit-buffer
UCS-A /org #
```

認証プロファイルの作成

iSCSI ブートの認証を使用する場合は、イニシエータとターゲットの両方に認証プロファイルを作成する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **create auth-profile** *profile-name*	指定された名前で認証プロファイルを作成します。名前には 16 文字以内の英数字を使用できます。
ステップ 3	UCS-A /org/auth-profile* # **set user-id** *id-name*	認証用にログインを作成します。
ステップ 4	UCS-A /org/auth-profile* # **set password**	認証用のパスワードを作成します。
ステップ 5	UCS-A /org/auth-profile* # **commit-buffer**	トランザクションをシステム設定にコミットします。
ステップ 6	UCS-A /org/auth-profile* # **exit**	現在のモードを終了します。
ステップ 7	ターゲットの認証プロファイルを作成するには、ステップ 2 ～ 6 を繰り返します。	

次の例は、イニシエータとターゲットの認証プロファイルを作成し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org
UCS-A /org # create auth-profile InitAuth
UCS-A /org/auth-profile* # set user-id init
UCS-A /org/auth-profile* # set  password
Enter a password:
Confirm the password:
UCS-A /org/auth-profile* # commit-buffer
UCS-A /org/auth-profile # exit
UCS-A /org # create auth-profile TargetAuth
UCS-A /org/auth-profile* # set user-id target
UCS-A /org/auth-profile* # set  password
Enter a password:
Confirm the password:
UCS-A /org/auth-profile* # commit-buffer
UCS-A /org/auth-profile # exit
```

次の作業

iSCSI デバイスのオーバーレイ vNIC として使用されるイーサネット vNIC を作成してから、iSCSI vNIC を作成します。

認証プロファイルの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **delete auth-profile** *auth-profile-name*	指定した認証プロファイルを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、iscsi-auth という認証プロファイルを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope org
UCS-A /org # delete auth-profile iscsi-auth
UCS-A /org* # commit-buffer
UCS-A /org #
```

イニシエータ プールへの IP アドレスのブロックの追加

iSCSI ブートに使用する IP アドレスのグループを作成できます。Cisco UCS Manager は指定した IP アドレスのブロックを予約します。

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

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルート組織モードを開始するには、/ を *org-name* として入力します。
ステップ 2	UCS-A /org# **scope ip-pool iscsi-initiator-pool**	iSCSI イニシエータ プールを指定するモードを開始します。
ステップ 3	UCS-A /org/ip-pool # **set descr** *description*	（任意） IP プールの説明を記入します。

	コマンドまたはアクション	目的
		（注） 説明にスペース、特殊文字、または句読点が含まれている場合は、説明を引用符で括る必要があります。引用符は、**show** コマンド出力の説明フィールドには表示されません。
ステップ 4	UCS-A /org/ip-pool # **set assignmentorder** {**default** | **sequential**}	次のいずれかになります。 • **default**：Cisco UCS Manager はプールからランダムな ID を選択します。 • **sequential**：Cisco UCS Manager はプールから最も小さい使用可能 ID を選択します。
ステップ 5	UCS-A /org/ip-pool# **create block** *from_ip_address to_ip_address default_gateway subnet_mask*	iSCSI イニシエータの IP アドレスのブロックを作成します。
ステップ 6	UCS-A/org/ip-pool/block# **show detail expand**	（任意） 作成した IP アドレスのブロックを表示します。
ステップ 7	UCS-A /org/ip-pool/block # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例に、iSCSI vNIC の IP イニシエータ プールを作成して、トランザクションをコミットする方法を示します。

```
UCS-A # scope org /
UCS-A /org # scope ip-pool iscsi-initiator-pool
UCS-A /org/ip-pool # create block 40.40.40.10 40.40.40.50 40.40.40.1 255.0.0.0
UCS-A /org/ip-pool/block # show detail expand
Block of IP Addresses:
    From: 40.40.40.10
    To: 40.40.40.50
    Default Gateway: 40.40.40.1
    Subnet Mask: 255.0.0.0
UCS-A /org/ip-pool/block # commit buffer
```

次の作業

1 つ以上のサービス プロファイルまたはサービス プロファイル テンプレートを設定し、iSCSI イニシエータ IP プールから iSCSI イニシエータ IP アドレスを取得します。

イニシエータ プールからの IP アドレスのブロックの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルート組織モードを開始するには、/ を *org-name* として入力します。
ステップ 2	UCS-A /org# **scope ip-pool iscsi-initiator-pool**	iSCSI イニシエータ プールを指定するモードを開始します。
ステップ 3	UCS-A /org/ip-pool# **delete block** *from_ip_address to_ip_address*	イニシエータ プールから指定した IP アドレス ブロックを削除します。
ステップ 4	UCS-A/org/ip-pool/block# **show detail expand**	（任意） IP アドレスのブロックが削除されたことを示します。
ステップ 5	UCS-A /org/ip-pool# **commit buffer**	トランザクションをシステム設定にコミットします。

次の例は、IP アドレスのブロックをイニシエータ プールから削除し、トランザクションをコミットします。

```
UCS-A # scope org /
UCS-A /org # scope ip-pool iscsi-initiator-pool
UCS-A /org/ip-pool # delete block 40.40.40.10 40.40.40.50 40.40.40.1 255.0.0.0
UCS-A /org/ip-pool # show detail expand

IP Pool:
    Name: iscsi-initiator-pool
    Size: 0
    Assigned: 0
    Descr:
UCS-A /org/ip-pool # commit buffer
```

iSCSI ブート ポリシーの作成

ブート ポリシーあたり最大 2 つの iSCSI vNIC を追加できます。一方の vNIC はプライマリ iSCSI ブート ソースとして動作し、もう一方はセカンダリ iSCSI ブート ソースとして動作します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **create boot-policy** *policy-name* [**purpose** {**operational** | **utility**}]	ブート ポリシーを指定されたポリシー名で作成し、組織ブート ポリシー モードを開始します。 この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。 ブート ポリシーを作成する場合、**operational** オプションを指定します。これにより、サーバは、サーバにインストールされているオペレーティング システムからブートするようにします。**utility** オプションは予約されており、シスコの担当者が指示した場合にのみ使用するようにします。
ステップ 3	UCS-A /org/boot-policy # **set descr** *description*	（任意） ブート ポリシーの説明を記入します。 （注） 説明にスペース、特殊文字、または句読点が含まれている場合は、説明を引用符で括る必要があります。引用符は、**show** コマンド出力の説明フィールドには表示されません。
ステップ 4	UCS-A /org/boot-policy # **set enforce-vnic-name** {**no** | **yes**}	（任意） [yes] を選択すると、Cisco UCS Manager はブート ポリシー内で指定されたデバイス名とサービス プロファイル内で指定されたものとが一致するかどうかをレポートします。 [no] を選択すると、Cisco UCS Manager はサービス プロファイルの任意の vNIC、vHBA、iSCSI デバイスを使用し、ブート ポリシー内で指定されたデバイス名とサービス プロファイル内で指定されたものとが一致するかどうかをレポートしません。
ステップ 5	UCS-A /org/boot-policy # **set reboot-on-update** {**no** | **yes**}	このブート ポリシーを使用するサーバが、ブート順序の変更後に自動的に再起動されるかどうかを指定します。 Cisco UCS Manager GUI で、[順序を変更したときにリブートする（Reboot on Boot Order Change）] チェック

	コマンドまたはアクション	目的
		ボックスがブート ポリシーについて選択されており、CD-ROM またはフロッピーがブート順の最後のデバイスの場合に、デバイスを取り外すか、装着すると、ブート順に直接効力がなく、サーバがリブートされません。
ステップ 6	UCS-A /org/boot-policy # **create iscsi**	ブート ポリシーに iSCSI ブートを追加します。
ステップ 7	UCS-A /org/boot-policy/iscsi # **create path** {**primary** | **secondary**}	Cisco UCS Manager が iSCSI ターゲットに到達するために使用する、プライマリ パスとセカンダリ パスを指定します。iSCSI ブートの場合は、2 つのパスを設定します。Cisco UCS Manager は、プライマリ パスを最初に使用し、それが失敗した場合、セカンダリ パスを使用します。
ステップ 8	UCS-A /org/boot-policy/iscsi/path # **create iscsivnicname** *iscsi-vnic-name*	iSCSI vNIC を作成します。
ステップ 9	UCS-A /org/boot-policy/iscsi/path # **exit**	iSCSI パス モードを終了します。
ステップ 10	UCS-A /org/boot-policy/iscsi/path # **set order** *order-num*	ブート順序内の iSCSI ブート順序を指定します。
ステップ 11	ステップ 8 ～ 10 を繰り返し、セカンダリ iSCSI vNIC を作成します。	（任意）
ステップ 12	UCS-A /org/boot-policy/iscsi # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、iscsi-boot-policy-LAN という名前の iSCSI ブート ポリシーを作成し、ブート ポリシーの説明を記入し、このポリシーを使用するサーバはブート順序変更時に自動でリブートしないよう指定し、iSCSI ブートのブート順序を 2 に設定し、iSCSI ブートを作成して iscsienic1 という vNIC に関連付け、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org* # create boot-policy iscsi-boot-policy-LAN purpose operational
UCS-A /org/boot-policy* # set descr "Boot policy that boots from iSCSI."
UCS-A /org/boot-policy* # set enforce-vnic-name yes
UCS-A /org/boot-policy* # set reboot-on-update no
UCS-A /org/boot-policy* # create iscsi
UCS-A /org/boot-policy/iscsi* # create path primary
UCS-A /org/boot-policy/iscsi/path* # set iscsivnicname iscsienic1
UCS-A /org/boot-policy/iscsi/path* # exit
UCS-A /org/boot-policy/iscsi* # set order 2
UCS-A /org/boot-policy/iscsi* # commit-buffer
UCS-A /org/boot-policy #
```

次の作業

ブート ポリシーをサービス プロファイルとテンプレートに含めます。

このブート ポリシーを含むサービス プロファイルがサーバに関連付けられた後で、サーバの [一般（General）] タブの [ブート順序の詳細（Boot Order Details）] 領域で実際のブート順序を確認できます。

ブート ポリシーからの iSCSI デバイスの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / と入力します。
ステップ 2	UCS-A /org # **scope boot-policy** *boot-pol-name*	指定したブート ポリシーでブート ポリシー組織モードを開始します。
ステップ 3	UCS-A /org/boot-policy # **delete iscsi**	ブート ポリシーから iSCSI ブートを削除します。
ステップ 4	UCS-A /org/boot-policy # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、boot-policy-iscsi という名前のブート ポリシーから iSCSI ブートを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # scope boot-policy boot-policy-iscsi
UCS-A /org/boot-policy # delete iscsi
UCS-A /org/boot-policy* # commit-buffer
UCS-A /org/boot-policy #
```

サービス プロファイル レベルでのイニシエータ IQN の設定

サービス プロファイルでは、特定の IQN または IQN のプールから取得される IQN を持つイニシエータを作成できます。

はじめる前に

CLI を使用して IQN を削除できません。

イニシエータ IQN の設定ガイドラインについては、イニシエータ IQN の設定, （589 ページ） を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / と入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	サービスプロファイルのサービスプロファイル組織モードを開始します。
ステップ 3	UCS-A /org/service-profile# **set iscsi-identity** {**initiator name***initiator-name*|**initiator-pool-name***pool-name*}	指定された名前でイニシエータを作成します。名前には16文字以内の英数字を使用できます。
ステップ 4	UCS-A /org/service-profile* # **commit buffer**	トランザクションをシステム設定にコミットします。
ステップ 5	UCS-A /org/auth-profile* # **exit**	現在のモードを終了します。

次の例では、iSCSIイニシエータの特定の名前を作成し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org # scope service-profile accounting
UCS-A /org/service-profile # set iscsi-identity initiator-name manual:IQN
UCS-A /org/service-profile* # commit-buffer
```

サービス プロファイルでの iSCSI vNIC の作成

サービス プロファイルに iSCSI vNIC を作成できます。

はじめる前に

iSCSIデバイスのオーバーレイ vNICとして使用される、サービスプロファイル内のイーサネット vNIC が必要です。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / と入力します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	サービス プロファイルのサービス プロファイル組織モードを開始します。
ステップ 3	UCS-A /org/service-profile # **create vnic-iscsi** *iscsi-vnic-name*.	iSCSI vNIC の名前を指定します。
ステップ 4	UCS-A /org/service-profile/vnic-iscsi* # **set iscsi-adaptor-policy** *iscsi-adaptor-name*	（任意） この iSCSI vNIC 用に作成した iSCSI アダプタ ポリシーを指定します。
ステップ 5	UCS-A /org/service-profile/vnic-iscsi* # **set auth-name** *authentication-profile-name*	（任意） iSCSI vNIC によって使用される認証プロファイルを設定します。設定する認証プロファイルがすでに存在している必要があります。詳細については、認証プロファイルの作成を参照してください。
ステップ 6	UCS-A /org/service-profile/vnic-iscsi* # **set identity** { **dynamic-mac** {*dynamic-mac-address* | **derived** } | **mac-pool** *mac-pool-name* }	iSCSI vNIC の MAC アドレスを指定します。 （注） MAC アドレスは、Cisco UCS NIC M51KR-B アダプタ専用に設定されます。
ステップ 7	UCS-A /org/service-profile/vnic-iscsi* # **set iscsi-identity** {**initiator-name** *initiator-name* | **initiator-pool-name** *iqn-pool-name*}	iSCSI イニシエータの名前、または iSCSI イニシエータの名前の指定に使用される IQN プールの名前を指定します。iSCSI イニシエータ名には最大 223 文字を使用できます。
ステップ 8	UCS-A /org/service-profile/vnic-iscsi* # **set overlay-vnic-name** *overlay-vnic-name*	オーバーレイ vNIC として iSCSI デバイスで使用される、イーサネット vNIC を指定します。詳細については、サービス プロファイルの vNIC の設定を参照してください。
ステップ 9	UCS-A /org/service-profile/vnic-iscsi* # **create eth-if**	iSCSI vNIC に割り当てられた VLAN のイーサネット インターフェイスを作成します。
ステップ 10	UCS-A /org/service-profile/vnic-iscsi/eth-if* # **set vlanname** *vlan-name*.	VLAN 名を指定します。デフォルトの VLAN は、default です。Cisco UCS M81KR 仮想インターフェイス カードおよび Cisco UCS VIC-1240 仮想インターフェイス カードの場合、指定する VLAN はオーバーレイ vNIC のネイティブ VLAN と同じである必要があります。Cisco UCS M51KR-B Broadcom BCM57711 アダプタの場合、指定した VLAN は、オーバーレイ vNIC に割り当てられたどの VLAN でも設定できます。

	コマンドまたはアクション	目的
ステップ 11	UCS-A /org/service-profile/vnic-iscsi # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、scsivnic1 という iSCSI vNIC を作成し、accounting という既存のサービス プロファイルに追加し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # scope service-profile accounting
UCS-A /org/service-profile # create vnic-iscsi iSCSI1
UCS-A /org/service-profile/vnic-iscsi* # set iscsi-adaptor-policy iscsiboot
UCS-A /org/service-profile/vnic-iscsi* # set auth-name initauth
UCS-A /org/service-profile/vnic-iscsi* # set identity dynamic-mac derived
UCS-A /org/service-profile/vnic-iscsi* # set iscsi-identity initiator-name iSCSI1
UCS-A /org/service-profile/vnic-iscsi* # set overlay-vnic-name eth1
UCS-A /org/service-profile/vnic-iscsi* # create eth-if
UCS-A /org/service-profile/vnic-iscsi/eth-if* # set vlanname default
UCS-A /org/service-profile/vnic-iscsi/eth-if* # commit buffer
```

次の作業

スタティック IP アドレス、設定された IP プールからの IP アドレス、または DHCP を使用してブートするように iSCSI イニシエータを設定します。

サービス プロファイルからの iSCSI vNIC の削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / と入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	サービス プロファイルのサービス プロファイル組織モードを開始します。
ステップ 3	UCS-A /org/service-profile # **delete vnic-iscsi** *iscsi-vnic-name*	指定したサービスプロファイルから指定した iSCSI vNIC を削除します。
ステップ 4	UCS-A /org/service-profile # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、scsivnic1 という iSCSI vNIC を削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # scope service-profile accounting
UCS-A /org/service-profile # delete vnic-iscsi scsivnic1
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile #
```

スタティック IP アドレスを使用してブートする iSCSI イニシエータの作成

サービス プロファイルで iSCSI イニシエータを作成し、スタティック IP アドレスを使用してブートするよう設定できます。

はじめる前に

次の設定が済んでいます。

- サービス プロファイルに iSCSI オーバーレイ vNIC を作成した。
- サービス プロファイルで iSCSI vNIC を作成した。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / と入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	サービス プロファイルのサービス プロファイル組織モードを開始します。
ステップ 3	UCS-A /org/service-profile # **scope vnic-iscsi** *iscsi-vnic-name*	指定した iSCSI vNIC のコンフィギュレーション モードを開始します。
ステップ 4	UCS-A /org/service-profile/iscsi-boot/vnic-iscsi # **create ip-if**	IP インターフェイスを作成します。
ステップ 5	UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/eth-if/ip-if* # **enter static-ip-params**	スタティック IP ブート パラメータを入力することを指定します。

	コマンドまたはアクション	目的
ステップ 6	UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/eth-if/ip-if/static-ip-params* # **set addr** *ip-address*	スタティック IP アドレスを指定します。
ステップ 7	UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/eth-if/ip-if/static-ip-params* # **set default-gw** *ip-address*	デフォルト ゲートウェイの IP アドレスを指定します。
ステップ 8	UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/eth-if/ip-if/static-ip-params* # **set primary-dns** *ip-address*	プライマリ DNS IP アドレスを指定します。
ステップ 9	UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/eth-if/ip-if/static-ip-params* # **set secondary-dns** *ip-address*	セカンダリ DNS IP アドレスを指定します。
ステップ 10	UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/eth-if/ip-if/static-ip-params* # **set subnet** *subnet-ip-address*	サブネット マスクを指定します。
ステップ 11	UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/eth-if/ip-if/static-ip-params* # **commit buffer**	トランザクションをシステム設定にコミットします。

次の例に、スタティック IP アドレスを使用してブートするようにイニシエータを設定し、トランザクションをコミットする方法を示します。

```
UCS-A # scope org
UCS-A /org # scope service-profile accounting
UCS-A /org/service-profile # scope vnic-iscsi iSCSI1
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi # create ip-if
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/ip-if* # enter static-ip-params
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/ip-if/static-ip-params* # set addr
10.104.105.193
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/ip-if/static-ip-params* # set default-gw
10.104.105.1
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/ip-if/static-ip-params* # set primary-dns
 11.11.11.100
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/ip-if/static-ip-params* # set secondary-dns
 11.11.11.100
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/ip-if/static-ip-params* # set subnet
255.255.255.0
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/ip-if/static-ip-params* # commit-buffer
```

次の作業

iSCSI ターゲットを作成します。

iSCSI イニシエータからのスタティック IP アドレス ブート パラメータの削除

サービス プロファイルで、iSCSI イニシエータからスタティック IP アドレス ブート パラメータを削除できます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / と入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	サービス プロファイルのサービス プロファイル組織モードを開始します。
ステップ 3	UCS-A /org/service-profile # **scope vnic-iscsi** *iscsi-vnic-name*	指定した iSCSI vNIC のコンフィギュレーション モードを開始します。
ステップ 4	UCS-A /org/service-profile/iscsi-boot/vnic-iscsi # **scope ip-if**	IP インターフェイスでコンフィギュレーション モードを開始します。
ステップ 5	UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/ip-if* # **delete static-ip-params**	イニシエータからスタティック IP ブート パラメータを削除します。
ステップ 6	UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/ip-if/static-ip-params* # **commit buffer**	トランザクションをシステム設定にコミットします。

次に、スタティック IP アドレス ブート パラメータをイニシエータから削除し、トランザクションをコミットする例を示します。

```
UCS-A # scope org
UCS-A /org # scope service-profile accounting
UCS-A /org/service-profile # scope vnic-iscsi iSCSI1
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi # scope ip-if
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/ip-if # delete static-ip-params
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/ip-if* # commit-buffer
```

IP プールからの IP アドレスを使用してブートする iSCSI イニシエータの作成

サービス プロファイルでは、iSCSI イニシエータを作成し、作成した IP プールからの IP アドレスを使用してブートするように設定できます。

はじめる前に

次の設定が済んでいます。

- サービス プロファイルにオーバーレイ vNIC を作成した
- サービス プロファイルで iSCSI vNIC を作成した。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / と入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	サービス プロファイルのサービス プロファイル組織モードを開始します。
ステップ 3	UCS-A /org/service-profile # **scope iscsi-boot**	iSCSI ブート パラメータを設定するコンフィギュレーション モードを開始します。
ステップ 4	UCS-A /org/service-profile/iscsi-boot # **scope vnic-iscsi** *iscsi-vnic-name*	指定した iSCSI vNIC のコンフィギュレーション モードを開始します。
ステップ 5	UCS-A /org/service-profile/iscsi-boot/vnic-iscsi* # **scope ip-if**	iSCSI イーサネット インターフェイスのコンフィギュレーション モードを開始します。
ステップ 6	UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/ip-if* # **enter pooled-ip-params**	以前に作成された iSCSI イニシエータ IP プールからの IP アドレスのいずれかを使用して iSCSI イニシエータ

	コマンドまたはアクション	目的
		がブートするよう指定します。
ステップ 7	UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/ip-if/pooled-ip-params* # **commit buffer**	トランザクションをシステム設定にコミットします。

次に、iSCSI イニシエータを作成し、IP プールからの IP アドレスを使用してブートするように設定する例を示します。

```
UCS-A # scope org
UCS-A /org # scope service-profile accounting
UCS-A /org/service-profile/iscsi-boot # scope vnic-iscsi iSCSI1
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi # scope ip-if
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/ip-if* # enter pooled-ip-params
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/ip-if/pooled-ip-params* # commit buffer
```

次の作業

iSCSI ターゲットを作成します。

iSCSI イニシエータからの IP プール ブート パラメータの削除

サービス プロファイルでは、iSCSI イニシエータを作成し、作成した IP プールからの IP アドレスを使用してブートするように設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / と入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	サービス プロファイルのサービスプロファイル組織モードを開始します。
ステップ 3	UCS-A /org/service-profile # **scope iscsi-boot**	iSCSI ブート パラメータを設定するコンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	UCS-A /org/service-profile/iscsi-boot/ # **scope vnic-iscsi** *iscsi-vnic-name*	指定した iSCSI vNIC のコンフィギュレーションモードを開始します。
ステップ 5	UCS-A /org/service-profile/iscsi-boot/vnic-iscsi # **enter ip-if**	IP インターフェイスでコンフィギュレーションモードを開始します。
ステップ 6	UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/ip-if* # **delete pooled-ip-params**	iSCSI イニシエータがブートのために IP プールからの IP アドレスを使用しないことを指定します。
ステップ 7	UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/ip-if/pooled-ip-params* # **commit buffer**	トランザクションをシステム設定にコミットします。

次に、IP アドレスを使用するブートを IP プール パラメータから削除し、トランザクションをコミットする例を示します。

```
UCS-A # scope org
UCS-A /org # scope service-profile accounting
UCS-A /org/service-profile # scope iscsi-boot
UCS-A /org/service-profile/iscsi-boot # scope vnic-iscsi iSCSI1
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi # enter ip-if
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/ip-if* # delete pooled-ip-params
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/ip-if/pooled-ip-params* # commit buffer
```

DHCP を使用してブートする iSCSI イニシエータの作成

サービス プロファイルで iSCSI イニシエータを作成し、DHCP を使用してブートするよう設定できます。

はじめる前に

次の設定が済んでいます。

- サービス プロファイルに iSCSI オーバーレイ vNIC を作成した。
- サービス プロファイルで iSCSI vNIC を作成した。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / と入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	サービス プロファイルのサービス プロファイル組織モードを開始します。
ステップ 3	UCS-A /org/service-profile # **scope iscsi-boot**	iSCSI ブート パラメータを設定するコンフィギュレーション モードを開始します。
ステップ 4	UCS-A /org/service-profile/iscsi-boot # **scope vnic-iscsi** *iscsi-vnic-name*	指定した iSCSI vNIC のコンフィギュレーション モードを開始します。
ステップ 5	UCS-A /org/service-profile/iscsi-boot/vnic-iscsi # **create ip-if**	IP インターフェイスを作成します。
ステップ 6	UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/ip-if* # **create dhcp-ip-params**	DHCP を使用してブートするようイニシエータを設定していることを指定します。
ステップ 7	UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/ip-if/dhcp-ip-params* # **commit buffer**	トランザクションをシステム設定にコミットします。

次の例に、DHCP を使用してブートするようにイニシエータを設定し、トランザクションをコミットする方法を示します。

```
UCS-A # scope org
UCS-A /org # scope service-profile accounting
UCS-A /org/service-profile # scope iscsi-boot
UCS-A /org/service-profile/iscsi-boot # scope vnic-iscsi iSCSI1
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi # create ip-if
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/ip-if* # create dhcp-ip-params
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/ip-if/dhcp-ip-params* # commit-buffer
```

次の作業

iSCSI ターゲットを作成します。

iSCSI イニシエータからの DHCP ブート パラメータの削除

サービス プロファイルで、iSCSI イニシエータから DHCP ブート パラメータを削除できます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / と入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	サービス プロファイルのサービス プロファイル組織モードを開始します。
ステップ 3	UCS-A /org/service-profile # **scope iscsi-boot**	iSCSI ブート パラメータを設定するコンフィギュレーション モードを開始します。
ステップ 4	UCS-A /org/service-profile/iscsi-boot # **scope vnic-iscsi** *iscsi-vnic-name*	指定した iSCSI vNIC のコンフィギュレーション モードを開始します。
ステップ 5	UCS-A /org/service-profile/iscsi-boot/vnic-iscsi # **enter ip-if**	IP インターフェイスでコンフィギュレーション モードを開始します。
ステップ 6	UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/ip-if* # **delete dhcp-ip-params**	イニシエータがブートのために DHCP を使用しないことを指定します。
ステップ 7	UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/ip-if/dhcp-ip-params* # **commit buffer**	トランザクションをシステム設定にコミットします。

次に、DHCP パラメータを使用してブート削除し、トランザクションをコミットする例を示します。

```
UCS-A # scope org
UCS-A /org # scope service-profile accounting
UCS-A /org/service-profile # scope iscsi-boot
UCS-A /org/service-profile/iscsi-boot # scope vnic-iscsi iSCSI1
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi # enter ip-if
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/ip-if* # delete dhcp-ip-params
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/ip-if/dhcp-ip-params* # commit-buffer
```

IQN プール

IQN プールは、iSCSI vNIC が Cisco UCS ドメインでイニシエータ ID として使用する iSCSI 修飾名（IQN）の集合です。

IQN プール メンバは、プレフィックス:サフィックス:数字の形式になります。ここで、プレフィックス、サフィックス、および数字のブロック（範囲）を指定することができます。

IQN プールは複数の IQN ブロックを含むことができます。それらは、数字の範囲とサフィックスは異なりますが、同じプレフィックスを共有します。

IQN プールの作成

（注） ほとんどの場合、最大 IQN サイズ（プレフィックス + サフィックス + 追加文字）は 223 文字です。Cisco UCS NIC M51KR-B アダプタを使用する場合、IQN サイズを 128 文字に制限する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルート組織モードを開始するには、*/* を *org-name* として入力します。
ステップ 2	UCS-A /org # **create iqn-pool** *pool-name*	指定されたプール名前で IQN プールを作成し、組織 IQN プール モードを開始します。 この名前には、1 ～ 32 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
ステップ 3	UCS-A /org/iqn-pool # **set iqn-prefix** *prefix*	IQN ブロック メンバーのプレフィックスを指定します。アダプタ カードによって制限されない限り、プレフィックスには最大 150 文字を使用できます。
ステップ 4	UCS-A /org/iqn-pool # **set descr** *description*	（任意） IQN プールの説明を記入します。256 文字以内で入力します。

	コマンドまたはアクション	目的
		（注） 説明にスペース、特殊文字、または句読点が含まれている場合は、説明を引用符で括る必要があります。引用符は、**show** コマンド出力の説明フィールドには表示されません。
ステップ 5	UCS-A /org/iqn-pool # **set assignmentorder** {**default** | **sequential**}	次のいずれかになります。 • **default**：Cisco UCS Manager はプールからランダム ID を選択します。 • **sequential**：Cisco UCS Manager はプールから最も小さい使用可能 ID を選択します。
ステップ 6	UCS-A /org/iqn-pool # **create block** *suffix from to*	IQN ブロック（範囲）を作成し、組織 IQN プール ブロック モードを開始します。ベース サフィックス、サフィックス開始番号、およびサフィックス終了番号を指定する必要があります。最終的な IQN プール メンバーは *prefix*:*suffix*:*number* という形式になります。サフィックスは最大 64 文字まで使用できます。 （注） IQN プールには、複数の IQN ブロックを含めることができます。複数のブロックを作成するには、組織 IQN プール モードから複数の **create block** コマンドを入力します。
ステップ 7	UCS-A /org/iqn-pool/block # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、pool4 という名前の IQN プールを作成し、プールの説明を記入し、プールに使用されるプレフィックスおよびサフィックス ブロックを指定し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # create iqn-pool pool4
UCS-A /org/iqn-pool* # set iqn-prefix iqn.alpha.com
UCS-A /org/iqn-pool* # set descr "This is IQN pool 4"
UCS-A /org/iqn-pool* # create block beta 3 5
UCS-A /org/iqn-pool/block* # commit-buffer
UCS-A /org/iqn-pool/block #
```

次の作業

IQN サフィックス プールをサービス プロファイルとテンプレートに含めます。

IQN プールへのブロックの追加

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **scope iqn-pool** *pool-name*	指定したプールの組織 IQN プール モードを開始します。
ステップ 3	UCS-A /org/iqn-pool # **create block** *suffix from to*	IQN サフィックスのブロック（範囲）を作成し、組織 IQN プール ブロック モードを開始します。ベース サフィックス、サフィックス開始番号、およびサフィックス終了番号を指定する必要があります。最終的な IQN プール メンバーは *prefix*:*suffix*:*number* という形式になります。 （注） IQN プールには、複数の IQN ブロックを含めることができます。複数のブロックを作成するには、組織 IQN プール モードから複数の **create block** コマンドを入力します。
ステップ 4	UCS-A /org/iqn-pool/block # **commit-buffer**	トランザクションをシステム設定にコミットします。
ステップ 5	UCS-A /org/iqn-pool/block # **exit**	（任意） 組織 IQN プール モードに戻ります。
ステップ 6	UCS-A /org/iqn-pool # **show block**	（任意） サフィックスのブロックを表示します。

この例では、IQN サフィックスのブロックを pool4 という名前の IQN プールに追加し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org # scope iqn-pool pool4
UCS-A /org/iqn-pool # create block beta 3 5
UCS-A /org/iqn-pool/block* # commit-buffer
UCS-A /org/iqn-pool/block # exit
UCS-A /org/iqn-pool # show block
Block of IQN Names:
    Suffix     From  To
    ---------- ----- --
    beta           3     5

UCS-A /org/iqn-pool #
```

IQN プールからのブロックの削除

プールからアドレスブロックを削除した場合、Cisco UCS Manager では、そのブロック内から vNIC または vHBA に割り当てられていたアドレスは再割り当てされません。削除されたブロックのすべての割り当て済みブロックは、次のいずれかが起きるまで、割り当てられた vNIC または vHBA に残ります。

- 関連付けられたサービス プロファイルが削除された場合。
- アドレスが割り当てられた vNIC または vHBA が削除された場合。
- vNIC または vHBA が異なるプールに割り当てられた場合。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **scope iqn-pool** *pool-name*	指定したプールの組織 IQN プール モードを開始します。
ステップ 3	UCS-A /org/iqn-pool # **delete block** *suffix from to*	IQN のブロック（範囲）を削除します。削除するブロック内のベース サフィクス、最初と最後の数を指定します。
ステップ 4	UCS-A /org/iqn-pool # **commit-buffer**	トランザクションをシステム設定にコミットします。

この例では、サフィックスのブロックを pool4 という名前の IQN プールから削除し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org # scope iqn-pool pool4
UCS-A /org/iqn-pool # delete block beta 0 12
UCS-A /org/iqn-pool* # commit-buffer
UCS-A /org/iqn-pool #
```

IQN プールの削除

プールを削除した場合、Cisco UCS Manager は、 でプールの vNIC または vHBA に割り当てられたアドレスを再割り当てしません。削除されたプールのすべての割り当て済みブロックは、次のいずれかが起きるまで、割り当てられた vNIC または vHBA に残ります。

- 関連付けられたサービス プロファイルが削除された場合。

- アドレスが割り当てられた vNIC または vHBA が削除された場合。
- vNIC または vHBA が異なるプールに割り当てられた場合。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルート組織モードを開始するには、/ を *org-name* として入力します。
ステップ 2	UCS-A /org # **delete iqn-pool** *pool-name*	指定された IQN プールを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、pool4 という名前の IQN プールを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # delete iqn-pool pool4
UCS-A /org* # commit-buffer
UCS-A /org #
```

IQN プール使用の表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルート組織モードを開始するには、/ を *org-name* として入力します。
ステップ 2	UCS-A /org # **scope iqn-pool** *pool-name*	指定したプールの組織 IQN プール モードを開始します。
ステップ 3	UCS-A /org/iqn-pool # **show pooled**	IQN ブロック メンバの割り当てを表示します。

次に、pool4 という名前の IQN プールにおけるサフィックスの割り当てを表示する例を示します。

```
UCS-A# scope org /
UCS-A /org # scope iqn-pool pool4
UCS-A /org/iqn-pool # show pooled
Pooled:
    Name       Assigned Assigned To Dn
    ---------- -------- --------------
```

```
    beta:3      No
    beta:4      No
    beta:5      No

UCS-A /org/iqn-pool #
```

iSCSI スタティック ターゲットの作成

スタティック ターゲットを作成できます。

はじめる前に

iSCSI vNIC を作成済みです。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルー織モードを開始するには、*org-name* に / と入力す。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	iSCSI ターゲットを追加するサービス プロファのサービス プロファイル組織モードを開始しま
ステップ 3	UCS-A /org/service-profile # **scope iscsi-boot**	iSCSI ブート パラメータを設定するモードを開ます。
ステップ 4	UCS-A /org/service-profile/iscsi-boot # **scope vnic-iscsi** *iscsi-vnic-name*	指定した vNIC 名で iSCSI vNIC モードを開始しま
ステップ 5	UCS-A /org/service-profile/iscsi-boot/vnic-iscsi # **create static-target-if** {**1** | **2**}	iSCSI vNIC のスタティック ターゲットを作成しライオリティ レベルを指定します。 有効なプライオリティ レベルは 1 または 2 です
ステップ 6	UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/static-target-if # **set name** *name*	iSCSI ターゲットの iSCSI Qualified Name（IQN）は拡張固有識別子（EUI）の名前を定義する正規現。 任意の英数字および次の特殊文字を入力するこできます。 • .（ピリオド） • :（コロン） • -（ダッシュ）

	コマンドまたはアクション	目的
		重要 この名前は、標準 IQN または EUI のラインを使用して正しい形式にする必ります。 次に、正しい形式の iSCSI ターゲット名の例ます。 • iqn.2001-04.com.example • iqn.2001-04.com.example:storage:diskarrays-sn- • iqn.2001-04.com.example:storage.tape1.sys • iqn.2001-04.com.example:storage.disk2.sys • eui.02004567A425678D
ステップ 7	UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/static-target-if # **set port** *port-num*	iSCSI ターゲットに関連付けられたポート。 1 ～ 65535 の整数を入力します。デフォルトです。
ステップ 8	UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/static-target-if # **set auth-name** *auth-profile*	（任意） ターゲットがそれ自体を認証する必要がありプロファイルを設定済みの場合、認証プロフの名前を指定する必要があります。 関連付けられた iSCSI 認証プロファイルの名
ステップ 9	UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/static-target-if # **set ipaddress** *ipv4-address*	iSCSI ターゲットに割り当てられた IPv4 アド
ステップ 10	UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/static-target-if # **create lun**	インターフェイスの位置に対応する LUN を作す。
ステップ 11	UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/static-target-if/lun* # **set id** *id-number*	ターゲット LUN ID を指定します。有効値は65535 です。
ステップ 12	UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/static-target-if/lun* # **exit**	現在のコンフィギュレーションモードを終了
ステップ 13	UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/static-target-if # **exit**	現在のコンフィギュレーションモードを終了
ステップ 14	UCS-A /org/service-profile/iscsi-boot/vnic-iscsi # **commit-buffer**	トランザクションをシステム設定にコミット

	コマンドまたはアクション	目的
ステップ 15	ステップ 5 ～ 14 を繰り返して 2 番目のスタティック ターゲットを作成します。	（任意）

次に、2 つの iSCSI スタティック ターゲット インターフェイスを作成して、トランザクションをコミットする例を示します。

```
UCS-A # scope org test
UCS-A /org # scope service-profile accounting
UCS-A /org/service-profile # scope iscsi-boot
UCS-A /org/service-profile/iscsi-boot # scope vnic-iscsi iSCSI1
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi # create static-target-if 1
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/static-target-if* # set name statictarget1
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/static-target-if* # set port 3260
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/static-target-if* # set auth-name
authprofile1
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/static-target-if* # set ip-address
192.168.10.10
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/static-target-if* # create lun
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/static-target-if/lun* # set id 1
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/static-target-if/lun* # exit
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/static-target-if* # exit
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi # commit-buffer
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi # create static-target-if 2
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/static-target-if* # set ipaddress
192.168.10.11
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/static-target-if* # set name statictarget2
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/static-target-if* # set port 3260
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/static-target-if* # set auth-name
authprofile1
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/static-target-if* # create lun
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/static-target-if/lun* # set id 1
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/static-target-if/lun* # exit
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/static-target-if* # exit
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi # commit-buffer
```

