Cisco UCS Manager ファームウェア リリース 3.2 管理ガイド

初版：2017 年 08 月 18 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、フィールドラベルなどのGUI要素は、イタリック体（italic）で示しています。 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、[Main titles] 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（**this font**）で示しています。 CLI コマンド内の変数は、イタリック体（*this font*）で示しています。
[ ]	角カッコの中の要素は、省略可能です。
{x | y | z}	どれか1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	どれか1つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。stringの前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

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

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

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

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

警告 安全上の重要事項

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

これらの注意事項を保管しておいてください。

Cisco UCS の関連ドキュメント

ドキュメント ロードマップ

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、ucs-docfeedback@external.cisco.com までコメントをお送りください。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。

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 Cisco UCS ドメインのコンポーネントであり、機能するためにはファームウェアが必要です。

このガイドでは、Cisco UCS Manager を使用して、ファームウェアを取得し、Cisco UCS ドメインのエンドポイントをアップグレードする方法について説明します。また、これらのエンドポイントをアップグレードする際に従う必要があるベスト プラクティスについても詳しく説明します。

Cisco UCS Manager リリース 3.1(1) 以降、シスコは Cisco UCS Manager の各リリースと併せて、次の各プラットフォーム用のユニファイド Cisco UCS Manager ソフトウェアおよびファームウェアアップグレードをリリースしました。

- Cisco UCS 6300 シリーズ Fabric Interconnect と Cisco UCS B シリーズ、および C シリーズ サーバ
- Cisco UCS 6200 シリーズ Fabric Interconnect と Cisco UCS B シリーズ、および C シリーズ サーバ

- Cisco UCS 6324 ファブリック インターコネクト（Cisco UCS B シリーズ サーバおよび C シリーズ サーバと接続）（UCS Mini とも呼ばれます）

図 *1*：*Cisco UCS 6300* シリーズ ファブリック インターコネクト（*Cisco UCS B* シリーズおよび *C* シリーズ サーバと接続）

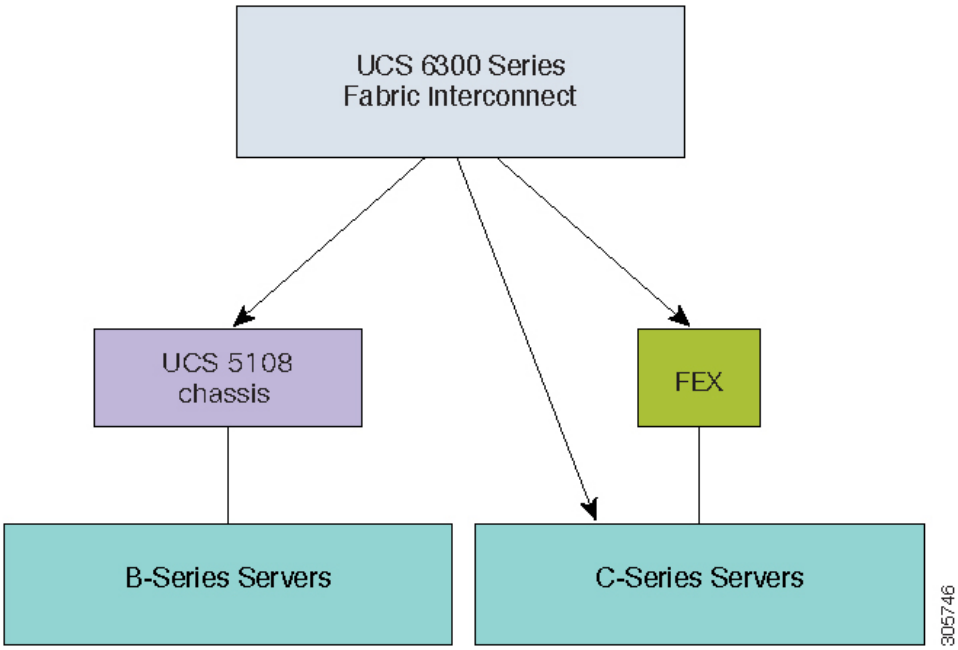


図 *2*：*Cisco UCS 6200* シリーズ *Fabric Interconnect* と *Cisco UCS B* シリーズ、および *C* シリーズ サーバ

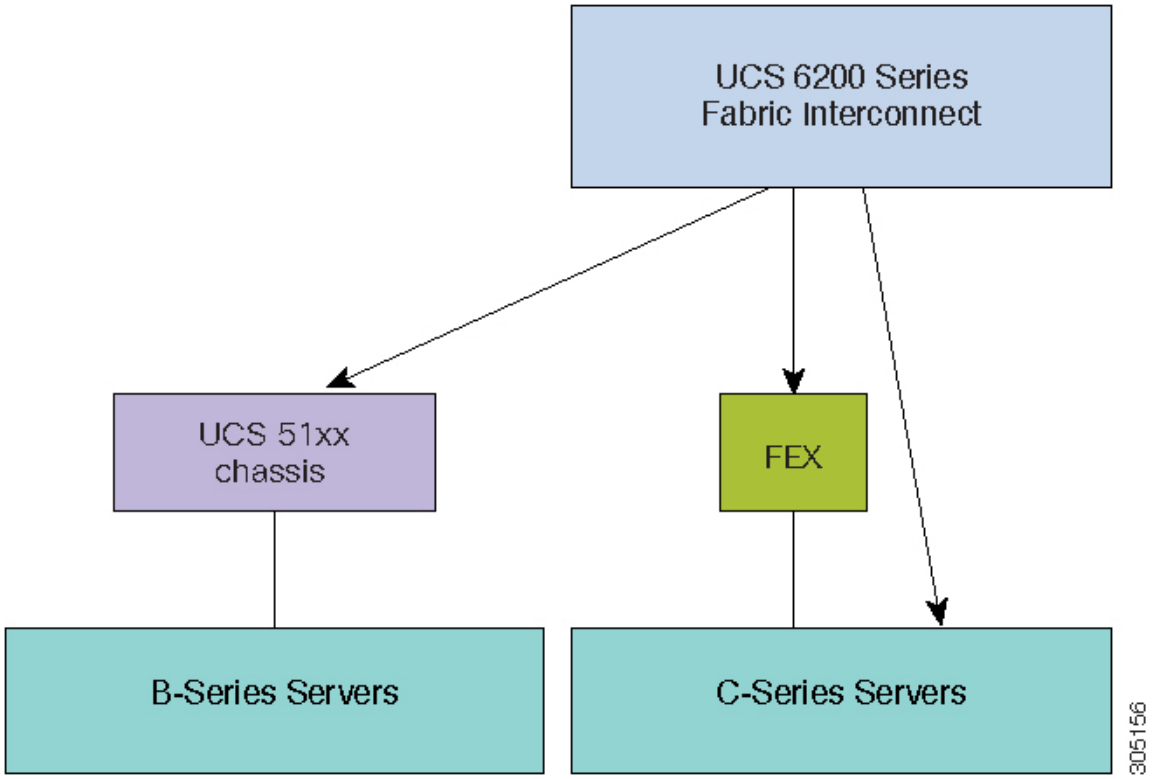
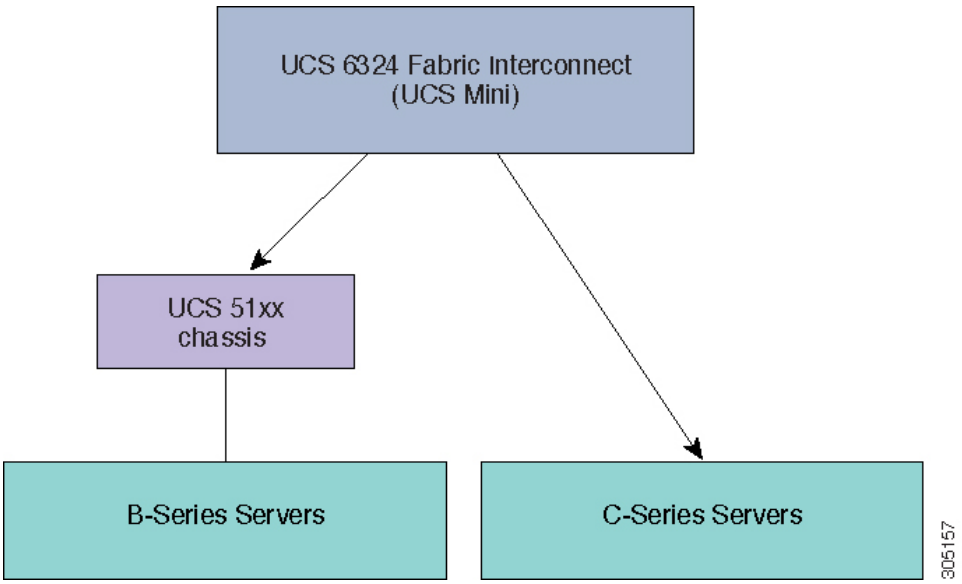


図 *3* : ***Cisco UCS B*** シリーズ サーバおよび ***C*** シリーズ サーバ向け ***Cisco UCS 6324*** ファブリック インターコネクト



次の図に、Cisco UCS Manager リリース 3.2 でサポートされる各種プラットフォームとファームウェア バンドルを示します。

各リリースには、次のファームウェア バンドルがあります。

- インフラストラクチャ ソフトウェア バンドル：このバンドルはAバンドルとも呼ばれます。このバンドルには、ファブリック インターコネクト、IO モジュール、および Cisco UCS Manager が機能するために必要なファームウェア イメージが含まれています。

  Cisco UCS Manager3.2 以降のリリースには、3 つの個別のインフラストラクチャ バンドルが含まれています。

  - Cisco UCS 6200 シリーズ ファブリック インターコネクト：ucs-k9-bundle-infra.3.2.x.xxx.A.bin
  - Cisco UCS 6300 シリーズ ファブリック インターコネクト：ucs-6300-k9-bundle-infra.3.2.x.xxx.A.bin
  - Cisco UCS 6324 ファブリック インターコネクト：ucs-mini-k9-bundle-infra.3.2.x.xxx.A.bin

- B シリーズ サーバ ソフトウェア バンドル：B バンドルとも呼ばれます。このバンドルには、B シリーズ ブレード サーバが機能するために必要なファームウェア イメージ（アダプタ、BIOS、CIMC、ボード コントローラ ファームウェアなど）が含まれています。『*Release Bundle Contents for Cisco UCS Manager, Release 3.2*』には、B シリーズ サーバ ソフトウェア バンドルの内容の詳細が掲載されています。

  （注） Cisco UCS Manager リリース 3.1(2) から、ローカル ディスクのように、B シリーズと C シリーズの両方のサーバ ソフトウェア バンドルに共通するエンドポイント用のファームウェアは、B シリーズと C シリーズの両方のサーバ ソフトウェア バンドルで入手できます。

- C シリーズ サーバ ソフトウェア バンドル：C バンドルとも呼ばれます。このバンドルには、C シリーズ ラック マウント サーバが機能するために必要なファームウェア イメージ（アダプタ、BIOS、CIMC、ボード コントローラ ファームウェアなど）が含まれています。C バンドルには、Cisco UCS S3260 ストレージ サーバ用のファームウェア イメージも含まれています。『*Release Bundle Contents for Cisco UCS Manager, Release 3.2*』には、C シリーズ サーバ ソフトウェア バンドルの内容の詳細が掲載されています。

  （注） Cisco UCS Manager リリース 3.1(2) から、ローカル ディスクのように、B シリーズと C シリーズの両方のサーバ ソフトウェア バンドルに共通するエンドポイント用のファームウェアは、B シリーズと C シリーズの両方のサーバ ソフトウェア バンドルで入手できます。

- 機能カタログ ソフトウェア バンドル：T バンドルとも呼ばれます。このバンドルには、実装固有の調整可能なパラメータ、ハードウェア仕様、および機能制限が指定されます。

  Cisco UCS Manager は機能カタログを使用して、新しく承認された DIMM やディスク ドライブなどのサーバ コンポーネントの表示と設定可能性を更新します。Cisco UCS Manager 機能カタログは単一のイメージですが、Cisco UCS Manager ソフトウェアにも組み込まれています。Cisco UCS Manager リリース 3.2 以降のリリースは、任意の 3.2 カタログ ファイルを使用

できますが、3.1 カタログ バージョンは使用できません。サーバ コンポーネントが特定の BIOS バージョンに依存していない場合、それを使用したり、Cisco UCS Manager に認識させたりすることは、主にカタログ バージョンの機能になります。機能カタログは、UCS インフラストラクチャ リリースにバンドルされるのに加えて、スタンドアロン イメージとしてリリースされる場合もあります。

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。

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。

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。

- 更新：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。

（注） 機能カタログのアップグレードの場合は、更新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。

Cisco UCS Manager ユーザ マニュアル

Cisco UCS Manager では、次の表に示す、使用例を基本とした従来よりもコンパクトな新しいマニュアルが用意されています。

ガイド	説明
『Cisco UCS Manager Getting Started Guide』	Cisco UCS アーキテクチャのほか、Cisco UCS Manager の初期設定や構成のベスト プラクティスなど、稼働前に必要な操作について説明しています。

ガイド	説明
『Cisco UCS Manager Administration Guide』	パスワード管理、ロール ベース アクセスの設定、リモート認証、通信サービス、CIMC セッション管理、組織、バックアップと復元、スケジューリング オプション、BIOS トークン、および遅延展開について説明しています。
『Cisco UCS Manager Infrastructure Management Guide』	Cisco UCS Manager によって使用および管理される物理および仮想インフラストラクチャ コンポーネントについて説明しています。
『Cisco UCS Manager Firmware Management Guide』	ファームウェアのダウンロードと管理、自動インストール によるアップグレード、サービス プロファイルによるアップグレード、ファームウェアの自動同期によるエンドポイントでの直接アップグレード、機能カタログの管理、展開シナリオ、およびトラブルシューティングについて説明しています。
『Cisco UCS Manager Server Management Guide』	新しいライセンス、Cisco UCS Central への Cisco UCS ドメインの登録、電力制限、サーバのブート、サーバプロファイルおよびサーバ関連ポリシーについて説明しています。
『Cisco UCS Manager Storage Management Guide』	Cisco UCS Manager の SAN や VSAN など、ストレージ管理のあらゆる側面について説明しています。
『Cisco UCS Manager Network Management Guide』	Cisco UCS Manager の LAN や VLAN 接続など、ネットワーク管理のあらゆる側面について説明しています。
『Cisco UCS Manager System Monitoring Guide』	Cisco UCS Manager における、システム統計を含むシステムおよびヘルス モニタリングのあらゆる側面について説明しています。
Cisco UCS S3260 サーバと Cisco UCS Manager との統合	Cisco UCS Manager を使用して管理している UCS S シリーズ サーバの管理のあらゆる側面について説明しています。

ファームウェアアップグレードをサポートするコンポーネント

Cisco UCS Manager でサポートされているさまざまなプラットフォームは、ファームウェア アップグレードをサポートするさまざまなコンポーネントを搭載しています。

- ファブリック インターコネクト：
  - Cisco UCS 6332
  - Cisco UCS 6332-16 UP
  - Cisco UCS 6248 UP
  - Cisco UCS 6296 UP
  - Cisco UCS 6324
- シャーシ コンポーネント：
  - ブレード サーバ シャーシ：
    - I/O モジュール

      （注） I/O モジュールは、プライマリ Cisco UCS Mini シャーシではサポートされません。ただし、セカンダリ Cisco UCS Mini シャーシでサポートされます。

    - 電源装置
  - Cisco UCS S3260 シャーシ：
    - シャーシ管理コントローラ（CMC）
    - シャーシ アダプタ
    - SAS エクスパンダ
    - ボード コントローラ
- サーバ コンポーネント：
  - ブレードおよびラック サーバ：
    - アダプタ
    - Cisco Integrated Management Controller（CIMC）
    - BIOS
    - ストレージ コントローラ

（注） ストレージ コントローラは、Cisco UCS Mini ではサポートされるサーバ コンポーネントではありません。

- ボード コントローラ

- Cisco UCS S3260 ストレージ サーバ ノード
  - Cisco Integrated Management Controller（CIMC）
  - BIOS
  - ボード コントローラ
  - ストレージ コントローラ

ファームウェア バージョンの用語

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、BIOS、CIMC、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、BIOS、CIMC、およびシスコのアダプタには、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。

バージョンをまたがるファームウェアのサポート

Cisco UCS Manager の A バンドル ソフトウェア（Cisco UCS Manager、Cisco NX-OS、IOM、FEX ファームウェア）は、サーバ上で以前のリリースの B バンドルまたは C バンドル（ホスト ファームウェア（FW）、BIOS、Cisco IMC、アダプタ FW およびドライバ）と同時に使用できます。

次の表に、Cisco UCS 6200 および 6300 ファブリック インターコネクトでサポートされる A、B、および C バンドルの混在バージョンを示します。

表 *1*：*Cisco UCS 6200* および *6300* ファブリック インターコネクトでサポートされる混在 *Cisco UCS* リリース

		インフラストラクチャのバージョン（A バンドル）			
ホスト FW のバージョン（B または C バンドル）	2.2(8)	3.1(1)	3.1(2)	3.1(3)	3.2(1)
2.2(8)	6200	6200	6200	6200	6200

		インフラストラクチャのバージョン（A バンドル）			
3.1(1)	-	6200、6332、6332-16UP	6200、6332、6332-16UP	6200、6332、6332-16UP	6200、6332、6332-16UP
3.1(2)	-	6200、6332、6332-16UP	6200、6332、6332-16UP	6200、6332、6332-16UP	6200、6332、6332-16UP
3.1(3)	-	6200、6332、6332-16UP	6200、6332、6332-16UP	6200、6332、6332-16UP	6200、6332、6332-16UP
3.2(1)	—	—	—	—	6200、6332、6332-16UP

次の表に、Cisco UCS Mini ファブリック インターコネクトでサポートされる A、B、および C の混在バンドル バージョンを示します。

表 *2*：*Cisco UCS Mini* ファブリック インターコネクトでサポートされる混在 *Cisco UCS* リリース

	インフラストラクチャのバージョン（A バンドル）			
ホスト FW のバージョン（B または C バンドル）	3.1(1)	3.1(2)	3.1(3)	3.2(1)
3.1(1)	6324	6324	6324	6324
3.1(2)	6324	6324	6324	6324
3.1(3)	6324	6324	6324	6324
3.2(1)	—	—	—	6324

