Cisco UCS B シリーズ GUI ファームウェア管理ガイド リリース 2.2

初版：2013 年 12 月 11 日

最終更新：2016 年 07 月 13 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	説明
GUI 要素	タブの見出し、領域名、フィールドのラベルのようなGUI要素は、[GUI 要素] のように示しています。 ウィンドウ、ダイアログボックス、ウィザードのタイトルのようなメイン タイトルは、**[メイン タイトル]** のように示しています。
マニュアルのタイトル	マニュアルのタイトルは、イタリック体（*italic*）で示しています。

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

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

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

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

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

警告 IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger.You are in a situation that could cause bodily injury.Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Cisco UCS の関連ドキュメント

ドキュメント ロードマップ

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

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

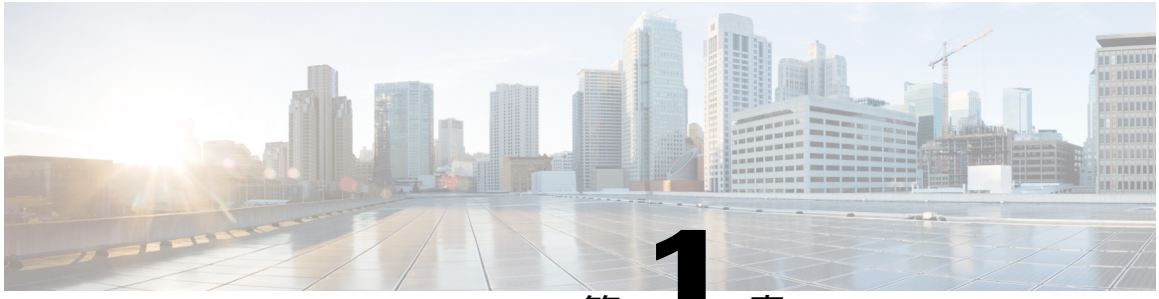
管理用の UCS Manager と統合されたラック サーバでサポートされるファームウェア バージョンとサポートされる UCS Manager バージョンについては、『Release Bundle Contents for Cisco UCS Software』を参照してください。

その他のマニュアル リソース

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

マニュアルに関するフィードバック

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



第 1 章

概要

この章は、次の項で構成されています。

ファームウェアの概要

Cisco UCS では、シスコから取得し、シスコによって認定されたファームウェアを使用して、Cisco UCS ドメインのエンドポイントをサポートします。各エンドポイントは、ファームウェアが機能するために必要となる Cisco UCS ドメインのコンポーネントです。Cisco UCS ドメインのエンドポイントのアップグレード順序は、アップグレード パスによって異なります。次の項目が含まれます。

- Cisco UCS Manager
- I/O モジュール
- ファブリック インターコネクト

- NIC や HBA ファームウェア、サービス プロファイルに含まれているファームウェア パッケージを使用してアップグレードできるオプション ROM（該当する場合）など、アダプタ上に物理的に存在するエンドポイント
- サービス プロファイルに含まれているファームウェア パッケージを使用してアップグレードできる BIOS、ストレージ コントローラ（RAID コントローラ）、Cisco Integrated Management Controller（CIMC）など、サーバ上に物理的に存在するエンドポイント

Cisco UCS ドメインのエンドポイントをアップグレードする適切な順序を確認するには、アップグレード パスに必要な手順の順序を参照してください。

（注） Cisco UCS リリース 1.4(1) 以降では、シスコは 1 つの大きなファームウェア パッケージではなく、複数のバンドルでファームウェア アップグレードをリリースしています。詳細については、ファームウェア イメージの管理, （49 ページ）を参照してください。

シスコでは、このマニュアルおよびテクニカル ノート『Unified Computing System Firmware Management Best Practices』において、ファームウェア イメージおよびファームウェア アップデートを管理するための一連のベスト プラクティスを保持しています。

このマニュアルでは、ファームウェアの管理について、次の定義を使用しています。

アップグレード

エンドポイントで実行しているファームウェアを、リリースやパッチなどの他のイメージに変更します。アップグレードには、アップデートとアクティベーションが含まれます。

Update

ファームウェア イメージをエンドポイントのバックアップ パーティションにコピーします。

アクティブ化

バックアップ パーティションのファームウェアをエンドポイントのアクティブなファームウェア バージョンとして設定します。アクティベーションには、エンドポイントのリブートが必要な場合やリブートが発生する場合があります。

Management Extension および機能カタログのアップグレードの場合は、アップデートとアクティブ化が同時に行われます。このようなアップグレードについては、アップデートまたはアクティブ化のいずれかのみを実行する必要があります。両方の手順を実行する必要はありません。

バージョンをまたがるファームウェアのサポート

Cisco UCS はバージョンをまたがるファームウェアをサポートしています。サーバ（ホスト ファームウェア（FW）、BIOS、CIMC、アダプタ FW およびドライバ）で以前のリリースの B バンドルまたは C バンドルと同時に使用できる Cisco UCS Manager A バンドル ソフトウェア（Cisco UCS Manager、Cisco NX-OS、IOM のファームウェア）については、該当するリリースの『Release Notes for Cisco UCS Software（Cisco UCS ソフトウェアのリリース ノート）』を参照してください。

Cisco UCSM リリース 2.2以降では、アダプタのファームウェア バージョンが Cisco UCSM のリリース バージョンと異なります。

重要 バージョンをまたがるファームウェアを設定する場合は、サーバのエンドポイントのファームウェアのバージョンが Cisco UCS ドメインの設定に対応するようにする必要があります。

FI クラスタ用のファームウェア自動同期

クラスタを構成するために、セカンダリ ファブリック インターコネクトを交換、またはスタンバイから HA への変換として追加するには、インフラストラクチャ バンドルのファームウェアのバージョンが一致する必要があります。管理者は現在、交換 FI を適切なバージョンに手動でアップグレードまたはダウングレードしてからクラスタに接続しています。ファームウェア自動同期を使用すると、交換 FI がスタンバイとして HA に追加されるときに、そのインフラストラクチャ バンドルを存続 FI と同じバージョンに自動的にアップグレードまたはダウングレードできます。ソフトウェア パッケージは、FI に存在する UCS ソフトウェアまたはファームウェアです。

ソフトウェアおよびハードウェアの要件

存続 FI 上のソフトウェア パッケージは、Cisco UCS リリース 1.4 以降である必要があります。ファブリック インターコネクトのモデル番号も同様です。たとえば、ファームウェア自動同期は、HA 用に設定されている 61XX および 62XX FI モデルの組み合わせの場合はトリガーされません。

実装

以前の実装では、ソフトウェア パッケージのバージョンに不一致が存在する場合、交換 FI を強制的にスタンドアロン モードとして設定します。交換 FI は、通常のアップグレードまたはダウングレード プロセスで、存続 FI 上のソフトウェア パッケージと同じバージョンに手動でアップグレードまたはダウングレードされます。次に、交換 FI がクラスタに追加されます。これは、交換 FI のアップグレードまたはダウングレードは手動プロセスであるからです。

現在のオプションに加えて、交換 FI のソフトウェア パッケージを存続 FI と同期するためのオプションが追加されました。ユーザがファームウェアを自動同期する場合、存続 FI のソフトウェア パッケージが交換 FI にコピーされます。次に、交換 FI のソフトウェア パッケージがアクティブになり、交換 FI がクラスタに追加されます。Cisco UCSM データベースと設定の同期は、HA クラスタが正常に構成されると通常のメカニズムによって発生します。

ファームウェア自動同期の利点

UCS クラスタ内の 1 つのファブリック インターコネクトで障害が発生した場合、自動同期の機能により、交換 FI のソフトウェア パッケージのリビジョンが存続 FI と同じになります。このプロセスでは、エンド ユーザは最小限の対話で、明確かつ簡潔なフィードバックを実行中に得ることができます。

ファームウェア アップグレードのオプション

Cisco UCS ファームウェアは、次の複数の方式によってアップグレードできます。

（注） 1 つ以上の Cisco UCS ドメインを、あるリリースから別のリリースにアップグレードするために実行するステップと必要な順序については、そのアップグレードパスの『Cisco UCS upgrade guide』を参照してください。特定のリリースからのアップグレードのためのアップグレードガイドが提供されていない場合は、そのリリースからの直接のアップグレードがサポートされていない場合があるため、Cisco Technical Assistance Center にお問い合わせください。

Cisco UCS Manager による Cisco UCS ドメインのアップグレード

そのドメインの Cisco UCS Manager を使用して Cisco UCS ドメインをアップグレードする場合は、次のいずれかのアップグレード オプションを選択できます。

- 自動インストールによるインフラストラクチャとサーバのアップグレード：このオプションでは、最初の段階ですべてのインフラストラクチャ コンポーネントをアップグレードします。次の段階で、ホスト ファームウェア パッケージを使用してすべてのサーバ エンドポイントをアップグレードできます。
- サービス プロファイルのファームウェア パッケージを使用してサーバをアップグレード：このオプションを使用すると 1 回のステップですべてのサーバのエンドポイントをアップグレードできるため、サーバのリブートによる中断時間を短くすることができます。サービスプロファイルの更新の延期導入とこのオプションを組み合わせて、スケジュールされたメンテナンス ウィンドウ時にサーバのリブートが行われるようにすることができます。
- インフラストラクチャおよびサーバのエンドポイントの直接アップグレード：このオプションでは、ファブリック インターコネクト、I/O モジュール、アダプタ、ボード コントローラなど、多数のインフラストラクチャとサーバのエンドポイントを直接アップグレードできます。ただし、直接アップグレードは、サーバ BIOS、ストレージ コントローラ、HBA ファームウェア、HBA オプション ROM、ローカル ディスクなど、すべてのエンドポイントで利用できるわけではありません。それらのエンドポイントは、サーバに関連付けられているサービスプロファイルに含まれているホストファームウェアパッケージによって、アップグレードする必要があります。

Cisco UCS Central による Cisco UCS ドメインのアップグレード

1 つ以上の Cisco UCS ドメインを Cisco UCS Central に登録している場合は、Cisco UCS Central を使用してドメイン内のすべてのファームウェアのコンポーネントを管理およびアップグレードできます。このオプションを使用すると、ファームウェア アップグレードの制御を集中化して、データセンターのすべての Cisco UCS ドメインを必要なレベルにすることができます。

Cisco UCS Central を使用すると、グローバルなファームウェア管理向けに設定されたすべての登録済み Cisco UCS ドメインの機能カタログ、インフラストラクチャ、およびサーバのエンドポイントをアップグレードできます。

自動インストールによるファームウェアアップグレード

自動インストールでは、次の 2 つの段階によって、Cisco UCS ドメインを 1 つのパッケージに含まれるファームウェア バージョンにアップグレードすることができます。

- インフラストラクチャ ファームウェアのインストール：Cisco UCS インフラストラクチャ ソフトウェア バンドルを使用して、ファブリック インターコネクト、I/O モジュール、Cisco UCS Manager などのインフラストラクチャ コンポーネントをアップグレードすることができます。
- サーバ ファームウェアのインストール：Cisco UCS B シリーズ ブレード サーバ ソフトウェア バンドルを使用して Cisco UCS ドメインのすべてのブレード サーバをアップグレードする、または Cisco UCS C シリーズ ラックマウント UCS 管理対象サーバ ソフトウェア バンドルを使用してすべてのラック サーバをアップグレードすることができます。

この 2 つの段階は独立したものであり、異なる時刻に実行することや、実行されるようにスケジュールすることができます。

自動インストールを使用して、インフラストラクチャ コンポーネントを Cisco UCS のあるバージョンに、またサーバ コンポーネントを異なるバージョンにアップグレードすることができます。

（注） ドメイン内の Cisco UCS Manager が Cisco UCS 2.1(1) より前のリリースである場合は、自動インストールを使用して、Cisco UCS ドメイン内のインフラストラクチャまたはサーバをアップグレードすることはできません。ただし、Cisco UCS Manager をリリース 2.1(1) 以降にアップグレードすると、自動インストールを使用して、ファームウェア レベルの最低要件を満たしている Cisco UCS ドメイン内の他のコンポーネントをアップグレードできます。詳細については、「自動インストールによるアップグレードに関する注意、ガイドライン、および制約事項，（28 ページ）」および該当する『Cisco UCS アップグレード ガイド』を参照してください。

インフラストラクチャ ファームウェアのインストール

インフラストラクチャ ファームウェアのインストール では、Cisco UCS Manager など、Cisco UCS ドメイン内のすべてのインフラストラクチャコンポーネントと、すべてのファブリックインターコネクトおよび I/O モジュールをアップグレードします。すべてのコンポーネントが、選択した Cisco UCS インフラストラクチャ ソフトウェア バンドルに含まれるファームウェア バージョンにアップグレードされます。

インフラストラクチャ ファームウェアのインストール では、Cisco UCS ドメイン ドメイン内の一部のインフラストラクチャ コンポーネントだけを対象とする部分アップグレードはサポートしていません。

メンテナンス ウィンドウに対応する特定の時刻にインフラストラクチャのアップグレードをスケジュールできます。ただし、インフラストラクチャのアップグレードが進行中の場合、別のインフラストラクチャのアップグレードをスケジュールすることはできません。次のアップグレードをスケジューリングするには、現在のアップグレードが完了するまで待つ必要があります。

（注） インフラストラクチャ ファームウェア アップグレードが今後行われる予定の場合は、キャンセルできます。ただし、インフラストラクチャ ファームウェア アップグレードがいったん開始すると、キャンセルすることはできません。

サーバ ファームウェアのインストール

サーバファームウェアのインストールでは、ホストファームウェアパッケージを使用して、Cisco UCS ドメイン内のすべてのサーバおよびコンポーネントをアップグレードします。サービスプロファイルに選択したホストファームウェアパッケージが含まれているサーバは、次のように、選択したソフトウェア バンドルのファームウェア バージョンにすべてアップグレードされます。

- シャーシ内のすべてのブレードサーバ用の Cisco UCS B シリーズブレードサーバ ソフトウェア バンドル。
- 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用の Cisco UCS C シリーズ ラックマウント UCS 管理対象サーバ ソフトウェア バンドル。

（注） Install Server Firmware ウィザードの設定が完了した後で、サーバ ファームウェアのアップグレード プロセスをキャンセルすることはできません。Cisco UCS Manager は、変更を即座に反映します。ただし、サーバが実際にリブートされるタイミングは、サーバに関連付けられたサービス プロファイル内のメンテナンス ポリシーによって異なります。

サービスプロファイルのファームウェアパッケージによるファームウェア アップグレード

サービス プロファイル内のファームウェア パッケージを使用して、サーバの BIOS など、サーバおよびアダプタのファームウェアをアップグレードできます。ホストファームウェアポリシーを定義して、これをサーバに関連付けられているサービス プロファイルにインクルードします。

デフォルトのホスト ファームウェア パックが更新され、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、サーバがリブートされ、新しいファームウェアが適用されます。この動作は、新たに検出されたサーバのみが対象であるため、ファームウェア自動同期サーバ ポリシーによって管理されません。

サービス プロファイルによって、I/O モジュール、ファブリック インターコネクト、または Cisco UCS Manager のファームウェアをアップグレードすることはできません。それらのエンドポイントのファームウェアは直接アップグレードする必要があります。

（注） Cisco UCS は、新しい管理ファームウェア パッケージの作成をサポートしなくなりました。必要な場合は、既存の管理ファームウェア パッケージを変更および更新することができます。ただし、管理ファームウェア パッケージをすべてのサービス プロファイルから削除し、ホスト ファームウェア パッケージを使用してサーバ上の Cisco Integrated Management Controller（CIMC）を更新することをお勧めします。

ホスト ファームウェア パッケージ

このポリシーでは、ホスト ファームウェア パッケージ（ホスト ファームウェア パック）を構成するファームウェア バージョンのセットを指定することができます。ホスト ファームウェア パッケージには、次のサーバおよびアダプタ エンドポイントのファームウェアが含まれています。

- アダプタ
- サーバ BIOS
- CIMC
- ボード コントローラ
- Flexフラッシュ コントローラ
- グラフィックス カード
- ホスト HBA
- ホスト HBA オプション ROM
- ホスト NIC
- ホスト NIC オプション ROM
- ローカル ディスク

（注） ローカルディスクは、デフォルトでホスト ファームウェア パックから除外されます。

ローカル ディスク ファームウェアを更新するには、ホスト ファームウェア パッケージにブレード パッケージを必ず含めます。ブレード パッケージには、ブレード サーバとラック サーバのローカル ディスク ファームウェアが含まれています。

- PSU

- SAS エクスパンダ
- RAID コントローラ
- ストレージ コントローラのオンボード デバイス
- ストレージ コントローラのオンボード デバイス Cpld
- ストレージ デバイスのブリッジ

メモ ブレードまたはラック サーバのローカル ディスク ファームウェアを更新するには、ホスト ファームウェア パッケージにブレード パッケージを必ず含めます。ブレード パッケージには、ブレード サーバとラック サーバの両方のローカル ディスク ファームウェアが含まれています。

ヒント 同じホスト ファームウェア パッケージに複数のファームウェアを含めることができます。たとえば、1 つのホスト ファームウェア パッケージで BIOS ファームウェアとストレージ コントローラ ファームウェアの両方を使用したり、異なる 2 つのアダプタのモデル用のアダプタ ファームウェアを使用することができます。ただし、同じ種類、ベンダー、モデル番号に対しては 1 つのファームウェア バージョンしか使用できません。システムはエンドポイントで必要なファームウェア バージョンを認識し、それ以外のファームウェア バージョンは無視します。

また、新しいホスト ファームウェア パッケージを作成するとき、または既存のホスト ファームウェア パッケージを変更するときに、ホスト ファームウェア パッケージから特定のコンポーネントのファームウェアを除外できます。たとえば、ホスト ファームウェア パッケージによって RAID コントローラ ファームウェアをアップグレードしない場合は、ファームウェア パッケージ コンポーネントのリストから RAID コントローラ ファームウェアを除外できます。

（注） 各ホスト ファームウェア パッケージは、すべてのファームウェア パッケージ（ブレードおよびラック）に共通の除外されたコンポーネントの1つのリストに関連付けられます。ファームウェア パッケージ タイプごとに別の除外リストを設定するには、別のホスト ファームウェア パッケージを使用します。

ファームウェアパッケージは、このポリシーが含まれ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にプッシュされます。

このポリシーにより、同じポリシーを使用しているサービス プロファイルが関連付けられているすべてのサーバでホストファームウェアが同一となります。したがって、サービスプロファイルをあるサーバから別のサーバに移動した場合でも、ファームウェア バージョンはそのまま変わりません。さらに、ファームウェアパッケージのエンドポイントのファームウェアバージョンを変更した場合、その影響を受けるサービス プロファイルすべてに新しいバージョンが適用されます。この結果、サーバがリブートされることがあります。

このポリシーはサービス プロファイルにインクルードする必要があります。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。

このポリシーは他のどのポリシーにも依存していません。しかし、ファブリック インターコネクトに適切なファームウェアがダウンロードされていることを確認する必要があります。Cisco UCS Manager によりサーバとサービス プロファイルの関連付けが実行される際にファームウェア イメージが使用できない場合、Cisco UCS Manager はファームウェア アップグレードを無視し、関連付けを終了します。

管理ファームウェア パッケージ

（注） Cisco UCS は、新しい管理ファームウェア パッケージの作成をサポートしなくなりました。必要な場合は、既存の管理ファームウェア パッケージを変更および更新することができます。ただし、管理ファームウェア パッケージをすべてのサービス プロファイルから削除し、ホスト ファームウェア パッケージを使用してサーバ上の Cisco Integrated Management Controller（CIMC）を更新することをお勧めします。

このポリシーでは、管理ファームウェア パッケージ（管理ファームウェア パック）を構成するファームウェアバージョンのセットを指定することができます。管理ファームウェアパッケージには、サーバの Cisco Integrated Management Controller（CIMC）が含まれています。CIMC を直接アップグレードする場合は、このパッケージを使用する必要はありません。

ファームウェアパッケージは、このポリシーが含まれ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にプッシュされます。このポリシーにより、同じポリシーを使用しているサービス プロファイルに関連付けられているすべてのサーバで CIMC ファームウェアが同一となります。したがって、サービスプロファイルをあるサーバから別のサーバに移動した場合でも、ファームウェア バージョンはそのまま変わりません。

このポリシーはサービス プロファイルにインクルードする必要があります。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。

このポリシーは他のどのポリシーにも依存していません。しかし、ファブリック インターコネクトに適切なファームウェアがダウンロードされていることを確認する必要があります。

サービスプロファイルのファームウェアパッケージを使用したファームウェアのアップグレードのステージ

サービス プロファイルのホスト ファームウェア パッケージ ポリシーを使用して、サーバおよびアダプタ ファームウェアをアップグレードすることができます。

注意 メンテナンス ウィンドウを設定およびスケジュールしている場合を除き、エンドポイントを追加するか既存のエンドポイントのファームウェア バージョンを変更してホスト ファームウェア パッケージを変更した場合は、変更を保存するとすぐに Cisco UCS Manager によって、エンドポイントがアップグレードされます。そのファームウェア パッケージに関連付けられているすべてのサーバがリブートされるため、サーバ間のデータ トラフィックが中断します。

新しいサービス プロファイル

新しいサービス プロファイルの場合、このアップグレードは次のステージで行われます。

ファームウェア パッケージ ポリシーの作成

このステージでは、ホスト ファームウェア パッケージを作成します。

サービス プロファイルのアソシエーション

このステージで、サービス プロファイルにファームウェア パッケージを含め、サービス プロファイルとサーバとの関連付けを形成します。システムによって、選択したファームウェア バージョンがエンドポイントにプッシュされます。サーバをリブートし、ファームウェア パッケージで指定したバージョンがエンドポイントで確実に実行されるようにします。

既存のサービス プロファイル

サーバと関連付けられているサービスプロファイルの場合は、メンテナンス ウィンドウを設定およびスケジュールしている場合を除いて、ファームウェア パッケージへの変更を保存するとすぐに Cisco UCS Manager によってファームウェアがアップグレードされ、サーバがリブートされます。メンテナンス ウィンドウを設定およびスケジュールしている場合は、Cisco UCS Manager によってその時間までアップグレードとサーバのリブートが延期されます。

サービス プロファイルのファームウェア パッケージに対するアップデートの影響

サービスプロファイルのファームウェアパッケージを使用してファームウェアをアップデートするには、パッケージ内のファームウェアをアップデートする必要があります。ファームウェア パッケージへの変更を保存した後の動作は、Cisco UCS ドメインの設定によって異なります。

次の表に、サービスプロファイルのファームウェアパッケージを使用するサーバのアップグレードに対する最も一般的なオプションを示します。

サービス プロファイル	メンテナンス ポリシー	アップグレード処理
ファームウェア パッケージがサービス プロファイルまたはアップデート中のサービス プロファイル テンプレートに含まれていない。 または 既存のサービス プロファイルまたはアップデート中のサービスプロファイルテンプレートを変更せずにファームウェアをアップグレードする。	メンテナンス ポリシーなし	ファームウェア パッケージのアップデート後に、次のいずれかを実行します。 • 一部のサーバまたはすべてのサーバを同時にリブートおよびアップグレードするには、サーバに関連付けられている1つ以上のサービスプロファイルまたはアップデート中のサービス プロファイル テンプレートにファームウェア パッケージを追加します。 • 一度に 1 台のサーバをリブートおよびアップグレードするには、各サーバに対して次の手順を実行します。 **1** 新しいサービス プロファイルを作成し、そのサービス プロファイルにファームウェア パッケージを含めます。 **2** サービス プロファイルからサーバの関連付けを解除します。 **3** サーバを新規サービス プロファイルと関連付けます。 **4** サーバがリブートされ、ファームウェアがアップグレードされた後に、新規サービス プロファイルからサーバの関連付けを解除し、このサーバを元のサービス プロファイルに関連付けます。 **注意** 元のサービス プロファイルにスクラブ ポリシーが含まれている場合は、サービス プロファイルの関連付けを解除すると、ディスクまたはBIOSが新規サービス プロファイルに関連してスクラビング処理されるときにデータが失われることがあります。

サービス プロファイル	メンテナンス ポリシー	アップグレード処理
ファームウェア パッケージが 1 つ以上のサービス プロファイルに含まれており、このサービス プロファイルが 1 つ以上のサーバに関連付けられている。 または ファームウェア パッケージがアップデート中のサービス プロファイルテンプレートに含まれており、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 1 つ以上のサーバに関連付けられている。	メンテナンス ポリシーなし または 即時アップデート用に設定されたメンテナンス ポリシー。	ファームウェア パッケージをアップデートすると、次のようになります。 **1** ファームウェア パッケージの変更は、保存と同時に有効になります。 **2** Cisco UCS によって、このポリシーをインクルードしているサービス プロファイルに関連付けられているすべてのサーバに照らして、モデル番号とベンダーが検証されます。モデル番号とベンダーがポリシーのファームウェア バージョンと一致する場合は、Cisco UCS によりサーバがリブートされ、ファームウェアがアップデートされます。 ファームウェア パッケージを含むサービス プロファイルに関連付けられているすべてのサーバが同時にリブートされます。

サービス プロファイル	メンテナンス ポリシー	アップグレード処理
ファームウェア パッケージが 1 つ以上のサービス プロファイルに含まれており、このサービス プロファイルが 1 つ以上のサーバに関連付けられている。 または ファームウェア パッケージがアップデート中のサービスプロファイルテンプレートに含まれており、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 1 つ以上のサーバに関連付けられている。	ユーザ確認応答に関して設定済み	ファームウェア パッケージをアップデートすると、次のようになります。 **1** Cisco UCS によって、変更を確認するように要求され、ユーザ確認応答済みのサーバのリブートが必要であることが通知されます。 **2** 点滅している [Pending Activities] ボタンをクリックし、リブートして新規ファームウェアを適用するサーバを選択します。 **3** Cisco UCS によって、このポリシーをインクルードしているサービス プロファイルに関連付けられているすべてのサーバに照らして、モデル番号とベンダーが検証されます。モデル番号とベンダーがポリシーのファームウェア バージョンと一致する場合は、Cisco UCS によりサーバがリブートされ、ファームウェアがアップデートされます。 サーバを手動でリブートしても、Cisco UCS によってファームウェア パッケージが適用されたり、保留中のアクティビティがキャンセルされることはありません。[Pending Activities] ボタンを使用して、保留中のアクティビティを確認応答するか、またはキャンセルする必要があります。

サービス プロファイル	メンテナンス ポリシー	アップグレード処理
ファームウェア パッケージが 1 つ以上のサービス プロファイルに含まれており、このサービス プロファイルが 1 つ以上のサーバに関連付けられている。 または ファームウェア パッケージがアップデート中のサービスプロファイルテンプレートに含まれており、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 1 つ以上のサーバに関連付けられている。	特定のメンテナンスウィンドウ時に有効になる変更に関して設定済み。	ファームウェアパッケージをアップデートすると、次のようになります。 1 Cisco UCS によって、変更を確認するように要求され、ユーザ確認応答済みのサーバのリブートが必要であることが通知されます。 2 点滅している [Pending Activities] ボタンをクリックし、リブートして新規ファームウェアを適用するサーバを選択します。 3 Cisco UCS によって、このポリシーをインクルードしているサービス プロファイルに関連付けられているすべてのサーバに照らして、モデル番号とベンダーが検証されます。モデル番号とベンダーがポリシーのファームウェア バージョンと一致する場合は、Cisco UCS によりサーバがリブートされ、ファームウェアがアップデートされます。 サーバを手動でリブートしても、Cisco UCS によってファームウェアパッケージが適用されたり、スケジュールされたメンテナンスアクティビティがキャンセルされることはありません。

Cisco UCS Central のファームウェア管理

Cisco UCS Central を使用すると、登録されているすべての Cisco UCS ドメインのすべてのファームウェア コンポーネントを管理することができます。

（注） Cisco UCS Central から Cisco UCS ドメインのファームウェアを管理するには、Cisco UCS Manager でグローバル ファームウェア管理オプションをイネーブルにする必要があります。グローバル ファームウェア管理オプションは、Cisco UCS Manager を Cisco UCS Central に登録するときにイネーブルにできます。また、管理要件に基づいてグローバル管理オプションのオン/オフを切り替えることもできます。

Cisco UCS ドメインは、Cisco UCS Central のドメイン グループに管理目的で分類されます。ファームウェアは、ドメイン グループ レベルで各ドメイン グループごとに別個に管理することも、ドメイン グループのルートからドメイン グループ全体に対して管理することもできます。Cisco UCS Central には、次の Cisco UCS ドメインのファームウェア パッケージを管理するオプションがあります。

- **機能カタログ**：ドメイン グループごとに機能カタログを 1 つ使用します。特定のドメイン グループに登録されたすべての Cisco UCS ドメインによって、ドメイン グループで定義された機能カタログが使用されます。
- **インフラストラクチャ ファームウェア**：ドメイン グループごとにインフラストラクチャ ファームウェア ポリシーを 1 つ使用します。特定のドメイン グループに登録されたすべての Cisco UCS ドメインによって、ドメイン グループで定義された同じインフラストラクチャ ファームウェア バージョンが使用されます。
- **ホスト ファームウェア**：ドメイン グループ内のさまざまなホスト ファームウェア コンポーネントに対して、複数のホスト ファームウェア ポリシーを設定できます。ドメイン グループに登録されている Cisco UCS ドメインでは、グループに定義されているホスト ファームウェア ポリシーを選択できます。Cisco UCS Central には、ドメイン グループのすべての Cisco UCS ドメインにホスト ファームウェアを同時にグローバルにアップグレードするオプションがあります。