次の作業

2 番目の iSCSI デバイスを設定するには、iSCSI vNIC、イニシエータおよびターゲットを作成する手順を繰り返します。

iSCSI スタティック ターゲットの削除

iSCSI スタティック ターゲットを削除できます。ただし、1 つの iSCSI スタティック ターゲットを削除した後、少なくとも 1 つの iSCSI スタティック ターゲットが残るようにする必要があります。したがって、1 つの iSCSI スタティック ターゲットを削除するには、2 つの iSCSI スタティック ターゲットが必要です。

（注） 2 つの iSCSI ターゲットがあり、優先順位 1 位のターゲットを削除すると、優先順位 2 位のターゲットが優先順位 1 位のターゲットになります。ただし、このターゲットは、Cisco UCS Manager では、引き続き優先順位 2 位のターゲットとして表示されます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / と入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	iSCSI ターゲットを追加するサービス プロファイルのサービスプロファイル組織モードを開始します。
ステップ 3	UCS-A /org/service-profile # **scope iscsi-boot**	iSCSI ブート パラメータを設定するモードを開始します。
ステップ 4	UCS-A /org/service-profile/iscsi-boot # **scope vnic-iscsi** *iscsi-vnic-name*	指定した vNIC 名で iSCSI vNIC モードを開始します。
ステップ 5	UCS-A /org/service-profile/iscsi-boot/vnic-iscsi # **delete static-target-if**	iSCSI vNIC のスタティック ターゲットを削除します。
ステップ 6	UCS-A /org/service-profile/iscsi-boot/vnic-iscsi # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、iSCSI スタティック ターゲットを削除してトランザクションをコミットする例を示します。

```
UCS-A # scope org test
UCS-A /org # scope service-profile sample
UCS-A /org # scope iscsi-boot
UCS-A /org/service-profile/iscsi-boot # scope vnic-iscsi trial
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi # delete static-target-if 1
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi # commit-buffer
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi #
```

iSCSI 自動ターゲットの作成

ベンダー ID の有無にかかわらず iSCSI 自動ターゲットを作成できます。

はじめる前に

iSCSI 自動ターゲットを作成する前に、これらの前提条件に適合する必要があります。

- すでにサービス プロファイルに iSCSI vNIC を作成してある。

- 使用している VIC の前提条件を検討した。詳細については、次を参照してください。 iSCSI ブートのガイドラインと前提条件, （587 ページ）

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / と入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	iSCSI ターゲット インターフェイスを追加するサービス プロファイルのサービス プロファイル組織モードを開始します。
ステップ 3	UCS-A /org # **scope iscsi-boot** 例：	iSCSI ブート パラメータを設定するモードを開始します。
ステップ 4	UCS-A /org/service-profile/iscsi-boot # **scope vnic-iscsi** *iscsi-vnic-name*	指定した vNIC 名の iSCSI vNIC サービス プロファイル組織モードを開始します。
ステップ 5	UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/ # **create auto-target-if**	iSCSI vNIC の自動ターゲットを作成します。 ベンダー ID なしで自動ターゲットを使用する場合は、イニシエータの名前を設定する必要があります。詳細については、サービス プロファイルでの iSCSI vNIC の作成を参照してください。
ステップ 6	UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/auto-target-if* # **set dhcp-vendor-id** *vendor-id*	（任意） 自動ターゲットのベンダー ID を設定します。ベンダー ID には、最大 32 文字の英数字を指定できます。
ステップ 7	UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/auto-target-if* # **exit**	現在のコンフィギュレーション モードを終了します。
ステップ 8	UCS-A /org/service-profile/iscis-boot/vnic-iscsi # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、iSCSI 自動ターゲットをベンダー ID なしで作成してトランザクションをコミットする例を示します。

```
UCS-A # scope org
UCS-A /org # scope service-profile accounting
UCS-A /org/service-profile # scope iscsi-boot
UCS-A /org/service-profile/iscsi-boot # scope vnic-iscsi iSCSI1
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi # create auto-target-if
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/auto-target-if* # exit
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi # commit-buffer
```

次に、iSCSI 自動ターゲットをベンダー ID ありで作成してトランザクションをコミットする例を示します。

```
UCS-A # scope org
UCS-A /org # scope service-profile accounting
UCS-A /org/service-profile # scope iscsi-boot
UCS-A /org/service-profile/iscsi-boot # scope vnic-iscsi iSCSI1
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi # create auto-target-if
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/auto-target-if* # set dhcp-vendor-id
iSCSI_Vendor
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi/auto-target-if* # exit
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi # commit-buffer
```

次の作業

2 番目の iSCSI デバイスを設定するには、iSCSI vNIC、イニシエータおよびターゲットを作成する手順を繰り返します。

iSCSI 自動ターゲットの削除

スタティック ターゲット セットがある場合にのみ自動ターゲットを削除できます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / と入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	iSCSI ターゲットを追加するサービス プロファイルでサービス プロファイル モードを開始します。
ステップ 3	UCS-A /org/service-profile # **scope iscsi-boot**	iSCSI ブート パラメータを設定するモードを開始します。
ステップ 4	UCS-A /org/service-profile/iscsi-boot # **scope vnic-iscsi** *iscsi-vnic-name*	指定した vNIC 名で iSCSI vNIC モードを開始します。
ステップ 5	UCS-A /org/service-profile/iscsi-boot/vnic-iscsi # **delete auto-target-if**	自動ターゲットを削除します。

	コマンドまたはアクション	目的
ステップ 6	UCS-A /org/service-profile/iscsi-boot/vnic-iscsi # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、iSCSI 自動ターゲットを削除し、トランザクションをコミットする例を示します。

```
UCS-A # scope org test
UCS-A /org # scope service-profile accounting
UCS-A /org/service-profile # scope iscsi-boot
UCS-A /org/service-profile/iscsi-boot # scope vnic-iscsi iSCSI1
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi # delete auto-target-if
UCS-A /org/service-profile/iscsi-boot/vnic-iscsi # commit-buffer
```

iSCSI ブートの確認

アダプタがブート中の場合、KVM コンソールを使用してブートアップ メッセージを確認します。KVM コンソールにアクセスする方法については、「*Starting the KVM Console*」の章を参照してください。

この手順は、Cisco UCS Manager GUI を使用した場合にのみ実行できます。詳細については、『*UCS Manager GUI Configuration Guide*』の「*Starting the KVM Console*」の章を参照してください。

- Cisco UCS M51KR-B Broadcom BCM57711 では、次のメッセージが表示されます。
  第 1 iSCSI ターゲットへログイン中です。（Logging in the 1st iSCSI Target….）成功しました。（Succeeded.）
- Cisco UCS M81KR 仮想インターフェイス カード では、次のメッセージが表示されます。
  オプション ROM が正常にインストールされました（Option ROM installed successfully.）

LAN ブート

LAN の集中プロビジョニング サーバから 1 つまたは複数のサーバをブートするブート ポリシーを設定できます。LAN（または PXE）ブートは、その LAN サーバからサーバに OS をインストールする際に頻繁に使用されます。

LAN ブート ポリシーには、複数のタイプのブート デバイスを追加できます。たとえば、ローカル ディスクや仮想メディア ブートをセカンダリ ブート デバイスとして追加できます。

ブート ポリシー用 LAN ブートの設定

はじめる前に

LAN ブート設定を含めるブート ポリシーを作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に **/** を入力します。
ステップ 2	UCS-A /org # **scope boot-policy** *policy-name*	指定されたブート ポリシーの組織ブート ポリシー モードを開始します。
ステップ 3	UCS-A /org/boot-policy #**create lan**	ブート ポリシーの LAN ブートを作成し、組織ブート ポリシーLAN モードを開始します。
ステップ 4	UCS-A /org/boot-policy/lan # **set order** {**1** | **2** | **3** | **4**}	LAN ブートのブート順序を指定します。
ステップ 5	UCS-A /org/boot-policy/lan #**create path** {**primary** | **secondary**}	プライマリまたはセカンダリ LAN ブート パスを作成し、組織ブート ポリシーの LAN パス モードを開始します。
ステップ 6	UCS-A /org/boot-policy/lan/path #**set vnic** *vnic-name*	ブート イメージへの LAN パスとして vNIC を使用するよう指定します。
ステップ 7	UCS-A /org/boot-policy/lan/path #**commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、lab2-boot-policy というブート ポリシーに入り、ポリシーに LAN ブートを作成し、ブート順序を 2 に設定し、vNIC1 および vNIC2 という名前の vNIC を使用するプライマリとセカンダリのパスを作成し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org* # scope boot-policy lab2-boot-policy
UCS-A /org/boot-policy* # create lan
UCS-A /org/boot-policy/lan* # set order 2
UCS-A /org/boot-policy/lan* # create path primary
UCS-A /org/boot-policy/lan/path* # set vnic vNIC1
UCS-A /org/boot-policy/lan/path* # exit
UCS-A /org/boot-policy/lan* # create path secondary
UCS-A /org/boot-policy/lan/path* # set vnic vNIC2
UCS-A /org/boot-policy/lan/path* # commit-buffer
UCS-A /org/boot-policy/lan/path #
```

次の作業

ブート ポリシーをサービス プロファイルとテンプレートに含めます。

ローカル デバイス ブート

Cisco UCS Manager では、異なるローカル デバイスから起動することができます。

（注） 拡張ブート順序を使用している Cisco UCS M3 および M4 ブレード/ラック サーバの場合は、最上位と第 2 レベルの両方のブート デバイスを選択できます。標準のブート順序を使用している Cisco UCS M1 および M2 ブレード/ラック サーバの場合は、最上位のデバイスのみを選択できます。

ローカル ディスク ブート

サーバにローカル ドライブがある場合、ブート ポリシーを設定して、トップレベルのローカル ディスク デバイスまたは第 2 レベルのデバイスのいずれかからサーバを起動できます。

- [ローカル LUN（Local LUN）]：ローカル ディスクまたはローカル LUN からの起動を有効にします。
- [ローカル JBOD（Local JBOD）]：ブート可能な JBOD からの起動を有効にします。
- [SD カード（SD card）]：SD カードからの起動を有効にします。
- [内部 USB（Internal USB）]：内部 USB からの起動を有効にします。
- [外部 USB（External USB）]：外部 USB からの起動を有効にします。
- [内蔵ローカル LUN（Embedded Local LUN）]：Cisco UCS C240 M4 サーバ上の内蔵ローカル LUN からの起動を有効にします。
- [内蔵ローカル ディスク（Embedded Local Disk）]：Cisco UCS C240 M4SX および M4L サーバの内蔵ローカル ディスクからの起動を有効にします。

（注） 第 2 レベルのデバイスは、拡張ブート順序を使用している Cisco UCS M3 および M4 ブレード/ラック サーバでのみ使用できます。標準のブート順序を使用している Cisco UCS M1 および M2 ブレード/ラック サーバの場合は、最上位の [ローカル ディスクの追加（Add Local Disk）] のみを選択できます。

仮想メディア ブート

サーバがアクセスできる仮想メディア デバイスから 1 つ以上のサーバをブートするよう、ブート ポリシーを設定することができます。仮想メディア デバイスは、物理 CD/DVD ディスク（読み取り専用）またはフロッピー ディスク（読み取り書き込み）のサーバへの挿入を疑似的に実行します。このタイプのサーバ ブートは、オペレーティング システムをサーバに手動でインストールする場合に使用するのが一般的です。

（注） 第 2 レベルのデバイスは、拡張ブート順序を使用している Cisco UCS M3 および M4 ブレード/ラック サーバでのみ使用できます。標準のブート順序を使用している Cisco UCS M1 および M2 ブレード/ラック サーバの場合は、最上位の [CD/DVD の追加（Add CD/DVD）] または [フロッピーの追加（Add Floppy）] のみを選択できます。

リモート仮想ドライブのブート

ブート ポリシーを設定して、サーバからアクセスできるリモート仮想ドライブから 1 つ以上のサーバを起動できます。

ブート ポリシー用ローカル ディスク ブート ポリシー設定

サービス プロファイルまたはサービス プロファイル テンプレートに制限されたローカル ブート ポリシーを作成することもできます。しかし、複数のサービスプロファイルまたはサービスプロファイル テンプレートに含むことのできるグローバルなブート ポリシーの作成を推奨します。

ブート ポリシーには、複数のタイプのブート デバイスを追加できます。たとえば、セカンダリ ブート デバイスとして、仮想メディア ブートを追加できます。

（注） リリース 2.2 以降では、ブート順序にトップレベルのローカル ストレージ デバイスを追加するには、**create local** コマンドの後に **create local-any** を使用します。ローカル ストレージ デバイスを含む以前のリリースからのポリシーがある場合は、それらはアップグレード中に local-any を使用するように変更されます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **scope boot-policy** *policy-name*	指定されたブート ポリシーの組織ブート ポリシー モードを開始します。
ステップ 3	UCS-A /org/boot-policy #**create storage**	ブート ポリシーのストレージブートを作成し、組織ブート ポリシー ストレージ モードを開始します。
ステップ 4	UCS-A /org/boot-policy/storage #**create local**	ローカル ストレージの場所を作成し、ブート ポリシーのローカル ストレージ モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	UCS-A /org/boot-policy/storage/local/ # **create** {**local-any** | **local-lun** | **sd-card** | **usb-extern** | **usb-intern** }	ローカル ストレージのタイプを指定します。次のいずれかになります。 • [local-any]：ローカル ストレージ デバイスのタイプ。このオプションは、レガシーまたは UEFI のブート モードで使用できます。 （注） 標準のブート順序を使用している Cisco UCS M1 および M2 のブレード サーバおよびラック サーバは local-any のみ使用できます。 • [local-lun]：ローカルのハード ディスク ドライブ。 • [sd-card]：SD カード。 • [usb-extern]：外部 USB カード。 • [usb-intern]：内部 USB カード。 拡張ブート順序を使用している Cisco UCS M3 および M4 ブレード/ラック サーバの場合は、最上位と第2レベルの両方のブート デバイスを選択できます。標準のブート順序を使用している Cisco UCS M1 および M2 ブレード/ラック サーバの場合は、最上位のデバイスのみを選択できます。
ステップ 6	UCS-A /org/boot-policy/storage/local/*local-storage-device* # **set order** *order_number*	指定したローカル ストレージ デバイスのブート順序を設定します。1 ～ 16 の整数を入力します。 Cisco UCS サーバで拡張ブート順序を使用する場合は、定義したブート順序が使用されます。用語「プライマリ」または「セカンダリ」を使用した標準のブート モードは、ブート順序を示唆するものではありません。同じデバイス クラス内での実際のブート順序は、PCIe バス スキャン順序により決定されます。

	コマンドまたはアクション	目的
ステップ 7	UCS-A /org/boot-policy/storage/local/*local-storage-device* # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、lab1-boot-policy という名前のブート ポリシーを作成し、そのポリシーのローカル ハード ディスク ドライブのブートを作成し、ブート順序を 3 に設定し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org* # scope boot-policy lab1-boot-policy
UCS-A /org/boot-policy* # create storage
UCS-A /org/boot-policy/storage* # create local
UCS-A /org/boot-policy/storage/local* # create local-lun
UCS-A /org/boot-policy/storage/local/sd-card* # set order 3
UCS-A /org/boot-policy/storage/local/sd-card* # commit-buffer
UCS-A /org/boot-policy/storage/local/sd-card #
```

次の例では、サービス プロファイル SP_lab1 のローカル SD カード ブートを作成し、ブート順序を 3 に設定し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org* # scope service-profile SP_lab1
UCS-A /org/service-profile # create boot-definition
UCS-A /org/service-profile/boot-definition* # create storage
UCS-A /org/service-profile/boot-definition/storage* # create local
UCS-A /org/service-profile/boot-definition/storage/local* # create sd-card
UCS-A /org/service-profile/boot-definition/storage/local* # set order 3
UCS-A /org/service-profile/boot-definition/storage/local* # commit-buffer
UCS-A /org/service-profile/boot-definition/storage/local #
```

次の例では、サービス プロファイル SP_lab1 のトップレベルのローカル デバイス ブートを作成し、ブート順序を 3 に設定し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org* # scope service-profile SP_lab1
UCS-A /org/service-profile # create boot-definition
UCS-A /org/service-profile/boot-definition* # create storage
UCS-A /org/service-profile/boot-definition/storage* # create local
UCS-A /org/service-profile/boot-definition/storage/local* # create local-any
UCS-A /org/service-profile/boot-definition/storage/local/local-any* # set order 3
UCS-A /org/service-profile/boot-definition/storage/local/local-any* # commit-buffer
UCS-A /org/service-profile/boot-definition/storage/local/local-any #
```

次の作業

ブート ポリシーをサービス プロファイルとテンプレートに含めます。

ブート ポリシー用仮想メディア ブートの設定

（注） 仮想メディアでは、USB を有効にする必要があります。USB の機能に影響する BIOS 設定を変更した場合は、仮想メディアにも影響します。したがって、最適なパフォーマンスを実現するためには、次の USB BIOS をデフォルト設定のままにしておくことを推奨します。

- [デバイスを起動不可にする（Make Device Non Bootable）]：[無効（disabled）] に設定します。
- [USB アイドル電源の最適化設定（USB Idle Power Optimizing Setting）]：[高パフォーマンス（high-performance）] に設定します。

はじめる前に

仮想メディア ブート設定を含めるブート ポリシーを作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **scope boot-policy** *policy-name*	指定されたブート ポリシーの組織ブート ポリシー モードを開始します。
ステップ 3	UCS-A /org/boot-policy #**create virtual-media** {**read-only** | **read-only-local** | **read-only-remote** | **read-write** | **read-write-drive** | **read-write-local** | **read-write-remote**}	ブート ポリシーの指定仮想メディア ブートを作成し、組織ブート ポリシーの仮想メディア モードを開始します。次のいずれかになります。 • [read-only]：ローカルまたはリモート CD/DVD。このオプションは、レガシーまたは UEFI のブート モードで使用できます。 • [read-only-local]：ローカル CD/DVD。 • [read-only-remote]：リモート CD/DVD。 • [read-write]：ローカルまたはリモート フロッピー ディスク ドライブ。このオプションは、レガシーまたは UEFI のブート モードで使用できます。 • [read-write-drive]：リモート USB ドライブ。 • [read-write-local]：ローカル フロッピー ディスク ドライブ。

	コマンドまたはアクション	目的
		• [read-write-remote]：リモート フロッピー ディスク ドライブ。 （注） 拡張ブート順序を使用している Cisco UCS M3 および M4 ブレード/ラック サーバの場合は、最上位と第 2 レベルの両方のブート デバイスを選択できます。標準のブート順序を使用している Cisco UCS M1 および M2 ブレード/ラック サーバの場合は、最上位のデバイスのみを選択できます。
ステップ 4	UCS-A /org/boot-policy/virtual-media # **set order** *order_number*	仮想メディア ブートのブート順序を設定します。1 ～ 16 の整数を入力します。
ステップ 5	UCS-A /org/boot-policy/virtual-media #**commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、lab3-boot-policy という名前のブート ポリシーを開始し、CD/DVD 仮想メディア ブートを作成し、ブート順序を 3 に設定し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org* # scope boot-policy lab3-boot-policy
UCS-A /org/boot-policy* # create virtual-media read-only-local
UCS-A /org/boot-policy/virtual-media* # set order 3
UCS-A /org/boot-policy/virtual-media* # commit-buffer
```

次の作業

ブート ポリシーをサービス プロファイルとテンプレートに含めます。

CIMC vMedia ブート ポリシーの作成

サービス プロファイルまたはサービス プロファイル テンプレートに制限されたローカル ブート ポリシーを作成することもできます。しかし、複数のサービスプロファイルまたはサービスプロファイル テンプレートに含むことのできるグローバルなブート ポリシーの作成を推奨します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /org # **create boot-policy** *policy-name*	ブート ポリシーを指定されたポリシー名で作成し、組織ブート ポリシー モードを開始します。
ステップ 3	UCS-A /org/boot-policy* # **create virtual-media** *?*	アクセスと起動が可能なローカルおよびリモートのデバイスのリストを表示します。
ステップ 4	UCS-A /org/boot-policy* # **create virtual-media** {**access** | **vMediaMappingName**}	アクセスと起動が可能なローカルおよびリモートのデバイスのリストを表示します。
ステップ 5	UCS-A /org/boot-policy* # **create virtual-media read-write-remote-drive vMediaMap0**}	指定した vMedia に対する vMedia ブート デバイス構成を作成します。
ステップ 6	UCS-A /org/boot-policy/virtual-media* # **commit-buffer**	トランザクションをシステム設定にコミットします。
ステップ 7	UCS-A /org/boot-policy/virtual-media* # **show detail expand**	次のブート順序を表示します。 **ブート仮想メディア**： [順序（Order）]：1 [アクセス（Access）]：読み取り/書き込みリモート vMedia ドライブ [名前（Name）]：vmediaMap0

次に、CIMC vMedia ブート ポリシーを作成する例を示します。

```
UCS-A# scope org /
UCS-A /org* # create boot-policy boot-policy vm-vmediamap-boot
UCS-A /org/boot-policy* # create virtual-media
```

CIMC vMedia マウントの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *chassis_id*/*blade_id*	指定サーバのシャーシ サーバ モードを開始します。
ステップ 2	UCS-A# /chassis/server #**scope cimc**	CIMC モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /chassis/server/cimc # **show vmedia-mapping-list detail expand**	vMediaマッピングの詳細を表示します。

次に、CIMC vMedia のマウントを表示する例を示します。

```
UCS-A# scope server 1/2
UCS-A /chassis/server # scope cimc
UCS-A /chassis/server/cimc # show vmedia-mapping-list detail expand

vMedia Mapping List:
vMedia Mapping:
Disk Id: 1
Mapping Name: cdd
Device Type: Cdd
Remote IP: 172.31.1.167
Image Path: cifs
Image File Name: ubunt-14.11-desktop-i386.iso
Mount Protocol: Cifs
Mount Status: Mounted
Error: None
Password:
User ID: Adminstrator

UCS-A /chassis/server/cimc #
```

ブート ポリシーの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / と入力します。
ステップ 2	UCS-A /org # **delete boot-policy** *policy-name*	指定されたブート ポリシーを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、boot-policy-LAN という名前のブート ポリシーを削除し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # delete boot-policy boot-policy-LAN
UCS-A /org* # commit-buffer
UCS-A /org #
```

UEFI ブート パラメータ

サーバの UEFI ブート モードは、プラットフォーム ハードウェアに保存されている情報によって決まります。UEFI OS ブート ローダに関する情報を含むブート エントリは、サーバの BIOS フラッシュに保存されます。2.2(4) より前の Cisco UCS Manager リリースでは、サービス プロファイルがあるサーバから別のサーバに移行されると、ブートローダ情報は宛先サーバで使用できなくなります。そのため、BIOS は、サーバを UEFI ブート モードでブートするためのブート ローダ情報をロードできません。

Cisco UCSM リリース 2.2(4) では、宛先サーバ上の UEFI OS ブート ローダの位置に関する情報を BIOS に提供する UEFI ブート パラメータが導入され、BIOS はその位置からブート ローダをロードできます。サーバは、そのブート ローダ情報を使用して、UEFI ブート モードでブートできます。

UEFI ブート パラメータに関する注意事項と制約事項

- ブート モードが UEFI の場合のみ、UEFI ブート パラメータを設定できます。
- Cisco UCS Manager をリリース 2.2(4) にアップグレードする場合は、サービス プロファイルの移行中に UEFI ブートが失敗しても自動的に処理されません。UEFI 対応 OS で正常にブートするには、ターゲット デバイスで UEFI ブート パラメータを明示的に作成しておく必要があります。
- UEFI ブート パラメータは、セカンドレベルのブート順序をサポートする、M3 以降のすべてのサーバでサポートされています。
- 次のデバイス タイプの UEFI ブート パラメータを指定できます。
  - SAN LUN
  - ISCSI LUN
  - ローカル LUN
- UEFI ブート パラメータは各オペレーティング システム固有のパラメータです。次のオペレーティング システムの UEFI ブート パラメータを指定できます。
  - VMware ESX
  - SUSE Linux
  - Microsoft Windows
  - Red Hat Enterprise Linux 7

ローカル LUN の UEFI ブート パラメータの設定

はじめる前に

ローカル LUN のブート モードが UEFI に設定されていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **scope boot-policy** *policy-name*	指定されたブート ポリシーの組織ブート ポリシー モードを開始します。
ステップ 3	UCS-A /org/boot-policy #**scope storage**	ブート ポリシーの組織ブート ポリシー ストレージ モードを開始します。
ステップ 4	UCS-A /org/boot-policy/storage #**scope local**	ブート ポリシー ローカル ストレージ モードを開始します。
ステップ 5	UCS-A /org/boot-policy/storage/local/ # **scope** {**local-any** | **local-lun** | **sd-card** | **usb-extern** | **usb-intern** }	ローカル ストレージのタイプを指定します。次のいずれかになります。 • [local-any]：ローカル ストレージデバイスのタイプ。このオプションは、レガシーまたは UEFI のブー

	コマンドまたはアクション	目的
		トモードで使用できます。 （注） 標準のブート順序を使用しているCisco UCS M1およびM2のブレードサーバおよびラックサーバはlocal-anyのみ使用できます。 • [local-lun]：ローカルのハードディスク ドライブ。 • [sd-card]：SD カード。 • [usb-extern]：外部 USB カード。

	コマンドまたはアクション	目的
		• [usb-intern]：内部 USB カード。 重要 UEFI ブート パラメータを設定可能なローカル ストレージの唯一のタイプは **local-lun** です。
ステップ 6	UCS-A /org/boot-policy/storage/local/local-lun # **scope local-lun-image-path** {**primary** | **secondary**}	ローカル LUN のイメージ パスを指定します。
ステップ 7	UCS-A /org/boot-policy/storage/local/local-lun/local-lun-image-path # **create uefi-boot-param**	UEFI のブート パラメータを作成し、UEFI ブート パラメータ モードを開始します。
ステップ 8	UCS-A /org/boot-policy/storage/local/local-lun/local-lun-image-path/uefi-boot-param* # **set bootloader-name** *name*	ブート ローダの名前を設定します。
ステップ 9	UCS-A /org/boot-policy/storage/local/local-lun/local-lun-image-path/uefi-boot-param* # **set bootloader-path** *path*	ブート ローダのパスを設定します。
ステップ 10	UCS-A /org/boot-policy/storage/local/local-lun/local-lun-image-path/uefi-boot-param* # **set boot-description** "*description*"	ブート ローダの説明を記入します。
ステップ 11	UCS-A /org/boot-policy/storage/local/local-lun/local-lun-image-path/uefi-boot-param* # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、ローカル LUN の UEFI ブート パラメータを作成し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org* # scope boot-policy bp1
UCS-A /org/boot-policy* # scope storage
UCS-A /org/boot-policy/storage* # scope local
```

```
UCS-A /org/boot-policy/storage/local* # scope local-lun
UCS-A /org/boot-policy/storage/local/local-lun # scope local-lun-image-path primary
UCS-A /org/boot-policy/storage/local/local-lun/local-lun-image-path # create uefi-boot-param
UCS-A /org/boot-policy/storage/local/local-lun/local-lun-image-path/uefi-boot-param* # set
 bootloader-name grub.efi
UCS-A /org/boot-policy/storage/local/local-lun/local-lun-image-path/uefi-boot-param* # set
 bootloader-path EFI\redhat
UCS-A /org/boot-policy/storage/local/local-lun/local-lun-image-path/uefi-boot-param* # set
 boot-description "Red Hat Enterprise Linux"
UCS-A /org/boot-policy/storage/local/local-lun/local-lun-image-path/uefi-boot-param* #
commit-buffer
```

iSCSI LUN の UEFI ブート パラメータの設定

はじめる前に

iSCSI LUN のブート モードが UEFI に設定されていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **scope boot-policy** *policy-name*	指定されたブート ポリシーの組織ブート ポリシー モードを開始します。
ステップ 3	UCS-A /org/boot-policy #**scope iscsi**	ブート ポリシーの組織ブート ポリシー iSCSI モードを開始します。
ステップ 4	UCS-A /org/boot-policy/iscsi # **scope path** {**primary** | **secondary**}	iSCSI LUN のイメージ パスを指定します。
ステップ 5	UCS-A /org/boot-policy/iscsi/path # **create uefi-boot-param**	UEFI のブート パラメータを作成し、UEFI ブート パラメータ モードを開始します。
ステップ 6	UCS-A /org/boot-policy/iscsi/path/uefi-boot-param* # **set bootloader-name** *name*	ブート ローダの名前を設定します。
ステップ 7	UCS-A /org/boot-policy/iscsi/path/uefi-boot-param* # **set bootloader-path** *path*	ブート ローダのパスを設定します。
ステップ 8	UCS-A /org/boot-policy/iscsi/path/uefi-boot-param* # **set boot-description** "*description*"	ブート ローダの説明を記入します。

	コマンドまたはアクション	目的
ステップ 9	UCS-A /org/boot-policy/iscsi/path/uefi-boot-param* # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、iSCSI LUN の UEFI ブート パラメータを作成し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org* # scope boot-policy bp2
UCS-A /org/boot-policy* # scope iscsi
UCS-A /org/boot-policy/iscsi # scope path primary
UCS-A /org/boot-policy/iscsi/path # create uefi-boot-param
UCS-A /org/boot-policy/iscsi/path/uefi-boot-param* # set bootloader-name grub.efi
UCS-A /org/boot-policy/iscsi/path/uefi-boot-param* # set bootloader-path EFI\redhat
UCS-A /org/boot-policy/iscsi/path/uefi-boot-param* # set boot-description "Red Hat Enterprise
 Linux"
UCS-A /org/boot-policy/iscsi/path/uefi-boot-param* # commit-buffer
```

SAN LUN の UEFI ブート パラメータの設定

はじめる前に

SAN LUN のブート モードが UEFI に設定されていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **scope boot-policy** *policy-name*	指定されたブート ポリシーの組織ブート ポリシー モードを開始します。
ステップ 3	UCS-A /org/boot-policy #**scope san**	ブート ポリシーの組織ブート ポリシー SAN モードを開始します。
ステップ 4	UCS-A /org/boot-policy/san # **scope san-image** {**primary** | **secondary**}	SAN イメージを開始します。

	コマンドまたはアクション	目的
ステップ 5	UCS-A /org/boot-policy/san/san-image # **scope path** {**primary** | **secondary**}	SAN LUN のイメージ パスを入力します。
ステップ 6	UCS-A /org/boot-policy/san/san-image/path # **create uefi-boot-param**	UEFI のブート パラメータを作成し、UEFI ブート パラメータ モードを開始します。
ステップ 7	UCS-A /org/boot-policy/san/san-image/path/uefi-boot-param* # **set bootloader-name** *name*	ブート ローダの名前を設定します。
ステップ 8	UCS-A /org/boot-policy/san/san-image/path/uefi-boot-param* # **set bootloader-path** *path*	ブート ローダのパスを設定します。
ステップ 9	UCS-A /org/boot-policy/san/san-image/path/uefi-boot-param* # **set boot-description** "*description*"	ブート ローダの説明を記入します。
ステップ 10	UCS-A /org/boot-policy/san/san-image/path/uefi-boot-param* # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、SAN LUN の UEFI ブート パラメータを作成し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org* # scope boot-policy bp3
UCS-A /org/boot-policy* # scope san
UCS-A /org/boot-policy/san # scope san-image primary
UCS-A /org/boot-policy/san/san-image # scope path primary
UCS-A /org/boot-policy/san/san-image/path # create uefi-boot-param
UCS-A /org/boot-policy/san/san-image/path/uefi-boot-param* # set bootloader-name grub.efi
UCS-A /org/boot-policy/san/san-image/path/uefi-boot-param* # set bootloader-path EFI\redhat
UCS-A /org/boot-policy/san/san-image/path/uefi-boot-param* # set boot-description "Red Hat
 Enterprise Linux"
UCS-A /org/boot-policy/san/san-image/path/uefi-boot-param* # commit-buffer
```

第 31 章

サービス プロファイル更新の遅延展開

この章の内容は、次のとおりです。

サービス プロファイルの遅延展開

サービス プロファイルの変更の一部、またはサービス プロファイル テンプレートの更新は、中断をともなうことや、サーバのリブートが必要になることがあります。ただし、これらの中断をともなう設定変更をいつ実行するかを、遅延展開によって制御できます。たとえば、サービス プロファイルの変更をすぐに展開するか、指定されたメンテナンス時間帯に展開するかを選択できます。また、サービス プロファイルの展開にユーザの明示的な確認応答が必要かどうかを選択できます。

遅延展開は、サーバとサービス プロファイルとの関連付けによって発生するすべての設定変更に使用できます。これらの設定変更は、サービスプロファイルへの変更、サービスプロファイルに含まれるポリシーへの変更、更新サービスプロファイルテンプレートへの変更によってプロンプト表示される場合があります。たとえば、サーバBIOS、RAIDコントローラ、ホストHBA、ネットワーク アダプタなどのホスト ファームウェア パッケージや管理ファームウェア パッケージによって、ファームウェアのアップグレードおよびアクティブ化を延期することもできます。ただし、Cisco UCS Manager、ファブリック インターコネクト、I/O モジュールなど、ファームウェア パッケージを使用しないコンポーネントのファームウェア イメージの直接展開を遅延させることはできません。

遅延展開は、サーバのリブートを必要とする次のアクションに使用できません。

- サーバとサービス プロファイルの最初の関連付け

- サービス プロファイルと別のサーバを関連付けない、サービス プロファイルのサーバからの関連付けの最終解除
- サーバの解放
- サーバの再認識
- サーバのリセット

サービス プロファイル変更の展開を遅延させる場合、1 つ以上のメンテナンス ポリシーを設定し、各サービスプロファイルにメンテナンスポリシーを設定する必要があります。展開が発生する時間帯を指定する場合、1 つ以上の繰り返しオカレンスまたはワンタイム オカレンスを持つスケジュールを少なくとも 1 つ作成し、そのスケジュールをメンテナンス ポリシーに含める必要があります。

遅延展開のスケジュール

スケジュールには、一連のオカレンスが含まれます。これらのオカレンスは、1 回だけ発生させるか、または毎週指定した日時に繰り返し発生させることができます。オカレンスの時間長や実行されるタスクの最大数といった、オカレンスで定義されるオプションにより、あるサービス プロファイルの変更が展開されるかどうかが決まります。たとえば、最大時間長またはタスク数に達したため特定のメンテナンス時間帯に変更を展開できない場合、この展開は次のメンテナンス時間に持ち越されます。

各スケジュールは、Cisco UCS ドメイン が 1 つまたは複数のメンテナンス時間帯に入っているかどうか、定期的に確認します。入っている場合、スケジュールはメンテナンス ポリシーで指定された制限に対し適切な展開を実行します。

スケジュールには、スケジュールに関連付けられたメンテナンス時間を決定する 1 つ以上のオカレンスが含まれています。オカレンスは次のいずれかになります。

ワンタイム オカレンス

ワンタイム オカレンスは、単一のメンテナンス時間を定義します。これらの時間帯は、その時間帯の最大時間長まで、または時間帯の中で実行可能なタスクの最大数に達するまで継続されます。

繰り返しオカレンス

繰り返しオカレンスは、一連のメンテナンス時間を定義します。これらの時間帯は、タスクの最大数に達するまで、またはオカレンスに指定された日の終わりに達するまで継続します。

メンテナンス ポリシー

メンテナンス ポリシーは、サーバに関連付けられたサービス プロファイル、または 1 つ以上のサービス プロファイルに関連付けられた更新中のサービス プロファイルに対して、サーバのリブートが必要になるような変更が加えられた場合の Cisco UCS Manager の対処方法を定義します。

メンテナンス ポリシーは、Cisco UCS Manager でのサービス プロファイルの変更の展開方法を指定します。展開は、次のいずれかの方法で実行されます。

- 即時
- ユーザが管理者権限で承認したときに実行する
- スケジュールで指定された時間に自動的に実行する
- ユーザによる確認応答の待機またはタイマー スケジュール オプションを伴わない次回のリブートまたはシャットダウン時

スケジュール済みのメンテナンス ウィンドウ中に変更を展開するように設定されているメンテナンス ポリシーでは、ポリシーに有効なスケジュールが含まれていることが必要です。この場合、最初に使用可能なメンテナンス ウィンドウ中に変更が展開されます。

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

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

遅延展開のための保留アクティビティ

Cisco UCS ドメイン で遅延展開を設定すると、Cisco UCS Manager ですべての保留アクティビティを表示することができます。ユーザの確認応答を待っているアクティビティと、スケジュールされたアクティビティを表示できます。

Cisco UCS ドメイン に保留中のアクティビティがある場合、Cisco UCS Manager GUI は管理者権限を持つユーザがログインしたときに通知します。

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

- 展開され、サーバと関連付けられるサービス プロファイルの名前
- 展開の影響を受けるサーバ
- 展開により発生する中断
- 展開によって実行される変更

（注） 特定の保留中アクティビティがサーバに適用されるメンテナンス時間を指定することはできません。メンテナンス期間は、保留中のアクティビティの数およびサービス プロファイルに割り当てられたメンテナンス ポリシーに依存します。ただし、管理者権限を持つユーザはすべて、ユーザの確認応答を待っているかメンテナンス期間かにかかわらず、手動で保留中のアクティビティを起動し、サーバをすぐにリブートできます。

遅延展開に関するガイドラインおよび制限事項

サービス プロファイルまたはサービス プロファイル テンプレートへのすべての変更を元に戻すことはできない

保留中の変更をキャンセルする場合、Cisco UCS Manager はサーバを再起動せずに変更のロールバックを試みます。ただし、複雑な変更を行った場合、Cisco UCS Manager は変更のロール バックのためサーバを 2 度目にリブートする必要がある場合があります。たとえば、vNIC を削除すると、Cisco UCS Manager はサービス プロファイルに含まれているメンテナンス ポリシーに従ってサーバをリブートします。サービス プロファイルで元の vNIC を復元しても、この再起動および変更はキャンセルできません。代わりに、Cisco UCS Manager は 2 回目の展開とサーバのリブートをスケジュールします。

サービス プロファイルの関連付けはメンテナンス時間の境界を超えてもよい

Cisco UCS Manager がサービス プロファイルの関連付けを開始した後、スケジューラとメンテナンス ポリシーは手順を制御する方法を持っていません。サービス プロファイルの関連付けが割り当てられたメンテナンス時間に完了しない場合、プロセスが完了するまで続行されます。たとえば、いくつかの段階の再試行やその他の問題のため、関連付けが完了しなかった場合に発生することがあります。

保留中のアクティビティの順序を指定できない

スケジュールされた展開は、独立して並行実行されます。展開が発生する順序は指定できません。また、あるサービス プロファイルの変更を他のものの完了を条件として実行することもできません。

保留中のアクティビティの部分的な展開を実行できない

Cisco UCS Manager は、サーバ プロファイルに加えられたすべての変更をスケジュールされたメンテナンス時間に適用します。サービス プロファイルに複数の変更を同時に加えた後にそれらの変更を別々のメンテナンス時間に振り分けることはできません。サービス プロファイルの変更を展開するとき、Cisco UCS Manager はデータベース内の最新の設定に一致するようにサービス プロファイルを更新します。

スケジュールの設定

スケジュールの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **create scheduler** *sched-name*	スケジューラを作成し、スケジューラ モードを開始します。
ステップ 3	UCS-A /system/scheduler # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、maintenancesched というスケジューラを作成し、トランザクションをコミットします。

