Cisco UCS Manager ファームウェア管理（CLI 用）、リリース 4.2

初版：2021 年 6 月 24 日

最終更新：2022 年 9 月 20 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/

© 2021–2022 Cisco Systems, Inc. All rights reserved.

目 次

はじめに

対象読者

このガイドは、次の1つ以上に責任を持つ、専門知識を備えたデータセンター管理者を主な対象にしています。

- サーバ管理
- ストレージ管理
- ネットワーク管理
- ネットワーク セキュリティ

表記法

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

テキストのタイプ	説明
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、**this font**で示しています。 CLI コマンド内の変数は、このフォント 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。装置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 の関連資料

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、次の URL で入手可能な『*Cisco UCS B-Series Servers Documentation Roadmap*』を参照してください。https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/UCS_roadmap.html

すべての C-Series マニュアルの完全なリストについては、次の URL で入手可能な『『*Cisco UCS C-Series Servers Documentation Roadmap*』』を参照してください。https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/ucs_rack_roadmap.html

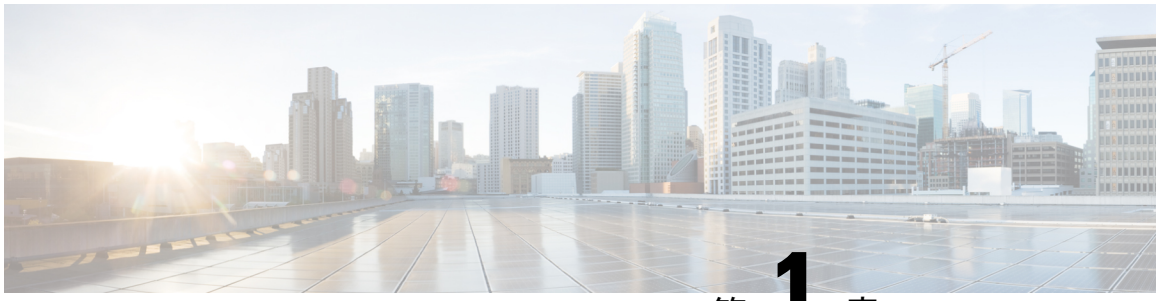
管理用の UCS Manager に統合されたラック サーバでサポートされるファームウェアと UCS Manager のバージョンについては、『Release Bundle Contents for Cisco UCS Software』[英語] を参照してください。

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、または誤りや記載漏れに関する報告は、ucs-docfeedback@external.cisco.com に送信してください。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、次の内容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 4.1(1) では、 Cisco UCS 64108 ファブリック インターコネクト から Cisco UCS 6400 シリーズ ファブリック インターコネクト を導入します。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にそれぞれユニファイド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 6400 シリーズ ファブリック インターコネクト と Cisco UCS B シリーズ、および C シリーズ サーバ
- 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 Fabric Interconnect と Cisco UCS B シリーズおよび C シリーズ サーバ（別名 UCS Mini）

***Figure 1: Cisco UCS 6400* 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**

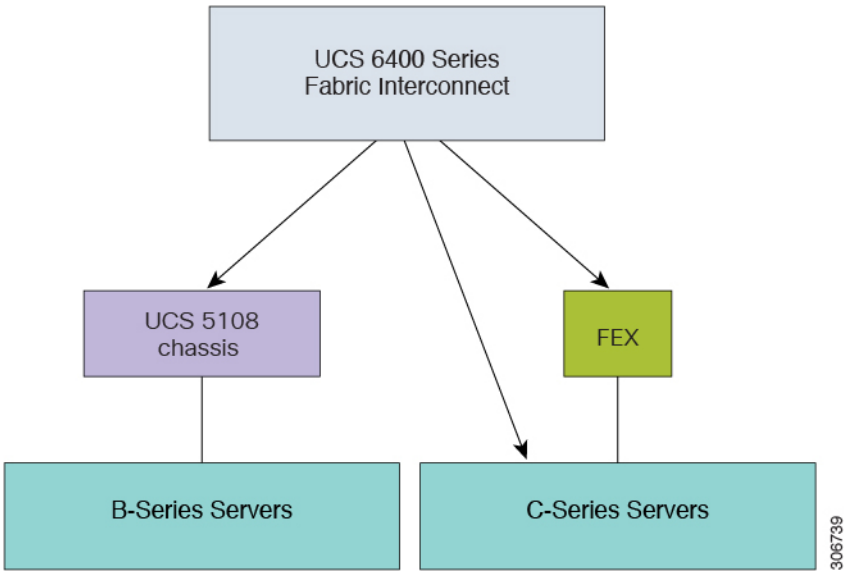


Figure 2: Cisco UCS 6300 シリーズ *Fabric Interconnect* と *Cisco UCS B* シリーズおよび *C* シリーズ サーバ

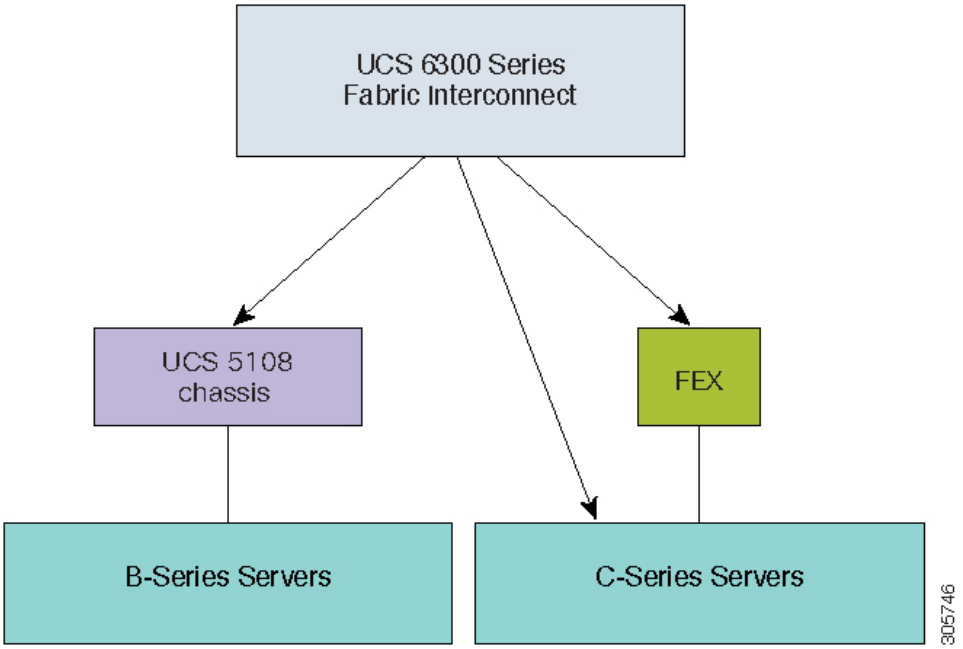


Figure 3: Cisco UCS 6200 シリーズ *Fabric Interconnect* と *Cisco UCS B* シリーズ、および *C* シリーズ サーバ

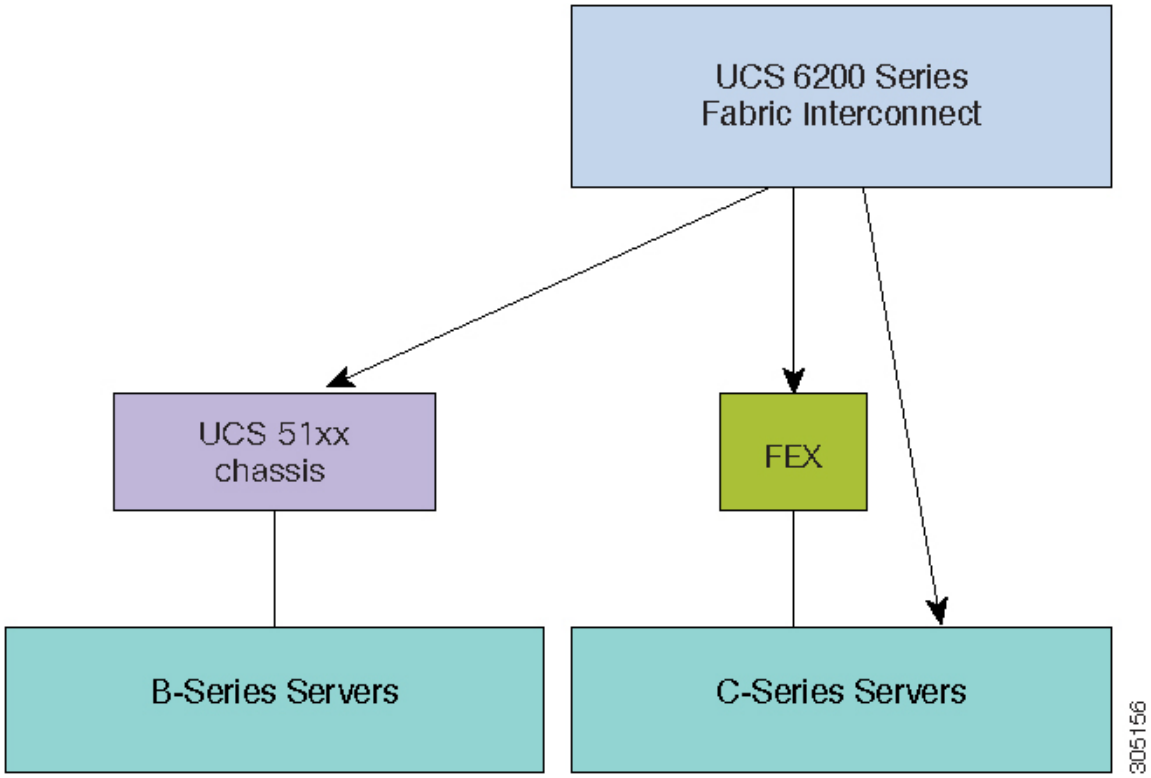
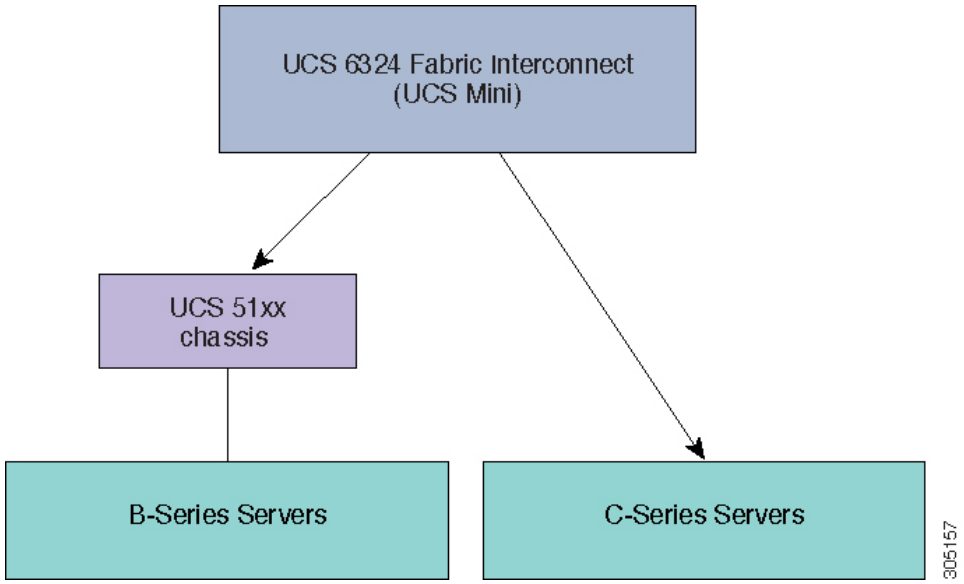


Figure 4: Cisco UCS B シリーズ サーバおよび ***C*** シリーズ サーバ向け ***Cisco UCS 6324*** ファブリック インターコネクト



次の図に、 Cisco UCS Manager リリース 4.1 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 Manager 4.1 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 6400 シリーズ ファブリック インターコネクト：ucs-6400-k9-bundle-infra.4.x.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.4.x.x.xxx.A.bin
  - 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.4.x.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.4.x.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。各 4.x リリースに対応する『*Release Bundle Contents for Cisco UCS Manager*』には、B シリーズ サーバー 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。

Note 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 C3260 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。4.1 以降のリリースに対応する『*Release Bundle Contents for Cisco UCS Manager*』には、C シリーズ サーバー 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。

Note 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 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 4.1 以降のリリースは、任意の 4.1 カタログ ファイルを使用できますが、4.0 または 3.2 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の順序は、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決定するアップグレード パスについては、ステップの決められた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。

Note 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 CLI ドキュメント

Cisco UCS Manager 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マニュアルが用意されています。

ガイド	説明
Cisco UCS Manager クイック スタート ガイド	Cisco UCS Manager の初期構成と構成のベストプラクティスを含め、Cisco UCS のアーキテクチャと初回操作について説明しています。
『Cisco UCS Manager アドミニストレーション ガイド』	パスワード管理、ロールベースのアクセス構成、リモート認証、通信サービス、CIMC セッションの管理、組織、バックアップと復元、スケジュール設定オプション、BIOS トークン、遅延導入について説明しています。
Cisco UCS Manager インフラストラクチャ管理ガイド	Cisco UCS Manager で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』	自動インストールを使用したファームウェアのダウンロード、管理、アップグレード、サービス プロファイルを使用したファームウェアのアップグレード、ファームウェア自動同期を使用したエンドポイントでの直接ファームウェアアップグレード、機能カタログの管理、導入シナリオ、トラブルシューティングについて説明しています。

ガイド	説明
Cisco UCS Manager サーバ管理ガイド	新しいランセンス、Cisco UCS Central への Cisco UCS ドメインの登録、パワー キャッピング、サーバブート、サーバプロファイル、サーバ関連のポリシーについて説明しています。
『Cisco UCS Manager Storage Management Guide』	SUN、VSAN など、Cisco UCS Managerでのストレージ管理のすべての側面について説明しています。
『Cisco UCS Manager Network Management Guide』	LAN 接続、VLAN 接続など、Cisco UCS Managerでのネットワーク管理のすべての側面について説明しています。
『Cisco UCS Manager System Monitoring Guide』	システム統計を含め、Cisco UCS Managerでのシステムおよびヘルス モニタリングのすべての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 による UCS S シリーズ サーバ管理のすべての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 64108 ファブリック インターコネクト
  - Cisco UCS 6454
  - 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 C3260 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 C3260 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。

実行されているバージョン

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。

スタートアップ バージョン

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、6300 および 6400 シリーズ 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、6300、6400* シリーズ 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）	4.0(1)	4.0(2)	4.0(4)	4.1(1)	4.1(2)	4.1(3)	4.2(1)
4.2(1)	—	—	—	—	—	—	6200、6332、6332-16UP、6454、64108
4.1(3)	—	—	—	6200、6332、6332-16UP、6454、64108	6200、6332、6332-16UP、6454、64108	6200、6332、6332-16UP、6454、64108	6200、6332、6332-16UP、6454、64108
4.1(2)	—	—	—	6200、6332、6332-16UP、6454、64108	6200、6332、6332-16UP、6454、64108	6200、6332、6332-16UP、6454、64108	6200、6332、6332-16UP、6454、64108
4.1(1)	—	—	—	6200、6332、6332-16UP、6454、64108	6200、6332、6332-16UP、6454、64108	6200、6332、6332-16UP、6454、64108	6200、6332、6332-16UP、6454、64108

	インフラストラクチャのバージョン（A バンドル）						
4.0(4)	6200、6332、6332-16UP、6454	6200、6332、6332-16UP、6454	6200、6332、6332-16UP、6454	6200、6332、6332-16UP、6454	6200、6332、6332-16UP、6454	6200、6332、6332-16UP、6454	6200、6332、6332-16UP、6454
4.0(2)	6200、6332、6332-16UP、6454	6200、6332、6332-16UP、6454	6200、6332、6332-16UP、6454	6200、6332、6332-16UP、6454	6200、6332、6332-16UP、6454	6200、6332、6332-16UP、6454	6200、6332、6332-16UP、6454

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）	4.0(1)	4.0(2)	4.0(4)	4.1(1)	4.1(2)	4.1(3)	4.2(1)
4.2(1)	—	—	—	—	—	—	6324
4.1(3)	—	—	—	6324	6324	6324	6324
4.1(2)	—	—	—	6324	6324	6324	6324
4.1(1)	—	—	—	6324	6324	6324	6324
4.0(4)	6324	6324	6324	6324	6324	6324	—
4.0(2)	6324	6324	6324	6324	6324	6324	—

次の表に、4.2(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 および C バンドルの混在バージョンを示します。

表 *3 : 4.2(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)	4.2(1)			
	6200	6300	6324	6400
	ucs-k9-bundle-infra.4.1. x. xxx. .bin	ucs-6300-k9-bundle-infra.4.1. x. xxx. .bin	ucs-mini-k9-bundle-infra.4.1. x. xxx. .bin	ucs-6400-k9-bundle-infra.4.1.x.xxx.A.bin

	インフラストラクチャのバージョン（A バンドル）			
4.2(1)	はい	はい	はい	はい
4.1(3)	はい	はい	はい	はい
4.1(2)	はい	はい	はい	はい
4.1(1)	はい	はい	はい	はい
4.0(1)、4.0(4)（B、C バンドル）	はい	はい	はい	はい

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) 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) 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。

- B シリーズ サーバ：UCS B200 M4、B260 M4、B420 M4、B460 M4、B200 M5、B480 M5
- C シリーズ サーバ：UCS C220 M4、C240 M4、C460 M4、C220 M5、C240 M5、C480 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

[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。

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 リリース 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、シャーシ、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、シャーシ、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 (各サービス パックにつき 1 回)。
- 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。

Note 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、シャーシ、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。その後、シャーシ ファームウェア パッケージを介してすべてのシャーシ コンポーネントをアップグレードし、ホスト ファームウェア パッケージを介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。
- 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。

Note 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、およびホスト ファームウェアをアップグレードできます。

各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はできません。Cisco UCS Central では、グローバル サービス プロファイル内でホスト ファームウェア ポリシーを使用して、ホスト ファームウェア コンポーネントをアップグレードする必要があります。