エンドポイントでの直接のファームウェアのアップグレード

正しい手順に従って、正しい順序でアップグレードを適用すれば、エンドポイントの直接のファームウェア アップグレードと新しいファームウェア バージョンのアクティブ化による、Cisco UCS ドメインのトラフィックの中断を最小限に留めることができます。

次のエンドポイントのファームウェアを直接アップグレードできます。

- アダプタ
- CIMC
- I/O モジュール
- ボード コントローラ
- Cisco UCS Manager
- ファブリック インターコネクト

アダプタおよびボード コントローラ ファームウェアも、サービス プロファイル内のホスト ファームウェア パッケージによってアップグレードできます。ホスト ファームウェア パッケージを使用して、このファームウェアをアップグレードする場合、ファームウェアのアップグレード プロセス中に、サーバをリブートする必要がある回数を削減できます。

（注） 管理ファームウェア パッケージによる CIMC のアップグレードまたは、サーバに関連付けられたサービス プロファイル内のファームウェア パッケージによるアダプタのアップグレードは、直接のファームウェア アップグレードより優先されます。サーバに関連付けられたサービス プロファイルにファームウェア パッケージが含まれる場合、エンドポイントを直接アップグレードすることはできません。直接のアップグレードを実行するには、サービスプロファイルからファームウェア パッケージを削除する必要があります。

直接のファームウェア アップグレードのステージ

Cisco UCS Manager は直接アップグレードのプロセスを 2 つのステージに分け、サーバやその他のエンドポイントのアップタイムに影響を与えずに、システムの実行中にエンドポイントにファームウェアをプッシュできるようにします。

アップデート

このステージでは、選択したファームウェア バージョンがプライマリ ファブリック インターコネクトから、エンドポイントのバックアップ パーティションにコピーされ、ファームウェア イメージが破損していないことが確認されます。アップデートプロセスでは、常にバックアップ スロットのファームウェアが上書きされます。

アップデート ステージは、次のエンドポイントにのみ適用されます。

- アダプタ
- CIMC
- I/O モジュール

アクティブ化

このステージでは、指定したイメージバージョン（通常はバックアップバージョン）がスタートアップ バージョンとして設定され、[Set Startup Version Only] を指定していない場合、エンドポイントがただちにリブートされます。エンドポイントがリブートされると、バックアップ パーティションがアクティブなパーティションになり、アクティブなパーティションがバックアップ パーティションになります。新しいアクティブなパーティションのファームウェアはスタートアップバージョンおよび実行されているバージョンになります。

指定したファームウェア イメージがすでにエンドポイントに存在するため、次のエンドポイントのみアクティベーションが必要です。

- Cisco UCS Manager
- ファブリック インターコネクト
- それらをサポートするサーバ上のボード コントローラ

ファームウェアをアクティブにすると、エンドポイントがリブートされ、新しいファームウェアがアクティブなカーネル バージョンおよびシステム バージョンになります。スタートアップ ファームウェアからエンドポイントをブートできない場合、デフォルトがバックアップ バージョンに設定され、エラーが生成されます。

注意 I/O モジュールに対して [Set Startup Version Only] を設定した場合、そのデータ パス内のファブリック インターコネクトがリブートされると、I/O モジュールがリブートされます。I/O モジュールに対して、[Set Startup Version Only] を設定しない場合、I/O モジュールがリブートし、トラフィックが中断します。また、Cisco UCS Manager がファブリック インターコネクトと I/O モジュールの間のプロトコルとファームウェア バージョンの不一致を検出した場合、Cisco UCS Manager は、ファブリック インターコネクトのファームウェアに一致するファームウェア バージョンを使用して I/O モジュールを自動的に更新し、ファームウェアをアクティブ化して、I/O モジュールを再度リブートします。

直接のファームウェア アップグレードの停止の影響

エンドポイントで、直接のファームウェア アップグレードを実行する場合、Cisco UCS ドメインで、1 つ以上のエンドポイントでトラフィックの中断や、停止が発生することがあります。

ファブリック インターコネクト ファームウェア アップグレードの停止の影響

ファブリック インターコネクトのファームウェアをアップグレードする場合、次の停止の影響や中断が発生します。

- ファブリック インターコネクトがリブートします。
- 対応する I/O モジュールがリブートします。

Cisco UCS Manager ファームウェア アップグレードの停止の影響

Cisco UCS Manager へのファームウェア アップグレードにより、次の中断が発生します。

- Cisco UCS Manager GUI：Cisco UCS Manager GUI にログインしているすべてのユーザがログアウトされ、それらのセッションが終了します。

  実行中の保存されていない作業が失われます。
- Cisco UCS Manager CLI：telnet によってログインしているすべてのユーザがログアウトされ、それらのセッションが終了します。

I/O モジュール ファームウェア アップグレードの停止の影響

I/O モジュールのファームウェアをアップグレードする場合、次の停止の影響と中断が発生します。

- 単一のファブリック インターコネクトのスタンドアロン設定の場合、I/O モジュールのリブート時にデータ トラフィックが中断されます。2 つのファブリック インターコネクトのクラス

タ設定の場合、データ トラフィックは他方の I/O モジュールおよびそのデータ パス内のファブリック インターコネクトにフェールオーバーします。

- 新しいファームウェアをスタートアップ バージョンとしてのみアクティブにした場合、対応するファブリック インターコネクトがリブートされると、I/O モジュールがリブートします。
- 新しいファームウェアを実行されているバージョンおよびスタートアップ バージョンとしてアクティブにした場合、I/O モジュールがただちにリブートします。
- ファームウェアのアップグレード後に、I/O モジュールを使用できるようになるまで最大 10 分かかります。

CIMC ファームウェア アップグレードの停止の影響

サーバの CIMC のファームウェアをアップグレードした場合、CIMC と内部プロセスのみが影響を受けます。サーバ トラフィックは中断しません。このファームウェア アップグレードにより、CIMC に次の停止の影響と中断が発生します。

- KVM コンソールおよび vMedia によってサーバで実行されているすべてのアクティビティが中断されます。
- すべてのモニタリングおよび IPMI ポーリングが中断されます。

アダプタ ファームウェア アップグレードの停止の影響

アダプタのファームウェアをアクティブにし、[Set Startup Version Only] オプションを設定していない場合、次の停止の影響と中断が発生します。

- サーバがリブートします。
- サーバ トラフィックが中断します。

ファームウェア バージョン

使用されるファームウェア バージョンの用語は、次のようなエンドポイントのタイプによって異なります。

CIMC、I/O モジュール、およびアダプタのファームウェア バージョン

各 CIMC、I/O モジュール、およびアダプタには、フラッシュにファームウェア用の 2 つのスロットがあります。各スロットに 1 つのバージョンのファームウェアを装着します。1 つのスロットはアクティブで、他方のスロットはバックアップ スロットです。コンポーネントは、アクティブとして指定されているスロットからブートします。

Cisco UCS Manager では次のファームウェア バージョンの用語が使われます。

Running Version

実行されているバージョンは、アクティブで、エンドポイントで使用されているファームウェアです。

Startup Version

スタートアップ バージョンは、エンドポイントの次回のブート時に使用されるファームウェアです。Cisco UCS Manager はアクティベーション操作によって、スタートアップ バージョンを変更します。

バックアップ バージョン

バックアップ バージョンは、他方のスロットのファームウェアで、エンドポイントによって使用されていません。このバージョンは、エンドポイントをアップデートしたが、まだアクティブにしていないファームウェアか、または最近アクティブ化されたバージョンによって交換された古いファームウェア バージョンなどです。Cisco UCS Manager はアップデート操作によって、バックアップ スロットのイメージを置き換えます。

スタートアップバージョンからエンドポイントをブートできない場合、バックアップバージョンからブートします。

ファブリック インターコネクトおよび Cisco UCS Manager のファームウェア バージョン

アクティブにできるのは、ファブリックインターコネクトのファームウェアとファブリックインターコネクト上の Cisco UCS Manager だけです。すべてのイメージがファブリック インターコネクトに保存されるため、ファブリック インターコネクトおよび Cisco UCS Manager ファームウェアにはバックアップバージョンがありません。その結果、ブート可能ファブリックインターコネクト イメージは、サーバ CIMC とアダプタのように、2 つに制限されません。代わりに、ブート可能ファブリック インターコネクト イメージは、ファブリック インターコネクトのメモリの空き領域と、そこに保存されるイメージの数によって制限されます。

ファブリック インターコネクトおよび Cisco UCS Manager ファームウェアには、カーネル ファームウェアとシステム ファームウェアの実行されているバージョンとスタートアップ バージョンがあります。カーネル ファームウェアとシステム ファームウェアは、同じバージョンのファームウェアを実行している必要があります。

ファームウェアのダウングレード

Cisco UCS ドメインのファームウェアは、アップグレードと同じ方法でダウングレードできます。ファームウェアのアップデート時に選択したパッケージまたはバージョンによって、アップグレードを実行するか、ダウングレードを実行するかが決まります。

重要

- ボード コントローラ ファームウェアをダウングレードする必要はありません。
- Cisco UCS B シリーズ ブレード サーバのボード コントローラ ファームウェアは、ダウングレードするように設計されていません。システム全体のファームウェア ダウングレード操作を実行する際、「Error: Update failed: Server does not support board controller downgrade」というエラー メッセージが表示された場合は、このエラー メッセージを無視して、システム ファームウェアのダウングレードを続行しても問題ありません。UCS Manager は、ボード コントローラ ファームウェアを自動的にスキップして、他のファームウェア コンポーネントのダウングレードを続行します。
- ブレード サーバのボード コントローラ ファームウェア バージョンは、インストール済みソフトウェア バンドルと同じか、または新しいバージョンである必要があります。ボード コントローラ ファームウェアのバージョンが、既存の Cisco UCS 環境で実行されているバージョンよりも新しい場合でも、ソフトウェア マトリックスまたは TAC のサポート範囲には違反しません。
- ボード コントローラ ファームウェアの更新は、他のコンポーネントのファームウェアと下位互換性があります。

（注）

Cisco UCS Manager GUI では、リリースでサポートされていないオプションを選択できません。ダウングレードするリリースでサポートされていないハードウェアが Cisco UCS ドメインに含まれている場合は、Cisco UCS Manager GUI にそのハードウェアのオプションとしてそのファームウェアが表示されないか、ダウングレードできません。

Intel® Xeon® プロセッサ E5-2600 v4 製品ファミリまたは TPM 2.0 でのファームウェア ダウングレード

UCS B200 M4、C220 M4、C240 M4 サーバ、および Intel® Xeon® プロセッサ E5-2600 v4 製品ファミリまたは TPM 2.0 での Cisco UCS の設定では、ダウングレード プロセスが次のシナリオで失敗します:

- CMC または BIOS、B および C バンドルを Cisco UCS Manager リリース 2.2(7) より前のリリースにダウングレードしようとしても、Cisco UCS Manager によってダウングレード プロセスは開始されません。このサーバにインストールされているタイプのプロセッサまたは TPM がサポートされていないため、指定された CIMC または BIOS、B/C バンドルにはダウングレードできないというエラー メッセージが表示されます。
- 先に Cisco UCS Manager のダウングレードを開始して、その後 B および C バンドル を Cisco UCS Manager リリース 2.2(7) より前のリリースにダウングレードした場合、BIOS と CIMC のダウングレードは成功しますが、FSM では失敗します。

ファームウェアのダウングレードと自動インストール

自動インストールを使用して、Cisco UCS ドメインを Cisco UCS のリリース 2.1 より前のリリースにダウングレードすることはできません。

サポートされていない機能をダウングレードの前に削除

Cisco UCS ドメインを以前のリリースにダウングレードする場合は、まず、以前のリリースでサポートされていない機能を現在のバージョンからすべて削除または設定解除して、機能しない設定をすべて修正する必要があります。

（注） 以前のリリースでサポートされていない機能をすべて削除または設定解除しないでダウングレードしようとすると、ダウングレードが失敗し、「This operation is not supported for UCSM version below 2.1」というメッセージが表示されます。

たとえば、Cisco UCS ドメインを Cisco UCS リリース 2.1 からリリース 2.0 にダウングレードする場合は、まず、サポートされていない機能を削除または設定解除する必要があります。サポートされていない機能として、VLAN ポート数の最適化や適切なサービス プロファイル設定などがあげられます。これらは iSCSI 関連の問題により正常に機能しません。

たとえば、Cisco UCS ドメインを Cisco UCS リリース 2.1 からリリース 1.4 にダウングレードする場合には、まず次のようなサポートされていない機能を削除または設定解除する必要があります。

- 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、ブート順序ポリシー、LAN 接続ポリシーなどのオブジェクトの iSCSI 設定（iSCSI vNIC とイニシエータ IQN を含む）
- FCoE アップリンク ポート
- FCoE ストレージ ポート
- ユニファイド アップリンク ポート
- アプライアンスのストレージ ポート

2232PP FEX を解放して取り外すことなく Cisco UCS ドメインを Cisco UCS 2232PP FEX で Cisco UCS リリース 2.1 以降からリリース 1.4 にダウングレードした場合、DME プロセスはクラッシュし、Cisco UCS Manager は応答しなくなります。

ファームウェアのダウングレードとイニシエータ IQN の設定

サービス プロファイル レベルで定義されているイニシエータ IQN がある場合は、Cisco UCS リリース 2.1(2) から Cisco UCS リリース 2.0(1) にダウングレードすると、そのイニシエータ IQN が iSCSI vNIC レベルで定義されているすべてのイニシエータ IQN にコピーされます。

サービス プロファイル レベルで定義されているイニシエータ IQN があり、サービス プロファイルに iSCSI vNIC が 1 つだけ存在している場合は、Cisco UCS リリース 2.1(2) から Cisco UCS リリース 2.1(1) 以前にダウングレードすると、そのサービス プロファイル レベルのイニシエータ IQN が iSCSI vNIC レベルで定義されているイニシエータ IQN にコピーされます。

複数の iSCSI vNIC がある場合に Cisco UCS リリース 2.1(1) から 2.0(2) にダウングレードすると、エラー メッセージが生成され、iSCSI vNIC レベルで定義されているすべてのイニシエータ IQN に同一のイニシエータ IQN をコピーできないことが示されます。

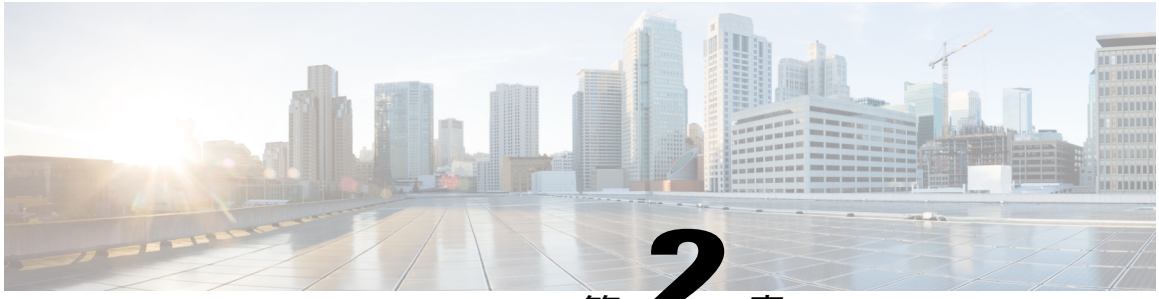
Cisco UCS Central からの登録解除

Cisco UCS をリリース 2.1(2) から以前のリリースにダウングレードし、その Cisco UCS ドメインを Cisco UCS Central に登録する場合は、ダウングレードする前に Cisco UCS Central から Cisco UCS ドメインを登録解除する必要があります。

ファームウェアのダウングレードの推奨手順

ファームウェアを以前のリリースにダウングレードする必要がある場合は、次の順序で実行することを推奨します。

1. ダウングレード先となるリリースから、現在のリリースにアップグレードしたときに作成した設定のバックアップを取り出します。
2. ダウングレード先のリリースでサポートされていない機能を削除または設定解除します。
3. Cisco UCS ドメインをダウングレードします。
4. erase-config を実行します。
5. ダウングレード先のリリースから設定のバックアップをインポートします。



第 2 章

注意、ガイドライン、および制約事項

この章は、次の項で構成されています。

ファームウェアアップグレードに関する注意、ガイドライン、および制約事項

Cisco UCS ドメインのエンドポイントのファームウェアをアップグレードする前に、次の注意、ガイドライン、および制約事項を考慮してください。

ファームウェアをアップグレードする前に、すべてのエラーを解消してください。

設定の変更とアップグレードに影響を与える可能性がある設定

Cisco UCS ドメインの設定に応じて、アップグレード後に設定を変更するには、次の変更が必要な場合があります。障害などの問題を回避するには、必要な変更を行ってからアップグレードすることを推奨します。

Cisco UCS リリース 2.1(2) 以降へのアップグレードがサービス プロファイル レベルで定義されているイニシエータ IQN に及ぼす影響

2 つの iSCSI vNIC があり、両方が同じイニシエータ IQN（Cisco UCS リリース 2.0(1) でサポート）を使用している場合は、アップグレードすると、単一のサービス プロファイル レベルのイニシエータ IQN が作成され、iSCSI vNIC のイニシエータ IQN はリセットされて値を失います。

Cisco UCS リリース 2.0(1) のサービス プロファイル全体において、iSCSI vNIC で同じイニシエータ IQN が使用されている場合は、アップグレードすると、サービス プロファイル レベルの重複したイニシエータ IQN が生成されます。このような構成では、サービス プロファイル レベルで

定義された重複イニシエータ IQN を持つ各 iSCSI vNIC に対してエラーが生成されます。これらのエラーは、サービス プロファイル レベルの重複イニシエータ IQN を変更すると解消されます。サービス プロファイル関連の操作（ホスト ファームウェア パッケージのアップデートなど）を実行する前に、これらのエラーを解消する必要があります。

デフォルトのメンテナンス ポリシーの設定を「ユーザ確認応答」にする

デフォルトのメンテナンスポリシーは、ホストメンテナンスポリシーによるサーバファームウェアのアップグレードなど、大きな影響を及ぼす変更がサービス プロファイルに加えられた場合にただちにサーバがリブートするように設定されています。サーバ トラフィックの予期せぬ中断を避けるため、デフォルトのメンテナンスポリシーのリブートポリシー設定をユーザ確認応答に変更することを推奨します。

デフォルトのメンテナンスポリシーのリブートポリシー設定をユーザ確認応答に変更すると、大きな影響を及ぼす変更のリストが保留中のアクティビティと共に一覧表示されます。これにより、サーバのリブートを制御することができます。

FCoE VLAN ID とイーサネット VLAN ID のオーバーラップは Cisco UCS リリース 2.0 以降では許可されない

注意 Cisco UCS 1.4 以前のリリースでは、イーサネット VLAN と FCoE VLAN で VLAN ID のオーバーラップが可能でした。ただし、Cisco UCS リリース 2.0 以降では、VLAN ID のオーバーラップは許可されません。アップグレード中に Cisco UCS Manager で VLAN ID のオーバーラップが検出されると、重大なエラーが生成されます。VLAN ID を再設定しない場合、Cisco UCS Manager によって重大なエラーが生成され、オーバーラップしている VLAN のイーサネット トラフィックがドロップされます。このため、イーサネットと FCoE の VLAN ID がオーバーラップしていないことを確認してから、Cisco UCS リリース 2.2 にアップグレードすることを推奨します。

アップリンク トランクの設定で VLAN ID 1 がネイティブ VLAN として定義および設定されている場合、イーサネット VLAN 1 ID を別の値に変更すると、ファブリック インターコネクトでネットワークの中断やフラッピングが生じ、その結果、HA イベントが発生して、大量のトラフィックが取り込まれ、サービスを一時的に使用できなくなります。

Cisco UCS 1.4 以前のリリースでは、VSAN の FCoE VLAN ID を明示的に設定しなかった場合、Cisco UCS Manager は、デフォルトの VSAN のデフォルト FCoE VLAN として VLAN 1 を割り当てました（デフォルトの VSAN ID 1 を使用）。これらのリリースでは、VLAN 1 は、イーサネット トラフィックのデフォルト VLAN としても使用されました。このため、FCoE VLAN および 1 つ以上のイーサネット VLAN のデフォルト VLAN ID を受け入れた場合は、VSAN の FCoE VLAN またはイーサネット VLAN の VLAN ID を再設定する必要があります。

Cisco UCS リリース 2.2 の新規インストールでは、デフォルトの VLAN ID は次のようになります。

- デフォルトのイーサネット VLAN ID は 1 です。
- デフォルトの FCoE VLAN ID は 4048 です。

FCoE ストレージ ポートのネイティブ VLAN に対して VLAN ID 4048 が使用されている場合に、Cisco UCS リリース 1.4 からリリース 2.0 にアップグレードすると、デフォルトの VLAN ID は次のようになります。

- デフォルトのイーサネット VLAN ID は 1 です。
- 現在のデフォルトの FCoE VLAN ID は維持されます。競合するイーサネット VLAN がある場合は、Cisco UCS Manager によって重大なエラーが生成されます。1 つの VLAN ID を、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。

（注） Cisco UCS ドメインでデフォルト VLAN ID の 1 つが使用されているため VLAN のオーバーラップが発生している場合は、1 つ以上のデフォルト VLAN ID を、使用または予約されていない VLAN ID に変更します。リリース 2.0 以降では は予約されます。

予約済み範囲の ID を持つ VSAN は正常に動作しない

予約範囲の ID を持つ VSAN は、アップグレード後に正常に動作しません。次を実行して、Cisco UCS Manager で設定されている VSAN が予約済み範囲に含まれないようにします。

VSAN に予約済み範囲の ID がある場合は、その VSAN ID を、使用または予約されていない VSAN ID に変更します。

ファームウェアアップグレードのハードウェアに関する注意事項および制限事項

Cisco UCS ドメインのハードウェアはアップグレード方法に影響を与えることがあります。エンドポイントをアップグレードする前に、次の注意事項および制約事項を考慮してください。

サーバまたはシャーシのメンテナンスなし

アップグレードの実施前や実施中に RAID 構成ハードディスクを交換しない

Cisco UCS インフラストラクチャやサーバ ファームウェアのアップグレードの実施前および実施中は、以下を順守してください。

- サーバのローカル ストレージ（ハード ディスクや SSD）の取り外し、挿入、交換を行わない。
- リビルド、アソシエーション、コピーバック、BGI など、ストレージ操作が実行されていないことを確認する。

常にホスト ファームウェア パッケージを使用して Cisco UCS Gen-2 アダプタをアップグレードする

Cisco UCS Gen-2 アダプタは、エンドポイントで直接アップグレードすることはできません。このようなアダプタのファームウェアは、ホストファームウェアパッケージを使用してアップグレードする必要があります。

Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter はアップグレードできない

Intel ベースのアダプタ カードである Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter（N20-AI0002）のファームウェアは、製造元でハードウェアに書き込まれます。このアダプタのファームウェアはアップグレードできません。

ファブリック インターコネクト数

2 つのファブリック インターコネクトのあるクラスタ設定の場合、ファブリック インターコネクト間のフェールオーバーを利用して、データ トラフィックを中断せずに、エンドポイントの直接のファームウェア アップグレードを実行できます。ただし、ホストまたは管理ファームウェア パッケージによってアップグレードする必要があるエンドポイントの場合は、データ トラフィックの中断が避けられません。

単一のファブリック インターコネクトのスタンドアロン設定の場合、エンドポイントの直接のファームウェアアップグレードを実行すると、データ トラフィックの中断を最小にできます。ただし、アップグレードを完了するために、ファブリック インターコネクトをリブートする必要があるため、トラフィックの中断は避けられません。

（注） NX-OS の内部電源シーケンサ ファームウェアが Cisco UCS アップグレード プロセスの一部として更新された場合、ファブリック インターコネクトはローダ プロンプトを表示します。続行するには、ファブリック インターコネクトをパワーサイクルします。

サポートされていないハードウェアは検出されない

新しいサーバまたはアダプタを、それらのサーバ/アダプタ未対応の Cisco UCS Manager リリースを使用している既存の Cisco UCS システムに追加した場合、そのシステムは検出されません。そのサーバまたはアダプタが現在の UCS ファームウェア バージョンでサポートされていないというエラー メッセージが FSM に表示されます。この問題を解決するには、次のいずれかを実行します。

- 互換性のある最新リリースに機能カタログを更新する。
- 新しいハードウェアに必要なバージョンに Cisco UCS Manager のインフラストラクチャ ファームウェアをアップグレードする。リリース ノートのハードウェア サポート マトリックスに互換性情報が詳細に記載されています。

アプライアンス ポート

ダイレクトアタッチドストレージにアプライアンス ポートを使用する場合は、イーサネットアップリンクに VLAN を追加する必要があります。そうすることで、起動時に vNIC を適切にピン接続できるようになります。

アップグレードのファームウェアおよびソフトウェアに関する注意事項および制約事項

エンドポイントをアップグレードする前に、次の注意事項および制約事項を考慮してください。

各エンドポイントの適切なタイプのファームウェア アップグレードの決定

アダプタやサーバ CIMC などの一部のエンドポイントは、直接のファームウェア アップグレードか、またはサービスプロファイルに含まれるファームウェアパッケージによって、アップグレードできます。Cisco UCS ドメインの設定によって、これらのエンドポイントのアップグレード方法が決まります。サーバに関連付けられているサービスプロファイルに、ホストファームウェアパッケージが含まれる場合、ファームウェア パッケージによって、それらのサーバのアダプタをアップグレードします。同様に、サーバに関連付けられているサービスプロファイルに管理ファームウェア パッケージが含まれる場合、ファームウェア パッケージによって、それらのサーバの CIMC をアップグレードします。

管理ファームウェア パッケージによる CIMC のアップグレードまたは、サーバに関連付けられたサービスプロファイル内のファームウェアパッケージによるアダプタのアップグレードは、直接のファームウェアアップグレードより優先されます。サーバに関連付けられたサービスプロファイルにファームウェア パッケージが含まれる場合、エンドポイントを直接アップグレードすることはできません。直接のアップグレードを実行するには、サービス プロファイルからファームウェア パッケージを削除する必要があります。

Cisco UCS Manager GUI ですべてのエンドポイントを同時にアクティブにしない

Cisco UCS Manager GUIを使用してファームウェアをアップデートする場合、[Activate Firmware] ダイアログボックスの [Filter] ドロップダウン リストで [ALL] を選択して、すべてのエンドポイントを同時にアクティブにしないでください。多くのファームウェア リリースやパッチには依存関係があるため、ファームウェアの更新を正常に実行するためにエンドポイントを特定の順序でアクティブにする必要があります。この順序はリリースやパッチの内容によって異なります。すべてのエンドポイントをアクティブにしても、更新が目的の順序で実行される保証はなく、エンドポイント、ファブリック インターコネクト、Cisco UCS Manager の間での通信が損なわれる可能性があります。特定のリリースやパッチの依存関係については、当該のリリースやパッチに付属のリリース ノートを参照してください。

使用可能なブートフラッシュおよびワークスペース パーティションの特定

ブートフラッシュ パーティションは、Cisco UCS Manager によって管理されるファームウェア イメージ専用です。アップグレードまたはダウングレードを開始するには、ブートフラッシュ パーティションの最低20%が使用可能である必要があります。ブートフラッシュのパーティションが容量の 70 % および 90 % を超えると障害が発生します。

ファブリック インターコネクトのワークスペース パーティションに格納されるのは、テクニカル サポート ファイル、コア ファイル、およびデバッグ プラグインです。アップグレードまたはダウングレードを開始するには、ワークスペース パーティションの最低 20 % が使用可能である必要があります。

アダプタおよび I/O モジュールのアクティベーションの影響

直接のアップグレード時に、アダプタに [Set Startup Version Only] を設定する必要があります。この設定では、アクティブ化されたファームウェアが pending-next-boot 状態に移行し、サーバがすぐにリブートしません。アクティブ化されたファームウェアは、サーバがリブートされるまで、アダプタで実行されているバージョンのファームウェアになりません。ホスト ファームウェア パッケージのアダプタに [Set Startup Version Only] を設定することはできません。

サーバがサービス プロファイルに関連付けられない場合、アクティブ化されたファームウェアは pending-next-boot 状態を維持します。Cisco UCS Manager は、サーバがサービス プロファイルに関連付けられるまで、エンドポイントをリブートせず、ファームウェアをアクティブにしません。必要に応じて、関連付けられていないサーバを手動でリブートまたはリセットして、ファームウェアをアクティブにできます。

I/O モジュールに対して [Set Startup Version Only] を設定した場合、そのデータ パス内のファブリック インターコネクトがリブートされると、I/O モジュールがリブートされます。I/O モジュールに対して、[Set Startup Version Only] を設定しない場合、I/O モジュールがリブートし、トラフィックが中断します。また、Cisco UCS Manager がファブリック インターコネクトと I/O モジュールの間のプロトコルとファームウェア バージョンの不一致を検出した場合、Cisco UCS Manager は、ファブリック インターコネクトのファームウェアに一致するファームウェア バージョンを使用して I/O モジュールを自動的に更新し、ファームウェアをアクティブ化して、I/O モジュールを再度リブートします。

不要なアラートを回避するためのアップグレード前の Call Home のディセーブル化（任意）

Cisco UCS ドメインをアップグレードすると、Cisco UCS Manager によってコンポーネントが再起動され、アップグレード プロセスが完了します。この再起動によって、サービスの中断およびコンポーネントの障害と同じイベントが発生し、Call Home アラートの送信がトリガーされます。アップグレードの開始前に Call Home をディセーブルにしない場合は、アップグレードに関連したコンポーネントの再起動によって生成されるアラートを無視してください。