次の表に、3.2 バンドルを備えたすべてのプラットフォームでサポートされる、B および C バンドルの混在バージョンを示します。

表 *3*：*3.2(1)A* バンドルを備えたすべてのプラットフォームでサポートされる、*B*、*C* バンドルの混在バージョン

	インフラストラクチャのバージョン（A バンドル）		
Host FW Versions (B, C Bundles)	3.2(1)		
	6200	6300	6324
	ucs-k9-bundle-infra.3.2.xxxx.A.bin	ucs-6300-k9-bundle-infra.3.2.xxxx.A.bin	ucs-mini-k9-bundle-infra.3.2.xxxx.A.bin

	インフラストラクチャのバージョン（A バンドル）		
2.2(8) （B、C バンドル）	Yes	—	—
3.1(1) （B、C バンドル）	Yes	Yes	Yes
3.1(2) （B、C バンドル）	Yes	Yes	Yes
3.1(3) （B、C バンドル）	Yes	Yes	Yes
3.2(1) （B、C バンドル）	Yes	Yes	Yes

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。

サーバ パック

サーバパックを使用すると、完全なサーバアップグレードを必要とせずに、既存のインフラストラクチャで新しいサーバプラットフォーム[1]を動的にサポートすることができます。このサポートは、Cisco UCS Manager カタログ イメージによって提供されます。このモデルにより、新しいサーバを有効化する新しい B シリーズ、または C シリーズ サーバ バンドルが既存のインフラストラクチャ A バンドルでサポートされます。

たとえば、リリース 3.1(1) より後のリリースの B または C サーバ バンドルは、リリース 3.1(1) のインフラストラクチャ A バンドルでサポートされます。ただし、リリース 3.1(1) 以降のリリースの B または C サーバ バンドルは、リリース 3.1(1) よりも前のすべてのリリースのインフラストラクチャ A バンドルでサポートされていません。

特定のリリースの『*Release Notes for Cisco UCS Manager*』には、そのリリースでのバージョンにまたがるファームウェア サポートの完全なマトリックスが記載されています。B または C サーバ バンドルに追加された新機能は、インフラストラクチャ A バンドルを該当するバージョンにアップグレードした後にのみ使用できるようになります。

現在以下のサーバがサーバ パックをサポートしています。

[1] この機能は特定のサーバ プラットフォームに適用されます。

- B シリーズ サーバ：UCS B200 M4、B260 M4、B420 M4、B460 M4、B200 M5
- C シリーズ サーバ：UCS C220 M4、C240 M4、C460 M4、C220 M5、C240 M5

既存のインフラストラクチャバンドルで周辺機器がサポートされていない場合、サーバパック機能によってサポートされません。この周辺機器をサポートするためには、インフラストラクチャバンドルをアップグレードする必要があります。たとえば、既存のインフラストラクチャ バンドルでサポートされていない新しいアダプタを使用してサーバがインストールされている場合、これらのアダプタのサポートには、インフラストラクチャ バンドルへのアップグレードが必要です。これらのアダプタは、サーバ パック機能を通じてサポートすることはできません。

新しいカタログイメージはハードウェアおよびソフトウェアコンポーネントを中断せずに使用できるため、サーバパックを使用すれば、ドメイン全体でのファームウェアアップグレードの運用オーバーヘッドを負担せずに、新しいサーバプラットフォームをアクティブなUCS ドメインにより柔軟に追加できるようになります。

軽量アップグレード

Cisco UCS Manager リリーズ 3.1(3) までは、特定のコンポーネントのみが変更された場合でも、ファームウェアをパッチリリースにアップグレードするには、ファームウェアバンドル全体をダウンロードしてアクティブ化する必要がありました。一部のコンポーネントに修正が加えられていなくても、すべてのコンポーネントのファームウェア バージョンが変更されていました。これにより、そのコンポーネント ファームウェアの不要な更新がトリガーされていました。

システムへのセキュリティ更新もパッチによって提供され、ファブリック インターコネクトとダウンタイムの再起動につながっていました。

Cisco UCS Manager リリース 3.1(3) では、軽量アップグレードが導入され、次のような方法でファームウェア アップグレードが向上しています。

- コンポーネントのファームウェア バージョンは、変更された場合にのみ更新されます。
- セキュリティ更新はサービス パックを通じて提供されます。リリース 3.1(3) では、軽量アップグレードはセキュリティ更新のみをサポートしています。
- サービスパック内では、更新は特定のコンポーネントにのみ適用される場合があります。これらのコンポーネントは、ファブリック インターコネクトの再起動なしで時々アップグレードされることがあります。
- インフラストラクチャおよびサーバ コンポーネントの更新は、共通のサービス パック バンドルを通じて提供されます。サーバ コンポーネントについては、変更したファームウェア イメージのみがサービス パック バンドルの一部となります。これにより、従来の B シリーズおよび C シリーズのバンドルと比較して、サービス パックのバンドルが小さくなりました。

サービス パック

サービス パックは、Cisco UCS Manager インフラストラクチャとサーバ コンポーネントにセキュリティ更新を適用するパッチです。サービス パックは、基本リリースに固有のものです。基本リリースにサービスパックを適用することはできますが、個別にサービスパックをインストールすることはできません。

サービス パックは、インフラストラクチャ コンポーネントとサーバ コンポーネント用の単一バンドルとして提供されます。インフラストラクチャおよびサーバの自動インストールを使用してサービスパックを適用することで、関連するインフラストラクチャコンポーネントおよびサーバコンポーネントをすべて更新できます。Cisco UCS Manager リリース 3.1(3) では、サービス パックのバンドルによって、インフラストラクチャ コンポーネントに対してのみ中断不要な更新が提供されます。インフラストラクチャ コンポーネントの中でも、ファブリック インターコネクトのサービス パックへの更新の場合、OpenSSL の修正などの特定のシナリオにおいては、ファブリック インターコネクトの再起動が必要になる可能性があります。サーバコンポーネントの更新が中断され、アプリケーションのダウンタイムが伴います。

サービス パックはメンテナンス リリース用に累積されます。最新のサービス パックには、特定のメンテナンスリリースの際にリリースされた以前のサービスパックからのすべての修正が含まれています。

以前に適用されたサービス パックは、Cisco UCS Manager GUI と Cisco UCS Manager CLI を介して削除または更新できます。その結果、コンポーネントのファームウェア バージョンは、基本のリリース バンドルに由来します。

サービス パックは、Cisco UCS Manager リリース 3.1(3) より前のメンテナンス リリースには適用されません。

サービス パックのバージョン

サービス パックのバージョンには、次のガイドラインが適用されます。

- サービス パックは基本のバンドルにのみ適用できます。たとえば、サービスパック 3.1(3)SP2 は 3.1(3) リリースにのみ適用できます。3.1(4) リリースとは互換性がないため、適用できません。
- 個別のメインテナンス リリースのサービス パックのバージョンの番号付けに関連はありません。たとえば、サービス パック 3.1(3)SP2 と 3.1(4)SP2 は別個のもので関連はありません。
- 個別のサービスパックを使用して、メンテナンスリリースごとに同じ修正を適用できます。たとえば、3.1(3)SP2 および 3.1(4)SP3 で同じ修正を適用できます。
- サービス パックではこれまでの修正内容が累積されています。同じメンテナンス リリースであれば、どのパッチ バージョンでも最新のサービス パックを適用できます。たとえば、3.1(3)SP3 には、3.1(3)SP2 および 3.1(3)SP1 に行われたすべての修正が含まれます。任意の 3.1(3) リリースに 3.1(3)SP3 を適用できます。

- メンテナンス リリースのサービス パックを、デフォルトのサービス パックのバージョンより下のバージョンにダウングレードすることはできません。
- サービス パックのアップグレードまたはダウングレードが失敗すると、そのメンテナンス リリースのデフォルトのサービスパックのバージョンが実行中のサービスパックのバージョンになります。次に例を示します。

  基本バンドルのバージョン：3.1(3b)

  デフォルトのサービス パックのバージョン：3.1(3)SP2（デフォルト）

  実行中のサービス パックのバージョン：3.1(3)SP3

  3.1(3)SP3 から 3.1(3)SP4 へのアップグレード中に、アップグレードが失敗すると、表示される実行中のサービス パックのバージョンは 3.1(3)SP2（デフォルト）となります。

次の表に、サービスパックが適用されるさまざまな状況で表示されるリリースバージョンと実行バージョンを示します。

リリース バージョン	表示される実行バージョン
3.1(3a)	基本バンドルのバージョン：3.1(3a) サービス パックのバージョン：3.1(3)SP0（デフォルト）
3.1(3)SP1	基本バンドルのバージョン：3.1(3a) サービス パックのバージョン：3.1(3)SP1
3.1(3)SP2	基本バンドルのバージョン：3.1(3a) サービス パックのバージョン：3.1(3)SP2
3.1(3b)	基本バンドルのバージョン：3.1(3b) サービス パックのバージョン：3.1(3)SP2（デフォルト）
3.1(3)SP3	基本バンドルのバージョン：3.1(3b) サービス パックのバージョン：3.1(3)SP3

サービス パックのロールバック

基本リリースに適用されたサービス パックをロールバックできます。次の項では、さまざまなロールバック シナリオ中にバンドルのバージョンおよびサービスパックのバージョンに加えられる変更について説明します。

サービス パックの削除

バンドルのバージョン	サービス パックのバージョン
バンドルのバージョンは変更されません。	サービスパックは、バンドルに付属するデフォルトのバージョンです。

以前のメンテナンス リリースへのインフラストラクチャ バンドルのダウングレード

バンドルのバージョン	サービス パックのバージョン
インフラストラクチャバンドルは、以前のメンテナンス リリースのバージョンに変更されます。	サービスパックは、以前のメンテナンスリリースでは有効ではないため、削除されます。

同じメンテナンスリリース内にあるが以前のサービスパックのバージョンであるインフラストラクチャ バンドルのダウングレード

バンドルのバージョン	サービス パックのバージョン
インフラストラクチャバンドルは、メンテナンス リリース パッチのバージョンに変更されます。	自動インストール中に対応するサービスパックのバージョンが指定されていない場合、インフラストラクチャのアップグレードまたはダウングレード中にサービスパックが削除されます。

サービス パックに関するガイドラインと制約事項

- FI の再起動が必要なサービス パックから FI の再起動が必要な別のサービス パックにアップグレードすると、FI は 2 回再起動されます。
- サーバ自動同期ポリシーは、サービス パックではサポートされていません。
- 下位の FI がリリース 3.1(3) より前のリリースで実行されている場合、サービス パックの自動同期はサポートされません。

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62XXおよび63XX 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ドメインを以降のリリースにアップグレードするために必要な手順については、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。アップグレード ガイドが提供されていない場合は、Cisco Technical Assistance Centerにお問い合わせください。そのリリースからの直接アップグレードはサポートされていない場合があります。

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、自動インストールを使用してアップグレードの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できます。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、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。
- シャーシ プロファイルのシャーシ ファームウェア パッケージを介したシャーシのアップグレード：このオプションにより、1 つの手順ですべての S3260 シャーシ エンドポイントをアップグレードできます。

（注） シャーシプロファイルとシャーシファームウェアパッケージは、S3260 シャーシのみに適用されます。

Cisco UCS Manager を通じた Cisco UCS ドメイン 内のS3X60 サーバ ノード のアップグレード

Cisco UCS Manager を通じて S3260 シャーシ とサーバを含む Cisco UCS ドメインを次のようにアップグレードできます。

- 自動インストール によるインフラストラクチャ コンポーネントのアップグレード：自動インストール を使用することで 1 つの手順で Cisco UCS Manager ソフトウェアおよびファブリック インターコネクト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できます。
- シャーシ プロファイルのシャーシ ファームウェア パッケージを介したシャーシのアップグレード：このオプションにより、1 つの手順ですべてのシャーシ エンドポイントをアップグレードできます。

  『*Cisco UCS S3260 Server Integration with Cisco UCS Manager*』には、シャーシ プロファイルとシャーシ ファームウェア パッケージに関する詳細情報が記載されています。
- 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時間中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。

また、各インフラストラクチャ、シャーシとサーバ エンドポイントでファームウェアを直接アップグレードすることもできます。このオプションにより、ファブリック インターコネクト、SAS エクスパンダ、CMC、シャーシ アダプタ、ストレージ コントローラ、ボード コントローラを含む、多くのインフラストラクチャ、シャーシ、サーバ 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、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。

『*Cisco UCS S3260 Server Integration with Cisco UCS Manager*』には、S3X60 サーバ ノードのファームウェア管理についての詳細情報が記載されています。

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 を使用してそれらの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。

サービス パックの更新のオプション

次のいずれかの方法で Cisco UCS ファームウェアをサービス パックにアップグレードできます。

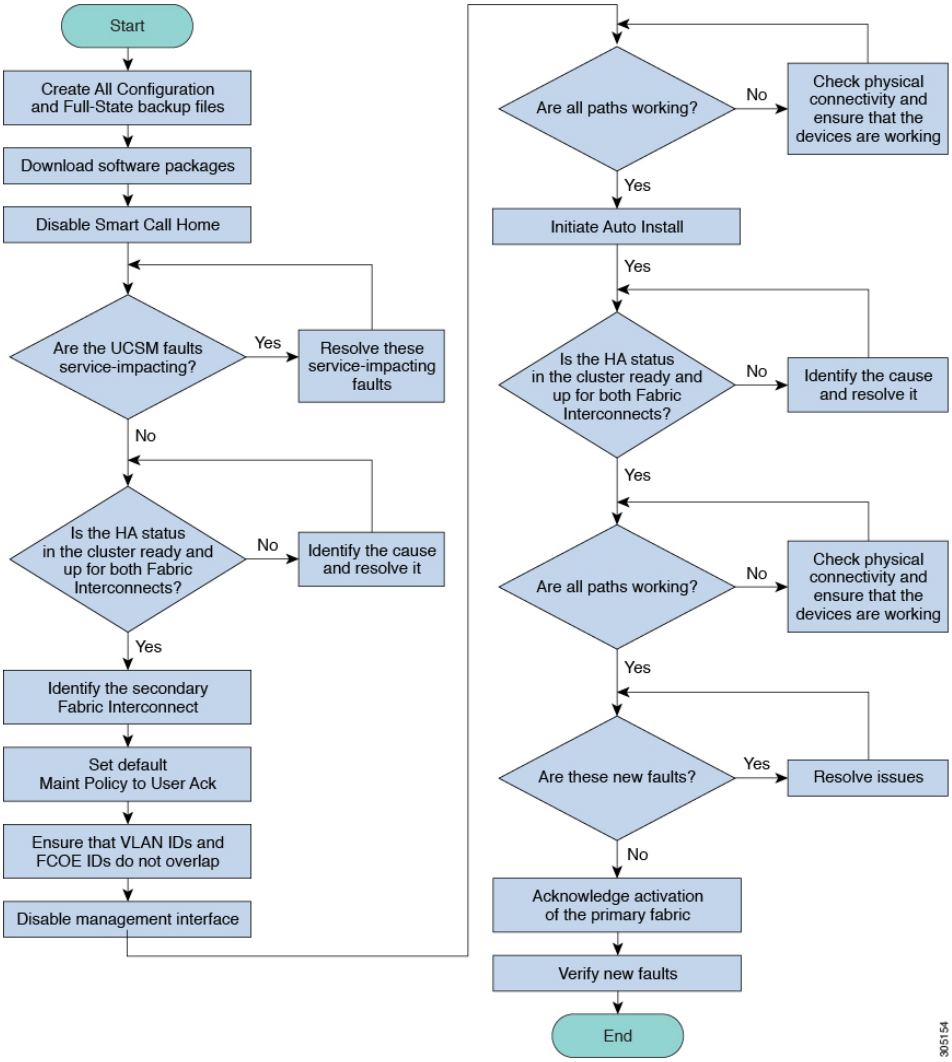
- インフラストラクチャの自動インストールを介してサービス パックにアップグレードする
- サーバの自動インストールを介してサービス パックにアップグレードする
- サービスプロファイルのファームウェア パッケージを介してサービスパックにアップグレードする
- シャーシ プロファイルのシャーシ ファームウェア パッケージを介してサービス パックにアップグレードする
- 基本のメンテナンス リリースで Cisco UCS Manager サービス パックを直接アクティブにする
- 基本のメンテナンス リリースでファブリック インターコネクトのサービス パックを直接アクティブにする

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 バージョンに自動的にアップグレードすることができます。

- インストール インフラストラクチャ ファームウェア：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。図 4：インフラストラクチャ ファームウェアの自動インストールのプロセス フロー，（20 ページ）に、インフラストラクチャ ファームウェアを自動的にインストールするための推奨プロセス フローを示します。

図 4：インフラストラクチャ ファームウェアの自動インストールのプロセス フロー



- インストール サーバ ファームウェア：必要に応じて、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したり、また 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アップグレードし、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。

シスコは、自動インストール を使用して Cisco UCS ドメイン をアップグレードすることを強く推奨します。

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

サーバ ファームウェアおよび BIOS のバージョンは、複数のサーバにわたって定期的に更新する必要があります。これを手動で行う場合は、連続的に行う必要があり、長いダウンタイムが必要となります。

更新テンプレートであるサービス プロファイル テンプレートの属性としてホスト ファームウェア ポリシーを定義することにより、ホスト ファームウェア パッケージを使用できます。サービス プロファイル テンプレートに加えたすべての変更は、そのインスタンス化されたサービス プロファイルに自動的に反映されます。その後、サービス プロファイルに関連付けられているサーバもファームウェア バージョンと同時にアップグレードされます。