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。

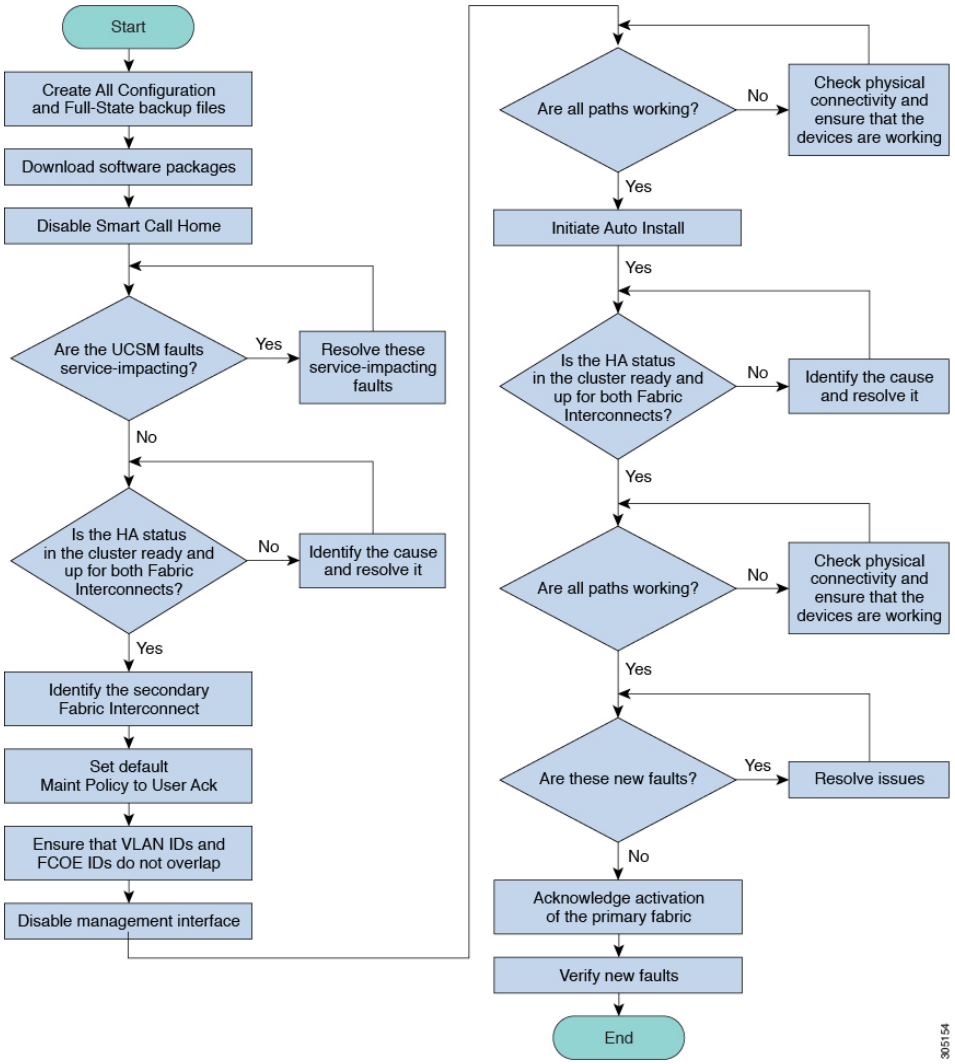
- インフラストラクチャの自動インストールを介してサービスパックにアップグレードする
- シャーシの自動インストールを介してサービス パックにアップグレードする
- サーバの自動インストールを介してサービス パックにアップグレードする
- サービス プロファイルのファームウェア パッケージを介してサービス パックにアップグレードする
- シャーシ プロファイルのシャーシ ファームウェア パッケージを介してサービス パックにアップグレードする
- 基本のメンテナンス リリースで Cisco UCS Manager サービス パックを直接アクティブにする
- 基本のメンテナンス リリースでファブリック 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 5 : 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）、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推奨されるプロセス フローを説明しています。

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



- [Install Chassis Firmware] : 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シャーシ コンポーネント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：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 のバージョンにアップグレードし、 シャーシと 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 と Fabric Evacuation 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。

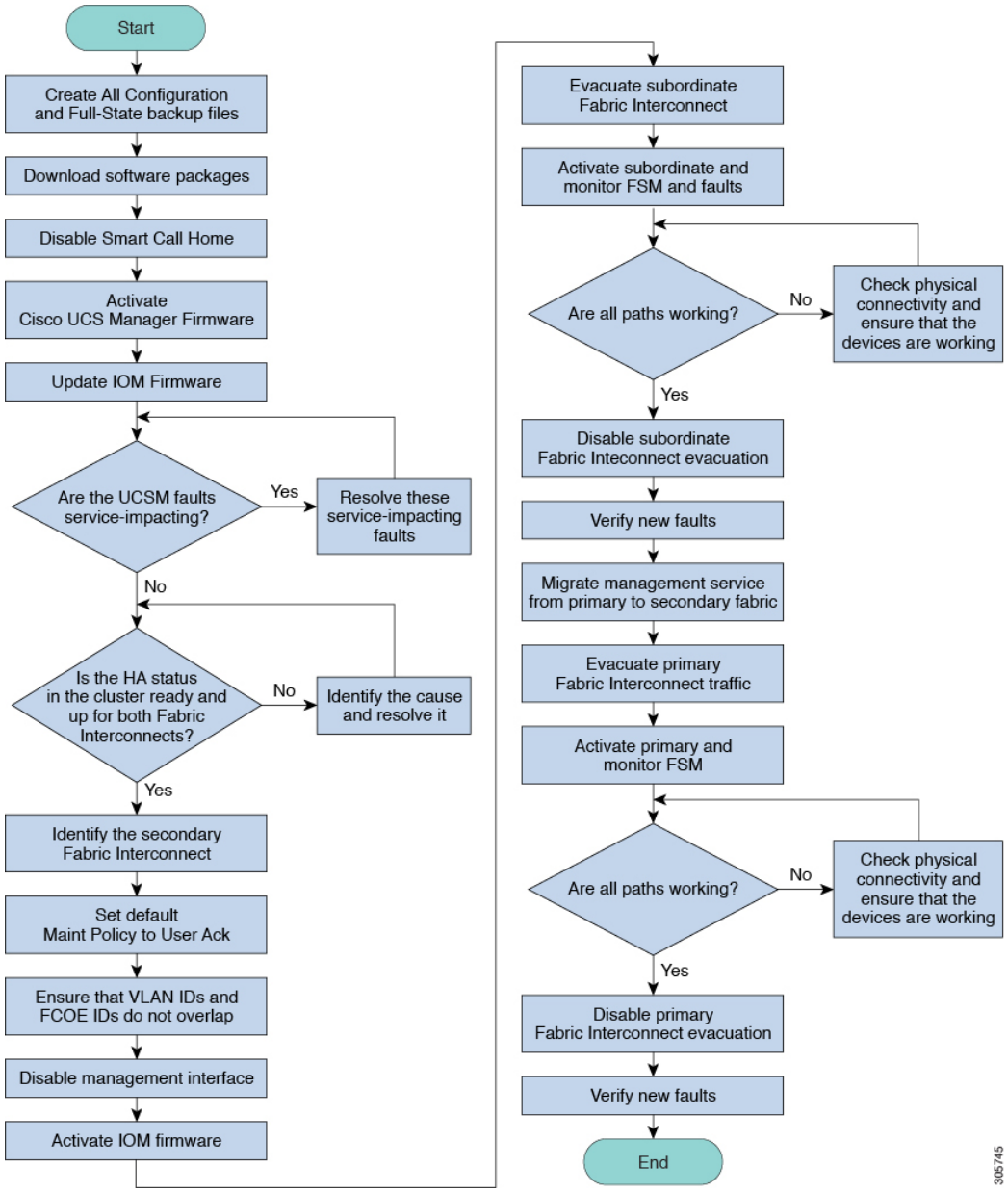
インフラストラクチャ	UCS 5108 シャーシ	UCS ラックサーバ	Cisco UCS C3260シャーシ

• Cisco UCS Manager
• ファブリック インターコネクト
 	
必ず Cisco UCS Manager をアップグレードしてからファブリック インターコネクトをアップグレードしてください。
	• 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

Note 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。

Figure 6: 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, on page 23は推奨されるプロセス フローを示しています。

Figure 6: 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。

Note 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 6400 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 4.1(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 6400 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 インターコネクトから Cisco UCS 6400 ファブリック インターコネクトに移行できますが、Cisco UCS 6400 ファブリック インターコネクトから Cisco UCS 6200シリーズファブリックインターコネクトには移行できません。次の間では移行できません。
  - Cisco UCS 6332 および Cisco UCS 6332 16UP ファブリック インターコネクト
  - Cisco UCS 6332 および Cisco UCS 6454 ファブリック インターコネクト
  - Cisco UCS 6332 および Cisco UCS 64108 ファブリック インターコネクト
  - Cisco UCS 6332 16UP および Cisco UCS 6454 ファブリック インターコネクト
  - Cisco UCS 6332 16UP および Cisco UCS 64108 ファブリック インターコネクト
- 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。

（注） UCS 6400 シリーズ ファブリック インターコネクトには統一されたイメージがあります - キックスタート イメージとシステム イメージはもはや分離されていません。

- 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 6400 シリーズ ファブリック インターコネクト 上のソフトウェア機能設定

Cisco UCS Manager リリース 4.0 (1) および 4.0 (2) では、Cisco UCS 6454 ファブリック インターコネクト のさまざまなソフトウェア機能のサポートが導入されました。 Cisco UCS Manager リリース4.1 では、Cisco UCS 64108 ファブリック インターコネクト でのこれらの機能のサポートが拡張されています。これらのソフトウェア機能は次のとおりです。

- スイッチング モード：Cisco UCS 6400 シリーズ ファブリック インターコネクト はイーサネットまたは FC スイッチング モードをサポートしていません。
- MAC セキュリティ :Cisco UCS 6400 シリーズ ファブリック インターコネクト で MAC セキュリティをサポートしていません。
- ブレークアウト アップリンク ポート：サポートされたブレークアウト ケーブルを使用して、1 つの QSFP ポートを 4 つの 10/25G ポートに分割をサポートします。これらのポートは、イーサネット アップリンクまたは FCoE アップリンク ポートの 10/25 G スイッチに接続するとしてのみ使用できます。これらは、サーバ ポート、FCoE ストレージ ポート、アプライアンス ポートまたはモニタリング ポートとして設定できません。
- MTU 設定：Cisco UCS 64108 ファブリック インターコネクト は QOS ドロップ クラス ポリシーの mtu 設定をサポートします。

Cisco UCS 6400 シリーズ ファブリック インターコネクト次のソフトウェア機能をサポートしません。

- 非ポート チャネル モードでのシャーシ ディスカバリ ポリシー：Cisco UCS 6400 シリーズ ファブリック インターコネクトはポート チャネル モードのみをサポートします。
- 非ポート チャネル モードでのシャーシ接続ポリシー：Cisco UCS 6400 シリーズ ファブリック インターコネクトはポート チャネル モードのみをサポートします。
- マルチキャスト ハードウェア ハッシュ：Cisco UCS 6400 シリーズ ファブリック インターコネクトはマルチキャスト ハードウェア ハッシュをサポートしていません。
- ダイナミック vNICS でのサービス プロファイル：Cisco UCS 6400 シリーズ ファブリック インターコネクトはダイナミック vNIC 接続ポリシーをサポートしていません。

- マルチキャスト最適化：Cisco UCS 6400 シリーズ ファブリック インターコネクトは QoS 用のマルチキャスト最適化をサポートしていません。
- NetFlow—Cisco UCS 6400 シリーズ ファブリック インターコネクト は Netflow に関連する構成をサポートしていません。
- ポート プロファイルと DVS 関連の設定：Cisco UCS 6400 シリーズ ファブリック インターコネクトはポート プロファイルおよび分散型仮想スイッチ（DVS）に関連する設定をサポートしていません。

Cisco UCS 6400 シリーズ ファブリック インターコネクトの次のソフトウェア機能の構成が変更されました。

- ユニファイド ポート:Cisco UCS 6400 シリーズ ファブリック インターコネクトは、最大 16 つのユニファイド ポートをサポートします。これらは FC として設定できます。これらのポートはモジュールの先頭にあります。
- VLAN の最適化: Cisco UCS 6400 シリーズ ファブリック インターコネクト では、PV カウントが 16000 を超えるとポート VLAN (VP) グルーピングを利用して VLAN ポート カウント数の最適化を設定できます。次の表は、Cisco UCS 6400 シリーズ ファブリック インターコネクト、Cisco UCS 6300 シリーズ ファブリック インターコネクト、および Cisco UCS 6200 シリーズ ファブリック インターコネクトで有効および無効にされた VLAN ポート数の最適化による PV カウントを示しています。

	6200 シリーズ FI	**6300 シリーズ FI**	**6400 シリーズ FI**
VLAN ポート カウントの最適化が無効にされた PV カウント	32000	16000	16000
VLAN ポート カウントの最適化が有効にされた PV カウント	64000	64000	64000

  Cisco UCS 6400 シリーズ ファブリック インターコネクト がイーサネット スイッチング モードのとき:

  - Fabric Interconnect（FI; をサポートしません**VLAN ポートの数の最適化有効**
  - Fabric Interconnect（FI; 16000 PVs と同様に**VLAN ポート数最適化 Disabled**に設定すると、EHM モードをサポートしています

- VLAN の制限：Cisco UCS 6400 シリーズ ファブリック インターコネクトは、システムで利用するために 128 個の VLAN を予約します。

Cisco UCS Manager リリース 4.2 へのファームウェア アップグレード

Cisco UCS Managerリリース 4.2 へのファームウェア アップグレードのシナリオ

Cisco UCS Manager リリース 4.2(x) へのインフラストラクチャ ソフトウェア バンドル（A バンドル）の直接アップグレードは、リリース 3.2(3) 以降のリリースでサポートされています。

Cisco UCS Mini では、Cisco UCS Manager リリース 4.2 (x) へのインフラストラクチャ ソフトウェア バンドル（A バンドル）の直接アップグレードは、リリース 3.2(3) 以降のリリースからサポートされています。

次の表に、さまざまなCisco UCS Managerリリースのアップグレード パスを示します。

（注） リリースアップグレードを開始する前に、各バージョンのファームウェア管理ガイドを参照して、制限事項とアップグレードを実行するための正しいパスを理解してください。

表 *4 :* リリース *4.2* へのパスのアップグレード

リリースからアップグレード	リリースにアップグレード	推奨されるアップグレード パス
2.1.x	4.2(x)	このリリースでは、リリース 4.2(x) への直接アップグレードはサポートされていません。リリース 4.2(x) にアップグレードするには、順序で、次を実行します。 **1.** リリース 3.2(3) または 4.0(x) にインフラストラクチャ A バンドルをアップグレードします。 **2.** 3.2(3) または 4.0(x) をリリースするすべてのサーバの B と C のバンドルをアップグレードします。 **3.** リリース 4.2(x) にインフラストラクチャ A バンドルをアップグレードします。

リリースからアップグレード	リリースにアップグレード	推奨されるアップグレード パス
2.2(1)、2.2(2)、2.2(3)、2.2(4)、2.2(5)、2.2 (6)、2.2 (7)	4.2(x)	このリリースでは、リリース 4.2(x) への直接アップグレードはサポートされていません。リリース 4.2(x) にアップグレードするには、順序で、次を実行します。 **1.** リリース 3.2(3) または 4.0(x) にインフラストラクチャ A バンドルをアップグレードします。 **2.** 3.2(3) または 4.0(x) をリリースするすべてのサーバの B と C のバンドルをアップグレードします。 **3.** リリース 4.2(x) にインフラストラクチャ A バンドルをアップグレードします。
2.2(8)	4.2(x)	このリリースでは、リリース 4.2(x) への直接アップグレードはサポートされていません。リリース 4.2(x) にアップグレードするには、順序で、次を実行します。 **1.** リリース 3.2(3) または 4.0(x) にインフラストラクチャ A バンドルをアップグレードします。 **2.** 3.2(3) または 4.0(x) をリリースするすべてのサーバの B と C のバンドルをアップグレードします。 **3.** リリース 4.2(x) にインフラストラクチャ A バンドルをアップグレードします。

リリースからアップグレード	リリースにアップグレード	推奨されるアップグレード パス
3.0(x)	4.2(x)	このリリースでは、リリース 4.2(x) への直接アップグレードはサポートされていません。リリース 4.2(x) にアップグレードするには、順序で、次を実行します。 **1.** リリース 3.2(3) または 4.0(x) にインフラストラクチャ A バンドルをアップグレードします。 **2.** 3.2(3) または 4.0(x) をリリースするすべてのサーバの B と C のバンドルをアップグレードします。 **3.** リリース 4.2(x) にインフラストラクチャ A バンドルをアップグレードします。
3.1 (1)、3.1 (2)	4.2(x) このリリースでは、リリース 4.1(x) への直接アップグレードはサポートされていません。リリース 4.0(x) にアップグレードするには、順序で、次を実行します。	このリリースでは、リリース 4.2(x) への直接アップグレードはサポートされていません。リリース 4.2(x) にアップグレードするには、順序で、次を実行します。 **1.** リリース 3.2(3) または 4.0(x) にインフラストラクチャ A バンドルをアップグレードします。 **2.** 3.2(3) または 4.0(x) をリリースするすべてのサーバの B と C のバンドルをアップグレードします。 **3.** リリース 4.2(x) にインフラストラクチャ A バンドルをアップグレードします。

リリースからアップグレード	リリースにアップグレード	推奨されるアップグレード パス
3.1(3)	4.2(x)	このリリースでは、リリース 4.2(x) への直接アップグレードはサポートされていません。リリース 4.2(x) にアップグレードするには、順序で、次を実行します。 **1.** リリース 3.2(3) または 4.0(x) にインフラストラクチャ A バンドルをアップグレードします。 **2.** 3.2(3) または 4.0(x) をリリースするすべてのサーバの B と C のバンドルをアップグレードします。 **3.** リリース 4.2(x) にインフラストラクチャ A バンドルをアップグレードします。
3.2(1)、3.2(2)	4.2(x)	このリリースでは、リリース 4.2(x) への直接アップグレードはサポートされていません。リリース 4.2(x) にアップグレードするには、順序で、次を実行します。 **1.** リリース 3.2(3) または 4.0(x) にインフラストラクチャ A バンドルをアップグレードします。 **2.** 3.2(3) または 4.0(x) をリリースするすべてのサーバの B と C のバンドルをアップグレードします。 **3.** リリース 4.2(x) にインフラストラクチャ A バンドルをアップグレードします。
3.2(3)	4.2(x)	リリース 4.2(x) に直接アップグレードします。
4.0(x)	4.2(x)	リリース 4.2(x) に直接アップグレードします。
4.1(x)	4.2(x)	リリース 4.2(x) に直接アップグレードします。

重要 **[Cisco UCS B シリーズ M5 サーバーをリリース 4.2(2) にアップグレードする（Upgrade Cisco UCS B-Series M5 servers to Release 4.2(2)）**：Cisco UCS B シリーズ M5 サーバを 4.0（4m）またはそれ以前のリリースからアップグレードする場合は、2 段階のアップグレードを実行します。

1. まず、サーバーを 4.1 リリース バージョンにアップグレードします。シスコでは、最新の 4.1(3) パッチ バージョンを推奨しています。
2. サーバーが 4.1 リリース バージョンで実行されたら、4.2(2) リリースにアップグレードします。

Cisco UCS Manager リリース 4.2 へのアップグレード条件

- Cisco UCS Manager リリース 4.2 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とサーバ バンドルが次の Cisco UCS Manager リリースのいずれかにあることを確認してください。
  - Cisco UCS Manager リリース 3.2(3) 以降のリリース