自動インストールによるアップグレードに関する注意、ガイドライン、および制約事項

自動インストールを使用して Cisco UCS ドメインのエンドポイントのファームウェアをアップグレードする前に、次の注意、ガイドライン、および制約事項を考慮してください。

（注） 次の注意事項は自動インストールに固有の事項であり、ファームウェア アップグレードに関する注意、ガイドライン、および制約事項,（23 ページ）の項目と併せて考慮する必要があります。

エンドポイントの状態

アップグレードを開始する前に、影響を受けるすべてのエンドポイントが次の状態であることが必要です。

- クラスタ設定の場合、ファブリック インターコネクトの高可用性ステータスに、両方が稼働中であると示されていることを確認します。
- スタンドアロン設定の場合、ファブリック インターコネクトの [Overall Status] が [Operable] であることを確認します。
- アップグレードするすべてのエンドポイントについて、動作可能な状態にあることを確認します。
- アップグレードするすべてのサーバについて、すべてのサーバが検出され、検出が失敗しないことを確認します。いずれかのサーバエンドポイントをアップグレードできないと、サーバ ファームウェアのインストールの処理は失敗します。

デフォルトのホスト ファームウェア ポリシーに関する推奨事項

Cisco UCS Manager をアップグレードすると、「default」という名前の新しいホスト ファームウェア ポリシーが作成され、まだホスト ファームウェア ポリシーが含まれていないすべてのサービス プロファイルに割り当てられます。デフォルトのホスト ファームウェア ポリシーは空白です。いかなるコンポーネントのいかなるファームウェア エントリも含まれていません。このデフォルトのポリシーは、ユーザの確認応答を受けてからサーバをリブートするのではなく、即時にリブートするように設定することもできます。

サーバ ファームウェアのアップグレード時に、Cisco UCS ドメインのブレード サーバやラック マウント サーバのファームウェアをデフォルトのホスト ファームウェア ポリシーに追加できます。アップグレードを完了するには、すべてのサーバをリブートする必要があります。

デフォルトのホスト ファームウェア ポリシーが割り当てられている各サービス プロファイルは、そこに含まれているメンテナンス ポリシーに従って、関連付けられているサーバをリブートします。メンテナンス ポリシーが即時リブートに設定されている場合は、[Install Server Firmware] ウィザードでの設定の完了後に、アップグレードをキャンセルしたり、サーバのリブートを阻止することはできません。これらのサービス プロファイルに関連付けられているメンテナンス ポリシーを検証して、時限リブートまたはユーザ確認応答のいずれが設定されているかを確認することを推奨します。

（注） 2.1(2a) より前のリリースからアップグレードする場合は、CSCup57496 の影響を受ける可能性があります。手動で CIMC をアップグレードしてサービス プロファイルを関連付けたら、管理ファームウェア パックを削除して CIMC のファームウェアをアクティブにします。詳細については、https://tools.cisco.com/bugsearch/bug/CSCup57496を参照してください。

使用可能なブートフラッシュ パーティション

ブートフラッシュ パーティションは、Cisco UCS Manager によって管理されるファームウェア イメージ専用です。自動インストールを開始するには、ブートフラッシュ パーティションの少なくとも 20 % が使用可能である必要があります。ブートフラッシュのパーティションが容量の 70 % および 90 % を超えると障害が発生します。

使用可能なワークスペース パーティション

ファブリック インターコネクトのワークスペース パーティションには、テクニカル サポート ファイル、コア ファイル、およびデバッグ プラグインが保存されます。アップグレードまたはダウングレードを開始するには、ワークステーション パーティションの少なくとも 20 % が使用可能である必要があります。

ファブリック インターコネクトの時刻、日付、およびタイムゾーンは同一でなければなりません

クラスタ構成内のファブリック インターコネクトを確実に同期させるには、それらが同じ日付、時刻、タイムゾーンに設定されていることを確認する必要があります。両方のファブリック インターコネクトに NTP サーバと正しいタイム ゾーンを設定することを推奨します。ファブリック インターコネクトの日付、時刻、タイムゾーンが同期していないと、自動インストール でエラーが発生することがあります。

インフラストラクチャとサーバのファームウェアを同時にアップグレードすることは不可能

インフラストラクチャのファームウェアをサーバのファームウェアと同時にアップグレードすることはできません。インフラストラクチャのファームウェアを先にアップグレードし、次にサーバのファームウェアをアップグレードすることを推奨します。インフラストラクチャのファームウェアのアップグレードが完了するまで、サーバのファームウェアのアップグレードは開始しないでください。

必要な権限

自動インストールを使用してエンドポイントをアップグレードするには、次の権限が必要です。

権限	実行できるアップグレード作業
admin	• インフラストラクチャ ファームウェアのインストールの実行 • サーバ ファームウェアのインストールの実行 • ホスト ファームウェア パッケージの追加、削除、および変更
サービス プロファイルの計算（ls-compute）	サーバ ファームウェアのインストールの実行
サービス プロファイルのサーバ ポリシー（ls-server-policy）	ホスト ファームウェア パッケージの追加、削除、および変更
サービス プロファイルの設定ポリシー（ls-config-policy）	ホスト ファームウェア パッケージの追加、削除、および変更

サーバ ファームウェアのインストールに対するホスト ファームウェア パッケージと管理ファームウェア パッケージの影響

サーバ ファームウェアのインストールでは、ホスト ファームウェア パッケージを使用してサーバをアップグレードするため、Cisco UCS ドメインのすべてのサーバを同じファームウェア バージョンにアップグレードする必要はありません。ただし、関連するサービス プロファイルにサーバ ファームウェアのインストールを設定したときに選択したホスト ファームウェア パッケージが含まれるサーバは、すべて指定したソフトウェア バンドルのファームウェア バージョンにアップグレードされます。

サーバに関連付けられているサービス プロファイルにホスト ファームウェア パッケージだけでなく管理ファームウェア パッケージも含まれている場合は、サーバ ファームウェアのインストールでは、管理ファームウェア パッケージのファームウェア バージョンを使用して、サーバの CIMC をアップグレードします。CIMC は、ホスト ファームウェア パッケージの CIMC の方が管理ファームウェア パッケージの CIMC より新しいバージョンの場合でも、ホスト ファームウェア パッケージのファームウェア バージョンにはアップグレードされません。ホスト ファームウェア パッケージを使用してサーバの CIMC をアップグレードする場合は、関連付けられたサービス プロファイルから管理ファームウェア パッケージを削除する必要があります。

サービス プロファイルにホスト ファームウェア パッケージが含まれていないサーバに対してサーバ ファームウェアのインストールを使用した場合の影響

サーバに関連付けられたサービス プロファイルにホスト ファームウェア パッケージが含まれていない場合、このサーバのエンドポイントのアップグレードにサーバ ファームウェアのインストールを使用すると、サーバ ファームウェアのインストールではデフォルトのホスト ファームウェア パッケージを使用してサーバをアップグレードします。サーバ ファームウェアのインストールでは、デフォルトのホスト ファームウェア パッケージのみ更新できます。

サーバに関連付けられているサービスプロファイルが以前にサーバファームウェアのインストール のデフォルトのホスト ファームウェア パッケージによって更新されている場合、このサーバの CIMC またはアダプタをアップグレードするには、次のいずれかの方法を使用する必要があります。

- サーバ ファームウェアのインストールを使用してデフォルトのホスト ファームウェア パッケージを変更し、次にサーバ ファームウェアのインストールを使用してサーバをアップグレードする。
- 新しいホスト ファームウェア パッケージ ポリシーを作成し、これを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、そのホスト ファームウェア パッケージ ポリシーを使用してサーバをアップグレードする。
- サービスプロファイルをサーバの関連付けから解除し、次にサーバのエンドポイントを直接アップグレードする。

新たに追加されたサーバのサーバ ファームウェアのアップグレード

サーバファームウェアのインストールを実行した後、Cisco UCS ドメインにサーバを追加すると、新しいサーバのファームウェアはサーバ ファームウェアのインストールによって自動的にアップグレードされません。新しく追加したサーバのファームウェアを、最後にサーバ ファームウェアのインストールを実行したときに使用したファームウェア バージョンにアップグレードする場合は、エンドポイントをそのサーバのファームウェアに手動でアップグレードする必要があります。サーバファームウェアのインストールには、ファームウェアバージョンの変更が毎回必要です。サーバを同じファームウェアバージョンにアップグレードするためにサーバファームウェアのインストールを再実行することはできません。

（注） リリース 2.2 へのアップグレードが終了すると、Cisco UCS Manager で [Firmware Auto Sync Server] ポリシーを使用して、新たに検出されたサーバを自動的に更新できます。詳細については、該当する『*Cisco UCS B* シリーズ ファームウェア管理ガイド』を参照してください。

Cisco UCS Central のファームウェア管理に関する注意、ガイドライン、および制約事項

Cisco UCS Central から Cisco UCS Manager のファームウェアの管理を開始する前に、次の注意、ガイドライン、および制約事項を考慮してください。

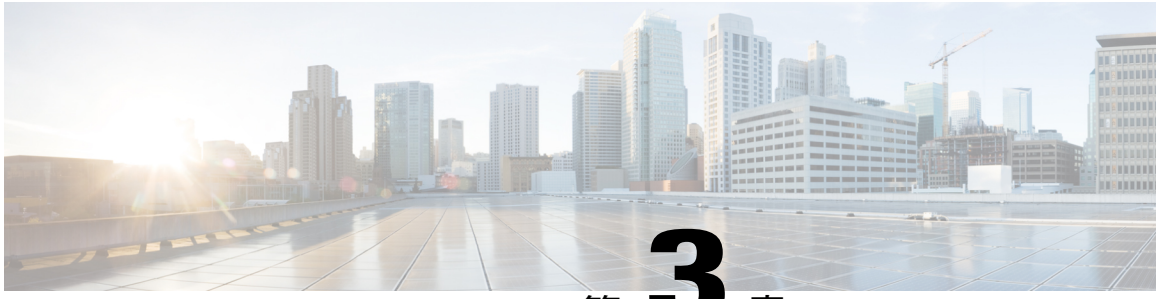
- ドメイン グループに定義したファームウェア ポリシーは、このドメイン グループに追加されるすべての新しい Cisco UCS ドメインに適用されます。ドメイン グループでファームウェア ポリシーが定義されていない場合、Cisco UCS ドメインは親ドメイン グループからポリシーを継承します。
- グローバル ポリシーは、Cisco UCS Manager が Cisco UCS Central との接続を失った場合でも Cisco UCS Manager にグローバルに残ります。Cisco UCS Manager でグローバルなポリシーの

いずれかに変更を適用するには、所有権をグローバルからローカルに変更する必要があります。

- ホスト ファームウェア パッケージを Cisco UCS Central から作成した場合は、これをサービス プロファイルに関連付けて、Cisco UCS ドメインにアップデートを展開する必要があります。
- Cisco UCS Central でホスト ファームウェア パッケージを変更すると、その変更はホスト ファームウェア アップデートに関連付けられた次のメンテナンス スケジュールの際に Cisco UCS ドメインに適用されます。
- Cisco UCS Central で定義したホスト ファームウェア メンテナンス ポリシーは、Cisco UCS ドメインの org-root に適用されます。Cisco UCS Central から Cisco UCS ドメインのサブ組織に対して別のホスト メンテナンス ポリシーを定義することはできません。
- サービス プロファイルとの関連付けを持たないサーバは、ホスト ファームウェア パックのデフォルト バージョンにアップグレードされます。これらのサーバにはメンテナンス ポリシーがないため、ただちにリブートされます。
- Cisco UCS Central でメンテナンス ポリシーを指定してユーザの確認応答をイネーブルにし、スケジュールを指定しない場合は、Cisco UCS Manager からのみ保留中のタスクに確認応答できます。Cisco UCS Central から保留中のアクティビティに確認応答するには、グローバルなスケジューラを使用してメンテナンスをスケジュールし、ユーザの確認応答をイネーブルにする必要があります。
- Cisco UCS Central でメンテナンス ポリシーをスケジュールし、ユーザの確認応答をイネーブルにすると、このタスクは保留中のアクティビティ タブにスケジュールで指定した時刻で表示されます。
- メンテナンス ポリシーの保留中のアクティビティは、ドメイン グループのセクションからのみ表示できます。
- 任意のファームウェアのスケジュールに対するユーザの確認応答をイネーブルにして、Cisco UCS ドメインでの予期せぬリブートを避けるようにしてください。

第 I 部

Cisco UCS Manager によるファームウェアの管理



第 3 章

ファームウェアのアップグレードの前提条件の実行

この章は、次の項で構成されています。

ファームウェアのアップグレードとダウングレードの前提条件

Cisco UCS ドメインのすべてのエンドポイントが完全に機能し、それらのエンドポイントのファームウェアのアップグレードまたはダウングレードを開始する前に、すべてのプロセスが完了している必要があります。機能状態でないエンドポイントはアップグレードまたはダウングレードすることはできません。たとえば、検出されていないサーバのファームウェアはアップグレードまたはダウングレードできません。最大回数の再試行後に失敗したFSMなどの未完了のプロセスによって、エンドポイントのアップグレードやダウングレードが失敗する可能性があります。FSMが実行中の場合、Cisco UCS Managerによって、更新とアクティベーションがキューに入れられ、FSM が正常に完了すると、それらが実行されます。

[Equipment] タブのコンポーネントの周囲の色付けされたボックスは、そのコンポーネントのエンドポイントがアップグレードまたはダウングレードできないことを示していることがあります。エンドポイントのアップグレードを試みる前に、そのコンポーネントのステータスを確認してください。

（注） Cisco UCS Manager GUI の [Installed Firmware] タブでは、これらの前提条件を実行するための十分な情報が得られません。

Cisco UCS ドメインのファームウェアをアップグレードまたはダウングレードする前に、次の前提条件を実行します。

- リリース ノートの内容を確認します。
- 適切なハードウェアおよびソフトウェア相互運用性の表を参照し、すべてのサーバのオペレーティング システムドライバのレベルが、アップグレード予定の Cisco UCS のリリースに対して正しいレベルになっていることを確認します。
- 設定を All Configuration バックアップ ファイルにバックアップします。
- クラスタ設定の場合、ファブリック インターコネクトの高可用性ステータスに、両方が稼働中であると示されていることを確認します。
- スタンドアロン設定の場合、ファブリック インターコネクトの [Overall Status] が [Operable] であることを確認します。
- データ パスが稼働中であることを確認します。詳細については、該当する『ファームウェア管理ガイド』の「データ パスの準備が整っていることの確認」セクションを参照してください。
- すべてのサーバ、I/O モジュール、アダプタが完全に機能することを確認します。動作不能なサーバはアップグレードできません。
- Cisco UCS ドメインに致命的または重大な障害がないことを確認します。このような障害がある場合は解決してから、システムをアップグレードしてください。致命的または重大な障害があると、アップグレードが失敗する可能性があります。
- すべてのサーバが検出されていることを確認します。サーバの電源を入れる必要はありません。また、サーバをサービス プロファイルと関連付ける必要もありません。
- ラックマウント サーバを Cisco UCS ドメインに統合する場合、Cisco UCS Manager で管理するシステムにラックマウント サーバをインストールし、統合する方法については、該当する『C-Series Rack-Mount Server Integration Guide』の指示に従います。

すべてのコンフィギュレーション バックアップ ファイルの作成

この手順は、All Configuration バックアップ ファイルの既存のバックアップ操作がないことを前提としています。

はじめる前に

手順

ステップ 1 [Navigation] ペインで [Admin] をクリックします。

ステップ 2 [All] ノードをクリックします。

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

ステップ 4 [Actions] 領域の [Backup Configuration] をクリックします。

ステップ 5 [Backup Configuration] ダイアログボックスで、[Create Backup Operation] をクリックします。

ステップ 6 [Create Backup Operation] ダイアログボックスで、次の操作を実行します。

a) 次のフィールドに入力します。

- [Admin State] フィールド： オプション ボタンをクリックすると、[OK] をクリックしてすぐにバックアップ操作が実行されます。
- [Type] フィールド：[All Configuration] オプション ボタンをクリックすると、すべてのシステムおよび論理設定情報を含む XML バックアップ ファイルが作成されます。
- [Preserve Identities] チェックボックス：Cisco UCS ドメインに、プールから取得され、保存する必要がある ID が含まれる場合、このチェックボックスをオンにします。

  [Logical Configuration] タイプのバックアップ操作のチェックボックスが選択されている場合、vHBA、WWPN、WWNN、vNIC、MAC、UUID を含む、プールから取得されたすべての ID がバックアップ ファイルに保存されます。

  （注） このチェックボックスが選択されていない場合、復元後に ID が再び割り当てられ、ユーザ ラベルは失われます。
- [Protocol] フィールド：ファイルをバックアップ サーバに転送するために使用するプロトコルを指定する場合、次のいずれかのオプション ボタンをクリックします。
  - FTP
  - TFTP
  - SCP
  - SFTP
  - USB A：ファブリック インターコネクト A に挿入された USB ドライブ。

    このオプションは特定のシステム設定でしか使用できません。
  - USB B：ファブリック インターコネクト B に挿入された USB ドライブ。

    このオプションは特定のシステム設定でしか使用できません。
- [Hostname] フィールド：バックアップ ファイルを格納する場所の IP アドレスまたはホスト名を入力します。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。ホスト名を使用する場合は、DNS サーバを使用するように Cisco UCS Manager を設定する必要があります。

- [Filename] フィールド：バックアップ コンフィギュレーション ファイルのフル パスを入力します。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。
- [User] フィールド：Cisco UCS Manager がバックアップ場所へのログインに使用する必要のあるユーザ名を入力します。プロトコルにTFTPを選択した場合は、このフィールドに入力する必要はありません。
- [Password] フィールド：ユーザ名に関連付けられたパスワードを入力します。プロトコルに TFTP を選択した場合は、このフィールドに入力する必要はありません。

b) [OK] をクリックします。

ステップ 7 Cisco UCS Manager に確認ダイアログボックスが表示されたら、[OK] をクリックします。
[Admin State] フィールド をイネーブルに設定すると、Cisco UCS Manager によって、選択した設定タイプのスナップショットが取得され、ファイルがネットワークの場所にエクスポートされます。[Backup Configuration] ダイアログボックスの [Backup Operations] テーブルに、バックアップ操作が表示されます。

ステップ 8 （任意） バックアップ操作の進行状況を表示するには、次の操作を実行します。

a) [Properties] 領域に操作が表示されない場合、[Backup Operations] テーブルの操作をクリックします。

b) [Properties] 領域で、[FSM Details] バーの下矢印をクリックします。

[FSM Details] 領域が展開され、操作のステータスが表示されます。

ステップ 9 [OK] をクリックし、[Backup Configuration] ダイアログボックスを閉じます。
バックアップ操作は完了するまで実行し続けます。進捗を表示するには、[Backup Configuration] ダイアログボックスを再度開きます。

ファブリックインターコネクトのアップグレード中のリブートによって生成される障害

ファームウェアのアップグレード中、ファブリック インターコネクト上のすべてのサービスが正しく機能するようにするために、ファブリック インターコネクトがリブートするときにダウンするポート設定とサービスが、ファブリック インターコネクトが再稼働状態に復帰した後に再確立されるようにすることが必要です。

ファブリック インターコネクトの最後のリブート後に再確立されないサービスはCisco UCS Manager に表示されます。Cisco UCS Manager は、ファブリック インターコネクトをリブートする前に未処理の障害のベースラインを作成します。ファブリック インターコネクトがリブートして再稼働

状態に復帰したら、最後のベースライン以降に生成された新しい障害を確認して、ファブリックのリブートによってダウンしたサービスを特定できます。

Cisco UCS Manager が未処理の障害のベースラインを作成してから特定の期間が経過すると、ベースラインはクリアされ、すべての障害が新しい障害として表示されます。この期間は、ベースラインの有効期限と呼ばれます。 障害のベースライン有効期限の変更, （41 ページ） には、Cisco UCS Manager でベースラインの有効期限を変更する方法に関する詳細が掲載されています。

シスコでは、ファブリック インターコネクトのリブートまたは待避を実行する前に、サービスに影響する障害を解決することを推奨します。

障害のベースライン有効期限の変更

Cisco UCS Manager では、ベースラインの有効期限を変更できます。

手順

ステップ 1 [Navigation] ペインで [Admin] をクリックします。

ステップ 2 [All] > [Faults, Events, and Audit Log] の順に展開します。

ステップ 3 [Work] ペインの [Settings] タブをクリックし、[Global Fault Policy] サブタブをクリックします。

ステップ 4 [Baseline Expiration Interval] 領域で、[dd:hh:mm:ss] フィールドを更新します。
[dd:hh:mm:ss] フィールドには、Cisco UCS Manager が障害のベースラインをクリアするまでに経過する必要がある日数、時間数、分数、および秒数を指定します。

デフォルトのベースライン有効期限は 24 時間です。

ステップ 5 [Save Changes] をクリックします。

ファブリック インターコネクトのアップグレード中に生成される障害の表示

手順

ステップ 1 [Navigation] ペインで [Admin] をクリックします。

ステップ 2 [All] > [Faults, Events, and Audit Log] の順に展開します。

ステップ 3 [Work] ペインで [New Faults] オプション ボタンをクリックします。
ベースラインを作成した後に生成されたすべての障害が表示されます。

ファブリック インターコネクトの全体のステータスの確認

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] > [Fabric Interconnects] の順に展開します。

ステップ 3 確認するファブリック インターコネクトのノードをクリックします。

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

ステップ 5 [Status] 領域で、[Overall Status] が [operable] であることを確認します。
ステータスが [operable] でない場合は、テクニカル サポート ファイルを作成およびダウンロードして、シスコのテクニカルサポートに問い合わせてください。ファームウェアアップグレードに進まないでください。テクニカル サポート ファイルの詳細については、『*Cisco UCS Manager B-Series Troubleshooting Guide*』を参照してください。

クラスタ設定の高可用性ステータスとロールの確認

高可用性ステータスは、クラスタ設定の両方のファブリック インターコネクトで同じです。

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] > [Fabric Interconnects] の順に展開します。

ステップ 3 クラスタのいずれかのファブリック インターコネクトのノードをクリックします。

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

ステップ 5 [High Availability Details] 領域のフィールドが表示されていない場合は、見出しの右側の [Expand] アイコンをクリックします。

ステップ 6 次のフィールドに次の値が表示されることを確認します。

フィールド名	必要な値
[Ready] フィールド	Yes
[State] フィールド	Up

値が異なる場合は、テクニカルサポートファイルを作成およびダウンロードして、シスコのテクニカル サポートに問い合わせてください。ファームウェア アップグレードに進まないでくださ

い。テクニカル サポート ファイルの詳細については、『*Cisco UCS Manager B-Series Troubleshooting Guide*』を参照してください。

ステップ 7 [Leadership] フィールドの値に注意して、ファブリック インターコネクトがプライマリであるか、下位であるかを判断します。
この情報は、ファブリック インターコネクトのファームウェアをアップグレードするために知っておく必要があります。

I/O モジュールのステータスの確認

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] > [Chassis] の順に展開します。

ステップ 3 I/O モジュールのステータスを確認するシャーシをクリックします。

ステップ 4 [Work] ペインの [IO Modules] タブをクリックします。

ステップ 5 各 I/O モジュールについて、次のカラムに次の値が表示されることを確認します。

フィールド名	必要な値
[Overall Status] カラム	ok
[Operability] カラム	operable

値が異なる場合は、テクニカルサポートファイルを作成およびダウンロードして、シスコのテクニカル サポートに問い合わせてください。ファームウェア アップグレードに進まないでください。テクニカル サポート ファイルの詳細については、『*Cisco UCS Manager B-Series Troubleshooting Guide*』を参照してください。

ステップ 6 手順 3 から 5 を繰り返して、各シャーシの I/O モジュールのステータスを確認します。

サーバのステータスの確認

サーバが操作不可能な場合、Cisco UCS ドメインの他のサーバのアップグレードに進むことができます。ただし、操作不可能なサーバはアップグレードできません。

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] タブの [Equipment] をクリックします。

ステップ 3 [Work] ペインの [Servers] タブをクリックして、すべてのシャーシのすべてのサーバのリストを表示します。

ステップ 4 各サーバについて、次のカラムに次の値が表示されることを確認します。

フィールド名	必要な値
[Overall Status] カラム	[ok]、[unassociated]、または障害を示していないすべての値 値が、[discovery-failed] などの障害を示している場合、そのサーバのエンドポイントをアップグレードできません。
[Operability] カラム	operable

ステップ 5 サーバが検出されていることを確認する必要がある場合、次の手順を実行します。

a) 検出のステータスを確認するサーバを右クリックし、[Show Navigator] を選択します。

b) [General] タブの [Status Details] 領域で、[Discovery State] フィールドに [complete] の値が表示されていることを確認します。
[Status Details] 領域のフィールドが表示されない場合は、見出しの右側の [Expand] アイコンをクリックします。

シャーシのサーバのアダプタのステータスの確認

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] > [Chassis] > *[Chassis Number]* > [Servers] の順に展開します。

ステップ 3 アダプタのステータスを確認するサーバをクリックします。

ステップ 4 [Work] ペインの [Inventory] タブをクリックします。

ステップ 5 [Inventory] タブの [Adapters] サブタブをクリックします。

ステップ 6 各アダプタについて、次のカラムに次の値が表示されることを確認します。

フィールド名	必要な値
[Overall Status] カラム	ok
[Operability] カラム	operable

フィールドに異なる値が表示され、アダプタが操作不可能な場合、Cisco UCS ドメインのサーバの他のアダプタのアップグレードに進むことができます。ただし、操作不可能なアダプタはアップグレードできません。

Cisco UCS PowerTool の取得と重複した IQN スクリプトの実行

Cisco UCS ドメインが iSCSI ブート用に設定されている場合は、Cisco UCS リリース 2.0(1) から Cisco UCS リリース 2.0(2) 以降にアップグレードする前に、複数のサービス プロファイルで使用される iSCSI vNIC がすべて一意のイニシエータ名を持っていることを確認する必要があります。

Cisco UCS PowerTool 内で実行するスクリプトを使用して、iSCSI ブート用の Cisco UCS 設定に重複する IQN が含まれているかどうかを確認します。

手順

ステップ 1 Cisco UCS PowerTool をダウンロードするには、次の手順を実行します。

a) お使いの Web ブラウザで、Web サイト http://developer.cisco.com/web/unifiedcomputing/microsoft に移動します。

b) [Cisco UCS PowerTool (PowerShell Toolkit) Beta Download] 領域まで下にスクロールします。

c) `CiscoUcs-PowerTool-0.9.6.0.zip` ファイルをダウンロードします。

d) ファイルを解凍し、プロンプトに従って Cisco UCS PowerTool をインストールします。
Cisco UCS PowerTool は、任意の Windows コンピュータにインストールできます。Cisco UCS Manager へのアクセスに使用しているコンピュータにインストールする必要はありません。

ステップ 2 Cisco UCS PowerTool を起動するには、コマンドラインに次のように入力します。
C:\Program Files (x86)\Cisco\Cisco UCS PowerTool>C:\Windows\System32\windowspowe rshell\v1.0\powershell.exe -NoExit -ExecutionPolicy RemoteSigned -File .\StartUc sPS.ps1

例：
次に、Cisco UCS PowerTool を起動した場合の処理の例を示します。

```
C:\Program Files (x86)\Cisco\Cisco UCS
PowerTool>C:\Windows\System32\windowspowershell\v1.0\powershell.exe
-NoExit -ExecutionPolicy RemoteSigned -File .\StartUcsPS.ps1
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.
```

ステップ 3 Cisco UCS PowerTool で、次の手順を実行します。

a) 次のように、Cisco UCS Manager に接続します。
PS C:\>**Connect-Ucs***IP_address*

b) 次の例のように、クレデンシャルを求めるプロンプトが表示された場合には、ユーザ名とパスワードを入力します。

```
cmdlet Connect-Ucs at command pipeline position 1
Supply values for the following parameters:
Credential
```

Cisco UCS PowerTool によって、ログイン後の画面に次のような内容が出力されます。

```
Cookie                : 1331303969/2af0afde-6627-415c-b85f-a7cae6233de3
Domains               :
LastUpdateTime        : 3/9/2012 6:20:42 AM
Name                  : 209.165.201.15
NoSsl                 : False
NumPendingConfigs     : 0
NumWatchers           : 0
Port                  : 443
Priv                  : {admin, read-only}
RefreshPeriod         : 600
SessionId             : web_49846_A
TransactionInProgress : False
Ucs                   : ucs-4
Uri                   : https://209.165.201.15
UserName              : admin
VirtualIpv4Address    : 209.165.201.15
Version               : 2.0(2i)3.0(1a)
WatchThreadStatus     : None
```

ステップ 4 Cisco UCS PowerTool で次のスクリプトを実行して、iSCSI 起動設定を検証し、重複した IQN がないかどうかを確認します。
PS C:\> **Get-UcsServiceProfile -type instance | Get-UcsVnicIScsi | ? { $_.InitiatorName -ne "" } | select Dn,InitiatorName | group InitiatorName | ? { $_.Count -gt 1 } | % { $obj = New-Object PSObject ; $obj | Add-Member Noteproperty Count $_.Count; $obj | Add-Member Noteproperty InitiatorName $_.Name; $obj | Add-Member Noteproperty Dn ($_ | select -exp Group | % { $_.Dn }); $obj }**