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。

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。

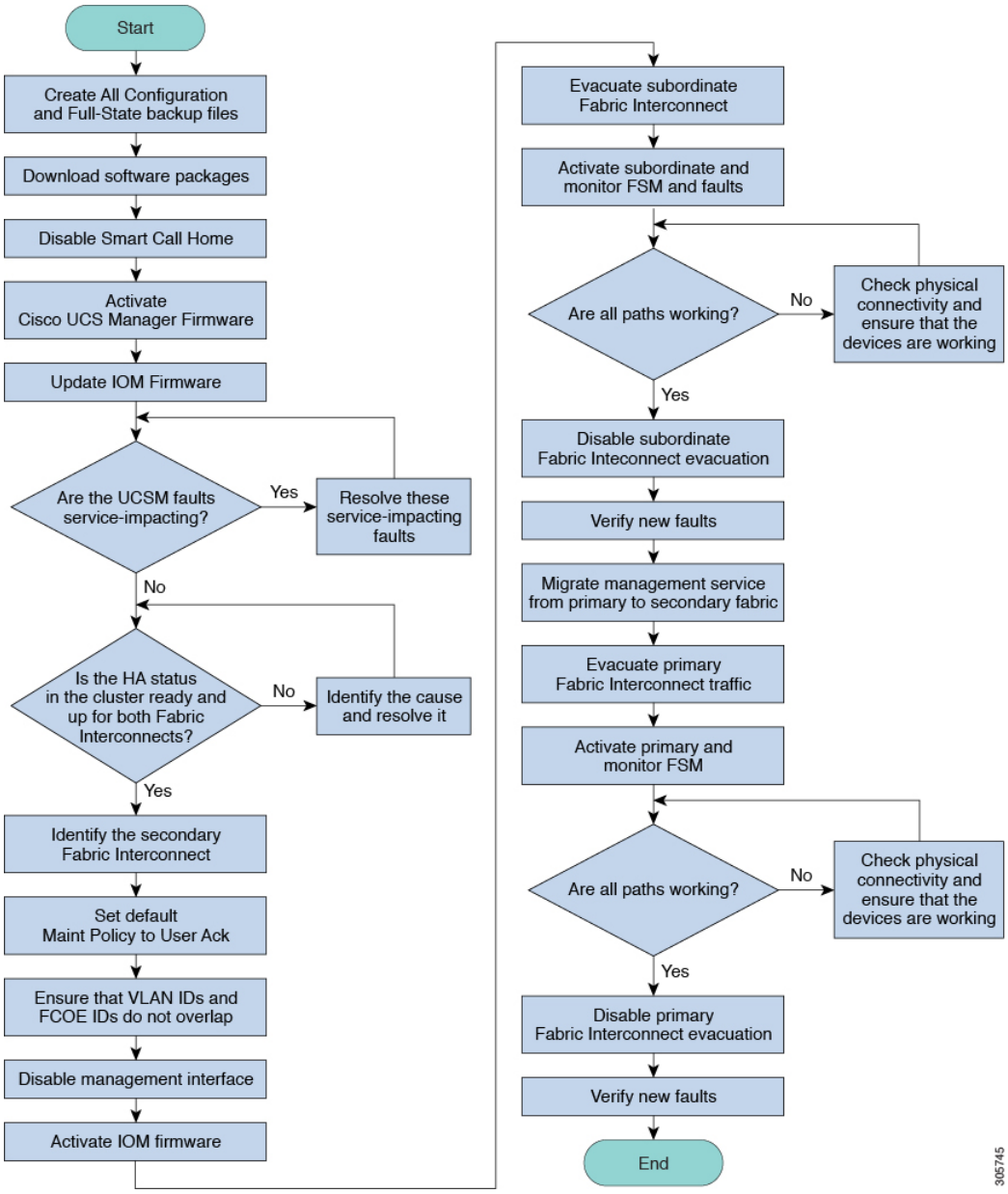
使用するターゲット シャーシに応じて、各種コンポーネントでファームウェアを直接アップグレードすることができます。

インフラストラクチャ	UCS 5108 シャーシ	UCS ラックサーバ	Cisco UCS S3260 シャーシ
• ファブリック インターコネクト • Cisco UCS Manager	• I/O モジュール • 電源装置 • サーバ： ◦ アダプタ ◦ CIMC ◦ BIOS ◦ ストレージ コントローラ ◦ ボード コントローラ	• アダプタ • CIMC • BIOS • ストレージ コントローラ • ボード コントローラ	• CMC • シャーシ アダプタ • SAS エクスパンダ • シャーシ ボード コントローラ • サーバ： ◦ CIMC ◦ BIOS ◦ ボード コントローラ ◦ ストレージ コントローラ

（注） サーバ エンドポイント上でのファームウェアの直接アップグレードは、検出され、関連付けられていないサーバとシスコ アダプタでのみ可能です。

図 5：インフラストラクチャ ファームウェアの手動インストールのプロセス フロー，（23 ページ）は推奨されるプロセス フローを示しています。

図 5：インフラストラクチャ ファームウェアの手動インストールのプロセス フロー



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） 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 6200 シリーズ ファブリック インターコネクトから Cisco UCS 6300 シリーズ ファブリック インターコネクトへの移行中のファームウェア アップグレード

移行中は次のガイドラインに従う必要があります。

- Cisco UCS 6200 シリーズ ファブリック インターコネクトは、Cisco UCS Managerリリース 3.1(1) 以降のリリースにアップグレードする必要があります。
- Cisco UCS 6300 シリーズ ファブリック インターコネクトには、アップグレード元の Cisco UCS 6200 シリーズ ファブリック インターコネクトと同じビルド バージョンをロードする必要があります。
- Cisco UCS 6200 シリーズ ファブリック インターコネクトと Cisco UCS 6300 シリーズ ファブリック インターコネクト間でのみ移行できます。Cisco UCS 6248 UP と Cisco UCS 6296 UP ファブリック インターコネクト間、または Cisco UCS 6332 と Cisco UCS 6332 16UP ファブリック インターコネクト間では移行できません。
- すべてのファブリック インターコネクトには、同じバージョンのキックスタート、システム、および UCSM イメージが必要です。
- ファブリック インターコネクトのアップグレードは、新しい FEX または仮想インターフェイス カードにアップグレードする前に実行する必要があります。
- クラスタ設定の場合、両方のファブリック インターコネクトに、ファブリック インターコネクトと FEX 間の対称接続トポロジが必要です。
- スタンドアロンインストールでは、ダウンタイムを想定する必要があります。ファブリック インターコネクトのアップグレードでは、本質的にトラフィックの中断が発生します。
- ベストプラクティスは、このハードウェアアップグレードを実行する前に、設定およびソフトウェアのフル バックアップを実行することです。

Cisco UCS Manager リリース 3.2 へのファームウェア アップグレード

Cisco UCS Manager リリース 3.2 へのアップグレード条件

- Cisco UCS Manager リリース 3.2 にアップグレードする前に、既存のインフラストラクチャおよびサーバ バンドルのリリース バージョンが Cisco UCS Manager 2.2(x) 以降であることを確認してください。

重要　Cisco UCS Manager リリース 2.2(1a) より前のインフラストラクチャ バンドルからのアップグレードはサポートされません。ただし、クラスタ内の FI を Cisco UCS Manager リリース 2.1(2) 以降のリリースで実行される FI に置き換えてから、自動同期機能を使用することで、この FI を直接 3.x(x) リリースにアップグレードできます。このようなシナリオでは、2.2(x) にまずアップグレードしてから 3.x(x) リリースにアップグレードする必要はありません。

- Cisco UCS Manager リリース 3.2 にアップグレードする前に、以下を実行して、使用中のキー リングが 2048 ビット以上のモジュラス サイズを備えているか確認してください。

1. 次のコマンドを使用して、使用中のキー リングのモジュラス サイズを確認します。

```
UCS-A# scope security
UCS-A /security # scope keyring keyring-name
UCS-A /security/keyring # show detail
```

2. デフォルトのキー リングを使用しており、モジュラス サイズが 2048 ビット未満である場合は、モジュラス サイズを 2048 ビット以上に再構成し、次のコマンドを使って証明書を再生成します。

```
UCS-A# scope security
UCS-A /security # scope keyring default
UCS-A /security/keyring # set modulus mod2048
UCS-A /security/keyring # set regenerate yes
UCS-A /security/keyring # commit-buffer
UCS-A /security/keyring # show detail
```

3. デフォルトとは異なるキー リングを使用しており、モジュラス サイズが 2048 ビット未満である場合は、既存のキー リングを削除して、モジュラス値が 2048 以上の新たなキー リングを作成する必要があります。

（注）　使用中のキー リングは削除できません。使用中のキー リングを削除するには、まず別のキー リングを使用するよう HTTPS を設定する必要があります。

Cisco UCS Manager リリース 3.1 以降のリリースでは、モジュラス サイズが 2048 ビット未満であるキー リングをサポートしていません。

Cisco UCS Manager リリース 3.2 へのアップグレードが失敗する条件

次のシナリオでは、以前のリリースから Cisco UCS Managerリリース 3.2 へのアップグレードが失敗し、Cisco UCS Manager は以前のバージョンにロールバックします。

- ファブリック インターコネクトのパーティションに十分な空き領域がない状態でのアップグレード
  - `/var/sysmgr` の空き容量が 20 % 未満
  - `/mnt/pss` の空き容量が 30 % 未満
  - `/bootflash` の空き容量が 20 % 未満
- 誤設定による Cisco UCS Manager の検証エラー

アップグレード中の SNMP の自動的な無効化

以前のリリースから Cisco UCS Managerリリース 3.2 にアップグレードするときに、SNMP が自動的に無効になります（有効化されていた場合）。SNMP の状態は、両方のファブリック インターコネクトのアップグレードの完了後に復元されます。アップグレード中、SNMP が自動的に無効になると、すべての SNMP 操作が一時停止します。シスコでは、両方のファブリック インターコネクトのアップグレードが完了してから SNMP 操作を再開することを推奨します。

重要 SNMP の状態は Cisco UCS Manager のアップグレード後に復元されますが、SNMP 操作は両方のファブリック インターコネクトのアップグレードの完了後にのみ実行できます。

マイナーまたはパッチリリースへのファームウェアアップグレード

Cisco UCS Manager ソフトウェアのリリース番号は、メジャー リリース識別番号、マイナー リリース識別番号、およびパッチ リリース識別番号で構成されます。マイナー リリース識別番号とパッチ リリース識別番号は、カッコ内に列挙されます。たとえば、ソフトウェア バージョン番号が **3.2(2a)** の場合は、次の構成になります。

- **3.2** はメジャー リリース識別番号
- **2** はマイナー リリース識別番号
- **a** はパッチ リリース識別番号

つまり、これらは **3.2** リリース トレインの**first**のマイナー リリースの **a** パッチを示しています。

メジャー リリース内でのメンテナンス リリースとパッチへのファームウェア アップグレードは、メジャー リリースと同じ方法で行います。

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。

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。

（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。

UCS M5 サーバがある Cisco UCS ドメイン

UCS M5 サーバがある Cisco UCS ドメインでは、Cisco UCS Manager リリース 3.2(1) からそれよりも前のリリースにダウングレードする場合は UCS M5 サーバの使用を中止する必要があります。これは、UCS M5 サーバが、Cisco UCS Manager リリース 3.2(1) 以降でのみサポートされているためです。

UCS M5 サーバの使用を停止せずに Cisco UCS Manager リリース 3.2(1) からそれよりも前のリリースにダウングレードすると、アップグレードの検証に失敗し、Cisco UCS Manager からダウングレード操作を続行する前にサーバを停止するよう求められます。

ブレード サーバのボード コントローラ ファームウェア

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。Cisco 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 バージョンが、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。

サポートされていない機能はダウングレードの前に設定解除が必要

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、以前のリリースでは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。サポートされていない機能の設定を解除せずに B または C のサーババンドルをダウングレードすると、その機能はダウングレードされたリリースで動作しない場合があります。たとえば、[On Next Reboot] メンテナンス ポリシーは、3.1 の B バンドルと C バンドルでサポートされます。任意のサーババンドルをダウングレードすると、このメンテナンスポリシー オプションは対応するサーバでは動作しません。

以前のリリースでサポートされていないすべての機能を設定解除せずにインフラストラクチャ バンドルをダウングレードしようとすると、ダウングレードに失敗する場合があります。

SNMP をダウングレードの前に無効化

Cisco UCS Manager リリース 3.2 からそれよりも前のリリースにダウングレードする前に、SNMP を無効にする必要があります。ダウングレード プロセスは、SNMP が無効にされるまで開始されません。

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. ダウングレード先のリリースから設定のバックアップを取得します。これは、現在のリリースにアップグレードしたときに作成したバックアップです。
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設定解除します。
3. Full State バックアップ ファイルと All Configuration バックアップ ファイルを作成します。
4. Cisco UCS Manager をダウングレードします。
5. erase-config を実行します。
6. 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。

（注） ステップ 5 および 6 は任意です。これらのステップは、既存の設定が使用不能になった場合にのみ実行します。この場合、ステップ 1 またはステップ 3 からコンフィギュレーション バックアップをインポートします。

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。

重要 Cisco UCS Central から Cisco UCS ドメインの登録を解除しないでください。

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。

（注） Cisco UCS Central のファームウェア管理の詳細については、『*Cisco UCS Central Administration Guide*』および『*Cisco UCS Central CLI Reference Manual*』の「Firmware Management」の章を参照してください。

第 2 章

ガイドラインと前提条件

ファームウェアアップグレードに関するガイドラインとベスト プラクティス

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、次の注意事項、ベスト プラクティス、および制約事項を考慮してください。

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 ドメインの設定によっては、アップグレード プロセスで追加の変更が必要な場合があります。

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 Release 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 Release 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、重複している VLAN からのイーサネット トラフィックが破棄されます。そのため、イーサネットと FCoE の VLAN ID が重複していないことを確認してから、Cisco UCS リリース 3.1 以降にアップグレードすることをお勧めします。

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 リリース 3.1 以降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。

（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 ID が 4030 ～ 4047 の VLAN 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。

- Cisco UCS ドメイン FC スイッチ モードを使用する予定の場合は、ID が 3040 ～ 4078 の範囲にある VSAN を設定しないでください。
- Cisco UCS ドメイン FC エンドホスト モードを使用する予定の場合は、ID が 3840 ～ 4079 の範囲にある VSAN を設定しないでください。

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に関するハードウェア関連のガイドライン

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

注意 更新が完了するまで、エンドポイントがあるハードウェアを取り外したり、メンテナンス作業を実行しないでください。ハードウェアが取り外されたり、その他のメンテナンス作業により使用できない場合、ファームウェアの更新は失敗します。この失敗により、バックアップパーティションが破損する場合があります。バックアップ パーティションが破損しているエンドポイントではファームウェアを更新できません。

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。

サードパーティ アダプタは必ずホスト 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

サードパーティ アダプタは、エンドポイントから直接アップグレードできません。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。

ファブリック インターコネクトの設定

クラスタ化されたファブリック インターコネクトは、データ パスの冗長性を意図的に提供します。ただし、データ トラフィックが中断されないように、サービス プロファイルに冗長イーサネットおよびストレージ（FC/FCoE）インターフェイスを設定する必要があります。また、対応するオペレーティング システムが 1 つのファブリック パスの停止を処理するように正しく設定されていることを確認する必要があります。

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、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。

アップグレードに関するファームウェアおよびソフトウェア関連のガイドライン

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

シスコのアダプタやサーバ 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。

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すると、必要な順序でアップデートが行われることが保証されず、エンドポイント、ファブリック インターコネクト、および Cisco UCS Manager 間の通信が中断することがあります。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 パーティションが 70 % を超えると、障害が発生しますが、自動インストールは続行します。ブートフラッシュ パーティションが 80 % を超えると、障害が発生し、自動インストールは続行しません。

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空き領域のチェック，（75 ページ） には、これらのパーティションで使用可能なストレージのモニタリングに関する詳細情報が掲載されています。

アダプタおよび I/O モジュールへのアクティベーションの影響の特定

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ていない場合、アクティブ化されたファームウェアは pending-next-boot 状態のままになります。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 パッチ内のファブリック 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。この再起動は、Call Home アラートをトリガーする、サービス中断と同様のイベントおよびコンポーネント障害を発生させます。アップグレードを開始する前に Call Home を無効にしない場合、アップグレード関連コンポーネントによってアラートが生成され、Call Home の設定に基づいて再起動と通知が送信されます。

ファブリック インターコネクト トラフィックの待避

リリース 2.2(4) で導入されたファブリック インターコネクト トラフィックの待避は、IOM または FEX を通じてファブリック インターコネクトに接続されているすべてのサーバからファブリック インターコネクトを通過するすべてのトラフィックを待避させる機能です。

システムの下位のファブリック インターコネクトをアップグレードすると、ファブリック インターコネクト上でアクティブなトラフィックが中断されます。このトラフィックは、プライマリ 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。手動によるアップグレードプロセス中は、次のようにファブリック エバキュエーションを使用できます。

1. [Admin Evac Mode] を [On] に設定して、ファブリック インターコネクトでアクティブなすべてのトラフィックを停止します。
2. フェールオーバーが設定されている vNIC に対して、Cisco UCS Manager や vCenter などのツールを使用して、トラフィックがフェールオーバーされたことを確認します。
3. 下位のファブリック インターコネクトをアップグレードします。

4 [Admin Evac Mode] を [Off] に設定して、停止されたすべてのトラフィック フローを再開します。

5 クラスタ リードを下位のファブリック インターコネクトに変更します。

6 ステップ 1 ~ 4 を繰り返し、他のファブリック インターコネクトをアップグレードします。

（注）

- ファブリック インターコネクト トラフィックの待避は、クラスタ設定でのみサポートされます。
- トラフィックの待避は、従属ファブリック インターコネクトからのみ実行できます。
- 待避が設定されているファブリック インターコネクトの IOM または FEX のバックプレーン ポートがダウンし、その状態が [Admin down] として表示されます。手動によるアップグレード プロセス中に、これらのバックプレーン ポートを [Up] 状態に移動させ、トラフィック フローを再開するには、[Admin Evac Mode] を明示的に [Off] に設定する必要があります。

自動インストール でのファブリック エバキュエーション

Cisco UCS Manager リリース 3.1(3) から、自動インストール 中にファブリック エバキュエーションを使用できます。自動インストールの開始時に、ファブリック エバキュエーションを有効にしてから 自動インストール を開始すると、次のイベント シーケンスが開始されます。

1 下位のファブリック インターコネクト（FI-B）が待避させられ、アクティブ化されます。

2 フェールオーバーが発生し、プライマリ ファブリック インターコネクト（FI-A）が下位のファブリック インターコネクトになります。FI-B がクラスタ リードになります。

3 FI-A は待避させられ、アクティブ化されます。

自動インストールでファブリック エバキュエーションを使用し、ファブリック エバキュエーションが 自動インストール の前にファブリック インターコネクトで有効になっていた場合、ファブリック エバキュエーションは 自動インストール が完了した後で無効になります。

プライマリ ファブリック インターコネクトでファブリック エバキュエーションが有効になっている状態で 自動インストール を開始しないでください。ファブリック エバキュエーションを 自動インストール の前にプライマリ ファブリック インターコネクトで手動で有効にした場合は、自動インストール の開始前に手動で無効にする必要があります。

（注）

- ファブリック インターコネクト トラフィックの待避は、クラスタ設定でのみサポートされます。
- トラフィックの待避は、従属ファブリック インターコネクトからのみ実行できます。
- 待避が設定されているファブリック インターコネクトのIOMまたはFEXのバックプレーン ポートがダウンし、その状態が [Admin down] として表示されます。これらのバックプレーン ポートは、自動インストール の完了後に [Up] 状態に復帰します。