```
UCS-A# scope system
UCS-A /system # create scheduler maintenancesched
UCS-A /system/scheduler* # commit-buffer
UCS-A /system/scheduler #
```

次の作業

スケジュールの 1 回限りの実行か繰り返し実行を作成します。

スケジュールへのワンタイム オカレンスの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope schedule** *sched-name*	スケジューラ システム モードを開始します。
ステップ 3	UCS-A /system/scheduler # **create occurrence one-time** *occurrence-name*	ワンタイム オカレンスを作成します。
ステップ 4	UCS-A /system/scheduler/one-time # **set date** *month day-of-month year hour minute*	このオカレンスを実行する日時を設定します。

	コマンドまたはアクション	目的
ステップ 5	UCS-A /system/scheduler/one-time # **set concur-tasks** {**unlimited** | *max-num-concur-tasks*	（任意） このオカレンスの間に同時実行可能なタスクの最大数を設定します。 タスクの最大数に達すると、スケジューラは新しいタスクをスケジュールする前に、[minimum interval] プロパティで設定された時間だけ待機します。
ステップ 6	UCS-A /system/scheduler/one-time # **set max-duration** {**none** | *num-of-days num-of-hours num-of-minutes num-of-seconds*}	（任意） このスケジュールオカレンスが実行可能な時間の最大長を設定します。Cisco UCS は、指定された時間内にできるだけ多くのスケジュール タスクを完了します。
ステップ 7	UCS-A /system/scheduler/one-time # **set min-interval** {**none** | *num-of-days num-of-hours num-of-minutes num-of-seconds*}	（任意） システムが新しいタスクを開始するまで待機する時間の最小長を設定します。
ステップ 8	UCS-A /system/scheduler/one-time # **set proc-cap** {**unlimited** | *max-num-of-tasks*}	（任意） このオカレンスの間に実行可能な、スケジュール設定されたタスクの最大数を設定します。
ステップ 9	UCS-A /system/scheduler/one-time # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、onetimemaint というワンタイム オカレンスを maintsched というスケジューラに作成し、同時実行タスクの最大数を 5 に設定し、開始日時を 2011 年 4 月 1 日 11：00 に設定し、トランザクションをコミットします。

```
UCS-A# scope system
UCS-A /system # scope scheduler maintsched
UCS-A /system/scheduler # create occurrence one-time onetimemaint
UCS-A /system/scheduler/one-time* # set date apr 1 2011 11 00
UCS-A /system/scheduler/one-time* # set concur-tasks 5
UCS-A /system/scheduler/one-time* # commit-buffer
UCS-A /system/scheduler/one-time #
```

スケジュールへの繰り返しオカレンスの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope schedule** *sched-name*	スケジューラ システム モードを開始します。
ステップ 3	UCS-A /system/scheduler # **create occurrence recurring** *occurrence-name*	繰り返しオカレンスを作成します。
ステップ 4	UCS-A /system/scheduler/recurring # **set day** {**even-day** | **every-day** | **friday** | **monday** | **never** | **odd-day** | **saturday** | **sunday** | **thursday** | **tuesday** | **wednesday**}	（任意） Cisco UCS でこのスケジュールのオカレンスを実行する曜日を選択します。 デフォルトでは、このプロパティは never に設定されています。
ステップ 5	UCS-A /system/scheduler/recurring # **set hour** *hour*	（任意） このオカレンスが開始する時間（時）を指定します。 （注） Cisco UCS は、最大長に達していない場合でも、すべての繰り返しオカレンスをそれが開始したのと同じ日に終了させます。たとえば、開始時刻を午後 11 時、最長継続時間を 3 時間に指定すると、Cisco UCS はこのオカレンスを午後 11 時に開始しますが、59 分しか経過していない午後 11 時 59 分に終了します。
ステップ 6	UCS-A /system/scheduler/recurring # **set minute** *minute*	（任意） このオカレンスが開始する時間（分）を指定します。
ステップ 7	UCS-A /system/scheduler/recurring # **set concur-tasks** {**unlimited** | *max-num-concur-tasks*	（任意） このオカレンスの間に同時実行可能なタスクの最大数を設定します。 タスクの最大数に達すると、スケジューラは新しいタスクをスケジュールする前に、[minimum interval] プロパティで設定された時間だけ待機します。

	コマンドまたはアクション	目的
ステップ 8	UCS-A /system/scheduler/recurring # **set max-duration** {**none** | *num-of-hours num-of-minutes num-of-seconds*}	（任意） このスケジュール オカレンスが実行可能な時間の最大長を設定します。Cisco UCS は、指定された時間内にできるだけ多くのスケジュール タスクを完了します。
ステップ 9	UCS-A /system/scheduler/recurring # **set min-interval** {**none** | *num-of-days num-of-hours num-of-minutes num-of-seconds*}	（任意） システムが新しいタスクを開始するまで待機する時間の最小長を設定します。
ステップ 10	UCS-A /system/scheduler/recurring # **set proc-cap** {**unlimited** | *max-num-of-tasks*}	（任意） このオカレンスの間に実行可能な、スケジュール設定されたタスクの最大数を設定します。
ステップ 11	UCS-A /system/scheduler/recurring # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、maintsched というスケジューラに recurringmaint という繰り返しオカレンスを作成し、同時実行タスクの最大数を 5 に設定し、このオカレンスの実行日を偶数日に設定し、11:05 から開始するように時間を設定してトランザクションをコミットします。

```
UCS-A# scope system
UCS-A /system # scope scheduler maintsched
UCS-A /system/scheduler # create occurrence recurring recurringmaint
UCS-A /system/scheduler/recurring* # set day even-day
UCS-A /system/scheduler/recurring* # set hour 11
UCS-A /system/scheduler/recurring* # set minute 5
UCS-A /system/scheduler/recurring* # set concur-tasks 5
UCS-A /system/scheduler/recurring* # commit-buffer
UCS-A /system/scheduler/recurring #
```

スケジュールからのワンタイム オカレンスの削除

これがスケジュールにおける唯一の実行である場合には、そのスケジュールは実行なしで再設定されます。スケジュールがメンテナンス ポリシーに含まれており、そのポリシーがサービス プロファイルに割り当てられている場合、サービス プロファイルに関連付けられているサーバに関連する保留中のアクティビティは展開できません。保留中のアクティビティを展開するには、1 回限りの実行か繰り返し実行かをスケジュールに追加する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /system # **scope scheduler** *sched-name*	スケジューラ システム モードを開始します。
ステップ 3	UCS-A /system/scheduler # **delete occurrence one-time** *occurrence-name*	指定されたワンタイム オカレンスを削除します。
ステップ 4	UCS-A /system/scheduler # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、maintsched スケジューラから onetimemaint というワンタイム オカレンスを削除し、トランザクションをコミットします。

```
UCS-A# scope system
UCS-A /system # scope scheduler maintsched
UCS-A /system/scheduler # delete occurrence one-time onetimemaint
UCS-A /system/scheduler* # commit-buffer
UCS-A /system/scheduler #
```

スケジュールからの繰り返しオカレンスの削除

これがスケジュールにおける唯一の実行である場合には、そのスケジュールは実行なしで再設定されます。スケジュールがメンテナンス ポリシーに含まれており、そのポリシーがサービス プロファイルに割り当てられている場合、サービス プロファイルに関連付けられているサーバに関連する保留中のアクティビティは展開できません。保留中のアクティビティを展開するには、1 回限りの実行か繰り返し実行かをスケジュールに追加する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope scheduler** *sched-name*	スケジューラ システム モードを開始します。
ステップ 3	UCS-A /system/scheduler # **delete occurrence recurring** *occurrence-name*	指定された繰り返しオカレンスを削除します。
ステップ 4	UCS-A /system/scheduler # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、maintsched スケジューラから onetimemaint という繰り返しオカレンスを削除し、トランザクションをコミットします。

```
UCS-A# scope system
UCS-A /system # scope scheduler maintsched
```

```
UCS-A /system/scheduler # delete occurrence recurring onetimemaint
UCS-A /system/scheduler* # commit-buffer
UCS-A /system/scheduler #
```

スケジュールの削除

このスケジュールがメンテナンス ポリシーに含まれている場合、ポリシーはスケジュールなしで再設定されます。そのポリシーがサービスプロファイルに割り当てられている場合、サービスプロファイルに関連付けられているサーバに関連する保留中のアクティビティは展開できません。保留中のアクティビティを展開するには、スケジュールをメンテナンス ポリシーに追加する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **delete scheduler** *sched-name*	スケジューラを削除し、スケジューラ モードを開始します。
ステップ 3	UCS-A /system # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、maintenanceschedというスケジューラを削除し、トランザクションをコミットします。

```
UCS-A# scope system
UCS-A /system # delete scheduler maintenancesched
UCS-A /system* # commit-buffer
UCS-A /system #
```

メンテナンス ポリシーの設定

メンテナンス ポリシーの作成

はじめる前に

このメンテナンス ポリシーを遅延展開のために設定する場合は、スケジュールを作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **create maint-policy** *policy-name*	指定されたメンテナンス ポリシーを作成し、メンテナンス ポリシー モードを開始します。
ステップ 3	UCS-A /org/maint-policy # **set reboot-policy** {**immediate** | **timer-automatic** | **user-ack**}	サービス プロファイルがサーバに関連付けられている場合、関連付けを完了するにはサーバをリブートする必要があります。reboot-policy コマンドを指定すると、このメンテナンス ポリシーを含むすべてのサービス プロファイルについてリブートが発生するタイミングを決定できます。有効な値は次のとおりです。 • **immediate**：サービス プロファイルが変更されると、すぐにサーバがリブートします。 • **timer-automatic**：set scheduler コマンドを使用して、メンテナンス操作がサーバに適用されるタイミングを指定するスケジュールを選択できます。Cisco UCS はサーバをリブートし、サービス プロファイルの変更をスケジュールされた時間に完了させます。 • **user-ack**：ユーザは、変更が適用される前に **apply pending-changes** コマンドを使用して変更を明示的に確認する必要があります。
ステップ 4	UCS-A /org/maint-policy # **set scheduler** *scheduler-name*	（任意） reboot-policy プロパティが timer-automatic に設定された場合、メンテナンス操作がサーバに適用されるタイミングを指定するスケジュールを選択する必要があります。Cisco UCS はサーバをリブートし、サービス プロファイルの変更をスケジュールされた時間に完了させます。
ステップ 5	UCS-A /org/maint-policy # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、maintenance というメンテナンス ポリシーを作成し、サービス プロファイルがサーバに関連付けられるとすぐにリブートするようシステムを設定し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # create maint-policy maintenance
UCS-A /org/maint-policy* # set reboot-policy immediate
```

```
UCS-A /org/maint-policy* # commit-buffer
UCS-A /org/maint-policy #
```

メンテナンス ポリシーの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **delete maint-policy** *policy-name*	指定されたメンテナンス ポリシーを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、maintenance という名前のメンテナンス ポリシーを削除し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # delete maint-policy maintenance
UCS-A /org/maint-policy* # commit-buffer
UCS-A /org/maint-policy #
```

保留アクティビティの管理

保留アクティビティの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	組織モードを開始します。 ルート組織モードを開始するには、*org-name* に / と入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	指定したサービスで組織サービス プロファイル モードを開始します。
ステップ 3	UCS-A /org/service-profile # **show pending-changes** [**detail** | **expand**]	保留中の変更に関する詳細を表示します。

次に、accounting というサービス プロファイルの保留中の変更を表示する例を示します。

```
UCS-A# scope org /
UCS-A /org # scope service-profile accounting
UCS-A /org/service-profile # show pending-changes detail

Pending Changes:
    Scheduler:
    Changed by: admin
    Acked by:
    Mod. date: 2010-09-20T20:36:09.254
    State: Untriggered
    Admin State: Untriggered
    Pend. Changes: 0
    Pend. Disr.: 0
UCS-A /org/service-profile #
```

ユーザの確認応答待ちサービス プロファイル変更の展開

Cisco UCS Manager CLI は、ユーザの確認応答待ちの、複数のサービス プロファイルの保留中のすべての変更を展開することはできません。複数のサービス プロファイルの、保留中のすべての変更を同時に展開するには、Cisco UCS Manager GUI を使用します。

重要 保留中のアクティビティを確認した後、Cisco UCS Manager が影響のあるサーバをリブートすることは禁止できません。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	組織モードを開始します。 ルート組織モードを開始するには、*org-name* に / と入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	指定したサービスで組織サービス プロファイル モードを開始します。
ステップ 3	UCS-A /org/service-profile # **apply pending-changes immediate**	保留中の変更をただちに適用します。 Cisco UCS Manager によって、保留中のアクティビティの影響を受けるサーバがただちにリブートされます。

次に、accounting というサービス プロファイルの保留中の変更を適用する例を示します。

```
UCS-A# scope org /
UCS-A /org # scope service-profile accounting
UCS-A /org/service-profile # apply pending-changes immediate
UCS-A /org/service-profile #
```

スケジュールされたサービス プロファイル変更の即時展開

Cisco UCS Manager CLI は、複数のサービス プロファイルの、スケジュールされているすべての変更を同時に展開することはできません。複数のサービス プロファイルの、スケジュールされているすべての変更を同時に展開するには、Cisco UCS Manager GUI を使用します。

重要 保留中のアクティビティを確認した後、Cisco UCS Manager が影響のあるサーバをリブートすることは禁止できません。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	組織モードを開始します。 ルート組織モードを開始するには、*org-name* に / と入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	指定したサービスで組織サービス プロファイル モードを開始します。
ステップ 3	UCS-A /org/service-profile # **apply pending-changes immediate**	保留中の変更をただちに適用します。 Cisco UCS Manager によって、保留中のアクティビティの影響を受けるサーバがただちにリブートされます。

次に、accounting というサービス プロファイルの保留中の変更を適用する例を示します。

```
UCS-A# scope org /
UCS-A /org # scope service-profile accounting
UCS-A /org/service-profile # apply pending-changes immediate
UCS-A /org/service-profile #
```

第 32 章

サービス プロファイル

この章の内容は、次のとおりです。

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。このプロファイルでは、アソシエーション時にサーバに設定されていた 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対して透過的です。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る場合を除き、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 による新規サーバの互換性チェックは実行されません。両方のハードウェアが似ていない場合、関連付け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に関するガイドラインおよび推奨事項

サービス プロファイルまたはサービス プロファイル テンプレートに含まれるポリシー（ローカルディスク設定ポリシーなど）やプールに固有のガイドラインと推奨事項に加え、サービスプロファイルとサーバを関連付ける機能に影響する以下のガイドラインと推奨事項も順守してください。

ラックマウント サーバで設定できる vNIC 数の制限

Cisco UCS Manager と統合されているラックマウント サーバでは、Cisco UCS P81E 仮想インターフェイス カード（N2XX-ACPCI01）などのサポート対象のアダプタごとに最大 56 の vNIC を設定できます。

ラックマウント サーバの電力制限はサポート対象外

電力制限はラック サーバではサポートされません。ラックマウント サーバに関連付けられているサービス プロファイルに電力制御ポリシーを含めた場合、そのポリシーは実行されません。

vNIC に関する QoS ポリシーのガイドライン

QoS ポリシーのプライオリティ設定が fc（ファイバ チャネル システム クラス）ではない場合にのみ、そのポリシーを vNIC に割り当てることができます。QoS ポリシーのプライオリティに他のシステム クラスを設定できます。

vHBA に関する QoS ポリシーのガイドライン

QoS ポリシーのプライオリティ設定が fc（ファイバ チャネル システム クラス）である場合にのみ、そのポリシーを vHBA に割り当てることができます。

QoS ポリシーのホスト制御設定は vNIC にのみ適用されます。vHBA には影響しません。

インバンド サービス プロファイル

インバンド サービス プロファイルの設定

この手順は、インバンド サービス プロファイルの作成方法を示しています。

（注） Cisco UCS Manager GUI で、[機器（Equipment）] タブのサーバ CIMC を使用するようにアウトオブバンド設定を設定したすべての Cisco UCS M3 および M4 サーバは、インバンド プロファイルに従って、自動的にインバンド ネットワーク（VLAN）および IPv4/IPv6 設定を取得します。インバンド プロファイル設定からネットワークまたは IP プール名を削除すると、サーバのインバンド設定がインバンド プロファイルから取得された場合は、サーバからインバンド設定が削除されます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope eth-uplink**	イーサネットアップリンクのコンフィギュレーション モードを開始します。
ステップ 2	UCS-A /eth-uplink/inband-profile# **scope inband-profile**	インバンド プロファイル コンフィギュレーション モードを開始します。
ステップ 3	UCS-A /eth-uplink/inband-profile # **set net-group-name***vlan-group-name*	インバンド プロファイルのネットワーク グループ名を設定します。
ステップ 4	UCS-A /eth-uplink/inband-profile # **set default-vlan-name***vlan-name*	インバンド プロファイルのデフォルト VLAN を設定します。
ステップ 5	UCS-A /eth-uplink/inband-profile # **set pool-name** *pool-name*	インバンドプロファイルの IP プールを設定します。
ステップ 6	UCS-A /eth-uplink/inband-profile # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、インバンド サービス プロファイル inband-profile を作成し、ネットワーク グループ名を inband-vlan-group に、デフォルトの VLAN を Inband_VLAN に、IP プールを inband_default にそれぞれ設定し、トランザクションをコミットします。

```
UCS-A #scope eth-uplink
UCS-A /eth-uplink # scope inband-profile
UCS-A /eth-uplink/inband-profile # set net-group-name inband-vlan-group
UCS-A /eth-uplink/inband-profile* # set default-vlan-name Inband_VLAN
UCS-A /eth-uplink/inband-profile* # set pool-name inband_default
UCS-A /eth-uplink/inband-profile* # commit-buffer
UCS-A /eth-uplink/inband-profile #
```

インバンド管理サービス プロファイルの設定

この手順は、インバンド管理サービス プロファイルを設定する方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** /	組織コンフィギュレーション モードを開始します。
ステップ 2	UCS-A /org # **create service-profile***sp-name*	指定されたサービス プロファイルを作成し、サービス プロファイルのコンフィギュレーション モードを開始します。
ステップ 3	UCS-A /org/service-profile # **create mgmt-iface***in-band*	指定された管理インターフェイスを作成し、管理インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	UCS-A /org/service-profile/mgmt-iface # **create mgmt-vlan**	管理 VLAN を作成し、管理 VLAN コンフィギュレーション モードを開始します。
ステップ 5	UCS-A/org/service-profile/mgmt-iface/mgmt-vlan # set **network-name** *network-name*	管理 VLAN のネットワーク名を設定します。
ステップ 6	UCS-A /org/service-profile/mgmt-iface/mgmt-vlan # **create ext-pooled-ip**	外部 IP プールを作成し、IP プール コンフィギュレーション モードを開始します。
ステップ 7	UCS-A /org/service-profile/mgmt-iface/mgmt-vlan/ext-pooled-ip # **set name** *pool-name*	外部 IPv4 プールの名前を設定します。
ステップ 8	UCS-A /org/service-profile/mgmt-iface/mgmt-vlan/ext-pooled-ip # **exit**	IPv4 プール コンフィギュレーション モードを終了します。
ステップ 9	UCS-A /org/service-profile/mgmt-iface/mgmt-vlan #**create ext-pooled-ip6**	外部 IPv6 プールを作成し、IPv6 プール コンフィギュレーション モードを開始します。
ステップ 10	UCS-A /org/service-profile/mgmt-iface/mgmt-vlan/ext-pooled-ip6 # **set name** *pool-name*	外部 IPv6 プールの名前を設定します。
ステップ 11	UCS-A /org/service-profile/mgmt-iface/mgmt-vlan/ext-pooled-ip6 # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、サービス プロファイル名 inband_sp を作成し、in-band という名前の管理インターフェイスを設定し、管理 VLAN を作成し、ネットワーク名を Inband_VLAN に設定し、外部 IPv4 プー

ルを作成してその名前を inband_default に設定し、外部 IP および外部 IPv6 管理プールを作成し、両方のプールの名前を inband_default に設定し、トランザクションをコミットします。

```
UCS-A# scope org
UCS-A /org # create service-profile inband_sp
UCS-A /org/service-profile* # create mgmt-iface in-band
UCS-A /org/service-profile/mgmt-iface* # create mgmt-vlan
UCS-A /org/service-profile/mgmt-iface/mgmt-vlan* # set network-name Inband_VLAN
UCS-A /org/service-profile/mgmt-iface/mgmt-vlan* # create ext-pooled-ip
UCS-A /org/service-profile/mgmt-iface/mgmt-vlan/ext-pooled-ip* # set name inband_default
UCS-A /org/service-profile/mgmt-iface/mgmt-vlan/ext-pooled-ip* # exit
UCS-A /org/service-profile/mgmt-iface/mgmt-vlan* # create ext-pooled-ip6
UCS-A /org/service-profile/mgmt-iface/mgmt-vlan/ext-pooled-ip6* # set name inband_default
UCS-A /org/service-profile/mgmt-iface/mgmt-vlan/ext-pooled-ip6* # commit-buffer
UCS-A /org/service-profile/mgmt-iface/mgmt-vlan/ext-pooled-ip6 # exit
UCS-A /org/service-profile/mgmt-iface/mgmt-vlan # exit
UCS-A /org/service-profile/mgmt-iface # exit
```

次の作業

サーバにインバンド管理インターフェイスのサービス プロファイルを関連付けます。

サービス プロファイルからのインバンド設定の削除

この手順では、サービス プロファイルからインバンド設定を削除する方法について説明します。

（注） デフォルト VLAN 名とデフォルト プール名を使用して Cisco UCS Manager でインバンド プロファイルが設定されると、サーバ CIMC は、サービス プロファイルから設定を削除してから 1 分以内にインバンド プロファイルからインバンド設定を自動的に取得します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** /	組織コンフィギュレーション モードを開始します。
ステップ 2	UCS-A/org # **scope service-profile** *blade1*	組織プロファイル コンフィギュレーション モードを開始します。
ステップ 3	UCS-A/org/service-profile # **delete mgmt-iface***in-band*	指定されたサービス プロファイルを削除します。
ステップ 4	UCS-A/org/service-profile # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、サービスプロファイルblade1にスコープし、管理インターフェイスインバンドを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope org
UCS-A /org # scope service-profile blade1
UCS-A /org/service-profile # delete mgmt-iface in-band
```

```
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile
```

CIMC でのインバンド管理の設定

この手順では、サーバ CIMC 上でインバンド管理を設定する方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *chassi-numserver-num*	指定サーバのシャーシサーバ モードを開始します。
ステップ 2	UCS-A /chassis/server # **scope cimc**	CIMC コンフィギュレーション モードを開始します。
ステップ 3	UCS-A /chassis/server /chassis/server/cimc # **create mgmt-iface***in-band*	指定された管理インターフェイスを作成し、管理インターフェイス コンフィギュレーションモードを開始します。
ステップ 4	UCS-A /chassis/server/cimc/mgmt-iface # **set ipv4 static**	IPv4 状態をスタティックに設定します。
ステップ 5	UCS-A /chassis/server/cimc/mgmt-iface # **set ipv6state static**	IPv6 状態をスタティックに設定します。
ステップ 6	UCS-A /chassis/server/cimc/mgmt-iface # **create mgmt-vlan**	管理 VLAN を作成し、管理 VLAN コンフィギュレーション モードを開始します。
ステップ 7	UCS-A /chassis/server/cimc/mgmt-iface/mgmt-vlan # **network-name** *network-name*	管理 VLAN のネットワーク名を設定します。
ステップ 8	UCS-A /chassis/server/cimc/mgmt-iface/mgmt-vlan **create ext-pooled-ip**	外部 IPv4 プールを作成し、IPv4 プール コンフィギュレーションモードを開始します。
ステップ 9	UCS-A /chassis/server/cimc/mgmt-iface/mgmt-vlan/ext-pooled-ip # **set name** *pool-name*	外部 IPv4 プールの名前を設定します。
ステップ 10	UCS-A /chassis/server/cimc/mgmt-iface/mgmt-vlan/ext-pooled-ip # **exit**	IPv4 プール コンフィギュレーション モードを終了します。
ステップ 11	UCS-A /chassis/server/cimc/mgmt-iface/mgmt-vlan #**create ext-pooled-ip6**	外部 IPv6 プールを作成し、IPv6 プール コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 12	UCS-A /chassis/server/cimc/mgmt-iface/mgmt-vlan/ext-pooled-ip6 # **set name** *pool-name*	外部 IPv6 プールの名前を設定します。
ステップ 13	UCS-A /chassis/server/cimc/mgmt-iface/mgmt-vlan/ext-pooled-ip6 # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、in-band という名前のサーバ 1 のシャーシ 1 上で管理インターフェイスを作成し、IPv4 および IPv6 状態をスタティックに設定し、管理 VLAN を作成します。続いて、ネットワーク名を Inband_VLAN に、外部 IP を作成してその名前を inband_default に、IPv4 および IPv6 プールを作成してその両方のプールの名前を inband_default にそれぞれ設定し、トランザクションをコミットします。

```
UCS-A# scope server 1/1
UCS-A /chassis/server # scope cimc
UCS-A /chassis/server/cimc # create mgmt-iface in-band
UCS-A /chassis/server/cimc/mgmt-iface* # set ipv4 static
UCS-A /chassis/server/cimc/mgmt-iface* # set ipv6state stati
UCS-A /chassis/server/cimc/mgmt-iface* # create mgmt-vlan
UCS-A /chassis/server/cimc/mgmt-iface/mgmt-vlan* # set network-name Inband_VLAN
UCS-A /chassis/server/cimc/mgmt-iface/mgmt-vlan* # create ext-pooled-ip
UCS-A /chassis/server/cimc/mgmt-iface/mgmt-vlan/ext-pooled-ip* # set name inband_default
UCS-A /chassis/server/cimc/mgmt-iface/mgmt-vlan/ext-pooled-ip* # exit
UCS-A /chassis/server/cimc/mgmt-iface/mgmt-vlan* # create ext-pooled-ip6
UCS-A /chassis/server/cimc/mgmt-iface/mgmt-vlan/ext-pooled-ip6* # set name inband_default
UCS-A /chassis/server/cimc/mgmt-iface/mgmt-vlan/ext-pooled-ip6* # commit-buffer
UCS-A /chassis/server/cimc/mgmt-iface/mgmt-vlan/ext-pooled-ip6 #
```

CIMC からのインバンド設定の削除

この手順は、サーバ CIMC からインバンド設定を削除する方法について説明します。

（注） デフォルト VLAN 名とデフォルト プール名を使用して Cisco UCS Manager でインバンド プロファイルが設定されると、サーバ CIMC は、サービス プロファイルから設定を削除してから 1 分以内にインバンド プロファイルからインバンド設定を自動的に取得します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *chassi-numserver-num*	指定サーバのシャーシ サーバ モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /chassis/server # **scope cimc**	CIMC コンフィギュレーション モードを開始します。
ステップ 3	UCS-A /chassis/server /chassis/server/cimc # **delete mgmt-iface***in-band*	指定されたサービス プロファイルを削除します。
ステップ 4	UCS-A /chassis/server /chassis/server/cimc # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、server 1 の chassis1 から in-band という名前の管理インターフェイスを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope server 1/1
UCS-A /chassis/server # scope cimc
UCS-A /chassis/server/cimc # delete mgmt-iface in-band
UCS-A /chassis/server/cimc* # commit-buffer
UCS-A /chassis/server/cimc #
```

初期テンプレートと既存のテンプレート

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。

（注） 初期テンプレートと標準のサービス プロファイルから作成されたサービス プロファイルは、[リセット（Reset）]がクリックされると、順次プール内で使用可能な最小の ID を取得します。

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、[リセット（Reset）] がクリックされると、順次プール内のより小さい ID が未使用の場合でも、同じ ID を保持します。

サービス プロファイル テンプレートの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルート組織モードを開始するには、*/* を *org-name* として入力します。
ステップ 2	UCS-A /org # **create service-profile** *profile-name* {**initial-template** | **updating-template**}	指定したサービス プロファイル テンプレートを作成し、組織サービス プロファイル モードを開始します。 このサービス プロファイル テンプレートを識別する一意の *profile-name* を入力します。 この名前には、2 ～ 32 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。この名前は、同じ組織内のすべてのサービスプロファイルおよびサービス プロファイル テンプレートで一意であることが必要です。
ステップ 3	UCS-A /org/service-profile # **set bios-policy** *policy-name*	指定された BIOS ポリシーをサービス プロファイルに関連付けます。
ステップ 4	UCS-A /org/service-profile # **set boot-policy** *policy-name*	指定されたブート ポリシーをサービス プロファイルに関連付けます。

	コマンドまたはアクション	目的
ステップ 5	UCS-A /org/service-profile # **set descr** *description*	（任意） サービス プロファイルに説明を記入します。 （注） 説明にスペース、特殊文字、または句読点が含まれている場合は、説明を引用符で括る必要があります。引用符は、**show** コマンド出力の説明フィールドには表示されません。
ステップ 6	UCS-A /org/service-profile # **set dynamic-vnic-conn-policy** *policy-name*	指定されたダイナミック vNIC 接続ポリシーをサービス プロファイルに関連付けます。
ステップ 7	UCS-A /org/service-profile # **set ext-mgmt-ip-state** {**none** | **pooled**}	管理 IP アドレスをサービス プロファイルに割り当てる方法を指定します。 次のオプションを使用して管理IPアドレス ポリシーを設定できます。 • [なし（None）] : サービス プロファイルには IP アドレスが割り当てられません。 • [プール済み（Pooled）] : サービス プロファイルには、管理 IP プールから IP アドレスが割り当てられます。 （注） サービス プロファイル テンプレートの管理 IP アドレスを static に設定すると、エラーが発生します。
ステップ 8	UCS-A /org/service-profile # **set host-fw-policy** *policy-name*	指定されたホスト ファームウェア ポリシーをサービス プロファイルに関連付けます。
ステップ 9	UCS-A /org/service-profile # **set identity** {**dynamic-uuid** {*uuid* | **derived**} | **dynamic-wwnn** {*wwnn* | **derived**} | **uuid-pool** *pool-name* | **wwnn-pool** *pool-name*}	サーバが UUID または WWNN を取得する方法を指定します。次のいずれかを実行できます。 • 一意の UUID を *nnnnnnnn-nnnn-nnnn-nnnnnnnnnnnn* 形式で作成する。 • 製造時にハードウェアに焼き付けられた UUID を取得する。 • UUID プールを使用する。 • 一意の WWNN を *hh* **:** *hh* **:** *hh* **:** *hh* **:** *hh* **:** *hh* **:** *hh* **:** *hh* 形式で作成する。 • 製造時にハードウェアに焼き付けられた WWNN を取得する。

	コマンドまたはアクション	目的
		• WWNN プールを使用する。
ステップ 10	UCS-A /org/service-profile # **set ipmi-access-profile** *profile-name*	指定された IPMI アクセス プロファイルをサービス プロファイルに関連付けます。
ステップ 11	UCS-A /org/service-profile # **set lan-connectivity-policy-name** *policy-name*	サービス プロファイルに指定された LAN 接続ポリシーを関連付けます。 （注） LAN 接続ポリシーとローカルで作成された vNIC を同じサービス プロファイルに含めることはできません。LAN 接続ポリシーをサービス プロファイルに追加すると、すべての既存の vNIC 設定が消去されます。
ステップ 12	UCS-A /org/service-profile # **set local-disk-policy** *policy-name*	指定されたローカル ディスク ポリシーをサービス プロファイルに関連付けます。
ステップ 13	UCS-A /org/service-profile # **set maint-policy** *policy-name*	指定されたメンテナンス ポリシーをサービス プロファイルに関連付けます。
ステップ 14	UCS-A /org/service-profile # **set mgmt-fw-policy** *policy-name*	指定された管理ファームウェア ポリシーをサービス プロファイルに関連付けます。
ステップ 15	UCS-A /org/service-profile # **set power-control-policy** *policy-name*	指定された電源管理ポリシーをサービス プロファイルに関連付けます。
ステップ 16	UCS-A /org/service-profile # **set san-connectivity-policy-name** *policy-name*	指定された SAN 接続ポリシーをサービス プロファイルに関連付けます。 （注） SAN 接続ポリシーとローカルで作成された vHBA を同じサービス プロファイルに含めることはできません。SAN 接続ポリシーをサービス プロファイルに追加すると、すべての既存の vHBA 設定が消去されます。
ステップ 17	UCS-A /org/service-profile # **set scrub-policy** *policy-name*	指定されたスクラブ ポリシーをサービス プロファイルに関連付けます。
ステップ 18	UCS-A /org/service-profile # **set sol-policy** *policy-name*	指定した Serial over LAN ポリシーをサービス プロファイルに関連付けます。
ステップ 19	UCS-A /org/service-profile # **set stats-policy** *policy-name*	指定された統計情報ポリシーをサービス プロファイルに関連付けます。

	コマンドまたはアクション	目的
ステップ 20	UCS-A /org/service-profile # **set user-label** *label-name*	サービス プロファイルに関連付けられたユーザ ラベルを指定します。
ステップ 21	UCS-A /org/service-profile # **set vcon** {**1** | **2**} **selection** {**all** | **assigned-only** | **exclude-dynamic** | **exclude-unassigned**}	指定された vCon に選択プリファレンスを指定します。
ステップ 22	UCS-A /org/service-profile # **set vcon-profile** *policy-name*	指定された vNIC/vHBA 配置プロファイルをサービス プロファイルに関連付けます。 （注） サービス プロファイルに vNIC/vHBA 配置プロファイルを割り当てるか、またはサービス プロファイルに vCon 選択プリファレンスを設定することができますが、両方を実行する必要はありません。
ステップ 23	UCS-A /org/service-profile # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、サービスプロファイルテンプレートを作成してトランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org* # create service-profile ServTemp2 updating-template
UCS-A /org/service-profile* # set bios-policy biospol1
UCS-A /org/service-profile* # set boot-policy bootpol32
UCS-A /org/service-profile* # set  descr "This is a service profile example."
UCS-A /org/service-profile* # set dynamic-vnic-conn-policy mydynvnicconnpolicy
UCS-A /org/service-profile* # set ext-mgmt-ip-state pooled
UCS-A /org/service-profile* # set host-fw-policy ipmi-user987
UCS-A /org/service-profile* # set identity dynamic-uuid derived
UCS-A /org/service-profile* # set ipmi-access-profile ipmiProf16
UCS-A /org/service-profile* # set local-disk-policy localdiskpol33
UCS-A /org/service-profile* # set maint-policy maintpol4
UCS-A /org/service-profile* # set mgmt-fw-policy mgmtfwpol75
UCS-A /org/service-profile* # set power-control-policy powcontrpol13
UCS-A /org/service-profile* # set scrub-policy scrubpol55
UCS-A /org/service-profile* # set sol-policy solpol2
UCS-A /org/service-profile* # set stats-policy statspol4
UCS-A /org/service-profile* # set user-label mylabel
UCS-A /org/service-profile* # vcon-policy myvconnpolicy
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile #
```

次の作業

- （任意）サービス プロファイルのブート定義を設定します。サービス プロファイルにブート ポリシーが関連付けられていない場合に限り、このオプションを使用します。
- サービス プロファイル テンプレートからサービス プロファイル インスタンスを作成します。