Cisco UCS PowerTool によって、次のように、画面に結果が表示されます。

```
Count InitiatorName              Dn
----- -------------              --
    2 iqn.2012-01.cisco.com:s... {org-root/ls-SP_1_6/is...
    2 iqn.2012-01.cisco.com:s... {org-root/ls-SP_2_1/is...
    2 iqn.2012-01.cisco.com:s... {org-root/ls-SP_2_41/i...
    4 iqn.2012-01.cisco.com:s... {org-root/ls-SP_2_7/is...
    2 iqn.2012-01.cisco.com:s... {org-root/org-sub1/ls-...
    2 iqn.2012-01.cisco.com:s... {org-root/org-sub2/ls-...
```

ステップ 5 （任意） .NET Frame work 3.5 Service Pack 1 がインストールされている場合は、次のスクリプトを使用して GUI で結果を表示できます。
PS C:\> **Get-UcsServiceProfile -type instance | Get-UcsVnicIScsi | ? { $_.InitiatorName -ne "" } | select Dn,InitiatorName | group InitiatorName | ? { $_.Count -gt 1 } | % { $obj = New-Object PSObject ; $obj**

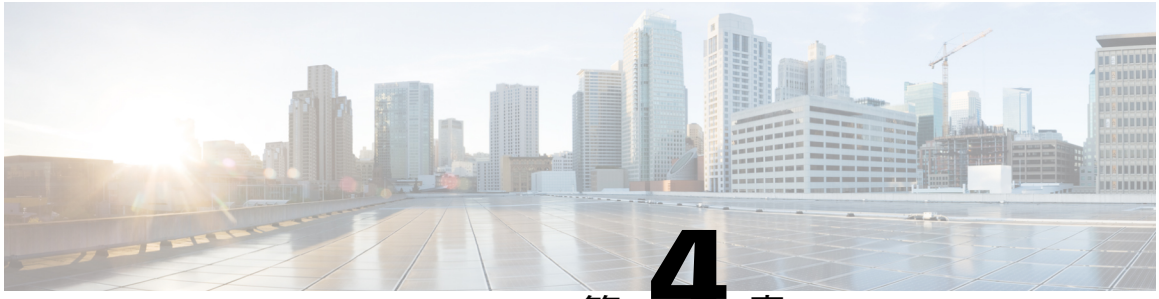
| Add-Member Noteproperty Count $_.Count; $obj | Add-Member Noteproperty InitiatorName $_.Name; $obj | Add-Member Noteproperty Dn ($_ | select -exp Group | % { $_.Dn }); $obj } | ogv

ステップ 6 次のように、Cisco UCS Manager から切断します。
PS C:\>**Disconnect-Ucs**

次の作業

Cisco UCS ドメインの複数のサービス プロファイルで IQN が重複している場合は、Cisco UCS リリース 2.1 以降にアップグレードする前に、Cisco UCS Manager で iSCSI vNIC を再設定し、それぞれが一意の IQN を持つようにします。

アップグレード前に、Cisco UCS ドメインのサービス プロファイル全体においてすべての iSCSI vNIC が一意であることを確認しなかった場合は、IQN の重複を警告するために、Cisco UCS Manager で iSCSI vNIC に関するエラーが発生します。また、サービス プロファイル内に重複した IQN 名（同じ名前が両方の iSCSI vNIC で使用されている場合など）がないことを確認しなかった場合は、Cisco UCS によってサービスプロファイルが再設定され、1 つの IQN を持つようになります。この障害をクリアして重複した IQN を再設定する方法の詳細については、『Cisco UCS B-Series Troubleshooting Guide』を参照してください。



第 4 章

Cisco UCS Manager でのファームウェアのダウンロードと管理

この章は、次の項で構成されています。

ファームウェア イメージの管理

Cisco では、Cisco UCS コンポーネントに対するすべてのファームウェア アップデートをイメージのバンドルで配信します。Cisco UCS ファームウェア アップデートは、次のようなバンドルで Cisco UCS ドメイン のファブリック インターコネクトにダウンロードできます。

Cisco UCS インフラストラクチャ ソフトウェア バンドル

このバンドルには、次のコンポーネントのアップデートに必要な次のファームウェア イメージが含まれます。

- Cisco UCS Manager ソフトウェア
- ファブリック インターコネクトのカーネル ファームウェアとシステム ファームウェア
- I/O モジュールのファームウェア

Cisco UCS B シリーズ ブレード サーバ ソフトウェア バンドル

このバンドルには、Cisco UCS ドメインのブレードサーバのファームウェアをアップデートするために必要な次のファームウェア イメージが含まれます。Cisco UCS Manager で最新のインフラストラクチャ バンドルに含まれていないブレードサーバがサポートされるように、リリースに対して作成されたバンドル以外に次のバンドルもインフラストラクチャ バンドル間でリリースできます。

- CIMC ファームウェア
- BIOS ファームウェア
- アダプタ ファームウェア
- ボード コントローラ ファームウェア
- 新規サーバで必要なサードパーティ製のファームウェア イメージ

Cisco UCS C シリーズ ラックマウント UCS 管理対象サーバ ソフトウェア バンドル

このバンドルには、Cisco UCS Manager に統合され、UCS Manager によって管理されるラックマウント サーバのコンポーネントのアップデートに必要な次のファームウェア イメージが含まれます。

- CIMC ファームウェア
- BIOS ファームウェア
- アダプタ ファームウェア
- ストレージ コントローラのファームウェア

（注） このバンドルは、スタンドアロン C シリーズ サーバには使用できません。このサーバのファームウェア管理システムでは、Cisco UCS Manager に必要なヘッダーを解釈できません。スタンドアロン C シリーズ サーバのアップグレード方法については、C シリーズのコンフィギュレーション ガイドを参照してください。

また、シスコではリリース ノートも提供しており、バンドルを取得したのと同じ Web サイトから入手できます。

ファームウェア イメージ ヘッダー

すべてのファームウェア イメージに、次の情報を含むヘッダーがあります。

- チェックサム
- バージョン情報

- コンポーネントイメージの互換性と依存関係を確認するためにシステムで使用される互換性情報

ファームウェア イメージ カタログ

Cisco UCS Managerには、ファブリック インターコネクトにダウンロードされているファームウェア イメージとそのコンテンツのカタログを示す 2 つのビューが用意されています。

パッケージ

このビューでは、ファブリック インターコネクトにダウンロードされているファームウェア バンドルが読み取り専用で表示されます。このビューは、イメージのコンテンツではなく、イメージを基準にソートされます。パッケージについては、このビューを使用して、ダウンロード済みの各ファームウェア バンドルに存在するコンポーネント イメージを確認できます。

イメージ

イメージ ビューには、システムで使用できるコンポーネント イメージが表示されます。このビューを使用して、ファームウェア バンドル全体を表示したり、バンドルごとにイメージをグループ化したりすることはできません。各コンポーネント イメージについて表示される情報には、コンポーネントの名前、イメージ サイズ、イメージ バージョン、およびコンポーネントのベンダーとモデルが含まれます。

このビューを使用して、各コンポーネントに使用できるファームウェア アップデートを識別できます。また、このビューを使用して、古くなったイメージや不要なイメージを削除することもできます。Cisco UCS Managerパッケージ内のすべてのイメージが削除されてから、パッケージが削除されます。

ヒント

Cisco UCS Manager によって、ファブリック インターコネクトのブートフラッシュにイメージが保存されます。クラスタ システムでは、すべてのイメージが互いに同期されるので、両方のファブリック インターコネクトにおけるブートフラッシュのスペース使用量は等しくなります。Cisco UCS Manager によって、ブートフラッシュの領域が不足していることが報告された場合は、古いイメージを削除して、領域を解放します。

シスコからのソフトウェア バンドルの入手

はじめる前に

Cisco UCS ドメインを更新するために、次のどのソフトウェア バンドルが必要なのかを判定します。

- Cisco UCS インフラストラクチャ ソフトウェア バンドル：すべての Cisco UCS ドメインで必要です。

- Cisco UCS B シリーズ ブレード サーバ ソフトウェア バンドル：ブレード サーバが含まれるすべての Cisco UCS ドメインで必要です。
- Cisco UCS C シリーズ ラックマウント UCS 管理対象サーバ ソフトウェア バンドル：統合されたラックマウント サーバが含まれる Cisco UCS ドメインのみで必要です。このバンドルには、Cisco UCS Manager がそれらのサーバを管理できるようにするためのファームウェアが含まれており、スタンドアロン C シリーズ ラックマウント サーバには適用されません。

手順

ステップ 1 Web ブラウザで、 Cisco.com を参照します。

ステップ 2 [Support] で [All Downloads] をクリックします。

ステップ 3 中央のペインで、[Servers - Unified Computing] をクリックします。

ステップ 4 入力を求められたら、Cisco.com のユーザ名およびパスワードを入力して、ログインします。

ステップ 5 右側のペインで、次のように必要なソフトウェア バンドルのリンクをクリックします。

Bundle	ナビゲーション パス
Cisco UCS インフラストラクチャ ソフトウェア バンドル	[Cisco UCS Infrastructure and UCS Manager Software] > [Unified Computing System (UCS) Infrastructure Software Bundle] をクリックします。
Cisco UCS B シリーズ ブレード サーバ ソフトウェア バンドル	[Cisco UCS B-Series Blade Server Software] > [Unified Computing System (UCS) Server Software Bundle] をクリックします。
Cisco UCS C シリーズ ラックマウント UCS 管理対象サーバ ソフトウェア バンドル	[Cisco UCS C-Series Rack-Mount UCS-Managed Server Software] > [Unified Computing System (UCS) Server Software Bundle] をクリックします。

ヒント これらのパスからアクセスできる Unified Computing System (UCS) Documentation Roadmap Bundle は、Cisco UCS のすべてのドキュメントのダウンロード可能な ISO イメージです。

ステップ 6 ソフトウェア バンドルをダウンロードする最初のページで、[Release Notes] リンクをクリックしてリリース ノートの最新版をダウンロードします。

ステップ 7 ダウンロードする各ソフトウェア バンドルについて、次の手順を実行します。

a) ダウンロードするリリースの最新のソフトウェア バンドルへのリンクをクリックします。
リリース番号の後には、数字と文字が括弧内に続きます。数字はメンテナンス リリース レベルを表し、文字はそのメンテナンス リリースのパッチを区別します。各メンテナンス リリースとパッチの内容の詳細については、最新版のリース ノートを参照してください。

b) 次のいずれかのボタンをクリックして、表示される指示に従います。

- [Download Now]：ソフトウェア バンドルをすぐにダウンロードできます。
- [Add to Cart]：後でダウンロードするソフトウェア バンドルをカートに追加します。

c) メッセージに従ってソフトウェア バンドルのダウンロードを完了します。

ステップ 8 Cisco UCS ドメインをアップグレードする前に、リリース ノートを参照してください。

次の作業

ソフトウェア バンドルをファブリック インターコネクトにダウンロードします。

離れた場所からのファブリックインターコネクトへのファームウェア イメージのダウンロード

はじめる前に

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] ノードをクリックします。

ステップ 3 [Work] ペインの [Firmware Management] タブをクリックします。

ステップ 4 [Installed Firmware] タブをクリックします。

ステップ 5 [Download Firmware] をクリックします。

ステップ 6 [Download Firmware] ダイアログボックスで、[Location of the Image File] フィールドの [Remote File System] オプション ボタンをクリックし、必須フィールドに入力します。

ステップ 7 [OK] をクリックします。
Cisco UCS Manager GUI によって、ファームウェア バンドルのファブリック インターコネクトへのダウンロードが開始されます。

ステップ 8 （任意） [Download Tasks] タブで、ダウンロードのステータスをモニタします。
（注） Cisco UCS Manager によって、ブートフラッシュの領域が不足していることが報告された場合は、[Packages] タブで古いバンドルを削除して、領域を解放します。ブートフラッシュの空き領域を表示するには、[Equipment] タブをクリックしてファブリック インターコネクトにナビゲートし、[General] タブの [Local Storage Information] 領域を展開します。

ステップ 9 必要なすべてのファームウェアバンドルがファブリックインターコネクトにダウンロードされるまで、このタスクを繰り返します。

次の作業

ローカル ファイル システムからファブリック インターコネクトへのファームウェア イメージのダウンロード

はじめる前に

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] ノードをクリックします。

ステップ 3 [Work] ペインの [Firmware Management] タブをクリックします。

ステップ 4 [Installed Firmware] タブをクリックします。

ステップ 5 [Download Firmware] をクリックします。

ステップ 6 [Download Firmware] ダイアログボックスで、[Location of the Image File] フィールドの [Local File System] オプション ボタンをクリックします。

ステップ 7 [Filename] フィールドに、フル パスとイメージ ファイルの名前を入力します。
ファームウェア イメージ ファイルが配置されているフォルダへの正確なパスがわからない場合は、[Browse] をクリックしてファイルにナビゲートします。

ステップ 8 [OK] をクリックします。
Cisco UCS Manager GUI によって、ファームウェア バンドルのファブリック インターコネクトへのダウンロードが開始されます。

ステップ 9 （任意） [Download Tasks] タブで、ダウンロードされたファームウェア バンドルのステータスをモニタします。

（注） Cisco UCS Manager によって、ブートフラッシュの領域が不足していることが報告された場合は、[Packages] タブで古いバンドルを削除して、領域を解放します。ブートフラッシュの空き領域を表示するには、[Equipment] タブのファブリック インターコネクトにナビゲートし、[General] タブの [Local Storage Information] 領域を展開します。

ステップ 10 必要なすべてのファームウェアバンドルがファブリックインターコネクトにダウンロードされるまで、このタスクを繰り返します。

次の作業

イメージ ダウンロードのキャンセル

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] ノードを展開します。

ステップ 3 [Work] ペインの [Firmware Management] タブをクリックします。

ステップ 4 [Download Tasks] タブで、キャンセルするタスクを右クリックし、[Delete] を選択します。

ファームウェア パッケージの内容の判断

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] ノードをクリックします。

ステップ 3 [Work] ペインの [Firmware Management] タブをクリックします。

ステップ 4 [Packages] サブタブで、パッケージの内容を表示するには、パッケージの横の [+] アイコンをクリックします。

ステップ 5 パッケージの内容のスナップショットを取得するには、次の手順を実行します。

a) イメージ名とその内容を含む行を強調表示します。

b) 右クリックし、[Copy] を選択します。

c) クリップボードの内容をテキスト ファイルまたはその他のドキュメントに貼り付けます。

ファブリック インターコネクトの空き領域のチェック

イメージのダウンロードが失敗した場合は、Cisco UCS でファブリック インターコネクトのブートフラッシュに十分な空き領域があるかどうかをチェックします。

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

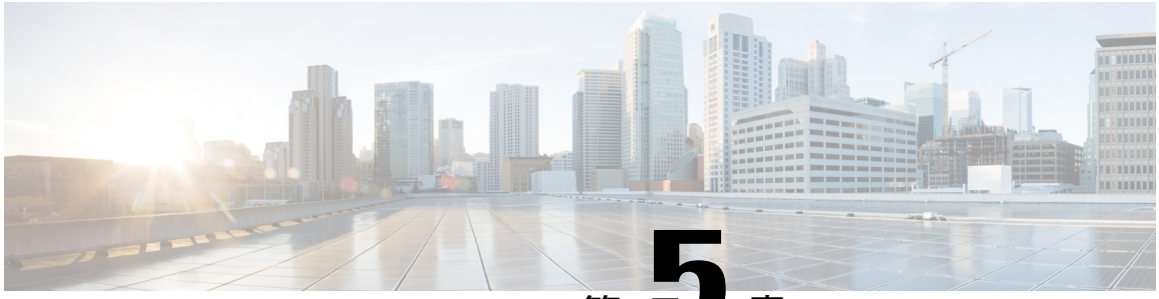
ステップ 2 [Equipment] > [Fabric Interconnects] の順に展開します。

ステップ 3 空き領域をチェックするファブリック インターコネクトをクリックします。

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

ステップ 5 [Local Storage Information] 領域を展開します。

ファームウェア イメージ バンドルをダウンロードする場合、ファブリック インターコネクトに、ファームウェア イメージ バンドルのサイズの少なくとも 2 倍の空き領域が必要です。ブートフラッシュに十分な領域がない場合は、ファブリック インターコネクトから、古いファームウェア、コア ファイル、その他の不要なオブジェクトを削除してください。



第 5 章

自動インストールによるファームウェアのアップグレード

この章は、次の項で構成されています。

自動インストール によるファームウェア アップグレード

自動インストールでは、次の 2 つの段階によって、Cisco UCS ドメインを 1 つのパッケージに含まれるファームウェア バージョンにアップグレードすることができます。

- インフラストラクチャ ファームウェアのインストール：Cisco UCS インフラストラクチャ ソフトウェア バンドルを使用して、ファブリック インターコネクト、I/O モジュール、Cisco UCS Manager などのインフラストラクチャ コンポーネントをアップグレードすることができます。
- サーバ ファームウェアのインストール：Cisco UCS B シリーズ ブレード サーバ ソフトウェア バンドルを使用して Cisco UCS ドメインのすべてのブレード サーバをアップグレードする、または Cisco UCS C シリーズ ラックマウント UCS 管理対象サーバ ソフトウェア バンドルを使用してすべてのラック サーバをアップグレードすることができます。

この 2 つの段階は独立したものであり、異なる時刻に実行することや、実行されるようにスケジュールすることができます。

自動インストールを使用して、インフラストラクチャ コンポーネントを Cisco UCS のあるバージョンに、またサーバ コンポーネントを異なるバージョンにアップグレードすることができます。

（注） ドメイン内の Cisco UCS Manager が Cisco UCS 2.1(1) より前のリリースである場合は、自動インストールを使用して、Cisco UCS ドメイン内のインフラストラクチャまたはサーバをアップグレードすることはできません。ただし、Cisco UCS Manager をリリース 2.1(1) 以降にアップグレードすると、自動インストールを使用して、ファームウェア レベルの最低要件を満たしている Cisco UCS ドメイン内の他のコンポーネントをアップグレードできます。詳細については、「自動インストールによるアップグレードに関する注意、ガイドライン、および制約事項, （28 ページ）」および該当する『Cisco UCS アップグレード ガイド』を参照してください。

自動インストール後の直接アップグレード

自動インストール中、デフォルト インフラストラクチャ パックのスタートアップ バージョンが設定されます。自動インストール後に Cisco UCS Manager、ファブリック インターコネクト、および IOM の直接アップグレードまたはアクティブ化を正常に完了するには、直接アップグレードまたはアクティブ化を開始する前に、スタートアップ バージョンがクリアされていることを確認します。デフォルト インフラストラクチャ パックのスタートアップ バージョンが設定されている場合、Cisco UCS Manager、ファブリック インターコネクト、および IOM を直接アップグレードまたはアクティブ化することはできません。デフォルトインフラストラクチャ パックのスタートアップ バージョンのクリア, （63 ページ） には、スタートアップ バージョンをクリアする詳細な手順が掲載されています。

インフラストラクチャ ファームウェアのインストール

インフラストラクチャ ファームウェアのインストール では、Cisco UCS Manager など、Cisco UCS ドメイン内のすべてのインフラストラクチャコンポーネントと、すべてのファブリックインターコネクトおよび I/O モジュールをアップグレードします。すべてのコンポーネントが、選択した Cisco UCS インフラストラクチャ ソフトウェア バンドルに含まれるファームウェア バージョンにアップグレードされます。

インフラストラクチャ ファームウェアのインストール では、Cisco UCS ドメイン ドメイン内の一部のインフラストラクチャ コンポーネントだけを対象とする部分アップグレードはサポートしていません。

メンテナンス ウィンドウに対応する特定の時刻にインフラストラクチャのアップグレードをスケジュールできます。ただし、インフラストラクチャのアップグレードが進行中の場合、別のインフラストラクチャのアップグレードをスケジュールすることはできません。次のアップグレードをスケジューリングするには、現在のアップグレードが完了するまで待つ必要があります。

（注） インフラストラクチャ ファームウェア アップグレードが今後行われる予定の場合は、キャンセルできます。ただし、インフラストラクチャ ファームウェア アップグレードがいったん開始すると、キャンセルすることはできません。

サーバ ファームウェアのインストール

サーバ ファームウェアのインストールでは、ホスト ファームウェア パッケージを使用して、Cisco UCS ドメイン内のすべてのサーバおよびコンポーネントをアップグレードします。サービス プロファイルに選択したホスト ファームウェア パッケージが含まれているサーバは、次のように、選択したソフトウェア バンドルのファームウェア バージョンにすべてアップグレードされます。

- シャーシ内のすべてのブレード サーバ用の Cisco UCS B シリーズ ブレード サーバ ソフトウェア バンドル。
- 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 サーバ用の Cisco UCS C シリーズ ラックマウント UCS 管理対象サーバ ソフトウェア バンドル。

（注） Install Server Firmware ウィザードの設定が完了した後で、サーバ ファームウェアのアップグレード プロセスをキャンセルすることはできません。Cisco UCS Manager は、変更を即座に反映します。ただし、サーバが実際にリブートされるタイミングは、サーバに関連付けられたサービス プロファイル内のメンテナンス ポリシーによって異なります。

自動インストールのための必要な手順

Cisco UCS ドメインのすべてのコンポーネントを同じパッケージ バージョンへアップグレードする場合は、自動インストールの各ステージを次の順序で実行する必要があります。

1. インフラストラクチャ ファームウェアのインストール
2. サーバ ファームウェアのインストール

この順序で実行すると、サーバのファームウェア アップグレードをインフラストラクチャのファームウェア アップグレードとは異なるメンテナンス ウィンドウにスケジュールすることができます。

自動インストールによるインフラストラクチャのファームウェアのアップグレード

Cisco UCS Manager GUI のリリースが 2.1(1) よりも古い場合、[Firmware Auto Install] タブは使用できません。

（注） ドメイン内の Cisco UCS Manager が Cisco UCS 2.1(1) より前のリリースである場合は、自動インストールを使用して、Cisco UCS ドメイン内のインフラストラクチャまたはサーバをアップグレードすることはできません。ただし、Cisco UCS Manager をリリース 2.1(1) 以降にアップグレードすると、自動インストールを使用して、ファームウェア レベルの最低要件を満たしている Cisco UCS ドメイン内の他のコンポーネントをアップグレードできます。詳細については、「自動インストールによるアップグレードに関する注意、ガイドライン、および制約事項, （28 ページ）」および該当する『Cisco UCS アップグレード ガイド』を参照してください。

はじめる前に

ファームウェアのアップグレードとダウングレードの前提条件, （37 ページ） に記載のすべての前提条件を満たす必要があります。

Cisco UCS ドメインが NTP サーバを使用して時間を設定しない場合、プライマリ ファブリック インターコネクトとセカンダリ ファブリックインターコネクトの時計が同期されていることを確認します。Cisco UCS Manager で NTP サーバを設定するか、時間を手動で同期することによってこれを行うことができます。

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] タブの [Equipment] ノードを展開します。

ステップ 3 [Work] ペインの [Firmware Management] タブをクリックします。

ステップ 4 [Work] ペインの [Firmware Auto Install] タブをクリックします。

ステップ 5 [Actions] 領域で、[Install Infrastructure Firmware] をクリックします。

ステップ 6 **[Install Infrastructure]** ダイアログ ボックスの [Prerequisites] ページで、先に進む前に警告に対処します。
警告は次のカテゴリに分類されています。

- 進行中の致命的または重大な障害があるかどうか。
- コンフィギュレーション バックアップが最近実行されているかどうか。
- 管理インターフェイスのモニタリング ポリシーが有効かどうか。
- 保留中のファブリック インターコネクトのリブート アクティビティがあるかどうか。
- NTP が設定されているかどうか。

各警告のハイパーリンクをクリックして直接処理することができます。処理した警告の各チェックボックスをオンにするか、警告を処理せずに続行する場合は [Ignore All] チェックボックスをオンにします。

ステップ 7 [Install Infrastructure Firmware] ダイアログボックスの [Properties] 領域で、次のフィールドに値を入力します。

名前	説明
[Name] フィールド	Cisco UCS によって作成および管理されるインフラストラクチャ パックの名前。このフィールドのデフォルト名を変更したり、カスタムインフラストラクチャ パックを作成することはできません。
[Description] フィールド	インフラストラクチャ パックのユーザ定義による説明。このフィールドはデフォルトで入力されています。ただし、必要に応じて独自の説明を入力することもできます。 256 文字以下で入力します。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。
[Version] ドロップダウン リスト	インフラストラクチャ コンポーネントのファームウェア アップグレードに使用できるソフトウェア バンドルのリスト。
[Force] チェックボックス	オンにすると、Cisco UCS では、選択したバージョンを前回インストールしようとしたときに失敗または中断した場合でも、インストールを試みます。

ステップ 8 [Install Infrastructure Firmware] ダイアログボックスの [Infrastructure Schedule] 領域で、次のいずれかの操作を実行します。

オプション	説明
[Start Time] フィールド	オカレンスが実行される日時。 フィールドの端にある下矢印をクリックして、カレンダーから日付を選択します。
[Upgrade Now] チェックボックス	オンにすると、Cisco UCS Manager は [Start Time][Start Time] フィールドフィールドを無視して、[OK] がクリックされるとすぐにインフラストラクチャ ファームウェアをアップグレードします。

ステップ 9 [OK] をクリックします。
[Firmware Auto Install] タブの [Firmware Installer] フィールドには、インフラストラクチャのファームウェア アップグレードのステータスが表示されます。

（注） ブートフラッシュに十分な空き領域がない場合、警告が表示され、アップグレード プロセスは停止します。

次の作業

プライマリ ファブリック インターコネクトのリブートを承認します。リブートを承認しない場合、Cisco UCS Manager はインフラストラクチャのアップグレードを完了できず、アップグレードは無期限に保留になります。

プライマリ ファブリック インター コネクトのリブートの確認

はじめる前に

注意 アップグレード時の中断を最小限に抑えるには、次のことを確認する必要があります。

- ファブリック インターコネクトのリブートを確認する前に、ファブリック インターコネクトに接続されているすべての IOM が稼動状態であることを確認します。すべての IOM が稼動状態ではない場合、ファブリック インターコネクトに接続されているすべてのサーバがただちに再検出され、大規模な中断が発生します。
- ファブリック インターコネクトとサービス プロファイルの両方がフェールオーバー用に設定されていることを確認します。
- プライマリ ファブリック インターコネクトのリブートを確認する前に、セカンダリ ファブリック インターコネクトからデータ パスが正常に復元されていることを確認します。詳細については、データ パスの準備が整っていることの確認, （115 ページ）を参照してください。

インフラストラクチャ ファームウェアをアップグレードした後、インフラストラクチャ ファームウェアのインストール は自動的にクラスタ設定内のセカンダリ ファブリック インターコネクトをリブートします。ただし、プライマリ ファブリック インターコネクトのリブートは、ユーザが承認する必要があります。リブートを承認しなかった場合、インフラストラクチャ ファームウェアのインストール はアップグレードを完了するのではなく、その承認を無期限に待ちます。

手順

ステップ 1 ツールバーの [Pending Activities] をクリックします。

ステップ 2 [Pending Activities] ダイアログボックスで、[User Acknowledged Activities] タブをクリックします。

ステップ 3 テーブルで、プライマリ ファブリック インターコネクトの保留中のリブートの行を探します。

ステップ 4 その行の[Reboot Now] カラムで [Acknowledge All] チェックボックスをオンにします。

ステップ 5 [OK] をクリックします。
Cisco UCS Manager によって、即座にプライマリ ファブリック インター コネクトがリブートされます。[OK] をクリックした後にこのリブートを停止することはできません。

インフラストラクチャファームウェアのアップグレードのキャンセル

（注） インフラストラクチャ ファームウェア アップグレードが今後行われる予定の場合は、キャンセルできます。ただし、インフラストラクチャ ファームウェア アップグレードがいったん開始すると、キャンセルすることはできません。

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] タブの [Equipment] ノードを展開します。

ステップ 3 [Work] ペインの [Firmware Management] タブをクリックします。

ステップ 4 [Work] ペインの [Firmware Auto Install] タブをクリックします。

ステップ 5 [Actions] 領域で、[Install Infrastructure Firmware] をクリックします。

ステップ 6 [Install Infrastructure Firmware] ダイアログボックスの [Actions] 領域で、[Cancel Infrastructure Upgrade] をクリックします。

ステップ 7 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ステップ 8 [OK] をクリックします。

デフォルト インフラストラクチャ パックのスタートアップ バージョンのクリア

Cisco UCS Manager、ファブリック インターコネクト、および IOM を直接アップグレードまたはアクティブ化する前に、デフォルト インフラストラクチャ パックのスタートアップ バージョンをクリアする必要があります。

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] ノードをクリックします。

ステップ 3 [Work] ペインの [Firmware Management] タブをクリックします。

ステップ 4 [Work] ペインの [Firmware Auto Install] タブをクリックします。

ステップ 5 [Actions] 領域で、[Clear Startup Version] をクリックします。

ステップ 6 表示される確認ダイアログボックスで [Yes] をクリックします。

ステップ 7 [OK] をクリックします。

自動インストールによるサーバ ファームウェアのアップグレード

Cisco UCS Manager GUI のリリースが 2.1(1) よりも古い場合、[Firmware Auto Install] タブは使用できません。

（注） ドメイン内の Cisco UCS Manager が Cisco UCS 2.1(1) より前のリリースである場合は、自動インストールを使用して、Cisco UCS ドメイン内のインフラストラクチャまたはサーバをアップグレードすることはできません。ただし、Cisco UCS Manager をリリース 2.1(1) 以降にアップグレードすると、自動インストールを使用して、ファームウェア レベルの最低要件を満たしている Cisco UCS ドメイン内の他のコンポーネントをアップグレードできます。詳細については、「自動インストールによるアップグレードに関する注意、ガイドライン、および制約事項, （28 ページ）」および該当する『Cisco UCS アップグレード ガイド』を参照してください。