  Cisco UCS Mini の場合、任意のリリース 3.2(x) または 4.0(x) リリースから、Cisco UCS Manager リリース 4.2 にアップグレードできます。
- Cisco UCS Manager リリース 4.2 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 3.2 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 4.2 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 4.2 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 4.2 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 **4.2(1d)** の場合は、次の構成になります。

- **4.2** はメジャー リリース識別番号
- **1** はマイナー リリース識別番号
- **d**はパッチ リリース識別番号

つまり、これらは**4.2**リリース トレインの**first**マイナー リリースの**d**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 のファームウェアを、アップグレードと同じ方法でダウングレードします。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。

Note Cisco UCS Manager CLI では、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をダウングレードすることはできません。サポートされていないリリースにハードウェアをダウングレードしようとすると、Cisco UCS Manager CLI からエラー メッセージが表示されます。

Cisco UCS Manager リリース 4.2 からのダウン グレード

Cisco UCS 64108 ファブリック インターコネクトを搭載したシステムでは、Cisco UCS Manager リリース 4.1 からダウングレードできません。

MD5 SNMPv3 ユーザ認証

リリースにダウン グレードするとよりも前Cisco UCS Managerリリース 3.2(3)、SNMPv3 ユーザの md5 認証は配置されません。このようなユーザを展開するには、次のいずれかの操作を行います。

- **[Auth Type]** フィールドを **[SHA]** に変更します。
- ユーザを削除し、それを再作成します。

SNMPv3 ユーザの AES プライバシー プロトコル

Cisco UCS Manager リリース 3.2(3) 以降のリリースでは、AES 暗号化なしの SNMPv3 ユーザはサポートされていません。したがって、Cisco UCS Managerリリース 3.2(3) より前のリリースにダウングレードすると、AES 暗号化を使用していない SNMPv3 ユーザは配置されません。このようなユーザを展開するには、次のいずれかの操作を行います。

- **AES-128** 暗号化を有効にする
- ユーザを削除し、それを再作成します。

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

Important

- 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 は自動的にボード コントローラ ファームウェアをスキップし、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けます。

- 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。

Note 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できます。

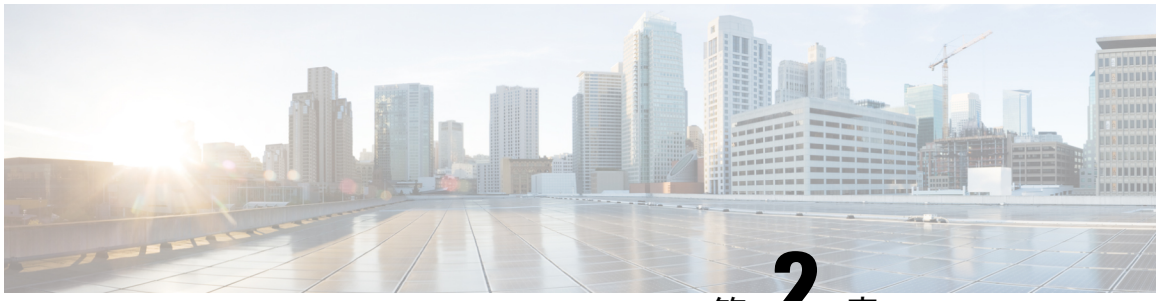
（注） Cisco UCS CentralからCisco UCS ドメインファームウェアを管理するには、Cisco UCS Manager でグローバルファームウェア管理オプションを有効にする必要があります。グローバルファームウェア管理オプションは、Cisco UCS Manager を Cisco UCS Central に登録するときに有効にできます。また、管理要件に基づいてグローバル管理オプションのオン/オフを切り替えることもできます。

重要 Cisco UCS CentralからCisco UCS ドメインを登録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 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 リリース 2.0 以降では許可されない

⚠

注意 Cisco UCS の 1.4 以前のリリースでは、イーサネット VLAN、FCoE VLAN は重複 VLAN ID を持つことができました。しかし、Cisco UCS リリース 2.0 以降では、VLAN ID の重複は許可されません。Cisco UCS Manager は、アップグレードの間に VLAN ID の重複を検出すると、深刻な障害と見なします。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 4043 ～ 4047 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 ドメインで 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 ドメインで FC エンドホスト モードを使用する予定の場合、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 更新プロセスが完了するまで、エンドポイントを含む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たりしないでください。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。

各エンドポイントに適したファームウェア アップグレードのタイプの決定

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更新する場合、[ファームウェアのアクティブ化（Activate Firmware）] ダイアログボックスの [フィルタ（Filter）] ドロップダウン リストで[すべて（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20%以上が使用可能でなければなりません。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 インターコネクト上のワークスペース 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 プラグインが格納されます。アップグレードまたはダウン グレードを開始するには、ワークスペース パーティションの 20% 以上が使用可能でなければなりません。

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、ファブリック インターコネクトと I/O モジュール間でプロトコルとファームウェア バージョンの不一致が Cisco UCS Managerで検出された場合、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と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、アップグレード プロセスを完了するために Cisco UCS Manager によってコンポーネントが再起動されます。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 インターコネクトのトラフィックの停止

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope fabric-interconnect** {**a** | **b**}	指定したファブリック インターコネクトのファブリック インターコネクト モードを開始します。
ステップ 2	UCS-A /fabric-interconnect # **stop server traffic** [**force**]	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。 ファブリック インターコネクトの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** オプションを使用します。
ステップ 3	UCS-A /fabric-interconnect # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、ファブリック インターコネクト B を通過するアクティブなすべてのトラフィックを停止する方法を示します。

```
UCS-A# scope fabric-interconnect b
UCS-A /fabric-interconnect # stop server traffic
Warning: 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.
UCS-A /fabric-interconnect # commit-buffer
```

ファブリック インターコネクトのトラフィックの再開

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope fabric-interconnect** {**a** | **b**}	指定したファブリック インターコネクトのファブリック インターコネクト モードを開始します。
ステップ 2	UCS-A /fabric-interconnect # **start server traffic**	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 3	UCS-A /fabric-interconnect # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、ファブリック インターコネクト B を通過するトラフィックを再開する方法を示します。

```
UCS-A# scope fabric-interconnect b
UCS-A /fabric-interconnect # start server traffic
Warning: Resetting fabric evacuation will cause server traffic that failed over to the
Primary Fabric Interconnect to fail back to this Fabric Interconnect.
UCS-A /fabric-interconnect # commit-buffer
```

ファブリックの退避の確認

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **show service-profile circuit server** *server-id*	指定されたサーバに関連付けられたサービス プロファイル用のネットワーク回路情報を表示します。

例

次の例は、ファブリック退避前の VIF パスを示しています。

（注）
- ファブリック インターコネクト A の VIF は、トラフィックがファブリック インターコネクトによって最初にアクティブであることを示します。
- ファブリック インターコネクト B の VIF は、退避前にパッシブです。

```
UCS-A# show service-profile circuit server 1/6
Service Profile: test1
Server: 1/6
    Fabric ID: A
        Path ID: 1
        VIF        vNIC           Link State  Oper State Prot State    Prot Role   Admin
 Pin  Oper Pin   Transport
        ---------- --------------- ----------- ---------- ------------- ----------
---------- ---------- ---------
               692 eth0            Up          Active     Active        Primary     0/0
        1/15       Ether
    Fabric ID: B
        Path ID: 1
        VIF        vNIC           Link State  Oper State Prot State    Prot Role   Admin
 Pin  Oper Pin   Transport
        ---------- --------------- ----------- ---------- ------------- ----------
---------- ---------- ---------
               693 eth0            Up          Active     Passive       Backup      0/0
        1/15       Ether
UCS-A#
```

次の例は、ファブリック インターコネクト A 退避後の VIF パスを示しています。

（注）
- フェールオーバー後、ファブリック インターコネクト A の VIF 状態はエラーになります。
- ファブリック インターコネクト B の VIF がアクティブとして引き継ぎます。

```
UCS-A# show service-profile circuit server 1/6
Service Profile: test1
Server: 1/6
    Fabric ID: A
        Path ID: 1
        VIF        vNIC           Link State  Oper State Prot State    Prot Role   Admin
 Pin  Oper Pin   Transport
        ---------- --------------- ----------- ---------- ------------- ----------
---------- ---------- ---------
               692 eth0            Error       Error      Active        Primary     0/0
        0/0        Ether
    Fabric ID: B
        Path ID: 1
        VIF        vNIC           Link State  Oper State Prot State    Prot Role   Admin
 Pin  Oper Pin   Transport
        ---------- --------------- ----------- ---------- ------------- ----------
---------- ---------- ---------
               693 eth0            Up          Active     Passive       Backup      0/0
```

```
        1/15       Ether
UCS-A#
```

ファブリック インターコネクトの退避ステータスの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope fabric-interconnect** {**a** | **b**}	指定したファブリック インターコネクトのファブリック インターコネクト モードを開始します。
ステップ 2	UCS-A /fabric-interconnect # **show detail**	指定されたファブリック インターコネクトに関する詳細を表示します。

例

次に、ファブリック インターコネクトの詳細なステータスを表示する例を示します。

（注） Admin Evacuation と Oper Evacuation はファブリック インターコネクトの退避ステータスを示します。

```
 UCS-A /fabric-interconnect # show detail

Fabric Interconnect:
    ID: B
    Product Name: Cisco UCS 6248UP
    PID: UCS-FI-6248UP
    VID: V01
    Vendor: Cisco Systems, Inc.
    Serial (SN): SSI171400HG
    HW Revision: 0
    Total Memory (MB): 16165
    OOB IP Addr: 10.193.32.172
    OOB Gateway: 10.193.32.1
    OOB Netmask: 255.255.255.0
    OOB IPv6 Address: ::
    OOB IPv6 Gateway: ::
    Prefix: 64
    Operability: Operable
    Thermal Status: Ok
    Admin Evacuation: On
    Oper Evacuation: On
    Current Task 1:
    Current Task 2:
    Current Task 3:
```

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 B480 M5 サーバ および 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 *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

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
UCS-PCI25-40010

ストレージ ディスク
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 *6:* 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 *7:* 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 *8:* 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。Cisco UCS M5 サーバの場合、安全なファームウェア アップデートがCisco UCS Managerリリース 3.2(2) で導入されています。

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、B200 M5、B480 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。

- Cisco UCS B200 M4 サーバでは、Cisco UCS Manager インフラストラクチャ ソフトウェア バンドルをアップグレードし、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) またはそれ以降のリリースにアップグレードします。Cisco UCS M5サーバの場合は、Cisco UCS Managerリリース 3.2(2) 以降のリリースにアップグレードします。

- Cisco UCS B200 M4、B200 M5 または B480 M5 サーバ上に 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。
- サーバを再認識します。『*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） 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 M44および M5サーバ、C480 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。

- サポートされている Cisco UCS M4 サーバでは、アップグレード、 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 ソフトウェアにバンドル Cisco UCS Manager リリース 3.1 (2) またはそれ以降のリリースです。Cisco UCS M5 サーバをアップグレード Cisco UCS Manager リリース 3.2(2) またはそれ以降のリリースです。
- 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） 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 （37 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。

- クラスタ構成の場合は、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ことが示されているかを確認します。
- スタンドアロン構成の場合、ファブリック インターコネクトの [全体のステータス（Overall Status）] が [操作可能（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ーについて、すべてのサーバーが検出され、検出が失敗しないことを確認します。サーバーエンドポイントがアップグレードできない場合、インストール サーバ ファームウェア が失敗します。
- 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 ゾーンを同一にする

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 ファームウェアをサーバ 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 ファームウェアを先にアップグレードし、次にサーバ 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 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 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

権限	実行できるアップグレード作業
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ー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、エンドポイントを手動でアップグレードしてそのサーバーのファームウェアを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 ドメイン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 Central にアップデートを展開する必要があります。
- Cisco UCS ドメイン 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 Central に適用されます。
- Cisco UCS ドメイン 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 Central 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 Manager 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有効にし、スケジュールを指定しない場合は、Cisco UCS Central 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ーの確認応答を有効にして、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

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、Cisco UCS ドメイン のすべてのエンドポイントが十分に機能し、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。再試行に最大回数失敗した FSM など、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。

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。
- クラスタ構成の場合は、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ことが示されているかを確認します。

- スタンドアロン構成の場合、ファブリック インターコネクトの [全体のステータス（Overall Status）] が [操作可能（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 （73 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、http://www.cisco.com/en/US/partner/products/ps11736/products_installation_and_configuration_guides_list.htmlCisco UCS Manager で管理するシステムにラックマウント サーバを設置および統合する方法については、該当する『C-Series Rack-Mount Server Integration Guide』の手順を参照してください。
- 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 リリース 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 プロファイルを再構成します。
  - ブート LUN が新しい IQN に認識されるように、各ネットワーク ストレージ デバイスで該当する IQN イニシエータ名を変更します。

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。

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **create backup** *URL* **all-configuration enabled**	**commit-buffer** コマンドを入力するとすぐに実行される、有効化された All Configuration バックアップ操作を作成します。 **all-configuration** オプションでは、サーバ関連、ファブリック関連、システム関連の設定をバックアップします 次のいずれかの構文を使用してバックアップするファイルの URL を指定します。 • **ftp:**// *username***@***hostname* / *path* • **scp:**// *username@hostname* / *path* • **sftp:**// *username@hostname* / *path* • **tftp:**// *hostname* **:** *port-num* / *path*
ステップ 3	UCS-A /system # **commit-buffer**	トランザクションをコミットします。

例

次の例では、SCP を使用して host35 という名前のホストに All Configuration バックアップ ファイルを作成し、トランザクションをコミットしています。

```
UCS-A# scope system
UCS-A /system* # create backup scp://user@host35/backups/all-config.bak all-configuration
 enabled
Password:
```

```
UCS-A /system* # commit-buffer
UCS-A /system #
```

Full State バックアップ ポリシーの構成

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として **/** を入力します。
ステップ 2	UCS-A /org # **scope backup-policy default**	All Configuration エクスポート ポリシー モードを開始します。
ステップ 3	UCS-A /org/backup-policy # **set hostname** {*hostname* | *ip-addr* | *ip6-addr*}	バックアップポリシーが格納されている場所のホスト名、IPv4 または IPv6 アドレスを指定します。これには、サーバー、ストレージアレイ、ローカル ドライブ、またはファブリック インターコネクトがネットワーク経由でアクセス可能な任意の読み取り/書き込みメディアなどがあります。

	コマンドまたはアクション	目的
		（注） IPv4 や IPv6 アドレスではなくホスト名を使用する場合、DNS サーバを設定する必要があります。Cisco UCS ドメインが Cisco UCS Central に登録されていないか、または DNS 管理が [ローカル（local）] に設定されている場合は、Cisco UCS Manager で DNS サーバを設定します。Cisco UCS ドメインが Cisco UCS Central に登録されていて、DNS 管理が [グローバル（global）] に設定されている場合は、Cisco UCS Central で DNS サーバを設定します。
ステップ 4	UCS-A /org/backup-policy # **set protocol** {**ftp** | **scp** | **sftp** | **tftp**}	リモート サーバーとの通信時に使用するプロトコルを指定します。
ステップ 5	UCS-A /org/backup-policy # **set user** *username*	システムがリモート サーバーへのログインに使用する必要のあるユーザー名を指定します。この手順は、TFTP プロトコルを使用する場合には適用されません。
ステップ 6	UCS-A /org/backup-policy # **set password**	**Enter** キーを押すと、パスワードを入力するように促されます。 リモート サーバーのユーザー名のパスワードを指定します。この手順は、TFTP プロトコルを使用する場合には適用されません。
ステップ 7	UCS-A /org/backup-policy # **set remote-file** *filename*	バックアップ ファイルのフルパスを指定します。このフィールドには、ファイル名とパスを含めることができます。ファイル名を省略すると、バックアップ手順によって、ファイルに名前が割り当てられます。
ステップ 8	UCS-A /org/backup-policy # **set adminstate** {**disable** | **enable**}	ポリシーの管理状態を指定します。次のいずれかになります。

	コマンドまたはアクション	目的
		• **[enabled]**：Cisco UCS Manager は、**[Schedule]** フィールドで指定されたスケジュールを使用してバックアップ ファイルをエクスポートします。 • **[disabled]**：Cisco UCS Manager はファイルをエクスポートしません。
ステップ 9	UCS-A /org/backup-policy # **set schedule** {**daily** | **weekly** | **bi-weekly**}	Cisco UCS Manager がバックアップ ファイルをエクスポートする頻度を指定します。
ステップ 10	UCS-A /org/backup-policy # **set descr** *description*	バックアップポリシーの説明を指定します。 256 文字以下で入力します。次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
ステップ 11	UCS-A /org/backup-policy # **commit-buffer**	トランザクションをコミットします。

例

次の例では、週単位のバックアップのための full state バックアップ ポリシーを設定し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org # scope backup-policy default
UCS-A /org/backup-policy # set hostname host35
UCS-A /org/backup-policy* # set protocol scp
UCS-A /org/backup-policy* # set user UserName32
UCS-A /org/backup-policy* # set password
Password:
UCS-A /org/backup-policy* # set remote-file /backups/full-state1.bak
UCS-A /org/backup-policy* # set adminstate enable
UCS-A /org/backup-policy* # set schedule weekly
UCS-A /org/backup-policy* # set descr "This is a full state weekly backup."
UCS-A /org/backup-policy* # commit-buffer
UCS-A /org/backup-policy #
```

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

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニターリング モードを開始します。
ステップ 2	UCS-A /monitoring # **scope callhome**	モニターリング Call Home モードを開始します。
ステップ 3	UCS-A /monitoring/callhome # **disable**	Call Home をイネーブルにします。
ステップ 4	UCS-A /monitoring/callhome # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、Smart Call Home を無効にし、トランザクションをコミットする例を示します。

```
UCS-A# scope monitoring
UCS-A /monitoring # scope callhome
UCS-A /monitoring/callhome # disable
UCS-A /monitoring/callhome* # commit-buffer
UCS-A /monitoring/callhome #
```

ファームウェア アップグレード中のフォールト抑制

障害抑制によって、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。障害抑制タスクを作成し、一時的な障害が発生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、障害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。フォールト抑制が終了した後に、Cisco UCS Manager がクリアされていない未処理の抑制された障害の通知を送信します。

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。

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、Cisco UCS Manager はファブリック インターコネクトの最後の再起動後に再確立されていないサービスをすべて表示します。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、未解決の障害の基準設定を作成します。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。この間隔は、「基準設定有効期限間隔」と呼ばれます。障害のベースライン有効期限の変更 （62ページ）、Cisco UCS Manager の基準設定の有効期限間隔を変更することに関する詳細情報を提供します。

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニターリング モードを開始します。
ステップ 2	UCS-A /monitoring # **scope fault policy**	モニターリング障害ポリシー モードを開始します。
ステップ 3	UCS-A /monitoring/fault-policy # **show**	障害ポリシーの詳細を表示します。

	コマンドまたはアクション	目的
ステップ 4	UCS-A /monitoring/fault-policy # **set baseline-expiration-interval** {*days hours minutes seconds*}	ベースライン有効期限を変更します。 デフォルトのベースライン有効期限は 24 時間です。 （注） ベースライン有効期限が切れると、すべての障害は新しい障害として表示されます。
ステップ 5	UCS-A /monitoring/fault-policy* # **commit**	トランザクションをコミットします。
ステップ 6	UCS-A /monitoring/fault-policy # **show**	障害ポリシーの詳細を表示します。

例

次に、障害のベースライン有効期限を変更する例を示します。