サービス プロファイル テンプレートからのサービス プロファイル インスタンスの作成

はじめる前に

サービス プロファイルのインスタンスの作成元になるサービス プロファイル テンプレートがあることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **create service-profile** *profile-name* **instance**	指定したサービス プロファイル インスタンスを作成し、組織サービス プロファイル モードを開始します。 このサービス プロファイル テンプレートを識別する一意の *profile-name* を入力します。 この名前には、2 ～ 32 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。この名前は、同じ組織内のすべてのサービス プロファイルおよびサービス プロファイル テンプレートで一意であることが必要です。
ステップ 3	UCS-A /org/service-profile # **set src-templ-name** *profile-name*	元になるサービス プロファイル テンプレートを指定してサービス プロファイル インスタンスに適用します。サービス プロファイル テンプレートからのすべての設定が、サービス プロファイル インスタンスに適用されます。
ステップ 4	UCS-A /org/service-profile # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、ServProf34 という名前のサービス プロファイル インスタンスを作成し、ServTemp2 という名前のサービスプロファイルテンプレートを適用し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org* # create service-profile ServProf34 instance
UCS-A /org/service-profile* # set src-templ-name ServTemp2
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile #
```

次の作業

サーバ、ラック サーバ、またはサーバ プールにサービス プロファイルを関連付けます。

ハードウェアベースのサービス プロファイルの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **create service-profile** *profile-name***instance**	指定したサービス プロファイル インスタンスを作成し、組織サービス プロファイル モードを開始します。 このサービス プロファイルを特定する一意の *profile-name* を入力します。 この名前には、2 ～ 32 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。この名前は、同じ組織内のすべてのサービス プロファイルおよびサービス プロファイル テンプレートで一意であることが必要です。
ステップ 3	UCS-A /org/service-profile # **set bios-policy** *policy-name*	指定された BIOS ポリシーをサービス プロファイルに関連付けます。
ステップ 4	UCS-A /org/service-profile # **set boot-policy** *policy-name*	指定されたブート ポリシーをサービス プロファイルに関連付けます。
ステップ 5	UCS-A /org/service-profile # **set descr** *description*	（任意） サービス プロファイルに説明を記入します。 （注） 説明にスペース、特殊文字、または句読点が含まれている場合は、説明を引用符で括る必要があります。引用符は、**show** コマンド出力の説明フィールドには表示されません。
ステップ 6	UCS-A /org/service-profile # **set dynamic-vnic-conn-policy** *policy-name*	指定されたダイナミック vNIC 接続ポリシーをサービス プロファイルに関連付けます。
ステップ 7	UCS-A /org/service-profile # **set ext-mgmt-ip-state** {**none** | **pooled** | **static**}	管理 IP アドレスをサービス プロファイルに割り当てる方法を指定します。 次のオプションを使用して管理 IP アドレス ポリシーを設定できます。

	コマンドまたはアクション	目的
		• [なし（None）]：サービス プロファイルには IP アドレスが割り当てられません。 • [プール済み（Pooled）]：サービス プロファイルには、管理 IP プールから IP アドレスが割り当てられます。 • [スタティック（Static）]：サービス プロファイルには、設定されたスタティック IP アドレスが割り当てられます。
ステップ 8	UCS-A /org/service-profile # **set host-fw-policy** *ipmi-user-name*	指定されたホスト転送ポリシーをサービス プロファイルに関連付けます。
ステップ 9	UCS-A /org/service-profile # **set identity** {**dynamic-uuid** {*uuid* | **derived**} | **dynamic-wwnn** {*wwnn* | **derived**} | **uuid-pool** *pool-name* | **wwnn-pool** *pool-name*}	サーバが UUID または WWNN を取得する方法を指定します。次のいずれかを実行できます。 • 一意の UUID を *nnnnnnnn-nnnn-nnnn-nnnnnnnnnnnn* 形式で作成する。 • 製造時にハードウェアに焼き付けられた UUID を取得する。 • UUID プールを使用する。 • 一意の WWNN を *hh* **:** *hh* **:** *hh* **:** *hh* **:** *hh* **:** *hh* **:** *hh* **:** *hh* 形式で作成する。 • 製造時にハードウェアに焼き付けられた WWNN を取得する。 • WWNN プールを使用する。
ステップ 10	UCS-A /org/service-profile # **set ipmi-access-profile** *profile-name*	指定された IPMI アクセス プロファイルをサービス プロファイルに関連付けます。
ステップ 11	UCS-A /org/service-profile # **set local-disk-policy** *policy-name*	指定されたローカル ディスク ポリシーをサービス プロファイルに関連付けます。
ステップ 12	UCS-A /org/service-profile # **set maint-policy** *policy-name*	指定されたメンテナンス ポリシーをサービス プロファイルに関連付けます。
ステップ 13	UCS-A /org/service-profile # **set mgmt-fw-policy** *policy-name*	指定された管理転送ポリシーをサービス プロファイルに関連付けます。

	コマンドまたはアクション	目的
ステップ 14	UCS-A /org/service-profile # **set power-control-policy** *policy-name*	指定された電源管理ポリシーをサービス プロファイルに関連付けます。
ステップ 15	UCS-A /org/service-profile # **set scrub-policy** *policy-name*	指定されたスクラブ ポリシーをサービス プロファイルに関連付けます。
ステップ 16	UCS-A /org/service-profile # **set sol-policy** *policy-name*	指定した Serial over LAN ポリシーをサービス プロファイルに関連付けます。
ステップ 17	UCS-A /org/service-profile # **set stats-policy** *policy-name*	指定された統計情報ポリシーをサービス プロファイルに関連付けます。
ステップ 18	UCS-A /org/service-profile # **set user-label** *label-name*	サービス プロファイルに関連付けられたユーザ ラベルを指定します。
ステップ 19	UCS-A /org/service-profile # **set vcon** {**1** | **2**} **selection** {**all** | **assigned-only** | **exclude-dynamic** | **exclude-unassigned**}	指定された vCon に選択プリファレンスを指定します。
ステップ 20	UCS-A /org/service-profile # **set vcon-policy** *policy-name*	指定された vNIC/vHBA 配置ポリシーをサーバ プロファイルに関連付けます。 （注） サービス プロファイルに vNIC/vHBA 配置プロファイルを割り当てるか、またはサービス プロファイルに vCon 選択プリファレンスを設定することができますが、両方を実行する必要はありません。
ステップ 21	UCS-A /org/service-profile # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、サービスプロファイルインスタンスを作成してトランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org* # create service-profile ServInst90 instance
UCS-A /org/service-profile* # set bios-policy biospol1
UCS-A /org/service-profile* # set boot-policy bootpol32
UCS-A /org/service-profile* # set  descr "This is a service profile example."
UCS-A /org/service-profile* # set ext-mgmt-ip-state pooled
UCS-A /org/service-profile* # set host-fw-policy ipmi-user987
UCS-A /org/service-profile* # set identity dynamic-uuid derived
UCS-A /org/service-profile* # set ipmi-access-profile ipmiProf16
UCS-A /org/service-profile* # set local-disk-policy localdiskpol33
UCS-A /org/service-profile* # set maint-policy maintpol4
UCS-A /org/service-profile* # set mgmt-fw-policy mgmtfwpol75
UCS-A /org/service-profile* # set power-control-policy powcontrpol13
UCS-A /org/service-profile* # set scrub-policy scrubpol55
UCS-A /org/service-profile* # set sol-policy solpol2
UCS-A /org/service-profile* # set stats-policy statspol4
UCS-A /org/service-profile* # set user-label mylabel
UCS-A /org/service-profile* # vcon-policy myvconnpolicy
```

```
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile #
```

次の作業

- （任意）サービス プロファイルのブート定義を設定します。サービス プロファイルにブート ポリシーが関連付けられていない場合に限り、このオプションを使用します。
- ブレード サーバ、サーバ プール、またはラック サーバにサービス プロファイルを関連付けます。

サービス プロファイルの vNIC の設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルート組織モードを開始するには、*/* を *org-name* として入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	指定したサービス プロファイルで組織サービス プロファイル モードを開始します。
ステップ 3	UCS-A /org/service-profile # **create vnic** *vnic-name* [**eth-if** *eth-if-name*] [**fabric** {**a** | **b**}]	指定したサービス プロファイルの vNIC を作成し、組織サービス プロファイルの vNIC モードを開始します。
ステップ 4	UCS-A /org/service-profile/vnic # **set adapter-policy** *policy-name*	vNIC に使用するアダプタ ポリシーを指定します。
ステップ 5	UCS-A /org/service-profile/vnic # **set fabric** {**a** | **a-b** | **b** | **b-a**}	vNIC に使用するファブリックを指定します。vNIC テンプレートを作成するときにステップ 3 でファブリックを指定しなかった場合は、このコマンドで指定するオプションがあります。 デフォルトのファブリック インターコネクトが使用できない場合に、この vNIC が第 2 のファブリック インターコネクトにアクセスできるようにするには、**a-b**（A がプライマリ）または **b-a**（B がプライマリ）を選択します。

	コマンドまたはアクション	目的
		（注） 次の状況下では、vNIC のファブリック フェールオーバーを有効にしないでください。 • Cisco UCS ドメイン がイーサネット スイッチ モードで動作している場合。vNIC ファブリック フェールオーバーはこのモードではサポートされません。1 つのファブリック インターコネクト上のすべてのイーサネットアップリンクが障害になった場合、vNIC は他のイーサネットアップリンクにフェールオーバーしません。 • ファブリック フェールオーバーをサポートしていないアダプタ（Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter など）を搭載しているサーバに、この vNIC を関連付けることを計画している場合。これを行った場合、Cisco UCS Manager により、サービス プロファイルとサーバを関連付けたときに設定エラーが生成されます。
ステップ 6	UCS-A /org/service-profile/vnic # **set identity** {**dynamic-mac** {*mac-addr* | **derived**} | **mac-pool** *mac-pool-name*}	vNIC の ID（MAC アドレス）を指定します。次のいずれかのオプションを使用して識別を設定できます。 • 一意の MAC アドレスを *nn* **:** *nn* **:** *nn* **:** *nn* **:** *nn* **:** *nn* の形式で作成します。 • 製造時にハードウェアに焼き付けられた MAC アドレスを取得する。 • MAC プールから MAC アドレスを割り当てる。
ステップ 7	UCS-A /org/service-profile/vnic # **set mtu** *size-num*	この vNIC で受け入れられる最大伝送単位、つまりパケット サイズ。 1500 ～ 9216 の整数を入力します。 （注） vNIC に対応する QoS ポリシーがある場合、ここで指定した MTU は、関連付けられた QoS システム クラスで指定された MTU と同等以下でなければなりません。この MTU 値が QoS システム クラスの MTU 値を超えている場合、データ転送中にパケットがドロップされる可能性があります。

	コマンドまたはアクション	目的
ステップ 8	UCS-A /org/service-profile/vnic # **set nw-control-policy** *policy-name*	vNICによって使用されるネットワーク制御ポリシー。
ステップ 9	UCS-A /org/service-profile/vnic # **set order** {*order-num* | **unspecified**}	vNIC に相対順序を指定します。
ステップ 10	UCS-A /org/service-profile/vnic # **set pin-group** *group-name*	vNIC によって使用される LAN ピン グループ。
ステップ 11	UCS-A /org/service-profile/vnic # **set qos-policy** *policy-name*	vNICによって使用されるサービス ポリシーの品質。
ステップ 12	UCS-A /org/service-profile/vnic # **set stats-policy** *policy-name*	vNIC によって使用される統計情報収集ポリシー。
ステップ 13	UCS-A /org/service-profile/vnic # **set template-name** *policy-name*	ダイナミック vNIC 接続ポリシーを vNIC に使用するように指定します。
ステップ 14	UCS-A /org/service-profile/vnic # **set vcon** {**1** | **2** | **3** | **4** | **any**}	指定された vCon に vNIC を割り当てます。Cisco UCS Manager が自動的に vNIC を割り当てるようにするには、**any** キーワードを使用します。
ステップ 15	UCS-A /org/service-profile/vnic # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、サービス プロファイルの vNIC を設定し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org* # scope service-profile ServInst90
UCS-A /org/service-profile* # create vnic vnic3 fabric a
UCS-A /org/service-profile/vnic* # set adapter-policy AdaptPol2
UCS-A /org/service-profile/vnic* # set fabric a-b
UCS-A /org/service-profile/vnic* # set identity mac-pool MacPool3
UCS-A /org/service-profile/vnic* # set mtu 8900
UCS-A /org/service-profile/vnic* # set nw-control-policy ncp5
UCS-A /org/service-profile/vnic* # set order 0
UCS-A /org/service-profile/vnic* # set pin-group EthPinGroup12
UCS-A /org/service-profile/vnic* # set qos-policy QosPol5
UCS-A /org/service-profile/vnic* # set stats-policy StatsPol2
UCS-A /org/service-profile/vnic* # set template-name VnicConnPol3
UCS-A /org/service-profile/vnic* # set set vcon any
UCS-A /org/service-profile/vnic* # commit-buffer
UCS-A /org/service-profile/vnic #
```

サービス プロファイルの vHBA の設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	指定したサービスで組織サービス プロファイル モードを開始します。
ステップ 3	UCS-A /org/service-profile # **create vhba** *vhba-name* [**fabric** {**a** | **b**}] [**fc-if** *fc-if-name*]	指定したサービス プロファイル用の vHBA を作成し、組織サービス プロファイルの vHBA モードを開始します。
ステップ 4	UCS-A /org/service-profile/vhba # **set adapter-policy** *policy-name*	vHBA に対し使用するアダプタ ポリシーを指定します。
ステップ 5	UCS-A /org/service-profile/vhba # **set admin-vcon** {**1** | **2** | **any**}	vHBA を 1 つまたはすべての仮想ネットワーク インターフェイス接続に割り当てます。
ステップ 6	UCS-A /org/service-profile/vhba # **set identity** {**dynamic-wwpn** {*wwpn* | **derived**} | **wwpn-pool** *wwn-pool-name*}	vHBA の WWPN を指定します。 次のいずれかのオプションを使用してストレージ ID を設定できます。 • 一意の WWPN を *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh* 形式で作成します。 WWPN は、20:00:00:00:00:00:00:00 ～ 20:FF:FF:FF:FF:FF:FF:FF または 50:00:00:00:00:00:00:00 ～ 5F:FF:FF:FF:FF:FF:FF:FF の範囲内で指定できます。 WWPN に Cisco MDS ファイバ チャネル スイッチと互換性を持たせる場合は、WWPN テンプレート 20:00:00:25:B5:XX:XX:XX を使用します。 • 製造時にハードウェアに焼き付けられた WWPN から WWPN 取得する。 • WWN プールから WWPN を割り当てる。

	コマンドまたはアクション	目的
ステップ 7	UCS-A /org/service-profile/vhba # **set max-field-size** *size-num*	vHBA がサポートするファイバチャネル フレーム ペイロードの最大サイズ（バイト数）を指定します。
ステップ 8	UCS-A /org/service-profile/vhba # **set order** {*order-num* | **unspecified**}	vHBA の PCI スキャン順序を指定します。
ステップ 9	UCS-A /org/service-profile/vhba # **set pers-bind** {**disabled** | **enabled**}	ファイバ チャネル ターゲットに対する永続的なバインディングをディセーブルまたはイネーブルにします。
ステップ 10	UCS-A /org/service-profile/vhba # **set pin-group** *group-name*	vHBA に使用する SAN ピン グループを指定します。
ステップ 11	UCS-A /org/service-profile/vhba # **set qos-policy** *policy-name*	vHBA に対し使用する QoS ポリシーを指定します。
ステップ 12	UCS-A /org/service-profile/vhba # **set stats-policy** *policy-name*	vHBA に使用する統計情報しきい値ポリシーを指定します。
ステップ 13	UCS-A /org/service-profile/vhba # **set template-name** *policy-name*	vHBA に使用する vHBA テンプレートを指定します。
ステップ 14	UCS-A /org/service-profile/vhba # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、サービス プロファイル用の vHBA を設定し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org* # scope service-profile ServInst90
UCS-A /org/service-profile* # create vhba vhba3 fabric b
UCS-A /org/service-profile/vhba* # set adapter-policy AdaptPol2
UCS-A /org/service-profile/vhba* # set admin-vcon any
UCS-A /org/service-profile/vhba* # set identity wwpn-pool SanPool7
UCS-A /org/service-profile/vhba* # set max-field-size 2112
UCS-A /org/service-profile/vhba* # set order 0
UCS-A /org/service-profile/vhba* # set pers-bind enabled
UCS-A /org/service-profile/vhba* # set pin-group FcPinGroup12
UCS-A /org/service-profile/vhba* # set qos-policy QosPol5
UCS-A /org/service-profile/vhba* # set stats-policy StatsPol2
UCS-A /org/service-profile/vhba* # set template-name SanConnPol3
UCS-A /org/service-profile/vhba* # commit-buffer
UCS-A /org/service-profile/vhba #
```

サービス プロファイルのローカル ディスクの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / と入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	指定したサービス プロファイルで組織サービス プロファイル モードを開始します。
ステップ 3	UCS-A /org/service-profile # **create local-disk-config**	サービス プロファイルのローカル ディスク設定を作成し、組織サービス プロファイルのローカル ディスク コンフィギュレーション モードを開始します。
ステップ 4	UCS-A /org/service-profile/local-disk-config # **set descr** *description*	（任意） ローカル ディスク設定に説明を記入します。
ステップ 5	UCS-A /org/service-profile/local-disk-config # **set mode** {**any-configuration** | **no-local-storage** | **no-raid** | **raid-0-striped** | **raid-1-mirrored** | **raid-5-striped-parity** | **raid-6-striped-dual-parity** | **raid-10-mirrored-and-striped**}	ローカル ディスクのモードを指定します。
ステップ 6	UCS-A /org/service-profile/local-disk-config # **create partition**	ローカル ディスクのパーティションを作成し、組織サービス プロファイルのローカル ディスク設定パーティション モードを開始します。
ステップ 7	UCS-A /org/service-profile/local-disk-config/partition # **set descr** *description*	（任意） パーティションの説明を記します。
ステップ 8	UCS-A /org/service-profile/local-disk-config/partition # **set size** {*size-num* | **unspecified**}	パーティションのサイズを MB 単位で指定します。
ステップ 9	UCS-A /org/service-profile/local-disk-config/partition # **set type** {**ext2** | **ext3** | **fat32** | **none** | **ntfs** | **swap**}	パーティション タイプを指定します。

	コマンドまたはアクション	目的
ステップ 10	UCS-A /org/service-profile/local-disk-config/partition # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、サービスプロファイルのローカルディスクを設定し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # scope service-profile ServInst90
UCS-A /org/service-profile # scope boot-definition
UCS-A /org/service-profile # create local-disk-config
UCS-A /org/service-profile/local-disk-config* # set mode raid-1-mirrored
UCS-A /org/service-profile/local-disk-config* # create partition
UCS-A /org/service-profile/local-disk-config/partition* # set size 1000000
UCS-A /org/service-profile/local-disk-config/partition* # set type ntfs
UCS-A /org/service-profile/local-disk-config/partition* # commit-buffer
UCS-A /org/service-profile/local-disk-config/partition #
```

サービス プロファイルの Serial over LAN の設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	指定したサービスで組織サービス プロファイル モードを開始します。
ステップ 3	UCS-A /org/service-profile # **create sol-config**	サービス プロファイルの Serial over LAN 設定を作成し、組織サービス プロファイルの SoL コンフィギュレーション モードを開始します。
ステップ 4	UCS-A /org/service-profile/sol-config # {**disable** | **enable**}	サービス プロファイルの Serial over LAN 設定をイネーブルまたはディセーブルにします。
ステップ 5	UCS-A /org/service-profile/sol-config # **set descr** *description*	（任意） Serial over LAN 設定に説明を加えます。
ステップ 6	UCS-A /org/service-profile/sol-config # **set speed** {**115200** | **19200** | **38400** | **57600** | **9600**}	シリアル ボー レートを指定します。

	コマンドまたはアクション	目的
ステップ 7	UCS-A /org/service-profile/sol-config # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、ServInst90 という名前のサービス プロファイルに Serial over LAN を設定し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # scope service-profile ServInst90
UCS-A /org/service-profile # create sol-config
UCS-A /org/service-profile/sol-config* # enable
UCS-A /org/service-profile/sol-config* # set descr "Sets serial over LAN to 9600 baud."
UCS-A /org/service-profile/sol-config* # set speed 9600
UCS-A /org/service-profile/sol-config* # commit-buffer
UCS-A /org/service-profile/sol-config #
```

サービス プロファイル ブート定義設定

サービス プロファイルのブート定義の設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に **/** を入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	指定したサービスで組織サービス プロファイル モードを開始します。
ステップ 3	UCS-A /org/service-profile # **create boot-definition**	サービスプロファイルのブート定義を作成し、組織サービス プロファイルのブート定義モードを開始します。
ステップ 4	UCS-A /org/service-profile/boot-definition # **set descr** *description*	（任意） ブート定義の説明を記入します。
ステップ 5	UCS-A /org/service-profile/boot-definition # **set reboot-on-update** {**no** | **yes**}	（任意） ブート順に変更を加えた後に、このブート定義を使用するすべてのサーバを自動的にリブートするかどうかを指定します。デフォルトでは、更新時のリブート オプションはディセーブルです。

	コマンドまたはアクション	目的
ステップ 6	UCS-A /org/service-profile/boot-definition # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、サービス プロファイルにブート定義を設定し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org* # scope service-profile ServInst90
UCS-A /org/service-profile* # create boot-definition
UCS-A /org/service-profile/boot-definition* # set descr "This boot definition reboots on
update."
UCS-A /org/service-profile/boot-definition* # set reboot-on-update yes
UCS-A /org/service-profile/boot-definition* # commit-buffer
UCS-A /org/service-profile/boot-definition #
```

次の作業

次の 1 つ以上のブート オプションをブート定義に設定し、ブート順序を設定します。

- **LAN Boot**：中央集中型プロビジョニング サーバからブートします。これは、このサーバから、別のサーバ上にオペレーティング システムをインストールするためによく使用されます。

  [LAN ブート（LAN Boot）] オプションを選択した場合は、サービス プロファイル ブート定義の LAN ブートの設定, （681 ページ） に進みます。

- **Storage Boot**：SAN 上のオペレーティング システム イメージからブートします。プライマリおよびセカンダリ SAN ブートを指定できます。プライマリ ブートが失敗した場合、サーバはセカンダリからのブートを試行します。

  システムに最高のサービス プロファイル モビリティを提供する SAN ブートの使用を推奨します。SAN からブートした場合、あるサーバから別のサーバにサービス プロファイルを移動すると、移動後のサーバは、まったく同じオペレーティング システム イメージからブートします。したがって、ネットワークからは、この新しいサーバはまったく同じサーバと認識されます。

  [ストレージ ブート（Storage Boot）] オプションを選択した場合は、サービス プロファイル ブート定義のストレージ ブートの設定, （682 ページ） に進みます。

- **Virtual Media Boot**：サーバへの物理 CD の挿入を模倣します。これは通常、サーバ上にオペレーティング システムを手動でインストールする場合に使用されます。

  [仮想メディア ブート（Virtual Media Boot）] オプションを選択した場合は、サービス プロファイル ブート定義の仮想メディア ブートの設定, （684 ページ） に進みます。

サービス プロファイル ブート定義の LAN ブートの設定

はじめる前に

サービス プロファイルのブート定義を設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に **/** を入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	指定したサービス プロファイルで組織サービスプロファイルモードを開始します。
ステップ 3	UCS-A /org/service-profile # **scope boot-definition**	組織サービス プロファイルのブート定義モードを開始します。
ステップ 4	UCS-A /org/service-profile/boot-definition # **create lan**	サービス プロファイルのブート定義にLANブートを作成し、サービスプロファイルのブート定義LANモードを開始します。
ステップ 5	UCS-A /org/service-profile/boot-definition/lan # **set order** {**1** | **2** | **3** | **4**}	LANブートのブート順序を指定します。
ステップ 6	UCS-A /org/service-profile/boot-definition/lan # **create path** {**primary** | **secondary**}	プライマリまたはセカンダリ LANブートパスを作成し、サービス プロファイルのブート定義 LAN パス モードを開始します。
ステップ 7	UCS-A /org/service-profile/boot-definition/lan/path # **set vnic** *vnic-name*	LAN イメージ パスに使用する vNIC を指定します。
ステップ 8	UCS-A /org/service-profile/boot-definition/lan/path # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、ServInst90 という名前のサービス プロファイルに入り、サービス プロファイルのブート定義に LAN ブートを作成し、ブート順序を 2 に設定し、プライマリ パスを作成し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org* # scope service-profile ServInst90
```

```
UCS-A /org/service-profile* # scope boot-definition
UCS-A /org/service-profile/boot-definition* # create lan
UCS-A /org/service-profile/boot-definition/lan* # set order 2
UCS-A /org/service-profile/boot-definition/lan* # create path primary
UCS-A /org/service-profile/boot-definition/lan/path* # set vnic vnic3
UCS-A /org/service-profile/boot-definition/lan/path* # commit-buffer
UCS-A /org/service-profile/boot-definition/lan/path #
```

サービス プロファイル ブート定義のストレージ ブートの設定

はじめる前に

サービス プロファイルのブート定義を設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	指定したサービスで組織サービス プロファイル モードを開始します。
ステップ 3	UCS-A /org/service-profile # **scope boot-definition**	組織サービス プロファイルのブート定義モードを開始します。
ステップ 4	UCS-A /org/service-profile/boot-definition # **create storage**	サービス プロファイルのブート定義にストレージ ブートを作成し、サービス プロファイルのブート定義ストレージ モードを開始します。
ステップ 5	UCS-A /org/service-profile/boot-definition/storage # **set order** {**1** | **2** | **3** | **4**}	ストレージ ブートのブート順序を指定します。
ステップ 6	UCS-A /org/service-profile/boot-definition/storage # **create** {**local** | **san-image** {**primary** | **secondary**}}	ローカル ストレージ ブートまたはSANイメージブートを作成します。SANイメージ ブートが作成されると、サービス プロファイルのブート定義ストレージ SANイメージ モードを開始します。
ステップ 7	UCS-A /org/service-profile/boot-definition/storage/san-image # **create path** {**primary** | **secondary**}	プライマリまたはセカンダリ SANイメージ パスを作成し、サービス プロファイルのブート

	コマンドまたはアクション	目的
		定義ストレージSANイメージパス モードを開始します。 Cisco UCS サーバで拡張ブート順序を使用する場合は、定義したブート順序が使用されます。用語「プライマリ」または「セカンダリ」を使用した標準のブート モードは、ブート順序を示唆するものではありません。同じデバイス クラス内での実際のブート順序は、PCIe バス スキャン順序により決定されます。
ステップ 8	UCS-A /org/service-profile/boot-definition/storage/san-image/path # **set lun** *lun-num*	SAN イメージ パスに使用される LUN を指定します。
ステップ 9	UCS-A /org/service-profile/boot-definition/storage/san-image/path # **set vhba** *vhba-name*	SAN イメージ パスに使用される vHBA を指定します。
ステップ 10	UCS-A /org/service-profile/boot-definition/storage/san-image/path # **set wwn** *wwn-num*	SAN イメージ パスに使用される WWN を指定します。
ステップ 11	UCS-A /org/service-profile/boot-definition/storage/san-image/path # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、ServInst90 という名前のサービス プロファイルに入り、サービス プロファイルのブート定義にストレージブートを作成し、ブート順序を 2 に設定し、プライマリ パスを作成し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org* # scope service-profile ServInst90
UCS-A /org/service-profile* # scope boot-definition
UCS-A /org/service-profile/boot-definition* # create storage
UCS-A /org/service-profile/boot-definition/storage* # create san-image primary
UCS-A /org/service-profile/boot-definition/storage* # set order 2
UCS-A /org/service-profile/boot-definition/storage/san-image* # create path primary
UCS-A /org/service-profile/boot-definition/storage/san-image/path* # set lun 27512
UCS-A /org/service-profile/boot-definition/storage/san-image/path* # set vhba vhba3
UCS-A /org/service-profile/boot-definition/storage/san-image/path* # set wwn
20:00:00:00:20:00:00:23
UCS-A /org/service-profile/boot-definition/storage/san-image/path* # commit-buffer
UCS-A /org/service-profile/boot-definition/storage/san-image/path #
```

サービス プロファイル ブート定義の仮想メディア ブートの設定

はじめる前に

サービス プロファイルのブート定義を設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に **/** を入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	指定したサービスで組織サービス プロファイル モードを開始します。
ステップ 3	UCS-A /org/service-profile # **scope boot-definition**	組織サービス プロファイルのブート定義モードを開始します。
ステップ 4	UCS-A /org/service-profile/boot-definition # **create virtual-media** {**read-only** | **read-write**}	サービス プロファイル ブート定義に読み取り専用または読み取りと書き込みの仮想メディア ブートを作成し、サービス プロファイルのブート定義仮想メディア モードを開始します。
ステップ 5	UCS-A /org/service-profile/boot-definition/virtual-media # **set order** {**1** | **2** | **3** | **4**}	仮想メディア ブートのブート順序を指定します。
ステップ 6	UCS-A /org/service-profile/boot-definition/virtual-media # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、ServInst90 という名前のサービス プロファイルに入り、サービス プロファイルのブート定義に読み取り専用権限で仮想メディア ブートを作成し、ブート順序を 3 に設定し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org* # scope service-profile ServInst90
UCS-A /org/service-profile* # scope boot-definition
UCS-A /org/service-profile/boot-definition* # create virtual-media read-only
UCS-A /org/service-profile/boot-definition/virtual-media* # set order 1
UCS-A /org/service-profile/boot-definition/virtual-media* # commit-buffer
UCS-A /org/service-profile/boot-definition/virtual-media #
```

サービス プロファイルのブート定義の削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / と入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	指定したサービスで組織サービス プロファイル モードを開始します。
ステップ 3	UCS-A /org/service-profile # **delete boot-definition**	サービス プロファイルのブート定義を削除します。
ステップ 4	UCS-A /org/service-profile # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、サービス プロファイルのブート定義を削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # scope service-profile ServInst90
UCS-A /org/service-profile # delete boot-definition
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile #
```

サービス プロファイルのファイバ チャネル ゾーン分割の設定

既存のストレージ接続ポリシーでの vHBA イニシエータ グループの設定

この手順では、既存のグローバル ファイバ チャネル ストレージ接続ポリシーを使用すると想定されています。このサービス プロファイルに対してのみストレージ接続ポリシー定義を作成する場合は、ローカル ストレージ接続ポリシー定義での vHBA イニシエータ グループの設定, （686 ページ） を参照してください。

すべてのサービス プロファイルで使用できるグローバル ファイバ チャネル ストレージ接続ポリシーを作成する方法については、ファイバ チャネル ストレージ接続ポリシーの作成, （411 ページ） を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	指定したサービス プロファイルで組織サービス プロファイル モードを開始します。
ステップ 3	UCS-A /org/service-profile # **create initiator-group** *group-name*	ファイバチャネルゾーン分割の指定イニシエータ グループを作成し、サービス プロファイルのイニシエータ グループモードを開始します。
ステップ 4	UCS-A /org/service-profile/initiator-group # **create initiator** *vhba-name*	イニシエータ グループの指定vHBAイニシエータを作成します。 必要に応じて、この手順を繰り返しグループに 2 番目の vHBA を追加します。
ステップ 5	UCS-A /org/service-profile/initiator-group # **set storage-connection-policy** *policy-name*	サービス プロファイルに指定されたストレージ接続ポリシーを関連付けます。
ステップ 6	UCS-A /org/service-profile # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、ServInst90 という名前のサービス プロファイルに対し 2 つの vHBA イニシエータを持つ initGroupZone1 という名前の vHBA イニシエータ グループを設定し、既存のファイバ チャネル ストレージ接続ポリシーを含め、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # scope service-profile ServInst90
UCS-A /org/service-profile # create initiator-group initGroupZone1
UCS-A /org/service-profile/initiator-group* # create initiator vhba1
UCS-A /org/service-profile/initiator-group* # create initiator vhba2
UCS-A /org/service-profile/initiator-group* # set storage-connection-policy scpolicyZone1
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile #
```

ローカル ストレージ接続ポリシー定義での vHBA イニシエータ グループの設定

この手順では、サービス プロファイルにローカル ファイバ チャネル ストレージ接続ポリシーを作成すると想定しています。既存のストレージ接続ポリシーを使用する場合は、既存のストレージ接続ポリシーでの vHBA イニシエータ グループの設定, （685 ページ） を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	指定したサービスプロファイルで組織サービスプロファイルモードを開始します。
ステップ 3	UCS-A /org/service-profile # **create initiator-group** *group-name*	ファイバチャネルゾーン分割の指定イニシエータ グループを作成し、サービスプロファイルのイニシエータ グループ モードを開始します。
ステップ 4	UCS-A /org/service-profile/initiator-group # **create initiator** *vhba-name*	vHBA イニシエータ グループの指定 vHBA イニシエータを作成します。 必要に応じて、この手順を繰り返しグループに 2 番目の vHBA を追加します。
ステップ 5	UCS-A /org/service-profile/initiator-group # **create storage-connection-def** *policy-name*	指定したストレージ接続ポリシー定義を作成し、ストレージ接続定義モードを開始します。
ステップ 6	UCS-A /org/service-profile/initiator-group/storage-connection-def # **create storage-target** *wwpn*	指定された WWPN を持つストレージ ターゲットエンドポイントを作成し、ストレージターゲット モードを開始します。

	コマンドまたはアクション	目的
ステップ 7	UCS-A /org/service-profile/initiator-group/storage-connection-def/storage-target # **set target-path** {**a** | **b**}	ターゲット エンドポイントとの通信に使用するファブリック インターコネクトを指定します。
ステップ 8	UCS-A /org/service-profile/initiator-group/storage-connection-def/storage-target # **set target-vsan** *vsan*	ターゲット エンドポイントとの通信に使用する VSAN を指定します。
ステップ 9	UCS-A /org/service-profile/initiator-group # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、ServInst90 という名前のサービス プロファイルに対し 2 つの vHBA イニシエータを持つ initGroupZone1 という名前の vHBA イニシエータ グループを設定し、scPolicyZone1 という名前のローカル ストレージ接続ポリシー定義を設定し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org* # scope service-profile ServInst90
UCS-A /org/service-profile # create initiator-group initGroupZone1
UCS-A /org/service-profile/initiator-group* # create initiator vhba1
UCS-A /org/service-profile/initiator-group* # create initiator vhba2
UCS-A /org/service-profile/initiator-group* # create storage-connection-def scPolicyZone1
UCS-A /org/service-profile/initiator-group/storage-connection-def* # create storage-target

20:10:20:30:40:50:60:70
UCS-A /org/service-profile/initiator-group/storage-connection-def/storage-target* # set
target-path a
UCS-A /org/service-profile/initiator-group/storage-connection-def/storage-target* # set
target-vsan default
UCS-A /org/service-profile/initiator-group* # commit-buffer
UCS-A /org/service-profile/initiator-group #
```

サービス プロファイルおよびサービス プロファイル テンプレートの管理

サービス プロファイルとブレード サーバまたはサーバ プールの関連付け

作成時にサービスプロファイルとブレードサーバまたはサーバプールを関連付けなかった場合、またはサービス プロファイルを関連付けるブレード サーバまたはサーバ プールを変更する場合には、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	指定したサービス プロファイルで組織サービス プロファイル モードを開始します。
ステップ 3	UCS-A /org/service-profile # **associate** {**server** *chassis-id/ slot-id* | **server-pool** *pool-name qualifier*} [**restrict-migration**]	サービス プロファイルを単一のサーバに関連付けます。または、指定したサーバプール ポリシー資格情報を使用して、指定したサーバ プールに関連付けます。 オプションの **restrict-migration** キーワードを追加すると、サービス プロファイルは別のサーバに移行されません。
ステップ 4	UCS-A /org/service-profile # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、ServProf34 という名前のサービス プロファイルとシャーシ 1 のスロット 4 のサーバを関連付け、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org* # scope service-profile ServProf34
UCS-A /org/service-profile* # associate server 1/4
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile #
```

サービス プロファイルとラック サーバの関連付け

作成時にサービス プロファイルをラック サーバを関連付けなかった場合、またはサービス プロファイルを関連付けるラック サーバを変更する場合には、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	指定したサービス プロファイルで組織サービス プロファイル モードを開始します。
ステップ 3	UCS-A /org/service-profile # **associate server** *serv-id* [**restrict-migration**]	サービス プロファイルと指定したラック サーバを関連付けます。 オプションの restrict-migration コマンドを追加すると、サービス プロファイルは別のサーバに移行されません。
ステップ 4	UCS-A /org/service-profile # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、ServProf34 という名前のサービス プロファイルとラック サーバ 1 を関連付け、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org* # scope service-profile ServProf34
UCS-A /org/service-profile* # associate server 1
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile #
```

サービス プロファイルとサーバまたはサーバ プールの関連付け解除

この手順では、サービス プロファイルとブレード サーバ、ラック サーバ、またはサーバ プールの関連付け解除について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / と入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	指定したサービス プロファイルで組織サービス プロファイル モードを開始します。
ステップ 3	UCS-A /org/service-profile # **disassociate**	サービス プロファイルとサーバまたはサーバ プールの関連付けを解除します。
ステップ 4	UCS-A /org/service-profile # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、ServProf34 という名前のサービス プロファイルとサーバの関連付けを解除し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org* # scope service-profile ServProf34
UCS-A /org/service-profile # disassociate
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile #
```

サービス プロファイルの名前の変更

サービス プロファイルの名前を変更すると、次のことが起こります。

- サービス プロファイルの以前の名前を参照するイベント ログと監査ログは、その名前のまま保持されます。
- 名前変更の操作を記録する、新しい監査データが作成されます。
- サービス プロファイルの以前の名前で生じたすべての障害データは、新しいサービス プロファイル名に転送されます。

（注） 保留中の変更があるサービス プロファイルの名前は変更できません。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に **/** を入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	指定したサービスで組織サービス プロファイル モードを開始します。
ステップ 3	UCS-A /org/service-profile # **rename-to** *new-profile-name*	指定されたサービス プロファイルの名前を変更します。 このコマンドを入力すると、CLI セッションのコミットされていないすべての変更が失われることがあるという警告がされます。続行するには確認のため y を入力します。 この名前には、2 ～ 32 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。この名前は、同じ組織内のすべてのサービス プロファイルおよびサービス プロファイル テンプレートで一意であることが必要です。