（注） Install Server Firmware ウィザードの設定が完了した後で、サーバ ファームウェアのアップグレード プロセスをキャンセルすることはできません。Cisco UCS Manager は、変更を即座に反映します。ただし、サーバが実際にリブートされるタイミングは、サーバに関連付けられたサービス プロファイル内のメンテナンス ポリシーによって異なります。

はじめる前に

ファームウェアのアップグレードとダウングレードの前提条件, （37 ページ） に記載のすべての前提条件を満たす必要があります。

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] タブの [Equipment] ノードを展開します。

ステップ 3 [Work] ペインの [Firmware Management] タブをクリックします。

ステップ 4 [Work] ペインの [Firmware Auto Install] タブをクリックします。

ステップ 5 [Actions] 領域で、[Install Server Firmware] をクリックします。

ステップ 6 [Install Server Firmware] ウィザードの [Prerequisites] ページで、このページに一覧されている前提条件とガイドラインを慎重に確認してから、次のいずれかを実行してください。

- 前提条件をすべて満たしている場合は、[Next] をクリックします。
- 前提条件をすべて満たしていない場合は [Cancel] をクリックして、サーバのファームウェアをアップグレードする前に前提条件を満たしてください。

ステップ 7 [Install Server Firmware] ウィザードの [Select Package Versions] ページで、次の手順を実行します。

a) Cisco UCS ドメインにブレード サーバが含まれている場合は、[B-Series Blade Server Software] 領域の[New Version] ドロップダウン リストから、これらのサーバをアップグレードするソフトウェア バンドルを選択します。

b) Cisco UCS ドメインにラックマウント サーバが含まれている場合は、[C-Series Rack-Mount Server Software] 領域の[New Version] ドロップダウン リストから、これらのサーバをアップグレードするソフトウェア バンドルを選択します。
Cisco UCS ドメインにブレード サーバとラック サーバの両方が含まれている場合は、[Select Package Versions] ページで B シリーズ ブレード サーバおよび C シリーズ ラックマウント サーバの新しいファームウェア バージョンを選択して、ドメイン内のすべてのサーバをアップグレードすることを推奨します。

（注） デフォルトのホスト ファームウェア パッケージを更新すると、関連付けられていないサーバと、ホスト ファームウェア パッケージを含まないサービス プロファイルを持つサーバのファームウェアがアップグレードされることがあります。このファームウェア アップグレードにより、サービス プロファイルで定義されたメンテナンス ポリシーに従ってこれらのサーバのリブートが発生する可能性があります。

c) [Next] をクリックします。

ステップ 8 [Install Server Firmware] ウィザードの [Select Host Firmware Packages] ページで、次の手順を実行します。

a) 選択したソフトウェアで更新するホスト ファームウェア パッケージが含まれる各組織のノードを展開します。

b) 更新する各ホスト ファームウェア パッケージの名前の隣にあるチェックボックスをオンにします。
この手順によって、選択したホスト ファームウェア パッケージが新しいバージョンのファームウェアによって更新されます。すべてのサーバを更新するには、Cisco UCS ドメインのすべてのサーバに関連付けられたサービス プロファイルに含まれているホスト ファームウェア パッケージを選択する必要があります。

c) [Next] をクリックします。

ステップ 9 [Install Server Firmware] ウィザードの [Host Firmware Package Dependenciess] ページで、次の手順を実行します。

a) テーブルに表示される各ホスト ファームウェア パッケージのノードを展開します。

b) ホスト ファームウェア パッケージが含まれるサービス プロファイルのリストを確認します。

c) 必要に応じて、次のいずれかのカラムにあるリンクをクリックします。

- [Host Pack DN] カラム：ホスト ファームウェア パッケージのナビゲータを開きます。
- [Service Profile DN] カラム：サービス プロファイルのナビゲータを開きます。

d) 次のいずれかを実行します。

- 選択したホスト ファームウェア パッケージを 1 つ以上変更する場合は、[Prev] をクリックします。
- 適切なホストのファームウェアパッケージを選択済みで、エンドポイントのサーバファームウェアのアップグレードの影響を確認する場合は、[Next] をクリックします。
- サーバのアップグレードをただちに開始する場合は、[Install] をクリックします。

ステップ 10 [Install Server Firmware] ウィザードの [Impacted Endpoints Summary] ページで、次の手順を実行します。

a) [Impacted Endpoints] テーブルで結果をフィルタリングするには、該当するチェックボックスをクリックします。
結果は、エンドポイントのタイプや、アップグレードの影響が重大であるかどうかによってフィルタリングできます。

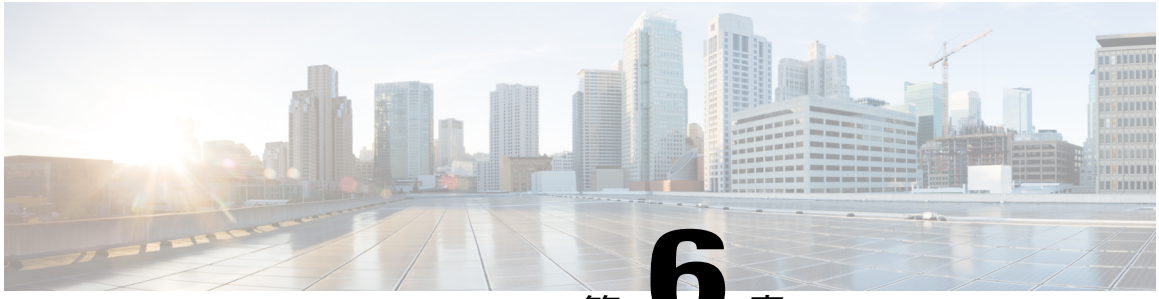
b) 影響を受けるエンドポイントのリストを確認します。

c) 必要に応じて、[Maintenance Policy] カラムのリンクをクリックして、そのポリシーのナビゲータを開きます。

d) 次のいずれかを実行します。

- 選択したホスト ファームウェア パッケージを 1 つ以上変更する場合は、[Prev] をクリックします。
- 適切なホスト ファームウェア パッケージを選択済みで、サーバのアップグレードを開始する場合は、[Install] をクリックします。

ステップ 11 （任意） サーバ ファームウェアのアップグレードの進行状況をチェックするには、アップグレードする各サーバの [FSM] タブをチェックします。
[Firmware Auto Install] タブの [Firmware Installer] フィールドには、インフラストラクチャ ファームウェアのアップグレードのステータスだけが表示されます。



第 6 章

ファームウェア自動同期サーバ ポリシーの使用

この章は、次の項で構成されています。

ファームウェアの自動同期

Cisco UCS Manager で [Firmware Auto Sync Server] ポリシーを使用して、新たに検出されたサーバのファームウェア バージョンをアップグレードする時期と方法を指定できます。このポリシーを使用すると、新たに検出された、関連付けられていないサーバのファームウェア バージョンをアップグレードして、デフォルトのホストファームウェアパックで定義されているファームウェアバージョンと一致させることができます。さらに、ファームウェアのアップグレードプロセスをサーバの検出直後に実行するか、後で実行するかを指定することもできます。

重要 ファームウェアの自動同期はデフォルトのホスト ファームウェア パックに基づいています。デフォルトのホスト ファームウェア パックを削除すると、Cisco UCS Manager で重大な問題が発生します。デフォルトのホスト ファームウェア パックは設定されているが、ブレード サーバまたはラックサーバのファームウェアが指定も設定もされていない場合は、軽度の問題が発生します。問題が発生した場合は、その程度に関係なく、[Firmware Auto Sync Server] ポリシーを設定する前にそれらの問題を解決する必要があります。

[Firmware Auto Sync Server] ポリシーの値は次のとおりです。

- [User Acknowledge]：[Pending Activities] ダイアログボックスで管理者がアップグレードを確認するまでサーバのファームウェアは同期されません。
- [No Action]：ファームウェアのアップグレードはサーバで開始されません。

このポリシーは Cisco UCS Manager GUI または Cisco UCS Manager CLI から設定できます。サーバのファームウェアは、次の状況が生じた場合に自動的にトリガーされます。

- サーバまたはサーバのエンドポイントのファームウェア バージョンがデフォルトのホスト ファームウェア パックで設定されているファームウェア バージョンと異なる場合。
- [Firmware Auto Sync Server] ポリシーの値が変更された場合。たとえば、最初に値を [No Action] に設定し、後から [User Acknowledge] に変更した場合などです。

重要 Cisco UCS Manager が Cisco UCS ドメインとしてCisco UCS Central に登録されている場合、このポリシーはローカル ポリシーとして実行されます。デフォルトのホスト ファームウェア パックが Cisco UCS Manager で定義されていない場合や削除された場合、このポリシーは実行されません。

ファームウェア自動同期サーバ ポリシーの設定

このポリシーを使用すると、新たに検出された、関連付けられていないサーバについて、そのファームウェア バージョンの更新時期と更新方法を設定することができます。

サーバの特定のエンドポイントのファームウェアバージョンがデフォルトのホストファームウェア パックのバージョンと異なる場合、Cisco UCS Manager の FSM の状態には、その特定のエンドポイントの更新ステータスのみが表示されます。サーバのファームウェア バージョンは更新されません。

はじめる前に

- このポリシーを設定するには、事前にデフォルトのホスト ファームウェア パックを作成しておく必要があります。
- このタスクを完了するには、管理者としてログインしている必要があります。

手順

ステップ 1 [Navigation] ペインで、[Equipment] タブをクリックします。

ステップ 2 [Equipment] タブの [Equipment] ノードを展開します。

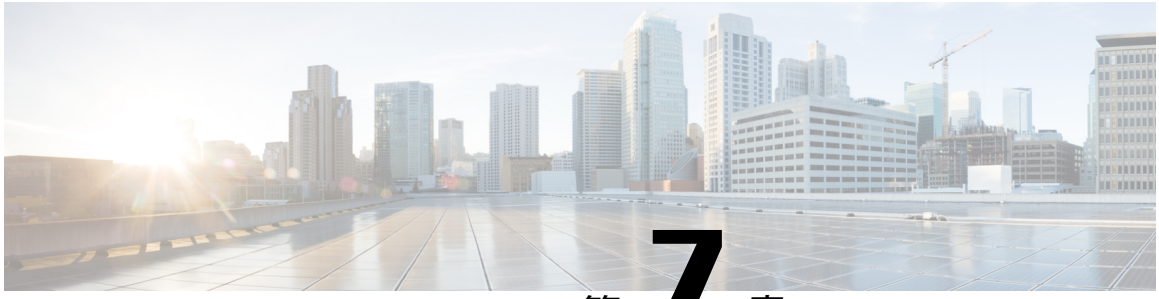
ステップ 3 [Work] ペインで、[Policies] タブをクリックします。

ステップ 4 [Global Policies] サブタブをクリックします。

ステップ 5 [Firmware Auto Sync Server Policy] 領域で、[Sync State] の値として次のいずれかを選択します。

- [User Acknowledge]：[Pending Activities] ダイアログボックスで管理者がアップグレードを確認するまでサーバのファームウェアは同期されません。
- [No Action]：ファームウェアのアップグレードはサーバで開始されません。

ステップ 6 [Save Changes] をクリックします。



第 7 章

エンドポイントのファームウェアの直接アップグレード

この章は、次の項で構成されています。

エンドポイントでの直接のファームウェアのアップグレード

正しい手順に従って、正しい順序でアップグレードを適用すれば、エンドポイントの直接のファームウェア アップグレードと新しいファームウェア バージョンのアクティブ化による、Cisco UCS ドメインのトラフィックの中断を最小限に留めることができます。

次のエンドポイントのファームウェアを直接アップグレードできます。

- アダプタ
- CIMC
- I/O モジュール

- ボード コントローラ
- Cisco UCS Manager
- ファブリック インターコネクト

アダプタおよびボードコントローラ ファームウェアも、サービスプロファイル内のホストファームウェア パッケージによってアップグレードできます。ホスト ファームウェア パッケージを使用して、このファームウェアをアップグレードする場合、ファームウェアのアップグレード プロセス中に、サーバをリブートする必要がある回数を削減できます。

（注） 管理ファームウェア パッケージによる CIMC のアップグレードまたは、サーバに関連付けられたサービス プロファイル内のファームウェア パッケージによるアダプタのアップグレードは、直接のファームウェア アップグレードより優先されます。サーバに関連付けられたサービス プロファイルにファームウェア パッケージが含まれる場合、エンドポイントを直接アップグレードすることはできません。直接のアップグレードを実行するには、サービスプロファイルからファームウェア パッケージを削除する必要があります。

直接のファームウェア アップグレードのステージ

Cisco UCS Manager は直接アップグレードのプロセスを 2 つのステージに分け、サーバやその他のエンドポイントのアップタイムに影響を与えずに、システムの実行中にエンドポイントにファームウェアをプッシュできるようにします。

アップデート

このステージでは、選択したファームウェア バージョンがプライマリ ファブリック インターコネクトから、エンドポイントのバックアップ パーティションにコピーされ、ファームウェア イメージが破損していないことが確認されます。アップデートプロセスでは、常にバックアップ スロットのファームウェアが上書きされます。

アップデート ステージは、次のエンドポイントにのみ適用されます。

- アダプタ
- CIMC
- I/O モジュール

アクティブ化

このステージでは、指定したイメージバージョン（通常はバックアップバージョン）がスタートアップ バージョンとして設定され、[Set Startup Version Only] を指定していない場合、エンドポイントがただちにリブートされます。エンドポイントがリブートされると、バックアップ パーティションがアクティブなパーティションになり、アクティブなパーティションがバックアップ パーティションになります。新しいアクティブなパーティションのファームウェアはスタートアップバージョンおよび実行されているバージョンになります。

指定したファームウェア イメージがすでにエンドポイントに存在するため、次のエンドポイントのみアクティベーションが必要です。

- Cisco UCS Manager
- ファブリック インターコネクト
- それらをサポートするサーバ上のボード コントローラ

ファームウェアをアクティブにすると、エンドポイントがリブートされ、新しいファームウェアがアクティブなカーネル バージョンおよびシステム バージョンになります。スタートアップ ファームウェアからエンドポイントをブートできない場合、デフォルトがバックアップ バージョンに設定され、エラーが生成されます。

注意 I/O モジュールに対して [Set Startup Version Only] を設定した場合、そのデータ パス内のファブリック インターコネクトがリブートされると、I/O モジュールがリブートされます。I/O モジュールに対して、[Set Startup Version Only] を設定しない場合、I/O モジュールがリブートし、トラフィックが中断します。また、Cisco UCS Manager がファブリック インターコネクトと I/O モジュールの間のプロトコルとファームウェア バージョンの不一致を検出した場合、Cisco UCS Manager は、ファブリック インターコネクトのファームウェアに一致するファームウェア バージョンを使用して I/O モジュールを自動的に更新し、ファームウェアをアクティブ化して、I/O モジュールを再度リブートします。

直接のファームウェア アップグレードの停止の影響

エンドポイントで、直接のファームウェア アップグレードを実行する場合、Cisco UCS ドメインで、1 つ以上のエンドポイントでトラフィックの中断や、停止が発生することがあります。

ファブリック インターコネクト ファームウェア アップグレードの停止の影響

ファブリック インターコネクトのファームウェアをアップグレードする場合、次の停止の影響や中断が発生します。

- ファブリック インターコネクトがリブートします。
- 対応する I/O モジュールがリブートします。

Cisco UCS Manager ファームウェア アップグレードの停止の影響

Cisco UCS Manager へのファームウェア アップグレードにより、次の中断が発生します。

- Cisco UCS Manager GUI：Cisco UCS Manager GUI にログインしているすべてのユーザがログアウトされ、それらのセッションが終了します。

  実行中の保存されていない作業が失われます。
- Cisco UCS Manager CLI：telnet によってログインしているすべてのユーザがログアウトされ、それらのセッションが終了します。

I/O モジュール ファームウェア アップグレードの停止の影響

I/O モジュールのファームウェアをアップグレードする場合、次の停止の影響と中断が発生します。

- 単一のファブリック インターコネクトのスタンドアロン設定の場合、I/Oモジュールのリブート時にデータ トラフィックが中断されます。2つのファブリック インターコネクトのクラスタ設定の場合、データ トラフィックは他方のI/Oモジュールおよびそのデータ パス内のファブリック インターコネクトにフェールオーバーします。
- 新しいファームウェアをスタートアップ バージョンとしてのみアクティブにした場合、対応するファブリック インターコネクトがリブートされると、I/Oモジュールがリブートします。
- 新しいファームウェアを実行されているバージョンおよびスタートアップ バージョンとしてアクティブにした場合、I/O モジュールがただちにリブートします。
- ファームウェアのアップグレード後に、I/O モジュールを使用できるようになるまで最大 10 分かかります。

CIMC ファームウェア アップグレードの停止の影響

サーバの CIMC のファームウェアをアップグレードした場合、CIMC と内部プロセスのみが影響を受けます。サーバ トラフィックは中断しません。このファームウェアアップグレードにより、CIMC に次の停止の影響と中断が発生します。

- KVM コンソールおよび vMedia によってサーバで実行されているすべてのアクティビティが中断されます。
- すべてのモニタリングおよび IPMI ポーリングが中断されます。

アダプタ ファームウェア アップグレードの停止の影響

アダプタのファームウェアをアクティブにし、[Set Startup Version Only] オプションを設定していない場合、次の停止の影響と中断が発生します。

- サーバがリブートします。
- サーバ トラフィックが中断します。

複数のエンドポイントのファームウェアのアップデート

この手順は、次のエンドポイント上のファームウェアをアップデートする場合に使用できます。

- アダプタ
- CIMC
- I/O モジュール

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] タブの [Equipment] ノードを展開します。

ステップ 3 [Work] ペインの [Firmware Management] タブをクリックします。

ステップ 4 [Installed Firmware] タブの [Update Firmware] をクリックします。
Cisco UCS Manager GUI によって、[Update Firmware] ダイアログボックスが開き、Cisco UCS ドメインのすべてのエンドポイントのファームウェア バージョンが確認されます。このステップは、シャーシとサーバの数に基づいて数分かかる場合があります。

ステップ 5 [Update Firmware] ダイアログボックスで、次の操作を実行します。

a) メニュー バーの [Filter] ドロップダウン リストから [ALL] を選択します。
すべてのアダプタやサーバの BIOS など、特定のタイプのすべてのエンドポイントのファームウェアをアップデートする場合は、そのタイプをドロップダウン リストから選択します。

b) [Select] フィールドで、次のいずれかの手順を実行します。

- すべてのエンドポイントを同じバージョンにアクティブ化するには、[Version] オプション ボタンをクリックし、[Set Version] ドロップダウン リストから適切なバージョンを選択します。
- すべてのエンドポイントを特定のバンドルに含まれるファームウェア バージョンにアクティブ化するには、[Bundle] オプション ボタンをクリックし、[Set Bundle] ドロップダウン リストから適切なバンドルを選択します。

c) [OK] をクリックします。
1 つ以上のエンドポイントを直接更新できない場合は、Cisco UCS Manager によって通知メッセージが表示されます。通知メッセージを確認した後、Cisco UCS Manager によって、サーバ上にある直接更新可能な他のすべてのエンドポイントのファームウェアが更新されます。

Cisco UCS Manager によって、選択したファームウェア イメージがバックアップ メモリ パーティションにコピーされ、そのイメージが破損していないことが確認されます。イメージは、アクティブにされるまで、バックアップ バージョンとして残ります。Cisco UCS Manager により、すべての更新が同時に開始されます。ただし、アップデートによって、完了する時間が異なることがあります。

[Update Firmware] ダイアログボックスで、すべてのアップデート済みエンドポイントについて、[Update Status] カラムに [ready] と表示されると、アップデートは完了です。

ステップ 6 （任意） 特定のエンドポイントのアップデートの進捗をモニタするには、エンドポイントを右クリックし、[Show Navigator] を選択します。
Cisco UCS Manager によって、[General] タブの [Update Status] 領域に進捗が表示されます。ナビゲータに [FSM] タブがある場合は、そこでも進捗をモニタできます。[Retry #] フィールドのエントリが、アップデートが失敗したことを示していない場合があります。再試行回数には、Cisco UCS Manager が更新ステータスを取得するときに発生する再試行も含まれます。

次の作業

アダプタ ファームウェア

アダプタのファームウェアのアップデート

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] > [Chassis] > *[Chassis Number]* > [Servers] の順に展開します。

ステップ 3 アップデートするアダプタがインクルードされたサーバのノードを展開します。

ステップ 4 [Adapters] を展開し、アップグレードするアダプタを選択します。

ステップ 5 [General] タブで [Update Firmware] をクリックします。

ステップ 6 [Update Firmware] ダイアログボックスで、次の操作を実行します。

a) [Version] ドロップダウン リストから、エンドポイントをアップデートするファームウェア バージョンを選択します。

b) [OK] をクリックします。
1 つ以上のエンドポイントを直接更新できない場合は、Cisco UCS Manager によって通知メッセージが表示されます。通知メッセージを確認した後、Cisco UCS Manager によって、サーバ上にある直接更新可能な他のすべてのエンドポイントのファームウェアが更新されます。

Cisco UCS Manager によって、選択されたファームウェア パッケージがバックアップ メモリ スロットにコピーされ、アクティブ化されるまでバックアップとして留まります。

ステップ 7 （任意） [Update Status] 領域でアップデートのステータスをモニタします。
アップデート プロセスは数分かかることがあります。[General] タブの [Firmware] 領域の [Backup Version] フィールドに、選択したファームウェア パッケージが表示されるまで、ファームウェアをアクティブにしないでください。

次の作業

アダプタでのファームウェアのアクティブ化

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] > [Chassis] > *[Chassis Number]* > [Servers] の順に展開します。

ステップ 3 アップデートしたファームウェアをアクティブにするアダプタが搭載されているサーバのノードを展開します。

ステップ 4 [Adapters] を展開し、ファームウェアをアクティブ化するアダプタを選択します。

ステップ 5 [General] タブの [Activate Firmware] をクリックします。

ステップ 6 [Activate Firmware] ダイアログボックスで、次の操作を実行します。

a) [Version To Be Activated] ドロップダウン リストから、適切なバージョンを選択します。
1 つ以上の選択したエンドポイントがバックアップ バージョンとして必要なバージョンで設定されていない場合は、[Set Version] ドロップダウン リストにそのバージョンが表示されません。各エンドポイントについて、[Startup Version] カラムからバージョンを選択する必要があります。

b) スタートアップ バージョンを設定し、エンドポイントで実行しているバージョンを変更しない場合、[Set Startup Version Only] チェックボックスをオンにします。
直接のアップグレード時に、アダプタに [Set Startup Version Only] を設定する必要があります。この設定では、アクティブ化されたファームウェアが pending-next-boot 状態に移行し、サーバがすぐにリブートしません。アクティブ化されたファームウェアは、サーバがリブートされるまで、アダプタで実行されているバージョンのファームウェアになりません。ホスト ファームウェア パッケージのアダプタに [Set Startup Version Only] を設定することはできません。

サーバがサービス プロファイルに関連付けられない場合、アクティブ化されたファームウェアは pending-next-boot 状態を維持します。Cisco UCS Manager は、サーバがサービス プロファイルに関連付けられるまで、エンドポイントをリブートせず、ファームウェアをアクティブにしません。必要に応じて、関連付けられていないサーバを手動でリブートまたはリセットして、ファームウェアをアクティブにできます。

c) [OK] をクリックします。

BIOS ファームウェア

サーバの BIOS ファームウェアのアップデート

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] > [Chassis] > *[Chassis Number]* > [Servers] の順に展開します。

ステップ 3 BIOS ファームウェアをアップデートするサーバのノードを展開します。

ステップ 4 [General] タブで [Inventory] タブをクリックします。

ステップ 5 [Motherboard] タブをクリックします。

ステップ 6 [Actions] 領域で [Update Bios Firmware] をクリックします。

ステップ 7 [Update Firmware] ダイアログボックスで、次の操作を実行します。

a) [Version] ドロップダウン リストから、サーバの BIOS のアップデートの対象となるファームウェア バージョンを選択します。

b) （任意） 互換性のない可能性や、現在実行中のタスクに関係なく、ファームウェアをアップデートする場合は、[Force] チェックボックスをオンにします。

c) [OK] をクリックします。

Cisco UCS Manager により、選択したサーバの BIOS ファームウェア パッケージがバックアップ メモリ スロットにコピーされますが、明示的にアクティブ化されるまで、バックアップのままです。

アップデートが完了すると、[Motherboard] タブの [BIOS] 領域で、[Backup Version] の [Update Status] カラムに [Ready] と表示されます。

次の作業

サーバの BIOS ファームウェアのアクティブ化

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] > [Chassis] > *[Chassis Number]* > [Servers] の順に展開します。

ステップ 3 アップデートした BIOS ファームウェアをアクティブ化するサーバのノードを展開します。

ステップ 4 [General] タブで [Inventory] タブをクリックします。

ステップ 5 [Motherboard] タブをクリックします。

ステップ 6 [Actions] 領域で [Activate Bios Firmware] をクリックします。

ステップ 7 [Activate Firmware] ダイアログボックスで、次の操作を実行します。

a) [Version To Be Activated] ドロップダウン リストから、適切なサーバ BIOS のバージョンを選択します。

b) スタートアップ バージョンを設定し、サーバで実行しているバージョンを変更しない場合は、[Set Startup Version Only] チェックボックスをオンにします。
[Set Startup Version Only] を設定した場合は、アクティブ化されたファームウェアが pending-next-boot 状態に移行し、サーバはすぐにはリブートされません。アクティブ化されたファームウェアは、サーバがリブートされるまでは、実行されているバージョンのファームウェアへ変更されません。

c) [OK] をクリックします。

CIMC ファームウェア

サーバの CIMC ファームウェアのアップデート

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] > [Chassis] > *[Chassis Number]* > [Servers] の順に展開します。

ステップ 3 CIMC をアップデートするサーバのノードを展開します。

ステップ 4 [General] タブで [Inventory] タブをクリックします。

ステップ 5 [CIMC] タブをクリックします。

ステップ 6 [Actions] 領域で [Update Firmware] をクリックします。

ステップ 7 [Update Firmware] ダイアログボックスで、次の操作を実行します。

a) [Version] ドロップダウン リストから、エンドポイントをアップデートするファームウェア バージョンを選択します。

b) [OK] をクリックします。

Cisco UCS Manager によって、選択されたファームウェア パッケージがバックアップ メモリ スロットにコピーされ、アクティブ化されるまでバックアップとして留まります。

ステップ 8 （任意） [Update Status] 領域でアップデートのステータスをモニタします。
アップデート プロセスは数分かかることがあります。[General] タブの [Firmware] 領域の [Backup Version] フィールドに、選択したファームウェア パッケージが表示されるまで、ファームウェアをアクティブにしないでください。

次の作業

サーバの CIMC ファームウェアのアクティブ化

CIMC のファームウェアのアクティベーションによって、データ トラフィックは中断しません。ただし、すべての KVM セッションに割り込み、サーバに接続しているすべての vMedia が切断されます。

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] > [Chassis] > *[Chassis Number]* > [Servers] の順に展開します。

ステップ 3 アップデートしたファームウェアをアクティブにする対象の Cisco Integrated Management Controller（CIMC）が搭載されているサーバのノードを展開します。

ステップ 4 [General] タブで [Inventory] タブをクリックします。

ステップ 5 [CIMC] タブをクリックします。

ステップ 6 [Actions] 領域の [Activate Firmware] をクリックします。

ステップ 7 [Activate Firmware] ダイアログボックスで、次の操作を実行します。

a) [Version To Be Activated] ドロップダウン リストから、適切なバージョンを選択します。
1 つ以上の選択したエンドポイントがバックアップ バージョンとして必要なバージョンで設定されていない場合は、[Set Version] ドロップダウン リストにそのバージョンが表示されません。各エンドポイントについて、[Startup Version] カラムからバージョンを選択する必要があります。

b) スタートアップ バージョンを設定し、エンドポイントで実行しているバージョンを変更しない場合、[Set Startup Version Only] チェックボックスをオンにします。
[Set Startup Version Only] を設定した場合は、アクティブ化されたファームウェアが pending-next-boot 状態に移行して、エンドポイントがすぐにリブートしません。アクティブ化されたファームウェアは、エンドポイントがリブートするまで、実行中のファームウェアのバージョンになりません。

c) [OK] をクリックします。

IOM ファームウェア

IOM のファームウェアのアップデート

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] > [Chassis] > *[Chassis Number]* > [IO Modules] の順に展開します。

ステップ 3 アップデートする I/O モジュールをクリックします。

ステップ 4 [General] タブで [Update Firmware] をクリックします。

ステップ 5 [Update Firmware] ダイアログボックスで、次の操作を実行します。

a) [Version] ドロップダウン リストから、エンドポイントをアップデートするファームウェア バージョンを選択します。

b) [OK] をクリックします。

Cisco UCS Manager によって、選択されたファームウェア パッケージがバックアップ メモリ スロットにコピーされ、アクティブ化されるまでバックアップとして留まります。