```
UCS-A# scope monitoring
UCS-A /monitoring # scope fault policy
UCS-A /monitoring/fault-policy # show

Fault Policy:
    Clear Action Clear Interval Retention Interval (dd:hh:mm:ss) Flap Interval (sec)
  Baseline Expiration Interval (dd:hh:mm:ss)
    ------------ -------------- ------------------------------- -----------------------
 ----------------------------------------
    Retain       00:00:20:00    00:01:00:00                     10
  10:00:00:12

UCS-A /monitoring/fault-policy # set baseline-expiration-interval 0 2 24 0
UCS-A /monitoring/fault-policy* # commit
UCS-A /monitoring/fault-policy # show

Fault Policy:
    Clear Action Clear Interval Retention Interval (dd:hh:mm:ss) Flap Interval (sec)
  Baseline Expiration Interval (dd:hh:mm:ss)
    ------------ -------------- ------------------------------- -----------------------
 ----------------------------------------
    Retain       10:00:00:00    01:01:01:01                     10
  00:02:24:00
UCS-A /monitoring/fault-policy #
```

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニターリング モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /monitoring # **show new-faults**	ベースライン化後、およびアップグレード中のファブリック インターコネクトのリブートにより生成された障害を示します。
ステップ 3	UCS-A /monitoring # **show baseline-faults**	アップグレード中のファブリック インターコネクトのリブート前にベースライン化された障害を示します。

例

次に、アップグレードプロセスのさまざまな段階で生成された障害を表示する方法の例を示します。

プライマリ ファブリック インターコネクトのリブート前の障害

```
UCS-A# show fault
Severity  Code     Last Transition Time     ID       Description
--------- -------- ----------------------- -------- -----------
Major     F0283    2015-06-17T21:08:09.301     57360 fc VIF 687 on server 1 / 6 of switch
 A  down, reason: NPV upstream port not available
Warning   F0156    2015-06-17T21:07:44.114     53557 Server, vendor(Cisco Systems Inc),
 model(N20-B6620-1), serial(QCI133400WR) in slot 1/3 presence: mismatch
Major     F0283    2015-06-16T21:02:33.014     72467 fc VIF 688 on server 1 / 6 of switch
 B  down, reason: NPV upstream port not available
Major     F0207    2015-06-15T22:40:11.636     57312 Adapter  host interface 1/6/1/1
link state: down
Major     F0479    2015-06-15T22:40:11.635     57311 Virtual interface 687 link state
is down
Major     F0207    2015-06-15T22:40:11.633     57310 Adapter  host interface 1/6/1/2
link state: down
Major     F0479    2015-06-15T22:40:11.632     57309 Virtual interface 688 link state
is down
```

プライマリ ファブリック インターコネクトのリブート後の障害

```
UCS-A# show fault
Severity  Code     Last Transition Time     ID       Description
--------- -------- ----------------------- -------- -----------
Major     F0209    2015-06-17T21:40:49.301     57760 Adapter uplink interface on server
 1 / 6 of switch A  down, Please verify the connectivity to Fabric Interconnect.
Major     F0207    2015-06-17T21:40:11.636     57712 Adapter  host interface 1/6/1/1
link state: down
Major     F0479    2015-06-17T21:40:11.635     57711 Virtual interface 685 link state
is down
Major     F0283    2015-06-17T21:08:09.301     57360 fc VIF 687 on server 1 / 6 of switch
 A  down, reason: NPV upstream port not available
Warning   F0156    2015-06-17T21:07:44.114     53557 Server, vendor(Cisco Systems Inc),
 model(N20-B6620-1), serial(QCI133400WR) in slot 1/3 presence: mismatch
Major     F0283    2015-06-16T21:02:33.014     72467 fc VIF 688 on server 1 / 6 of switch
 B  down, reason: NPV upstream port not available
Major     F0207    2015-06-15T22:40:11.636     57312 Adapter  host interface 1/6/1/1
link state: down
Major     F0479    2015-06-15T22:40:11.635     57311 Virtual interface 687 link state
is down
```

```
Major     F0207    2015-06-15T22:40:11.633     57310 Adapter  host interface 1/6/1/2
link state: down
Major     F0479    2015-06-15T22:40:11.632     57309 Virtual interface 688 link state
is down
```

プライマリ ファブリック インターコネクトのリブートにより生成された障害を表示する方法

```
UCS-A /monitoring # show new-faults
Severity  Code     Last Transition Time     ID       Description
--------- -------- ----------------------- -------- -----------
Major     F0209    2015-06-17T21:40:49.301     57760 Adapter uplink interface on server
 1 / 6 of switch A  down, Please verify the connectivity to Fabric Interconnect.
Major     F0207    2015-06-17T21:40:11.636     57712 Adapter  host interface 1/6/1/1
link state: down
Major     F0479    2015-06-17T21:40:11.635     57711 Virtual interface 685 link state
is down
```

プライマリ ファブリック インターコネクトのリブート前の障害を表示する方法

```
UCS-A# show baseline-faults
Severity  Code     Last Transition Time     ID       Description
--------- -------- ----------------------- -------- -----------
Major     F0283    2015-06-17T21:08:09.301     57360 fc VIF 687 on server 1 / 6 of switch
 A  down, reason: NPV upstream port not available
Warning   F0156    2015-06-17T21:07:44.114     53557 Server, vendor(Cisco Systems Inc),
 model(N20-B6620-1), serial(QCI133400WR) in slot 1/3 presence: mismatch
Major     F0283    2015-06-16T21:02:33.014     72467 fc VIF 688 on server 1 / 6 of switch
 B  down, reason: NPV upstream port not available
Major     F0207    2015-06-15T22:40:11.636     57312 Adapter  host interface 1/6/1/1
link state: down
Major     F0479    2015-06-15T22:40:11.635     57311 Virtual interface 687 link state
is down
Major     F0207    2015-06-15T22:40:11.633     57310 Adapter  host interface 1/6/1/2
link state: down
Major     F0479    2015-06-15T22:40:11.632     57309 Virtual interface 688 link state
is down
```

ファブリック インターコネクトの動作の確認

Cisco UCS ドメイン をハイ アベイラビリティ クラスタ設定で実行する場合は、両方のファブリック インターコネクトの動作を確認する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fabric-interconnect** {**a** | **b**}	指定したファブリック インターコネクトのファブリック インターコネクト モードを開始します。
ステップ 2	UCS-A /fabric-interconnect # **show**	ファブリック インターコネクトの情報を表示します。

	コマンドまたはアクション	目的
		ファブリック インターコネクトの動作が Operable 状態であることを確認します。動作可能な状態でない場合は、**show tech-support** コマンドを実行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。**show tech-support** コマンドの詳細については、『*Cisco UCS Manager B-Series Troubleshooting Guide*』を参照してください。

例

次の例では、両方のファブリック インターコネクトの動作が Operable 状態として表示されています。

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect # show
Fabric Interconnect:
    ID OOB IP Addr     OOB Gateway     OOB Netmask     Operability
    -- --------------- --------------- --------------- -----------
    A  192.168.100.10  192.168.100.20  255.255.255.0   Operable

UCS-A /fabric-interconnect # exit
UCS-A# scope fabric-interconnect b
UCS-A /fabric-interconnect # show
Fabric Interconnect:
    ID OOB IP Addr     OOB Gateway     OOB Netmask     Operability
    -- --------------- --------------- --------------- -----------
    B  192.168.100.11  192.168.100.20  255.255.255.0   Operable
```

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **show cluster state**	ハイ アベイラビリティ クラスタの両方のファブリック インターコネクトの動作状態およびリーダーシップ ロールを表示します。 両方のファブリック インターコネクト（A および B）が Up 状態であること、および HA が Ready 状態であることを確

	コマンドまたはアクション	目的
		認します。ファブリック インターコネクトが Up 状態でない場合、または HA が Ready 状態でない場合、 **show tech-support** コマンドを実行し、シスコ テクニカル サポートにお問い合わせください。ファームウェア アップグレードに進まないでください。 **show tech-support** コマンドの詳細については、『*Cisco UCS Troubleshooting Guide*』を参照してください。 また、どのファブリック インターコネクトがプライマリ ロールで、どのファブリック インターコネクトが従属ロールであるかにも注目してください。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この情報が必要です。

例

次の例の表示では、両方のファブリック インターコネクトが Up 状態、HA が Ready 状態、ファブリックインターコネクトAがプライマリ ロール、ファブリックインターコネクト B が従属ロールです。

```
UCS-A# show cluster state
Cluster Id: 0x4432f72a371511de-0xb97c000de1b1ada4

A: UP, PRIMARY
B: UP, SUBORDINATE

HA READY
```

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

始める前に

このメンテナンス ポリシーを遅延展開のために設定する場合は、スケジュールを作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、[org-name] に **/** を入力します。
ステップ 2	UCS-A /org # **scope maint-policy default**	デフォルト メンテナンス ポリシーのメンテナンス ポリシー モードを開始します。
ステップ 3	UCS-A /org/maint-policy # **set reboot-policy** {**immediate** | **timer-automatic** | **user-ack**}	サービス プロファイルがサーバーに関連付けられている場合、関連付けを完了するにはサーバーをリブートする必要があります。reboot-policy コマンドを指定すると、このメンテナンス ポリシーを含むすべてのサービス プロファイルについて発生するタイミングを決定できます。有効な値は次のとおりです。 • **immediate**：サービス プロファイルが変更されると、すぐにサーバーがリブートします。 • **timer-automatic** ：**set scheduler** コマンドを使用して、メンテナンス操作が適用されるタイミングを指定するスケジュールを選択できます。スケジュールした時間に Cisco UCS によってサーバーがリブートされ、サービスプロファイルの変更が完了します。 • **user-ack** ：ユーザーは、変更が適用される前に **apply pending-changes** コマンドを使用して変更を明示的に確認する必要があります。

	コマンドまたはアクション	目的
		デフォルト メンテナンス ポリシーのリブート ポリシーを **user-ack** に設定することを推奨します。
ステップ 4	（任意） UCS-A /org/maint-policy # **set scheduler** *scheduler-name*	reboot-policy プロパティが timer-automatic に設定された場合、メンテナンス操作がサーバーに適用されるタイミングを指定するスケジュールを選択する必要があります。スケジュールした時間に Cisco UCS によってサーバーがリブートされ、サービスプロファイルの変更が完了します。
ステップ 5	UCS-A /org/maint-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、デフォルト メンテナンス ポリシーのリブート ポリシーを変更し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # scope maint-policy default
UCS-A /org/maint-policy* # set reboot-policy user-ack
UCS-A /org/maint-policy* # commit-buffer
UCS-A /org/maint-policy #
```

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 モニタリング モードを開始します。

UCS-A# **scope monitoring**

ステップ 2 管理インターフェイス モニタリング ポリシーをイネーブルにするか、ディセーブルにします。

UCS-A /monitoring # **set mgmt-if-mon-policy admin-state** {**enabled** | **disabled**}

ステップ 3 UCS-A /monitoring # **commit-buffer**

トランザクションをシステムの設定にコミットします。

ステップ 4 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 5 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 6 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。

例

次に、管理インターフェイス モニタリング ポリシーを無効にし、トランザクションをコミットする例を示します。

```
UCS-A# scope monitoring
UCS-A /monitoring # set mgmt-if-mon-policy admin-state enabled
UCS-A /monitoring* # commit-buffer
UCS-A /monitoring #
```

I/O モジュールのステータスの確認

Cisco UCS がハイ アベイラビリティ クラスタ設定で実行されている場合、すべてのシャーシで両方の I/O モジュールのステータスを確認する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope chassis** *chassis-id*	指定したシャーシでシャーシ モードを開始します。
ステップ 2	UCS-A /chassis # **scope iom** *iom-id*	選択した I/O モジュールでシャーシ I/O モジュール モードを開始します。
ステップ 3	UCS-A # **show**	指定したシャーシの指定した I/O モジュールのステータスを表示します。 I/O モジュールの全体的なステータスが Operable 状態であることを確認します。

	コマンドまたはアクション	目的
		全体的なステータスが Operable 状態ではない場合、 **show tech-support** コマンドを実行し、シスコ テクニカル サポートにお問い合わせください。ファームウェア アップグレードに進まないでください。 **show tech-support** コマンドの詳細については、『*Cisco UCS Troubleshooting Guide*』を参照してください。

例

次の例では、シャーシ 1 の両方の I/O モジュールの全体的なステータスが Operable 状態として表示されています。

```
UCS-A# scope chassis 1
UCS-A /chassis # scope iom 1
UCS-A /chassis/iom # show
IOM:
    ID         Side  Fabric ID Overall Status
    ---------- ----- --------- --------------
             1 Left  A         Operable

UCS-A /chassis/iom # exit
UCS-A /chassis # scope iom 2
UCS-A /chassis/iom # show
IOM:
    ID         Side  Fabric ID Overall Status
    ---------- ----- --------- --------------
             2 Right B         Operable
```

サーバのステータスの確認

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *chassis-id / server-id*	指定したシャーシの指定したサーバについて、シャーシのサーバ モードを入力します。
ステップ 2	UCS-A /chassis/server # **show status detail**	サーバのステータスの詳細を表示します。 サーバの全体的なステータスが Ok、Unavailable、または障害を示さない値か確認します。全体的なステータスが障害を示す状態（Discovery Failed など）の

	コマンドまたはアクション	目的
		場合、そのサーバのエンド ポイントはアップグレードできません。

例

次の例では、シャーシ 1 のサーバ 7 の全体的なステータスが Ok 状態として表示されています。

```
UCS-A# scope server 1/7
UCS-A /chassis/server # show status detail
Server 1/7:
    Slot Status: Equipped
    Conn Path: A,B
    Conn Status: A,B
    Managing Instance: B
    Availability: Unavailable
    Admin State: In Service
    Overall Status: Ok
    Oper Qualifier: N/A
    Discovery: Complete
    Current Task:
```

シャーシのサーバのアダプタのステータスの確認

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *chassis-id / server-id*	指定したシャーシ内の指定したサーバでシャーシ サーバ モードを開始します
ステップ 2	UCS-A /chassis/server # **show adapter status**	アダプタのステータスを表示します。 アダプタの全体的なステータスがOperable状態であることを確認します。アダプタの全体的なステータスがOperable以外の状態にある場合は、アップグレードできません。ただし、Cisco UCS ドメイン 内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。

例

次の例では、シャーシ 1 のサーバ 7 のアダプタの全体的なステータスが Operable 状態として表示されています。

```
UCS-A# scope server 1/7
UCS-A /chassis/server # show adapter status
```

```
Server 1/1:
    Overall Status
    --------------
    Operable
```

UCS Manager の正常性およびアップグレード前チェック ツール

UCS Manager の正常性およびアップグレード前チェック ツールは、アップグレード前にクラスタが正常であることを確認するために設計された、自動正常性およびアップグレード前チェック機能を提供します。この健全性チェックを実行するだけでなく、正常でないと判明したすべてのクラスタに対して修正措置を講じることが必要です。続行する前に、UCS Manager 正常性チェックによって報告されたすべての問題を修正してください。

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 [ナビゲーション]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	ファブリック インターコネクトに基づいて、次のいずれかを実行します。 **オプション** / **説明** **show platform fwm info hw-stm | grep '1.' | wc –l** — UCS 6200 シリーズ、UCS 6332、および UCS 6332-16UP ファブリック インターコネクトの MAC アドレスの合計数を返します。 **show hardware internal libsdk mtc l2 mac-table-ce valid-only | egrep "^ *[0-9]" | wc -l** — UCS 6324 (UCS ミニ) ファブリック インターコネクトの MAC アドレスの合計数を返します。 **show hardware mac address-table 1 | wc -l** — UCS 6400 シリーズ ファブリック インターコネクトの 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。

例

次の例では、従属 UCS 6332 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
```

次の例では、従属 UCS 6400 シリーズ 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 hardware mac address-table 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。

例

次の例では、flogi テーブルおよび従属ファブリック インターコネクト A にログインしたサーバの数が返され、ファブリック インターコネクトのファイバ チャネル データ パスがファイバ チャネル エンドホスト モードで稼働していることを確認できます。

```
UCS-A /fabric-interconnect # connect nxos a
UCS-A(nxos)# show npv flogi-table
```

```
--------------------------------------------------------------------------------
SERVER                                                                  EXTERNAL
INTERFACE VSAN FCID            PORT NAME               NODE NAME        INTERFACE
--------------------------------------------------------------------------------
vfc705    700  0x69000a 20:00:00:25:b5:27:03:01 20:00:00:25:b5:27:03:00 fc3/1
vfc713    700  0x690009 20:00:00:25:b5:27:07:01 20:00:00:25:b5:27:07:00 fc3/1
vfc717    700  0x690001 20:00:00:25:b5:27:08:01 20:00:00:25:b5:27:08:00 fc3/1

Total number of flogi = 3.

UCS-A(nxos)# show npv flogi-table | grep fc | wc -l
3
```

ファイバ チャネル スイッチ モードのデータ パスの確認

Cisco UCS ドメインのアップグレード時に最適な結果を得るためには、アップグレードを開始する前、および従属ファブリック インターコネクトをアクティブ化した後にこのタスクを実行し、2 つの結果を比較することを推奨します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A /fabric-interconnect # **connect nxos** {**a** | **b**}	ファブリック インターコネクトの NX-OS モードを開始します。
ステップ 2	UCS-A(nxos)# **show flogi database**	flogi セッションのテーブルを表示します。
ステップ 3	UCS-A(nxos)# **show flogi database | grep –I fc | wc –1**	ファブリック インターコネクトにログインしたサーバの数を返します。 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。