ファブリック インターコネクト トラフィックの待避の設定

ここで説明する手順を使用することも、このビデオ（http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/enable_and_disable_fi_traffic_evacuation.html）の [Play] をクリックしてファブリック インターコネクト トラフィックの待避を有効および無効にする方法を視聴することもできます。

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] > [Fabric Interconnects] > *[Fabric_Interconnect_Name]* の順に展開します。

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 [General] タブの [Actions] 領域で、[Configure Evacuation] をクリックします。
[Configure Evacuation] ダイアログボックスが表示されます。

ステップ 5 指定したファブリック インターコネクトを通過するトラフィックの待避を設定するには、[Admin Evac Mode] フィールドにある次のオプション ボタンの 1 つをクリックします。

- [On]：指定したファブリック インターコネクトを通過するアクティブなすべてのトラフィックを停止します。
- [Off]：指定したファブリック インターコネクトを通過するトラフィックを再開します。

ステップ 6 （任意） ファブリック インターコネクトを通過するトラフィックをその現在の待避状態に関係なく待避させるには、[Force] チェックボックスをオンにします。

ステップ 7 [Apply] をクリックします。
警告ダイアログボックスが表示されます。

```
Enabling fabric evacuation will stop all traffic through this Fabric Interconnect from
servers attached through IOM/FEX.
The traffic will fail over to the Primary Fabric Interconnect for fail over vnics.
Are you sure you want to continue?
```

ステップ 8 [OK] をクリックして、ファブリック インターコネクト トラフィックの待避を確定して続行します。

セキュア ファームウェア アップデート

Cisco UCS Manager リリース 3.1(2) では、セキュア ファームウェア アップデートが採用されています。これは、サード パーティの Intel ネットワークおよびストレージ アダプタ用にアダプタのファームウェアを安全に更新できるものです。アダプタ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できるのはサーバ管理者のみです。root 権限を持つ OS 管理者は、アダプタ ファームウェアをダウングレードできません。

次の Cisco UCS サーバがセキュア ファームウェア アップデートをサポートしています。

- Cisco UCS C460 M4 サーバ
- Cisco UCS C240 M4 サーバおよび Cisco UCS C240 M5 サーバ
- Cisco UCS C220 M4 サーバおよび Cisco UCS C220 M5 サーバ
- Cisco UCS B200 M4 サーバ および Cisco UCS B200 M5 サーバ
- Cisco UCS C480 M5 サーバ

セキュア ファームウェア アップデートをサポートするネットワーク アダプタとストレージ ディスク

Cisco ブレード サーバでサポートされるストレージ ディスク

次の Intel NVMe ストレージ ディスクは Cisco UCS B200 M5 サーバ および Cisco UCS B480 M5 サーバ でのセキュア ファームウェア アップデートをサポートしています。

表 *4* : サポートされる *NVMe* ストレージ ディスク

NVMe ストレージ ディスク
UCSC-NVMEHW-H800
UCSC-NVMEHW-H1600
UCSC-NVMEHW-H3200
UCSC-NVMEHW-H6400
UCSC-NVMEHW-H7680

以下の NVMe ストレージ ディスクは、UCSB-LSTOR-PT ストレージ コントローラが搭載された Cisco UCS B200 M4 サーバ上でセキュア ファームウェア アップデートをサポートしています。

ストレージ ディスク
UCS-PCI25-8003
UCS-PCI25-16003

ストレージ ディスク
UCS-PCI25-40010
UCS-PCI25-80010

（注） Cisco UCS B200 M4 サーバ上では、以下のものに対するセキュア ファームウェア アップデートはサポートされていません。

- SAS ストレージ コントローラを搭載する NVMe ディスク。
- Cisco UCS B200 M4 サーバ上の NVMe ディスクと HDD の組み合わせ。
- ネットワーク アダプタ。

Cisco ラック サーバでサポートされているネットワーク アダプタとストレージ ディスク

次の NVMe ストレージ ディスクは Cisco UCS C220 M5 サーバ サーバ、Cisco UCS C240 M5 サーバ サーバ、および Cisco UCS C480 M5 サーバ サーバでのセキュア ファームウェア アップデートをサポートしています。

表 *5* : サポートされる ***NVMe*** ストレージ ディスク

NVMe ストレージ ディスク
UCSC-NVMEHW-H800
UCSC-NVMEHW-H1600
UCSC-NVMEHW-H3200
UCSC-NVMEHW-H6400
UCSC-NVMEHW-H7680
UCSC-NVME-H16003 ～ UCSC-F-H16003
UCSC-NVME-H32003
UCSC-NVME-H38401
UCSC-NVME-H64003
UCSC-NVME-H76801

以下の Intel ネットワーク アダプタは、Cisco UCS C460、C240、および C220 M4 サーバ上でセキュア ファームウェア アップデートをサポートしています。

表 *6*：サポートされるネットワーク アダプタ

ネットワーク アダプタ
UCSC-PCIE-IQ10GF
UCSC-PCIE-ID10GF
UCSC-PCIE-ID40GF

次の Intel NVMe ストレージディスクは、Cisco UCS C460 M4 サーバ、Cisco UCS C240 M4 サーバ、および Cisco UCS C220 M4 サーバ でのセキュア ファームウェア アップデートをサポートしています。

表 *7*：サポートされる *NVMe* ストレージ ディスク

NVMe ストレージ ディスク	説明
UCS-PCI25-8003	P3600 2.5"
UCS-PCI25-16003	P3600 2.5"
UCS-PCI25-40010	P3700 2.5"
UCS-PCI25-80010	P3700 2.5"
UCSC-F-I80010	P3700 HHHL
UCSC-F-I160010	P3700 HHHL
UCSC-F-I20003	P3600 HHHL

Cisco UCS サーバ上セキュア ファームウェア サポートのガイドライン

Cisco UCS Manager リリース 3.1(2) では、セキュア ファームウェア アップデートのサポートが導入されています。

重要 CIMC がバージョン 2.0(13) 以降を実行し、Cisco UCS Manager がリリース 3.1(2) 以降のリリースを実行していることを確認します。CIMC が 2.0(13) よりも前のバージョンを実行し、Cisco UCS Manager がリリース 3.1(2) よりも前のリリースを実行している場合、セキュア ファームウェア アップデートを実行できません。

ブレード サーバに対するガイドライン

Cisco UCS B200 M4 サーバおよび Cisco UCS B200 M5 サーバ でのセキュア ファームウェア アップデートについては、次の手順を実行します。

- 以前のリリースの Cisco UCS Manager を実行している場合は、Cisco UCS Manager インフラストラクチャ ソフトウェア バンドルと B シリーズ サーバ ソフトウェア バンドルを Cisco UCS Manager リリース 3.1(2) にアップグレードします。詳細については、『*Cisco UCS Manager Firmware Management Guide, Release 3.2*』を参照してください。
- Cisco UCS B200 M4 サーバおよび Cisco UCS B200 M5 サーバ に UCSB-LSTOR-PT ストレージ コントローラを取り付け、NVMe ディスクを挿入します。
- Cisco UCS B200 M4 サーバまたは Cisco UCS B200 M5 サーバ を再認識させます。『*Cisco UCS Manager Infrastructure Management Guide, Release 3.2*』の「*Reacknowledging a Blade Server*」セクションを参照してください。

（注） NVMe ディスクのホット プラグはサポートされていません。サーバ検出に失敗せず、NVMe ディスクが CIMC および BIOS で認識されることを確認します。サーバがデフォルト ホスト ファームウェア パッケージを使用するサービス プロファイルに関連付けられた後、自動インストール がトリガーされます。NVMe ディスクは、自動インストール 中に最新のファームウェアで更新できます。

Cisco UCS Manager リリース 3.1(2) は NVMe ブートをサポートしていません。NVMe ディスクは、ホスト OS が SAN または iSCSI ブートにある、データ LUN としてのみ使用できます。

（注） サーバ検出に失敗せず、NVMe ディスクが CIMC および BIOS で認識されることを確認します。サーバがデフォルト ホスト ファームウェア パッケージを使用するサービス プロファイルに関連付けられた後、自動インストール がトリガーされます。NVMe ディスクは、自動インストール 中に最新のファームウェアで更新できます。

Cisco UCS Manager リリース 3.2(1) は NVMe ブートをサポートしています。

ラック サーバに対するガイドライン

Cisco UCS C460、C240、および C220 M4 および M5 サーバでのセキュア ファームウェア アップデートについては、次の手順を実行します。

- 以前のリリースの Cisco UCS Manager を実行している場合は、Cisco UCS Manager インフラストラクチャ ソフトウェア バンドルと C シリーズ サーバ ソフトウェア バンドルを Cisco UCS Manager リリース 3.1(2)リリース 3.1(2) にアップグレードします。詳細については、『*Cisco UCS Manager Firmware Management Guide, Release 3.2*』を参照してください。

- Cisco UCS サーバを再認識させます。『*Cisco UCS Manager Infrastructure Management Guide, Release 3.2*』の「*Reacknowledging a Rack Server*」セクションを参照してください。

（注） NVMe ディスクのホット プラグはサポートされていません。サーバ検出に失敗せず、NVMe ディスクが CIMC および BIOS で認識されることを確認します。サーバがデフォルト ホスト ファームウェア パッケージを使用するサービス プロファイルに関連付けられた後、自動インストール がトリガーされます。NVMe ディスクは、自動インストール 中に最新のファームウェアで更新できます。

Cisco UCS Manager リリース 3.1(2) は NVMe ブートをサポートしていません。NVMe ディスクは、ホスト OS が SAN または iSCSI ブートにある、データ LUN としてのみ使用できます。

（注） サーバ検出に失敗せず、NVMe ディスクが CIMC および BIOS で認識されることを確認します。サーバがデフォルト ホスト ファームウェア パッケージを使用するサービス プロファイルに関連付けられた後、自動インストール がトリガーされます。NVMe ディスクは、自動インストール 中に最新のファームウェアで更新できます。

Cisco UCS Manager リリース 3.2(1) は NVMe ブートをサポートしています。

自動インストールによるアップグレードに関する注意事項とガイドライン

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ガイドラインとベスト プラクティス，（31 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ようになっていることが必要です。

- 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、インストール サーバ ファームウェア の処理は失敗します。
- アップグレードする各サーバについて、ストレージ コントローラとローカル ディスク上で実行されているファームウェアのバージョンを確認し、それらが [Ready] 状態になっていることを確認します。

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、デフォルトのホスト ファームウェア ポリシーを変更して、Cisco UCS ドメイン内のブレード サーバおよびラックマウント サーバ用のファームウェアを追加できます。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 ポリシーに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。これは Cisco UCS には該当しません。

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	• インストールインフラストラクチャファームウェアの実行 • インストール サーバ ファームウェアの実行 • 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）	インストール サーバ ファームウェアの実行
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

インストール サーバ ファームウェア へのホスト ファームウェア パッケージの影響

インストール サーバ ファームウェア 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 プロファイルにインストール サーバ ファームウェア 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 インストール サーバ ファームウェア 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インストール サーバ ファームウェア を使用すると、インストール サーバ ファームウェア 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。インストール サーバ ファームウェア 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 インストール サーバ ファームウェア 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。

- インストール サーバ ファームウェア 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 インストール サーバ ファームウェア 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

インストール サーバ ファームウェアを実行した後、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インストールサーバファームウェア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、最後にインストールサーバファームウェア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。インストール サーバ ファームウェアには、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インストール サーバ ファームウェアを再実行することはできません。

（注） 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。

Cisco UCS Central のファームウェア管理に関する注意事項、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。

（注） Cisco UCS Central のファームウェア管理の詳細については、『*Cisco UCS Central Administration Guide*』および『*Cisco UCS Central CLI Reference Manual*』の「Firmware Management」の章を参照してください。

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、アップデート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、次の作業を実行します。

- リリース ノートの内容を確認します。
- 適切な『Hardware and Software Interoperability Matrix』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 のリリースに適切なレベルであ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、データ パスの準備が整っていることの確認, （61 ページ）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 シリーズ ラックマウント サーバのインストール ガイドの指示に従います。
- iSCSI ブート用に設定されている Cisco UCS ドメインの場合、次の操作を行ってから、Cisco UCS Release 3.1(1) 以降にアップグレードしてください。
  - 複数のサービス プロファイルで使用されているすべての iSCSI vNIC に、一意のイニシエータ名が指定されていることを確認します。
  - いずれかの iSCSI vNIC にサーバ プロファイルと同じイニシエータ名が指定されている場合、Cisco UCS は、1 つの一意のイニシエータ名を持つようにサービス プロファイルを再設定します。
  - ブート LUN が新しい IQN に表示されるように、各ネットワーク ストレージ デバイスで対応する IQN 発信側名を変更します。

アップグレード前検証

ファームウェアをインストールする前に、次のアップグレード前検証を実行してください。

バックアップ ファイルの作成

Cisco UCS Manager からバックアップを実行する場合は、システム設定全体またはその一部のスナップショットを作成し、ファイルをネットワーク上の場所にエクスポートします。バックアップは、システムが起動されて動作している間に実行できます。バックアップ操作では、管理プレーンからの情報だけが保存されます。バックアップは、サーバまたはネットワーク トラフィックには影響しません。

シスコでは、Cisco UCS ファームウェア アップグレードを開始する前に、次のバックアップ ファイルを作成することを推奨します。

- [All Configuration] バックアップ ファイル：すべてのシステムおよび論理設定の XML バックアップ
- [Full State] バックアップ ファイル：システム全体のバイナリ スナップショット

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

バックアップ サーバの IPv4 アドレスまたは IPv6 アドレスおよび認証クレデンシャルを取得します。

手順

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：[Enabled] 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。

  システム全体のスナップショットが含まれるバイナリ ファイルを作成するには、[Full State] オプション ボタンをクリックします。
- [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。

  このチェックボックスがバックアップ操作の [Logical Configuration] で選択されている場合は、vHBA、WWPN、WWNN、vNIC、MAC、UUID などのプールから取得したすべての ID がバックアップ ファイルに保持されます。

  （注） このチェックボックスが選択されていない場合、ID は再び割り当てられ、ユーザ ラベルは復旧後に失われます。
- [Location of the Backup File] フィールド：ローカル ファイル システムにバックアップ ファイルを保存するには、[Local File System] オプション ボタンをクリックします。リモート ファイル システムにバックアップ ファイルを保存するには、[Local File System] オプション ボタンをクリックします。

  場所が [Local File System] に設定されている場合、Cisco UCS Manager GUI によって [Filename] フィールドが表示されます。[Remote File System] に設定されている場合、Cisco UCS Manager GUI によって次に説明する残りのフィールドが表示されます。

- [Filename] フィールド：ローカル ファイル システム内の新しい場所にナビゲートするには、[Browse] をクリックします。
- [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に、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
- [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、Cisco UCS Manager で DNS サーバを使用するように設定する必要があります。
- [Remote File] 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。

完全な状態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

はじめる前に

バックアップ サーバの IPv4 アドレスまたは IPv6 アドレスおよび認証クレデンシャルを取得します。

手順

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：[Enabled] 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：システム全体のスナップショットが含まれるバイナリ ファイルを作成するには、[Full State] オプション ボタンをクリックします。
- [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。

  このチェックボックスがバックアップ操作の [Logical Configuration] で選択されている場合は、vHBA、WWPN、WWNN、vNIC、MAC、UUID などのプールから取得したすべての ID がバックアップ ファイルに保持されます。

  （注） このチェックボックスが選択されていない場合、ID は再び割り当てられ、ユーザ ラベルは復旧後に失われます。

- [Location of the Backup File] フィールド：ローカル ファイル システムにバックアップ ファイルを保存するには、[Local File System] オプション ボタンをクリックします。リモート ファイル システムにバックアップ ファイルを保存するには、[Remote File System] オプション ボタンをクリックします。

  場所が [Local File System] に設定されている場合、Cisco UCS Manager GUI によって [Filename] フィールドが表示されます。[Remote File System] に設定されている場合、Cisco UCS Manager GUI によって次に説明する残りのフィールドが表示されます。

- [Filename] フィールド：ローカル ファイル システム内の新しい場所にナビゲートするには、[Browse] をクリックします。
- [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に、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

- [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、Cisco UCS Manager で DNS サーバを使用するように設定する必要があります。
- [Remote File] 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。

ファームウェア アップグレードのための Cisco Smart Call Home の設定

Cisco Smart Call Home は、Cisco UCS の Call Home 機能を強化する Web アプリケーションです。Smart Call Home により、予防的な診断および重要なシステム イベントのリアルタイムの電子メール アラートが提供されます。それにより、ネットワークの可用性が高まり、運用効率が向上しま

す。Smart Call Home は、Cisco UCS の Cisco Unified Computing Support サービスと Cisco Unified Computing Mission Critical Support サービスによって提供されるセキュア接続のサービスです。『*Cisco UCS Manager Administration Management Guide*』には、Smart Call Home の設定に関する詳細情報が掲載されています。

ファームウェア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、電子メール アラートがトリガーされる可能性があります。Smart Call Home を無効にすることで、ファームウェア アップグレード プロセス中にこのようなアラートや TAC への自動サポート ケースを回避できます。

Smart Call Home の無効化

はじめる前に

Smart Call Home がすでに有効になっている必要があります。

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] > [Communication Management] > [Call Home] の順に展開します。

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 [Admin] 領域で次の作業を行い、Smart Call Home を無効にします。

a) [State] フィールドで、[Off] をクリックします。

（注） このフィールドを [On] に設定すると、Cisco UCS Manager GUI のこのタブに残りのフィールドが表示されます。

Call Home アラートは、Smart Call Home を再度有効にするまで生成されません。

ファームウェア アップグレード中のフォールト抑制

フォールト抑制を使用すると、予定されたメンテナンス時間中に SNMP トラップおよび Call Home 通知を抑制することができます。フォールト抑制タスクを作成し、一時的な障害がレイズまたはクリアされるたびに通知が送信されることを防止できます。

障害は、期限切れになるか、フォールト抑制タスクがユーザによって手動で停止されるまで抑制されたままになります。障害抑制が終了すると、Cisco UCS Manager はクリアされなかった未処理の抑制された障害に関する通知を送信します。

ファームウェア アップグレード中のすべてのコンポーネントのフォールト抑制を有効にすると、期限切れになるか、またはアップグレード後にコンポーネントが再稼働状態になるまで、そのコンポーネントに関連するエラーが抑制されます。たとえば、ファブリック インターコネクト障害がファームウェア アップグレード中に抑制されるように設定されている場合、アップグレード中にそのファブリック インターコネクトによってトリガーされたすべての障害は表示されません。

UCS Manager の障害の表示

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	[Faults] をクリックします。
ステップ 4	[Work] ペインで、[All] チェックボックスをオンにします。
ステップ 5	サービスに影響を及ぼす障害が存在しないことを確認してください。