ステップ 6 （任意） [Update Status] 領域でアップデートのステータスをモニタします。
アップデート プロセスは数分かかることがあります。[General] タブの [Firmware] 領域の [Backup Version] フィールドに、選択したファームウェア パッケージが表示されるまで、ファームウェアをアクティブにしないでください。

次の作業

複数の IOM でのファームウェアのアクティブ化

この手順により、これらのエンドポイントのファームウェアのアクティベーションで、データ トラフィックの中断を最小限に抑えることができます。正しいオプションを設定した次の順序でエンドポイントをアクティブにしないと、エンドポイントがリブートし、データ トラフィックが一時中断する可能性があります。

⚠ **注意**

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] タブの [Equipment] ノードを展開します。

ステップ 3 [Work] ペインの [Firmware Management] タブをクリックします。

ステップ 4 [Installed Firmware] タブの [Activate Firmware] をクリックします。
1 つ以上の選択したエンドポイントがバックアップ バージョンとして必要なバージョンで設定されていない場合は、[Set Version] ドロップダウン リストにそのバージョンが表示されません。各エンドポイントについて、[Startup Version] カラムからバージョンを選択する必要があります。

ステップ 5 IOM ファームウェアをアクティブにするには、[Activate Firmware] ダイアログボックスで、次の手順を実行します。

a) [Filter] ドロップダウン リストから、[IO Modules] を選択します。
b) [Set Version] ドロップダウン リストから、現在の 2.0 リリースのバージョンを選択します。
c) [Ignore Compatibility Check] チェックボックスをオンにします。
d) [Set Startup Version Only] チェックボックスをオンにします。

重要 I/O モジュールに対して [Set Startup Version Only] を設定した場合、そのデータ パス内のファブリック インターコネクトがリブートされると、I/O モジュールがリブートされます。I/O モジュールに対して、[Set Startup Version Only] を設定しない場合、I/O モジュールがリブートし、トラフィックが中断します。また、Cisco UCS Manager がファブリック インターコネクトと I/O モジュールの間のプロトコルとファームウェア バージョンの不一致を検出した場合、Cisco UCS Manager は、ファブリック インターコネクトのファームウェアに一致するファームウェア バージョンを使用して I/O モジュールを自動的に更新し、ファームウェアをアクティブ化して、I/O モジュールを再度リブートします。

e) [Apply] をクリックします。
すべての IOM の [Activate Status] カラムに [pending-next-boot] が表示されている場合は、ステップ 6 に進みます。

ステップ 6 [OK] をクリックします。

IOM でのファームウェアのアクティブ化

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] > [Chassis] > *[Chassis Number]* > [IO Modules] の順に展開します。

ステップ 3 アップデートしたファームウェアをアクティブにする I/O モジュールが含まれている、[IO Module] ノードを選択します。

ステップ 4 [General] タブの [Activate Firmware] をクリックします。

ステップ 5 [Activate Firmware] ダイアログボックスで、次の操作を実行します。

a) [Version To Be Activated] ドロップダウン リストから、適切なバージョンを選択します。
1 つ以上の選択したエンドポイントがバックアップ バージョンとして必要なバージョンで設定されていない場合は、[Set Version] ドロップダウン リストにそのバージョンが表示されません。各エンドポイントについて、[Startup Version] カラムからバージョンを選択する必要があります。

b) スタートアップ バージョンを設定し、エンドポイントで実行しているバージョンを変更しない場合、[Set Startup Version Only] チェックボックスをオンにします。
[Set Startup Version Only] を設定した場合は、アクティブ化されたファームウェアが pending-next-boot 状態に移行して、エンドポイントがすぐにリブートしません。アクティブ化されたファームウェアは、エンドポイントがリブートするまで、実行中のファームウェアのバージョンになりません。

c) [OK] をクリックします。

ボード コントローラ ファームウェア

ボード コントローラは、すべての B シリーズ ブレード サーバと C シリーズ ラック サーバ用のさまざまなプログラマブルロジックおよび電源コントローラを管理します。ボードコントローラ更新ユーティリティを使用すると、重要なハードウェアを更新することができます。

Cisco UCS Managerリリース 2.1(2a) で導入されたボード コントローラを使用すると、ボード コントローラ更新ユーティリティを使用してデジタル コントローラ コンフィギュレーション ファイルを更新することにより、電圧レギュレータなどのコンポーネントを最適化できます。これより前のリリースでは、電圧レギュレータを更新するには物理コンポーネントを変更する必要がありました。これらの更新はハードウェア レベルであり、下位互換性を保つように設計されています。したがって、ボード コントローラのバージョンを最新に保つことが常に望まれます。

Cisco UCS B シリーズ M3 および M4 ブレード サーバのボード コントローラ ファームウェアのアクティブ化に関する注意事項

次の注意事項は、Cisco UCS B シリーズ M3 および M4 ブレード サーバのボード コントローラ ファームウェアに適用されます。

- ボード コントローラ ファームウェアをダウングレードする必要はありません。
- ブレード サーバのボード コントローラ ファームウェア バージョンは、インストール済みソフトウェア バンドルと同じか、または新しいバージョンである必要があります。ボード コントローラ ファームウェアのバージョンが、既存の Cisco UCS 環境で実行されているバージョンよりも新しい場合でも、ソフトウェア マトリックスまたは TAC のサポート範囲には違反しません。
- ボード コントローラ ファームウェアの更新は、他のコンポーネントのファームウェアと下位互換性があります。

リリース 2.2(4b) より前のリリースで実行されている一部の Cisco UCS B200 M4 ブレード サーバは、CSCuu15465 に掲載されている誤った Cisco UCS Manager アラートを生成する場合があります。この誤ったボード コントローラ不一致アラートは、Cisco UCS Manager 機能カタログ 2.2(4c)T および 2.2(5b)T で解決されました。機能カタログ 2.2(4c)T または 2.2(5b)T のいずれかを使用する場合、このアラートは表示されなくなります。

（注） 詳細については、https://tools.cisco.com/bugsearch/bug/CSCuu15465 を参照してください。

機能カタログの更新は、次の手順で適用できます。

1. 2.2(4c) Infra/Catalog または 2.2(5b) Infra/Catalog ソフトウェア バンドルをダウンロードします。Cisco UCS Manager でのファームウェアのダウンロードと管理, （49 ページ） には、ソフトウェア バンドルのダウンロードに関する詳細情報が掲載されています。
2. カタログ バージョン 2.2(4c)T または 2.2(5b)T（または含まれているカタログ バージョン）をロードしてカタログをアクティブにします。「機能カタログ更新のアクティブ化」には、Cisco UCS Manager で機能カタログをアクティブ化する方法の詳細が掲載されています。

3 新しく挿入されたブレード サーバを停止します。

4 以前のボードコントローラ バージョンがあるホスト ファームウェア パック ポリシーにサービス プロファイルを関連付けます。

サービス プロファイルが更新されたホスト ファームウェア パック ポリシーに関連付けられると、誤った不一致アラート（CSCuu15465 のバグによるものなど）は発生しなくなります。

5 [Save（保存）] をクリックします。

6 ブレード サーバを再検出します。

Cisco UCS C シリーズ M3 および M4 ラック サーバのボード コントローラ ファームウェアのアクティブ化に関する注意事項

次の注意事項は、Cisco UCS C シリーズ M3 および M4 ラック サーバのボード コントローラ ファームウェアに適用されます。

- ボード コントローラ ファームウェアと CIMC ファームウェアは、同じパッケージ バージョンのものである必要があります。
- Cisco UCS C220 M4 または C240 M4 サーバの C シリーズ サーバ ファームウェアを Cisco UCS Manager 2.2(6c) にアップグレードする場合は、次の重大なアラームが表示されます。

  ```
  Board controller upgraded, manual a/c power cycle required on server x
  ```

  CSCuv45173 に記載されているとおり、このアラームは誤って重大なアラームとして分類されています。このアラームはサーバの機能に影響を与えないため、無視しても構いません。

  このアラームが表示されないようにするには、次のいずれかを行います。

  - Cisco UCS Manager でカスタム ホスト ファームウェア パッケージを作成して、ボード コントローラ ファームウェアを Cisco UCS Manager 2.2(6c) への更新から除外し、古いバージョンを保持します。
  - Cisco UCS Manager インフラストラクチャ（A バンドル）をリリース 2.2(6c) にアップグレードし、『*Release Notes for Cisco UCS Manager, Release 2.2*』の表 2 の混在ファームウェア サポート マトリックスに従って、すべての Cisco UCS C220 M4 または C240 M4 サーバ上でホスト ファームウェア（C バンドル）を引き続き古いバージョンで実行します。

  （注） 詳細については、次を参照してください。 https://tools.cisco.com/bugsearch/bug/CSCuv45173

- ボード コントローラのアップグレード後に、ボード コントローラのアクティブ化ステータスに [Pending Power Cycle] が表示される場合、手動による電源の再投入が必要です。また、エラーも生成されます。電源の再投入後、エラーはクリアされ、ボードコントローラのアクティブ化ステータスに [Ready] が表示されます。

Cisco UCS B シリーズ M2 ブレード サーバのボード コントローラ ファームウェアのアクティブ化

ボード コントローラ ファームウェアは、eUSB、LED、I/O コネクタなど、サーバの多くの機能を制御します。

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] タブの [Equipment] ノードを展開します。

ステップ 3 [Work] ペインの [Firmware Management] タブをクリックします。

ステップ 4 [Installed Firmware] タブの [Activate Firmware] をクリックします。
Cisco UCS Manager GUI によって、[Activate Firmware] ダイアログボックスが開き、Cisco UCS ドメインのすべてのエンドポイントのファームウェア バージョンが確認されます。このステップは、シャーシとサーバの数に基づいて数分かかる場合があります。

ステップ 5 [Activate Firmware] ダイアログボックスのメニュー バーにある [Filter] ドロップダウン リストから、[Board Controller] を選択します。
Cisco UCS Manager GUI によって、[Activate Firmware] ダイアログボックスにボード コントローラを備えたすべてのサーバが表示されます。

ステップ 6 [Select] フィールドで、次のいずれかの手順を実行します。

- すべてのサーバのボードコントローラのファームウェアを同じバージョンにアクティブ化するには、[Version] オプション ボタンをクリックし、[Set Version] ドロップダウン リストから適切なバージョンを選択します。
- すべてのサーバのボードコントローラのファームウェアを、特定のバンドルに含まれるファームウェアのバージョンにアクティブ化するには、[Bundle] オプション ボタンをクリックし、[Set Bundle] ドロップダウン リストから適切なバンドルを選択します。

ステップ 7 [OK] をクリックします。

Cisco UCS B シリーズ M3 および M4 ブレード サーバのボード コントローラ ファームウェアのアクティブ化

ボード コントローラ ファームウェアは、eUSB、LED、I/O コネクタなど、サーバの多くの機能を制御します。

M3 および M4 ボード コントローラ ファームウェアには次のような制限があります。

- アップグレード完了後はファームウェアをダウングレードできない。
- Cisco UCS Managerリリース 2.1(2a) 以降を使用している必要がある。

- ブレード サーバのボード コントローラ ファームウェア バージョンが、インストール済みソフトウェア バンドルと同じ、または新しいバージョンである必要がある。

M3およびM4ブレードサーバのボードコントローラのファームウェアをアクティブ化する前に、次の注意事項を確認してください。

- ボードコントローラ ファームウェアのバージョンが、既存のCisco UCS環境で実行されているバージョンよりも新しい場合でも、ソフトウェア マトリックスまたはTACのサポート範囲には違反しません。
- ボード コントローラ ファームウェアの更新は、常に他のコンポーネントのファームウェアと下位互換性があります。ただし、Cisco UCS Managerでボードコントローラのファームウェアをダウングレードすることはできません。
- CIMCやアダプタなどのブレード サーバ コンポーネントが、ボード コントローラのファームウェア バージョンより前のファームウェア バージョンを実行している場合、ボード コントローラで実行されているファームウェアバージョンに合わせてブレードのコンポーネントをアップグレードする必要はありません。

また、CSCuu15465に記述されている、ボード コントローラの「不一致」アラートが生成される不具合の影響を受ける可能性があります。これは誤ったアラートで、UCSM機能カタログ2.2(4c)Tおよび2.2(5b)Tで解決されています。

（注） 詳細については、https://tools.cisco.com/bugsearch/bug/CSCuu15465を参照してください。

機能カタログの更新は、次の手順で適用できます。

1. 2.2(4c) Infra/Catalogまたは2.2(5b) Infra/Catalogソフトウェア バンドルをダウンロードします。Cisco UCS Managerでのファームウェアのダウンロードと管理, （49ページ） には、ソフトウェア バンドルのダウンロードに関する詳細情報が掲載されています。
2. カタログ バージョン2.2(4c)Tまたは2.2(5b)T（または含まれているカタログ バージョン）をロードしてカタログをアクティブにします。「機能カタログ更新のアクティブ化」には、Cisco UCS Managerで機能カタログをアクティブ化する方法の詳細が掲載されています。
3. 新しく挿入されたブレード サーバを停止します。
4. 以前のボードコントローラ バージョンがあるホスト ファームウェア パック ポリシーにブレード サーバを関連付けます。

   誤った不一致アラートは、CSCuu15465に対する修正がカタログに行われているため発生しません。

（注） これはカタログのみの修正です。

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] タブの [Equipment] ノードを展開します。

ステップ 3 [Work] ペインの [Firmware Management] タブをクリックします。

ステップ 4 [Installed Firmware] タブの [Activate Firmware] をクリックします。
Cisco UCS Manager GUI によって、[Activate Firmware] ダイアログボックスが開き、Cisco UCS ドメインのすべてのエンドポイントのファームウェア バージョンが確認されます。このステップは、シャーシとサーバの数に基づいて数分かかる場合があります。

ステップ 5 [Activate Firmware] ダイアログボックスのメニュー バーにある [Filter] ドロップダウン リストから、[Board Controller] を選択します。
Cisco UCS Manager GUI によって、[Activate Firmware] ダイアログボックスにボード コントローラを備えたすべてのサーバが表示されます。

ステップ 6 更新するボード コントローラに合わせて、[Startup Version] ドロップダウン リストからバージョンを選択します。

ステップ 7 [OK] をクリックします。

ステップ 8 （任意） 異なるアーキテクチャの CPU にアップグレードする場合には、[Force Board Controller Activation] オプションを使用してファームウェア バージョンを更新することもできます。たとえば、サンディ ブリッジ CPU からアイビー ブリッジ CPU にアップグレードする場合などです。

Cisco UCS C シリーズ M3 および M4 ラック サーバのボード コントローラ ファームウェアのアクティブ化

ボード コントローラ ファームウェアは、eUSB、LED、I/O コネクタなど、サーバの多くの機能を制御します。

M3 および M4 ボード コントローラ ファームウェアには次のような制限があります。

- Cisco UCS Managerリリース 2.2(1a) 以降を使用している必要がある。
- ボード コントローラ ファームウェアと CIMC ファームウェアは、同じパッケージ バージョンのものである必要があります。
- ボード コントローラのアップグレード後に、ボード コントローラのアクティブ化ステータスに [Pending Power Cycle] が表示される場合、手動による電源の再投入が必要です。また、エラーも生成されます。電源の再投入後、エラーはクリアされ、ボードコントローラのアクティブ化ステータスに [Ready] が表示されます。

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] タブの [Equipment] ノードを展開します。

ステップ 3 [Work] ペインの [Firmware Management] タブをクリックします。

ステップ 4 [Installed Firmware] タブの [Activate Firmware] をクリックします。
Cisco UCS Manager GUI によって、[Activate Firmware] ダイアログボックスが開き、Cisco UCS ドメインのすべてのエンドポイントのファームウェア バージョンが確認されます。このステップは、シャーシとサーバの数に基づいて数分かかる場合があります。

ステップ 5 [Activate Firmware] ダイアログボックスのメニュー バーにある [Filter] ドロップダウン リストから、[Board Controller] を選択します。
Cisco UCS Manager GUI によって、[Activate Firmware] ダイアログボックスにボード コントローラを備えたすべてのサーバが表示されます。

ステップ 6 更新するボード コントローラに合わせて、[Startup Version] ドロップダウン リストからバージョンを選択します。

ステップ 7 [OK] をクリックします。

ステップ 8 （任意） 異なるアーキテクチャの CPU にアップグレードする場合には、[Force Board Controller Activation] オプションを使用してファームウェア バージョンを更新することもできます。たとえば、サンディ ブリッジ CPU からアイビー ブリッジ CPU へのアップグレードなどです。

Cisco UCS Manager ファームウェア

Cisco UCS Manager ソフトウェアでファームウェアをアクティブ化するときには、次のガイドラインとベスト プラクティスを考慮してください。

- クラスタ設定の場合、両方のファブリック インターコネクトの Cisco UCS Manager は同じバージョンを実行する必要があります。
- Cisco UCS Manager のアクティブ化により、管理機能が短期間にわたってダウンします。すべての仮想シェル（VSH）接続が切断されます。
- クラスタ設定の場合、両方のファブリック インターコネクトの Cisco UCS Manager がアクティブ化されます。
- ファブリック インターコネクトをリセットする必要がないため、Cisco UCS Manager の更新はサーバ アプリケーション I/O に影響を与えません。
- 従属ファブリック インターコネクトがダウンしている間に Cisco UCS Manager が更新された場合、従属ファブリック インターコネクトは復帰時に自動的に更新されます。

アップグレードの検証

Cisco UCS Managerは、アップグレードまたはダウングレードプロセスを検証し、すべてのファームウェア アップグレードの検証エラー（非推奨のハードウェアなど）を [Upgrade Validation] タブに表示します。アップグレードの検証エラーがある場合、アップグレードは失敗し、Cisco UCS Manager は以前のリリースにロールバックします。アップグレードを続ける前に、これらの障害を解決する必要があります。

自動インストールメソッドでインフラストラクチャファームウェアのアップグレードまたはダウングレードを実行する場合、Cisco UCS Manager でアップグレードまたはダウングレード プロセスの問題を報告する必要がなければ [Skip Validation] チェックボックスをオンにします。逆に、アップグレードまたはダウングレード プロセスの問題を報告するには、[Skip Validation] チェックボックスをオフにします。デフォルトでは、[Skip Validation] チェックボックスはオフになっています。

Cisco UCS Manager ソフトウェアのアクティブ化

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] タブの [Equipment] ノードを展開します。

ステップ 3 [Work] ペインの [Firmware Management] タブをクリックします。

ステップ 4 [Installed Firmware] タブの [Activate Firmware] をクリックします。
Cisco UCS Manager GUI によって、[Activate Firmware] ダイアログボックスが開き、Cisco UCS ドメインのすべてのエンドポイントのファームウェア バージョンが確認されます。このステップは、シャーシとサーバの数に基づいて数分かかる場合があります。

ステップ 5 [Activate Firmware] ダイアログボックスの [UCS Manager] 行で、次の手順を実行します。

a) [Startup Version] カラムのドロップダウンリストから、ソフトウェアをアップデートするバージョンを選択します。

b) [OK] をクリックします。

Cisco UCS Manager によって、選択したバージョンが起動バージョンに指定され、ファブリックインターコネクトがアップグレードされたときにアクティベーションを実行するようにスケジュールされます。

ファブリック インターコネクトのファームウェア

従属ファブリック インターコネクトでのファームウェアのアクティブ化

はじめる前に

クラスタの下位ファブリックインターコネクトであるファブリックインターコネクトを特定します。

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] タブの [Equipment] ノードを展開します。

ステップ 3 [Work] ペインの [Firmware Management] タブをクリックします。

ステップ 4 [Installed Firmware] タブの [Activate Firmware] をクリックします。
Cisco UCS Manager GUI によって、[Activate Firmware] ダイアログボックスが開き、Cisco UCS ドメインのすべてのエンドポイントのファームウェア バージョンが確認されます。このステップは、シャーシとサーバの数に基づいて数分かかる場合があります。

ステップ 5 メニュー バーの [Filter] ドロップダウン リストから、[Fabric Interconnects] を選択します。

ステップ 6 下位ファブリック インターコネクトの [Activate Firmware] ダイアログボックスの行で、次の手順を実行します。

a) [Kernel] 行で、[Startup Version] カラムのドロップダウンリストからアップグレードするファームウェア バージョンを選択します。

b) [System] 行で、[Startup Version] カラムのドロップダウンリストからアップグレードするファームウェア バージョンを選択します。

ステップ 7 [Apply] をクリックします。

ステップ 8 下位ファブリック インターコネクトの高可用性ステータスを確認します。
ファブリック インターコネクトの [High Availability Details] 領域に次の値が表示されない場合は、シスコのテクニカル サポートに問い合わせてください。プライマリ ファブリック インターコネクトのアップデートに進まないでください。

フィールド名	必要な値
[Ready] フィールド	Yes
[State] フィールド	Up

次の作業

プライマリ ファブリック インターコネクトでのファームウェアのアクティブ化

この手順は、従属ファブリック インターコネクトでのファームウェアのアクティブ化，（91 ページ）から直接続いており、[Firmware Management] タブが表示されていることを前提としています。

はじめる前に

下位のファブリック インターコネクトをアクティブにします。

手順

ステップ 1 [Installed Firmware] タブの [Activate Firmware] をクリックします。
Cisco UCS Manager GUI によって、[Activate Firmware] ダイアログボックスが開き、Cisco UCS ドメインのすべてのエンドポイントのファームウェア バージョンが確認されます。このステップは、シャーシとサーバの数に基づいて数分かかる場合があります。

ステップ 2 メニュー バーの [Filter] ドロップダウン リストから、[Fabric Interconnects] を選択します。

ステップ 3 下位ファブリック インターコネクトの [Activate Firmware] ダイアログボックスの行で、次の手順を実行します。

a) [Kernel] 行で、[Startup Version] カラムのドロップダウンリストからアップグレードするファームウェア バージョンを選択します。

b) [System] 行で、[Startup Version] カラムのドロップダウンリストからアップグレードするファームウェア バージョンを選択します。

ステップ 4 [Apply] をクリックします。

ステップ 5 ファブリック インターコネクトの高可用性ステータスを確認します。
ファブリック インターコネクトの [High Availability Details] 領域に次の値が表示されない場合は、シスコのテクニカル サポートに問い合わせてください。

フィールド名	必要な値
[Ready] フィールド	Yes
[State] フィールド	Up

スタンドアロンファブリックインターコネクトでのファームウェアのアクティブ化

単一のファブリック インターコネクトのスタンドアロン設定の場合、エンドポイントの直接のファームウェアアップグレードを実行すると、データ トラフィックの中断を最小にできます。ただし、アップグレードを完了するために、ファブリック インターコネクトをリブートする必要があるため、トラフィックの中断は避けられません。

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] タブの [Equipment] ノードを展開します。

ステップ 3 [Fabric Interconnects] ノードを展開して、スタンドアロン ファブリック インターコネクトをクリックします。

ステップ 4 [General] タブで [Activate Firmware] をクリックします。

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

名前	説明
[Kernel Version] ドロップダウン リスト	カーネルとして使用するバージョンを選択します。
[Force] チェックボックス	オンにすると、Cisco UCS では、選択したバージョンを前回インストールしようとしたときに失敗または中断した場合でも、インストールを試みます。
[System Version] ドロップダウン リスト	システムとして使用するバージョンを選択します。
[Force] チェックボックス	オンにすると、Cisco UCS では、選択したバージョンを前回インストールしようとしたときに失敗または中断した場合でも、インストールを試みます。

ステップ 6 [OK] をクリックします。

コンポーネントのファームウェア バージョンの確認

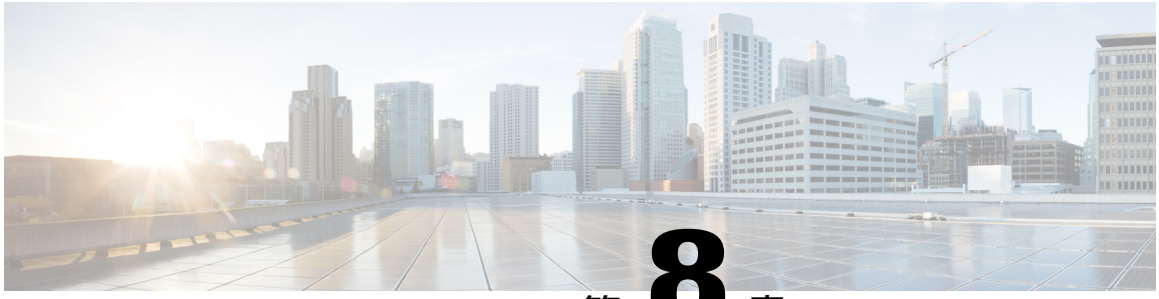
手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] タブの [Equipment] ノードを展開します。

ステップ 3 [Work] ペインの [Firmware Management] タブをクリックします。

ステップ 4 [Installed Firmware] タブで、各コンポーネントに対して一覧表示されたファームウェア バージョンを確認します。



第 8 章

サービス プロファイルのファームウェア パッケージによるファームウェアのアップグレード

この章は、次の項で構成されています。

サービス プロファイルのファームウェア パッケージによるファームウェア アップグレード

サービス プロファイル内のファームウェア パッケージを使用して、サーバの BIOS など、サーバおよびアダプタのファームウェアをアップグレードできます。ホストファームウェアポリシーを定義して、これをサーバに関連付けられているサービス プロファイルにインクルードします。

デフォルトのホスト ファームウェア パックが更新され、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、サーバがリブートされ、新しいファームウェアが適用されます。この動作は、新たに検出されたサーバのみが対象であるため、ファームウェア自動同期サーバ ポリシーによって管理されません。

サービスプロファイルによって、I/O モジュール、ファブリック インターコネクト、または Cisco UCS Manager のファームウェアをアップグレードすることはできません。それらのエンドポイントのファームウェアは直接アップグレードする必要があります。

（注） Cisco UCS は、新しい管理ファームウェア パッケージの作成をサポートしなくなりました。必要な場合は、既存の管理ファームウェア パッケージを変更および更新することができます。ただし、管理ファームウェア パッケージをすべてのサービス プロファイルから削除し、ホスト ファームウェア パッケージを使用してサーバ上の Cisco Integrated Management Controller（CIMC）を更新することをお勧めします。

ホスト ファームウェア パッケージ

このポリシーでは、ホスト ファームウェア パッケージ（ホスト ファームウェア パック）を構成するファームウェア バージョンのセットを指定することができます。ホスト ファームウェア パッケージには、次のサーバおよびアダプタ エンドポイントのファームウェアが含まれています。

- アダプタ
- サーバ BIOS
- CIMC
- ボード コントローラ
- Flexフラッシュ コントローラ
- グラフィックス カード
- ホスト HBA
- ホスト HBA オプション ROM
- ホスト NIC
- ホスト NIC オプション ROM
- ローカル ディスク

（注） ローカルディスクは、デフォルトでホスト ファームウェア パックから除外されます。

ローカル ディスク ファームウェアを更新するには、ホスト ファームウェア パッケージにブレード パッケージを必ず含めます。ブレード パッケージには、ブレード サーバとラック サーバのローカル ディスク ファームウェアが含まれています。

- PSU
- SAS エクスパンダ
- RAID コントローラ
- ストレージ コントローラのオンボード デバイス

- ストレージ コントローラのオンボード デバイス Cpld
- ストレージ デバイスのブリッジ

メモ　ブレードまたはラック サーバのローカル ディスク ファームウェアを更新するには、ホスト ファームウェア パッケージにブレード パッケージを必ず含めます。ブレード パッケージには、ブレード サーバとラック サーバの両方のローカル ディスク ファームウェアが含まれています。

ヒント　同じホスト ファームウェア パッケージに複数のファームウェアを含めることができます。たとえば、1 つのホスト ファームウェア パッケージで BIOS ファームウェアとストレージ コントローラ ファームウェアの両方を使用したり、異なる 2 つのアダプタのモデル用のアダプタ ファームウェアを使用することができます。ただし、同じ種類、ベンダー、モデル番号に対しては 1 つのファームウェア バージョンしか使用できません。システムはエンドポイントで必要なファームウェア バージョンを認識し、それ以外のファームウェア バージョンは無視します。

また、新しいホスト ファームウェア パッケージを作成するとき、または既存のホスト ファームウェア パッケージを変更するときに、ホスト ファームウェア パッケージから特定のコンポーネントのファームウェアを除外できます。たとえば、ホスト ファームウェア パッケージによって RAID コントローラ ファームウェアをアップグレードしない場合は、ファームウェア パッケージ コンポーネントのリストから RAID コントローラ ファームウェアを除外できます。

（注）　各ホスト ファームウェア パッケージは、すべてのファームウェア パッケージ（ブレードおよびラック）に共通の除外されたコンポーネントの1つのリストに関連付けられます。ファームウェア パッケージ タイプごとに別の除外リストを設定するには、別のホスト ファームウェア パッケージを使用します。

ファームウェアパッケージは、このポリシーが含まれ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にプッシュされます。

このポリシーにより、同じポリシーを使用しているサービス プロファイルが関連付けられているすべてのサーバでホストファームウェアが同一となります。したがって、サービスプロファイルをあるサーバから別のサーバに移動した場合でも、ファームウェア バージョンはそのまま変わりません。さらに、ファームウェアパッケージのエンドポイントのファームウェアバージョンを変更した場合、その影響を受けるサービス プロファイルすべてに新しいバージョンが適用されます。この結果、サーバがリブートされることがあります。

このポリシーはサービス プロファイルにインクルードする必要があります。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。

このポリシーは他のどのポリシーにも依存していません。しかし、ファブリック インターコネクトに適切なファームウェアがダウンロードされていることを確認する必要があります。Cisco UCS Manager によりサーバとサービス プロファイルの関連付けが実行される際にファームウェア イ