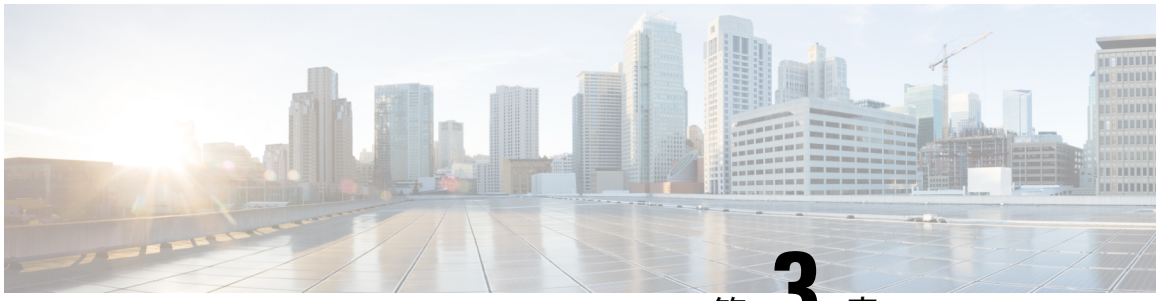
例

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、イメージのバンドル内の Cisco UCS コンポーネントに、すべてのファームウェア アップデートを提供します。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 4.0 以降のリリースには、4 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。

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

Note Cisco UCS 6400 シリーズ ファブリック インターコネクトには、個別のキック スタートイメージとシステムイメージがありません。

Note 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、UCS 6300 シリーズ 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 6400 シリーズ ファブリック インターコネクト をアクティブに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となる、次のファームウェアイメージが含まれます。リリース用に作成された最新のバンドルに加えて、最新のインフラストラクチャ バンドルに含まれないブレード サーバに対して Cisco UCS Manager をイネーブルにするために、次のバンドルもリリースされる場合があります。

- 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 と統合されその管理を受けているラックマウント サービスのコンポーネントの更新に必要な、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

Note 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。これらのサーバのファームウェア管理システムは、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 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。

Tip 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

Before you begin

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 6400 シリーズ ファブリック インターコネクト、6300 シリーズ ファブリック インターコネクト、6200 シリーズ ファブリック インターコネクト、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 サーバーを含むすべての Cisco UCS ドメイン に必要。
- 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：統合ラックマウント サーバーを含む Cisco UCS ドメインにのみ必要。このバンドルには、Cisco UCS Managerを使用してこれらのサーバーを管理するためのファームウェアが含まれています。このバンドルはスタンドアロンの C シリーズ ラックマウント サーバーには適用できません。

Procedure

ステップ 1 Web ブラウザで、Cisco.com を参照します。

ステップ 2 [サポート（Support）] で [すべてをダウンロード（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 のユーザー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。

作成	ナビゲーション パス
Cisco UCS 6400 シリーズ ファブリック インターコネクト、6300 シリーズ ファブリック インターコネクト、6200 シリーズ ファブリック インターコネクト、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。

作成	ナビゲーション パス
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。

Tip これらのパスからアクセスできる Unified Computing System（UCS）ドキュメント ロードマップ バンドルは、すべての Cisco UCS ドキュメントを含む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、[リリース ノート（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 4.0 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。

- [今すぐダウンロード（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。
- [カートに追加（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 ノートをお読みください。

What to do next

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

Note 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。

Before you begin

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。

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope firmware**	ファームウェア モードを開始します。
ステップ 2	UCS-A /firmware # **download image** *URL*	ファームウェア バンドルをダウンロードします。シスコから提供されたダウンロード パスを使用し、次のいずれかの構文で URL を指定します。 • **ftp://** *server-ip-addr* **/** *path* • **scp://**username@server-ip-addr/ **/** *path* • **sftp://**username@server-ip-addr/ **/** *path* • **tftp://**server-ip-addr**:** *port-num* **//** {5}path{5} **Note** [TFTP] ではファイル サイズが 32 MB に制限されます。ファームウェア バンドルはそれよりも大幅に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推奨します。 • **usbA:/** *path*

	Command or Action	Purpose
		• **usbB:**/ *path* **Note** 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。 **Note** IP アドレスではなくホスト名を使用する場合、Cisco UCS Managerで DNS サーバを設定します。
ステップ 3	リモート サーバのパスワードを入力します。	リモート サーバのユーザ名のパスワード。プロトコルが tfpt の場合、このフィールドは適用されません。
ステップ 4	UCS-A /firmware # **show download-task**	ダウンロード タスクのステータスを表示します。イメージのダウンロードが完了すると、タスク状態が Downloading から Downloaded に変更されます。CLI の表示は自動的には更新されないので、タスクのステータスに Downloaded が表示されるまで何度も **show download-task** コマンドを入力する必要があります。
ステップ 5	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。	

Example

次に、SCP を使用してファームウェア パッケージをダウンロードする例を示します。

```
UCS-A# scope firmware
UCS-A /firmware # download image
scp://user1@111.100.10.10/images/ucs-k9-bundle.4.0.1.988.bin
OR
download image usbB:/username/ucs-k9-bundle-b-series.4.0.1a.B.bin
```

```
UCS-A /firmware # show download-task
UCS-A /firmware #
```

What to do next

ファームウェア バンドル イメージ ファイルのダウンロードが完了したら、エンドポイント上でファームウェアを更新します。

ファームウェア パッケージのダウンロード ステータスの表示

ファームウェアのダウンロード操作が開始された後、パッケージがまだダウンロード中か、または完了したか判別するために、ダウンロード ステータスを確認できます。

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope firmware**	ファームウェア モードを開始します。
ステップ 2	UCS-A /firmware # **show download-task**	ダウンロード タスクのステータスを表示します。イメージのダウンロードが完了すると、タスク状態が Downloading から Downloaded に変更されます。CLI の表示は自動的には更新されないので、タスクのステータスに Downloaded が表示されるまで何度も **show download-task** コマンドを入力する必要があります。

Example

次に、ファームウェア パッケージのダウンロード ステータスを表示する例を示します。ダウンロード状態によりファームウェア パッケージのダウンロードが完了したことが示されるまで、 **show download-task** コマンドの入力を続けます。

```
UCS-A# scope firmware
UCS-A /firmware # show download-task

Download task:
File Name                                 Protocol   Server           Userid      State
---------                                 --------   ---------------  ---------   -----
ucs-mini-k9-bundle-infra.4.0.1a.A.bin  Scp       100.100.100.10   user1       Downloading

UCS-A /firmware # show download-task

Download task:
File Name                                 Protocol   Server           Userid      State
---------                                 --------   ---------------  ---------   -----
ucs-mini-k9-bundle-infra.4.0.1a.A.bin  Scp       100.100.100.10   user1       Downloading

UCS-A /firmware # show download-task

Download task:
```

```
File Name                                 Protocol   Server           Userid      State
---------                                 --------   ---------------  ---------   -----
ucs-mini-k9-bundle-infra.4.0.1a.A.bin  Scp       100.100.100.10    user1      Downloaded
```

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope firmware**	ファームウェア モードを開始します。
ステップ 2	UCS-A /firmware # **delete download-task** *image_filename*	指定されたイメージ ファイルを削除します。
ステップ 3	UCS-A /firmware # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、イメージのダウンロードを取り消します。

```
UCS-A# scope firmware
UCS-A /firmware # delete download-task ucs-k9-bundle-b-series.4.0.1a.B.bin
UCS-A /firmware* # commit-buffer
UCS-A /firmware*
```

ファブリック インターコネクトの利用可能なすべてのソフトウェア イメージの表示

この手順は任意で、すべてのエンドポイントのファブリック インターコネクトの使用可能なソフトウェア イメージを表示します。各エンドポイント モードでの **show image** コマンドの使用によっても、エンドポイントの使用可能なソフトウェア イメージを表示できます。

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope firmware**	ファームウェア モードを開始します。

	Command or Action	Purpose
ステップ 2	UCS-A /firmware # **show image**	ファブリック インターコネクトにダウンロードされたすべてのソフトウェア イメージが表示されます。 **Note** エンドポイントを直接アップデートする場合、ソフトウェア バージョン番号を指定する必要があります。エンドポイントでファームウェアを直接アップデートする場合、右の列のバージョン番号に注意してください。

Example

次に、ファブリック インターコネクトの使用可能なすべてのソフトウェア イメージを表示する例を示します。

```
UCS-A# scope firmware
UCS-A /firmware # show image

Name                                       Type                 Version
------------------------------------------ -------------------- -------
ucs-2200.3.2.2cS2.gbin                     Chassis Adaptor      3.2(2cS2)
ucs-2200.4.0.0.46.gbin                     Chassis Adaptor      4.0(0.46)
ucs-3260.3.0.4d.gbin                       Chassis Management Controller
                                                                3.0(4d)
ucs-3260.4.0.0.149.gbin                    Chassis Management Controller
                                                                4.0(0.149)
ucs-3260.4.0.0.155.gbin                    Chassis Management Controller
                                                                4.0(0.155)
ucs-6100-k9-kickstart.5.0.3.N2.3.22cS2.gbin   Fabric Interconnect Kernel
                                                                5.0(3)N2(3.22cS2)
ucs-6100-k9-kickstart.5.0.3.N2.4.00.46.gbin   Fabric Interconnect Kernel
                                                                5.0(3)N2(4.00.46)
ucs-6100-k9-system.5.0.3.N2.3.22cS2.gbin      Fabric Interconnect System
                                                                5.0(3)N2(3.22cS2)
ucs-6100-k9-system.5.0.3.N2.4.00.46.gbin      Fabric Interconnect System
                                                                5.0(3)N2(4.00.46)
ucs-adaptor-pcie-ucsc-pcie-x710ta4.800031CA-1.812.1.gbin
                                           Adapter              800031CA-1.812.1
ucs-adaptor-pcie-ucsc-pcie-xxx710da2.8000364C-1.812.1.gbin
                                           Adapter              8000364C-1.812.1
ucs-bmc-brdprog-S3260M5.2.0.gbin           Board Controller     2.0


...
```

ファブリックインターコネクトの利用可能なすべてのパッケージの表示

この手順は任意で、すべてのエンドポイントのファブリック インターコネクトの使用可能なソフトウェア パッケージを表示します。各エンドポイント モードでの **show package** コマンドの使用によっても、エンドポイントの使用可能なソフトウェア イメージを表示できます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope firmware**	ファームウェア モードを開始します。
ステップ 2	UCS-A /firmware # **show package**	ファブリック インターコネクトにダウンロードされたすべてのソフトウェア パッケージが表示されます。 （注） エンドポイントを直接アップデートする場合、ソフトウェア バージョン番号を指定する必要があります。エンドポイントでファームウェアを直接アップデートする場合、右の列のバージョン番号に注意してください。

例

次に、ファブリック インターコネクトの使用可能なすべてのソフトウェア パッケージを表示する例を示します。

```
UCS-A# scope firmware
UCS-A /firmware # show package
Name                                       Version
------------------------------------------ -------
ucs-c125-bios.C125.4.0.0.15.0504180159.gbin
ucs-c125-bios.C125.4.0.0.17.0518180446.gbin
ucs-c125-k9-cimc.4.0.0.130.gbin
ucs-c125-k9-cimc.4.0.0.149.gbin
ucs-k9-bundle-c-series.3.1.3h.C.gbin       3.1(3h)C
ucs-k9-bundle-c-series.4.0.0.112.C.gbin    4.0(0.112)C
ucs-k9-bundle-c-series.4.0.0.115.C.gbin    4.0(0.115)C
ucs-k9-bundle-infra.3.2.2eS9.A.gbin        3.2(2eS9)A
ucs-k9-bundle-infra.4.0.0.57.A.gbin        4.0(0.57)A
ucs-manager-k9.4.0.0.8769.gbin
ucs-manager-k9.4.0.0.8777.gbin
ucs-manager-k9.4.0.0.8911.gbin
```

ファームウェア パッケージの内容の判断

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope firmware**	ファームウェア モードを開始します。
ステップ 2	UCS-A /firmware # **show package** *package-name* **expand**	指定したファームウェア パッケージの内容を表示します。

例

次に、ファームウェア パッケージの内容を表示する例を示します。

```
UCS-A# scope firmware
UCS-A /firmware # show package ucs-k9-bundle-infra.4.0.0.57.A.gbin expand
Package ucs-k9-bundle-infra.4.0.0.57.A.gbin:
    Images:
        ucs-2200.4.0.0.46.gbin
        ucs-6100-k9-kickstart.5.0.3.N2.4.00.46.gbin
        ucs-6100-k9-system.5.0.3.N2.4.00.46.gbin
        ucs-manager-k9.4.0.0.56b.gbin
```

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fabric-interconnect** {**a** | **b**}	指定したファブリックのファブリック インターコネクト モードを開始します。
ステップ 2	UCS-A /fabric-interconnect # **show storage** [**detail** | **expand**}	指定したファブリックの空き領域を表示します。

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

例

次の例は、ファブリック インターコネクトの空き領域を表示します。

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect # show storage
Storage on local flash drive of fabric interconnect:
    Partition        Size (MBytes)    Used Percentage
    ---------------- ---------------- ---------------
    bootflash        16342            81
    opt              3873             3
    spare            5759             2
    usbdrive         Nothing          Empty
    var_sysmgr       2000             24
    var_tmp          600              2
    volatile         240              Empty
    workspace        3848             6
UCS-A /fabric-interconnect #
```

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、インフラストラクチャ コンポーネントをアップグレードします。ファームウェア イメージの管理 （79 ページ）はCisco UCS Managerリリース 4.0。の使用可能なインフラストラクチャ ソフトウェア バンドルに関する詳細を提供します。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

（99 ページ）では、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に関して Cisco が推奨するプロセスを説明しています。

- シャーシ ファームウェアのインストール] を使用して、 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 シャーシのコンポーネント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：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 のバージョンにアップグレードし、 シャーシと 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 Release 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 （51 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。

後の直接アップグレード 自動インストール

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。Cisco UCS Manager後に自動インストール、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 バージョンが構成されている場合、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 （107 ページ） は、スタートアップ バージョンをクリアするための詳細な手順を提供します。

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/
```

ファームウェア インストールの準備

自動インストールを使用して、Cisco UCS ドメインを単一のパッケージに含まれているファームウェア バージョンにアップグレードできます。自動インストールでは、3つの独立した段階でファームウェアをインストールする機能を提供:インフラストラクチャ ファームウェアのインストール、シャーシ ファームウェアのインストール、およびサーバ ファームウェアのインストール。自動インストール中に、IOM、アダプタ、BIOS、CIMCなどの一部のエンドポイントのファームウェアが最初に更新されてからアクティブになります。

エンドポイントのファームウェアを更新するには、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 パーティションにステージングする必要があります。更新フェーズでは、エンドポイントの再起動は不要です。アクティブ化の段階で、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。したがって、自動インストールプロセスを完了するのにかかる時間には、次のことを実行するために必要な時間が含まれます。

- すべてのエンドポイントのバックアップ パーティションにファームウェアを更新またはステージングする

（注） 自動インストール完了に費やされる時間の大半は、この処理です。

- すべてのエンドポイント上でファームウェアをアクティブ化します。
- 該当するすべてのエンドポイントを再起動します。

Cisco UCS Managerリリース 3.2(3) では、インフラストラクチャ、サーバコンポーネント、およびS3260 シャーシファームウェアを同時にアップデートまたはステージングし、アクティベーション プロセスから独立させることができます。ステージング ファームウェアにはエンドポイントの再起動は含まれないため、この機能を使用すると、メンテナンス期間を待たずにすべてのエンドポイントでファームウェアをステージングできます。その結果、自動インストールプロセスの完了にかかる時間には、ファームウェアをすべてのエンドポイントのバックアップパーティションにステージングするのにかかる時間が含まれなくなりました。したがって、メンテナンスに必要な停止時間を大幅に減らすことができます。

自動インストールを実行する前にこの機能を使用してファームウェアをステージングする場合は、バックアップの更新をスキップしてファームウェアのアクティブ化とエンドポイントの再起動を続行できます。この機能を使用してエンドポイントにファームウェアをステージングしない場合は、自動インストールを引き続き使用してコンポーネントを更新してアクティブ化することができます。エンドポイントのバックアップ パーティションにファームウェアをステージングする機能によって、コンポーネントのファームウェアを更新してアクティブ化するための自動インストールの従来の機能が変わることはありません。

インフラストラクチャ ファームウェア パックのインストールの準備

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として **/** を入力します。
ステップ 2	UCS-A /org # **scope fw-infra-pack** *name*	組織インフラストラクチャ ファームウェア ポリシー モードを開始します。
ステップ 3	UCS-A /org/fw-infra-pack # **scope fw-backup-version infra**	インフラストラクチャのバックアップ ファームウェア モードを開始します。
ステップ 4	UCS A/org/fw-infra-pack/fw-backup-version # **set bundle-vers** *firmware_version*	指定のファームウェアバージョンをバックアップ インフラストラクチャ ファームウェアバージョンとして設定します。

	コマンドまたはアクション	目的
ステップ 5	UCS-A /org/fw-infra-pack/fw-backup-version* # **commit-buffer**	トランザクションをコミットします。

例

この例では、バックアップインフラストラクチャ ファームウェアバージョンを設定する方法を示します。

```
UCS-A# scope org
UCS-A /org # scope fw-infra-pack default
UCS-A /org/fw-infra-pack # scope fw-backup-version infra
UCS-A /org/fw-infra-pack/fw-backup-version # set bundle-vers 4.0(1a)A
UCS-A /org/fw-infra-pack/fw-backup-version* # commit-buffer
```

シャーシ ファームウェア パックのインストールの準備

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として **/** を入力します。
ステップ 2	UCS-A /org # **scope fw-chassis-pack** *name*	組織シャーシ ファームウェア ポリシー モードを開始します。
ステップ 3	UCS A/org/fw-chassis-pack # **scope fw-backup-version chassis**	シャーシのバックアップ ファームウェア モードを開始します。
ステップ 4	UCS-A /org/fw-chassis-pack/fw-backup-version # **set bundle-vers** *firmware_version*	バックアップ シャーシ ファームウェア バージョンとして指定されたファームウェアバージョンを設定します。
ステップ 5	UCS A/org/fw-chassis-pack/fw-backup-バージョン * # **commit-buffer**	トランザクションをコミットします。

例

この例では、バックアップ シャーシ ファームウェアバージョンを設定する方法を示します。

```
UCS-A# scope org
UCS-A /org # scope fw-chassis-pack default
```

```
UCS-A /org/fw-chassis-pack # scope fw-backup-version chassis
UCS-A /org/fw-chassis-pack/fw-backup-version # set bundle-vers 4.0(1a)C
UCS-A /org/fw-chassis-pack/fw-backup-version* # commit-buffer
```

インストールのブレードのホスト ファームウェア パックの準備

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として / を入力します。
ステップ 2	UCS-A /org # **scope fw-host-pack** *name*	組織ホスト ファームウェア ポリシー モードを開始します。
ステップ 3	UCS A/org/fw-host-pack # **scope fw-backup-version blade**	ブレード サーバのバックアップ ファームウェア モードを開始します。
ステップ 4	UCS-A /org/fw-host-pack/fw-backup-version # **set bundle-vers** *firmware_version*	ファームウェアバージョン ブレード サーバのバックアップのホストとして指定されたファームウェアバージョンを設定します。
ステップ 5	UCS A/org/fw-host-pack/fw-backup-バージョン * # **commit-buffer**	トランザクションをコミットします。