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

ファブリック インターコネクトが再起動するときにダウンするポート設定とサービスは、ファブリック インターコネクトがアップ状態に戻ったときに再確立されるようにすることがきわめて重要です。

Cisco UCS Manager リリース 3.1 以降では、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が 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，（54 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、[Faults] タブをクリックします。
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 フェールオーバー用の vNIC 設定の確認

Cisco UCS システムでは、次のいずれかが発生するとファブリック障害が発生する場合があります。

- ファブリック インターコネクトで障害が発生し、その結果、そのファブリック インターコネクトに接続されているすべてのシャーシでファブリック障害が発生する。
- FEX で障害が発生し、その結果、その FEX に接続されているシャーシでファブリック障害が発生する。
- ファブリック インターコネクトと FEX 間のリンクで障害が発生し、その結果、特定の FEX に接続されているシャーシ内のサーバの一部でファブリック障害が発生する。
- CNA ポートで障害が発生し、その結果、サーバでファブリック障害が発生する。

冗長ハードウェアが設置されており、vNIC がフェールオーバー用に設定されている場合、ファブリック障害によってファブリック フェールオーバーが発生します。ファームウェアをアップグ

レードする前に、vNIC がファブリック フェールオーバー用に設定されていることを確認してください。

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] > [Service_Profile_Name] の順に展開します。

ステップ 3 指定されたサービス プロファイルを展開し、[vNICs] を選択します。

ステップ 4 [vNICs] を展開し、指定されたサービス プロファイルの最初の vNIC 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 [Properties] 領域で、[Fabric ID] が [Fabric A] であり、[Enable Failover] 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。

ステップ 7 [Navigation] ペインで、指定されたサービス プロファイルの次の vNIC を選択します。

ステップ 8 [Work] ペインで、[General] タブをクリックします。

ステップ 9 [Properties] 領域で、[Fabric ID] が [Fabric B] であり、[Enable Failover] 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。

ステップ 10 指定されたサービス プロファイルのすべての vNICs を確認するまで、ステップ 4 ～ 9 を繰り返します。

重要 フェールオーバーが確実に発生するようにするために、代替 vNIC が Fabric A と Fabric B に固定されていることを確認します。

ファブリック インターコネクトの運用性の確認

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 ユニットであるか、従属ユニット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。

デフォルト メンテナンス ポリシーの設定

サービス プロファイルの変更の一部、またはサービス プロファイル テンプレートの更新は、中断をともなうことや、サーバのリブートが必要になることがあります。メンテナンス ポリシーは、サーバに関連付けられたサービス プロファイル、または 1 つ以上のサービス プロファイルに関連付けられた更新中のサービス プロファイルに対して、サーバのリブートが必要になるような変更が加えられた場合の Cisco UCS Manager の対処方法を定義します。

メンテナンス ポリシーは、Cisco UCS Manager でのサービス プロファイルの変更の展開方法を指定します。展開は、次のいずれかの方法で実行されます。

- 即時
- ユーザが管理者権限で承認したときに実行する
- スケジュールで指定された時間に自動的に実行する
- サーバをリブートしたときに実行する

ここで説明する手順を使用することも、このビデオ（http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/configure_the_default_maintenance_policy.html）の [Play] をクリックしてデフォルトのメンテナンス ポリシーを [User Ack] として設定する方法を視聴することもできます。

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 [Maintenance Policies] を展開し、[default] をクリックします。

ステップ 5 [Work] ペインの [Main] タブをクリックします。

ステップ 6 [Properties] 領域で、[Reboot Policy] として [User Ack] を選択します。
[On Next Boot] チェックボックスが表示されます。

サービス プロファイルの関連付けが完了するか、変更が加えられたときは、サーバを手動でリブートする必要があります。

ステップ 7 （任意） [On Next Boot] オプションを有効にするには、[On Next Boot] チェックボックスをオンにします。
[On Next Boot] オプションが有効な場合、ホスト OS のリブート、シャットダウン、リセット、またはサーバ リセットとシャットダウンにより、[User Ack] メンテナンス ウィンドウを待っている変更を適用するために、関連 FSM もトリガーされます。

ステップ 8 [Save Changes] をクリックします。

管理インターフェイスの無効化

ファームウェアをアップグレードする前に、セカンダリ ファブリック インターコネクトの管理インターフェイスをシャットダウンします。これにより、サーバと管理インターフェイス間のアクティブな KVM 接続がすべてリセットされます。GUI フローがプライマリ ファブリック インターコネクトにフェールオーバーされるため、GUI から切断される時間が短縮されます。

Cisco UCS Manager によって管理インターフェイスの障害が検出されると、障害レポートが生成されます。障害レポートの数が設定された数に達した場合、システムは管理インターフェイスが使

用不能であると見なし、障害を生成します。デフォルトでは、管理インターフェイス モニタリング ポリシーは有効です。『*Cisco UCS Manager* システム モニタリング ガイド』には、管理インターフェイス モニタリング ポリシーに関する詳細が掲載されています。

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] > [Communication Management] の順に展開します。

ステップ 3 [Management Interfaces] をクリックします。

ステップ 4 [Work] ペインで、[Management Interfaces] タブをクリックして、ファブリック インターコネクトの管理 IP アドレスを確認します。

ステップ 5 [Management Interfaces Monitoring Policy] タブをクリックし、[Admin Status] フィールドで [Enabled] オプションボタンをクリックして、管理インターフェイスのモニタリングポリシーを有効にします。
Cisco UCS Manager によって管理インターフェイスの障害が検出されると、障害レポートが生成されます。

ステップ 6 ファブリック インターコネクトに接続されているアップストリーム スイッチへの Telnet セッションを開きます。

ステップ 7 ファブリック インターコネクトの管理ポートが接続されているインターフェイスの設定を確認し、スイッチの shut コマンドを使用して無効にします。
このインターフェイスを通じて開いているすべての KVM セッションが終了します。

ステップ 8 KVM セッションを再接続して、これらのセッションがセカンダリ ファブリック インターコネクトのアップグレードの影響を受けないようにします。

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

フィールド名	必要な値
[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 [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 3 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 4 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。

データ パスの準備が整っていることの確認

以下の項では、データ パスの準備ができていることを確認する手順を説明します。

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とき、すべてのダイナミック vNIC が新しいプライマリ ファブリック インターコネクトで動作中であることを確認する必要があります。データ パスの中断を避けるため、以前のプライマリ ファブリック インターコネクト上で新しいソフトウェアを有効にする前に、vNIC が動作中であることを確認します。

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 [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。
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 –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 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 3 章

Cisco UCS Manager によるファームウェアの管理

Cisco UCS Manager でのファームウェアのダウンロードと管理

ファームウェア イメージの管理

シスコでは、Cisco UCS コンポーネントに対するすべてのファームウェアのアップデートをイメージのバンドルで配布します。各イメージは、1 つのハードウェア コンポーネントに固有のファームウェア パッケージを表します。たとえば、IOM イメージや Cisco UCS Manager イメージなどです。Cisco UCS ファームウェアのアップデートは、Cisco UCS ドメイン のファブリック インターコネクトに次のバンドルで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

Cisco UCS Manager リリース 3.1 以降のリリースには、3 つの独立したインフラストラクチャ バンドルが含まれています。

これらのバンドルには、次のコンポーネントをアップデートするために必要となるファームウェア イメージなどがあります。

- 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

（注） あるプラットフォーム用の UCS インフラストラクチャ バンドルは、別のプラットフォームをアクティブ化するために使用できません。たとえば、Cisco UCS 6200 シリーズのファブリック インターコネクトのインフラストラクチャ バンドルを使用して Cisco UCS 6300 シリーズのファブリック インターコネクトをアクティブ化することはできません。

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 は、使用できるすべてのイメージのインベントリを維持します。イメージ カタログには、イメージとパッケージのリストが含まれます。パッケージは、ダウンロードされたときに作成される読み取り専用オブジェクトです。これはディスク領域を占有せず、パッケージのダウンロードの一部として展開されたイメージのリストまたはコレクションを表します。個々のイメージがダウンロードされるときに、パッケージ名はイメージ名と同じままです。

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。パッケージ内のすべてのイメージを削除した後、Cisco UCS Manager はパッケージ自体を削除します。

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。ブートフラッシュ パーティションが 70 % を超え、合計使用スペースが 90 % を超えると、エラーが発生します。Cisco UCS Manager がこのような障害を生成した場合、領域を解放するために古いイメージを削除します。

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には、次のどのソフトウェア バンドルが必要かを判断します。

- Cisco UCS 6300 シリーズ、6200 シリーズ、および 6324 ファブリック インターコネクト用の 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 6300 シリーズ、6200 シリーズ、および 6324 ファブリック インターコネクト用の Cisco UCS インフラストラクチャ ソフトウェア バンドル	[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	[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	[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) 最新リリースの 3.2 ソフトウェア バンドル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

（注） クラスタ セットアップでは、ダウンロードの開始に使用されたファブリック インターコネクトに関係なく、ファームウェア バンドルのイメージ ファイルは両方のファブリック インターコネクトにダウンロードされます。Cisco UCS Manager は、両方のファブリック インターコネクトにあるすべてのファームウェア パッケージとイメージを同期状態にします。ファブリック インターコネクトの 1 つがダウンした場合でも、ダウンロードは正常に終了します。オンラインに復帰したときに、イメージがもう片方のファブリック インターコネクトに同期されます。

はじめる前に

必要なファームウェア バンドルをシスコから入手します。

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] 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、次のフィールドに入力します。

名前	説明
[Protocol] フィールド	リモート サーバとの通信時に使用するプロトコル。次のいずれかになります。 • FTP • TFTP （注） TFTP ファイルのサイズ制限は 32 MB です。ファームウェア バンドルはそれよりサイズが大きい可能性があるため、ファームウェアのダウンロードに TFTP を選択しないことをお勧めします。 • 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。 • [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。 （注） USB A および USB B は、Cisco UCS 6324（UCS Mini）および Cisco UCS 6300 シリーズ ファブリック インターコネクトにのみ適用されます。 Cisco UCS 6300 シリーズ ファブリック インターコネクトでは、2 個のポートのうちの最初のポートのみ検出されます。
[Server] フィールド	ファイルがリモート サーバのファイルである場合は、ファイルが存在するリモート サーバの IP アドレスまたはホスト名。ファイルがローカル ソースのファイルである場合、このフィールドには「local」が表示されます。 （注） IPv4 や IPv6 アドレスではなくホスト名を使用する場合、DNS サーバを設定する必要があります。Cisco UCS ドメイン が Cisco UCS Central に登録されていない、または DNS 管理がローカルに設定されている場合は、Cisco UCS Manager で DNS サーバを設定します。Cisco UCS ドメイン が Cisco UCS Central に登録されており、DNS 管理がグローバルに設定されている場合は、Cisco UCS Central で DNS サーバを設定します。
[Filename] フィールド	ファームウェア ファイルの名前。

名前	説明
[Path] フィールド	リモート サーバ上のファイルへの絶対パス。 SCP を使用する場合、絶対パスは常に必要です。他のプロトコルを使用する場合は、ファイルがデフォルトのダウンロードフォルダにあれば、リモートパスを指定する必要はありません。ファイルサーバの設定方法の詳細については、システム管理者に問い合わせてください。
[User] フィールド	システムがリモートサーバへのログインに使用する必要のあるユーザ名。プロトコルが TFTP の場合、このフィールドは適用されません。
[Password] フィールド	リモート サーバのユーザ名のパスワード。プロトコルが TFTP の場合、このフィールドは適用されません。

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 から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、領域を空けます。ブートフラッシュの空き領域を表示するには、そのファブリック インターコネクトに移動し、[Equipment] をクリックし、[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

ファームウェアバンドルのイメージファイルが完全にダウンロードされたら、エンドポイント上でファームウェアを更新します。

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

（注） クラスタ セットアップでは、ダウンロードの開始に使用されたファブリック インターコネクトに関係なく、ファームウェア バンドルのイメージ ファイルは両方のファブリック インターコネクトにダウンロードされます。Cisco UCS Manager は、両方のファブリック インターコネクトにあるすべてのファームウェア パッケージとイメージを同期状態にします。ファブリック インターコネクトの 1 つがダウンした場合でも、ダウンロードは正常に終了します。オンラインに復帰したときに、イメージがもう片方のファブリック インターコネクトに同期されます。

はじめる前に

必要なファームウェア バンドルをシスコから入手します。

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] 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、イメージ ファイルのフル パスと名前を入力します。
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。

（注） Cisco UCS Mini の HTML5 GUI でファームウェア イメージ ファイルを検索するには、[Choose File] をクリックします。

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

ファームウェアバンドルのイメージファイルが完全にダウンロードされたら、エンドポイント上でファームウェアを更新します。

イメージ ダウンロードのキャンセル

イメージのダウンロード タスクは、タスクの進行中にのみキャンセルできます。イメージのダウンロードの完了後に、ダウンロード タスクを削除しても、ダウンロード済みのイメージは削除されません。イメージ ダウンロード タスクに関係する FSM はキャンセルできません。

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] 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ら、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、およびテクニカル サポート ファイルを削除してください。

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。

- インストール インフラストラクチャ ファームウェア：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。ファームウェア イメージの管理，（65 ページ）では、Cisco UCS Manager リリース 3.2 で使用可能なインフラストラクチャ ソフトウェア バンドルについて詳しく説明します。自動インストールによる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推奨プロセス，（78 ページ）では、インフラストラクチャ ファームウェアを自動的にインストールするための推奨されるプロセスについて詳しく説明します。
- インストール サーバ 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 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したり、また 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アップグレードし、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事項とガイドライン，（42 ページ）を参照してください。

Cisco UCS Manager リリース 3.1(1l)、3.1(2b)、3.1(2c)、および 3.1(2e) で、[Redundancy] を [Grid] に設定し、[Power Capping] を [No Cap] に設定して電源ポリシーを設定している場合、自動インストール を使用した Cisco UCS Manager ソフトウェアのアクティブ化は失敗します。Cisco UCS Manager リリース 3.1(2b) より前、および 3.1(2e) より後の Cisco UCS Manager リリースでは、自動インストール を使用した Cisco UCS Manager ソフトウェアのアクティブ化は構成された電源ポリシーに基づく失敗がなくなりました。

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。デフォルトのインフラストラクチャ パックおよびサービス パックのスタートアップ バージョンのクリア，（85 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。

自動内部バックアップ

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中に、完全な状態のバックアップ ファイルが自動的に作成されます。Cisco UCS Managerリリース 2.2(4) では、FSM ステータスで表示される 2 つの新しいバックアップ段階が追加されました。これらを次に示します。

1. **InternalBackup**：設定をバックアップします。
2. **PollInternalBackup**：バックアップの完了を待ちます。

バックアップが正常に完了すると、「bkp.*timestamp*.tgz」という名前のバックアップ ファイルが、両方のファブリック インターコネクトの `/workspace/backup` ディレクトリに保存されます。ここには、最新のバックアップ ファイルのみが保存されます。

バックアップが失敗した場合は、「**internal backup failed**」というマイナーエラーがログに記録されます。このエラーは、Cisco UCS Managerリリース 2.2(4) より前のリリースにダウングレードした場合は記録されません。

このバックアップ ファイルからファブリック インターコネクトの設定を復元する前に、local-mgmt から copy コマンドを使用して、バックアップ ファイルをファブリック インターコネクトからファイル サーバにコピーします。

次に、自動内部バックアップ ファイルをファイル サーバにコピーする方法の例を示します。

```
UCS-A# connect local-mgmt
UCS-A (local-mgmt) # copy workspace:/backup/bkp.1429690478.tgz
scp://builds@10.190.120.2://home/builds/
```

インストール インフラストラクチャ ファームウェア

インストール インフラストラクチャ ファームウェア では、Cisco UCS Manager を含む 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。

インストール インフラストラクチャ ファームウェア 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。

インストール サーバ ファームウェア

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

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ファームウェアのアップグレードの推奨プロセス

シスコでは、自動インストールによる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について、次のプロセスを推奨します。

1. ソフトウェアをステージングし、アップグレードを準備します。
   a. すべてのコンフィギュレーション ファイルと完全な状態のバックアップ ファイルを作成します。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, （49 ページ）と完全な状態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, （51 ページ）には、詳細情報が掲載されています。
   b. ファームウェア パッケージを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, （70 ページ）とローカル 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, （73 ページ）には、詳細情報が掲載されています。
   c. Smart Call Home を無効にします。Smart Call Home の無効化, （53 ページ）には、Smart Call Home の無効化に関する詳細情報が掲載されています。
2. ファブリック アップグレードを準備します。

a Cisco UCS Manager の障害を確認し、サービスに影響を及ぼす障害を解決します。UCS Manager の障害の表示, （54 ページ）には、障害の確認に関する詳細が掲載されています。

b 高可用性ステータスを確認し、セカンダリ ファブリック インターコネクトを特定します。クラスタ設定の高可用性ステータスとロールの確認, （57 ページ）には、詳細情報が掲載されています。

c デフォルトのメンテナンス ポリシーを設定します。デフォルト メンテナンス ポリシーの設定, （57 ページ）には、詳細情報が掲載されています。また、このビデオ（http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/configure_the_default_maintenance_policy.html）の [Play] をクリックして、デフォルトのメンテナンス ポリシーを [User Ack] として設定する方法を視聴することもできます。

d VLAN と FCOE ID が重複していないことを確認します。

e 管理インターフェイスを無効にします。管理インターフェイスの無効化, （58 ページ）には、セカンダリ ファブリック インターコネクトの管理インターフェイスの無効化に関する詳細情報が掲載されています。

f すべてのパスが動作していることを確認します。データ パスの準備が整っていることの確認, （61 ページ）には、詳細情報が掲載されています。

3 自動インストールによって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。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, （80 ページ）には、詳細情報が掲載されています。また、このビデオ（http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/upgrade_the_infrastructure_firmware_with_auto_install.html）の [Play] をクリックして、自動インストールで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方法を視聴することもできます。

4 クラスタの高可用性ステータスを確認します。

5 すべてのパスが動作していることを確認します。

6 新しい障害を確認します。 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, （55 ページ） には、詳細情報が掲載されています。

7 プライマリ ファブリックのアクティブ化を確認します。プライマリ ファブリック インター コネクトのリブートの確認, （83 ページ）には、詳細情報が掲載されています。また、このビデオ（http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/acknowledge_pending_reboot_of_the_primary_fabric_interconnect.html）の [Play] をクリックして、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方法を視聴することもできます。

8 新しい障害を確認します。

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 Manager 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事項とガイドライン，（42 ページ）および該当する『Cisco UCS upgrade guide』を参照してください。