メージが使用できない場合、Cisco UCS Manager はファームウェア アップグレードを無視し、関連付けを終了します。

管理ファームウェア パッケージ

（注） Cisco UCS は、新しい管理ファームウェア パッケージの作成をサポートしなくなりました。必要な場合は、既存の管理ファームウェア パッケージを変更および更新することができます。ただし、管理ファームウェア パッケージをすべてのサービス プロファイルから削除し、ホスト ファームウェア パッケージを使用してサーバ上の Cisco Integrated Management Controller（CIMC）を更新することをお勧めします。

このポリシーでは、管理ファームウェア パッケージ（管理ファームウェア パック）を構成するファームウェアバージョンのセットを指定することができます。管理ファームウェアパッケージには、サーバの Cisco Integrated Management Controller（CIMC）が含まれています。CIMC を直接アップグレードする場合は、このパッケージを使用する必要はありません。

ファームウェアパッケージは、このポリシーが含まれ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にプッシュされます。このポリシーにより、同じポリシーを使用しているサービス プロファイルに関連付けられているすべてのサーバで CIMC ファームウェアが同一となります。したがって、サービスプロファイルをあるサーバから別のサーバに移動した場合でも、ファームウェア バージョンはそのまま変わりません。

このポリシーはサービス プロファイルにインクルードする必要があります。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。

このポリシーは他のどのポリシーにも依存していません。しかし、ファブリック インターコネクトに適切なファームウェアがダウンロードされていることを確認する必要があります。

サービス プロファイルのファームウェア パッケージを使用したファームウェアのアップグレードのステージ

サービス プロファイルのホスト ファームウェア パッケージ ポリシーを使用して、サーバおよびアダプタ ファームウェアをアップグレードすることができます。

注意 メンテナンス ウィンドウを設定およびスケジュールしている場合を除き、エンドポイントを追加するか既存のエンドポイントのファームウェアバージョンを変更してホストファームウェア パッケージを変更した場合は、変更を保存するとすぐに Cisco UCS Manager によって、エンドポイントがアップグレードされます。そのファームウェア パッケージに関連付けられているすべてのサーバがリブートされるため、サーバ間のデータ トラフィックが中断します。

新しいサービス プロファイル

新しいサービス プロファイルの場合、このアップグレードは次のステージで行われます。

ファームウェア パッケージ ポリシーの作成

このステージでは、ホスト ファームウェア パッケージを作成します。

サービス プロファイルのアソシエーション

このステージで、サービス プロファイルにファームウェア パッケージを含め、サービス プロファイルとサーバとの関連付けを形成します。システムによって、選択したファームウェア バージョンがエンドポイントにプッシュされます。サーバをリブートし、ファームウェア パッケージで指定したバージョンがエンドポイントで確実に実行されるようにします。

既存のサービス プロファイル

サーバと関連付けられているサービスプロファイルの場合は、メンテナンス ウィンドウを設定およびスケジュールしている場合を除いて、ファームウェア パッケージへの変更を保存するとすぐに Cisco UCS Manager によってファームウェアがアップグレードされ、サーバがリブートされます。メンテナンス ウィンドウを設定およびスケジュールしている場合は、Cisco UCS Manager によってその時間までアップグレードとサーバのリブートが延期されます。

サービス プロファイルのファームウェア パッケージに対するアップデートの影響

サービスプロファイルのファームウェアパッケージを使用してファームウェアをアップデートするには、パッケージ内のファームウェアをアップデートする必要があります。ファームウェア パッケージへの変更を保存した後の動作は、Cisco UCS ドメインの設定によって異なります。

次の表に、サービスプロファイルのファームウェアパッケージを使用するサーバのアップグレードに対する最も一般的なオプションを示します。

サービス プロファイル	メンテナンス ポリシー	アップグレード処理
ファームウェア パッケージがサービス プロファイルまたはアップデート中のサービス プロファイル テンプレートに含まれていない。 または 既存のサービス プロファイルまたはアップデート中のサービスプロファイルテンプレートを変更せずにファームウェアをアップグレードする。	メンテナンス ポリシーなし	ファームウェア パッケージのアップデート後に、次のいずれかを実行します。 • 一部のサーバまたはすべてのサーバを同時にリブートおよびアップグレードするには、サーバに関連付けられている1つ以上のサービスプロファイルまたはアップデート中のサービス プロファイル テンプレートにファームウェア パッケージを追加します。 • 一度に 1 台のサーバをリブートおよびアップグレードするには、各サーバに対して次の手順を実行します。 **1** 新しいサービス プロファイルを作成し、そのサービス プロファイルにファームウェア パッケージを含めます。 **2** サービス プロファイルからサーバの関連付けを解除します。 **3** サーバを新規サービス プロファイルと関連付けます。 **4** サーバがリブートされ、ファームウェアがアップグレードされた後に、新規サービス プロファイルからサーバの関連付けを解除し、このサーバを元のサービス プロファイルに関連付けます。 **注意** 元のサービス プロファイルにスクラブ ポリシーが含まれている場合は、サービス プロファイルの関連付けを解除すると、ディスクまたはBIOSが新規サービス プロファイルに関連してスクラビング処理されるときにデータが失われることがあります。

サービス プロファイル	メンテナンス ポリシー	アップグレード処理
ファームウェア パッケージが 1 つ以上のサービス プロファイルに含まれており、このサービス プロファイルが 1 つ以上のサーバに関連付けられている。 または ファームウェア パッケージがアップデート中のサービスプロファイルテンプレートに含まれており、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 1 つ以上のサーバに関連付けられている。	メンテナンス ポリシーなし または 即時アップデート用に設定されたメンテナンス ポリシー。	ファームウェア パッケージをアップデートすると、次のようになります。 **1** ファームウェア パッケージの変更は、保存と同時に有効になります。 **2** Cisco UCS によって、このポリシーをインクルードしているサービス プロファイルに関連付けられているすべてのサーバに照らして、モデル番号とベンダーが検証されます。モデル番号とベンダーがポリシーのファームウェア バージョンと一致する場合は、Cisco UCS によりサーバがリブートされ、ファームウェアがアップデートされます。 ファームウェア パッケージを含むサービス プロファイルに関連付けられているすべてのサーバが同時にリブートされます。

サービス プロファイル	メンテナンス ポリシー	アップグレード処理
ファームウェア パッケージが 1 つ以上のサービス プロファイルに含まれており、このサービス プロファイルが 1 つ以上のサーバに関連付けられている。 または ファームウェア パッケージがアップデート中のサービス プロファイルテンプレートに含まれており、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 1 つ以上のサーバに関連付けられている。	ユーザ確認応答に関して設定済み	ファームウェアパッケージをアップデートすると、次のようになります。 **1** Cisco UCS によって、変更を確認するように要求され、ユーザ確認応答済みのサーバのリブートが必要であることが通知されます。 **2** 点滅している [Pending Activities] ボタンをクリックし、リブートして新規ファームウェアを適用するサーバを選択します。 **3** Cisco UCS によって、このポリシーをインクルードしているサービス プロファイルに関連付けられているすべてのサーバに照らして、モデル番号とベンダーが検証されます。モデル番号とベンダーがポリシーのファームウェア バージョンと一致する場合は、Cisco UCS によりサーバがリブートされ、ファームウェアがアップデートされます。 サーバを手動でリブートしても、Cisco UCS によってファームウェアパッケージが適用されたり、保留中のアクティビティがキャンセルされることはありません。[Pending Activities] ボタンを使用して、保留中のアクティビティを確認応答するか、またはキャンセルする必要があります。

サービス プロファイル	メンテナンス ポリシー	アップグレード処理
ファームウェア パッケージが 1 つ以上のサービス プロファイルに含まれており、このサービス プロファイルが 1 つ以上のサーバに関連付けられている。 または ファームウェア パッケージがアップデート中のサービスプロファイルテンプレートに含まれており、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 1 つ以上のサーバに関連付けられている。	特定のメンテナンスウィンドウ時に有効になる変更に関して設定済み。	ファームウェア パッケージをアップデートすると、次のようになります。 **1** Cisco UCS によって、変更を確認するように要求され、ユーザ確認応答済みのサーバのリブートが必要であることが通知されます。 **2** 点滅している [Pending Activities] ボタンをクリックし、リブートして新規ファームウェアを適用するサーバを選択します。 **3** Cisco UCS によって、このポリシーをインクルードしているサービス プロファイルに関連付けられているすべてのサーバに照らして、モデル番号とベンダーが検証されます。モデル番号とベンダーがポリシーのファームウェア バージョンと一致する場合は、Cisco UCS によりサーバがリブートされ、ファームウェアがアップデートされます。 サーバを手動でリブートしても、Cisco UCS によってファームウェア パッケージが適用されたり、スケジュールされたメンテナンスアクティビティがキャンセルされることはありません。

ホスト ファームウェア パッケージの作成

ヒント 同じホスト ファームウェア パッケージに複数のファームウェアを含めることができます。たとえば、1 つのホスト ファームウェア パッケージで BIOS ファームウェアとストレージ コントローラ ファームウェアの両方を使用したり、異なる 2 つのアダプタのモデル用のアダプタ ファームウェアを使用することができます。ただし、同じ種類、ベンダー、モデル番号に対しては 1 つのファームウェア バージョンしか使用できません。システムはエンドポイントで必要なファームウェア バージョンを認識し、それ以外のファームウェア バージョンは無視します。

新しいホスト ファームウェア パッケージを作成するときに、ホスト ファームウェア パッケージから特定のコンポーネントのファームウェアを除外することもできます。

重要 各ホスト ファームウェア パッケージは、すべてのファームウェア パッケージ（ブレードおよびラック）に共通の除外されたコンポーネントの1つのリストに関連付けられます。ファームウェア パッケージ タイプごとに別の除外リストを設定するには、別のホスト ファームウェア パッケージを使用します。

はじめる前に

手順

ステップ 1 [Navigation] ペインで [Servers] をクリックします。

ステップ 2 [Servers] > [Policies] の順に展開します。

ステップ 3 ポリシーを作成する組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 [Host Firmware Packages] を右クリックし、[Create Package] を選択します。

ステップ 5 [Create Host Firmware Package] ダイアログボックスで、パッケージの一意の名前と説明を入力します。
この名前には、1 ～ 32 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。

ステップ 6 サーバとコンポーネントを選択してホスト ファームウェア パッケージを設定するには、[How would you like to configure the Host Firmware Package] フィールドの [Simple] オプション ボタンを選択します。

ステップ 7 [Blade] および [Rack] ドロップダウン リストから、ファームウェア パッケージを選択します。

ステップ 8 [Excluded Components] 領域で、このホスト ファームウェア パッケージから除外するコンポーネントに対応するチェックボックスをオンにします。
コンポーネント チェックボックスを 1 つもオンにしない場合は、リスト内のすべてのコンポーネントがホスト ファームウェア パッケージに含まれます。

（注） ローカル ディスクは、デフォルトでホスト ファームウェア パックから除外されます。

ローカル ディスク ファームウェアを更新するには、ホスト ファームウェア パッケージにブレード パッケージを必ず含めます。ブレード パッケージには、ブレード サーバとラック サーバのローカル ディスク ファームウェアが含まれています。

ステップ 9 高度なオプションを使用してホスト ファームウェア パッケージを設定するには、[How would you like to configure the Host Firmware Package] フィールドの [Advanced] オプション ボタンを選択します。

ステップ 10 各サブタブで、パッケージに含めるファームウェアのタイプごとに次の手順を実行します。

a) [Select] カラムで、該当する行のチェックボックスがオンになっていることを確認します。

b) [Vendor]、[Model]、、および [PID] カラムで、情報がこのパッケージを使用して更新するサーバに一致していることを確認します。

c) [Version] カラムで、ファームウェアの更新後のファームウェア バージョンを選択します。

ステップ 11 必要なすべてのファームウェアをパッケージに追加したら、[OK] をクリックします。

次の作業

ホスト ファームウェア パッケージのアップデート

既存のホスト ファームウェア パッケージを変更するときに、ホスト ファームウェア パッケージから特定のコンポーネントのファームウェアを除外することもできます。

重要 各ホスト ファームウェア パッケージは、すべてのファームウェア パッケージ（ブレードおよびラック）に共通の除外されたコンポーネントの1つのリストに関連付けられます。ファームウェア パッケージ タイプごとに別の除外リストを設定するには、別のホスト ファームウェア パッケージを使用します。

はじめる前に

手順

ステップ 1 [Navigation] ペインで [Servers] をクリックします。

ステップ 2 [Servers] > [Policies] の順に展開します。

ステップ 3 アップデートするポリシーを含む組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 [Host Firmware Packages] を展開し、アップデートするポリシーを選択します。

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

ステップ 6 各サブタブで、パッケージに含めるファームウェアのタイプごとに次の手順を実行します。

a) [Select] カラムで、該当する行のチェックボックスがオンになっていることを確認します。

b) [Vendor]、[Model]、、および [PID] カラムで、情報がこのパッケージを使用して更新するサーバに一致していることを確認します。

c) [Version] カラムで、ファームウェアの更新後のファームウェア バージョンを選択します。

ステップ 7 ホスト ファームウェア パッケージのコンポーネントを変更するには、[Modify Package Versions] をクリックします。
[Modify Package Versions] ウィンドウが表示されます。

ステップ 8 [Blade] および [Rack] サーバ サブタブで、ファームウェア パッケージを選択します。

ステップ 9 [Excluded Components] 領域で、このホスト ファームウェア パッケージから除外するコンポーネントに対応するチェックボックスをオンにします。

コンポーネント チェックボックスを 1 つもオンにしない場合は、リスト内のすべてのコンポーネントがホスト ファームウェア パッケージに含まれます。

（注） ローカル ディスクは、デフォルトでホスト ファームウェア パックから除外されます。

ローカル ディスク ファームウェアを更新するには、ホスト ファームウェア パッケージにブレード パッケージを必ず含めます。ブレード パッケージには、ブレード サーバとラック サーバのローカル ディスク ファームウェアが含まれています。

ステップ 10 [Save Changes] をクリックします。

管理ファームウェア パッケージのアップデート

（注） Cisco UCS は、新しい管理ファームウェア パッケージの作成をサポートしなくなりました。必要な場合は、既存の管理ファームウェア パッケージを変更および更新することができます。ただし、管理ファームウェア パッケージをすべてのサービス プロファイルから削除し、ホスト ファームウェア パッケージを使用してサーバ上の Cisco Integrated Management Controller（CIMC）を更新することをお勧めします。

はじめる前に

手順

ステップ 1 [Navigation] ペインで [Servers] をクリックします。

ステップ 2 [Servers] > [Policies] の順に展開します。

ステップ 3 アップデートするポリシーを含む組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 [Management Firmware Packages] を展開し、アップデートするポリシーを選択します。

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

ステップ 6 ファームウェア テーブルで、次の手順を実行します。

a) [Select] カラムで、該当する行のチェックボックスがオンになっていることを確認します。

b) [Vendor]、[Model]、、および [PID] カラムで、情報がこのパッケージを使用して更新するサーバに一致していることを確認します。

c) [Version] カラムで、ファームウェアの更新後のファームウェア バージョンを選択します。

ステップ 7 [Save Changes] をクリックします。

既存のサービス プロファイルへのファームウェア パッケージの追加

手順

ステップ 1 [Navigation] ペインで [Servers] をクリックします。

ステップ 2 [Servers] > [Service Profiles] の順に展開します。

ステップ 3 アップデートするサービス プロファイルが含まれている組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 ファームウェア パッケージを追加するサービス プロファイルをクリックします。

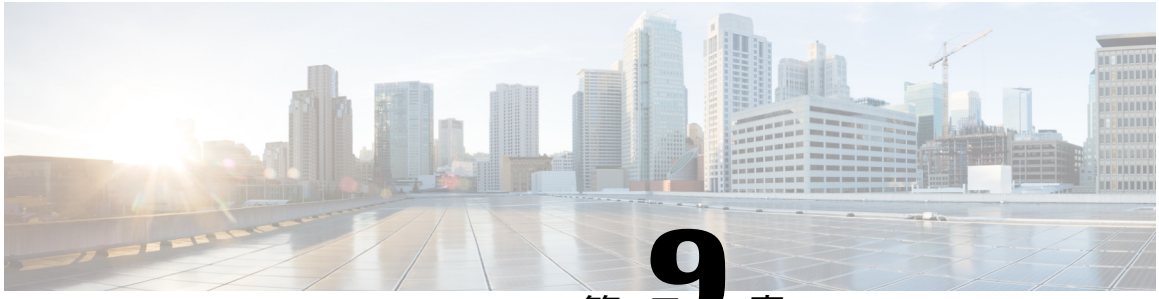
ステップ 5 [Work] ペインの [Policies] タブをクリックします。

ステップ 6 下矢印をクリックして、[Firmware Policies] セクションを展開します。

ステップ 7 ホスト ファームウェア パッケージを追加するには、[Host Firmware] ドロップダウン リストから目的のポリシーを選択します。

ステップ 8 管理ファームウェア パッケージを追加するには、[Management Firmware] ドロップダウン リストから目的のポリシーを選択します。

ステップ 9 [Save Changes] をクリックします。



第 9 章

Cisco UCS Manager の機能カタログの管理

この章は、次の項で構成されています。

機能カタログ

機能カタログは調整可能なパラメータ、文字列、およびルールのセットです。Cisco UCS はカタログを使用してサーバの新しく資格を持ったDIMMやディスク ドライブなどのコンポーネントの表示と設定可能性を更新します。

カタログは、シャーシ、CPU、ローカル ディスク、I/O モジュールなどのハードウェア コンポーネントによって分割されます。カタログを使用すると、該当するコンポーネントで利用可能なプロバイダーのリストを表示できます。1 つのハードウェア コンポーネントに対して 1 つのプロバイダーが存在します。各プロバイダーは、ベンダー、モデル（PID）、およびリビジョンによって識別されます。各プロバイダーに対して、装置の製造元とフォーム ファクタの詳細を表示することもできます。

特定のカタログのリリースに依存するハードウェア コンポーネントの詳細については、『Service Notes for the B- Series server』のコンポーネントのサポートの表を参照してください。特定のリリースで導入されたコンポーネントの情報については、『Cisco UCS Release Notes』を参照してください。

機能カタログの内容

機能カタログの内容は次のとおりです。

実装固有の調整可能なパラメータ

- 電力および熱に関する制約
- スロット範囲および番号
- アダプタ機能

ハードウェア固有のルール

- BIOS、CIMC、RAIDコントローラ、アダプタなどのコンポーネントのファームウェア互換性
- 診断
- ハードウェア固有のリブート

ユーザ表示文字列

- CPN や PID/VID などの部品番号
- コンポーネントの説明
- 物理レイアウト/寸法
- OEM 情報

機能カタログの更新

Cisco UCS インフラストラクチャ ソフトウェア バンドルには、機能カタログの更新が含まれています。Cisco Technical Assistance Center から特に指示された場合を除いて、Cisco UCS インフラストラクチャ ソフトウェアバンドルをダウンロード、更新、およびアクティブ化した後に、機能カタログの更新をアクティブ化する必要があるだけです。

機能カタログの更新をアクティブ化すると、Cisco UCSによってすぐに新しいベースライン カタログに更新されます。それ以外の作業は行う必要がありません。機能カタログの更新では、Cisco UCS ドメイン内のコンポーネントをリブートまたは再インストールする必要はありません。

各 Cisco UCS インフラストラクチャ ソフトウェア バンドルには、ベースライン カタログが含まれます。まれに、シスコが Cisco UCS リリースの間で機能カタログの更新をリリースし、ファームウェア イメージをダウンロードするのと同じサイトで更新を入手できるようにする場合があります。

（注） 機能カタログのバージョンは、使用している Cisco UCS のバージョンによって決まります。たとえば、Cisco UCS 2.0 リリースは、機能カタログのあらゆる 2.0 リリースと一緒に使用できますが、1.0 リリースと一緒に使用することはできません。特定の Cisco UCS リリースでサポートされている機能カタログのリリースについては、http://www.cisco.com/go/unifiedcomputing/b-series-doc で入手可能な『*Cisco UCS B-Series Servers Documentation Roadmap*』にある『*Release Notes for Cisco UCS Administration Software*』を参照してください。

機能カタログ更新のアクティブ化

手順

ステップ 1 [Navigation] ペインで [Admin] をクリックします。

ステップ 2 [Admin] タブで [All] を展開します。

ステップ 3 [Capability Catalog] ノードをクリックします。

ステップ 4 [Work] ペインで [Catalog Update Tasks] タブをクリックします。

ステップ 5 [Activate Catalog] をクリックします。

ステップ 6 [Activate Catalog] ダイアログボックスで、[Version to be Activated] ドロップダウン リストからアクティブ化する機能カタログの更新を選択します。

ステップ 7 [OK] をクリックします。

機能カタログが最新であることの確認

はじめる前に

手順

ステップ 1 [Navigation] ペインで [Admin] をクリックします。

ステップ 2 [Admin] タブで [All] を展開します。

ステップ 3 [Capability Catalog] ノードをクリックします。

ステップ 4 [Work] ペインで [Catalog Update Tasks] タブをクリックします。
機能カタログの最新バージョンは、このタブの右上にあります。

ステップ 5 Cisco.com で、機能カタログの利用可能な最新リリースを確認します。
機能カタログのアップデートの場所については、シスコからの機能カタログのアップデートの入手方法, （112 ページ）を参照してください。

ステップ 6 より新しいバージョンの機能カタログを Cisco.com で入手できる場合は、そのバージョンを使用して機能カタログをアップデートします。

機能カタログ プロバイダーの表示

手順

ステップ 1 [Navigation] ペインで [Admin] をクリックします。

ステップ 2 [Admin] タブで、[All] > [Capability Catalog] を展開します。

ステップ 3 [Work] ペインで、表示するプロバイダーのタブをクリックします。

ステップ 4 プロバイダーの詳細情報を表示するには、次の手順を実行します。

a) テーブルで、表示するプロバイダーのベンダー、モデル、リビジョンの行をクリックします。

b) 見出しの右側にある [Expand] アイコンをクリックし、次の領域のプロパティを表示します。

- [Equipment Manufacturing] 領域
- [Form Factor] 領域

個別の機能カタログ更新のダウンロード

シスコからの機能カタログのアップデートの入手方法

手順

ステップ 1 Web ブラウザで、Cisco.com に移動します。

ステップ 2 [Support] で [All Downloads] をクリックします。

ステップ 3 中央のペインで、[Unified Computing and Servers] をクリックします。

ステップ 4 入力を求められたら、Cisco.com のユーザ名およびパスワードを入力して、ログインします。

ステップ 5 右側のペインで、[Cisco UCS Infrastructure and UCS Manager Software] > [Unified Computing System (UCS) Manager Capability Catalog] をクリックします。

ステップ 6 機能カタログの最新リリースのリンクをクリックします。

ステップ 7 次のいずれかのボタンをクリックして、表示される指示に従います。

- [Download Now]：カタログのアップデートをただちにダウンロードできます。
- [Add to Cart]：後でダウンロードできるよう、カタログのアップデートをカートに入れます。

ステップ 8 プロンプトに従い、カタログのアップデートのダウンロードを完了します。

次の作業

機能カタログをアップデートします。

リモート ロケーションからの機能カタログの更新

機能カタログの一部分のみの更新はできません。 機能カタログを更新すると、カタログ イメージ内のコンポーネントがすべて更新されます

B シリーズ サーバ バンドルには、そのサーバの機能カタログの更新が含まれています。 個別の機能カタログの更新をダウンロードする必要はありません。 機能カタログの更新をアクティブ化するだけです。

手順

ステップ 1 [Navigation] ペインで [Admin] をクリックします。

ステップ 2 [Admin] タブで [All] を展開します。

ステップ 3 [Capability Catalog] ノードをクリックします。

ステップ 4 [Work] ペインで [Catalog Update Tasks] タブをクリックします。

ステップ 5 [Update Catalog] をクリックします。

ステップ 6 [Update Catalog] ダイアログ ボックスで、[Location of the Image File] フィールドの [Remote File System] オプション ボタンをクリックし、必須フィールドに入力します。

ステップ 7 [OK] をクリックします。

Cisco UCS Manager はイメージをダウンロードし、機能カタログを更新します。 ハードウェア コンポーネントをリブートする必要はありません。

次の作業

ローカル ファイル システムからの機能カタログの更新

機能カタログの一部分のみの更新はできません。 機能カタログを更新すると、カタログ イメージ内のコンポーネントがすべて更新されます

B シリーズ サーバ バンドルには、そのサーバの機能カタログの更新が含まれています。 個別の機能カタログの更新をダウンロードする必要はありません。 機能カタログの更新をアクティブ化するだけです。

手順

ステップ 1 [Navigation] ペインで [Admin] をクリックします。

ステップ 2 [Admin] タブで [All] を展開します。

ステップ 3 [Capability Catalog] ノードをクリックします。

ステップ 4 [Work] ペインで [Catalog Update Tasks] タブをクリックします。

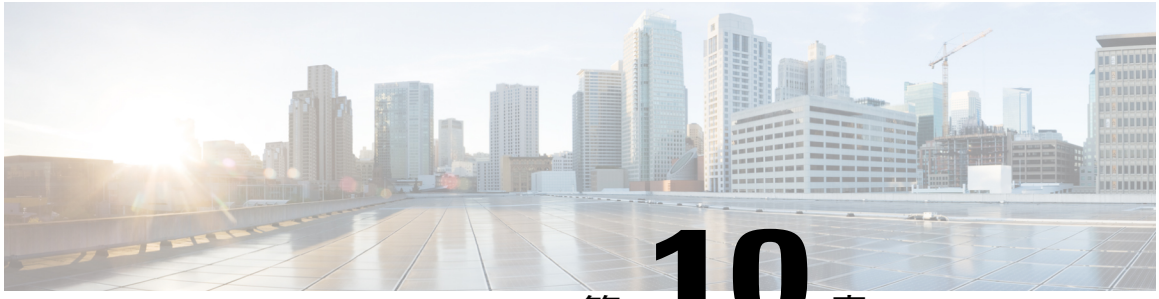
ステップ 5 [Update Catalog] をクリックします。

ステップ 6 [Download Firmware] ダイアログボックスで、[Location of the Image File] フィールドの [Local File System] オプション ボタンをクリックします。

ステップ 7 [Filename] フィールドに、フル パスとイメージ ファイルの名前を入力します。
ファームウェア イメージ ファイルが配置されているフォルダへの正確なパスがわからない場合は、[Browse] をクリックしてファイルにナビゲートします。

ステップ 8 [OK] をクリックします。

Cisco UCS Manager はイメージをダウンロードし、機能カタログを更新します。 ハードウェア コンポーネントをリブートする必要はありません。



第 10 章

データ パスの準備が整っていることの確認

この章は、次の項で構成されています。

ダイナミック vNIC が稼働中であることの確認

ダイナミック vNIC、および VMware vCenter との統合を含む Cisco UCS をアップグレードする場合、データ パスの中断を回避するために、以前のプライマリ ファブリック インターコネクトで新しいソフトウェアをアクティブにする前に、すべてのダイナミック vNIC が新しいファブリック インターコネクトで稼働中であることを確認する必要があります。

この手順は Cisco UCS Manager GUI で実行します。

手順

ステップ 1 [Navigation] ペインで [VM] をクリックします。

ステップ 2 [VM] タブで、[All] > [VMware] > [Virtual Machines] を展開します。

ステップ 3 ダイナミック vNIC を確認する仮想マシンを展開し、ダイナミック vNIC を選択します。

ステップ 4 [Work] ペインで、[VIF] タブをクリックします。

ステップ 5 [VIF] タブで、各 VIF の [Status] カラムが [Online] であることを確認します。

ステップ 6 すべての仮想マシンですべてのダイナミック vNIC の VIF のステータスが [Online] であることを確認するまで、ステップ 3 ～ 5 を繰り返します。

イーサネット データ パスの確認

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。
ステップ 2	UCS-A(nxos)# **show int br | grep -v down | wc –l**	アクティブなイーサネット インターフェイスの数を返します。 この数がアップグレードの前に稼働していたイーサネット インターフェイスの数と一致することを確認します。
ステップ 3	UCS-A(nxos)# **show platform fwm info hw-stm | grep '1.'| wc –l**	MAC アドレスの合計数を返します。 この数がアップグレード前の MAC アドレスの数と一致することを確認します。

次の例では、従属ファブリック インターコネクト A のアクティブなイーサネット インターフェイスおよび MAC アドレスの数が返され、ファブリック インターコネクトのイーサネット データ パスが稼働していることを確認できます。

```
UCS-A /fabric-interconnect # connect nxos a
UCS-A(nxos)# show int br | grep -v down  | wc -l
86
UCS-A(nxos)# show platform fwm info hw-stm | grep '1.' | wc -l
80
```

ファイバ チャネル エンドホスト モードのデータ パスの確認

Cisco UCS ドメインのアップグレード時に最適な結果を得るためには、アップグレードを開始する前、および従属ファブリック インターコネクトをアクティブ化した後にこのタスクを実行し、2 つの結果を比較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 /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 npv flogi-table**	flogi セッションのテーブルを表示します。
ステップ 3	UCS-A(nxos)# **show npv flogi-table | grep fc | wc -l**	ファブリック インターコネクトにログインしたサーバの数を返します。 出力は、アップグレードの開始前にこの確認を行ったときに受け取った出力と一致している必要があります。