例

この例では、ブレード サーバのバックアップ ホスト ファームウェアバージョンを設定する方法を示します。

```
UCS-A# scope org
UCS-A /org # scope fw-host-pack default
UCS-A /org/fw-host-pack # scope fw-backup-version blade
UCS-A /org/fw-host-pack/fw-backup-version # set bundle-vers 4.0(1a)B
UCS-A /org/fw-host-pack/fw-backup-version* # commit-buffer
```

インストールのラック ホスト ファームウェア パックの準備

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として / を入力します。
ステップ 2	UCS-A /org # **scope fw-host-pack** *name*	組織ホスト ファームウェア ポリシー モードを開始します。
ステップ 3	UCS A/org/fw-host-pack # **scope fw-backup-version rack**	ラックマウント サーバのバックアップ ファームウェア モードを開始します。
ステップ 4	UCS-A /org/fw-host-pack/fw-backup-version # **set bundle-vers** *firmware_version*	ラックマウント サーバのバックアップのホスト ファームウェア バージョンとして指定されたファームウェアバージョンを設定します。
ステップ 5	UCS A/org/fw-host-pack/fw-backup-バージョン * # **commit-buffer**	トランザクションをコミットします。

例

この例では、ラックマウント サーバのバックアップ ホスト ファームウェア バージョンを設定する方法を示します。

```
UCS-A# scope org
UCS-A /org # scope fw-host-pack default
UCS-A /org/fw-host-pack # scope fw-backup-version rack
UCS-A /org/fw-host-pack/fw-backup-version # set bundle-vers 4.0(1a)C
UCS-A /org/fw-host-pack/fw-backup-version* # commit-buffer
```

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。
    1. 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 （57 ページ） と Full State バックアップ ポリシーの構成 （58 ページ） では詳細情報を提供します。
    2. 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 （84 ページ）は詳細な情報を提供します。
    3. Cisco UCS Manager リリース 3.2(3) または以降のリリースを使用している場合は、インフラストラクチャのファームウェアをステージングします。インフラストラクチャ ファームウェア パックのインストールの準備 （94 ページ）は、インフラストラクチャ ファームウェアのステージングに関する詳細情報を提供します。

（注） この手順はオプションですが、これもお勧めします。

    4. Smart Call Home を無効にします。Smart Call Home の無効化 （61 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。
    1. 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。
    2. 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 （66 ページ） は詳細情報を提供します。
    3. デフォルト 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 （67 ページ） には、メンテナンス ポリシーに関する詳細情報と、デフォルトのメンテナンス ポリシーを **[User-Ack]** に設定する方法が掲載されています。
    4. VLAN と FCOE ID が重複していないことを確認します。
    5. 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 （69 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。
    6. すべてのパスが機能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 （73 ページ）詳細な情報を提供します。

3. 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（100ページ）
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 （63 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。
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 （105 ページ） は詳細情報を提供します。
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ファームウェアのアップグレード

Cisco UCS Manager CLI のリリースが 2.1(1) よりも古い場合、**auto-install** 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 Release 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 （51 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。

始める前に

- にリストされているすべての前提条件を満たす必要があります。ファームウェアのアップグレードとダウングレードの前提条件 （55 ページ）

- Cisco UCS Manager リリース 3.2(3) または以降のリリースを使用している場合は、インフラストラクチャのファームウェアをステージングします。インフラストラクチャ ファームウェア パックのインストールの準備 （94 ページ）は、インフラストラクチャ ファームウェアのステージングに関する詳細情報を提供します。

（注） この手順はオプションですが、これもお勧めします。

Cisco UCS ドメインで NTP サーバを使用して時刻を設定しない場合、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クロックを必ず同期させてください。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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope firmware**	ファームウェア モードを開始します。
ステップ 2	UCS-A /firmware # **scope auto-install**	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自動インストール モードを開始します。
ステップ 3	UCS A/firmware/auto-install # **install infra infra-vers** *infrastructure-bundle-version* **servicepack-vers** *servicepack-bundle-version*[**starttime** *mon dd yyyy hh min sec*[**force**] [**evacuate**] [**skipvalidation**]	インフラストラクチャ ファームウェアおよびサービス パック バンドルを更新してアクティブ化します。 即座にアップグレードを開始したくない場合は、**starttime** を使用してインフラストラクチャ ファームウェアのアップグレードをスケジュールする必要があります。**starttime** を使用する場合は、アップグレードをいつスケジュールするかを指定するために、次の情報を入力してください。 • *mon*：jan や feb など目的の月の名前の最初の 3 文字。 • *dd*：月の目的の日（1 ～ 31）。 • *yyyy*：2012 などの目的の年（西暦）。 • *hh*：アップグレードを開始する時刻の時（0 ～ 23）。

	コマンドまたはアクション	目的
		• *min*：アップグレードを開始する時刻の分（0 ～ 60）。 • *sec*：アップグレードを開始する時刻の秒（0 ～ 60）。 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クティブにするには、**force** キーワードを使用します。 **注意** アップグレードを続行する前に、表示されたチェックリストを見直して、すべての要件が満たされていることを確認します。 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。 **evacuate** キーワードを使用して、自動インストール を経由し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を有効にします。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。 （注） 自動インストール の間に、ファブリック エバキュエーションを有効にし、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いずれかのファブリック インターコネクトで手動で有効にされていた場合、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。
ステップ 4	（任意） UCS-A /firmware/auto-install # **install infra servicepack-vers** *servicepack-bundle-version* [**force**]	既存の基本インフラストラクチャ パック上のサービス パック バンドルを更新してアクティブ化します。

例

次に、Cisco UCS インフラストラクチャ ソフトウェア バンドル でインフラストラクチャをファームウェアにアップグレードする例を示します。

```
UCS-A# scope firmware
UCS-A /firmware # scope auto-install
UCS-A /firmware/auto-install # install infra infra-vers 4.0(1a)A
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: 4.0(1a)A
UCS-A /firmware/auto-install #
```

次に、**evacuate** オプションが有効になっている Cisco UCS インフラストラクチャ ソフトウェア バンドル でインフラストラクチャをファームウェアにアップグレードする例を示します。

```
UCS-A# scope firmware
UCS-A /firmware # scope auto-install
UCS-A /firmware/auto-install # install infra infra-vers 4.0(1a)A evacuate
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

Evacuate option: true
Warning: Please note that if fabric evacuation was configured ON manually on any of the
 FIs, it will be turned OFF in the process of Auto Install.

Triggering Install-Infra with:
   Infrastructure Pack Version: 4.0(1a)A
UCS-A /firmware/auto-install #
```

次に、インフラストラクチャをサービス パックのバージョンにアップグレードする例を示します。

```
UCS-A# scope firmware
UCS-A /firmware # scope auto-install
```

```
UCS-A /firmware/auto-install # install infra infra-vers 4.0(1a)A servicepack-vers 4.0(1)SP1
 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):
```

次のタスク

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

始める前に

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

- ファブリック インターコネクトのリブートを確認する前に、ファブリック インターコネクトに接続されているすべての IOM が稼動状態であることを確認します。すべての IOM が稼動状態ではない場合、ファブリック インターコネクトに接続されているすべてのサーバがただちに再検出され、大規模な中断が発生します。
- ファブリック インターコネクトとサービス プロファイルの両方がフェールオーバー用に設定されていることを確認します。
- プライマリ ファブリック インターコネクトのリブートを確認する前に、セカンダリ ファブリック インターコネクトからデータ パスが正常に復元されていることを確認します。詳細については、データ パスの準備が整っていることの確認 （73 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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope firmware**	ファームウェア モードを開始します。
ステップ 2	UCS-A /firmware # **scope auto-install**	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自動インストール モードを開始します。
ステップ 3	UCS-A /firmware/auto-install # **acknowledge primary fabric-interconnect reboot**	プライマリ ファブリック インターコネクトの保留中のリブートを確認します。
ステップ 4	UCS-A /firmware/auto-install # **commit-buffer**	トランザクションをシステムの設定にコミットします。 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。トランザクショ

	コマンドまたはアクション	目的
		ンをコミットした後でこのリブートを停止することはできません。

例

次に、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し、トランザクションをコミットする例を示します。

```
UCS-A# scope 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 #
```

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope firmware**	ファームウェア モードを開始します。
ステップ 2	UCS-A /firmware # **scope auto-install**	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自動インストールモードを開始します。
ステップ 3	UCS-A /firmware/auto-install # **cancel install infra**	スケジュールされたインフラストラクチャ ファームウェアのアップグレードをキャンセルします。
ステップ 4	UCS-A /firmware/auto-install # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、スケジュールされたインフラストラクチャ ファームウェアのアップグレードをキャンセルし、トランザクションをコミットする例を示します。

```
UCS-A# scope firmware
UCS-A /firmware # scope auto-install
UCS-A /firmware/auto-install # cancel install infra
UCS-A /firmware/auto-install* # commit-buffer
UCS-A /firmware/auto-install #
```

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として **/** を入力します。
ステップ 2	UCS-A /org # **scope fw-infra-pack** *name*	組織インフラストラクチャ ファームウェア ポリシー モードを開始します。
ステップ 3	UCS-A /org/fw-infra-pack # **set infra-bundle-version ""**	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。
ステップ 4	（任意） UCS-A /org/fw-infra-pack # **set servicepack-vers ""**	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。
ステップ 5	UCS-A /org/fw-infra-pack* # **commit-buffer**	トランザクションをコミットします。

例

次の例では、デフォルト インフラストラクチャ パックのスタートアップ バージョンをクリアする方法を示します。

```
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
```

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の FSM ステータスの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope firmware**	ファームウェア モードを開始します。
ステップ 2	UCS-A /firmware # **scope auto-install**	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自動インストール モードを開始します。
ステップ 3	UCS-A /firmware/auto-install # **show fsm status expand**	FSM のステータスを表示します。

例

次に、FSM のステータスを表示する例を示します。

```
UCS-A /firmware/auto-install # show fsm status expand

    FSM Status:

        Affected Object: sys/fw-system/fsm
        Current FSM: Deploy
        Status: Success
        Completion Time: 2017-02-03T18:02:13.699
        Progress (%): 100

        FSM Stage:

        Order  Stage Name                                Status       Try
        ------ ------------------------------------------ ------------ ---
        1      DeployWaitForDeploy                        Success      0
        2      DeployResolveDistributableNames            Skip         0
        3      DeployResolveDistributable                 Skip         0
        4      DeployResolveImages                        Skip         0
        5      DeployDownloadImages                       Skip         0
        6      DeployCopyAllImagesToPeer                  Skip         0
        7      DeployInternalBackup                       Skip         0
        8      DeployPollInternalBackup                   Success      0
        9      DeployActivateUCSM                         Skip         0
        10     DeployPollActivateOfUCSM                   Success      0
        11     DeployUpdateIOM                            Success      0
        12     DeployPollUpdateOfIOM                      Success      0
        13     DeployActivateIOM                          Success      0
        14     DeployPollActivateOfIOM                    Success      0
        15     DeployFabEvacOnRemoteFI                    Skip         0
        16     DeployPollFabEvacOnRemoteFI                Skip         0
        17     DeployActivateRemoteFI                     Success      0
        18     DeployPollActivateOfRemoteFI               Success      0
        19     DeployFabEvacOffRemoteFI                   Skip         0
        20     DeployPollFabEvacOffRemoteFI               Skip         0
        21     DeployWaitForUserAck                       Skip         0
        22     DeployPollWaitForUserAck                   Success      0
```

```
23      DeployFailOverToRemoteFI                Skip        0
24      DeployPollFailOverToRemoteFI            Skip        0
25      DeployActivateLocalFI                   Success     0
26      DeployPollActivateOfLocalFI             Success     0
27      DeployActivateUCSMServicePack           Skip        0
28      DeployPollActivateOfUCSMServicePack     Success     0
```

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**

Note 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**

Note **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**

Tip 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。

Important 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。

Caution 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 パッケージの作成または更新

メンテナンス ポリシーを含まない 1 つ以上のサービス プロファイルにポリシーが含まれている場合、Cisco UCS Managerはサーバーとアダプタのファームウェアを新しいバージョンで更新してアクティブ化します。メンテナンス ウィンドウを設定し、スケジュールしていない限り、ユーザーがホスト ファームウェア パッケージ ポリシーを保存すると、Cisco UCS Manager はすぐにサーバーを再起動します。

Tip 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。

Important 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。

Before you begin

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。

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、[org-name] に / を入力します。
ステップ 2	UCS A org/ # **create fw-host-pack** パック名	ホストファームウェアパッケージを選択したパッケージ名で作成し、組織ファームウェア ホストパッケージモードを開始します。
ステップ 3	(Optional) UCS-A /org/fw-host-pack # **set descr** *description*	ホストファームウェアパッケージの説明を記入します。 **Note** 説明にスペース、特殊文字、または句読点が含まれている場合、説明を引用符で括る必要があります。引用符は、**show** コマンド出力の説明フィールドには表示されません。

	Command or Action	Purpose
ステップ 4	UCS-A org/fw-host-pack # **create pack-image** "*hw-vendor-name*" "*hw モデル*" {**adapter** |**board-controller** | **cimc** | **graphics-card** |**host-hba** |**host-hba-optionrom** |**host-nic** |**local-disk** |**raid-controller** |**server-bios**}} "*version-num*"	ホスト ファームウェア パッケージのパッケージ イメージを作成し、組織ファームウェア ホスト パッケージ イメージ モードを開始します。*hw-vendor-name* は、ベンダーのフルネームと一致する必要があり、引用符で始まって引用符で終わる必要があります。 *hw-vendor-name* および *hw-model* 値は、 **show image detail** コマンド入力時にパッケージイメージの判別を容易にするラベルです。*version-num* 値は、パッケージのイメージに使用されているファームウェアのバージョン番号を指定します。 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 はファームウェアアップデートをインストールできません。
ステップ 5	UCS-A org/fw-host-pack # **create exclude-server-component** {**adapter** |**board-controller** |**cimc** |**flexflash-controller** |**graphics-card** |**host-hba** |**host-hba-optionrom** |**host-nic** |**host-nic-optionrom** |**local-disk** |**psu** |**raid-controller** |**sas-expander** |**server-bios** |**unspecified**}	ホストファームウェア パッケージから指定されたコンポーネントを除外します。 **Note** デフォルトでは、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ています。
ステップ 6	Required: UCS-A org/fw-host-pack # **delete exclude-server-component** {**adapter** |**board-controller** |**cimc** |**flexflash-controller** |**graphics-card** |**host-hba** |**host-hba-optionrom** |**host-nic** |**host-nic-optionrom** |**local-disk** |**psu** |**raid-controller** |**sas-expander** |**server-bios** |**unspecified**}	ホストファームウェア パッケージから指定されたコンポーネントを含めます。
ステップ 7	(Optional) UCS-A org/fw-host-pack/pack-image # **set blade-vers** *blade-version-num*	B シリーズ サーバ パッケージ イメージのバージョン番号を指定します。この番号を変更すると、サービス プロファイル経由でファームウェアを使用して、すべての B シリーズ サーバ コ

	Command or Action	Purpose
		ンポーネントのファームウェア更新が実行されます。このステップは、ホストファームウェアパッケージ更新時にのみ使用し、作成時には使用しません。 ホストファームウェアパッケージには複数のパッケージイメージを含めることができます。その他のコンポーネントについて、追加パッケージイメージを作成するには、手順 4 と 5 を繰り返します。
ステップ 8	(Optional) UCS-A org/fw-host-pack/pack-image # **set rack-vers** *rack-version-num*	C シリーズ サーバ パッケージ イメージのバージョン番号を指定します。この番号を変更すると、サービス プロファイル経由でファームウェアを使用して、すべての C シリーズ サーバ コンポーネントのファームウェア更新が実行されます。このステップは、ホストファームウェアパッケージ更新時にのみ使用し、作成時には使用しません。 ホストファームウェアパッケージには複数のパッケージイメージを含めることができます。その他のコンポーネントについて、追加パッケージイメージを作成するには、手順 4 と 5 を繰り返します。
ステップ 9	(Optional) UCS-A org/fw-host-pack/pack-image # **set servicepack-vers** *servicepack-version-num*	サービスパック バージョン番号を指定します。基本のサーバ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。 ホストファームウェアパッケージからサービスパックを削除するには、使用 "" サービス パック バージョン番号として。 サービスパックからのイメージは、ブレード パッケージまたはラック パッケージからのイメージよりも優先されます。

	Command or Action	Purpose
ステップ 10	UCS-A org/fw-host-pack/pack-image # **commit-buffer**	トランザクションをコミットします。 Cisco UCS Manager 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内のファームウェア バージョンに一致する場合、Cisco UCS Manager は、サービス プロファイルに含まれているメンテナンス ポリシー内の設定に従ってファームウェアを更新します。

Example

次に、app1 ホスト ファームウェア パッケージを作成して、バージョン 02.00.77 ファームウェアでアダプタ パッケージイメージを作成し、トランザクションをコミットする例を示します。

```
UCS-A# scope org
UCS-A /org # create fw-host-pack app1
UCS-A /org/fw-host-pack* # set descr "This is a host firmware package example."
UCS-A /org/fw-host-pack* # create pack-image "Cisco Systems Inc" "N20-AQ0102" adapter
"02.00.77"
UCS-A /org/fw-host-pack/pack-image* # commit-buffer
UCS-A /org/fw-host-pack/pack-image #
```

次に、app1 ホスト ファームウェア パッケージからサーバ BIOS コンポーネントを除外し、トランザクションをコミットする例を示します。

```
UCS-A# scope org
UCS-A /org # enter fw-host-pack app1
UCS-A /org/fw-host-pack* # create exclude-server-component server-bios
UCS-A /org/fw-host-pack/exclude-server-component* # commit-buffer
UCS-A /org/fw-host-pack/exclude-server-component #
```

次の例では、app1 ホスト ファームウェア パッケージにサービス パックを追加し、トランザクションをコミットします。

```
UCS-A# scope org
UCS-A /org # scope fw-host-pack app1
UCS-A /org/fw-host-pack # set servicepack-vers 4.0(1)SP1
UCS-A /org/fw-host-pack* # commit-buffer
UCS-A /org/fw-host-pack #
```

次の例では、app1 ホスト ファームウェア パッケージからサービス パックを削除し、トランザクションをコミットします。

```
UCS-A# scope org
UCS-A /org # scope fw-host-pack app1
UCS-A /org/fw-host-pack # set servicepack-vers ""
UCS-A /org/fw-host-pack* # commit-buffer
UCS-A /org/fw-host-pack #
```

What to do next

ポリシーをサービス プロファイルとテンプレートのうち一方、または両方に含めます。

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。

（注） サーバー プールの一部であるサーバーでは、**ファームウェア自動同期サーバー ポリシー**を使用できません。

[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のファームウェア バージョンの更新時期と更新方法を指定して、デフォルトのホスト ファームウェア パックのファームウェア バージョンと一致させることができます。