Cisco UCS Manager リリース 3.1(3) から、自動インストール を使用して Cisco UCS Manager および両方のファブリック インターコネクトにサービスパックをインストールできます。基本のインフラストラクチャ パックにサービス パックを適用することはできますが、個別にサービス パックをインストールすることはできません。

インフラストラクチャ パックをアップグレードせずに、互換性のあるサービス パックを 自動インストール経由でインストールできます。これにより、両方のファブリック インターコネクトでサービスパックのインストールがトリガーされます。特定のサービスパックをインストールするには、ファブリック インターコネクトを再ロードする必要があります。

サービス パックを使用するインフラストラクチャ ファームウェアの 自動インストール は、すべてのインフラストラクチャ コンポーネントが Cisco UCS Manager リリース 3.1(3) 以降のリリースである場合にのみサポートされます。

ここで説明する手順を使用することも、このビデオ（http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/upgrade_the_infrastructure_firmware_with_auto_install.html）の [Play] をクリックして、自動インストールによって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方法を視聴することもできます。

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，（47 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] 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、[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）、\（バックスラッシュ）、^（キャラット）、"（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。
[Infra Pack] 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。

名前	説明
[Service Pack] 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のアップグレードに使用できるサービス パック バンドルのリスト。 基本のインフラ パックを選択せずに直接サービス パックにアップグレードすることはできません。 （注） サービス パックは基本のメンテナンス リリースにのみ適用できます。たとえば、サービスパック 3.1(3)SP2 は 3.1(3) リリースにのみ適用できます。3.1(4) リリースに適用することはできません。 [Service Pack] を [<not set>] に設定すると、サービス パックがファームウェア パッケージから削除されます。
[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。
[Evacuate] チェックボックス	オンにすると、自動インストールによってアップグレードされている各ファブリック インターコネクト上でファブリック エバキュエーションが有効になります。両方のファブリック インターコネクトが待避させられますが、同時ではありません。 デフォルトでは、このチェックボックスはオフになっており、ファブリック エバキュエーションは無効になっています。

ステップ 8 [Install Infrastructure Firmware] ダイアログボックスの [Infrastructure Upgrade 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。

特定のサービスパックをインストールするには、ファブリックインターコネクトを再ロードする必要があります。このようなシナリオでは、サービス パックのインストールを完了させるためにプライマリ ファブリック インターコネクトの再起動を確認する必要があります。

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

ここで説明する手順を使用することも、このビデオ（http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/acknowledge_pending_reboot_of_the_primary_fabric_interconnect.html）の [Play] をクリックしてプライマリ ファブリック インターコネクトのリブートを確認する方法を視聴することもできます。

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承認する前に、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, （61 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、インストール インフラストラクチャ ファームウェア 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、インストール インフラストラクチャ ファームウェア 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 [Fabric Interconnects] サブタブをクリックし、[Reboot now] をクリックします。

ステップ 4 表示される**警告**ダイアログボックスで [Yes] をクリックします。
警告ダイアログ ボックスには、最後のリブート後に未確認の障害があることが示され、続行するかどうかを尋ねられます。

ステップ 5 表示される [Reboot now] ダイアログボックスで [Yes] をクリックし、ファブリック インターコネクトをリブートして、保留中の変更を適用します。
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。[Yes] 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] 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、[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。

デフォルトのインフラストラクチャ パックおよびサービス 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、デフォルトのインフラストラクチャ パックおよびサービス 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

（注） ドメイン内の Cisco UCS Manager が Cisco UCS Manager 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事項とガイドライン，（42 ページ）および該当する『Cisco UCS upgrade guide』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，（47 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] 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、[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) サーバをサービス パックのファームウェア バージョンにアップグレードするには、[Service-Pack Firmware] 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サービス パックを選択します。

d) [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 Dependencies] 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。

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。

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。

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
- BIOS
- CIMC

（注） ラック マウント サーバでは、ホスト ファームウェア パックから CIMC を除外し、ボード コントローラをアップグレードまたはダウングレードすると、アップグレードまたはダウングレードが失敗する可能性があります。これは、CIMC ファームウェアのバージョンとボード コントローラ ファームウェアのバージョンに互換性がない可能性があるためです。

- ボード コントローラ
- Flex Flash コントローラ
- GPU
- FC アダプタ
- HBA Option 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。

Cisco UCS Manager リリース 3.1(1) で、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。Cisco UCS Manager リリース 3.1(2) から、ローカル ディスクおよびその他の共通エンドポイント用のファームウェアは、ブレード パッケージとラック パッケージの両方で入手できます。

- PSU
- SAS エクスパンダ
- ストレージ 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

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 BIOS 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 BIOS ファームウェアを除外できます。

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。

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即座に適用されます。これによりサーバのリブートが発生する可能性があります。

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アソシエーション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 はファームウェアのアップグレードを無視し、アソシエーションを終了します。

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、メンテナンス期間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。	[On Next Boot] オプションで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** リブートして新しいファームウェアを適用するには、次のいずれかの手順を実行します。 • 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。 • 手動でサーバをリブートします。 **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すると、Cisco UCS によってファームウェア パッケージが適用されます。これは、[On Next Boot] オプションによって有効になります。

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

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します。

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 Package]、[Rack Package]、および [Service Pack] の各ドロップダウン リストから、ファームウェア パッケージを選択します。
[Service Pack] からのイメージは、[Blade Package] または [Rack Package] のイメージよりも優先されます。

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。

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。
モデルとモデル番号（PID）は、このファームウェア パッケージに関連付けられているサーバに一致する必要があります。誤ったモデルまたはモデル番号を選択すると、Cisco UCS Manager はファームウェア更新ファイルをインストールできません。

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

ポリシーはサービス プロファイルとテンプレートのうち一方、または両方にインクルードします。

ホスト ファームウェア パッケージのアップデート

ポリシーが 1 つ以上のサービス プロファイルに含まれており、それらのサービス プロファイルにメンテナンス ポリシーが含まれていない場合、Cisco UCS Manager によってサーバとアダプタのファームウェアが新しいバージョンで更新され、アクティブ化されます。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ない場合、ホスト ファームウェア パッケージ ポリシーを保存するとすぐに Cisco UCS Manager によってサーバが再起動されます。

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

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します。

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。
モデルとモデル番号（PID）は、このファームウェア パッケージに関連付けられているサーバに一致する必要があります。誤ったモデルまたはモデル番号を選択すると、Cisco UCS Manager はファームウェア更新ファイルをインストールできません。

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 ブレード パッケージを変更するには、[Blade Package] ドロップダウン リストから、ブレード パッケージのバージョンを選択します。

ステップ 9 ラック パッケージを変更するには、[Rack Package] ドロップダウン リストから、ラック パッケージのバージョンを選択します。

ステップ 10 サービス パックを変更するには、[Service Pack] ドロップダウン リストから、サービス パックのバージョンを選択します。
サービス パックを削除するには、[<not set>] を選択します。

ステップ 11 [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。

ステップ 12 [OK] をクリックします。
Cisco UCS Manager はモデル番号とベンダーを、このポリシーがインクルードされているサービス プロファイルに関連付けられているすべてのサーバと照合します。モデル番号とベンダーがポリシー内のファームウェア バージョンに一致する場合、Cisco UCS Manager により、サービス プロファイルに含まれているメンテナンス ポリシー内の設定に従ってファームウェアが更新されます。

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

サービスプロファイルにメンテナンスポリシーが含まれておらず、サーバに関連付けられている場合、Cisco UCS Manager はサーバのファームウェアを新しいバージョンに更新してからアクティブにし、サービス プロファイルに対する変更が保存されるとただちにサーバをリブートします。

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 [Save Changes] をクリックします。

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かどうかを指定できます。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。

- [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。

  この値は、デフォルトで選択されます。

- [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。

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 [User Ack] に設定し、後から [No Action] 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] 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 [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。

- [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。
- [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。

  このオプションは、デフォルトで選択されます。

ステップ 6 [Save Changes] をクリックします。

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。エンドポイントでのインフラストラクチャ ファームウェアの直接アップグレードの推奨プロセス，（108ページ）では、エンドポイントで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推奨プロセスについて詳しく説明されています。

次のコンポーネントのファームウェアを直接アップグレードできます。

インフラストラクチャ	UCS 5108 シャーシ	UCS ラックサーバ	Cisco UCS S3260 シャーシ
• ファブリック インターコネクト • Cisco UCS Manager	• I/O モジュール • 電源装置 • サーバ： ◦ アダプタ ◦ CIMC ◦ BIOS ◦ ストレージ コントローラ ◦ ボード コントローラ	• アダプタ • CIMC • BIOS • ストレージ コントローラ • ボード コントローラ	• CMC • シャーシ アダプタ • SAS エクスパンダ • シャーシ ボード コントローラ • サーバ： ◦ CIMC ◦ BIOS ◦ ボード コントローラ ◦ ストレージ コントローラ

Cisco UCS S3260 シャーシの場合、シャーシ プロファイル内のシャーシ ファームウェア パッケージを通じて、CMC、シャーシ アダプタ、シャーシ ボード コントローラ、SAS エクスパンダ、およびローカル ディスクのファームウェアをアップグレードできます。『*Cisco UCS S3260 Server Integration with Cisco UCS Manager, Release 3.2*』には、シャーシ プロファイルとシャーシ ファームウェア パッケージに関する詳細情報が記載されています。

アダプタ、ボード コントローラ、CIMC、および BIOS ファームウェアは、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。

重要 すべてのサーバ コンポーネントは、同じリリース レベルで維持する必要があります。これらのコンポーネントはリリースごとに同時にテストされているので、互いのバージョンが一致していないと、予期しないシステム動作が発生する可能性があります。

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、UCS 5108 シャーシの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

Cisco UCS S3260 高密度ストレージ ラック サーバ シャーシでは、アップデートの段階は以下のエンドポイントのみに適用されます。

- シャーシ管理コントローラ（CMC）
- 共有アダプタ
- SAS エクスパンダ
- サーバ：
  - BIOS
  - CIMC
  - アダプタ

⚠

注意 更新が完了するまで、エンドポイントがあるハードウェアを取り外したり、メンテナンス作業を実行しないでください。ハードウェアが取り外されたり、その他のメンテナンス作業により使用できない場合、ファームウェアの更新は失敗します。この失敗により、バックアップ パーティションが破損する場合があります。バックアップ パーティションが破損しているエンドポイントではファームウェアを更新できません。

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
- Cisco UCS S3260 高密度ストレージ ラック サーバ シャーシ：
  - CMC
  - 共有アダプタ
  - シャーシとサーバのボード コントローラ
  - SAS エクスパンダ
  - ストレージ コントローラ
  - BIOS
  - CIMC

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。

M シリーズ シャーシとサーバエンドポイントの直接のファームウェア アップグレードによる停止の影響

重要 Cisco UCS Manager リリース 3.1(2) 以降では、Cisco UCS M シリーズ サーバはサポートされていません。

CMC ファームウェア アップグレードによる停止の影響

シャーシの CMC のファームウェアをアップグレードする際、停止は発生しません。

共有アダプタ ファームウェア アップグレードによる停止の影響

共有アダプタのファームウェアをアクティブ化する際、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。
- ストレージ コントローラがリブートします。

ストレージ コントローラのファームウェア アップグレードによる停止の影響

ストレージ コントローラのファームウェアをアクティブ化する際、次の停止の影響と中断が発生します。

- ローカル ブート ポリシーが設定されているサーバがリブートします。iSCSI ブート ポリシーが設定されているサーバがリブートしません。
- サーバ トラフィックが中断します。
- ストレージ コントローラがリブートします。

ボード コントローラのファームウェア アップグレードによる停止の影響

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際、次の停止の影響と中断が発生します。

- 共有アダプタがリブートします。
- カートリッジと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。
- ストレージ コントローラがリブートします。

BIOS ファームウェア アップグレードによる停止の影響

BIOS へのファームウェア アップグレードにより、サーバがリブートします。

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。

サーバでのボード コントローラ ファームウェア アップグレードによる停止の影響

サーバ上でボード コントローラのファームウェアをアクティブ化する場合、アップグレード中にサーバの電源がオフになり、アップグレードの完了後に電源がオンになります。

ストレージ コントローラ、ボード コントローラ、および共有アダプタのファームウェアのアクティブ化中は、サーバの電源をオフにすることを推奨します。アクティブ化中にサーバの電源をオフにしない場合、Cisco UCSM はサーバの電源をオフにし、最大 16 分待機しようとします。この間にサーバの電源がまだオフになっていないことを Cisco UCSM が検出すると、FSM は失敗し、Cisco UCSM が電源をオフにしたサーバの電源をオンにしません。FSM は 8 分後に起動しようとします。

UCSM が正常にサーバの電源をオフにすると、アクティブ化の完了後に、必要な電源状態に基づいて関連するサーバの電源をオンにします。

エンドポイントでのインフラストラクチャファームウェアの直接アップグレードの推奨プロセス

シスコでは、エンドポイントでのインフラストラクチャ ファームウェアの直接アップグレードについて、次のプロセスを推奨します。

1. ソフトウェアをステージングし、アップグレードを準備します。
   - **a** すべてのコンフィギュレーション ファイルと完全な状態のバックアップ ファイルを作成します。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, （49 ページ）と完全な状態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, （51 ページ）には、詳細情報が掲載されています。
   - **b** ファームウェア パッケージを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, （70 ページ）とローカル 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, （73 ページ）には、詳細情報が掲載されています。
   - **c** Smart Call Home を無効にします。Smart Call Home の無効化, （53 ページ）には、詳細情報が掲載されています。
2. Cisco UCS Manager ソフトウェアをアクティブにします。Cisco UCS Manager ソフトウェアのアクティブ化, （112 ページ）には、詳細情報が掲載されています。また、このビデオ（http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/activate_ucsm.html）の [Play] をクリックして、Cisco UCS Manager ソフトウェアをアクティブ化する方法を視聴することもできます。
3. IOM ファームウェアを更新します。IOM のファームウェアのアップデート, （115 ページ）には、詳細情報が掲載されています。また、このビデオ（http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/update_and_activate_iom.html）の [Play] をクリックして、IOM ファームウェアを更新する方法を視聴することもできます。
4. ファブリック アップグレードを準備します。
   - **a** UCS Manager の障害を確認し、サービスに影響を及ぼす障害を解決します。UCS Manager の障害の表示, （54 ページ）には、詳細情報が掲載されています。
   - **b** 高可用性ステータスを確認し、セカンダリ ファブリック インターコネクトを特定します。クラスタ設定の高可用性ステータスとロールの確認, （57 ページ）には、詳細情報が掲載されています。
   - **c** デフォルトのメンテナンス ポリシーを設定します。デフォルト メンテナンス ポリシーの設定, （57 ページ）には、詳細情報が掲載されています。また、このビデオ（http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/configure_the_default_maintenance_policy.html）の [Play] をクリックして、デフォルトのメンテナンス ポリシーを [User Ack] として設定する方法を視聴することもできます。

d VLAN と FCOE ID が重複していないことを確認します。

e 管理インターフェイスを無効にします。管理インターフェイスの無効化, （58 ページ）には、詳細情報が掲載されています。

f IOM ファームウェアをアクティブにします。IOM でのファームウェアのアクティブ化, （117 ページ）には、詳細情報が掲載されています。また、このビデオ（http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/update_and_activate_iom.html）の [Play] をクリックして、IOM ファームウェアをアクティブ化する方法を視聴することもできます。

5 従属ファブリック インターコネクトをアクティブにします。

a 従属ファブリック インターコネクトのトラフィックを待避させます。ファブリック インターコネクト トラフィックの待避の設定, （37 ページ）には、詳細情報が掲載されています。また、このビデオ（http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/enable_and_disable_fi_traffic_evacuation.html）の [Play] をクリックして、ファブリック インターコネクト トラフィックを待避させる方法を視聴することもできます。

b 従属ファブリック インターコネクト（FI-B）をアクティブにし、FSM をモニタします。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, （118 ページ）には、詳細情報が掲載されています。また、このビデオ（http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/activate_the_firmware_on_a_subordinate_fabric_interconnect.html）の [Play] をクリックして、従属ファブリック インターコネクトでファームウェアをアクティブ化する方法を視聴することもできます。

c すべてのパスが動作していることを確認します。データ パスの準備が整っていることの確認, （61 ページ）には、詳細情報が掲載されています。

d 従属ファブリック インターコネクトのトラフィック待避を無効にします。ファブリック インターコネクト トラフィックの待避の設定, （37 ページ）には、詳細情報が掲載されています。また、このビデオ（http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/enable_and_disable_fi_traffic_evacuation.html）の [Play] をクリックして、ファブリック インターコネクトのトラフィック待避を無効にする方法を視聴することもできます。

e 新しい障害を確認します。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, （55 ページ）

6 プライマリ ファブリック インターコネクト（FI-A）をアクティブにします。

a 管理サービスをプライマリ ファブリック インターコネクトからセカンダリ ファブリック インターコネクトに移行し、クラスタ リードをセカンダリ ファブリック インターコネクトに変更します。ファブリック インターコネクト クラスタ リードのスイッチオーバー, （122 ページ）には、詳細情報が掲載されています。また、このビデオ（http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/switch_over_fabric_interconnect_cluster_lead.html）の [Play] をクリックして、あるファブリック インターコネクトから別のファブリック インターコネクトにクラスタ リードをスイッチオーバーする方法を視聴することもできます。

b プライマリ ファブリック インターコネクトのトラフィックを待避させます。

c プライマリ ファブリック インターコネクト（FI-A）をアクティブにし、FSM をモニタします。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, （119 ページ）には、詳細情報が掲載されています。また、このビデオ（http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/activate_the_firmware_on_a_primary_fabric_interconnect.html）の [Play] をクリックして、プライマリ ファブリック インターコネクトでファームウェアをアクティブ化する方法を視聴することもできます。

d すべてのパスが動作していることを確認します。

e プライマリ ファブリック インターコネクトのトラフィック待避を無効にします。

f 新しい障害を確認します。

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、シャーシおよびサーバのエンドポイント上のファームウェアを更新する場合に使用できます。関連するホストのファームウェア パックの一部であるサーバエンドポイントは、この手順を使用して更新することはできず、エラーが表示されます。この手順を使用してこれらのサーバコンポーネントを更新するには、割り当てられたホストのファームウェア パックからそれらを除外してください。

注意 更新が完了するまで、エンドポイントがあるハードウェアを取り外したり、メンテナンス作業を実行しないでください。ハードウェアが取り外されたり、その他のメンテナンス作業により使用できない場合、ファームウェアの更新は失敗します。この失敗により、バックアップ パーティションが破損する場合があります。バックアップ パーティションが破損しているエンドポイントではファームウェアを更新できません。