	コマンドまたはアクション	目的
ステップ 4	UCS-A /org/service-profile/ # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、ServInst90 から ServZoned90 にサービス プロファイル名を変更し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org* # scope service-profile ServInst90
UCS-A /org/service-profile* # rename-to ServZoned90
Rename is a standalone operation. You may lose any uncommitted changes in this CLI session.
Do you want to continue? (yes/no): y
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile #
```

サービス プロファイルに割り当てられた UUID の、サービス プロファイル テンプレートのプールからのリセット

更新中のサービス プロファイル テンプレートに割り当てられている UUID サフィックス プールを変更しても、Cisco UCS Manager により、そのテンプレートにより作成されたサービス プロファイルに割り当てられている UUID は変更されません。Cisco UCS Manager を使用して、新しくサービス プロファイルに割り当てられたプールから UUID を割り当て、これを関連付けられたサーバに反映させるには、UUID をリセットする必要があります。サービス プロファイルおよび関連付けられたサーバに割り当てられている UUID は、次の状況でのみリセットできます。

- サービス プロファイルが更新中のサービス プロファイル テンプレートから作成されていて、UUID サフィックス プールから割り当てられた UUID が含まれている。
- UUID サフィックス プール名がサービス プロファイルで指定されている。たとえば、プール名が空でない場合です。
- UUID の値が 0 でない（サーバ ハードウェアに由来しない）。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	UUID をリセットする組織でコマンド モードを開始します。システムにマルチテナント機能が含まれていない場合、ルート組織モードに入るには、/ を *org-name* として入力します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	関連付けられたサーバの UUID を別の UUID 接尾辞プールにリセットする必要があるサービス プロファイルを入力します。
ステップ 3	UCS-A /org/service-profile # **set identity dynamic-uuid derived**	サービス プロファイルがプールから UUID を動的に取得するように指定します。
ステップ 4	UCS-A /org/service-profile # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、サービス プロファイルの UUID を別の UUID 接尾辞プールにリセットする例を示します。

```
UCS-A# scope org /
UCS-A /org # scope service-profile ServInst90
UCS-A /org/service-profile # set identity dynamic-uuid derived
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile #
```

vNIC に割り当てられた MAC アドレスの、サービス プロファイル テンプレートのプールからのリセット

更新中のサービス プロファイル テンプレートに割り当てられている MAC プールを変更しても、Cisco UCS Manager より、そのテンプレートにより作成されたサービス プロファイルに割り当てられている MAC アドレスは変更されません。Cisco UCS Manager を使用して、新しくサービス プロファイルに割り当てられたプールから MAC アドレスを割り当て、これを関連付けられたサーバに反映させるには、MAC アドレスをリセットする必要があります。サービス プロファイルおよび関連付けられたサーバに割り当てられている MAC アドレスは、次の状況でのみリセットできます。

- サービスプロファイルが更新中のサービスプロファイルテンプレートから作成されていて、MAC プールから MAC アドレスが割り当てられている。
- MAC プール名がサービス プロファイルで指定されている。たとえば、プール名が空でない場合です。
- MAC アドレスの値が 0 でない（サーバ ハードウェアに由来しない）。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	MAC アドレスをリセットするサービス プロファイルを含む組織でコマンドモードを開始します。システムにマルチテナント機能が含まれていない

	コマンドまたはアクション	目的
		場合、ルート組織モードに入るには、/ を *org-name* として入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	関連するサーバの MAC アドレスを別の MAC アドレスにリセットする必要があるサービス プロファイルでコマンド モードを開始します。
ステップ 3	UCS-A /org/service-profile # **scope vnic** *vnic-name*	MAC アドレスをリセットする vNIC でコマンド モードを開始します。
ステップ 4	UCS-A /org/service-profile/vnic # **set identity dynamic-mac derived**	vNIC がプールから MAC アドレスを動的に取得するように指定します。
ステップ 5	UCS-A /org/service-profile/vnic # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、サービス プロファイルで vNIC の MAC アドレスをリセットする例を示します。

```
UCS-A# scope org /
UCS-A /org # scope service-profile ServInst90
UCS-A /org/service-profile #  scope vnic dynamic-prot-001
UCS-A /org/service-profile/vnic # set identity dynamic-mac derived
UCS-A /org/service-profile/vnic* # commit-buffer
UCS-A /org/service-profile/vnic #
```

vHBA に割り当てられた WWPN の、サービス プロファイル テンプレートのプールからのリセット

更新中のサービスプロファイルテンプレートに割り当てられている WWPN プールを変更しても、Cisco UCS Manager により、そのテンプレートにより作成されたサービス プロファイルに割り当てられている WWPN は変更されません。Cisco UCS Manager を使用して、新しくサービス プロファイルに割り当てられたプールから WWPN を割り当て、これを関連付けられたサーバに反映させるには、WWPN をリセットする必要があります。サービスプロファイルおよび関連付けられたサーバに割り当てられている WWPN は、次の状況でのみリセットできます。

- サービスプロファイルが更新中のサービスプロファイルテンプレートから作成されていて、WWPN プールから WWPN が割り当てられている。
- WWPN プール名がサービス プロファイルで指定されている。たとえば、プール名が空でない場合です。
- WWPN の値が 0 でない（サーバ ハードウェアに由来しない）。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	WWPN をリセットするサービス プロファイルを含む組織でコマンド モードを開始します。システムにマルチテナント機能が含まれていない場合、ルート組織モードに入るには、/ を *org-name* として入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	WWPN をリセットする vHBA のサービス プロファイルを入力します。
ステップ 3	UCS-A /org/service-profile # **scope vhba** *vhba-name*	WWPN をリセットする vHBA でコマンド モードを開始します。
ステップ 4	UCS-A /org/service-profile/vhba # **set identity dynamic-wwpn derived**	vHBA がプールから WWPN を動的に取得するように指定します。
ステップ 5	UCS-A /org/service-profile/vhba # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、サービス プロファイルで vHBA の WWPN をリセットする例を示します。

```
UCS-A# scope org /
UCS-A /org # scope service-profile ServInst90
UCS-A /org/service-profile #  scope vhba vhba3
UCS-A /org/service-profile/vhba # set identity dynamic-wwpn derived
UCS-A /org/service-profile/vhba* # commit-buffer
UCS-A /org/service-profile/vhba #
```

vHBA に割り当てられた **WWPN** の、サービス プロファイル テンプレートのプールからのリセット

第 33 章

Cisco UCS における電源管理

この章の内容は、次のとおりです。

Cisco UCS の電力の制限

電力制限により、サーバの最大電力消費を制御します。UCS B シリーズ ブレード サーバおよび UCS Mini の場合は、Cisco UCS Manager で電力割り当てを管理できます。また、混合 UCS ドメインの電源も管理できます。

UCS Manager は、次のサーバでの電力制限をサポートしています。

- UCS Mini 6324
- UCS 6300 シリーズ ファブリック インターコネクト

ポリシー方式のシャーシ グループ電力制限または手動でのブレード レベルの電力制限方式を使用して、シャーシ内のすべてのサーバに適用される電源を割り当てることができます。

Cisco UCS Manager は、サーバへの電力割り当てに役立つ次の電源管理ポリシーを提供しています。

電源管理ポリシー	説明
電源ポリシー	Cisco UCS ドメイン 内のすべてのシャーシに電源の冗長性を指定します。
電力制御ポリシー	シャーシ内の各ブレードの初期電源割り当てを計算するための優先順位を指定します。
グローバル電力割り当て（Global Power Allocation）	シャーシ内のすべてのサーバに適用されるポリシー方式のシャーシ グループの電力制限または手動でのブレードレベルの電力制限を指定します。
グローバル電力プロファイリング（Global Power Profiling）	サーバの電力制限値を計算する方法を指定します。有効な場合、サーバは、ベンチマークを用いて検出中にプロファイリングされます。このポリシーは、グローバル電力割り当てポリシーが [ポリシーに基づくシャーシ グループの上限（Policy Driven Chassis Group Cap）] に設定されている場合に適用されます。

ブレードに測定された電源の表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# power-cap-mgmt # **show power-measured** .	測定された電力を表示します。

次の例は、ブレードに測定された最小および最大電力制限値の一覧を示しています。

```
UCS-A# show power-measured
Measured Power:
    Device Id (W)  Minimum power (W) Maximum power (W) OperMethod
    -------------- ----------------- ----------------- ----------
    blade   1/1    168               252               Pnuos
    blade   1/2    350               580               Static
    blade   1/3    350               560               Static
    blade   1/4    350               398               Static
    blade   1/5    350               544               Static
    blade   1/6    350               560               Static
    blade   1/7    180               276               Pnuos
    blade   1/8    350               544               Static
```

ラック サーバの電源管理

電力制限はラック サーバではサポートされません。

電源管理の注意事項

CIMC をリセットすると、CIMC がリブートするまで、Cisco UCS の電力モニタリング機能が短時間使用不能になります。通常、リセットには20秒しかかかりませんが、その間にピーク電力制限を超える可能性があります。低電力制限が設定された環境で、設定された電力制限を超えないようにするには、CIMCのリブートまたはアクティブ化を交互に実施することを検討してください。

電源投入操作時の電源管理

電源投入時のブート調整

Cisco UCS Managerは、使用可能な電力量に基づいて、できるだけ多くのブレードをブートしようとします。ブレードをブートするために必要な電力が使用できない場合、UCS Manager は有限状態マシン（FSM）の CheckPowerAvailability ステージでのブートに切り替え、ブレードで「サーバ x/y に電源投入するために使用可能な電力が不足しています（Insufficient power available to power-on server x/y）」とのエラーが表示されます。

必要な電力が使用可能になると、FSM はブレードの電源投入を続行します。ブレードの電源がオフになった後、割り当てられた電力バジェットは再利用されます。

（注） ブレードに割り当てられた電力バジェットが再利用されると、割り当てられた電力は0Wとして表示されます。

制限事項

UCS Managerの外部のブレードに電源を投入する場合は、UCS Managerは電力バジェットをブレードに割り当てず、「サーバ x/y に電力制限を適用できませんでした（Power cap application failed for server x/y）」とのエラーが表示されます。

サービス プロファイルの関連付け中の電力割り当て

サービス プロファイルの関連付け中にブレードに割り当てられる電力は、使用されている電力制御ポリシーと、電力グループから使用可能な電力によって決まります。正常なサービス プロファイルの関連付け中に電力がサーバに割り当てられた後は、ブレードの最小電力制限が保証されます。電力制御ポリシーの優先度が no-cap に設定されている場合、ブレードには可能な最大電力制限が割り当てられ、表示されている測定済みの最大電力制限を上回る場合があります。

（注） 関連付けられたブレードの優先度が no-cap に変更され、最大電力制限を割り当てることができない場合は、次のいずれかのエラーが表示される場合があります。

- `PSU-insufficient`：PSU に使用可能な電力が不足しています。
- `Group-cap-insufficient`：グループの制限値がブレードには不足しています。

電源ポリシーの設定

Cisco UCS サーバの電源ポリシー

電源ポリシーはグローバルで、Cisco UCS Manager インスタンスが管理するすべてのシャーシによって継承されます。サービス プロファイルに電源ポリシーを追加して、Cisco UCS ドメイン 内のすべてのシャーシの電源に対して冗長性を指定することができます。このポリシーは PSU ポリシーとも呼ばれます。

電源の冗長性の詳細については、『*Cisco UCS 5108 Server Chassis Hardware Installation Guide*』 を参照してください。

電源ポリシーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に **/** を入力します。
ステップ 2	UCS-A /org # **scope psu-policy**	PSU ポリシー モードを開始します。
ステップ 3	UCS-A /org/psu-policy # **set redundancy** {**grid** | **n-plus-1** | **non-redund**}	次のいずれかの冗長タイプを指定します。 • **grid**：2 つの電源がオンにされます。そうでなければ、シャーシに N+1 よりも高い冗長性が要求されます。1 つの電源に障害が発生し、そのため 1 台または 2 台の PSU に電源障害が発生した場合、別の電源回路に接続され機能が存続している PSU がシャーシに電力を供給し続けます。

	コマンドまたはアクション	目的
		（注） [グリッド（Grid）] 冗長性のためには、電源に接続された少なくとも 4 台の PSU が必要です。接続された使用可能な PSU の数がこれに満たないと、電源ポリシーが適用できず、[冗長なし（Non Redundant）] が使用されます。 • **n-plus-1** 冗長性のためには、電源に接続された少なくとも 3 台の PSU が必要です。接続された使用可能な PSU の数がこれに満たないと、電源ポリシーが適用できず、**non-redund** が使用されます。 • **non-redund**：設置されたすべての電源装置（PSU）がオンになり、負荷が均等に分散されます。小規模構成の場合にのみ、単一 PSU で電力を供給できます。 小規模の構成とは、210 V 電源で 2500 W 未満の電力を必要とする構成、または 110 V 電源で 1300 W 未満の電力を必要とする構成です。 電源の冗長性の詳細については、『*Cisco UCS 5108 Server Chassis Installation Guide*』を参照してください。
ステップ 4	UCS-A /org/psu-policy # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、グリッド冗長性を使用するように電源ポリシーを設定し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # scope psu-policy
UCS-A /org/psu-policy # set redundancy grid
UCS-A /org/psu-policy* # commit-buffer
UCS-A /org/psu-policy #
```

グローバル電力プロファイリングポリシーの表示と変更

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A /power-cap-mgmt # **show profile-policy**	電力プロファイル ポリシーを表示します。
ステップ 2	UCS-A /power-cap-mgmt # **set profile** {**no** | **yes**}	プロファイル ポリシーを設定します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /power-cap-mgmt* # **comm-buffer**	トランザクションをシステム設定にコミットします。
ステップ 4	UCS-A /power-cap-mgmt # **show profile-policy**	グローバル電力プロファイリング ポリシーがオンであるかどうかを表示します。 [グローバル電力プロファイリング ポリシー（Global Power Profiling Policy）] : 電力プロファイリング（Power Profiling） o

次の例は、グローバル電力プロファイリング ポリシーを表示する方法を示しています。

```
UCS-A /power-cap-mgmt # show profile-policy
Global Power Profiling Policy:
    Power Profiling
    ---------------
    No

UCS-A /power-cap-mgmt # set profile-policy
no   yes

UCS-A /power-cap-mgmt # set profile-policy yes
UCS-A /power-cap-mgmt* # comm-buffer
UCS-A /power-cap-mgmt # show profile-policy

Global Power Profiling Policy:
    Power Profiling
    ---------------
    Yes
```

グローバル電力割り当てポリシーの設定

グローバル電力割り当てポリシー

グローバル電力割り当てポリシーは、ポリシー方式のシャーシ グループ電力制限またはブレード レベルの手動電力制限のいずれの電力割り当て方式をシャーシ内のサーバに適用するかを指定するグローバル ポリシーです。

デフォルトのポリシー方式のシャーシ グループ電力制限による電力割り当て方式を適用することを推奨します。

重要 ブレード レベルの手動電力制限の設定に変更を加えると、ポリシー方式のシャーシ グループ電力制限に設定されたグループや設定オプションが失われる結果になります。

グローバル電力割り当てポリシーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope power-cap-mgmt**	電力制限管理モードを開始します。
ステップ 2	UCS-A /power-cap-mgmt # **set cap-policy** {**manual-blade-level-cap** | **policy-driven-chassis-group-cap**}	指定された電力制限管理モードにグローバル制限ポリシーを設定します。 デフォルトでは、グローバル制限ポリシーは [ポリシーに基づくシャーシ グループの上限（Policy Driven Chassis Group Cap）] に設定されます。
ステップ 3	UCS-A /power-cap-mgmt # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、手動ブレードの電力制限にグローバル制限ポリシーを設定し、トランザクションをコミットします。

```
UCS-A# scope power-cap-mgmt
UCS-A /power-cap-mgmt # set cap-policy manual-blade-level-cap
UCS-A /power-cap-mgmt* # commit-buffer
UCS-A /power-cap-mgmt #
```

サーバの電源 CAP 値の表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope power-cap-mgmt**	電力制限管理モードを開始します。
ステップ 2	UCS-A /power-cap-mgmt # **show power-measured**	最小および最大電源 CAP 値を表示します。

次の例は、最小および最大電源 CAP 値を表示する方法を示しています。

```
UCS-A# scope power-cap-mgmt
UCS-A /power-cap-mgmt # show power-measured

Measured Power:
    Device Id (W)  Minimum power (W) Maximum power (W) OperMethod
    -------------- ----------------- ----------------- ----------
    blade   1/1    234               353               Pnuos
```

```
UCS-A /power-cap-mgmt #
```

グローバル電力プロファイル ポリシーの設定

グローバル電力プロファイリング ポリシー

グローバル電力プロファイリング ポリシーは、電力割り当てをシャーシ内のすべてのサーバにどのように適用するかを指定するグローバル ポリシーです。ポリシーは、グローバル電力割り当てポリシーが [ポリシーに基づくシャーシ グループの上限（Policy Driven Chassis Group Cap）]**policy-driven-chassis-group-cap** に設定されている場合に適用されます。グローバル電力プロファイリング ポリシーは次のいずれかに設定できます。

- [無効（Disabled）]：ブレードの最小/最大電力の制限値は、各コンポーネントの静的消費電力値に基づき算出されます。
- [有効（Enabled）]：ブレードの最小/最大電力の制限値は、サーバディスカバリの一部として測定されます。これらの値は、ブレードの実際の消費電力とほぼ同じです。

（注） グローバル電力プロファイリング ポリシーを有効にした後、最小/最大電力の上限値を取得するためにブレードを再認識させる必要があります。

重要 電力プロファイリングは、Cisco UCS B460 M4 ブレードではサポートされていません。

グローバル電力プロファイル ポリシーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope power-cap-mgmt**	電力制限管理モードを開始します。
ステップ 2	UCS-A /power-cap-mgmt # **set profile-policy** {**no** | **yes**}	グローバル電力プロファイリングポリシーをイネーブル化またはディセーブル化します。
ステップ 3	UCS-A /power-cap-mgmt # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例に、グローバル電力プロファイル ポリシーを有効にし、トランザクションをコミットする方法を示します。

```
UCS-A# scope power-cap-mgmt
UCS-A /power-cap-mgmt # set profile-policy yes
UCS-A /power-cap-mgmt* # commit-buffer
UCS-A /power-cap-mgmt #
```

ポリシー方式のシャーシ グループの電力制限の設定

ポリシー方式のシャーシ グループの電力制限

グローバル制限ポリシーで、ポリシー方式のシャーシ グループの電力制限を選択すると、Cisco UCS は、停電のリスクを負うことなく、サーバのオーバーサブスクリプションを維持できます。オーバーサブスクリプションは、二重のプロセスによって実現できます。たとえば、Cisco UCS のシャーシ レベルでは、電源グループのメンバー間で使用可能な電力量を分割し、ブレード レベルでは、シャーシに割り当てられた電力量をプライオリティに基づいてブレード間で分割します。

サービス プロファイルの関連付けや関連付け解除が実行されるたびに、Cisco UCS Manager はシャーシ内の各ブレード サーバへの電力割り当てを再計算します。必要に応じて、優先順位の低いサービス プロファイルの電力が優先順位の高いサービス プロファイルに再分配されます。

データセンターの回路ブレーカーを安全に保護するために、UCS 電源グループは 1 秒未満で電力をキャップします。ブレードは、シャーシの電力配分が最適化されるまで20秒間その上限にとどまる必要があります。これは、必要とされる一時的なスパイクに反応することがないよう、意図的によりゆっくりとしたタイムスケールで実行されます。

（注） システムは、各スロットのサーバを起動するのに十分な電力をリザーブしています。これは、スロットが空の場合でも同様です。このリザーブ電力が、より多くの電力を必要とするサーバで使用されることはありません。電力制限に準拠しないブレードはペナルティを課されます。

UCS Manager の電源グループ

電源グループは、すべてが同じ配電ユニット（PDU）から電源を得ているシャーシのセットです。Cisco UCS Manager では、1 つ以上のシャーシを含む電源グループを作成し、その電源グループに AC ワット単位でピーク電力キャップを設定することができます。

シャーシ レベルで電力制限を実装するには、以下が必要です。

- IOM、CIMC、および BIOS バージョン 1.4 以上
- 2 つの電源装置（PSU）

ピーク電力キャップは、特定の電源グループ内のすべてのブレード サーバで使用可能な最大電力を表すスタティック値です。電源グループにブレードを追加、または電源グループからブレード

を除外し、手動でピーク電力値を変更しなかった場合、電源グループはピーク電力キャップを調整して、その電源グループ内のすべてのブレードの基本的な電源投入要件に適合させます。

最低AC 890ワットが各シャーシに設定されます。これは、空のシャーシに電源を供給するために必要な最低電力量である DC 電力 800 ワットに変換されます。ハーフ幅のブレードを関連付けるには、グループの制限値を AC 電力 1475 ワットに設定する必要があります。フル幅のブレードでは、AC 電力 2060 ワットに設定する必要があります。

シャーシが電源グループに追加されると、シャーシ内のブレードに関連付けられているすべてのサービス プロファイルが、その電源グループの一部になります。同様に、シャーシに新規ブレードを追加すると、そのブレードは、当然のこととして、シャーシの電源グループの一部になります。

（注） 電源グループの作成は、サーバ プールの作成とは異なります。ただし、電源修飾子を作成してサーバ プール ポリシーに追加することで、サーバ プールに同じ電源グループのメンバを組み入れることができます。

シャーシを除外または削除すると、そのシャーシは電源グループから削除されます。

UCS Manager は明示的な電源グループと暗黙的な電源グループをサポートしています。

- [明示的（Explicit）]：電源グループを作成し、シャーシとラックを追加し、グループに電力バジェットを割り当てることができます。
- [暗黙的（Implicit）]：電力消費を安全限界内に制限することで、シャーシが常に保護されるようにします。 デフォルトでは、明示的な電源グループに属さないすべてのシャーシがデフォルト グループに割り当てられ、適切な制限が設定されます。UCS Managerに接続する新しいシャーシは、別の電源グループに移動するまで、デフォルトの電源グループに追加されます。

次の表は、電源バジェットの割り当て時および電源グループとの連動時に、表示される可能性のあるエラー メッセージを示しています。

エラー メッセージ	原因	推奨処置
電力グループ POWERGROUP_NAME のバジェットが不十分です（Insufficient budget for power group POWERGROUP_NAME） および/または グループの上限が低いため、シャーシ N には上限を設定できません。（Chassis N cannot be capped as group cap is low.）上限を上げることを検討してください。（Please consider raising the cap.） および/または 管理者が以前の値 N を使用して電力グループ GROUP_NAME に不十分なコミットを行いました（Admin committed insufficient for power group GROUP_NAME, using previous value N） および/または シャーシ N の電源制限アプリケーションが失敗しました（Power cap application failed for chassis N）	シャーシに電力制限を割り当てている状態で下限が満たされなかった場合、またはブレードの追加や電源ポリシーの変更のために電力要件が増えた場合に、これらのメッセージのいずれかが表示されます。	電力制限を、指定された電源グループの [電源グループ（Power Group）] ページに表示された [操作を可能にする最小電力の上限（W）（Minimum Power Cap for Allowing Operations (W)）] の値まで増やします。

エラー メッセージ	原因	推奨処置
使用可能な PSU 電力がシャーシとブレードで不足しているため、シャーシ N には上限を設定できません。（Chassis N cannot be capped as the available PSU power is not enough for the chassis and the blades.）入力電源を確認して問題を解決するか、PSU を交換してください（Please correct the problem by checking input power or replace the PSU）	シャーシの電力バジェット要件が使用可能なPSU電力を上回っている場合に表示されます。	PSU入力電力と冗長性ポリシーをチェックし、シャーシ用に十分な電力が使用可能であることを確認します。 PSUに障害がある場合は、PSUを交換します。
サーバ N の電源制限アプリケーションが失敗しました（Power cap application failed for server N）	サーバが割り当てを超える電力を消費しており、制限できない場合、または電力が割り当てられていないサーバに電源が投入されている場合に表示されます。	関連付けられていないサーバの電源をオフにします。
サーバの電力消費が上限に達したので P 状態が低下しました（P-State lowered as consumption hit power cap for server）	サーバが、割り当てられた電力以下に電力消費を削減するよう制限されている場合に表示されます。	これは情報メッセージです。 サーバ電力を制限する必要がない場合は、サービス プロファイルの電力制御ポリシーの [電力の制限（Power Capping）] フィールドの値を [no-cap] に設定します。
シャーシ N にハイラインとローラインの PSU 入力電源が混在しています。（Chassis N has a mix of high-line and low-line PSU input power sources.）	このエラーは、シャーシにハイラインとローラインの PSU 入力電源が混在して接続されている場合に発生します。	これは、サポートされていない設定です。PSUはすべて同様の電源に接続する必要があります。

電源グループの作成

はじめる前に

グローバル電力割り当てポリシーが [ポリシーに基づくシャーシ グループの上限（Policy Driven Chassis Group Cap）] に設定されていることを確認してください。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope power-cap-mgmt**	電力制限管理モードを開始します。
ステップ 2	UCS-A /power-cap-mgmt # **create power-group** *power-group-name*	電源グループを作成し、電源グループ モードを開始します。
ステップ 3	UCS-A /power-cap-mgmt/power-group # **set peak** {*peak-num* | **disabled** | **uninitialized**}	電源グループに使用可能な最大ピーク時電力（W）を指定します。
ステップ 4	UCS-A /power-cap-mgmt/power-group # **create chassis** *chassis-id*	指定されたシャーシを電源グループに追加し、電源グループ シャーシ モードを開始します。
ステップ 5	UCS-A /power-cap-mgmt/power-group/chassis # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、powergroup1 という電力グループを作成し、電源グループの最大ピーク時電力（10000 W）を指定し、シャーシ 1 をグループに追加し、トランザクションをコミットします。

```
UCS-A# scope power-cap-mgmt
UCS-A /power-cap-mgmt # create power-group powergroup1
UCS-A /power-cap-mgmt/power-group* # set peak 10000
UCS-A /power-cap-mgmt/power-group* # create chassis 1
UCS-A /power-cap-mgmt/power-group/chassis* # commit-buffer
UCS-A /power-cap-mgmt/power-group/chassis #
```

電源グループの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope power-cap-mgmt**	電力制限管理モードを開始します。
ステップ 2	UCS-A /power-cap-mgmt # **delete power-group** *power-group-name*	指定された電源グループを削除します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /power-cap-mgmt/power-group/chassis # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、powergroup1 という名前の電源グループを削除し、トランザクションをコミットします。

```
UCS-A# scope power-cap-mgmt
UCS-A /power-cap-mgmt # delete power-group powergroup1
UCS-A /power-cap-mgmt* # commit-buffer
UCS-A /power-cap-mgmt #
```

電力制御ポリシー

Cisco UCS は、電力制御ポリシーの優先順位設定をブレード タイプおよびコンフィギュレーションとともに使用し、シャーシ内の各ブレードへの初期電力割り当てを計算します。通常の動作中、シャーシ内のアクティブなブレードは、同じシャーシ内のアイドル ブレードから電力を借りることができます。すべてのブレードがアクティブになり電力制限に到達した場合は、優先順位が高い電力制御ポリシーを含むサービス プロファイルが、優先順位が低い電力制御ポリシーを含むサービス プロファイルよりも優先されます。

優先順位は 1 ～ 10 の段階にランク付けされており、1 が最も高い優先順位、10 が最も低い優先順位を表します。デフォルトの優先順位は 5 です。

ミッション クリティカルなアプリケーションの場合は、no-cap という特別な優先順位も使用できます。プライオリティを no-cap に設定すると、Cisco UCS がその特定のサーバから未使用の電力を利用することを防止します。この設定により、そのサーバにはサーバ タイプに応じた最大許容電力が割り当てられます。

（注） 電力制御ポリシーはサービス プロファイルに含める必要があります。また、このサービス プロファイルをイネーブルにするには、サーバに関連付ける必要があります。

電力制御ポリシーの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、org-name に / と入力します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /org # **create power-control-policy** *power-control-pol-name*	電力制御ポリシーを作成し、電力制御ポリシー モードを開始します。
ステップ 3	UCS-A /org/power-control-policy # **set priority** {*priority-num* | **no-cap**}	電力制御ポリシーにプライオリティを指定します。
ステップ 4	UCS-A /org/power-control-policy # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、powerpolicy15 という電力制御ポリシーを作成し、プライオリティをレベル 2 に設定し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # create power-control-policy powerpolicy15
UCS-A /org/power-control policy* # set priority 2
UCS-A /org/power-control policy* # commit-buffer
UCS-A /org/power-control policy #
```

次の作業

サービス プロファイルに電力制御ポリシーを含めます。

電力制御ポリシーの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、org-name に / と入力します。
ステップ 2	UCS-A /org # **delete power-control-policy** *power-control-pol-name*	指定された電力制御ポリシーを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、powerpolicy15 という名前の電力制御ポリシーを削除し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # delete power-control-policy powerpolicy15
UCS-A /org* # commit-buffer
UCS-A /org #
```

手動によるブレード レベル電力制限の設定

手動ブレード レベルの電力制限

手動によるブレード レベルの電力制限がグローバル制限ポリシーで設定されている場合は、Cisco UCS ドメイン の各ブレード サーバに対して電力制限を設定できます。

次の設定オプションを使用できます。

- [有効（Enabled）]：サーバが一度に消費可能な最大電力量を指定できます。 この最大値には、0 ～ 1100 W の任意の量を指定できます。
- [無効（Disabled）]：サーバに対して電力使用制限を課しません。サーバは、必要なだけ電力を使用できます。

サーバの電力使用量の瞬間的な上昇がそのサーバに設定された最大値以上になっても、Cisco UCS Manager によってサーバが切断またはシャットダウンされることはありません。代わりに、サーバで使用可能な量まで電力が Cisco UCS Manager によって削減されます。この削減により、サーバの速度（CPU 速度など）が低下する可能性があります。

（注） 手動によるブレード レベル電力制限は、[機器（Equipment）]>[ポリシー（Policies）]>[グローバル ポリシー（Global Policies）]>[グローバル電力制御ポリシー（Global Power Allocation Policy）] の順に設定します。電力制御ポリシーで設定された優先順位は関係ありません。

サーバのブレード レベル電力制限の設定

はじめる前に

グローバル電力割り当てポリシーが [手動によるブレード レベルの上限（Manual Blade Level Cap）] に設定されていることを確認してください。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *chassis-id/server-id*	指定サーバのシャーシ サーバ モードを開始します。
ステップ 2	UCS-A /chassis/server # **set power-budget committed** {**disabled** | *watts*}	次のいずれかの電力使用量レベルにサーバをコミットします。 • **disabled**：サーバの電力使用量を制限しません。

	コマンドまたはアクション	目的
		• *watts*：サーバの電力使用量の上限をユーザが指定できます。この設定を選択した場合は、サーバが使用できる最大ワット数を入力します。範囲は 0 ～ 10000000 W です。
ステップ 3	UCS-A /chassis/server # **commit-buffer**	トランザクションをシステム設定にコミットします。
ステップ 4	UCS-A /chassis/server # **show power-budget**	（任意）電力使用量レベル設定を表示します。

次に、サーバの電力使用量を最大1000 Wに設定し、トランザクションをコミットする例を示します。

```
UCS-A# scope server 2/4
UCS-A /chassis/server # set power-budget committed 1000
UCS-A /chassis/server* # commit-buffer
UCS-A /chassis/server # show power-budget
Power Budget:
    Committed (W): 1100
    Oper Committed (W): Disabled

UCS-A /chassis/server #
```

ブレード レベル電力制限の表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *chassis-id/server-id*	指定サーバのシャーシ サーバ モードを開始します。
ステップ 2	UCS-A /chassis/server # **show stats**	サーバで収集された電力使用量の統計情報を表示します。

次に、サーバの電力使用量を表示する例を示します。

```
UCS-A# scope server 2/4
UCS-A /chassis/server # show stats

Mb Power Stats:
    Time Collected: 2010-04-15T21:18:04.992
    Monitored Object: sys/chassis-1/blade-2/board
    Suspect: No
    Consumed Power (W): 118.285194
    Input Voltage (V): 11.948000
    Input Current (A): 9.900000
    Thresholded: Input Voltage Min
```

```
UCS-A /chassis/server #
```

第 34 章

タイム ゾーンの管理

この章の内容は、次のとおりです。

タイム ゾーン

Cisco UCS では、Cisco UCS Manager に正しい時刻を表示するために、ドメイン固有のタイムゾーンの設定と NTP サーバが必要です。これらの両方を Cisco UCS ドメインに設定しなければ、時間は正確に表示されません。

タイム ゾーンの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope services**	システム サービス モードを開始します。
ステップ 3	UCS-A /system/services # **set timezone**	この時点で、大陸、国、およびタイム ゾーン領域に対応する番号を入力するように求められます。プロンプトごとに適切な情報を入力します。

	コマンドまたはアクション	目的
		ロケーション情報の指定を完了すると、プロンプトが表示され、正しいタイム ゾーン情報が設定されているか確認するよう求められます。確認する場合は **1**（yes）を入力し、操作をキャンセルする場合は **2**（no）を入力します。
ステップ 4	UCS-A /system/services # **commit-buffer**	トランザクションをシステム設定にコミットします。
ステップ 5	UCS-A /system/services # **exit**	システム モードを開始します。
ステップ 6	UCS-A /system/services # **exit**	EXEC モードを開始します。
ステップ 7	UCS-A /system/services # **show timezone**	設定されているタイムゾーンを表示します。

次に、太平洋標準時領域にタイム ゾーンを設定し、トランザクションを確定し、設定したタイム ゾーンを表示する例を示します。

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # set timezone
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa            4) Arctic Ocean     7) Australia       10) Pacific Ocean
2) Americas          5) Asia             8) Europe
3) Antarctica        6) Atlantic Ocean   9) Indian Ocean
#? Artic ocean
Please enter a number in range.
#? 2
Please select a country.
 1) Anguilla              18) Ecuador              35) Paraguay
 2) Antigua & Barbuda     19) El Salvador          36) Peru
 3) Argentina             20) French Guiana        37) Puerto Rico
 4) Aruba                 21) Greenland            38) St Kitts & Nevis
 5) Bahamas               22) Grenada              39) St Lucia
 6) Barbados              23) Guadeloupe           40) St Pierre & Miquelon
 7) Belize                24) Guatemala            41) St Vincent
 8) Bolivia               25) Guyana               42) Suriname
 9) Brazil                26) Haiti                43) Trinidad & Tobago
10) Canada                27) Honduras             44) Turks & Caicos Is
11) Cayman Islands        28) Jamaica              45) United States
12) Chile                 29) Martinique           46) Uruguay
13) Colombia              30) Mexico               47) Venezuela
14) Costa Rica            31) Montserrat           48) Virgin Islands (UK)
15) Cuba                  32) Netherlands Antilles 49) Virgin Islands (US)
16) Dominica              33) Nicaragua
17) Dominican Republic    34) Panama
#? 45
Please select one of the following time zone regions.
 1) Eastern Time
 2) Eastern Time - Michigan - most locations
 3) Eastern Time - Kentucky - Louisville area
 4) Eastern Time - Kentucky - Wayne County
 5) Eastern Standard Time - Indiana - most locations
 6) Eastern Standard Time - Indiana - Crawford County
 7) Eastern Standard Time - Indiana - Starke County
 8) Eastern Standard Time - Indiana - Switzerland County
 9) Central Time
```

```
10) Central Time - Michigan - Wisconsin border
11) Central Time - North Dakota - Oliver County
12) Mountain Time
13) Mountain Time - south Idaho & east Oregon
14) Mountain Time - Navajo
15) Mountain Standard Time - Arizona
16) Pacific Time
17) Alaska Time
18) Alaska Time - Alaska panhandle
19) Alaska Time - Alaska panhandle neck
20) Alaska Time - west Alaska
21) Aleutian Islands
22) Hawaii
#? 16

The following information has been given:

        United States
        Pacific Time

Therefore timezone 'America/Los_Angeles' will be set.
Local time is now:      Fri May 15 07:39:25 PDT 2009.
Universal Time is now:  Fri May 15 14:39:25 UTC 2009.
Is the above information OK?
1) Yes
2) No
#? 1
UCS-A /system/services* # commit-buffer
UCS-A /system/services # exit
UCS-A /system # exit
UCS-A# show timezone
Timezone: America/Los_Angeles (Pacific Time)
UCS-A#
```

NTP サーバの追加

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope services**	システム サービス モードを開始します。
ステップ 3	UCS-A /system/services # **create ntp-server** {*hostname* | *ip-addr*|*ip6-addr*}	指定したホスト名、IPv4 または IPv6 アドレスで NTP サーバを使用するようシステムを設定します。
ステップ 4	UCS-A /system/services # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、IP アドレス 192.168.200.101 を持つ NTP サーバを設定し、トランザクションを確定する例を示します。

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # create ntp-server 192.168.200.101
```

```
UCS-A /system/services* # commit-buffer
UCS-A /system/services #
```

次の例では、IP アドレス 4001::6 を持つ NTP サーバを設定し、トランザクションをコミットします。

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # create ntp-server 4001::6
UCS-A /system/services* # commit-buffer
UCS-A /system/services #
```

NTP サーバの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope services**	システム サービス モードを開始します。
ステップ 3	UCS-A /system/services # **delete ntp-server** {*hostname* | *ip-addr*|*ip6-addr*}	指定したホスト名、IPv4 または IPv6 アドレスの NTP サーバを削除します。

次に、IP アドレス 192.168.200.101 を持つ NTP サーバを削除し、トランザクションを確定する例を示します。

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # delete ntp-server 192.168.200.101
UCS-A /system/services* # commit-buffer
UCS-A /system/services #
```

次に、IPv6 アドレス 4001::6 を持つ NTP サーバを削除し、トランザクションを確定する例を示します。

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # delete ntp-server 4001::6
UCS-A /system/services* # commit-buffer
UCS-A /system/services #
```

システム クロックの手動設定

システム クロックの変更はただちに反映されます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope services**	システム サービス モードを開始します。
ステップ 3	UCS-A /system/services # **set clock** *mon date year hour min sec*	システム クロックを設定します。

次に、システム クロックを設定し、トランザクションをコミットする例を示します。

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # set clock apr 14 2010 15 27 00
UCS-A /system/services #
```

第 35 章

シャーシの管理

この章の内容は、次のとおりです。

シャーシの削除および解放に関するガイドライン

Cisco UCS Manager を使用してシャーシを削除するか解放するかを決定する場合は、次のガイドラインを考慮してください。

シャーシの稼働中止

物理的に存在し接続されているシャーシを、一時的に Cisco UCS Manager 設定から削除する場合は、シャーシの稼働停止を実行します。解放されたシャーシは最終的に再稼働することが予測されるので、シャーシ情報部分は Cisco UCS Manager によって、将来使用するために残されています。