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。

始める前に

- 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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、org-name に / と入力します。
ステップ 2	UCS-A /org # **scope fw-autosync-policy**	ファームウェア自動同期ポリシー モードを開始します。
ステップ 3	UCS-A /org/fw-autosync-policy # **set auto-sync**{*user-acknowledge* | *no-actions*}	次の値のいずれかを指定してポリシーを設定します。 • [user-acknowledge]：管理者が**server** コマンド モードで検出されたサー

	コマンドまたはアクション	目的
		バを確認するまで、サーバのファームウェアは同期されません。 • [no-action]：ファームウェアのアップグレードはサーバで開始されません。 この値は、デフォルトで選択されます。
ステップ 4	UCS-A /org/fw-autosync-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、[Firmware Auto Sync Server] ポリシーを設定し、トランザクションをシステムにコミットする方法を示しています。

```
UCS-A # scope org
UCS-A /org # scope fw-autosync-policy
UCS-A /org/fw-autosync-policy # set auto-sync user-acknowledge
UCS-A /org/fw-autosync-policy* # commit-buffer
UCS-A /org/fw-autosync-policy #
```

次のタスク

値を [user-acknowledge] に設定した場合は、ファームウェアを同期させるために、保留中のサーバ アクティビティを確認する必要があります。

サーバのファームウェア自動同期の確認

ファームウェア自動同期サーバー ポリシーを [User Acknowledge] に設定した場合は、保留中のサーバ アクティビティを確認する必要があります。保留中のサーバ アクティビティを確認しないと、サーバのファームウェア バージョンまたはサーバ内のエンドポイントが更新されず、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 バージョンと一致しなくなります。

始める前に

- 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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	UCS-A /chassis # **scope server** *server ID*	サーバ コマンド モードを開始します。
ステップ 3	UCS-A /chassis/server # **fw-sync** {*acknowledge discard*}	保留中のサーバ ファームウェアの同期を確認または破棄します。
ステップ 4	UCS-A /chassis/server # **commit-buffer**	トランザクションをサーバにコミットします。

例

次の例は、保留中のサーバ ファームウェアの更新を確認して、トランザクションをコミットする方法を示しています。

```
UCS-A # scope chassis
UCS-A /chassis # scope server 1
UCS-A /chassis/server # fw-sync acknowledge
UCS-A /chassis/server* # commit-buffer
UCS-A /chassis/server #
```

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, on page 130は、エンドポイント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際に、Cisco が推奨するプロセスを説明しています。

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 C3260シャーシ

• Cisco UCS Manager
• ファブリック インターコネクト
 	
必ず Cisco UCS Manager をアップグレードしてからファブリック インターコネクトをアップグレードしてください。
	• 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 C3260 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 4.0*』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。

Important 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 C3260 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

Caution 更新プロセスが完了するまで、エンドポイントを含む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たりしないでください。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 C3260 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。

⚠

Caution 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、ファブリック インターコネクトと I/O モジュール間でプロトコルとファームウェア バージョンの不一致が Cisco UCS Manager で検出された場合、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と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。

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。
   1. すべての構成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 （57 ページ） と Full State バックアップ ポリシーの構成 （58 ページ） は、詳細情報を提供します。
   2. 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 （84 ページ）は詳細な情報を提供します。
   3. Smart Call Home を無効にします。Smart Call Home の無効化 （61 ページ） は、詳細情報を提供します。
2. Cisco UCS Manager ソフトウェアのアクティブ化 （132 ページ）
3. IOM ファームウェアをアップデートします。IOM でのファームウェアのアップデートおよびアクティブ化 （136 ページ） は、詳細情報を提供します。
4. ファブリック アップグレードを準備します。
   1. 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。
   2. 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 （66 ページ） は、詳細情報を提供します。
   3. デフォルトのメンテナンス ポリシーを構成します。デフォルト メンテナンス ポリシーの設定 （67 ページ） は、詳細情報を提供します。
   4. VLAN と FCOE ID が重複していないことを確認します。
   5. 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 （69ページ） は、詳細情報を提供します。
   6. IOM ファームウェアをアクティブ化します。IOM でのファームウェアのアップデートおよびアクティブ化 （136 ページ） は、詳細情報を提供します。
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。
   1. 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 インターコネクトのトラフィックの停止 （43 ページ） は、詳細情報を提供します。
   2. 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。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 （139ページ） は、詳細情報を提供します。

3. 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 （73 ページ） は、詳細情報を提供します。
4. 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 インターコネクトのトラフィックの再開 （44 ページ） は、詳細情報を提供します。
5. 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 （63 ページ） は、詳細情報を提供します。

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。
   1. 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 （141 ページ） は、詳細情報を提供します。
   2. 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。
   3. 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 コネクトのリブートの確認 （105 ページ） は、詳細情報を提供します。
   4. すべてのパスが動作していることを確認します。
   5. 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。ファブリック インターコネクトのトラフィックの再開 （44 ページ） は、詳細情報を提供します。
   6. 新しい障害を確認します。

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 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

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **show image**	Cisco UCS Manager（システム）の使用可能なイメージを表示します。
ステップ 3	UCS-A /system # **activate firmware** *version-num*	システムの選択されたファームウェア バージョンをアクティブにします。 **Note** Cisco UCS Manager のアクティブ化にファブリック インターコネクトのリブートは必要ありません。ただし、アクティブ化の一環として、管理サービスは短時間ダウンし、すべての VSH シェルが終了します。
ステップ 4	UCS-A /system # **commit-buffer**	トランザクションをコミットします。 Cisco UCS Manager によって、選択したバージョンがスタートアップ 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。

Example

次に、Cisco UCS Manager をアップグレードして、トランザクションをコミットする例を示します。

```
UCS-A# scope system
UCS-A# /system # show image
Name                                        Type                Version
------------------------------------------- ------------------- -------
ucs-manager-k9.4.0.1.0.bin                  System              4.0(1a)

UCS-A# /system # activate firmware 4.0(1a)
UCS-A# /system* # commit-buffer
UCS-A# /system #
```

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。

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope firmware**	
ステップ 2	UCS A/firmware # **show image type** mgmt-service-pack	Cisco UCS Manager（システム）の使用可能なイメージを表示します。
ステップ 3	UCS-A /firmware # **exit**	
ステップ 4	UCS-A# **scope system**	システム モードを開始します。
ステップ 5	UCS-A /system # **activate service-pack** *version-num* **module security**	システムの選択されたサービス パック バージョンをアクティブにします。 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に求められます。切断された直後に再度ログインするように求められた場合、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。
ステップ 6	UCS-A /system # **commit-buffer**	トランザクションをコミットします。

	Command or Action	Purpose
ステップ 7	(Optional) UCS-A /system # **show version**	システムで、サービス パック バージョンを含む、ファームウェアのバージョンの概要を示しています。

Example

次の例では、Cisco UCS Manager をバージョン 3.1(3)SP2 にアップグレードし、トランザクションをコミットします。

```
UCS-A# scope firmware
UCS-A# /firmware # show image type mgmt-service-pack
Name                                       Type                 Version
------------------------------------------ -------------------- -------
ucs-manager-k9.service-pack.3.1.3.SP1.gbin    Mgmt Service Pack    3.1(3)SP1
ucs-manager-k9.service-pack.3.1.3.SP2.gbin    Mgmt Service Pack    3.1(3)SP2
ucs-manager-k9.service-pack.3.1.4.SP1.gbin    Mgmt Service Pack    3.1(4)SP1
UCS-A# /firmware # exit
UCS-A# scope system
UCS-A# /system # activate service-pack 3.1(3)SP2 module security
As part of activation, all cli sessions will be terminated.
Continue with activation? (yes/no) yes
UCS-A# /system* # commit-buffer
UCS-A# /system # show version
UCSM:
    Running-Vers: 3.1(2.172a)
    Package-Vers: 3.1(2.173)A
    Activate-Status: Ready

UCSM Service Pack:
    Running-Vers: 3.1(3)SP2
    Running-Modules: security
    Package-Vers:
    Activate-Status: Ready


UCS-A# /system #
```

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

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **remove service-pack**	システムからのアクティブ化されたサービス パックを削除します。 システムからサービス パックを削除中には、すべての CLI セッションが終了しました。

	Command or Action	Purpose
ステップ 3	UCS-A /system # **commit-buffer**	トランザクションをコミットします。

Example

次の例では、Cisco UCS Manager からサービス パックを削除し、トランザクションをコミットします。

```
UCS-A# scope system
UCS-A# /system # remove service-pack
As part of activation, all cli sessions will be terminated.
Continue with activation? (yes/no)yes
UCS-A# /system* # commit-buffer
```

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 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。

IOM でのファームウェアのアップデートおよびアクティブ化

システムがハイ アベイラビリティ クラスタ設定で稼働している場合は、両方の I/O モジュールをアップデートし、アクティブにする必要があります。

Caution 更新プロセスが完了するまで、エンドポイントを含む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たりしないでください。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。

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A # **scope chassis** *chassis-id*	指定したシャーシでシャーシ モードを開始します。
ステップ 2	UCS-A /chassis # **scope iom** *iom-id*	選択した I/O モジュールでシャーシ I/O モジュール モードを開始します。
ステップ 3	UCS-A /chassis/iom # **show image**	I/O モジュールの使用可能なソフトウェア イメージを表示します。
ステップ 4	UCS-A /chassis/iom # **update firmware** *version-num*	I/O モジュールの選択したファームウェア バージョンをアップデートします。
ステップ 5	(Optional) UCS-A /chassis/iom # **commit-buffer**	トランザクションをコミットします。 ステップ 7 でファームウェアをアクティブにする前に、ステップ 6 で **show**

	Command or Action	Purpose
		firmware コマンドを使用してファームウェアのアップデートが正常に完了したことを確認する場合のみ、このステップを使用します。このステップをスキップして、同じトランザクションで **update-firmware** および **activate-firmware** コマンドをコミットできます。ただし、ファームウェアのアップデートが正常に完了していない場合は、ファームウェアのアクティブ化が開始されません。 Cisco UCS Manager によって、選択したファームウェア イメージがバックアップ メモリ パーティションにコピーされ、そのイメージが破損していないことが確認されます。イメージは、明示的に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。
ステップ 6	(Optional) UCS-A /chassis/iom # **show firmware**	ファームウェアのアップデートのステータスを表示します。 ファームウェアのアップデートが正常に完了したことを確認する場合にのみ、このステップを使用します。アップデート ステータスが Ready になったら、ファームウェアのアップデートは完了です。CLI の表示は自動的には更新されないため、タスクのステータスが Updating から Ready に変更されるまで何度も **show firmware** コマンドを入力する必要がある場合があります。アップデート ステータスが Ready になったらステップ 7 に進みます。
ステップ 7	UCS-A /chassis/iom # **activate firmware** *version-num* [**set-startup-only**]	I/O モジュールの選択したファームウェア バージョンをアクティブにします。 ファブリック インターコネクトがそのデータ パスでリブートする場合にのみ I/O モジュールをリブートする場合、**set-startup-only** キーワードを使用します。 **set-startup-only** キーワードを使用しない場合、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。さら

	Command or Action	Purpose
		に、Cisco UCS Manager は I/O モジュールとの間で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すると、一致するファームウェア バージョンで I/O モジュールをアップデートし、ファームウェアをアクティブにし、再度 I/O モジュールをリブートします。
ステップ 8	UCS-A /chassis/iom # **commit-buffer**	トランザクションをコミットします。
ステップ 9	(Optional) UCS-A /chassis/iom # **show firmware**	ファームウェアのアクティベーションのステータスを表示します。 ファームウェアのアクティベーションが正常に完了したことを確認する場合にのみ、このステップを使用します。CLI の表示は自動的には更新されないため、タスクのステータスが Activating から Ready に変更されるまで何度も **show firmware** コマンドを入力する必要がある場合があります。

Example

次の例では、同じトランザクションで I/O モジュールのファームウェアをアップデートしてアクティブ化します。ファームウェアのアップデートとアクティベーションが正常に完了したかどうかについて確認は行いません。

```
UCS-A# scope chassis 1
UCS-A# /chassis # scope iom 1
UCS-A# /chassis/iom # show image
Name                                       Type                 Version
------------------------------------------ -------------------- -------
ucs-2200.4.0.0.332.bin                     IOM                  4.0(1a)

UCS-A# /chassis/iom # update firmware 4.0(1a)
UCS-A# /chassis/iom* # activate firmware 4.0(1a) set-startup-only
UCS-A# /chassis/iom* # commit-buffer
UCS-A# /chassis/iom #
```

次の例では、I/Oモジュールのファームウェアをアップデートし、アップデートが正常に完了したことを確認してからファームウェアのアクティベーションを開始して、I/Oモジュールのファームウェアをアクティブ化し、アクティベーションが正常に完了したことを確認します。

```
UCS-A# scope chassis 1
UCS-A# /chassis # scope iom 1
```

```
UCS-A# /chassis/iom # show image
Name                                       Type                Version
------------------------------------------ ------------------- -------
ucs-2200.4.0.0.332.bin                     IOM                 4.0(1)

UCS-A# /chassis/iom # update firmware 4.0(1)
UCS-A# /chassis/iom* # commit-buffer
UCS-A# /chassis/iom # show firmware
IOM      Fabric ID Running-Vers    Update-Status   Activate-Status
-------- --------- --------------- --------------- ---------------
       1 A         4.0(1)          Updating        Ready

UCS-A# /chassis/iom # show firmware
IOM      Fabric ID Running-Vers    Update-Status   Activate-Status
-------- --------- --------------- --------------- ---------------
       1 A         4.0(1)          Ready           Ready

UCS-A# /chassis/iom # activate firmware 4.0(1) ignorecompcheck
UCS-A# /chassis/iom* # commit-buffer
UCS-A# /chassis/iom # show firmware
IOM      Fabric ID Running-Vers    Update-Status   Activate-Status
-------- --------- --------------- --------------- ---------------
       1 A         4.0(1)          Ready           Activating

UCS-A# /chassis/iom # show firmware
IOM      Fabric ID Running-Vers    Update-Status   Activate-Status
-------- --------- --------------- --------------- ---------------
       1 A         4.0(1)          Ready           Ready
```

ファブリック インターコネクトのファームウェア

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

ハイ アベイラビリティ クラスタ設定の 2 台のファブリック インターコネクトのファームウェアを更新する場合、プライマリ ファブリック インターコネクトをアクティブ化する前に、従属ファブリック インターコネクトをアクティブにする必要があります。各ファブリック インターコネクトの役割の決定の詳細については、クラスタ設定の高可用性ステータスとロールの確認, on page 66を参照してください。

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。

Tip Cisco UCS ドメインのファブリック インターコネクト設定時に作成された管理者アカウントのパスワードを回復する必要がある場合、実行中のカーネルバージョンと実行中のシステム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。

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope fabric-interconnect** {**a** | **b**}	指定したファブリック インターコネクトのファブリック インターコネクト モードを開始します。
ステップ 2	UCS-A /fabric-interconnect # **show image**	ファブリック インターコネクトの利用可能なソフトウェア イメージを表示します。
ステップ 3	UCS-A /fabric-interconnect # **activate firmware** {**kernel-version** *kernel-ver-num* | **system-version** *system-ver-num*}	ファブリック インターコネクトの選択されたファームウェア バージョンをアクティブにします。 **Note** kernel-version と system-version は、同じである必要があります。
ステップ 4	UCS-A /fabric-interconnect # **commit-buffer**	トランザクションをコミットします。 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てから、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、ファブリック インターコネクトへのデータ トラフィックを中断するすべてのI/Oモジュールをリブートします。

Example

次の例では、ファブリック インターコネクトをバージョン 5.0(3)N2(3.10.123) にアップグレードし、トランザクションをコミットします。

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect # show image
Name                                       Type                 Version
------------------------------------------ -------------------- -------
ucs-6300-k9-kickstart.5.0.3.N2.3.10.123.bin   Fabric Interconnect Kernel
                                                                  5.0(3)N2(3.10.123)
ucs-6300-k9-system.5.0.3.N2.3.10.123.bin      Fabric Interconnect System
                                                                  5.0(3)N2(3.10.123)

UCS-A /fabric-interconnect # activate firmware kernel-version 5.0(3)N2(3.10.123)
system-version 5.0(3)N2(3.10.123)
UCS-A /fabric-interconnect* # commit-buffer
UCS-A /fabric-interconnect #
```

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。

重要 クラスタのフェールオーバー中は、新しいプライマリ ファブリック インターコネクトが選択されるまで仮想 IP アドレスにアクセスできません。

手順

	コマンドまたはアクション	目的
ステップ 1	（任意） UCS-A# **show cluster state**	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** {**force primary** | **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。

例

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

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope firmware**	
ステップ 2	UCS A/firmware # **show image type** fabric-interconnect-service-pack	ファブリック インターコネクトの使用可能なサービスパックが表示されます。
ステップ 3	UCS-A /firmware # **exit**	
ステップ 4	UCS-A# **scope fabric-interconnect** {**a** | **b**}	fabric-interconnect モードを開始します。
ステップ 5	UCS-A /fabric-interconnect # **activate service-pack** *version-num* [**security**]	システムの選択されたサービス パック バージョンをアクティブにします。 **Note** Cisco UCS Manager ファームウェアをアクティブにします。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。
ステップ 6	UCS-A /fabric-interconnect # **commit-buffer**	トランザクションをコミットします。
ステップ 7	(Optional) UCS-A /fabric-interconnect # **show version**	ファブリックインターコネクトで、サービス パック バージョンを含む、ファームウェアのバージョンの概要を示しています。

Example

次に、ファブリック インターコネクトをアップグレードして、トランザクションをコミットする例を示します。

```
UCS-A# scope firmware
UCS-A# /firmware # show image type fabric-interconnect-service-pack
Name                                       Type                  Version
------------------------------------------ --------------------- -------
ucs-6400-servicepack.4.0.1.SP1.gbin        Fabric Interconnect Service Pack
                                                                  4.0(1)SP1
ucs-6400-servicepack.4.0.1.SP2.gbin        Fabric Interconnect Service Pack
                                                                  4.0(1)SP2
ucs-6300-servicepack.4.0.1.SP1.gbin        Fabric Interconnect Service Pack
                                                                  4.0(1)SP1
ucs-6300-servicepack.4.0.1.SP2.gbin        Fabric Interconnect Service Pack
                                                                  4.0(1)SP2
ucs-mini-servicepack.4.0.1.SP1.gbin        Fabric Interconnect Service Pack
                                                                  4.0(1)SP1
ucs-mini-servicepack.4.0.1.SP2.gbin        Fabric Interconnect Service Pack
                                                                  4.0(1)SP2