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] 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、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 は、直接更新できるサーバ上の他のすべてのエンドポイントのファームウェアを更新します。

Cisco UCS Managerr 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、アクティブにするまで、バックアップ バージョンとして残されます。Cisco UCS Manager はすべてのアップデートを同時に開始します。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 がアップデート 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

ファームウェアをアクティブにします。

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。これらのエラーを解決し、[Force] オプションを使用してアップグレードを続行する必要があります。

たとえば、M1 および M2 ブレード サーバがリリース 3.1(1) でサポートされていない場合、リリース 2.2(x) からリリース 3.1(1) にアップグレードするときに M1 または M2 ブレード サーバが構成に存在すると、それらは検証エラーとして [Upgrade Validation] タブに報告され、アップグレードが失敗します。

Cisco UCS Manager でアップグレードまたはダウングレード プロセスを検証しない場合は、[Skip Validation] チェックボックスをオンにします。

Cisco UCS Manager ソフトウェアのアクティブ化

ここで説明する手順を使用することも、このビデオ（http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/activate_ucsm.html）の [Play] をクリックして Cisco UCS Manager ソフトウェアをアクティブ化する方法を視聴することもできます。

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] 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 はアクティブなすべてのセッションを切断し、すべてのユーザをログアウトさせ、ソフトウェアをアクティブにします。アップグレードが完了すると、再度ログインするよう求められます。切断された後すぐに再度ログインするよう求められた場合、ログインは失敗します。Cisco UCS Manager のアクティベーションが完了するまで数分待つ必要があります。

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。

Cisco UCS Manager ソフトウェアのサービス パックのアクティブ化

ここで説明する手順を使用して、Cisco UCS Manager ソフトウェアのサービス パックをアクティブ化することができます。このプロセスでは、ファブリック インターコネクトのアップグレードまたは再起動は必要ありません。

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] 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、[UCS Manager] を選択します。

ステップ 6 [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) [UCS Manager Service Pack] 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サービス パックのバージョンを選択します。

b) [OK] をクリックします。

Cisco UCS Manager はアクティブなすべてのセッションを切断し、すべてのユーザをログアウトさせ、ソフトウェアをアクティブにします。アップグレードが完了すると、再度ログインするよう求められます。切断された後すぐに再度ログインするよう求められた場合、ログインは失敗します。Cisco UCS Manager のアクティベーションが完了するまで数分待つ必要があります。

Cisco UCS Manager ソフトウェアからのサービス パックの削除

ここで説明する手順を使用して、Cisco UCS Manager ソフトウェアからサービス パックを削除することができます。

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] 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、[UCS Manager] を選択します。

ステップ 6 [Activate Firmware] ダイアログボックスの [UCS Manager Service Pack] の行で、[Startup Version] カラム のドロップダウンリストからサービス パックのバージョンとして [<not set>] を選択します。

ステップ 7 [OK] をクリックします。

IOM ファームウェア

Cisco UCS I/O モジュール（IOM）は、ブレード サーバ エンクロージャにユニファイド ファブリック テクノロジーを組み込みます。これにより、ブレード サーバとファブリック インターコネクト間の複数の 10 ギガビット イーサネット接続を提供し、診断、配線、管理を簡素化します。IOM により、ファブリック インターコネクトとブレード サーバ シャーシ間での I/O ファブリックが拡張され、すべてのブレードおよびシャーシを 1 つに接続する、損失のない確実な Fibre Channel over Ethernet（FCoE）ファブリックを使用できます。

IOM は分散ライン カードと同様であるため、スイッチングを実行せず、ファブリック インターコネクトの拡張として管理されます。このようなアプローチを取ることで、ブレード シャーシから各種スイッチが取り払われ、システム全体構造の複雑さが低減します。また、Cisco UCS の規模を拡大してシャーシの数を増やしても、必要なスイッチの数が増えることはありません。これにより、すべてのシャーシを可用性の高い 1 つの管理ドメインとして扱うことが可能になります。

IMO では、ファブリック インターコネクトと併せてシャーシ環境（電源、ファン、ブレードを含む）も管理できます。したがって、個別のシャーシ管理モジュールは必要ありません。IMO は、ブレード サーバ シャーシの背面に設置します。各ブレード シャーシは最大 2 つの IOM をサポートできるため、容量と冗長性を向上させることができます。

IOM ファームウェアの更新およびアクティブ化に関するガイドライン

IOM でファームウェアを更新および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。

- 各 IOM は、実行中のイメージとバックアップ イメージの 2 つのイメージを格納します。

- 更新操作では、IOM のバックアップ イメージが新しいファームウェア バージョンに置き換えられます。
- アクティブ化操作では、現在の起動イメージがバックアップイメージに降格します。新しい起動イメージが代わりに配置され、このバックアップイメージから起動するようにシステムが設定されます。
- アクティブなイメージのみを設定するには、[Set Startup Version Only] チェックボックスをオンにします。リセットは実行されません。このプロセスを使用すると、複数の IOM をアップグレードし、同時にリセットできます。ファブリック インターコネクトが更新およびアクティブ化されると、ファブリック インターコネクトは対応する IOM をリブートし、ダウンタイムを低減します。
- IOM とファブリック インターコネクトは、互いに互換性がある必要があります。
- ファブリック インターコネクトで実行されるソフトウェアが互換性のないバージョンを実行する IOM を検出した場合、ファブリック インターコネクトのシステム ソフトウェアと同じバージョンにするために IOM の自動更新を実行します。
  Cisco UCS Manager はこの状況を通知するために障害を生成します。また、自動更新の進行中、IOM の検出状態は [Auto updating] を示します。
- Cisco UCS Manager では、[Installed Firmware] タブで IOM ファームウェアをシャーシ レベルで確認できます。

次の項で詳しく説明する手順を使用するか、またはこのビデオ（http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/update_and_activate_iom.html）の [Play] をクリックして、IOM ファームウェアを更新およびアクティブ化する方法を視聴できます。

IOM のファームウェアのアップデート

注意 更新が完了するまで、エンドポイントがあるハードウェアを取り外したり、メンテナンス作業を実行しないでください。ハードウェアが取り外されたり、その他のメンテナンス作業により使用できない場合、ファームウェアの更新は失敗します。この失敗により、バックアップパーティションが破損する場合があります。バックアップ パーティションが破損しているエンドポイントではファームウェアを更新できません。

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] > [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

ファームウェアをアクティブにします。

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 [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] を選択しないでください。選択すると、すべてのエンドポイントが同時にアクティブになります。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。

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-reboot 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。

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

ここで説明する手順を使用することも、このビデオ（http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/activate_the_firmware_on_a_subordinate_fabric_interconnect.html）の [Play] をクリックして従属ファブリック インターコネクトのファームウェアをアクティブ化する方法を視聴することもできます。

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] 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。
Cisco UCS Manager はファームウェアの更新とアクティベーションを実行し、ファブリック インターコネクトと、そのファブリック インターコネクトへのデータ パスにあるすべての I/O モジュー

ルをリブートします。このファブリック インターコネクトへの両方向のデータ トラフィックは中断します。しかし、Cisco UCS ドメインはトラフィックとポート フェールオーバーを許可するよう設定されているため、データ トラフィックはプライマリ ファブリック インターコネクトにフェールオーバーし、中断しません。

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

必要な値が従属ファブリック インターコネクトの高可用性ステータスに格納されている場合は、プライマリ ファブリック インターコネクトの更新とアクティベーションを実行します。

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, （118 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。ここで説明する手順を使用することも、このビデオ（http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/activate_the_firmware_on_a_primary_fabric_interconnect.html）の [Play] をクリックしてプライマリ ファブリック インターコネクトのファームウェアをアクティブ化する方法を視聴することもできます。

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。

Cisco UCS Manager はファームウェアの更新とアクティベーションを実行し、ファブリック インターコネクトと、そのファブリック インターコネクトへのデータ パスにあるすべての I/O モジュールをリブートします。このファブリック インターコネクトへの両方向のデータ トラフィックは中断します。しかし、Cisco UCS ドメインはトラフィックとポート フェールオーバーを許可するよう設定されているため、データ トラフィックはもう一方のファブリック インターコネクトにフェールオーバーし、このファブリック インターコネクトがプライマリとなります。このファブリック インターコネクトが再度稼働状態になると、このファブリック インターコネクトは従属ファブリック インターコネクトになります。

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。

ヒント パスワードを Cisco UCS ドメインのファブリック インターコネクトの設定時に作成した admin アカウントに復旧する場合、実行中のカーネルのバージョンと実行中のシステムのバージョンを把握しておく必要があります。他のアカウントを作成しない場合、これらのファームウェアのバージョンのパスをテキスト ファイルに保存し、必要なときに参照できるようにしておくことを推奨します。

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] ノードをクリックします。

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。
[Service Pack Version] ドロップダウンリスト	適用するサービス パックのバージョンを選択します。 （注） サービス パックは基本のメンテナンス リリースにのみ適用できます。たとえば、サービスパック 3.1(3)SP2 は 3.1(3) リリースにのみ適用できます。3.1(4) リリースに適用することはできません。 [Service Pack] を [<not set>] に設定すると、サービス パックがファブリック インターコネクトから削除されます。

ステップ 6 [OK] をクリックします。

Cisco UCS Manager はファームウェアをアクティブにし、ファブリック インターコネクトと、そのファブリック インターコネクトへのデータ パスにあるすべての I/O モジュールをリブートします。スタンドアロン ファブリック インターコネクトでは、これにより Cisco UCS ドメイン内のすべてのデータ トラフィックが中断します。

ファブリック インターコネクト クラスタ リードのスイッチオーバー

この操作は、Cisco UCS Manager CLI でのみ実行できます。ここで説明する手順を使用することも、このビデオ（http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/switch_over_fabric_interconnect_cluster_lead.html）の [Play] をクリックして、あるファブリック インターコネクトから別のファブリック インターコネクトにクラスタ リードをスイッチオーバーする方法を視聴することもできます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **show cluster state**	（任意） クラスタ内のファブリック インターコネクトの状態と、クラスタが HA レディであるかどうかを表示します。
ステップ 2	UCS-A# **connect local-mgmt**	クラスタのローカル管理モードを開始します。
ステップ 3	UCS-A (local-mgmt) # **cluster** {**forceprimary** | **lead** {**a** | **b**}}	次のいずれかのコマンドを使用して、従属ファブリック インターコネクトをプライマリに変更します。 **force** ローカル ファブリック インターコネクトがプライマリになるように強制します。 **lead** 指定した従属ファブリック インターコネクトをプライマリにします。

次に、ファブリック インターコネクト B を従属からプライマリに変更する例を示します。

```
UCS-A# show cluster state
Cluster Id: 0xfc436fa8b88511e0-0xa370000573cb6c04

A: UP, PRIMARY
B: UP, SUBORDINATE

HA READY
UCS-A# connect local-mgmt
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2011, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
```

```
UCS-A(local-mgmt)# cluster lead b
UCS-A(local-mgmt)#
```

ファブリック インターコネクトでのサービス パックの有効化

ここで説明する手順を使用して、ファブリックインターコネクトでサービスパックを有効化できます。

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] 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 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 [Service Pack] の行で、[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サービス パックの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。
Cisco UCS Manager は、ファームウェアを有効化します。場合によっては、Cisco UCS Manager によってファブリックインターコネクトが再起動され、そのファブリックインターコネクトに対するデータ トラフィックが中断されます。

ファブリック インターコネクトからのサービス パックの削除

ここで説明する手順を使用して、ファブリックインターコネクトからサービスパックを削除することができます。

Open SLL などの特定のシナリオでは、サービス パックを削除すると FI の再起動が発生します。

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] 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 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 [Service Pack] の行で、[Startup Version] カラム のドロップダウン リストからサービス パックのバージョンとして [<not set>] を選択します。

ステップ 7 [OK] をクリックします。

アダプタ ファームウェア

Cisco Unified Computing System は、幅広いコンバージド（統合型）ネットワーク アダプタ（CNA）をサポートします。CNA は、LAN および SAN トラフィックを単一のインターフェイスに統合することで、複数のネットワーク インターフェイス カード（NIC）とホストバス アダプタ（HBA）の必要性をなくします。

すべての Cisco UCS ネットワーク アダプタは、次のことが可能です。

- 必要なネットワーク インターフェイス カードとホスト バス アダプタの数を削減可能
- Cisco UCS Manager ソフトウェアで管理
- 2 つのファブリック エクステンダと 2 つのファブリック インターコネクトを備えた冗長構成で使用可能
- 配線は初回のみ、その後はソフトウェアで機能の有効化や設定が行える「ワイヤワンス（wire-once）」アーキテクチャに対応
- ファイバ チャネル マルチパスをサポート

シスコ仮想インターフェイス カード（VIC）は、256 の仮想インターフェイスを提供し、Cisco VM-FEX テクノロジーをサポートします。Cisco VIC は、仮想化環境の実際のワークロード モビリティを実現するための I/O ポリシーの整合性と可視性を提供します。Cisco VIC は、B シリーズ ブレード サーバおよび C シリーズ ラック サーバのフォーム ファクタで使用できます。

アダプタのファームウェアのアップデート

注意 更新が完了するまで、エンドポイントがあるハードウェアを取り外したり、メンテナンス作業を実行しないでください。ハードウェアが取り外されたり、その他のメンテナンス作業により使用できない場合、ファームウェアの更新は失敗します。この失敗により、バックアップ パーティションが破損する場合があります。バックアップ パーティションが破損しているエンドポイントではファームウェアを更新できません。

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] > [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を搭載し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、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、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 は、直接更新できるサーバ上の他のすべてのエンドポイントのファームウェアを更新します。

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 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

ファームウェアをアクティブにします。

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ていない場合、アクティブ化されたファームウェアは pending-next-boot 状態のままになります。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

Basic Input/Output System（BIOS）は、システムのハードウェア コンポーネントをテストおよび初期化し、ストレージ デバイスからオペレーティング システムを起動します。Cisco UCS には、システム動作を制御する複数の BIOS 設定があります。BIOS ファームウェアは、直接 Cisco UCS Manager からアップデートできます。

サーバの BIOS ファームウェアのアップデート

注意 更新が完了するまで、エンドポイントがあるハードウェアを取り外したり、メンテナンス作業を実行しないでください。ハードウェアが取り外されたり、その他のメンテナンス作業により使用できない場合、ファームウェアの更新は失敗します。この失敗により、バックアップ パーティションが破損する場合があります。バックアップ パーティションが破損しているエンドポイントではファームウェアを更新できません。

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] > [Chassis] > *[Chassis Number]* > [Servers] の順に展開します。

ステップ 3 BIOS の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 BIOS 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) （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

ファームウェアをアクティブにします。

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

Cisco Integrated Management Controller（CIMC）は、Cisco UCS でのサーバの管理とモニタリングに使用されます。CIMC には、管理およびモニタリング タスク用に GUI、CLI、IPMI などのオプションが用意されています。C シリーズ サーバでは、CIMC は独立したチップで実行されます。そのため、大規模なハードウェア障害やシステムのクラッシュ時でもサービスを提供することができます。CIMC は、サーバの初期設定やサーバ動作に関する問題のトラブルシューティングにも役立ちます。CIMC ファームウェアは、直接 Cisco UCS Manager から更新できます。

サーバの CIMC ファームウェアのアップデート

注意 更新が完了するまで、エンドポイントがあるハードウェアを取り外したり、メンテナンス作業を実行しないでください。ハードウェアが取り外されたり、その他のメンテナンス作業により使用できない場合、ファームウェアの更新は失敗します。この失敗により、バックアップ パーティションが破損する場合があります。バックアップ パーティションが破損しているエンドポイントではファームウェアを更新できません。

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] > [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

ファームウェアをアクティブにします。

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。

注意 更新が完了するまで、エンドポイントがあるハードウェアを取り外したり、メンテナンス作業を実行しないでください。ハードウェアが取り外されたり、その他のメンテナンス作業により使用できない場合、ファームウェアの更新は失敗します。この失敗により、バックアップ パーティションが破損する場合があります。バックアップ パーティションが破損しているエンドポイントではファームウェアを更新できません。

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] > [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-reboot 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。

PSU ファームウェア

PSU ファームウェアは、Cisco UCS Manager から直接更新できます。

PSU でのファームウェアのアップデート

注意 更新が完了するまで、エンドポイントがあるハードウェアを取り外したり、メンテナンス作業を実行しないでください。ハードウェアが取り外されたり、その他のメンテナンス作業により使用できない場合、ファームウェアの更新は失敗します。この失敗により、バックアップ パーティションが破損する場合があります。バックアップ パーティションが破損しているエンドポイントではファームウェアを更新できません。

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] > [Chassis] の順に展開します。

ステップ 3 管理する PSU に対応するシャーシを選択します。

ステップ 4 [Work] ペインの [PSUs] をクリックします。

ステップ 5 [Firmware Management] タブをクリックします。

ステップ 6 アップグレードする PSU を右クリックし、[Update Firmware] を選択します。

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、選択したファームウェア 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、明示的にそれをアクティブにするまで、そのまま残ります。

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

ファームウェアをアクティブにします。

PSU 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] の順に展開します。

ステップ 3 管理する PSU に対応するシャーシを選択します。

ステップ 4 [Work] ペインの [PSUs] をクリックします。

ステップ 5 アップグレードする PSU を右クリックし、[Activate Firmware] を選択します。

ステップ 6 [General] タブの [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-reboot 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。以前は、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 以降のブレード 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 以降のブレード 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。シスコからのソフトウェア バンドルの入手, （68 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, （139ページ）には、Cisco UCS Manager による機能カタログのアクティブ化に関する情報が詳細に説明されています。
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 以降のラック 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 以降のラック 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、https://tools.cisco.com/bugsearch/bug/CSCuv45173を参照してください。

- 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 M3 以降のブレード サーバでのボード コントローラ ファームウェアのアクティブ化

（注） このアクティブ化手順を実行すると、サーバはリブートされます。サーバに関連付けられているサービス プロファイルにメンテナンス ポリシーが含まれているかどうかに応じて、リブートはただちに行われることがあります。ボード コントローラ ファームウェアをアップグレードする際は、サーバ BIOS のアップグレードと同時に、（Cisco UCS ドメイン のアップグレードの最後の手順として）サービス プロファイル内のホスト ファームウェア パッケージから行うことをお勧めします。これによって、アップグレード プロセス中にサーバをリブートする回数を低減できます。

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] 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。