シャーシの削除

削除は、システムから物理的にシャーシを取り外すときに実行されます。シャーシの物理的な削除が完了すると、そのシャーシの設定は、Cisco UCS Manager で削除できます。

（注） 現在物理的に存在し接続されている場合、Cisco UCS Managerからシャーシを削除できません。

削除されたシャーシを設定に追加し直す必要がある場合は、再接続し、再検出する必要があります。再検出中、Cisco UCS Managerは以前シャーシが持っていたIDと異なる新しいIDを割り当てます。

Cisco UCS M シリーズ モジュラ サーバに関する重要な考慮事項

Cisco UCS M シリーズ モジュラ サーバでは、シャーシIDが*x*に変わると、そのサービス プロファイルの関連付けも変わります。シャーシ*x*に前に関連付けられていたサービス プロファイルが、このシャーシに関連付けられます。この結果、新しい仮想ドライブの作成が要求されることになります。既存の仮想ドライブは孤立状態になります。

このシナリオでは、空き領域の制限あるいはディスク グループの違いにより、仮想ドライブの作成が失敗する可能性があります。いずれの場合も、サービス プロファイルの関連付けを成功させるためには、孤立した仮想ドライブを削除する必要があります。

削除されたシャーシを再プロビジョニングする方法は、新しいシャーシをプロビジョニングする場合と同様です。

シャーシの確認

シャーシをファブリック インターコネクトに接続するリンクの数を増減させた場合は、次の手順を実行します。シャーシを確認することにより、Cisco UCS Managerがリンク数の変化を認識していること、および使用可能なリンクすべてでトラフィックがフローしていることを確認できます。

ファブリック インターコネクト上でサーバ ポートを作成または削除した後、1分以上待ってからシャーシを再認識させます。シャーシを再認識させるのが早すぎると、シャーシからのサーバ トラフィックのピン接続が、有効または無効にしたポートに対する変更を使用して更新されない場合があります。

手順

	コマンドまたはアクション	目的
ステップ1	UCS-A# **acknowledge chassis** *chassis-num*	指定シャーシを認識します。
ステップ2	UCS-A# **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、シャーシ2を認識し、トランザクションをコミットします。

```
UCS-A# acknowledge chassis 2
UCS-A* # commit-buffer
UCS-A #
```

シャーシの稼働中止

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **decommission chassis** *chassis-num*	指定されたシャーシを解放します。
ステップ 2	UCS-A# **commit-buffer**	トランザクションをシステム設定にコミットします。

稼働が停止するまでに数分かかる場合があります。

次の例では、シャーシ 2 を解放し、トランザクションをコミットします。

```
UCS-A# decommission chassis 2
UCS-A* # commit-buffer
UCS-A # show chassis

Chassis:
    Chassis    Overall Status           Admin State
    ---------- ---------------------- -----------
             1 Operable               Acknowledged
             2 Accessibility Problem  Decommission
UCS-A #
```

シャーシの削除

はじめる前に

次の手順を実行する前に、シャーシを物理的に取り外します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **remove chassis** *chassis-num*	指定したシャーシを削除します。
ステップ 2	UCS-A# **commit-buffer**	トランザクションをシステム設定にコミットします。

削除が完了するまでに数分かかる場合があります。

次に、シャーシ 2 を削除し、トランザクションをコミットする例を示します。

```
UCS-A# remove chassis 2
UCS-A* # commit-buffer
UCS-A #
```

シャーシの再稼働

この手順により、シャーシがコンフィギュレーションに再度追加され、このシャーシにシャーシディスカバリ ポリシーが適用されます。この手順を実行すると、シャーシおよびシャーシ内のすべてのサーバにアクセスできるようになります。

はじめる前に

show chassis decommissioned または **show chassis inventory** コマンドを使用して、稼働停止するシャーシに関する次の情報を収集します。

- ベンダー名
- Model name
- [シリアル番号（Serial number）]

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **recommission chassis** *vendor-name model-name serial-num*	指定したシャーシを再稼働します。
ステップ 2	UCS-A# **commit-buffer**	トランザクションをシステム設定にコミットします。 （注） シャーシを再稼働し、トランザクションをコミットした後すぐに **show chassis** コマンドを実行すると、シャーシの管理状態に変更が見られない場合があります。再稼働後にシャーシの状態が変更するまでに時間がかかることがあるためです。

次に、Cisco UCS 5108 シャーシを再稼働し、トランザクションをコミットする例を示します。

```
UCS-A# show chassis

Chassis:
    Chassis    Overall Status           Admin State
    ---------- ---------------------- -----------
             1 Accessibility Problem    Decommission

UCS-A# recommission chassis "Cisco Systems Inc" "N20-C6508" FOX1252GNNN
UCS-A* # commit-buffer
UCS-A #
```

シャーシの番号付け直し

（注） Cisco UCS Manager を通じたブレードサーバの番号の再設定はできません。ブレードサーバに割り当てられる ID は、シャーシ内のその物理スロットで決まります。ブレードサーバの番号を再設定するには、サーバをシャーシ内の別のスロットに物理的に移動する必要があります。

はじめる前に

シャーシ間で ID を交換する場合は、まず両方のシャーシを解放し、シャーシ解放 FSM が完了するのを待ってから、番号の再設定手順に進みます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **show chassis inventory**	シャーシに関する情報を表示します。
ステップ 2	シャーシインベントリに以下が含まれていないことを確認してください。	• 番号を付け直すシャーシ • 使用する番号を持つシャーシ これらのシャーシのいずれかがシャーシ インベントリにリストされている場合は、これらのシャーシをデコミッションします。続行前に、デコミッション FSM が完了し、シャーシがシャーシ インベントリにリストされなくなるまで待機する必要があります。これには数分かかる場合があります。 どのシャーシがデコミッションされたかを確認するには、**show chassis decommissioned** コマンドを発行します。
ステップ 3	UCS-A# **recommission chassis** *vendor-name model-name serial-num* [*chassis-num*]	指定したシャーシを再稼働し、番号を付け直します。
ステップ 4	UCS-A# **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、2 つの Cisco UCS シャーシ（シャーシ 8 とシャーシ 9）を稼働停止し、それらの ID を入れ替え、トランザクションをコミットする例を示します。

```
UCS-A# show chassis inventory

    Chassis    PID       Vendor         Serial (SN) HW Revision
    ------- --------- ---------------   ----------- -------------
          1 N20-C6508 Cisco Systems Inc FOX1252GAAA 0
```

```
          2 N20-C6508 Cisco Systems Inc FOX1252GBBB 0
          3 N20-C6508 Cisco Systems Inc FOX1252GCCC 0
          4 N20-C6508 Cisco Systems Inc FOX1252GDDD 0
          5 N20-C6508 Cisco Systems Inc FOX1252GEEE 0
          6 N20-C6508 Cisco Systems Inc FOX1252GFFF 0
          7 N20-C6508 Cisco Systems Inc FOX1252GGGG 0
          8 N20-C6508 Cisco Systems Inc FOX1252GHHH 0
          9 N20-C6508 Cisco Systems Inc FOX1252GIII 0
         10 N20-C6508 Cisco Systems Inc FOX1252GJJJ 0
         11 N20-C6508 Cisco Systems Inc FOX1252GKKK 0
         12 N20-C6508 Cisco Systems Inc FOX1252GLLL 0
         13 N20-C6508 Cisco Systems Inc FOX1252GMMM 0
         14 N20-C6508 Cisco Systems Inc FOX1252GNNN 0

UCS-A# decommission chassis 8
UCS-A*# commit-buffer
UCS-A# decommission chassis 9
UCS-A*# commit-buffer
UCS-A# show chassis inventory

    Chassis    PID       Vendor         Serial (SN) HW Revision
    ------- --------- ---------------   ----------- -------------
          1 N20-C6508 Cisco Systems Inc FOX1252GAAA 0
          2 N20-C6508 Cisco Systems Inc FOX1252GBBB 0
          3 N20-C6508 Cisco Systems Inc FOX1252GCCC 0
          4 N20-C6508 Cisco Systems Inc FOX1252GDDD 0
          5 N20-C6508 Cisco Systems Inc FOX1252GEEE 0
          6 N20-C6508 Cisco Systems Inc FOX1252GFFF 0
          7 N20-C6508 Cisco Systems Inc FOX1252GGGG 0
         10 N20-C6508 Cisco Systems Inc FOX1252GJJJ 0
         11 N20-C6508 Cisco Systems Inc FOX1252GKKK 0
         12 N20-C6508 Cisco Systems Inc FOX1252GLLL 0
         13 N20-C6508 Cisco Systems Inc FOX1252GMMM 0
         14 N20-C6508 Cisco Systems Inc FOX1252GNNN 0

UCS-A# show chassis decommissioned

    Chassis    PID       Vendor         Serial (SN) HW Revision
    ------- --------- ---------------   ----------- -------------
          8 N20-C6508 Cisco Systems Inc FOX1252GHHH 0
          9 N20-C6508 Cisco Systems Inc FOX1252GIII 0

UCS-A# recommission chassis "Cisco Systems Inc" "N20-C6508" FOX1252GHHH 9
UCS-A* # commit-buffer
UCS-A# recommission chassis "Cisco Systems Inc" "N20-C6508" FOX1252GIII 8
UCS-A* # commit-buffer
UCS-A # show chassis inventory

    Chassis    PID       Vendor         Serial (SN) HW Revision
    ------- --------- ---------------   ----------- -------------
          1 N20-C6508 Cisco Systems Inc FOX1252GAAA 0
          2 N20-C6508 Cisco Systems Inc FOX1252GBBB 0
          3 N20-C6508 Cisco Systems Inc FOX1252GCCC 0
          4 N20-C6508 Cisco Systems Inc FOX1252GDDD 0
          5 N20-C6508 Cisco Systems Inc FOX1252GEEE 0
          6 N20-C6508 Cisco Systems Inc FOX1252GFFF 0
          7 N20-C6508 Cisco Systems Inc FOX1252GGGG 0
          8 N20-C6508 Cisco Systems Inc FOX1252GIII 0
          9 N20-C6508 Cisco Systems Inc FOX1252GHHH 0
         10 N20-C6508 Cisco Systems Inc FOX1252GJJJ 0
         11 N20-C6508 Cisco Systems Inc FOX1252GKKK 0
         12 N20-C6508 Cisco Systems Inc FOX1252GLLL 0
         13 N20-C6508 Cisco Systems Inc FOX1252GMMM 0
         14 N20-C6508 Cisco Systems Inc FOX1252GNNN 0
```

ロケータ LED の切り替え

シャーシのロケータ LED の電源投入

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope chassis** *chassis-num*	指定したシャーシでシャーシ モードを開始します。
ステップ 2	UCS-A /chassis # **enable locator-led**	シャーシ ロケータ LED の電源を投入します。
ステップ 3	UCS-A /chassis # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、シャーシ 2 のロケータ LED の電源を投入し、トランザクションをコミットする例を示します。

```
UCS-A# scope chassis 2
UCS-A /chassis # enable locator-led
UCS-A /chassis* # commit-buffer
UCS-A /chassis #
```

シャーシのロケータ LED の電源切断

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope chassis** *chassis-num*	指定したシャーシでシャーシ モードを開始します。
ステップ 2	UCS-A /chassis # **disable locator-led**	シャーシ ロケータ LED の電源を切断します。
ステップ 3	UCS-A /chassis # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、シャーシ 2 のロケータ LED の電源を切断し、トランザクションをコミットする例を示します。

```
UCS-A# scope chassis 2
UCS-A /chassis # disable locator-led
UCS-A /chassis* # commit-buffer
UCS-A /chassis #
```

第 36 章

ブレード サーバの管理

この章の内容は、次のとおりです。

ブレード サーバ管理

Cisco UCS Manager 経由で Cisco UCS ドメイン 内のすべてのブレード サーバを管理およびモニタできます。電源状態の変更など一部のブレードサーバ管理タスクは、サーバおよびサービスプロファイルから実行できます。

残りの管理タスクは、サーバ上でだけ実行できます。

シャーシ内のブレードサーバスロットが空の場合、そのスロットに関する情報、エラー、および障害が Cisco UCS Manager から提供されます。サーバ ミスマッチ エラーを解決し、そのスロット内のブレード サーバを Cisco UCS Manager で再検出するために、スロットを再認識させることもできます。

Cisco UCS B460 M4 ブレード サーバ管理

Cisco UCS B460 M4 ブレード サーバは、Cisco UCS 拡張コネクタで接続された 2 台の Cisco UCS B260 最大幅ブレード サーバから構成されています。各ブレード サーバはノードと呼ばれ、マスター ノードまたはスレーブ ノードになることができます。

各 Cisco UCS B460 M4 ブレード サーバには 2 つの異なるノードが存在するため、以下について注意する必要があります。

- マスター ノードは常に、最も大きな番号が付いたスロットのノードです。
- Cisco UCS B460 ブレード サーバが Cisco UCS Manager で参照される際は、マスターのスロット番号が参照されます。
- Cisco UCS B460 M4 ブレード サーバから Cisco UCS 拡張コネクタを取り外すと、Cisco UCS Manager GUI の [物理ディスプレイ（Physical Display）] 領域には、両方のマスター ノード スロットと両方のスレーブ ノード スロットで [解決が必要（Needs Resolution）] が表示されます。
- ヘルス LED には、マスター ノードとスレーブ ノードの個々の状態、および両方のノードを組み合せた状態が表示されます。複合ヘルス LED には常に、最も状態が悪いノードのステータスが表示されます。ヘルス LED アラームは個別に表示されます。
- Cisco UCS Manager GUI では、マスターまたはスレーブ ノードのロケータ LED のオン/オフを切り替えることができます。Cisco UCS Manager CLI では、ロケータ LED のオン/オフを個々に切り替えるか、両方のロケータ LED のオン/オフを同時に切り替えることができます。
- Cisco UCS B460 M4 ブレード サーバに対する電力制限は、サーバ レベルで適用されます。各ノードの制限値は合計値の半分です。
- ファームウェアを更新すると、マスターとスレーブ ノードの両方が同時に更新されます。個々のノードでファームウェアを更新することはできません。
- ローカル ディスクの設定は、マスター ノードでのみサポートされます。
- Cisco UCS B460 ブレード サーバは、マスターまたはスレーブ ノードによって生成された SEL ログを区別しません。ログは同じページに表示され、スロット番号で区別されます。

- Cisco UCS Manager GUI では、[ストレージ（Storage）] タブの [ローカル ディスクの設定ポリシー（Local Disk Configuration Policy）] と [実際のディスク設定（Actual Disk Configurations）] 領域に、Cisco UCS B460 ブレード サーバのマスター ノードのデータだけが表示されます。スレーブ ノード用のフィールドは表示されません。

Cisco UCS B460 M4 ブレード サーバへのアップグレード

Cisco UCS B260 M4 ブレード サーバがある場合、アップグレード キットを購入して Cisco UCS B460 M4 ブレード サーバに変換することができます。詳細については、該当の『*Cisco UCS Hardware Installation Guide*』を参照してください。

はじめる前に

2 台の Cisco UCS B260 M4 ブレード サーバと Cisco UCS スケーラビリティ コネクタが必要です。

手順

ステップ 1 既存の Cisco UCS B260 M4 ブレード サーバがサービス プロファイルに関連付けられていないことを確認します。

ステップ 2 1 台目のブレード サーバの上か下のシャーシに 2 台目の Cisco UCS B260 M4 ブレード サーバを挿入します。

（注） 2 台目のブレード サーバに Cisco UCS スケーラビリティ ターミネータが付いていない場合は、1 台目のブレード サーバのターミネータを使用します。

ステップ 3 両方の Cisco UCS B260 M4 ブレード サーバを停止させます。

ステップ 4 ファームウェアを同期します。
自動的に新しいサーバを更新するには、Cisco UCS Manager の [ファームウェア自動同期サーバ（Firmware Auto Sync Server）] ポリシーを使用します。詳細については、該当する『*Cisco UCS B-Series Firmware Management Guide*』を参照してください。

ステップ 5 Cisco UCS スケーラビリティ ターミネータを Cisco UCS スケーラビリティ コネクタに置き換えます。
スロットのプレゼンスはミスマッチに変わりますが、検出はトリガーされません。

ステップ 6 新しい Cisco UCS B460 M4 ブレード サーバを再認識します。

ブレードサーバの削除および解放に関するガイドライン

Cisco UCS Manager を使用してブレード サーバを削除するか解放するかを決定する場合は、次のガイドラインを考慮してください。

ブレード サーバの解放

解放は、ブレード サーバが物理的に存在し接続しているときに、一時的に設定から削除する場合に実行します。解放されたブレード サーバは最終的に再稼働することが予測されるので、サーバの情報部分は、将来の使用に備え、Cisco UCS Manager によって保持されます。

ブレード サーバの取り外し

削除は、ブレード サーバをシャーシから接続解除して、Cisco UCS Manager から物理的に削除する（取り外す）場合に実行します。ブレード サーバが物理的に存在し、シャーシに接続しているときは、Cisco UCS Manager から削除できません。ブレード サーバの物理的な削除が完了すると、そのブレード サーバの設定を Cisco UCS Manager で削除できます。

削除時、そのブレード サーバへのアクティブ リンクは無効化され、すべてのエントリがデータベースから削除されます。サーバは検出時に割り当てられたすべてのサーバ プールから自動的に削除されます。

（注） 自動的に削除されるのは、ディスカバリ中に自動的にサーバ プールへ追加されたサーバだけです。サーバ プールに手動で追加したサーバは手動で削除する必要があります。

削除したブレード サーバを再び設定に追加するには、それを再び接続して検出する必要があります。Cisco UCS Manager に再導入したサーバは、新しいサーバとして処理され、詳細なディスカバリ プロセスが実施されます。このため、Cisco UCS Manager によって、以前とは異なる新しい ID がサーバに割り当てられることがあります。

予期しないサーバ電力変更を回避するための推奨事項

サーバがサービス プロファイルに関連付けられていない場合は、サーバの物理的な [電源（Power）] または [リセット（Reset）] ボタンなど、サーバの電源状態を変更するために使用可能な手段をすべて使用できます。

サーバがサービス プロファイルに関連付けられているか、サービス プロファイルに割り当てられている場合は、サーバの電源状態の変更は次の方法でのみ行う必要があります。

- Cisco UCS Manager GUI で、サーバまたはサーバに関連付けられたサービス プロファイルの [全般（General）] タブに移動し、[アクション（Actions）] 領域で [ブート サーバ（Boot Server）] または [シャットダウン サーバ（Shutdown Server）] を選択します。
- Cisco UCS Manager CLI で、サーバまたはサーバに関連付けられたサービス プロファイルを調べ、**power up** または **power down** コマンドを使用します。

重要 電源がオフになっている関連サーバには、次のオプションのいずれも使用しないでください。

- GUI の [リセット（Reset）]
- **cycle cycle-immediate** または CLI の **reset hard-reset-immediate**
- サーバの物理的な [電源（Power）] または [リセット（Reset）] ボタン

現在電源がオフになっているサーバに対して、リセットまたはサイクルを実施するか、サーバの物理的な電源ボタンを使用すると、サーバの実際の電力状態がサービス プロファイルで必要とされる電源状態の設定と同期しなくなる可能性があります。サーバと Cisco UCS Manager 間の通信が中断したり、サービス プロファイルの設定が変更されると、Cisco UCS Manager によって、必要とされる電源の状態がサービス プロファイルからサーバに適用される場合があり、この結果予期しない電力変化が発生する可能性があります。

電源の同期に関する問題は、次に示すように予期しないサーバの再起動につながる可能性があります。

サービス プロファイルで必要とされる電源状態	現在のサーバの電源状態	通信が中断された後のサーバの電源状態
アップ	電源オフ	電源オン
ダウン	電源オン	電源オン （注） 実行中のサーバは、サービス プロファイルに必要とされる電源状態に関係なくシャットダウンされません。

ブレード サーバのブート

はじめる前に

ブレード サーバまたはサーバ プールにサービス プロファイルを関連付けます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	指定したサービス プロファイルで組織サービス プロファイル モードを開始します。
ステップ 3	UCS-A /org/service-profile # **power up**	サービスプロファイルに関連付けられたブレード サーバをブートします。
ステップ 4	UCS-A /org/service-profile # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、ServProf34 という名前のサービス プロファイルに関連付けられたブレード サーバをブートし、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org* # scope service-profile ServProf34
UCS-A /org/service-profile* # power up
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile #
```

ブレード サーバのシャットダウン

この手順を使用して、インストールされているオペレーティング システムによりサーバをシャットダウンする場合、Cisco UCS Manager により、この OS のグレースフル シャットダウン シーケンスがトリガーされます。

はじめる前に

ブレード サーバまたはサーバ プールにサービス プロファイルを関連付けます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / と入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	指定したサービス プロファイルで組織サービス プロファイル モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /org/service-profile # **power down**	サービス プロファイルに関連付けられたブレード サーバをシャットダウンします。
ステップ 4	UCS-A /org/service-profile # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、ServProf34 という名前のサービス プロファイルに関連付けられたブレード サーバをシャットダウンし、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # scope service-profile ServProf34
UCS-A /org/service-profile # power down
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile #
```

ブレード サーバの電源再投入

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *chassis-num/ server-num*	指定したブレード サーバでシャーシ サーバ モードを開始します。
ステップ 2	UCS-A /chassis/server # **cycle** {**cycle-immediate** | **cycle-wait**}	ブレード サーバの電源を再投入します。 ブレード サーバの電源再投入をただちに開始するには、**cycle-immediate** キーワードを使用します。保留中のすべての管理操作が完了した後に電源再投入が開始されるようスケジュールするには、**cycle-wait** キーワードを使用します。
ステップ 3	UCS-A# **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、シャーシ 2 のブレード サーバ 4 の電源をただちに再投入し、トランザクションをコミットする例を示します。

```
UCS-A#  scope server 2/4
UCS-A /chassis/server # cycle cycle-immediate
UCS-A /chassis/server* # commit-buffer
UCS-A /chassis/server #
```

ブレード サーバのハード リセットの実行

サーバをリセットすると、Cisco UCS Manager により、リセット ライン上にパルスが送信されます。オペレーティング システムのグレースフル シャットダウンを選択することができます。オペレーティング システムでグレースフル シャットダウンがサポートされていない場合、サーバ電源の再投入が行われます。サーバのリセット前にすべての管理操作を完了させるオプションを Cisco UCS Manager に適用した場合、それらの管理操作がサーバのリセット前に完了するかどうかは保証されていません。

（注） 電源切断状態からサーバをブートする場合は、[リセット（Reset）] を使用しないでください。

このプロセスで電源投入を続行すると、サーバの望ましい電源状態が実際の電源状態と同期しなくなり、サーバが後で予期せずシャットダウンすることがあります。選択したサーバを電源切断状態から安全にリブートするには、[キャンセル（Cancel）] をクリックし、[サーバの起動（Boot Server）] アクションを選択します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *chassis-num/ server-num*	指定サーバのシャーシ サーバ モードを開始します。
ステップ 2	UCS-A /chassis/server # **reset** {**hard-reset-immediate** | **hard-reset-wait**}	ブレードサーバのハードリセットを実行します。 サーバのハード リセットをただちに開始するには、**hard-reset-immediate** キーワードを使用します。保留中のすべての管理操作が完了した後にハード リセットが開始されるようスケジュールするには、**hard-reset-wait** キーワードを使用します。
ステップ 3	UCS-A /server # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、シャーシ 2 のブレード サーバ 4 のハード リセットをただちに実行し、トランザクションをコミットする例を示します。

```
UCS-A#  scope server 2/4
UCS-A /chassis/server # reset hard-reset-immediate
UCS-A /chassis/server* # commit-buffer
UCS-A /chassis/server #
```

ブレード サーバの認識

サーバ、およびそのサーバのエンドポイントすべてを再検出させるには、次の手順を実行します。たとえば、サーバがディスカバリ状態など、予期していなかった状態から抜け出せなくなっている場合に、この手順を使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **acknowledge server** *chassis-num/ server-num*	指定されたブレード サーバを認識します。
ステップ 2	UCS-A# **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、シャーシ 2 のサーバ 4 を認識し、トランザクションをコミットします。

```
UCS-A#  acknowledge server 2/4
UCS-A* # commit-buffer
UCS-A #
```

シャーシからのブレード サーバの削除

はじめる前に

次の手順を実行する前に、サーバをシャーシから物理的に取り外します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **remove server** *chassis-num/ server-num*	指定したブレードサーバを削除します。
ステップ 2	UCS-A# **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、シャーシ 2 のブレード サーバ 4 を削除し、トランザクションをコミットする例を示します。

```
UCS-A#  remove server 2/4
UCS-A* # commit-buffer
UCS-A #
```

次の作業

ブレード サーバを物理的に再設置する場合は、スロットを再認識して、Cisco UCS Manager にこのサーバを再検出させる必要があります。

詳細については、ブレード サーバの認識, （737 ページ） を参照してください。

ブレード サーバの解放

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **decommission server** *chassis-num/ server-num*	指定されたブレード サーバを解放します。
ステップ 2	UCS-A# **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、シャーシ 2 のブレード サーバ 4 を解放し、トランザクションをコミットします。

```
UCS-A# decommission server 2/4
UCS-A* # commit-buffer
UCS-A #
```

ブレード サーバのロケータ LED の電源投入

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *chassis-num/ server-num*	指定したシャーシでシャーシ サーバ モードを開始します。
ステップ 2	UCS-A /chassis/server # **enable locator-led** [**multi-master** | **multi-slave**]	ブレード サーバのロケータ LED の電源を投入します。Cisco UCS B460 M4 ブレード サーバの場合は、次のキーワードを追加できます。 • **multi-master**：マスター ノードのみに対して LED を点灯します。 • **multi-slave**：スレーブ ノードのみに対して LED を点灯します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /chassis/server # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、シャーシ 2 でブレード サーバ 4 のロケータ LED 電源を投入し、トランザクションをコミットする例を示します。

```
UCS-A# scope server 2/4
UCS-A /chassis/server # enable  locator-led
UCS-A /chassis/server* # commit-buffer
UCS-A /chassis/server #
```

次に、シャーシ 2 でブレード サーバ 7 のロケータ LED 電源を投入し、トランザクションをコミットする例を示します。

```
UCS-A# scope chassis 2/7
UCS-A /chassis/server # enable locator-led multi-master
UCS-A /chassis/server* # commit-buffer
UCS-A /chassis/server #
```

ブレード サーバのロケータ LED の電源切断

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *chassis-num/ server-num*	指定したシャーシでシャーシ モードを開始します。
ステップ 2	UCS-A /chassis/server # **disable locator-led** [**multi-master** | **multi-slave**]	ブレード サーバのロケータ LED の電源を切断します。Cisco UCS B460 M4 ブレード サーバの場合は、次のキーワードを追加できます。 • **multi-master**：マスター ノードのみに対して LED を消灯します。 • **multi-slave**：スレーブ ノードのみに対して LED を消灯します。
ステップ 3	UCS-A /chassis/server # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、シャーシ 2 のブレード サーバ 4 のロケータ LED の電源を切断し、トランザクションをコミットする例を示します。

```
UCS-A# scope chassis 2/4
UCS-A /chassis/server # disable locator-led
```

```
UCS-A /chassis/server* # commit-buffer
UCS-A /chassis/server #
```

次に、シャーシ 2 のブレード サーバ 7 のロケータ LED の電源を切断し、トランザクションをコミットする例を示します。

```
UCS-A# scope chassis 2/7
UCS-A /chassis/server # disable locator-led multi-master
UCS-A /chassis/server* # commit-buffer
UCS-A /chassis/server #
```

ブレード サーバの CMOS のリセット

サーバのトラブルシューティング時に、CMOS のリセットが必要になる場合もあります。CMOS のリセットは、通常のサーバ メンテナンスには含まれません。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *chassis-num/server-num*	指定したシャーシでシャーシ サーバ モードを開始します。
ステップ 2	UCS-A /chassis/server # **reset-cmos**	ブレード サーバの CMOS をリセットします。
ステップ 3	UCS-A /chassis/server # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、シャーシ 2 のブレード サーバ 4 の CMOS をリセットし、トランザクションをコミットする例を示します。

```
UCS-A# scope server 2/4
UCS-A /chassis/server # reset-cmos
UCS-A /chassis/server* # commit-buffer
UCS-A /chassis/server #
```

ブレード サーバの CIMC のリセット

ファームウェアでのサーバのトラブルシューティング時に、CIMC のリセットが必要になる場合もあります。CIMC のリセットは、通常のサーバ メンテナンスには含まれません。CIMC のリセット後、サーバは、そのサーバで実行されているバージョンのファームウェアを使ってブートされます。

CIMC をリセットすると、CIMC がリブートするまで、Cisco UCS の電力モニタリング機能が短時間使用不能になります。通常、リセットには20秒しかかかりませんが、その間にピーク電力制限を超える可能性があります。低電力制限が設定された環境で、設定された電力制限を超えないようにするには、CIMC のリブートまたはアクティブ化を交互に実施することを検討してください。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *chassis-num*/*server-num*	指定したシャーシでシャーシ サーバ モードを開始します。
ステップ 2	UCS-A /chassis/server # **scope CIMC**	シャーシ サーバ CIMC モードを開始します。
ステップ 3	UCS-A /chassis/server/CIMC # **reset**	ブレード サーバの CIMC をリセットします。
ステップ 4	UCS-A /chassis/server/CIMC # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、シャーシ 2 のブレード サーバ 4 の CIMC をリセットし、トランザクションをコミットする例を示します。

```
UCS-A# scope server 2/4
UCS-A /chassis/server # scope CIMC
UCS-A /chassis/server/cimc # reset
UCS-A /chassis/server/cimc* # commit-buffer
UCS-A /chassis/server/cimc #
```

ブレード サーバの TPM のクリア

TPM のサポートが含まれている Cisco UCS M4 ブレード サーバおよびラックマウント サーバでのみ、TPM をクリアできます。

注意 TPM のクリアは危険性のある操作です。OS が起動を停止することがあります。また、データを損失する可能性もあります。

はじめる前に

TPM が有効である必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** [*chassis-num*/*server-num* | *dynamic-uuid*]	指定したサーバのサーバ モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A# /chassis/server # **scope tpm** *tpm-ID*	指定された TPM の組織 TPM モードを開始します。
ステップ 3	UCS-A# /chassis/server/tpm # **set adminaction clear-config**	TPM のクリアを指定します。
ステップ 4	UCS-A# /chassis/server/tpm # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、ブレード サーバの TPM をクリアする方法の例を示します。

```
UCS-A# scope server 1/3
UCS-A# /chassis/server # scope tpm 1
UCS-A# /chassis/server/tpm # set adminaction clear-config
UCS-A#/chassis/server/tpm* # commit-buffer
```

ブレード サーバの破損した BIOS の復旧

非常に珍しいケースですが、ブレード サーバの問題により、破損した BIOS の復旧が必要になることがあります。この手順は、通常のサーバ メンテナンスには含まれません。BIOS の復旧後、ブレード サーバは、そのサーバで実行されているバージョンのファームウェアを使用してブートします。

はじめる前に

重要 サーバ上で破損している BIOS の復旧を試行する前に、そのサーバに接続またはマップされている USB ストレージをすべて取り外します。外部 USB ドライブが vMedia からサーバに取り付けられた、またはマップされている場合、BIOS の回復に失敗します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *chassis-id/server-id*	指定したシャーシ内の指定したブレード サーバでシャーシ サーバ モードを開始します。
ステップ 2	UCS-A /chassis/server # **recover-bios** *version*	指定した BIOS バージョンをロードし、アクティブにします。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /chassis/server # **commit-buffer**	トランザクションをコミットします。

次に、BIOS を復旧する例を示します。

```
UCS-A# scope server 1/7
UCS-A /chassis/server # recover-bios S5500.0044.0.3.1.010620101125
UCS-A /chassis/server* # commit-buffer
UCS-A /chassis/server #
```

ブレード サーバからの NMI の発行

システムが応答しないままになっており、Cisco UCS Manager で、CIMC から Non Maskable Interrupt（NMI）を BIOS またはオペレーティング システムに発行する必要がある場合は、次の手順を実行します。このアクションにより、サーバにインストールされているオペレーティング システム応じて、コア ダンプまたはスタック トレースが作成されます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** [*chassis-num*/*server-num* | *dynamic-uuid*]	指定したサーバのサーバ モードを開始します。
ステップ 2	UCS-A /chassis/server # **diagnostic-interrupt**	
ステップ 3	UCS-A /chassis/server* # **commit-buffer**	保留中のすべてのトランザクションをコミットします。

次に、シャーシ 2 のサーバ 4 から NMI を送信し、トランザクションをコミットする例を示します。

```
UCS-A# scope server 2/4
UCS-A /chassis/server # diagnostic-interrupt
UCS-A /chassis/server* # commit-buffer
UCS-A /chassis/server #
```

ヘルス LED アラーム

ブレード ヘルス LED は、各 Cisco UCS B シリーズ ブレード サーバの前面にあります。Cisco UCS Manager では、センサー故障が発生すると、ブレード ヘルス LED が緑色からオレンジ色またはオレンジ色の点滅に変化します。

ヘルス LED アラームには次の情報が表示されます。

名前	説明
[重大度（Severity）] カラム	アラームの重大度。次のいずれかになります。 • [クリティカル（Critical）] : ブレードヘルス LED がオレンジで点滅します。 • [マイナー（Minor）] : ブレード ヘルス LED がオレンジに点灯します。
[説明（Description）] カラム	アラームの簡単な説明。
[センサー ID（Sensor ID）] カラム	アラームをトリガーしたセンサーの ID。
[センサー名（Sensor Name）] カラム	アラームをトリガーしたセンサーの名前。

ヘルス LED ステータスの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *chassis-id/blade-id*	指定サーバのシャーシ サーバ モードを開始します。
ステップ 2	UCS-A /chassis/server # **show health-led expand**	選択したサーバのヘルス LED およびセンサー アラームを表示します。

次の例では、シャーシ 1 サーバ 1 のヘルス LED ステータスとセンサー アラームを表示する方法を示します。

```
UCS-A# scope server 1/1
UCS-A /chassis/server # show health-led
Health LED:
    Severity: Minor
    Reason:: P0V75_STBY:Voltage Threshold Crossed;TEMP_SENS_FRONT:Temperature Threshold
Crossed;
    Color: Amber
    Oper State:: On

    Sensor Alarm:
        Severity: Minor
        Sensor ID: 7
        Sensor Name: P0V75_STBY
        Alarm Desc: Voltage Threshold Crossed

        Severity: Minor
```

```
        Sensor ID: 76
        Sensor Name: TEMP_SENS_FRONT
        Alarm Desc: Temperature Threshold Crossed

        Severity: Minor
        Sensor ID: 91
        Sensor Name: DDR3_P1_D2_TMP
        Alarm Desc: Temperature Threshold Crossed

UCS-A /chassis/server #
```

第 37 章

ラックマウント サーバの管理

この章の内容は、次のとおりです。

ラックマウント サーバ管理

Cisco UCS Manager を使用して、Cisco UCS ドメイン に統合されているすべてのラックマウント サーバを管理およびモニタすることができます。電力制限を除くすべての管理およびモニタリング機能がラックマウント サーバでサポートされます。電源状態の変更など一部のラックマウント サーバ管理タスクは、サーバとサービス プロファイルの両方から行うことができます。残りの管理タスクは、サーバ上でだけ実行できます。

Cisco UCS Manager は、検出された各ラックマウント サーバに関する情報、エラー、および障害を提供します。

ヒント　サポート対象の Cisco UCS ラックマウント サーバを Cisco UCS Manager に統合する方法については、使用している Cisco UCS Manager のリリースに応じた Cisco UCS C シリーズ サーバの統合ガイドを参照してください。

ラックマウントサーバの削除および解放に関するガイドライン

Cisco UCS Manager を使用してラックマウント サーバを削除するか解放するかを決定する場合は、次のガイドラインを考慮してください。

ラックマウント サーバの解放

解放は、ラックマウント サーバが物理的に存在し接続しているときに、一時的に設定から削除する場合に実行します。解放されたラックマウント サーバは最終的に再稼働することが予測されるので、サーバの情報部分は、将来の使用に備え、Cisco UCS Manager によって保持されます。

ラックマウント サーバの削除

削除は、ラックマウントサーバをファブリック エクステンダから接続解除して、システムから物理的に削除する（取り外す）場合に実行します。ラックマウント サーバが物理的に存在し、ファブリック エクステンダに接続しているときは、Cisco UCS Manager から削除できません。ラックマウント サーバの接続を解除した後、そのラックマウント サーバの設定を Cisco UCS Manager から削除できます。

削除時、管理インターフェイスは接続解除され、すべてのエントリがデータベースから削除されます。サーバは検出時に割り当てられたすべてのサーバ プールから自動的に削除されます。

（注）　自動的に削除されるのは、検出時に自動的にサーバプールに追加されたサーバだけです。サーバ プールに手動で追加したサーバは手動で削除する必要があります。

削除したラックマウント サーバを再び設定に追加する場合は、それを再び接続して検出する必要があります。Cisco UCS Manager に再導入したサーバは、新しいサーバのように処理され、詳細なディスカバリ プロセスが実施されます。このため、Cisco UCS Manager によって、以前とは異なる新しい ID がサーバに割り当てられることがあります。

予期しないサーバ電力変更を回避するための推奨事項

サーバがサービス プロファイルに関連付けられていない場合は、サーバの物理的な [電源（Power）] または [リセット（Reset）] ボタンなど、サーバの電源状態を変更するために使用可能な手段をすべて使用できます。

サーバがサービス プロファイルに関連付けられているか、サービス プロファイルに割り当てられている場合は、サーバの電源状態の変更は次の方法でのみ行う必要があります。

- Cisco UCS Manager GUI で、サーバまたはサーバに関連付けられたサービス プロファイルの [全般（General）] タブに移動し、[アクション（Actions）] 領域で [ブート サーバ（Boot Server）] または [シャットダウン サーバ（Shutdown Server）] を選択します。
- Cisco UCS Manager CLI で、サーバまたはサーバに関連付けられたサービス プロファイルを調べ、**power up** または **power down** コマンドを使用します。