次の例では、flogi テーブルおよび従属ファブリック インターコネクト A にログインしたサーバの数が返され、ファブリック インターコネクトのファイバ チャネル データ パスがファイバ チャネル エンドホスト モードで稼働していることを確認できます。

```
UCS-A /fabric-interconnect # connect nxos a
UCS-A(nxos)# show npv flogi-table
--------------------------------------------------------------------------------
SERVER                                                                 EXTERNAL
INTERFACE VSAN FCID            PORT NAME               NODE NAME       INTERFACE
--------------------------------------------------------------------------------
vfc705    700  0x69000a 20:00:00:25:b5:27:03:01 20:00:00:25:b5:27:03:00 fc3/1
vfc713    700  0x690009 20:00:00:25:b5:27:07:01 20:00:00:25:b5:27:07:00 fc3/1
vfc717    700  0x690001 20:00:00:25:b5:27:08:01 20:00:00:25:b5:27:08:00 fc3/1

Total number of flogi = 3.

UCS-A(nxos)# show npv flogi-table | grep fc | wc -l
3
```

ファイバ チャネル スイッチ モードのデータ パスの確認

Cisco UCS ドメインのアップグレード時に最適な結果を得るためには、アップグレードを開始する前、および従属ファブリック インターコネクトをアクティブ化した後にこのタスクを実行し、2 つの結果を比較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 /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 flogi database**	flogi セッションのテーブルを表示します。
ステップ 3	UCS-A(nxos)# **show flogi database | grep –I fc | wc –1**	ファブリック インターコネクトにログインしたサーバの数を返します。

	コマンドまたはアクション	目的
		出力は、アップグレードの開始前にこの確認を行ったときに受け取った出力と一致している必要があります。

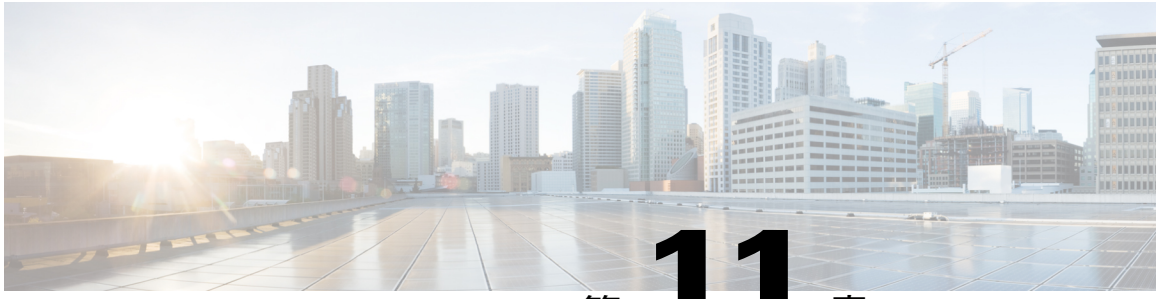
次の例では、flogiテーブルおよび従属ファブリック インターコネクトAにログインしたサーバの数が返され、ファブリック インターコネクトのファイバ チャネル データ パスがファイバ チャネル エンドホスト モードで稼働していることを確認できます。

```
UCS-A /fabric-interconnect # connect nxos a
UCS-A(nxos)# show flogi database
--------------------------------------------------------------------------------
INTERFACE        VSAN    FCID           PORT NAME               NODE NAME
--------------------------------------------------------------------------------
vfc726           800   0xef0003  20:00:00:25:b5:26:07:02 20:00:00:25:b5:26:07:00
vfc728           800   0xef0007  20:00:00:25:b5:26:07:04 20:00:00:25:b5:26:07:00
vfc744           800   0xef0004  20:00:00:25:b5:26:03:02 20:00:00:25:b5:26:03:00
vfc748           800   0xef0005  20:00:00:25:b5:26:04:02 20:00:00:25:b5:26:04:00
vfc764           800   0xef0006  20:00:00:25:b5:26:05:02 20:00:00:25:b5:26:05:00
vfc768           800   0xef0002  20:00:00:25:b5:26:02:02 20:00:00:25:b5:26:02:00
vfc772           800   0xef0000  20:00:00:25:b5:26:06:02 20:00:00:25:b5:26:06:00
vfc778           800   0xef0001  20:00:00:25:b5:26:01:02 20:00:00:25:b5:26:01:00

Total number of flogi = 8.
UCS-A(nxos)# show flogi database | grep fc | wc -l
8
```

第 II 部

Cisco UCS Central によるファームウェアの管理



第 11 章

Cisco UCS Central でのファームウェアのダウンロードと管理

この章は、次の項で構成されています。

Cisco.com からのファームウェアのダウンロード

指定された間隔でシスコの Web サイトと通信してファームウェア イメージのリストを取得するように、Cisco UCS Central を設定できます。イメージのダウンロード用にシスコのクレデンシャルを設定した後に、リフレッシュを行うと、Cisco UCS Central によって Cisco.com から使用可能なイメージ データが取得され、ファームウェア イメージ ライブラリにファームウェア イメージが表示されます。ファームウェア イメージのバージョンを使用してポリシーを作成する場合、または [Store Locally] オプションを使用してイメージをダウンロードする場合には、実際のファームウェア イメージをダウンロードできます。

重要　Cisco.com から Cisco UCS Central にファームウェアをダウンロードするには、Cisco.com アカウントを作成してください。「Cisco.Com アカウントの設定」を参照してください

（注）　Cisco.com アカウントのユーザを変更すると、イメージ ライブラリが完全に同期されます。同期中は、ダウンロード操作を実行できません。これは、ライブラリのサイズによって、最大 10 分かかることがあります。

ファームウェア ライブラリからのイメージの削除

ライブラリからファームウェア イメージを削除するオプションを次に示します。

- **ファームウェア イメージの削除**：イメージを選択して削除をクリックすると、ファームウェア ライブラリ内のダウンロードされたイメージを削除できます。
- **ファームウェア イメージのメタデータのパージ**：パージ オプションを使用すると、イメージのメタデータを削除できます。ライブラリからファームウェア イメージを削除した後でも、メタデータは引き続き存在しています。このメタデータ情報を使用すると、イメージを削除した後でも Cisco.com から実際のファームウェア イメージをいつでもダウンロードすることができます。ファームウェア イメージ ライブラリからファームウェア イメージと関連するメタデータを完全に削除する場合は、実際のファームウェア イメージを削除し、ライブラリからメタデータをパージしてください。

  重要　メタデータに対応するイメージがファームウェア イメージ ライブラリにすでにダウンロードされている場合は、イメージを削除しないでメタデータをパージすることはできません。

シスコからのファームウェアのダウンロードの設定

シスコからのファームウェアのダウンロードを設定すると、Cisco UCS Central によって Cisco.com からファームウェアのメタデータがダウンロードされ、いつでも Cisco UCS Central からダウンロードして保存できるよう、情報が保存されます。

手順

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

ステップ 2 [Navigation] ペインで、[Images] を展開します。

ステップ 3 [Configure Downloads From Cisco] をクリックします。

ステップ 4 [Work] ペインの [General] タブで、フィールドに必須情報を入力します。
Cisco UCS Central がログインに使用する Cisco.com アカウントのユーザ名とパスワードが正しいことを確認してください。

ステップ 5 [Proxy] タブで、プロキシ アカウントの必須情報を入力します。

ステップ 6 [Save（保存）] をクリックします。

シスコからのファームウェア イメージのダウンロード

Cisco.com からのファームウェア イメージのダウンロードを設定し、イメージ ライブラリをリフレッシュすると、Cisco UCS Central で使用可能なすべてのファームウェア イメージのメタデータにアクセスできるようになります。ファームウェア イメージは次の方法でダウンロードできます。

- **ファームウェア ポリシーの作成**：ファームウェア ポリシーを作成し、特定のイメージを選択すると、ファームウェア ポリシーで指定したイメージが Cisco UCS Central によって自動的にダウンロードされます。
- **イメージをローカルに保存**：ローカルに保存するオプションを選択すると、選択したファームウェア イメージが Cisco.com からダウンロードされ、イメージ ライブラリに保存されます。

ここでは、ローカルに保存するオプションを使用してイメージをダウンロードする手順について説明します。

手順

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

ステップ 2 [Navigation] ペインで、[Images] を展開します。

ステップ 3 [Library] をクリックします。

ステップ 4 [Work] ペインで、[Packages] タブをクリックします。
シスコからダウンロードされたイメージのメタデータには、[Source] として [Cisco] が、[State] として [not-downloaded] が指定されています。

ステップ 5 バンドルを右クリックして、オプションから [Store Locally] を選択します。

リモートからのファームウェアのダウンロード

はじめる前に

選択したファイル転送プロトコルをサポートするリモート サーバを設定し、このサーバから Cisco UCS Central へのアクセスを可能にする必要があります。

手順

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

ステップ 2 [Navigation] ペインで、[Images] を展開します。

ステップ 3 [Library] をクリックします。

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

ステップ 5 [Downloads] タブで [Download Firmware] をクリックします。

ステップ 6 [Download Firmware] ダイアログボックスの [Location of the Image File] で、[Remote File System] を選択し、必須フィールドに入力します。

ステップ 7 [OK] をクリックします。

ローカル ファイル システムからのファームウェアのダウンロード

はじめる前に

シスコからファームウェア イメージを入手してローカル ファイル システムに保存し、ファームウェアをローカル システムから Cisco UCS Central にダウンロードするよう設定する必要があります。

手順

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

ステップ 2 [Navigation] ペインで、[Images] を展開します。

ステップ 3 [Library] をクリックします。

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

ステップ 5 [Downloads] タブで [Download Firmware] をクリックします。

ステップ 6 [Download Firmware] ダイアログボックスの [Location of the Image File] で、[Local File System] を選択します。

ステップ 7 [Download Image into Image Library] をクリックします。
ダイアログボックスにファイルを選択するオプションが表示されます。

ステップ 8 ローカル システムにあるファームウェア ファイルの場所を参照してファイルを選択するには、[Browse] をクリックします。

ステップ 9 [Submit] をクリックします。`
イメージが正常にダウンロードされると、[Firmware Image Download] ダイアログボックスに確認メッセージが表示されます。

ステップ 10 [Firmware Image Download] ダイアログボックスで、[OK] をクリックします。

イメージのダウンロードのエラーの表示

ファームウェア イメージのダウンロード処理のエラーは、同じ [Library of Images] パネルに表示できます。

手順

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

ステップ 2 [Navigation] ペインで、[Images] を展開します。

ステップ 3 [Library] をクリックします。

ステップ 4 [Work] ペインで [Faults] タブをクリックします。
エラーのテーブルに、ダウンロードに関するすべてのエラーと詳細が表示されます。

ライブラリでのファームウェア イメージの表示

ダウンロードされたファームウェア イメージとイメージのメタデータは、[Library of Images] パネルに表示できます。

手順

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

ステップ 2 [Navigation] ペインで、[Images] を展開します。

ステップ 3 [Library] をクリックします。

ステップ 4 [Work] ペインで [Packages] タブをクリックします。
利用可能なパッケージが表示されます。パッケージを選択して [Properties] をクリックすると、特定のパッケージの詳細を表示できます。

イメージ ライブラリ上のイメージのメタデータの削除

パージ オプションを使用すると、[Library of Images] からファームウェア イメージのメタデータを削除することができます。パージ オプションでは、すでにダウンロードされたイメージのメタデータだけをクリアします。

（注） 機能カタログ、インフラストラクチャとホストのファームウェア パッケージなど、ファームウェア パッケージのいずれかを削除するには、各ドメイン グループの下にあるファームウェア管理セクション、またはドメイン グループのルートから削除を実行できます。

手順

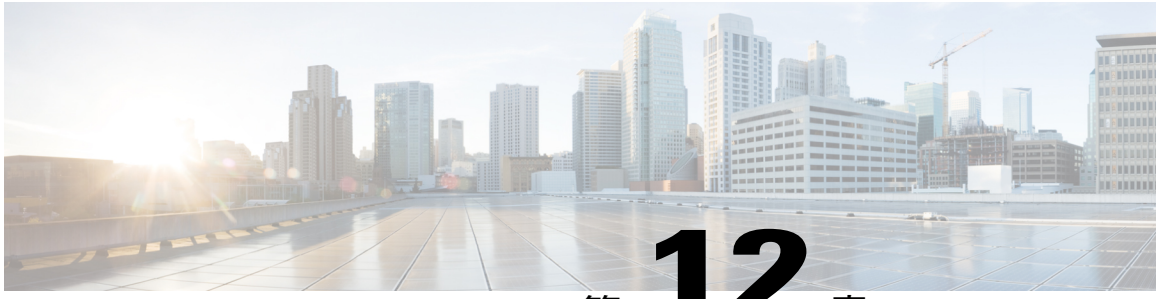
ステップ 1 メニュー バーで、[Operations Management] をクリックします。

ステップ 2 [Navigation] ペインで、[Images] を展開します。

ステップ 3 [Library] をクリックします。

ステップ 4 [Work] ペインで [Library of Images] から削除するファームウェア イメージのメタデータを選択し、[Purge] をクリックします。

ステップ 5 Cisco UCS Central GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。



第 12 章

Cisco UCS Central による Cisco UCS ドメインのファームウェアのアップグレード

この章は、次の項で構成されています。

Cisco UCS ドメインのファームウェアのアップグレード

登録されている Cisco UCS ドメインに対して、インフラストラクチャとサーバのファームウェアのアップグレードを Cisco UCS Central から実行できます。

必要に応じて、各ドメイン グループの Cisco UCS ドメインを異なるバージョンのファームウェアにアップグレードできます。また、Cisco UCS Central には、ファブリック インターコネクトのリブートを Cisco UCS Central からグローバルに確認するオプション、または各 Cisco UCS ドメインから個別に確認するオプションがあります。

Cisco UCS ドメインのインフラストラクチャ ファームウェアのアップグレードの設定

Cisco UCS Central では、Cisco UCS ドメイン グループ 1 つに対してインフラストラクチャ ファームウェア パッケージを 1 つに限り作成できます。ドメイン グループのメンバーである Cisco UCS ドメインは、同じバージョンのインフラストラクチャ ファームウェアを実行します。

（注） インフラストラクチャ ファームウェアの更新は、ドメイン グループのルートまたはドメイン グループ レベルで設定できます。ドメイン グループのルート レベルでファームウェアを更新すると、ルートの下にあるすべてのドメイン グループが同じインフラストラクチャ ファームウェアのバージョンへ更新されます。

手順

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

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

ステップ 3 [Infrastructure Firmware] をクリックします。

ステップ 4 [Work] ペインの [Policies] タブで [Create] をクリックします。

ステップ 5 [Scheduler] 領域で、スケジュールを指定して、ドメイン グループの Cisco UCS ドメインのインフラストラクチャ ファームウェアを適用します。

ステップ 6 [Version] 領域で、インフラストラクチャ ファームウェアのバージョンを選択します。
[Impacted Endpoints] 領域に、インフラストラクチャ ファームウェア ポリシーによって影響を受けるエンドポイントが表示されます。これらのエンドポイントはファームウェアのアップグレード時にリブートされるため、アップグレード プロセス中に使用できなくなるときがあります。

ステップ 7 [Save（保存）] をクリックします。

次の作業

Cisco UCS Central によって、インフラストラクチャ ファームウェアの更新とファブリック インターコネクトのリブート用に 2 つのスケジュールが自動的に作成されます。これらのスケジュールは、Cisco UCS Manager によって更新されます。このスケジュールに基づいて、インフラストラクチャ ファームウェアのアップグレード プロセスが、登録されている Cisco UCS ドメインで開始され、Cisco UCS Central で最初の保留アクティビティ確認メッセージが生成されます。最初の保留中のアクティビティを確認すると、コンポーネントが指定したインフラストラクチャ ファームウェア パッケージによって更新されます。

インフラストラクチャ ファームウェアが更新されると、別の保留中のアクティビティの通知を受信します。この確認によって、ファブリック インターコネクトの予期せぬリブートが防止されま

す。ファブリックインターコネクトをリブートし、インフラストラクチャファームウェアのアップグレードを完了するには、この保留中のアクティビティを確認する必要があります。

（注） ドメイン グループ内に複数のドメインが存在する場合は、インフラストラクチャファームウェアのアップグレードプロセスが完了するまで、各Cisco UCS ドメインの保留中の各アクティビティを確認する必要があります。

保留中のアクティビティの確認

Cisco UCS ドメインのサービス プロファイルでグローバルなメンテナンス ポリシーおよびグローバルなホスト ファームウェア パッケージを使用している場合、Cisco UCS Central にはファームウェア アップグレードを展開する前にユーザの確認を行うオプションがあります。

[User Ack] リブート ポリシーを使用してメンテナンス ポリシーを作成している場合は、Cisco UCS Manager で実際のファームウェア アップグレードを確認する必要があります。グローバルのスケジュールでメンテナンス ポリシーを作成し、[User Ack] をイネーブルにしている場合は、Cisco UCS Central ですべての Cisco UCS ドメインの実際のアップグレードを確認する必要があります。

（注） 保留中のアクティビティは、[Infrastructure Firmware] セクションおよび [Host Firmware] セクションで表示および確認できます。ここでは、[Host Firmware] セクションで保留中のアクティビティを確認する手順について説明します。

手順

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

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

ステップ 3 [Work] ペインの [Pending Activities] タブをクリックします。

ステップ 4 表示されたリストから保留中のアクティビティを選択し、右クリックして、[Acknowledge] をクリックします。

インフラストラクチャ ファームウェア パッケージの削除

手順

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

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

ステップ 3 [Work]ペインには、作成されたすべてのインフラストラクチャ ファームウェア パッケージのリストが表示されます。

ステップ 4 [Delete] をクリックします。

ステップ 5 Cisco UCS Central GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ホスト ファームウェア パッケージの作成

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、[Servers] > [Policies] > [root] を展開します。

ステップ 3 [Host Firmware Packages] をクリックします。

ステップ 4 [Work] ペインで、[Create a Host FW Pack] をクリックします。

ステップ 5 [Create a Host FW Pack] ダイアログボックスで、次のフィールドに入力します。

a) [Name] と [Description] に入力します。
b) [Blade Version] 領域で、ブレード サーバのバージョンを選択します。
c) [Rack Version] 領域で、ラック サーバのバージョンを選択します。
d) [Modular Version] 領域で、モジュラ サーバのバージョンを選択します。

ステップ 6 [Impacted Endpoints] ダイアログボックスに、このホスト ファームウェア ポリシーの影響を受けるエンドポイントのリストが表示されます。
これらのエンドポイントはファームウェアのアップグレード時にリブートされるため、アップグレード処理中の使用は制限されます。

ステップ 7 [OK] をクリックします。

次の作業

Cisco UCS Central で作成したホスト ファームウェア ポリシーは、ドメイン グループに登録された Cisco UCS ドメインのサービス プロファイルへの関連付けに使用できます。

ホスト ファームウェア アップグレードの展開

Cisco UCS Central で定義したすべてのホスト ファームウェア ポリシーを、[Install Servers] を使用して特定の B、C、M バンドルに更新できます。

はじめる前に

ホスト ファームウェア パッケージを作成しておく必要があります。

手順

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

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

ステップ 3 [Host Firmware] をクリックします。

ステップ 4 [Work] ペインで、表示されるホスト ファームウェア パッケージのリストから展開するファームウェア バージョンを選択します。

ステップ 5 テーブル ヘッダーの [Install Servers] をクリックします。

ステップ 6 [Install Servers] ダイアログボックスで、[Blade Version]、[Rack Version]、[Modular Version]、[Impacted Endpoints] を選択します。

ステップ 7 [Upgrade host Firmware Warning] メッセージ ダイアログボックスで、[Yes] をクリックします。
選択したエンドポイントのサーバでグローバルなホスト ファームウェア アップグレード ポリシーを使用している場合は、ホスト ファームウェア パッケージによってアップグレードされます。

ホスト ファームウェア パッケージの削除

手順

ステップ 1 メニュー バーで、[Servers] をクリックします。

ステップ 2 [Navigation] ペインで、[Servers] > [Policies] > [root] を展開します。

ステップ 3 [Host Firmware Packages] をクリックします。

ステップ 4 [Work] ペインには、作成したすべてのホスト ファームウェア パッケージのリストが表示されます。

ステップ 5 削除するホスト ファームウェア パッケージの名前をクリックして選択します。
テーブル ヘッダーの領域にアクションのアイコンが表示されます。

ステップ 6 [Delete] をクリックします。

ステップ 7 Cisco UCS Central GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ファームウェア アップグレードのスケジューリング

ファームウェア アップグレードのスケジュール

ファームウェアをアップグレードする場合、次のような方法で Cisco UCS Central からアップグレードをスケジュールすることができます。

- 1 回のオカレンスとして
- 指定間隔で繰り返すオカレンスとして

ユーザの確認を必要とするスケジュールを設定すると、ファブリック インターコネクトは明示的な確認なしではリブートしません。

メンテナンス ポリシーの作成

Cisco UCS Central では、ホスト ファームウェアの更新に対して、次の種類のメンテナンス ポリシーを作成できます。

- **Immediate**：immediate オプションを指定すると、サーバはユーザの確認なしでただちにリブートされます。
- **Timer-automatic**：timer-automatic オプションを指定すると、サーバのリブートは、このメンテナンス ポリシーに対して選択したスケジュールに基づいて実行されます。

重要 timer-automatic オプションを使用する場合は、Cisco UCS Central でスケジュールを作成し、メンテナンス ポリシーで指定する必要があります。Cisco UCS Central でスケジュールを作成する場合、このスケジュールされたメンテナンス ポリシーは Cisco UCS Central でのみ確認できます。このメンテナンス ポリシーを使用するサーバは、このスケジュールで定義されたメンテナンス時間帯にのみリブートされます。スケジュールで user-acknowledgment が有効の場合、サーバのリブートを確認する必要があります。

- **User-acknowledgment**：user-acknowledgment オプションを指定すると、サーバをリブートする前に、各 Cisco UCS ドメインの保留中のアクティビティの通知が送信されます。

重要 user-acknowledgment オプションには、Cisco UCS ドメインの管理者が Cisco UCS ドメイン内の個々のサーバを異なる時刻にリブートすることを決定できるオプションがあります。

手順

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

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

ステップ 3 [Work] ペインで、[Create Maintenance Policy] をクリックします。

ステップ 4 [Create Maintenance Policy] ダイアログボックスで、必須フィールドに入力します。

ステップ 5 [OK] をクリックします。

次の作業

Cisco UCS Manager でメンテナンス ポリシーをサービス プロファイルに関連付けます。

1 回のオカレンスのスケジュールの作成

手順

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

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

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

ステップ 4 [Create Schedule] ダイアログボックスで、[Properties] 領域に詳細情報を入力します。

ステップ 5 [One Time Occurrences] タブを選択し、[Create One Time Occurrence] をクリックします。

ステップ 6 [Create One Time Occurrence] ダイアログボックスで、詳細情報を入力します。

ステップ 7 [OK] をクリックします。

ステップ 8 [Create Schedule] ダイアログボックスで [OK] をクリックします。
作成した 1 回のみの実行のスケジュールが [Schedule] テーブルに追加されます。

繰り返すオカレンスのスケジュールの作成

手順

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

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

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

ステップ 4 [Create Schedule] ダイアログボックスで、[Properties] 領域に詳細情報を入力します。

ステップ 5 [Recurring Occurrences] タブを選択し、[Create Recurring Occurrence] をクリックします。

ステップ 6 [Create Recurring Occurrence] ダイアログボックスで、詳細情報を入力します。

ステップ 7 [OK] をクリックします。

ステップ 8 [Create Schedule] ダイアログボックスで [OK] をクリックします。
作成した繰り返し実行のスケジュールがテーブルに追加されます。

ファームウェア アップグレードのスケジュールの削除

手順

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

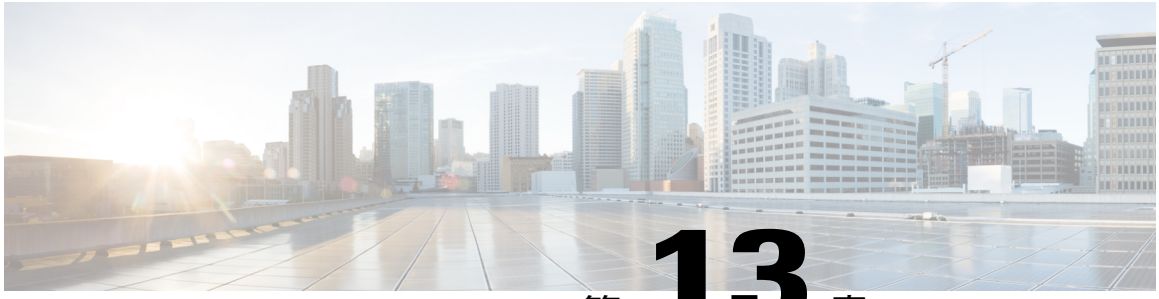
ステップ 2 [Navigation] ペインで、[Domain Groups] > [Domain Groups Root] > [Schedules] を展開します。

ステップ 3 [Work] ペインには、スケジュールされているすべてのファームウェア イベントのリストが表示されます。

ステップ 4 削除するスケジュールの名前をクリックして選択します。
テーブル ヘッダーの領域にアクションのアイコンが表示されます。

ステップ 5 [Delete] をクリックします。

ステップ 6 Cisco UCS Central GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。



第 13 章

Cisco UCS Central での機能カタログの管理

この章は、次の項で構成されています。

機能カタログ

機能カタログは調整可能なパラメータ、文字列、およびルールのセットです。Cisco UCS はカタログを使用してサーバの新しく資格を持ったDIMMやディスク ドライブなどのコンポーネントの表示と設定可能性を更新します。

カタログは、シャーシ、CPU、ローカル ディスク、I/O モジュールなどのハードウェア コンポーネントによって分割されます。カタログを使用すると、該当するコンポーネントで利用可能なプロバイダーのリストを表示できます。1 つのハードウェア コンポーネントに対して 1 つのプロバイダーが存在します。各プロバイダーは、ベンダー、モデル（PID）、およびリビジョンによって識別されます。各プロバイダーに対して、装置の製造元とフォーム ファクタの詳細を表示することもできます。

特定のカタログのリリースに依存するハードウェア コンポーネントの詳細については、『Service Notes for the B- Series server』のコンポーネントのサポートの表を参照してください。特定のリリースで導入されたコンポーネントの情報については、『Cisco UCS Release Notes』を参照してください。

機能カタログの内容

機能カタログの内容は次のとおりです。

実装固有の調整可能なパラメータ

- 電力および熱に関する制約
- スロット範囲および番号
- アダプタ機能

ハードウェア固有のルール

- BIOS、CIMC、RAIDコントローラ、アダプタなどのコンポーネントのファームウェア互換性
- 診断
- ハードウェア固有のリブート

ユーザ表示文字列

- CPN や PID/VID などの部品番号
- コンポーネントの説明
- 物理レイアウト/寸法
- OEM 情報

機能カタログの更新

Cisco UCS インフラストラクチャ ソフトウェア バンドルには、機能カタログの更新が含まれています。Cisco Technical Assistance Center から特に指示された場合を除いて、Cisco UCS インフラストラクチャ ソフトウェアバンドルをダウンロード、更新、およびアクティブ化した後に、機能カタログの更新をアクティブ化する必要があるだけです。

機能カタログの更新をアクティブ化すると、Cisco UCSによってすぐに新しいベースライン カタログに更新されます。それ以外の作業は行う必要がありません。機能カタログの更新では、Cisco UCS ドメイン内のコンポーネントをリブートまたは再インストールする必要はありません。

各 Cisco UCS インフラストラクチャ ソフトウェア バンドルには、ベースライン カタログが含まれます。まれに、シスコが Cisco UCS リリースの間で機能カタログの更新をリリースし、ファームウェア イメージをダウンロードするのと同じサイトで更新を入手できるようにする場合があります。

（注） 機能カタログのバージョンは、使用している Cisco UCS のバージョンによって決まります。たとえば、Cisco UCS 2.0 リリースは、機能カタログのあらゆる 2.0 リリースと一緒に使用できますが、1.0 リリースと一緒に使用することはできません。特定の Cisco UCS リリースでサポートされている機能カタログのリリースについては、http://www.cisco.com/go/unifiedcomputing/b-series-doc で入手可能な『*Cisco UCS B-Series Servers Documentation Roadmap*』にある『*Release Notes for Cisco UCS Administration Software*』を参照してください。

Cisco UCS ドメインの機能カタログの更新の設定

Cisco UCS Central では、Cisco UCS ドメイン グループごとに機能カタログを 1 つに限り作成できます。グループのメンバーである Cisco UCS ドメインは、すべて同じバージョンのファームウェアを実行します。

（注） 機能カタログの更新は、ドメイン グループのルートまたはドメイン グループのレベルで設定できます。ドメイン グループのルート レベルで機能カタログを更新すると、ルートの下にあるドメイン グループで機能カタログが定義されていない場合は同じ機能カタログのバージョンになります。

手順

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

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

ステップ 3 [Capability Catalog] をクリックします。

ステップ 4 [Work] ペインで、[Create] をクリックします。

ステップ 5 [Version] テーブルで、選択した Cisco UCS Central ドメイン グループに含まれる Cisco UCS ドメインに関連付ける機能カタログのバージョンを選択します。
親グループから継承したバージョンがある場合は、ここで選択した機能カタログのバージョンによって、継承したバージョンは上書きされます。

ステップ 6 [Save（保存）] をクリックします。

Cisco UCS Central によって、指定した Cisco UCS ドメインの機能カタログの更新がトリガーされます。