Cisco UCS C シリーズ M3 以降のラック サーバでのボード コントローラ ファームウェアのアクティブ化

（注） このアクティブ化手順を実行すると、サーバはリブートされます。サーバに関連付けられているサービス プロファイルにメンテナンス ポリシーが含まれているかどうかに応じて、リブートはただちに行われることがあります。ボード コントローラ ファームウェアをアップグレードする際は、サーバ BIOS のアップグレードと同時に、（Cisco UCS ドメイン のアップグレードの最後の手順として）サービス プロファイル内のホスト ファームウェア パッケージから行うことをお勧めします。これによって、アップグレード プロセス中にサーバをリブートする回数を低減できます。

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] 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。

第 4 章

Cisco UCS Manager での機能カタログの管理

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。同じメジャー リリース バージョン内で機能カタログをアップグレードできます。Cisco UCS 3.2(x) リリースは、3.2(x) リリースの機能カタログで動作しますが、3.1、3.0、2.2、2.1、およびそれ以前のリリースのバージョンでは動作しません。たとえば、3.1(1) システムにはリリース 3.1(2) の機能カタログを使用できますが、3.0(1) システムでは使用できません。

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 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 [All] > [Capability Catalog] の順に展開します。

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 [All] > [Capability Catalog] の順に展開します。

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 http://www.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, （140 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 http://www.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 [All] > [Capability Catalog] の順に展開します。

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、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 5 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

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、http://www.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、[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 [All] > [Capability Catalog] の順に展開します。

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

機能カタログの更新をアクティブ化します。

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 [All] > [Capability Catalog] の順に展開します。

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、イメージ ファイルのフル パスと名前を入力します。
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 5 章

ファームウェアのトラブルシューティング

アップグレード中のファブリックインターコネクトの回復

1 つまたは両方のファブリック インターコネクトがフェールオーバーまたはファームウェア アップグレード中に失敗した場合は、次のいずれかのアプローチを使用してこれらのファブリック インターコネクトを回復できます。

- ファブリック インターコネクトに稼動中のイメージがない場合にファブリック インターコネクトを回復する。
- ファブリック インターコネクトに稼動中のイメージがある場合にファブリック インターコネクトを回復する。
- アップグレードまたはフェールオーバー中に無応答のファブリック インターコネクトを回復する。
- 自動インストール によるアップグレード中に障害が発生した FSM からファブリック インターコネクトを回復する。

ファブリックインターコネクトまたはブートフラッシュに稼動中のイメージがない場合のファブリック インターコネクトの回復

両方または一方のファブリック インターコネクトがファームウェア アップグレード中にダウンし、リブートされ、ローダープロンプトで停止した場合、かつファブリックインターコネクトに稼動中のイメージがない場合は、次の手順を実行できます。

手順

ステップ 1 スイッチをリブートし、コンソールでCtrl+L**Ctrl+L** キーを押して、起動時にローダー プロンプトを表示させます。

（注） ローダー プロンプトを画面に表示するには、選択したキーの組み合わせを複数回押さなければならない場合があります。

例：
```
loader>
```

ステップ 2 TFTP を通じてキックスタート イメージを受信するようにインターフェイスを設定します。

a) loader>プロンプトでシステムのローカル IP アドレスとサブネット マスクを入力して、Enter**Enter** キーを押します。

例：
```
loader> set ip 10.104.105.136 255.255.255.0
```

b) デフォルト ゲートウェイの IP アドレスを指定します。

例：
```
loader> set gw 10.104.105.1
```

c) 必要なサーバからキックスタート イメージ ファイルを起動します。

例：
```
loader> boot
tftp://10.104.105.22/tftpboot/Images.3.0.2/ucs-6300-k9-kickstart.5.0.2.N1.3.02d56.bin
switch(boot)#
```

（注） ブートフラッシュにキックスタート イメージがある場合は、このステップは不要です。

ステップ 3 switch(boot)# プロンプトで init system**init system** コマンドを入力します。
このコマンドによって、ファブリック インターコネクトが再フォーマットされます。

例：
```
switch(boot)# init system
```

ステップ 4 管理インターフェイスを設定します。

a) 設定モードに変更し、mgmt0 インターフェイスの IP アドレスを設定します。

例：
```
switch(boot)# config t
switch(boot)(config)# interface mgmt0
```

b) ip address**ip address** コマンドを入力して、システムのローカル IP アドレスとサブネット マスクを設定します。

例：
```
switch(boot)(config-if)# ip address 10.104.105.136 255.255.255.0
```

c) no shutdown**no shutdown** コマンドを入力して、システムで mgmt0 インターフェイスを有効にします。

例：
```
switch(boot)(config-if)# no shutdown
```

d) ip default-gateway**ip default-gateway** コマンドを入力して、デフォルト ゲートウェイの IP アドレスを設定します。

例：
```
switch(boot)(config-if)# exit
switch(boot)(config)# ip default-gateway 10.104.105.1
```

e) **exit** を入力して、EXEC モードを終了します。

例：
```
switch(boot)(config)# exit
```

ステップ 5 キックスタート、システム、および Cisco UCS Manager 管理イメージを TFTP サーバからブートフラッシュにコピーします。

例：
```
switch(boot)# copy
scp://<username>@10.104.105.22/tftpboot/Images.3.0.2/ucs-6300-k9-kickstart.5.0.2.N1.3.02d56.bin
 bootflash://
switch(boot)# copy
scp://<username>@10.104.105.22/tftpboot/Images.3.0.2/ucs-6300-k9-system.5.0.2.N1.3.02d56.bin
 bootflash://
switch(boot)# copy
scp://<username>@10.104.105.22/tftpboot/Images.3.0.2/ucs-manager-k9.3.0.2d56.bin bootflash://
```

ステップ 6 ブートフラッシュに installables および installables/switch ディレクトリを個別に作成します。

例：
```
switch(boot)# mkdir bootflash:installables
switch(boot)# mkdir bootflash:installables/switch
```

ステップ 7 キックスタート、システム、および Cisco UCS Manager イメージを installables/switch ディレクトリにコピーします。

例：
```
switch(boot)# copy ucs-6300-k9-kickstart.5.0.2.N1.3.02d56.bin bootflash:installables/switch/
switch(boot)# copy ucs-6300-k9-system.5.0.2.N1.3.02d56.bin bootflash:installables/switch/
switch(boot)# copy ucs-manager-k9.3.02d56.bin bootflash:installables/switch/
```

ステップ 8 管理イメージが nuova-sim-mgmt-nsg.0.1.0.001.bin にリンクされていることを確認します。nuova-sim-mgmt-nsg.0.1.0.001.bin は予約済みシステム イメージが使用し、管理イメージを Cisco UCS Manager 準拠にするための名前です。

例：

```
switch(boot)# copy bootflash:installables/switch/ucs-manager-k9.3.02d56.bin
nuova-sim-mgmt-nsg.0.1.0.001.bin
```

ステップ 9 スイッチをリロードします。

例：

```
switch(boot)# reload
This command will reboot this supervisor module. (y/n) ? y
```

ステップ 10 キックスタート イメージから起動します。

例：

```
loader> dir
nuova-sim-mgmt-nsg.0.1.0.001.bin
ucs-6300-k9-kickstart.5.0.2.N1.3.02d56.bin
ucs-6300-k9-system.5.0.2.N1.3.02d56.bin
ucs-manager-k9.3.02d56.bin
loader> boot ucs-6300-k9-kickstart.5.0.2.N1.3.02d56.bin
switch(boot)#
```

ステップ 11 システム イメージをロードします。
システム イメージが完全にロードされたら、[Basic System Configuration Dialog] ウィザードが表示されます。このウィザードを使用してファブリック インターコネクトを設定します。

例：

```
switch(boot)# load ucs-6300-k9-system.5.0.2.N1.3.02d56.bin
Uncompressing system image: bootflash:/ucs-6300-k9-system.5.0.2.N1.3.02d56.bin

...

---- Basic System Configuration Dialog ----

  This setup utility will guide you through the basic configuration of
  the system. Only minimal configuration including IP connectivity to
  the Fabric interconnect and its clustering mode is performed through these steps.

...

Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
Applying configuration. Please wait.

Configuration file - Ok
```

ステップ 12 Cisco UCS Manager にログインし、ファームウェアをダウンロードします。

例：

```
UCS-A# scope firmware
UCS-A /firmware # download image scp://<username>@<server ip>//<downloaded image
location>/<infra bundle name>
Password:
UCS-A /firmware # download image scp://<username>@<server ip>//<downloaded image
location>/<b-series bundle name>
Password:
UCS-A /firmware # download image scp://<username>@<server ip>//<downloaded image
location>/<c-series bundle name>
Password:
UCS-A /firmware # show download-task
```

```
Download task:
    File Name Protocol Server          Userid          State
    --------- -------- --------------- --------------- -----
    ucs-k9-bundle-b-series.3.0.2.B.bin
              Scp      10.104.105.22   abcdefgh        Downloading
    ucs-k9-bundle-c-series.3.0.2.C.bin
              Scp      10.104.105.22   abcdefgh        Downloading
    ucs-k9-bundle-infra.3.0.2.A.bin
              Scp      10.104.105.22   abcdefgh        Downloading
UCS-A /firmware #
```

ステップ 13 ファームウェアのダウンロードが完了したら、ファブリックインターコネクトファームウェアと Cisco UCS Manager ファームウェアをアクティブ化します。
このステップにより、Cisco UCS Manager およびファブリック インターコネクトが目的のバージョンに更新されてリブートされます。

例：

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect* # activate firmware kernel-version 5.0(2)N1(3.02d56)
ignorecompcheck
Warning: When committed this command will reset the end-point
UCS-A /fabric-interconnect* # activate firmware system-version 5.0(2)N1(3.02d56)
ignorecompcheck
Warning: When committed this command will reset the end-point
UCS-A /fabric-interconnect* # commit-buffer
UCS-A /fabric-interconnect # exit

UCS-A# scope system
UCS-A /system # show image

Name                                          Type                 Version
--------------------------------------------- -------------------- -------
ucs-manager-k9.3.02d56.bin                    System               3.0(2d)
UCS-A /system # activate firmware 3.0(2d) ignorecompcheck
The version specified is the same as the running version
UCS-A /system # activate firmware 3.0(2d) ignorecompcheck
The version specified is the same as the running version
UCS-A /system #
```

ブートフラッシュに稼動中のイメージがある場合のアップグレード中のファブリック インターコネクトの回復

次の手順は、両方または一方のファブリックインターコネクトがファームウェアアップグレード中にダウンし、リブートされ、ローダー プロンプトで停止した場合に実行できます。

はじめる前に

次の手順を実行するには、ブートフラッシュに稼動中のイメージが存在する必要があります。

手順

ステップ 1 スイッチをリブートし、コンソールで Ctrl+L キーを押して、起動時にローダー プロンプトを表示させます。

（注） ローダー プロンプトを画面に表示するには、選択したキーの組み合わせを複数回押さなければならない場合があります。

例：
```
loader>
```

ステップ 2 dir コマンドを実行します。
ブートフラッシュ内の使用可能なカーネル、システム、および Cisco UCS Manager イメージのリストが表示されます。

例：
```
loader> dir
nuova-sim-mgmt-nsg.0.1.0.001.bin
ucs-6300-k9-kickstart.5.0.2.N1.3.02d56.bin
ucs-6300-k9-system.5.0.2.N1.3.02d56.bin
ucs-manager-k9.3.02d56.bin
```

ステップ 3 ブートフラッシュからカーネル ファームウェア バージョンを起動します。
（注） ここで使用できるカーネル イメージが、起動できる稼動イメージです。

例：
```
loader> boot ucs-6300-k9-kickstart.5.0.2.N1.3.02d56.bin
```

ステップ 4 管理イメージが nuova-sim-mgmt-nsg.0.1.0.001.bin にリンクされていることを確認します。
nuova-sim-mgmt-nsg.0.1.0.001.bin は予約済みシステム イメージが使用し、管理イメージを Cisco UCS Manager 準拠にするための名前です。

例：
```
switch(boot)# copy ucs-manager-k9.1.4.1k.bin nuova-sim-mgmt-nsg.0.1.0.001.bin
```

ステップ 5 システム イメージをロードします。

例：
```
switch(boot)# load ucs-6300-k9-system.5.0.2.N1.3.02d56.bin
```

ステップ 6 Cisco UCS Manager にログインし、ファブリック インターコネクトと Cisco UCS Manager ソフトウェアを必要なバージョンにアップデートします。

アップグレードまたはフェールオーバー中の無応答のファブリックインターコネクトの回復

アップグレードまたはフェールオーバー中は、新たなリスクを避けるため、次のタスクを実行しないでください。

- Pmon の停止と開始
- FI のリブート（電源の再投入または CLI）
- HA フェールオーバー

手順

ステップ 1 CSCup70756 で説明されているように **httpd_cimc.sh** プロセスが失われた場合、KVM にアクセスできなくなります。フェールオーバーを続けるか、Cisco テクニカル サポートに連絡します。

ステップ 2 プライマリ側で KVM にアクセスできなくなった場合は、フェールオーバーを続行して問題を解決します。

ステップ 3 セカンダリ側で KVM が必要であるか、またはダウンしている場合は、デバッグ プラグインを使用してそのサービスのみを開始します。デバッグ イメージを実行するには、TAC にお問い合わせください。

ステップ 4 CSCuo50049 で説明されている /dev/null 問題が発生した場合は、必要に応じて両方のステップでデバッグ プラグインを使用して権限を 666 に修正します。Cisco テクニカル サポートに連絡してデバッグ コマンドを実行します。

ステップ 5 CSCup70756 および CSCuo50049 の両方が発生した場合、VIP が失われる可能性があります。VIP が失われた場合は、次の手順を実行します。

1. GUI からプライマリ物理アドレスにアクセスし、GUI を使用して、回復するすべての IO モジュールのバックプレーン ポートを確認します。
2. GUI がダウンしている場合、NXOS show fex detail コマンドを使用して、IO モジュールのバックプレーン ポートを確認します。
3. 回避策を実行し、両方のファブリック インターコネクトのクラスタの状態が UP になっていることを確認します。
4. 両方のファブリック インターコネクトのクラスタの状態が UP になっている場合は、SSH CLI 構文を使用してプライマリ ファブリック インターコネクトのリブートを再確認して、アップグレードを続行します。

```
UCS-A# scope firmware
UCS-A /firmware # scope auto-install
UCS-A /firmware/auto-install # acknowledge primary fabric-interconnect reboot
UCS-A /firmware/auto-install* # commit-buffer
UCS-A /firmware/auto-install #
```

自動インストール によるアップグレード中に障害が発生した FSM からのファブリック インターコネクトの回復

次の状態が発生した場合には、いずれに対しても、これらの手順が実行できます。

- ファブリック インターコネクトにサービス パックがインストールされている状態で、Cisco UCS Manager リリース 3.1(2) からリリース 3.1(3) に 自動インストール を使用して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している。
- FSM の DeployPollActivate の段階で複数回再試行したか、FSM の障害のために、ファブリック インターコネクトの両方またはいずれかがダウンしている。

手順

ステップ 1 下位のファブリック インターコネクト上の FSM の DeployPollActivate 段階で複数の再試行が確認された場合、または FSM に障害が発生した場合には、次の操作を行います。

a) デフォルトのインフラストラクチャ パックおよびサービス パックのスタートアップ バージョンをクリアします。

例：
```
UCS-A# scope org
UCS-A /org # scope fw-infra-pack default
UCS-A /org/fw-infra-pack # set infra-bundle-version ""
UCS-A /org/fw-infra-pack* # commit-buffer
```

b) 下位のファブリック インターコネクトからサービス パックを削除します。

例：
```
UCS-A# scope fabric-interconnect b
UCS-A# /fabric-interconnect # remove service-pack security
UCS-A# /fabric-interconnect* # commit-buffer
```

ステップ 2 自動インストール経由で強制オプションを使用して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。

例：
```
UCS-A# scope firmware
UCS-A /firmware # scope auto-install
UCS-A /firmware/auto-install # install infra infra-vers 3.1(3a)A force
This operation upgrades firmware on UCS Infrastructure Components
(UCS manager, Fabric Interconnects and IOMs).
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup
(3) Check if Management Interface Monitoring Policy is enabled
(4) Check if there is a pending Fabric Interconnect Reboot activitiy
(5) Ensure NTP is configured
(6) Check if any hardware (fabric interconnects, io-modules, servers or adapters) is
unsupported in the target release
Do you want to proceed? (yes/no): yes
```

```
Triggering Install-Infra with:
Infrastructure Pack Version: 3.1(3a)A
```

ステップ 3 プライマリ ファブリック インターコネクトのリブートを承認します。

例：
```
UCS-A /firmware/auto-install # acknowledge primary fabric-interconnect reboot
UCS-A /firmware/auto-install* # commit-buffer
UCS-A /firmware/auto-install #
```

ステップ 4 現在の下位のファブリック インターコネクト上の FSM の DeployPollActivate 段階で複数の再試行が確認された場合、または FSM に障害が発生した場合には、次の操作を行います。

a) デフォルトのインフラストラクチャ パックおよびサービス パックのスタートアップ バージョンをクリアします。

例：
```
UCS-A# scope org
UCS-A /org # scope fw-infra-pack default
UCS-A /org/fw-infra-pack # set infra-bundle-version ""
UCS-A /org/fw-infra-pack* # commit-buffer
```

b) 現在の下位のファブリック インターコネクトからサービス パックを削除します。

例：
```
UCS-A# scope fabric-interconnect a
UCS-A# /fabric-interconnect # remove service-pack security
UCS-A# /fabric-interconnect* # commit-buffer
```

両方のファブリック インターコネクトには、リリース 3.1(3) ファームウェアと、実行バージョンおよびスタートアップ バージョンのデフォルトのサービス パックが反映されます。

ファームウェア アップグレード中の IO モジュールの回復

ファームウェアのアップグレード中に IO モジュールを回復するには、ピア IO モジュールからその IO モジュールをリセットします。リセット後に、その IO モジュールはファブリック インターコネクトから設定を取得できます。

ピア I/O モジュールからの I/O モジュールのリセット

I/O モジュールのアップグレードが失敗したり、メモリ リークにより Cisco UCS Manager から I/O モジュールにアクセスできなくなったりする場合があります。このような場合でも、アクセスできない I/O モジュールをそのピア I/O モジュールからリブートできます。

I/O モジュールをリセットすると、I/O モジュールが工場出荷時の設定に復元され、すべてのキャッシュ ファイルと一時ファイルが削除されますが、サイズ制限付きの OBFL ファイルは保持されます。

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]* > [IO Modules] の順に展開します。

ステップ 3 リセットする I/O モジュールのピア I/O モジュールを選択します。

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 [Actions] 領域で、[Reset Peer IO Module] をクリックします。