重要 電源がオフになっている関連サーバには、次のオプションのいずれも使用しないでください。

- GUI の [リセット（Reset）]
- **cycle cycle-immediate** または CLI の **reset hard-reset-immediate**
- サーバの物理的な [電源（Power）] または [リセット（Reset）] ボタン

現在電源がオフになっているサーバに対して、リセットまたはサイクルを実施するか、サーバの物理的な電源ボタンを使用すると、サーバの実際の電力状態がサービス プロファイルで必要とされる電源状態の設定と同期しなくなる可能性があります。サーバと Cisco UCS Manager 間の通信が中断したり、サービス プロファイルの設定が変更されると、Cisco UCS Manager によって、必要とされる電源の状態がサービス プロファイルからサーバに適用される場合があり、この結果予期しない電力変化が発生する可能性があります。

電源の同期に関する問題は、次に示すように予期しないサーバの再起動につながる可能性があります。

サービス プロファイルで必要とされる電源状態	現在のサーバの電源状態	通信が中断された後のサーバの電源状態
アップ	電源オフ	電源オン

サービス プロファイルで必要とされる電源状態	現在のサーバの電源状態	通信が中断された後のサーバの電源状態
ダウン	電源オン	電源オン （注） 実行中のサーバは、サービス プロファイルに必要とされる電源状態に関係なくシャットダウンされません。

ラックマウント サーバのブート

はじめる前に

ラックマウント サーバとサービス プロファイルを関連付けます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に / を入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	指定したサービス プロファイルで組織サービス プロファイル モードを開始します。
ステップ 3	UCS-A /org/service-profile # **power up**	サービス プロファイルに関連付けられたラックマウント サーバをブートします。
ステップ 4	UCS-A /org/service-profile # **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例は、ServProf34 という名前のサービス プロファイルに関連付けられたラックマウント サーバをブートし、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org* # scope service-profile ServProf34
UCS-A /org/service-profile # power up
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile #
```

ラックマウント サーバのシャットダウン

この手順を使用して、インストールされているオペレーティング システムによりサーバをシャットダウンする場合、Cisco UCS Manager により、この OS のグレースフル シャットダウン シーケンスがトリガーされます。

はじめる前に

ラックマウント サーバとサービス プロファイルを関連付けます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* に **/** と入力します。
ステップ 2	UCS-A /org # **scope service-profile** *profile-name*	指定したサービス プロファイルで組織サービス プロファイル モードを開始します。
ステップ 3	UCS-A /org/service-profile # **power down**	サービス プロファイルに関連付けられたラックマウント サーバをシャットダウンします。
ステップ 4	UCS-A /org/service-profile # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、ServProf34 という名前のサービス プロファイルに関連付けられたラックマウント サーバをシャットダウンし、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # scope service-profile ServProf34
UCS-A /org/service-profile # power down
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile #
```

ラックマウント サーバの電源再投入

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *server-num*	指定したラックマウント サーバでサーバ モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /server # **cycle** {**cycle-immediate** | **cycle-wait**}	ラックマウント サーバの電源を再投入します。 ラックマウント サーバの電源再投入をただちに開始するには、**cycle-immediate** キーワードを使用します。保留中のすべての管理操作が完了した後に電源再投入が開始されるようスケジュールするには、**cycle-wait** キーワードを使用します。
ステップ 3	UCS-A# **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、ラックマウント サーバ 2 の電源をただちに再投入し、トランザクションをコミットする例を示します。

```
UCS-A#  scope server 2
UCS-A /server # cycle cycle-immediate
UCS-A /server* # commit-buffer
UCS-A /server #
```

ラックマウント サーバのハード リセットの実行

サーバをリセットすると、Cisco UCS Manager により、リセット ライン上にパルスが送信されます。オペレーティング システムのグレースフル シャットダウンを選択することができます。オペレーティング システムでグレースフル シャットダウンがサポートされていない場合、サーバ電源の再投入が行われます。サーバのリセット前にすべての管理操作を完了させるオプションを Cisco UCS Manager に適用した場合、それらの管理操作がサーバのリセット前に完了するかどうかは保証されていません。

（注） 電源切断状態からサーバをブートする場合は、[リセット（Reset）] を使用しないでください。

このプロセスで電源投入を続行すると、サーバの望ましい電源状態が実際の電源状態と同期しなくなり、サーバが後で予期せずシャットダウンすることがあります。選択したサーバを電源切断状態から安全にリブートするには、[キャンセル（Cancel）] をクリックし、[サーバの起動（Boot Server）] アクションを選択します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *server-num*	指定したラックマウント サーバでサーバ モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /server # **reset** {**hard-reset-immediate** | **hard-reset-wait**}	ラックマウント サーバのハードリセットを実行します。 ラックマウント サーバのハードリセットをただちに開始するには、**hard-reset-immediate** キーワードを使用します。保留中のすべての管理操作が完了した後にハードリセットが開始されるようスケジュールするには、**hard-reset-wait** キーワードを使用します。
ステップ 3	UCS-A /server # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、ラックマウント サーバ 2 のハードリセットをただちに実行し、トランザクションをコミットする例を示します。

```
UCS-A#  scope server 2
UCS-A /server # reset hard-reset-immediate
UCS-A /server* # commit-buffer
UCS-A /server #
```

ラックマウント サーバの認識

サーバ、およびそのサーバのエンドポイントすべてを再検出させるには、次の手順を実行します。たとえば、サーバがディスカバリ状態など、予期していなかった状態から抜け出せなくなっている場合に、この手順を使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **acknowledge server** *server-num*	指定されたラックマウント サーバを認識します。
ステップ 2	UCS-A# **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、ラックマウント サーバ 2 を認識し、トランザクションをコミットします。

```
UCS-A#  acknowledge server 2
UCS-A* # commit-buffer
UCS-A #
```

ラックマウント サーバの解放

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **decommission server** *server-num*	指定されたラックマウント サーバを解放します。
ステップ 2	UCS-A# **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、ラックマウント サーバ 2 を解放し、トランザクションをコミットします。

```
UCS-A# decommission server 2
UCS-A* # commit-buffer
UCS-A #
```

ラックマウント サーバの番号付け直し

はじめる前に

サーバ間で ID を交換する場合は、まず両方のサーバを解放し、サーバ解放 FSM が完了するのを待ってから、番号の再設定手順に進みます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **show server inventory**	サーバに関する情報を表示します。
ステップ 2	サーバ インベントリに以下が含まれていないことを確認してください。	• 番号を付け直すラックマウント サーバ • 使用する番号を持つラックマウント サーバ これらのラックマウント サーバのいずれかがサーバ インベントリにリストされている場合は、これらのサーバをデコミッションします。続行前に、デコミッション FSM が完了し、ラックマウント サーバがサーバ インベントリにリストされなくなるまで待機する必要があります。これには数分かかる場合があります。

	コマンドまたはアクション	目的
		どのサーバがデコミッションされたかを確認するには、**show server decommissioned** コマンドを発行します。
ステップ 3	UCS-A# **recommission server** *vendor-name model-name serial-numnew-id*	指定したラックマウントサーバをリコミッションし、番号を付け直します。
ステップ 4	UCS-A# **commit-buffer**	トランザクションをシステム設定にコミットします。

次の例では、ID 2 のラックマウント サーバをデコミッションし、ID を 3 に変更し、そのサーバをリコミッションし、トランザクションをコミットします。

```
UCS-A# show server inventory

Server  Equipped PID Equipped VID Equipped Serial (SN) Slot Status      Ackd Memory (MB)
Ackd Cores
------- ------------ ------------ -------------------- ---------------- ----------------
----------
1/1     UCSB-B200-M3 V01          FCH1532718P          Equipped         131072
16
1/2     UCSB-B200-M3 V01          FCH153271DF          Equipped         131072
16
1/3     UCSB-B200-M3 V01          FCH153271DL          Equipped         114688
16
1/4     UCSB-B200-M3 V01                               Empty
1/5                                                    Empty
1/6                                                    Empty
1/7     N20-B6730-1  V01          JAF1432CFDH          Equipped         65536
16
1/8                                                    Empty
1       R200-1120402W V01          QCI1414A02J          N/A              49152
12
2       R210-2121605W V01          QCI1442AHFX          N/A              24576            8
4       UCSC-BSE-SFF-C200 V01      QCI1514A0J7          N/A              8192             8

UCS-A# decommission server 2
UCS-A*# commit-buffer
UCS-A# show server decommissioned

Vendor            Model         Serial (SN) Server
----------------- ----------    ----------- ------
Cisco Systems Inc R210-2121605W QCI1442AHFX 2

UCS-A# recommission chassis "Cisco Systems Inc" "R210-2121605W" QCI1442AHFX 3
UCS-A* # commit-buffer
UCS-A # show server inventory

Server  Equipped PID Equipped VID Equipped Serial (SN) Slot Status      Ackd Memory (MB)
Ackd Cores
------- ------------ ------------ -------------------- ---------------- ----------------
----------
1/1     UCSB-B200-M3 V01          FCH1532718P          Equipped         131072
16
1/2     UCSB-B200-M3 V01          FCH153271DF          Equipped         131072
16
1/3     UCSB-B200-M3 V01          FCH153271DL          Equipped         114688
16
1/4     UCSB-B200-M3 V01                               Empty
1/5                                                    Empty
1/6                                                    Empty
1/7     N20-B6730-1  V01          JAF1432CFDH          Equipped         65536
```

```
16
1/8                                                  Empty
1       R200-1120402W V01          QCI1414A02J        N/A              49152
12
3       R210-2121605W V01          QCI1442AHFX        N/A              24576            8
4       UCSC-BSE-SFF-C200 V01      QCI1514A0J7        N/A              8192             8
```

ラックマウント サーバの削除

はじめる前に

次の手順を実行する前に、ラックマウント サーバとファブリック エクステンダを接続しているCIMC LOM ケーブルを物理的に外します。ハイ アベイラビリティ構成の場合は、両方のケーブルを外します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **remove server** *server-num*	指定したラックマウント サーバを削除します。
ステップ 2	UCS-A# **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、ラックマウント サーバ 4 を削除し、トランザクションをコミットする例を示します。

```
UCS-A#  remove server 4
UCS-A* # commit-buffer
UCS-A #
```

次の作業

ラックマウント サーバを物理的に再接続する場合は、それを再認識して、Cisco UCS Manager にこのサーバを再検出させる必要があります。

詳細については、ラックマウント サーバの認識, （753 ページ） を参照してください。

ラックマウント サーバのロケータ LED の電源投入

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *server-num*	指定したラックマウント サーバでサーバ モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /server # **enable locator-led**	ラックマウント サーバのロケータ LED の電源を投入します。
ステップ 3	UCS-A /server # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、ラックマウント サーバ 2 のロケータ LED の電源を投入し、トランザクションをコミットする例を示します。

```
UCS-A# scope server 2
UCS-A /server # enable  locator-led
UCS-A /server* # commit-buffer
UCS-A /server #
```

ラックマウント サーバのロケータ LED の電源切断

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *server-num*	指定したラックマウント サーバでサーバ モードを開始します。
ステップ 2	UCS-A /server # **disable locator-led**	ラックマウント サーバのロケータ LED の電源を切断します。
ステップ 3	UCS-A /server # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、ラックマウント サーバ 2 のロケータ LED の電源を切断し、トランザクションをコミットする例を示します。

```
UCS-A# scope server 2
UCS-A /server # disable  locator-led
UCS-A /server* # commit-buffer
UCS-A /server #
```

ラックマウント サーバの CMOS のリセット

サーバのトラブルシューティング時に、CMOS のリセットが必要になる場合もあります。CMOS のリセットは、通常のサーバ メンテナンスには含まれません。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *server-num*	ラックマウント サーバでサーバ モードを開始します。
ステップ 2	UCS-A /server # **reset-cmos**	ラックマウント サーバの CMOS をリセットします。
ステップ 3	UCS-A /server # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、ラックマウント サーバ 2 の CMOS をリセットし、トランザクションをコミットする例を示します。

```
UCS-A# scope server 2
UCS-A /server # reset-cmos
UCS-A /server* # commit-buffer
UCS-A /server #
```

ラックマウント サーバの CIMC のリセット

ファームウェアでのサーバのトラブルシューティング時に、CIMC のリセットが必要になる場合もあります。CIMC のリセットは、通常のサーバ メンテナンスには含まれません。CIMC のリセット後、サーバは、そのサーバで実行されているバージョンのファームウェアを使ってブートされます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *server-num*	指定したラックマウント サーバでサーバ モードを開始します。
ステップ 2	UCS-A /server # **scope CIMC**	サーバ CIMC モードに入ります。
ステップ 3	UCS-A /server/CIMC # **reset**	ラックマウント サーバの CIMC をリセットします。
ステップ 4	UCS-A /server/CIMC # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、ラックマウント サーバ 2 の CIMC をリセットし、トランザクションをコミットする例を示します。

```
UCS-A# scope server 2
UCS-A /server # scope CIMC
UCS-A /server/cimc # reset
UCS-A /server/cimc* # commit-buffer
UCS-A /server/cimc #
```

ラックマウント サーバの TPM のクリア

TPM のサポートが含まれている Cisco UCS M4 ブレード サーバおよびラックマウント サーバでのみ、TPM をクリアできます。

注意 TPM のクリアは危険性のある操作です。OS が起動を停止することがあります。また、データを損失する可能性もあります。

はじめる前に

TPM が有効である必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *server-num*	ラックマウント サーバでサーバ モードを開始します。
ステップ 2	UCS-A# /server # **scope tpm** *tpm-ID*	指定された TPM の組織 TPM モードを開始します。
ステップ 3	UCS-A# /server/tpm # **set adminaction clear-config**	TPM のクリアを指定します。
ステップ 4	UCS-A# /server/tpm # **commit-buffer**	トランザクションをシステム設定にコミットします。

次に、ラックマウント サーバの TPM をクリアする方法の例を示します。

```
UCS-A# scope server 3
UCS-A# /server # scope tpm 1
UCS-A# /server/tpm # set adminaction clear-config
UCS-A# /server/tpm* # commit-buffer
```

ラックマウント サーバの破損した BIOS の復旧

非常に珍しいケースですが、ラックマウント サーバの問題により、破損した BIOS の復旧が必要になることがあります。この手順は、ラックマウント サーバの通常メンテナンスには含まれません。BIOS の復旧後、ラックマウント サーバは、そのサーバで実行されているバージョンのファームウェアを使用してブートします。

はじめる前に

重要 サーバ上で破損している BIOS の復旧を試行する前に、そのサーバに接続またはマップされている USB ストレージをすべて取り外します。外部 USB ドライブが vMedia からサーバに取り付けられた、またはマップされている場合、BIOS の回復に失敗します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *server-id*	指定したラックマウント サーバでサーバ モードを開始します。
ステップ 2	UCS-A /server # **recover-bios** *version*	指定した BIOS バージョンをロードし、アクティブにします。
ステップ 3	UCS-A /server # **commit-buffer**	トランザクションをコミットします。

次に、BIOS を復旧する例を示します。

```
UCS-A# scope server 1
UCS-A /server # recover-bios S5500.0044.0.3.1.010620101125
UCS-A /server* # commit-buffer
UCS-A /server #
```

ラックマウント サーバのステータスの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **show server status**	Cisco UCS ドメイン のすべてのサーバのステータスを表示します。

次に、Cisco UCS ドメイン 内のすべてのサーバのステータスを表示する例を示します。番号が 1 および 2 のサーバはラックマウント サーバであるため、それらのサーバには表にリストされているスロットがありません。

```
Server Slot  Status    Availability  Overall Status  Discovery
------------------------------------------------------------------------
1/1          Equipped  Unavailable   Ok              Complete
1/2          Equipped  Unavailable   Ok              Complete
1/3          Equipped  Unavailable   Ok              Complete
1/4          Empty     Unavailable   Ok              Complete
1/5          Equipped  Unavailable   Ok              Complete
1/6          Equipped  Unavailable   Ok              Complete
1/7          Empty     Unavailable   Ok              Complete
1/8          Empty     Unavailable   Ok              Complete
1            Equipped  Unavailable   Ok              Complete
2            Equipped  Unavailable   Ok              Complete
```

ラックマウント サーバからの NMI の発行

システムが応答しないままになっており、Cisco UCS Manager で、CIMC から Non Maskable Interrupt（NMI）を BIOS またはオペレーティング システムに発行する必要がある場合は、次の手順を実行します。このアクションにより、サーバにインストールされているオペレーティング システム応じて、コア ダンプまたはスタック トレースが作成されます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** [*chassis-num*/*server-num* | *dynamic-uuid*]	指定したサーバのサーバ モードを開始します。
ステップ 2	UCS-A /chassis/server # **diagnostic-interrupt**	
ステップ 3	UCS-A /chassis/server* # **commit-buffer**	保留中のすべてのトランザクションをコミットします。

次に、シャーシ 2 のサーバ 4 から NMI を送信し、トランザクションをコミットする例を示します。

```
UCS-A# scope server 2/4
UCS-A /chassis/server # diagnostic-interrupt
UCS-A /chassis/server* # commit-buffer
UCS-A /chassis/server #
```

第 38 章

CIMC セッション管理

この章の内容は、次のとおりです。

CIMC セッション管理の概要

Cisco UCS Manager 内の KVM、vMedia、および SoL セッションを表示および終了できます。管理者権限を持つユーザは、任意のユーザの KVM、vMedia、および SoL セッションを切断できます。.Cisco Integrated Management Controller（CIMC）により、セッション情報が Cisco UCS Manager に提供されます。Cisco UCS Manager は CIMC からイベントを取得すると、そのセッション テーブルを更新し、すべてのユーザに情報を表示します。

セッション情報は次の情報で構成されます。

- 名前：セッションを開始したユーザの名前。
- セッション ID：セッションに関連付けられた ID。ブレードのセッション ID の形式は [unique identifier] _ [chassis id] _ [Blade id] です。ラックのセッション ID の形式は [unique identifier] _ 0 _ [Rack id] です。
- セッション タイプ：KVM、vMedia、または SoL。
- ユーザの権限レベル：読み取り/書き込み、読み取り専用、または付与。
- 管理状態：アクティブまたは非アクティブ。値は、セッションがアクティブの場合はアクティブです。値は、セッション終了コマンドが発行されたが、セッションが終了していない場合は非アクティブとなります。この状況は、サーバの FSM が別の操作で進行中である場合、または CIMC への接続が失われた場合に発生します。
- 送信元アドレス：セッションが開かれたコンピュータの IP アドレス。
- サービス プロファイル：セッションに関連付けられたサービス プロファイル。CIMC セッションのサービス プロファイルの属性値は、セッションがサービス プロファイルから提供された IP アドレスで開くときにだけ表示されます。

- サーバ：セッションに関連付けられたサーバの名前。
- ログイン時刻：セッションが開始された日時。
- 最終更新時刻：セッション情報が CIMC により更新された最終時刻。

新しいセッションは通常、ユーザがKVM、vMedia、またはSOLに接続するときに追加されます。Pnuos vMedia セッションは、ユーザ名 __vmediausr__ を用いたサーバ検出時にセッション テーブルに表示されます。

CIMC セッション データは Cisco UCS Manager GUI の [CIMC セッション（CIMC Sessions）] タブで使用できます。ユーザによって終了された CIMC セッションは、適切な詳細とともにログに記録された監査です。

（注） このガイドに記載されている GUI および CLI タスクを実行するには、2.1(2a) 以上の CIMC イメージ バージョンがブレード サーバのセッション管理サポートに必要です。1.5(1l) 以上の最新の CIMC イメージ バージョンが、ラック サーバに必要です。

ローカル ユーザにより開かれた CIMC セッションの表示

ローカル ユーザにより開かれたすべての CIMC セッションまたは特定のローカル ユーザにより開かれた CIMC セッションを表示するには、このタスクを実行します。

（注） 特定のサーバまたはサービス プロファイル オプションの CIMC セッションの表示は CLI にありません。これは、GUI で使用できます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope security**	セキュリティ コンフィギュレーション モードを開始します。
ステップ 2	UCS-A /security # **show cimc-sessions local**	ローカル ユーザにより開かれたすべての CIMC セッションを表示します。
ステップ 3	UCS-A /security # **show cimc-sessions local** *user-name*	特定のローカル ユーザにより開かれたすべての CIMC セッションを表示します。

次に、以下を表示する例を示します。

- ローカル ユーザにより開かれたすべての CIMC セッション

- 特定のローカル ユーザにより開かれた CIMC セッション
- 特定のローカル ユーザにより開かれた CIMC セッションの詳細

```
All sessions opened by local users:
UCS-A # scope security
UCS-A /security # show cimc-sessions local

Session ID   Type     User      Source Addr     Admin State
----------   ------ --------- --------------- ------------
42_1_1       Kvm      admin     10.106.22.117     Active
4_1_5        Kvm      admin     10.106.22.117     Active
5_1_5        Vmedia   admin     10.106.22.117     Active

Session opened by a specific local user:
UCS-A /security # show cimc-sessions local admin
Session ID   Type     User      Source Addr     Admin State
----------   ------ --------- --------------- ------------
42_1_1       Kvm      admin     10.106.22.117     Active

Details of session opened by a specific local user:
UCS-A /security # show cimc-sessions local admin detail
Session ID 42_1_1
   Type: Kvm
   User: admin
   Source Addr: 10.106.22.117
   Login Time: 2013-06-28T06:09:53.000
   Last Updated Time: 2013-06-28T06:21:52.000
   Admin State: Active
   Priv: RW
   Server: sys/chassis-1/blade-1
   Service Profile:
```

リモート ユーザにより開かれた CIMC セッションの表示

リモート ユーザにより開かれたすべての CIMC セッションまたは特定のリモート ユーザにより開かれた CIMC セッションを表示するには、このタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope security**	セキュリティ コンフィギュレーション モードを開始します。
ステップ 2	UCS-A /security # **show cimc-sessions remote**	リモート ユーザにより開かれたすべての CIMC セッションを表示します。
ステップ 3	UCS-A /security # **show cimc-sessions remote** *user-name*	特定のリモート ユーザにより開かれたすべての CIMC セッションを表示します。

次に、以下を表示する例を示します。

- リモート ユーザにより開かれたすべての CIMC セッション
- 特定のリモート ユーザにより開かれた CIMC セッション

- 特定のリモート ユーザにより開かれた CIMC セッションの詳細

```
All sessions opened by remote users:
UCS-A # scope security
UCS-A /security # show cimc-sessions remote

Session ID   Type     User             Source Addr      Admin State
----------   ------ ---------        ---------------   ------------
43_1_1       Kvm     administrator     10.106.22.117     Active
6_1_5        Kvm     test-remote       10.106.22.117     Active
7_1_5        Vmedia  test-remote       10.106.22.117     Active

Session opened by a specific remote user:
UCS-A /security # show cimc-sessions remote administrator

Session ID   Type     User             Source Addr      Admin State
----------   ------ ---------        ---------------   ------------
43_1_1       Kvm     administrator     10.106.22.117     Active

Details of session opened by a specific remote user:
UCS-A /security # show cimc-sessions remote administrator detail
Session ID 43_1_1
   Type: Kvm
   User: administrator
   Source Addr: 10.106.22.117
   Login Time: 2013-06-28T06:09:53.000
   Last Updated Time: 2013-06-28T06:21:52.000
   Admin State: Active
   Priv: RW
   Server: sys/chassis-1/blade-1
   Service Profile:
```

IPMI ユーザにより開かれた CIMC セッションの表示

IPMI ユーザにより開かれた CIMC セッションを表示するには、次の手順を完了します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope org** *org-name*	ルート組織モードを開始します。
ステップ 2	UCS-A /org # **scope ipmi-access-profile** *profile-name*	IPMI アクセス プロファイル名を入力します。
ステップ 3	UCS-A /org/ipmi-access-profile # **scope ipmi-user** *user-name*	IPMI ユーザ名を入力します。
ステップ 4	UCS-A /org/ipmi-access-profile/ipmi-user # **show cimc-sessions**	指定された IPMI ユーザによって開かれたすべての CIMC セッションを表示します。

次の例では、IPMI ユーザにより開かれたすべての CIMC セッションを表示する方法を示します。

```
UCS-A # scope org Finance
UCS-A /org* # scope ipmi-access-profile ReadOnly
UCS-A /org/ipmi-access-profile* # scope ipmi-user alice
```

```
UCS-A /org/ipmi-access-profile/ipmi-user # show cimc-sessions

Session ID    Type    User        Source Addr       Admin State
----------   ------  ---------   ---------------   --------------
45_1_1        sol     alice       10.106.22.117     Active
```

サーバの CIMC セッションのクリア

このタスクでは、サーバで開かれたすべてのCIMCセッションをクリアする方法を示します。セッション タイプとユーザ名に基づいて、サーバの CIMC セッションをクリアすることもできます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope security**	セキュリティ コンフィギュレーション モードを開始します。
ステップ 2	UCS-A /security # **terminate cimc-sessions server** *chassis-id/blade-id*	シャーシの特定のブレード サーバの CIMC セッションをクリアします。
ステップ 3	UCS-A /security # **terminate cimc-sessions server** *Rack-server-id*	特定のラック サーバの CIMC セッションをクリアします。
ステップ 4	UCS-A /security # **terminate cimc-sessions server** *server-id* **type** *session-type*	サーバの特定のタイプのCIMCセッションをクリアします。
ステップ 5	UCS-A /security # **terminate cimc-sessions server** *server-id* **user-name** *user-name*	サーバの特定のユーザのCIMCセッションをクリアします。

最初の例では、サーバのすべての CIMC セッションをクリアする方法を示します。2 番目の例では、サーバの特定のタイプの CIMC セッションをクリアする方法を示します。3 番目の例では、サーバの特定のユーザの CIMC セッションをクリアする方法を示します。

```
UCS-A /security # scope security
UCS-A /security # terminate cimc-sessions server 2/1
This will close KVM sessions. Are you sure? (yes/no):yes
UCS-A /security

UCS-A # scope security
UCS-A /security # terminate cimc-sessions server 2/1 type kvm
This will close KVM sessions. Are you sure? (yes/no):yes

UCS-A # scope security
UCS-A /security # terminate cimc-sessions server 2/1 user-name test-user
This will close KVM sessions. Are you sure? (yes/no):yes
```

ローカル ユーザにより開かれたすべての CIMC セッションのクリア

このタスクでは、ローカル ユーザにより開かれたセッションをクリアする方法を示します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope security**	セキュリティ コンフィギュレーション モードを開始します。
ステップ 2	UCS-A /security # **terminate cimc-sessions local-user** *user-name*	ローカル ユーザにより開かれたすべての CIMC セッションをクリアします。
ステップ 3	UCS-A /security # **terminate cimc-sessions local-user** *user-name* **type** {**kvm** | **vmedia sol** | **all**}	ローカルユーザにより開かれた特定のセッション タイプのすべての CIMC セッションをクリアします。

次の例では、ローカル ユーザにより開かれた CIMC セッションをクリアする方法を示します。

```
UCS-A /security# scope security
UCS-A /security# terminate cimc-sessions local-user testuser
This will close cimc sessions. Are you sure? (yes/no):yes
UCS-A /security#
```

リモート ユーザにより開かれたすべての CIMC セッションのクリア

このタスクでは、リモート ユーザにより開かれた CIMC セッションをクリアする方法を示します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope security**	セキュリティ コンフィギュレーション モードを開始します。
ステップ 2	UCS-A /security # **terminate cimc-sessions remote-user** *user-name*	リモート ユーザにより開かれたすべての CIMC セッションをクリアします。
ステップ 3	UCS-A /security # **terminate cimc-sessions remote-user** *user-name* **type** {**kvm** | **vmedia sol** | **all**}	リモートユーザにより開かれた特定のセッション タイプのすべての CIMC セッションをクリアします。

次の例では、リモート ユーザにより開かれたすべての CIMC セッションをクリアする方法を示します。

```
UCS-A /security# scope security
UCS-A /security# terminate cimc-sessions remote-user testuser
This will close cimc sessions. Are you sure? (yes/no):yes
UCS-A /security#
```

ローカル ユーザにより開かれた特定の CIMC セッションのクリア

このタスクでは、ローカル ユーザによって開かれた特定の CIMC セッションをクリアする方法を示します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope security**	セキュリティ コンフィギュレーション モードを開始します。
ステップ 2	UCS-A /security # **scope local-user** *user-name*	ローカル ユーザ モードを開始します。
ステップ 3	UCS-A /security/local user # **terminate cimc-session** *session-id*	選択した CIMC セッションをクリアします。
ステップ 4	UCS-A /security/local user* # **commit-buffer**	トランザクションをコミットします。

次の例では、ローカル ユーザによって開かれた特定の CIMC セッションをクリアし、トランザクションをコミットする方法を示します。

```
UCS-A /security# scope security
UCS-A /security# scope local-user admin
UCS-A /security/local user # terminate cimc-session 6_1_2
UCS-A /security/local user*# commit-buffer
UCS-A /security/local user#
```

リモート ユーザにより開かれた特定の CIMC セッションのクリア

このタスクでは、リモート ユーザによって開かれた特定の CIMC セッションをクリアする方法を示します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope security**	セキュリティ コンフィギュレーション モードを開始します。
ステップ 2	UCS-A /security # **scope remote -user** *user-name*	リモート ユーザ モードを開始します。
ステップ 3	UCS-A /security/remote user # **terminate cimc-session** *session-id*	選択した CIMC セッションをクリアします。
ステップ 4	UCS-A /security/remote user* # **commit-buffer**	トランザクションをコミットします。

次の例では、リモート ユーザによって開かれた特定の CIMC セッションをクリアし、トランザクションをコミットする方法を示します。

```
UCS-A /security# scope security
UCS-A /security# scope remote-user admin
UCS-A /security/remote user # terminate cimc-session 6_1_3
UCS-A /security/remote user*# commit-buffer
UCS-A /security/remote user#
```

IPMI ユーザにより開かれた CIMC セッションのクリア

IPMI ユーザにより開かれた CIMC セッションをクリアするには、次の手順を完了します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope org** *org-name*	ルート組織モードを開始します。
ステップ 2	UCS-A /org # **scope ipmi-access-profile** *profile-name*	IPMI アクセス プロファイル名を入力します。
ステップ 3	UCS-A /org/ipmi-access-profile # **scope ipmi-user** *user-name*	IPMI ユーザを入力します。
ステップ 4	UCS-A /org/ipmi-access-profile/ipmi-user # **terminate cimc-sessions** *session-id*	IPMI ユーザによって開かれた特定の CIMC セッションを終了します。
ステップ 5	UCS-A /org/ipmi-access-profile/ipmi-user * **commit-buffer**	変更をコミットします。

次の例では、IPMI ユーザによって開かれた特定の CIMC セッションをクリアし、変更をコミットする方法を示します。

```
UCS-A # scope org Finance
UCS-A /org* # scope ipmi-access-profile ReadOnly
UCS-A /org/ipmi-access-profile* # scope ipmi-user alice
UCS-A /org/ipmi-access-profile/ipmi-user # terminate cimc-sessions 5_1_2
UCS-A /org/ipmi-access-profile/ipmi-user* # commit-buffer
```

第 39 章

設定のバックアップと復元

この章の内容は、次のとおりです。

UCS でのバックアップの操作

Cisco UCS Manager からバックアップを実行する場合は、システム設定全体またはその一部のスナップショットを作成し、ファイルをネットワーク上の場所にエクスポートします。Cisco UCS Manager を使用して、サーバにデータをバックアップすることはできません。

バックアップは、システムが起動されて動作している間に実行できます。バックアップ操作では、管理プレーンからの情報だけが保存されます。バックアップは、サーバまたはネットワーク トラフィックには影響しません。

バックアップ タイプ

Cisco UCS Manager および Cisco UCS Central では、次のタイプのバックアップを 1 つ以上実行できます。

- [Full ステート（Full state）]：システム全体のスナップショットが含まれるバイナリファイル。このバックアップにより生成されたファイルを使用して、ディザスタ リカバリ時にシステムを復元できます。このファイルにより、元のファブリック インターコネクト上で設定を復元または再構築できます。また、別のファブリック インターコネクト上で設定を再現することもできます。このファイルは、インポートには使用できません。

（注） バックアップ ファイルのエクスポート元となったシステムと同じバージョンを実行しているシステムを復元するために使用できるのは、Full State バックアップ ファイルのみです。

- [すべての設定（All configuration）]：すべてのシステム設定と論理設定が含まれる XML ファイル。このバックアップにより生成されたファイルを使用して、これらの設定を元のファブリック インターコネクトまたは別のファブリック インターコネクトにインポートできます。このファイルは、システムの復元には使用できません。このファイルには、ローカル認証されたユーザのパスワードは含まれません。
- [システム設定（System configuration）]：ユーザ名、ロール、ロケールなどのすべてのシステム設定が含まれる XML ファイル。このバックアップにより生成されたファイルを使用して、これらの設定を元のファブリック インターコネクトまたは別のファブリック インターコネクトにインポートできます。このファイルは、システムの復元には使用できません。
- [論理設定（Logical configuration）]：サービス プロファイル、VLAN、VSAN、プール、ポリシーなどのすべての論理設定が含まれる XML ファイル。このバックアップにより生成されたファイルを使用して、これらの設定を元のファブリック インターコネクトまたは別のファブリック インターコネクトにインポートできます。このファイルは、システムの復元には使用できません。

バックアップ操作の考慮事項と推奨事項

バックアップ操作を作成する前に、次のことを考慮してください。

バックアップの場所

バックアップ場所とは、Cisco UCS Manager でバックアップ ファイルをエクスポートするネットワーク上の宛先またはフォルダのことです。バックアップ操作は、バックアップ ファイルを保存する場所ごとに 1 つしか保持できません。

バックアップ ファイル上書きの可能性

ファイル名を変更しないでバックアップ操作を再実行すると、サーバ上にすでに存在するファイルがCisco UCS Managerによって上書きされます。既存のバックアップ ファイルが上書きされるのを回避するには、バックアップ操作内のファイル名を変更するか、既存のファイルを別の場所にコピーします。

バックアップの複数のタイプ

同じ場所に対して複数種類のバックアップを実行し、エクスポートできます。バックアップ操作を再実行する前に、バックアップ タイプを変更する必要があります。バックアップ タイプの識別を容易にし、また既存のバックアップ ファイルが上書きされるのを回避するために、ファイル名を変更することを推奨します。

スケジュール バックアップ

バックアップ操作を前もって作成し、そのバックアップの実行準備が整うまで管理状態をディセーブルのままにしておくことはできます。Cisco UCS Manager は、バックアップ操作の管理状態がイネーブルに設定されるまで、バックアップ操作の実行や、コンフィギュレーション ファイルの保存、エクスポートを行いません。

増分バックアップ

Cisco UCS Manager の増分バックアップを行うことはできません。

フル ステート バックアップの暗号化

パスワードなどの機密情報がクリア テキストでエクスポートされることがないように、フル ステート バックアップは暗号化されます。

スケジュール バックアップ

次のタイプのバックアップをスケジュールするようにCisco UCSにポリシーを設定できます。

- フル ステート
- All コンフィギュレーション

他のタイプのバックアップはスケジュールできません。

フルステート バックアップ ポリシー

フルステートバックアップポリシーを使用すると、システム全体のスナップショットの定期的なフルステートバックアップをスケジュールすることができます。フルステートバックアップを行う間隔は、日単位、週単位、または隔週単位で設定できます。

Cisco UCS Managerは、リモートサーバ上のバックアップ ファイルの最大数を維持します。maxfilesパラメータは、Cisco UCS Manager が Cisco UCS Central に登録される際に使用されます。maxfiles

パラメータは Cisco UCS Central でユーザが設定できるパラメータで、Cisco UCS Central に保存するバックアップ ファイルの数を制御します。

Cisco UCS Manager が Cisco UCS Central に登録されておらず、ユーザがリモート バックアップ サーバ上のバックアップ ファイルを保存している場合、バックアップ ファイルは Cisco UCS Manager によって管理されません。リモート マシンのサーバ管理者は、ディスク使用率を監視してバックアップ ファイルのローテンションを行い、新しいバックアップ ファイル用の領域を確保する必要があります。

すべての構成のエクスポート ポリシー

すべての構成のバックアップ ポリシーでは、定期的なバックアップをスケジュールし、すべてのシステム設定と論理設定をエクスポートできます。このバックアップには、ローカル認証されたユーザのパスワードは含まれません。すべての構成のバックアップを行う間隔は、日単位、週単位、または隔週単位で設定できます。

Cisco UCS は、リモート サーバ上のバックアップ ファイルの最大数を維持します。この数を超えると、Cisco UCS は最も古いバックアップ ファイルを上書きします。

設定のインポート

Cisco UCS からエクスポートされたコンフィギュレーション ファイルをインポートできます。ファイルは、同じ Cisco UCS からエクスポートされたものである必要はありません。

（注） 上位のリリースから下位のリリースに設定をインポートすることはできません。

インポート機能は、すべてのコンフィギュレーション ファイル、システム コンフィギュレーション ファイル、および論理コンフィギュレーション ファイルで使用できます。インポートは、システムがアップ状態で、稼働中に実行できます。インポート操作によって情報が変更されるのは、管理プレーンだけです。インポート操作によって行われる一部の変更（サーバに割り当てられた vNIC に対する変更など）により、サーバのリブートまたはトラフィックを中断する他の動作が行われることがあります。

インポート操作はスケジュールできません。ただし、インポート操作を前もって作成し、そのインポートの実行準備が整うまで管理状態をディセーブルのままにしておくことはできます。Cisco UCS は、管理状態がイネーブルに設定されるまで、コンフィギュレーション ファイルに対してインポート操作を実行しません。

インポート操作は、コンフィギュレーション バックアップ ファイルを保存する場所ごとに 1 つしか保持できません。

インポート方法

次のいずれかの方法を使用して、Cisco UCS によるシステム設定のインポートおよびアップデートを実行できます。

- [マージ（Merge）]：インポートされたコンフィギュレーション ファイルの情報は、既存の設定情報と比較されます。競合が存在する場合、インポートされた設定ファイルの情報で Cisco UCS ドメイン の情報が上書きされます。
- [置換（Replace）]：現在の設定情報が、インポートされたコンフィギュレーション ファイルの情報で一度に 1 つのオブジェクトについて置き換えられます。

システムの復元

この復元機能は、ディザスタ リカバリに使用できます。

Cisco UCS からエクスポートされた任意のフル ステート バックアップ ファイルからシステム設定を復元できます。このファイルは、復元するシステム上の Cisco UCS からエクスポートされたものでなくてもかまいません。別のシステムからエクスポートされたバックアップ ファイルを使用して復元する場合、ファブリック インターコネクト、サーバ、アダプタ、および I/O モジュールまたは FEX 接続を含めて、同じまたは同様のシステム設定およびハードウェアを持つシステムを使用することを推奨します。ハードウェアまたはシステム設定が一致しない場合、復元されたシステムが完全には機能しないことがあります。2 つのシステムの I/O モジュール リンク間またはサーバ間に不一致がある場合、復元操作後にシャーシまたはサーバまたはその両方を承認します。

この復元機能は、フル ステート バックアップ ファイルにだけ使用できます。フル ステート バックアップ ファイルはインポートできません。復元は、初期システムセットアップで実行します。詳細については、該当する『*Cisco UCS Central Installation and Upgrade Guide*』を参照してください。

（注） バックアップ ファイルのエクスポート元となったシステムと同じバージョンを実行しているシステムを復元するために使用できるのは、Full State バックアップ ファイルのみです。

バックアップ操作とインポート操作に必要なユーザロール

バックアップ操作とインポート操作を作成し、実行するには、管理ロールを持つユーザ アカウントが必要です。

バックアップ操作の設定

バックアップ操作の作成

はじめる前に

バックアップ サーバの IPv4 アドレスまたは IPv6 アドレスおよび認証クレデンシャルを取得します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **create backup** *URL backup-type* {**disabled** | **enabled**}	バックアップ操作を作成します。次のいずれかの構文を使用してバックアップするファイルの *URL* を指定します。 • **ftp:**// *username@hostname/ path* • **scp:**// *username@hostname/ path* • **sftp:**// *username@hostname/ path* • **tftp:**// *hostname***:** *port-num/ path* *backup-type* 引数には、次のいずれかの値を指定できます。 • **all-configuration**：サーバ関連、ファブリック関連、システム関連の設定をバックアップします • **logical-configuration**：ファブリックおよびサービス プロファイルの関連の設定をバックアップします • **system-configuration**：システム関連の設定をバックアップします • **full-state**：ディザスタ リカバリのために完全な状態をバックアップします

	コマンドまたはアクション	目的
		（注） • 完全な状態のバックアップファイルはインポート操作を使用してインポートできません。これらは、ファブリック インターコネクトの設定を復元するためにのみ使用されます。 • バックアップファイルのエクスポート元となったシステムと同じバージョンを実行しているシステムを復元するために使用できるのは、Full State バックアップ ファイルのみです。 複数のバックアップ操作を保存できますが、各ホスト名につき 1 種類の操作だけが保存されます。 **enable** キーワードを使用した場合、バックアップ操作は **commit-buffer** コマンドを入力するとすぐに自動的に実行されます。**disable** キーワードを使用すると、バックアップ操作は有効にされるまで実行されません。バックアップ操作をイネーブルにする場合、バックアップ操作を作成するときに使用したホスト名を指定する必要があります。
ステップ **3**	UCS-A /system # **commit-buffer**	トランザクションをコミットします。

次の例では、ホスト名 host35 に対する disabled all-configuration バックアップ操作を作成し、トランザクションをコミットする方法を示します。

```
UCS-A# scope system
UCS-A /system* # create backup scp://user@host35/backups/all-config9.bak all-configuration
 disabled
Password:
UCS-A /system* # commit-buffer
UCS-A /system #
```

バックアップ操作の実行

手順

	コマンドまたはアクション	目的
ステップ **1**	UCS-A# **scope system**	システム モードを開始します。
ステップ **2**	UCS-A /system # **scope backup** *hostname*	指定したホスト名でシステム バックアップ モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /system/backup # **enable**	バックアップ操作をイネーブルにします。 （注） FTP、SCP、SFTP を使用するバックアップ操作では、パスワードの入力を求められます。トランザクションをコミットする前にパスワードを入力します。
ステップ 4	UCS-A /system/backup # **commit-buffer**	トランザクションをコミットします。

次に、host35 というバックアップ操作をイネーブルにし、SCP プロトコルのパスワードを入力し、トランザクションをコミットする例を示します。

```
UCS-A# scope system
UCS-A /system # scope backup host35
UCS-A /system/backup # enable
Password:
UCS-A /system/backup* # commit-buffer
UCS-A /system/backup #
```

バックアップ操作の変更

バックアップ操作を修正して、別のバックアップ タイプのファイルをその場所に保存したり、前のバックアップ ファイルが上書きされないようにファイル名を変更したりすることができます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope backup** *hostname*	指定したホスト名でシステム バックアップ モードを開始します。
ステップ 3	UCS-A /system/backup # **disable**	（任意） トランザクションのコミット時にバックアップ操作が自動的に実行されないようにするために、イネーブルになっているバックアップ操作をディセーブルにします。
ステップ 4	UCS-A /system/backup # **enable**	（任意） トランザクションをコミットすると、ただちにバックアップ操作が自動的に実行されるようにします。

	コマンドまたはアクション	目的
ステップ 5	UCS-A /system/backup # **set descr** *description*	（任意） バックアップ操作の説明を指定します。 （注） 説明にスペース、特殊文字、または句読点が含まれている場合は、説明を引用符で括る必要があります。引用符は、showコマンド出力の説明フィールドには表示されません。
ステップ 6	UCS-A /system/backup # **set protocol** {**ftp** | **scp** | **sftp** | **tftp**}	（任意） リモート サーバとの通信時に使用するプロトコルを指定します。
ステップ 7	UCS-A /system/backup # **set remote-file** *filename*	（任意） バックアップする設定ファイルの名前を指定します。
ステップ 8	UCS-A /system/backup # **set type** *backup-type*	（任意） 作成するバックアップ ファイルのタイプを指定します。*backup-type* 引数には、次のいずれかの値を指定できます。 • **all-configuration**：サーバ関連、ファブリック関連、システム関連の設定をバックアップします • **logical-configuration**：ファブリックおよびサービス プロファイルの関連の設定をバックアップします • **system-configuration**：システム関連の設定をバックアップします • **full-state**：ディザスタ リカバリのために完全な状態をバックアップします （注） • 完全な状態のバックアップ ファイルはインポート操作を使用してインポートできません。これらは、ファブリック インターコネクトの設定を復元するためにのみ使用されます。 • バックアップ ファイルのエクスポート元となったシステムと同じバージョンを実行しているシステムを復元するために使用できるのは、Full State バックアップ ファイルのみです。

	コマンドまたはアクション	目的
ステップ 9	UCS-A /system/backup # **set preserve-pooled-values** {**no** | **yes**}	（任意） vHBA WWPN、vNIC MAC、WWNN、UUID など、プールから抽出された ID 値をバックアップで保存するかどうかを指定します。
ステップ 10	UCS-A /system/backup # **set user** *username*	（任意） システムがリモート サーバへのログインに使用する必要のあるユーザ名を指定します。この手順は、TFTP プロトコルを使用する場合には適用されません。
ステップ 11	UCS-A /system/backup # **set password**	（任意） Enter キーを押すと、パスワードを入力するように促されます。 リモート サーバのユーザ名のパスワードを指定します。この手順は、TFTP プロトコルを使用する場合には適用されません。
ステップ 12	UCS-A /system/backup # **commit-buffer**	トランザクションをコミットします。

次に、説明を追加し、host35 バックアップ操作のプロトコル、ユーザ名、およびパスワードを変更し、トランザクションをコミットする例を示します。

```
UCS-A# scope system
UCS-A /system # scope backup host35
UCS-A /system/backup # set descr "This is a backup operation for host35."
UCS-A /system/backup* # set protocol sftp
UCS-A /system/backup* # set user UserName32
UCS-A /system/backup* # set password
Password:
UCS-A /system/backup* # set preserve-pooled-values no
UCS-A /system/backup* # commit-buffer
UCS-A /system #
```

バックアップ操作の削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **delete backup** *hostname*	指定したホスト名のバックアップ操作を削除します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /system # **commit-buffer**	トランザクションをコミットします。

次に、host35 というホスト名のバックアップ操作を削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope system
UCS-A /system # delete backup host35
UCS-A /system* # commit-buffer
UCS-A /system #
```

スケジュール バックアップの設定

フルステート バックアップ ポリシーの設定

はじめる前に

バックアップ サーバの IPv4 アドレスまたは IPv6 アドレスおよび認証クレデンシャルを取得します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルート組織モードを開始するには、*/* を *org-name* として入力します。
ステップ 2	UCS-A /org #**scope backup-policy default**	すべての構成のエクスポート ポリシー モードを開始します。
ステップ 3	UCS-A /org/backup-policy # **set hostname** {*hostname* | *ip-addr* | *ip6-addr*}	バックアップ ポリシーが格納されている場所のホスト名、IPv4 または IPv6 アドレスを指定します。これは、サーバ、ストレージ アレイ、ローカル ドライブ、またはファブリック インターコネクトがネットワーク経由でアクセス可能な任意の読み取り/書き込みメディアなどがあります。

	コマンドまたはアクション	目的
		（注） IPv4 や IPv6 アドレスではなくホスト名を使用する場合、DNS サーバを設定する必要があります。Cisco UCS ドメイン が Cisco UCS Central に登録されていないか、または DNS 管理が [ローカル（local）] に設定されている場合は、Cisco UCS Manager で DNS サーバを設定します。Cisco UCS ドメイン Cisco UCS Central に登録されていないか、DNS 管理が [グローバル（global）] に設定されている場合は、Cisco UCS Central で DNS サーバを設定します。
ステップ 4	UCS-A /org/backup-policy # **set protocol** {**ftp** | **scp** | **sftp** | **tftp**}	リモート サーバとの通信時に使用するプロトコルを指定します。
ステップ 5	UCS-A /org/backup-policy # **set user** *username*	システムがリモート サーバへのログインに使用する必要のあるユーザ名を指定します。この手順は、TFTP プロトコルを使用する場合には適用されません。
ステップ 6	UCS-A /system/backup-policy # **set password**	Enter キーを押すと、パスワードを入力するように促されます。 リモートサーバのユーザ名のパスワードを指定します。この手順は、TFTP プロトコルを使用する場合には適用されません。
ステップ 7	UCS-A /system/backup-policy # **set remote-file** *filename*	バックアップ ファイルのフル パスを指定します。このフィールドには、ファイル名とパスを含めることができます。ファイル名を省略すると、バックアップ手順によって、ファイルに名前が割り当てられます。
ステップ 8	UCS-A /system/backup-policy # **set adminstate** {**disabled** | **enabled**}	ポリシーの管理状態を指定します。次のいずれかになります。 • [enabled]：Cisco UCS Manager は、[スケジュール（Schedule）] フィールドで指定されたスケジュールを使用してバックアップ ファイルをエクスポートします。 • [disabled]：Cisco UCS Manager はファイルをエクスポートしません。
ステップ 9	UCS-A /system/backup-policy # **set schedule** {**daily** | **weekly** | **bi-weekly**}	Cisco UCS Manager がバックアップ ファイルをエクスポートする頻度を指定します。

	コマンドまたはアクション	目的
ステップ 10	UCS-A /system/backup-policy # **set descr** *description*	バックアップ ポリシーの説明を指定します。 256 文字以内で入力します。次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
ステップ 11	UCS-A /backup-policy # **commit-buffer**	トランザクションをコミットします。

次の例では、週単位のバックアップのためのフルステートバックアップポリシーを設定し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org # scope backup-policy default
UCS-A /org/backup-policy # set hostname host35
UCS-A /org/backup-policy* # set protocol scp
UCS-A /org/backup-policy* # set user UserName32
UCS-A /backup-policy* # set password
Password:
UCS-A /backup-policy* # set remote-file /backups/full-state1.bak
UCS-A /backup-policy* # set adminstate enabled
UCS-A /backup-policy* # set schedule weekly
UCS-A /backup-policy* # set descr "This is a full state weekly backup."
UCS-A /backup-policy* # commit-buffer
UCS-A /backup-policy #
```

すべての構成のエクスポート ポリシーの設定

はじめる前に

バックアップ サーバの IPv4 アドレスまたは IPv6 アドレスおよび認証クレデンシャルを取得します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルート組織モードを開始するには、*/* を *org-name* として入力します。
ステップ 2	UCS-A /org #**scope cfg-export-policy default**	すべての構成のエクスポート ポリシー モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /org/cfg-export-policy # **set hostname** {*hostname* | *ip-addr* | *ip6-addr*}	コンフィギュレーション ファイルが格納されている場所のホスト名、IPv4 または IPv6 アドレスを指定します。これは、サーバ、ストレージ アレイ、ローカル ドライブ、またはファブリック インターコネクトがネットワーク経由でアクセス可能な任意の読み取り/書き込みメディアなどがあります。 （注） IPv4 や IPv6 アドレスではなくホスト名を使用する場合、DNS サーバを設定する必要があります。Cisco UCS ドメインが Cisco UCS Central に登録されていないか、または DNS 管理が [ローカル（local）] に設定されている場合は、Cisco UCS Manager で DNS サーバを設定します。Cisco UCS ドメイン Cisco UCS Central に登録されていないか、DNS 管理が [グローバル（global）] に設定されている場合は、Cisco UCS Central で DNS サーバを設定します。
ステップ 4	UCS-A /org/cfg-export-policy # **set protocol** {**ftp** | **scp** | **sftp** | **tftp**}	リモート サーバとの通信時に使用するプロトコルを指定します。
ステップ 5	UCS-A /org/cfg-export-policy # **set user** *username*	システムがリモート サーバへのログインに使用する必要のあるユーザ名を指定します。この手順は、TFTP プロトコルを使用する場合には適用されません。
ステップ 6	UCS-A /system/cfg-export-policy # **set password**	Enter キーを押すと、パスワードを入力するように促されます。 リモートサーバのユーザ名のパスワードを指定します。この手順は、TFTP プロトコルを使用する場合には適用されません。
ステップ 7	UCS-A /system/cfg-export-policy # **set remote-file** *filename*	エクスポートされたコンフィギュレーション ファイルのフル パスを指定します。このフィールドには、ファイル名とパスを含めることができます。ファイル名を省略すると、バックアップ手順によって、ファイルに名前が割り当てられます。
ステップ 8	UCS-A /system/cfg-export-policy # **set adminstate** {**disabled** | **enabled**}	ポリシーの管理状態を指定します。次のいずれかになります。 • [enabled]：Cisco UCS Manager は、[スケジュール（Schedule）] フィールドで指定されたスケジュールを使用して設定情報をエクスポートします。

	コマンドまたはアクション	目的
		• [disabled]：Cisco UCS Manager は情報をエクスポートしません。
ステップ 9	UCS-A /system/cfg-export-policy # **set schedule** {**daily** | **weekly** | **bi-weekly**}	Cisco UCS Manager が設定情報をエクスポートする頻度を指定します。
ステップ 10	UCS-A /system/cfg-export-policy # **set descr** *description*	コンフィギュレーション エクスポート ポリシーの説明を指定します。 256 文字以内で入力します。次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
ステップ 11	UCS-A /cfg-export-policy # **commit-buffer**	トランザクションをコミットします。

次の例では、週単位のバックアップのためのすべての構成のエクスポート ポリシーを設定し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org # scope cfg-export-policy default
UCS-A /org/cfg-export-policy # set hostname host35
UCS-A /org/cfg-export-policy* # set protocol scp
UCS-A /org/cfg-export-policy* # set user UserName32
UCS-A /cfg-export-policy* # set password
Password:
UCS-A /cfg-export-policy* # set remote-file /backups/all-config9.bak
UCS-A /cfg-export-policy* # set adminstate enabled
UCS-A /cfg-export-policy* # set schedule weekly
UCS-A /cfg-export-policy* # set descr "This is an all configuration backup."
UCS-A /cfg-export-policy* # commit-buffer
UCS-A /cfg-export-policy #
```

バックアップ/エクスポートの設定リマインダの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の設定モードを開始します。ルート組織モードを開始するには、*/* を *org-name* として入力します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /org #**scope backup-exp-policy**	バックアップ/エクスポート設定ポリシー モードを開始します。
ステップ 3	UCS-A /org/backup-exp-policy #**show**	既存のバックアップ/エクスポートの設定ポリシーを表示します。
ステップ 4	UCS-A /org/backup-exp-policy # **set adminstate** {**disable** | **enable**}	ポリシーの管理状態を指定します。次のいずれかになります。 • [enable]：指定時間内にバックアップが実行されない場合、Cisco UCS Manager はエラーを発生させます。 • [disable]：指定時間内にバックアップが実行されない場合、Cisco UCS Manager はエラーを発生させません。
ステップ 5	UCS-A /org/backup-exp-policy #**set frequency** *Number_of_Days*	バックアップを行うよう通知されるまでの日数を指定します。1～365の整数を入力します。デフォルト値は 30 日です。
ステップ 6	UCS-A /org/backup-exp-policy #**commit-buffer**	トランザクションをコミットします。

次に、現在のバックアップ/エクスポートの設定ポリシーを確認し、リマインダの頻度を変更し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # scope backup-exp-policy
UCS-A /org/backup-exp-policy # set frequency 5
UCS-A /org/backup-exp-policy* # commit-buffer
UCS-A /org/backup-exp-policy #
```

インポート操作の設定

インポート操作の作成

フル ステート バックアップ ファイルはインポートできません。次のコンフィギュレーション ファイルのいずれもインポートできます。

- All コンフィギュレーション
- システム設定
- Logical コンフィギュレーション

はじめる前に

コンフィギュレーション ファイルをインポートするための次の情報を収集します。

- バックアップ サーバの IP アドレスおよび認証クレデンシャル
- バックアップ ファイルの完全修飾名

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **create import-config** *URL* {**disabled** | **enabled**} {**merge** | **replace**}	インポート操作を作成します。次のいずれかの構文を使用してインポートされるファイルの URL を指定します。 • **ftp://** *username@hostname/ path* • **scp://** *username@hostname/ path* • **sftp://** *username@hostname/ path* • **tftp://** *hostname***:** *port-num/ path* 複数のインポート操作を保存できますが、各ホスト名につき 1 種類の操作だけが保存されます。 **enable** キーワードを使用した場合、インポート操作は **commit-buffer** コマンドを入力するとすぐに自動実行されます。**disable** キーワードを使用すると、インポート操作は有効にされるまで実行されません。インポート操作をイネーブルにする場合、インポート操作を作成するときに使用したホスト名を指定する必要があります。 **merge** キーワードを使用すると、設定情報が既存の情報とマージされます。競合する場合、現在のシステム上の情報が、インポート設定ファイル内の情報に置き換えられます。**replace** キーワードを使用すると、システムはインポート設定ファイル内の各オブジェクトを取得し、現在のコンフィギュレーション内の対応するオブジェクトを上書きします。
ステップ 3	UCS-A /system/import-config# **set descr** *description*	（任意） インポート操作の説明を記入します。 （注） 説明にスペース、特殊文字、または句読点が含まれている場合は、説明を引用符で括る必要があります。引用符は、show コマンド出力の説明フィールドには表示されません。

	コマンドまたはアクション	目的
ステップ 4	UCS-A /system/import-config # **commit-buffer**	トランザクションをコミットします。

次の例は、現在のコンフィギュレーションを置き換えるディセーブル状態のホスト名 host35 のインポート操作を作成し、トランザクションをコミットします。

```
UCS-A# scope system
UCS-A /system* # create import-config scp://user@host35/backups/all-config9.bak disabled
replace
Password:
UCS-A /system/import-config* # commit-buffer
UCS-A /system/import-config #
```

インポート操作の実行

フル ステート バックアップ ファイルはインポートできません。次のコンフィギュレーション ファイルのいずれもインポートできます。

- All コンフィギュレーション
- システム設定
- Logical コンフィギュレーション

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope import-config** *hostname*	指定したホスト名でシステム バックアップ モードを開始します。
ステップ 3	UCS-A /system/import-config # **enable**	インポート操作をイネーブルにします。
ステップ 4	UCS-A /system/import-config # **commit-buffer**	トランザクションをコミットします。

次に、host35 というホスト名に対しインポート操作をイネーブルにし、トランザクションをコミットする例を示します。

```
UCS-A# scope system
UCS-A /system # scope import-config host35
UCS-A /system/import-config # enable
UCS-A /system/import-config* # commit-buffer
UCS-A /system/import-config #
```

インポート操作の変更

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope import-config** *hostname*	指定したホスト名でシステムインポート コンフィギュレーション モードを開始します。
ステップ 3	UCS-A /system/import-config # **disable**	（任意） トランザクションのコミット時にインポート操作が自動的に実行されないようにするために、イネーブルになっているインポート操作をディセーブルにします。
ステップ 4	UCS-A /system/import-config # **enable**	（任意） トランザクションをコミットすると、ただちにインポート操作が自動的に実行されるようにします。
ステップ 5	UCS-A /system/import-config # **set action** {**merge** | **replace**}	（任意） インポート操作に使用する次のいずれかのアクション タイプを指定します。 • **Merge**：設定情報が既存の情報とマージされます。競合する場合、現在のシステム上の情報が、インポート設定ファイル内の情報に置き換えられます。 • **Replace**：インポート設定ファイル内の各オブジェクトが採用され、現在の設定内の対応するオブジェクトは上書きされます。
ステップ 6	UCS-A /system/import-config # **set descr** *description*	（任意） インポート操作の説明を記入します。 （注） 説明にスペース、特殊文字、または句読点が含まれている場合は、説明を引用符で括る必要があります。引用符は、show コマンド出力の説明フィールドには表示されません。
ステップ 7	UCS-A /system/import-config # **set password**	（任意） Enter キーを押すと、パスワードを入力するように促されます。

	コマンドまたはアクション	目的
		リモート サーバのユーザ名のパスワードを指定します。この手順は、TFTP プロトコルを使用する場合には適用されません。 （注） Cisco UCS Manager では、このパスワードは保存されません。したがって、インポート操作をイネーブルにしてただちに実行する場合を除き、このパスワードを入力する必要はありません。
ステップ 8	UCS-A /system/import-config # **set protocol** {**ftp** | **scp** | **sftp** | **tftp**}	（任意） リモート サーバとの通信時に使用するプロトコルを指定します。
ステップ 9	UCS-A /system/import-config # **set remote-file** *filename*	（任意） インポートする設定ファイルの名前を指定します。
ステップ 10	UCS-A /system/import-config # **set user** *username*	（任意） システムがリモート サーバへのログインに使用する必要のあるユーザ名を指定します。この手順は、TFTP プロトコルを使用する場合には適用されません。
ステップ 11	UCS-A /system/import-config # **commit-buffer**	トランザクションをコミットします。

次に、説明を追加し、host35 インポート操作のパスワード、プロトコル、およびユーザ名を変更し、トランザクションをコミットする例を示します。

```
UCS-A# scope system
UCS-A /system # scope import-config host35
UCS-A /system/import-config # set descr "This is an import operation for host35."
UCS-A /system/import-config* # set password
Password:
UCS-A /system/import-config* # set protocol sftp
UCS-A /system/import-config* # set user jforlenz32
UCS-A /system/import-config* # commit-buffer
UCS-A /system/import-config #
```

インポート操作の削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /system # **delete import-config** *hostname*	指定したホスト名のインポート操作を削除します。
ステップ 3	UCS-A /system # **commit-buffer**	トランザクションをコミットします。

次に、host35 というホスト名のインポート操作を削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope system
UCS-A /system # delete import-config host35
UCS-A /system* # commit-buffer
UCS-A /system #
```

ファブリック インターコネクトの設定の復元

バックアップ ファイルのエクスポート元のシステムと同じバージョンを実行しているシステムを復元するには、フル ステート バックアップ ファイルを使用することを推奨します。同じリリース トレインの場合でも、フル ステート バックアップを使用してシステムを復元できます。たとえば、リリース 2.1(3a) を実行しているシステムから作成したフル ステート バックアップを使用して、リリース 2.1(3f) を実行するシステムを復元できます。

VSAN または VLAN 設定の問題を回避するには、バックアップ時にプライマリ ファブリック インターコネクトであったファブリック インターコネクトでバックアップを復元する必要があります。

はじめる前に

システム コンフィギュレーションを復元するための次の情報を収集します。

- ファブリック インターコネクト管理ポートの IPv4 アドレスとサブネット マスク、または IPv6 アドレスとプレフィックス
- デフォルトのゲートウェイの IPv4 アドレスまたは IPv6 アドレス
- バックアップ サーバの IPv4 アドレスまたは IPv6 アドレスと認証クレデンシャル
- Full State バックアップ ファイルの完全修飾名

（注） システムを復元するには、Full State コンフィギュレーション ファイルへのアクセスが必要です。その他のタイプのコンフィギュレーション ファイルやバックアップ ファイルでは、システムを復元できません。

手順

ステップ 1 コンソール ポートに接続します。

ステップ 2 ファブリック インターコネクトがオフの場合はオンにします。
ファブリック インターコネクトがブートする際、Power On Self-Test のメッセージが表示されます。

ステップ 3 インストール方式プロンプトに **console** と入力します。

ステップ 4 **restore** と入力して、フル ステート バックアップから設定を復元します。

ステップ 5 **y** と入力して、フル ステート バックアップから復元することを確定します。

ステップ 6 ファブリック インターコネクトの管理ポートの IP アドレスを入力します。

ステップ 7 ファブリック インターコネクトの管理ポートのサブネット マスクを入力します。

ステップ 8 デフォルト ゲートウェイの IP アドレスを入力します。

ステップ 9 バックアップ コンフィギュレーション ファイルを取得する際に使用する、次のいずれかのプロトコルを入力します。

- **scp**
- **ftp**
- **tftp**
- **sftp**

ステップ 10 バックアップ サーバの IP アドレスを入力します。

ステップ 11 フル ステート バックアップ ファイルのフル パスおよびファイル名を入力します。

（注） バックアップ ファイルのエクスポート元となったシステムと同じバージョンを実行しているシステムを復元するために使用できるのは、Full State バックアップ ファイルのみです。

ステップ 12 バックアップ サーバにアクセスするためのユーザ名とパスワードを入力します。
ファブリック インターコネクトがバックアップ サーバにログインし、指定されたフル ステート バックアップ ファイルのコピーを取得し、システム設定を復元します。クラスタ設定の場合、セカンダリ ファブリック インターコネクトを復元する必要はありません。セカンダリ ファブリック インターコネクトがリブートすると、Cisco UCS はただちにその設定をプライマリ ファブリック インターコネクトと同期させます。

次に、FTP を使用して 20.10.20.10 のバックアップ サーバから取得された Backup.bak ファイルからシステム設定を復元する例を示します。

```
Enter the configuration method. (console/gui) ? console

Enter the setup mode; setup newly or restore from backup. (setup/restore) ? restore

NOTE:
  To configure Fabric interconnect using a backup file on a remote server,
  you will need to setup management interface.
  The management interface will be re-configured (if necessary),
  based on information stored in the backup file.
```

```
  Continue to restore this Fabric interconnect from a backup file (yes/no) ? yes

  Physical Switch Mgmt0 IPv4 address : 192.168.10.10

  Physical Switch Mgmt0 IPv4 netmask : 255.255.255.0

  IPv4 address of the default gateway : 192.168.10.1

  Enter the protocol to get backup file (scp/ftp/tftp/sftp) ?  scp
  Enter the IP address of backup server: 20.10.20.10
  Enter fully qualified backup file name: Backup.bak
  Enter user ID: user
  Enter password:
    Retrieved backup configuration file.
  Configuration file - Ok


Cisco UCS 6100 Series Fabric Interconnect
UCS-A login:
```

設定の削除

注意 必要な場合に限り設定を削除してください。設定を削除すると、設定が完全に削除され、システムが未設定の状態でリブートします。その後、バックアップ ファイルから設定を復元する必要、または初期システム セットアップを実行する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **connect local-mgmt**	ローカル管理 CLI を開始します。
ステップ 2	UCS-A(local-mgmt)# **erase configuration**	設定を削除します。 設定の削除を確認するプロンプトが表示されます。**yes** と入力すると、設定は削除され、システムが未設定の状態でリブートします。

次に、設定を削除する例を示します。

```
UCS-A# connect local-mgmt
UCS-A(local-mgmt)# erase configuration
All UCS configurations will be erased and system will reboot. Are you sure? (yes/no): yes
```

第 40 章

忘れたパスワードの復旧

この章の内容は、次のとおりです。

amin アカウントのパスワードの復旧

admin アカウントは、システム管理者またはスーパーユーザのアカウントです。アドミニストレータが admin アカウントのパスワードを失うと、重大なセキュリティ上の問題が発生する可能性があります。admin アカウントのパスワードを回復させる手順では、すべてのファブリック インターコネクトに電源を再投入する必要があり、データ伝送が一時的に停止します。

admin アカウントのパスワードを復旧する場合、実際にはそのアカウントのパスワードを変更します。admin アカウントに対応する元のパスワードを取得することはできません。

admin 以外のすべてのローカル アカウントのパスワードは、Cisco UCS Manager からリセットできます。ただし、aaa または admin 権限を持つアカウントを使用して Cisco UCS Manager にログインする必要があります。

注意 Cisco UCS Mini の場合、この手順では、Cisco UCS ドメイン 内のファブリック インターコネクトをシャーシ スロットからすべて取り外す必要があります。したがって、Cisco UCS ドメイン内のすべてのデータ送信は、ファブリック インターコネクトがシャーシ スロットに取り付け直されるまで停止します。

他の Cisco UCS 構成でこの手順を実行する場合は、すべてのファブリック インターコネクトの電源を切る必要があります。したがって、Cisco UCS ドメイン 内のすべてのデータ送信は、ファブリック インターコネクトが再起動されるまで停止します。

ファブリックインターコネクトのリーダーシップロールの決定

（注） 管理者パスワードがわからなくなった場合にクラスタ内のファブリック インターコネクトの権限を判別するには、両方のファブリック インターコネクトの IP アドレスから Cisco UCS Manager GUI を開きます。従属ファブリック インターコネクトは失敗し、次のメッセージが表示されます。

UCSM GUI はセカンダリ ノードでは使用できません。（UCSM GUI is not available on secondary node.）

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **show cluster state**	クラスタの両方のファブリック インターコネクトの動作状態およびリーダーシップ ロールを表示します。

次に、クラスタの両方のファブリックインターコネクトのリーダーシップロールを表示する例を示します。ここでは、ファブリック インターコネクト A がプライマリ ロールで、ファブリック インターコネクト B が従属ロールです。

```
UCS-A# show cluster state
Cluster Id: 0x4432f72a371511de-0xb97c000de1b1ada4

A: UP, PRIMARY
B: UP, SUBORDINATE

HA READY
```

スタンドアロン設定の admin アカウント パスワードの復旧

この手順により、ファブリック インターコネクトで初期システム セットアップの実行時に admin アカウントに設定したパスワードを復旧できます。admin アカウントは、システム管理者またはスーパーユーザのアカウントです。

はじめる前に

1 ファブリック インターコネクトのコンソール ポートを、コンピュータ ターミナルまたはコンソール サーバに物理的に接続します。

2 次のファームウェアの実行中のバージョンを確認します。

- ファブリック インターコネクトのファームウェア カーネル バージョン
- ファームウェア システム バージョン

ヒント この情報を検索するには、Cisco UCS ドメイン で任意のユーザ アカウントを使用してログインします。

手順

ステップ 1 コンソール ポートに接続します。

ステップ 2 ファブリック インターコネクトの電源を次のように再投入します。

a) Cisco UCS Mini の場合は、シャーシ スロットからファブリック インターコネクトを引き出します。それ以外の構成の場合は、ファブリック インターコネクトの電源をオフにします。

b) Cisco UCS Mini の場合は、ファブリック インターコネクトをスライドさせてシャーシ スロットに戻します。それ以外の構成の場合は、ファブリック インターコネクトの電源をオンにします。

ステップ 3 コンソールで次のいずれかのキーの組み合わせを押して、起動時に `loader` プロンプトを表示させます。

- Ctrl+l
- Ctrl+Shift+r

場合によっては、`loader` プロンプトを画面に表示する際に、選択したキーの組み合わせを複数回押す必要があります。

ステップ 4 ファブリック インターコネクトのカーネル ファームウェア バージョンをブートします。

```
loader >
boot /installables/switch/
kernel_firmware_version
```

例：

```
loader > boot /installables/switch/ucs-6100-k9-kickstart.4.1.3.N2.1.0.11.gbin

loader > boot /installables/switch/ucs-mini-k9-kickstart.5.0.3.N2.3.01a.bin
```

ステップ 5 config ターミナル モードを開始します。

```
Fabric(boot)#
config terminal
```

ステップ 6 admin パスワードをリセットします。

```
Fabric(boot)(config)#
admin-password
```

password

大文字と数字がそれぞれ 1 つ以上含まれる強力なパスワードを選択します。このパスワードは空にできません。

新しいパスワードはクリア テキスト モードで表示されます。

ステップ 7 config ターミナル モードを終了し、ブート プロンプトに戻ります。

ステップ 8 ファブリック インターコネクトのシステム ファームウェア バージョンをブートします。

```
Fabric(boot)#
load /installables/switch/
system_firmware_version
```

例：

```
Fabric(boot)# load /installables/switch/ucs-6100-k9-system.4.1.3.N2.1.0.211.bin

Fabric(boot)# load /installables/switch/ucs-mini-k9-system.5.0.3.N2.3.01a.bin
```

ステップ 9 システム イメージがロードされたら、Cisco UCS Manager にログインします。

クラスタ設定の admin アカウント パスワードの復旧

この手順により、ファブリック インターコネクトで初期システム セットアップの実行時に admin アカウントに設定したパスワードを復旧できます。admin アカウントは、システム管理者またはスーパーユーザのアカウントです。

はじめる前に

1. ファブリック インターコネクトのいずれか 1 つのコンソール ポートを、コンピュータ ターミナルまたはコンソール サーバに物理的に接続します。
2. 次の情報を入手します。
   - ファブリック インターコネクトのファームウェア カーネル バージョン
   - ファームウェア システム バージョン
   - プライマリ リーダーシップ ロールを持つファブリック インターコネクトと、従属ファブリック インターコネクト

ヒント この情報を検索するには、Cisco UCS ドメイン で任意のユーザ アカウントを使用してログインします。

手順

ステップ 1 コンソール ポートに接続します。

ステップ 2 従属ファブリック インターコネクトの場合は、次の手順を実行します。

a) Cisco UCS Mini の場合は、シャーシ スロットからファブリック インターコネクトを引き出します。それ以外の構成の場合は、ファブリック インターコネクトの電源をオフにします。

b) Cisco UCS Mini の場合は、ファブリック インターコネクトをスライドさせてシャーシ スロットに戻します。それ以外の構成の場合は、ファブリック インターコネクトの電源をオンにします。

c) コンソールで次のいずれかのキーの組み合わせを押して、起動時に `loader` プロンプトを表示させます。

- Ctrl+l
- Ctrl+Shift+r

場合によっては、`loader` プロンプトを画面に表示する際に、選択したキーの組み合わせを複数回押す必要があります。

ステップ 3 プライマリ ファブリック インターコネクトの電源を次のように再投入します。

a) Cisco UCS Mini の場合は、シャーシ スロットからファブリック インターコネクトを引き出します。それ以外の構成の場合は、ファブリック インターコネクトの電源をオフにします。

b) Cisco UCS Mini の場合は、ファブリック インターコネクトをスライドさせてシャーシ スロットに戻します。それ以外の構成の場合は、ファブリック インターコネクトの電源をオンにします。

ステップ 4 コンソールで次のいずれかのキーの組み合わせを押して、起動時に `loader` プロンプトを表示させます。

- Ctrl+l
- Ctrl+Shift+r

場合によっては、`loader` プロンプトを画面に表示する際に、選択したキーの組み合わせを複数回押す必要があります。

ステップ 5 プライマリ ファブリック インターコネクトのカーネル ファームウェア バージョンをブートします。

```
loader > boot /installables/switch/
kernel_firmware_version
```

例：

```
loader > boot /installables/switch/ucs-6100-k9-kickstart.4.1.3.N2.1.0.11.gbin

loader > boot /installables/switch/ucs-mini-k9-kickstart.5.0.3.N2.3.01a.bin
```

ステップ 6 config ターミナル モードを開始します。

```
Fabric(boot)# config terminal
```

ステップ 7 admin パスワードをリセットします。

```
Fabric(boot)(config)# admin-password password
```

大文字と数字がそれぞれ 1 つ以上含まれる強力なパスワードを選択します。このパスワードは空にできません。

新しいパスワードはクリア テキスト モードで表示されます。

ステップ 8 config ターミナル モードを終了し、ブート プロンプトに戻ります。

ステップ 9 プライマリ ファブリック インターコネクトのシステム ファームウェア バージョンをブートします。

```
Fabric(boot)# load /installables/switch/
system_firmware_version
```

例：

```
Fabric(boot)# load /installables/switch/ucs-6100-k9-system.4.1.3.N2.1.0.211.bin

Fabric(boot)# load /installables/switch/ucs-mini-k9-system.5.0.3.N2.3.01a.bin
```

ステップ 10 システム イメージがロードされたら、Cisco UCS Manager にログインします。

ステップ 11 従属ファブリック インターコネクトのコンソールで、次の手順を実行してシステムを起動します。

a) 従属ファブリック インターコネクトのカーネル ファームウェア バージョンをブートします。

```
loader > boot /installables/switch/
kernel_firmware_version
```

b) 従属ファブリック インターコネクトのシステム ファームウェア バージョンをブートします。

```
Fabric(boot)# load /installables/switch/
system_firmware_version
```