UCS-A# /firmware # exit
UCS-A# scope fabric-interconnect a
UCS-A# /fabric-interconnect # activate service-pack 4.0(1)SP0 security
UCS-A# /fabric-interconnect* # commit-buffer
UCS-A# /fabric-interconnect # show version
 Fabric Interconnect A:
    Running-Kern-Vers: 7.0(3)N2(4.00.226)
    Running-Sys-Vers: 7.0(3)N2(4.00.226)
    Running-Service-Pack-Vers: 4.0(1)SP0(Default)
    Package-Vers: 4.0(0.147)A
    Package-Service-Pack-Vers:
    Startup-Kern-Vers: 7.0(3)N2(4.00.226)
    Startup-Sys-Vers: 7.0(3)N2(4.00.226)
    Startup-Service-Pack-Vers: 4.0(1)SP0(Default)
    Act-Kern-Status: Ready
    Act-Sys-Status: Ready
    Act-Service-Pack-Status: Ready
    Bootloader-Vers: v05.28(01/18/2018)
```

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

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。

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope fabric-interconnect** {**a** | **b**}	fabric-interconnect モードを開始します。
ステップ 2	UCS-A /fabric-interconnect # **remove service-pack security**	ファブリック インターコネクトからアクティベート済みサービス パックを削除します。

	Command or Action	Purpose
ステップ 3	UCS-A /fabric-interconnect # **commit-buffer**	トランザクションをコミットします。

Example

次に、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、トランザクションをコミットする例を示します。

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

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：

- 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ソフトウェアを使用した管理
- 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。

アダプタでのファームウェアのアップデートおよびアクティブ化

⚠

Caution 更新プロセスが完了するまで、エンドポイントを含む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たりしないでください。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。

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope adapter** *chassis-id / blade-id / adapter-id*	指定したアダプタでシャーシ サーバ アダプタ モードを開始します。
ステップ 2	UCS-A /chassis/server/adapter # **show image**	アダプタの使用可能なソフトウェア イメージを表示します。
ステップ 3	UCS-A /chassis/server/adapter # **update firmware** *version-num*	アダプタの選択したファームウェアバージョンをアップデートします。
ステップ 4	(Optional) UCS-A /chassis/server/adapter # **commit-buffer**	トランザクションをコミットします。 ステップ 6 でファームウェアをアクティブにする前に、ステップ 5 で **show firmware** コマンドを使用してファームウェアのアップデートが正常に完了したことを確認する場合のみ、このステップを使用します。このステップをスキップして、同じトランザクションで **update-firmware** および **activate-firmware** コマンドをコミットできます。ただし、ファームウェアのアップデートが正常に完了していない場合は、ファームウェアのアクティブ化が開始されません。 Cisco UCS Manager によって、選択したファームウェア イメージがバックアップ メモリ パーティションにコピーされ、そのイメージが破損していないことが確認されます。イメージは、明示的に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。
ステップ 5	(Optional) UCS-A /chassis/server/adapter # **show firmware**	ファームウェアのアップデートのステータスを表示します。 ファームウェアのアップデートが正常に完了したことを確認する場合にのみ、このステップを使用します。アップデート ステータスが Ready になったら、ファームウェアのアップデートは完了です。CLI の表示は自動的には更新されないため、タスクのステータスが Updating から Ready に変更されるまで何度も **show firmware** コマンドを入力する必要があ

	Command or Action	Purpose
		る場合があります。アップデートステータスが Ready になったらステップ 6 に進みます。
ステップ 6	UCS-A /chassis/server/adapter # **activate firmware** *version-num* [**set-startup-only**]	アダプタの選択したファームウェアバージョンをアクティブにします。 アクティブ化したファームウェアを pending-next-boot 状態にし、サーバをただちにリブートしない場合は、**set-startup-only** キーワードを使用します。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は **set-startup-only** キーワードは使用できません。
ステップ 7	UCS-A /chassis/server/adapter # **commit-buffer**	トランザクションをコミットします。 サーバがサービス プロファイルに関連付けられていない場合、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。
ステップ 8	(Optional) UCS-A /chassis/server/adapter # **show firmware**	ファームウェアのアクティベーションのステータスを表示します。 ファームウェアのアクティベーションが正常に完了したことを確認する場合にのみ、このステップを使用します。CLI の表示は自動的には更新されないため、タスクのステータスが Activating から Ready に変更されるまで何度も **show firmware** コマンドを入力する必要がある場合があります。

Example

次に、ファームウェアのアップデートおよびファームウェアのアクティベーションが正常に完了したことを確認せずに、同じトランザクションでアダプタのファームウェアをバージョン 4.1(0.123) にアップデートし、アクティブ化する例を示します。

```
UCS-A# scope adapter 1/1/1
UCS-A# /chassis/server/adapter # show image
Name                                       Type                Version
------------------------------------------ ------------------- -------
ucs-m82-8p-vic.4.1.0.123.bin               Adapter             4.1(0.123)

UCS-A# /chassis/server/adapter # update firmware 4.1(0.123)
UCS-A# /chassis/server/adapter* # activate firmware 4.1(0.123) set-startup-only
UCS-A# /chassis/server/adapter* # commit-buffer
UCS-A# /chassis/server/adapter #
```

次に、アダプタのファームウェアをバージョン 4.1(0.123) にアップデートし、ファームウェアのアクティベーションを開始する前にファームウェアのアップデートが正常に完了したことを確認し、アダプタのファームウェアをアクティブにし、ファームウェアのアクティベーションが正常に完了したことを確認する例を示します。

```
UCS-A# scope adapter 1/1/1
UCS-A# /chassis/server/adapter # show image
Name                                       Type                Version
------------------------------------------ ------------------- -------
ucs-m82-8p-vic.4.1.0.123.bin               Adapter             4.2(1.13)

UCS-A# /chassis/server/adapter # update firmware 4.2(3.13)
UCS-A# /chassis/server/adapter* # commit-buffer
UCS-A# /chassis/server/adapter # show firmware
Adapter 1:
    Running-Vers: 4.2(3.13)
    Package-Vers: 4.0(0.128)B
    Update-Status: Updating
    Activate-Status: Ready

UCS-A# /chassis/server/adapter # show firmware
Adapter 1:
    Running-Vers: 4.2(3.13)
    Package-Vers: 4.0(0.128)B
    Update-Status: Ready
    Activate-Status: Ready

UCS-A# /chassis/server/adapter # activate firmware 4.2(3.13)
Warning: When committed this command will reset the end-point
UCS-A# /chassis/server/adapter* # commit-buffer
UCS-A# /chassis/server/adapter # show firmware
Adapter 1:
    Running-Vers: 4.2(3.13)
    Package-Vers: 4.0(0.128)B
    Update-Status: Ready
    Activate-Status: Activating

UCS-A# /chassis/server/adapter # show firmware
Adapter 1:
```

```
    Running-Vers: 4.2(3.13)
    Package-Vers: 4.0(0.128)B
    Update-Status: Ready
    Activate-Status: Pending Next Boot

UCS-A# /chassis/server/adapter # exit
UCS-A# /chassis/server # cycle cycle-immediate
UCS-A# /chassis/server* # commit-buffer
UCS-A# /chassis/server # scope adapter 1
UCS-A# /chassis/server/adapter # show firmware
Adapter 1:
    Running-Vers: 4.2(3.13)
    Package-Vers: 4.0(0.128)B
    Update-Status: Ready
    Activate-Status: Ready
UCS-A# /chassis/server/adapter #
```

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 ファームウェアの更新とアクティブ化

重要 すべての M3 世代以降のサーバで、Cisco UCS Manager CLI を使用し、サーバの BIOS ファームウェアを更新してアクティブ化できます。以前のサーバでは、Cisco UCS Manager CLI による BIOS ファームウェアの更新はサポートされていません。

注意 更新プロセスが完了するまで、エンドポイントを含む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たりしないでください。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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *chassis-id / blade-id*	指定サーバーのシャーシ サーバー モードを開始します。
ステップ 2	UCS-A /chassis/server # scope bios	シャーシ サーバBIOSモードを開始します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /chassis/server/bios # **show image**	使用可能な BIOS ファームウェア イメージを表示します。
ステップ 4	UCS-A /chassis/server/bios # **update firmware** バージョン番号	サーバの選択した BIOS ファームウェアを更新します。
ステップ 5	（任意） UCS-A /chassis/server/bios # **commit-buffer**	トランザクションをコミットします。 ステップ 7 でファームウェアをアクティブにする前に、ステップ 6 で **show firmware** コマンドを使用してファームウェアのアップデートが正常に完了したことを確認する場合のみ、このステップを使用します。このステップをスキップして、同じトランザクションで **update-firmware** および **activate-firmware** コマンドをコミットできます。ただし、ファームウェアのアップデートが正常に完了していない場合は、ファームウェアのアクティブ化が開始されません。 Cisco UCS Manager によって、選択したファームウェア イメージがバックアップ メモリ パーティションにコピーされ、そのイメージが破損していないことが確認されます。イメージは、明示的に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。
ステップ 6	（任意） UCS-A /chassis/server/bios # **show firmware**	ファームウェアのアップデートのステータスを表示します。 ファームウェアのアップデートが正常に完了したことを確認する場合にのみ、このステップを使用します。アップデート ステータスが Ready になったら、ファームウェアのアップデートは完了です。CLI の表示は自動的には更新されないため、タスクのステータスが Updating から Ready に変更されるまで何度も **show firmware** コマンドを入力する必要がある場合があります。アップデート ステータスが Ready になったらステップ 7 に進みます。

	コマンドまたはアクション	目的
ステップ 7	UCS-A /chassis/server/bios # **activate firmware** バージョン番号	選択したサーバ BIOS ファームウェア バージョンをアクティブにします。
ステップ 8	UCS-A /chassis/server/bios # **commit-buffer**	トランザクションをコミットします。
ステップ 9	（任意） UCS A/シャーシ/bios #**show firmware**	ファームウェアのアクティベーションのステータスを表示します。 ファームウェアのアクティベーションが正常に完了したことを確認する場合にのみ、このステップを使用します。CLIの表示は自動的には更新されないため、タスクのステータスが Activating から Ready に変更されるまで何度も **show firmware** コマンドを入力する必要がある場合があります。

例

次の例では、同じトランザクションでBIOSファームウェアの更新とアクティベーションを行います。ファームウェアの更新とアクティベーションが正常に完了したことの確認は行いません。

```
UCS-A# scope server 1/1
UCS-A# /chassis/server # scope bios
UCS-A# /chassis/server/bios # show image
Name                                       Type                 Version
------------------------------------------ -------------------- -------
ucs-b200-m2-bios.S5500.2.1.3c.0.081120151437.bin
                                           Server BIOS
S5500.2.1.3c.0.081120151437
ucs-b200-m3-bios.B200M3.2.2.6c.0.110420151250.bin
                                           Server BIOS
B200M3.2.2.6c.0.110420151250
ucs-b200-m4-bios.B200M4.3.1.0.4.113020151739.bin
                                           Server BIOS
B200M4.3.1.0.4.113020151739

UCS-A# /chassis/server/bios # update firmware B200M4.3.1.0.4.113020151739
UCS-A# /chassis/server/bios* # activate firmware B200M4.3.1.0.4.113020151739
UCS-A# /chassis/server/bios* # commit-buffer
UCS-A# /chassis/server/bios #
```

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およびアクティブ化

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。

⚠

Caution 更新プロセスが完了するまで、エンドポイントを含む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たりしないでください。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。

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope server** *chassis-id* / *blade-id*	指定サーバーのシャーシ サーバー モードを開始します。
ステップ 2	UCS-A /chassis/server # **scope cimc**	シャーシ サーバー CIMC モードを開始します。
ステップ 3	UCS-A /chassis/server/cimc # **show image**	アダプタの使用可能なソフトウェア イメージを表示します。
ステップ 4	UCS-A /chassis/server/cimc # **update firmware** バージョン番号	サーバの CIMC の選択したファームウェア バージョンをアップデートします。
ステップ 5	(Optional) UCS-A /chassis/server/cimc # **commit-buffer**	トランザクションをコミットします。 ステップ 7 でファームウェアをアクティブにする前に、ステップ 6 で **show firmware** コマンドを使用してファームウェアのアップデートが正常に完了したことを確認する場合のみ、このステップを使用します。このステップをスキップして、同じトランザクションで **update-firmware** および **activate-firmware** コマンドをコミットできます。ただし、ファームウェアのアップデートが正常に完了していない場

	Command or Action	Purpose
		合は、ファームウェアのアクティブ化が開始されません。 Cisco UCS Manager によって、選択したファームウェア イメージがバックアップ メモリ パーティションにコピーされ、そのイメージが破損していないことが確認されます。イメージは、明示的に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。
ステップ 6	(Optional) UCS-A /chassis/server/cimc # **show firmware**	ファームウェアのアップデートのステータスを表示します。 ファームウェアのアップデートが正常に完了したことを確認する場合にのみ、このステップを使用します。アップデート ステータスが Ready になったら、ファームウェアのアップデートは完了です。CLI の表示は自動的には更新されないため、タスクのステータスが Updating から Ready に変更されるまで何度も **show firmware** コマンドを入力する必要がある場合があります。アップデート ステータスが Ready になったらステップ 7 に進みます。
ステップ 7	UCS-A /chassis/server/cimc # **activate firmware** バージョン番号	サーバの CIMC の選択したファームウェア バージョンをアクティブにします。
ステップ 8	UCS-A /chassis/server/cimc # **commit-buffer**	トランザクションをコミットします。
ステップ 9	(Optional) UCS-A /chassis/server/cimc # **show firmware**	ファームウェアのアクティベーションのステータスを表示します。 ファームウェアのアクティベーションが正常に完了したことを確認する場合にのみ、このステップを使用します。CLI の表示は自動的には更新されないため、タスクのステータスが Activating から Ready に変更されるまで何度も **show firmware** コマンドを入力する必要がある場合があります。

Example

次の例では、同じトランザクションで CIMC のファームウェアをアップデートしてアクティブ化します。ファームウェアのアップデートとアクティベーションが正常に完了したかどうかについて確認は行いません。

```
UCS-A# scope server 1/1
UCS-A# /chassis/server # scope cimc
UCS-A# /chassis/server/cimc # show image
Name                                       Type                Version
------------------------------------------ ------------------- -------
ucs-b200-m3-k9-cimc.4.0.1.bin              CIMC                4.0(1)
ucs-b200-m3-k9-cimc.4.0.1.bin              CIMC                4.0(1)
ucs-b200-m4-k9-cimc.4.0.1.bin              CIMC                4.0(1)
ucs-b200-m5-k9-cimc.4.0.1.bin              CIMC                4.0(1)
ucs-b22-m3-k9-cimc.4.0.1.bin               CIMC                4.0(1)

...

UCS-A# /chassis/server/cimc # update firmware 4.0(1)
UCS-A# /chassis/server/cimc* # activate firmware 4.0(1) set-startup-only
UCS-A# /chassis/server/cimc* # commit-buffer
UCS-A# /chassis/server/cimc #
```

次の例では、CIMC のファームウェアをアップデートし、アップデートが正常に完了したことを確認してからファームウェアのアクティベーションを開始して、CIMC のファームウェアをアクティブ化し、アクティベーションが正常に完了したことを確認します。

```
UCS-A# scope server 1/1
UCS-A# /chassis/server # scope cimc
UCS-A# /chassis/server/cimc # show image
Name                                       Type              Version
------------------------------------------ ----------------- -------------
ucs-b200-m1-k9-cimc.4.0.1.bin              CIMC                 4.0(1)
ucs-b200-m1-k9-cimc.4.0.1.bin              CIMC                 4.0(1)
ucs-b200-m1-k9-cimc.4.0.1.bin              CIMC                 4.0(1)
ucs-b200-m3-k9-cimc.4.0.1.bin              CIMC                 4.0(1)
...

UCS-A# /chassis/server/cimc # update firmware 4.0(1)
UCS-A# /chassis/server/cimc* # commit-buffer
UCS-A# /chassis/server/cimc # show firmware
Running-Vers    Update-Status   Activate-Status
--------------- --------------- ---------------
4.0(1)          Updating        Ready

UCS-A# /chassis/server/cimc # show firmware
Running-Vers    Update-Status   Activate-Status
--------------- --------------- ---------------
4.0(1)          Ready           Ready

UCS-A# /chassis/server/cimc # activate firmware 4.0(1)
UCS-A# /chassis/server/cimc* # commit-buffer
UCS-A# /chassis/server/cimc # show firmware
Running-Vers    Update-Status   Activate-Status
```

```
--------------- --------------- ---------------
4.0(1)          Ready           Activating

UCS-A# /chassis/server/cimc # show firmware
Running-Vers    Update-Status   Activate-Status
--------------- --------------- ---------------
4.0(1)          Ready           Ready
```

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 更新プロセスが完了するまで、エンドポイントを含む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たりしないでください。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

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope chassis** *chassis-id*	指定したシャーシでシャーシ モードを開始します。
ステップ 2	UCS-A /chassis # **scope psu** *psu-id*	指定した PSU で PSU モードを開始します。
ステップ 3	UCS-A /chassis/psu # **show detail**	PSU の使用可能なソフトウェア イメージを表示します。
ステップ 4	UCS-A /chassis/psu # **update firmware** *version-num* [**force**]	PSUの選択したファームウェアバージョンを更新します。 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クティブにするには、オプションの **force** キーワードを使用できます。 **注意** アップグレードを続行する前に、表示されたチェックリストを見直して、すべての要件が満たされていることを確認します。

	コマンドまたはアクション	目的
ステップ 5	（任意） UCS-A /chassis/psu # **commit-buffer**	トランザクションをコミットします。 Cisco UCS Manager によって、選択したファームウェア イメージがバックアップ メモリ パーティションにコピーされ、そのイメージが破損していないことが確認されます。イメージは、明示的に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。

例

次の例では、PSU ファームウェアを更新し、トランザクションをコミットする方法を示します。

```
UCS-A# scope chassis 1
UCS-A# /chassis # scope psu 2
UCS-A# /chassis/psu # show detail
PSU:
    PSU: 2
    Overall Status: Operable
    Operability: Operable
    Threshold Status: OK
    Power State: On
    Presence: Equipped
    Thermal Status: OK
    Voltage Status: OK
    Product Name: Platinum II AC Power Supply for UCS 5108 Chassis
    PID: UCSB-PSU-2500ACDV
    VID: V01
    Part Number: 341-0571-01
    Vendor: Cisco Systems Inc
    Serial (SN): DTM190304FD
    HW Revision: 0
    Firmware Version: 05.10
    Type: DV
    Wattage (W): 2500
    Input Source: 210AC 50 380DC
    Current Task:
UCS-A# /chassis/psu # update firmware 05.10
UCS-A# /chassis/psu* # commit-buffer
UCS-A# /chassis/psu #
```

PSU でのファームウェアのアクティブ化

⚠

注意 更新プロセスが完了するまで、エンドポイントを含む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たりしないでください。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

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope chassis** *chassis-id*	指定したシャーシでシャーシ モードを開始します。
ステップ 2	UCS-A /chassis # **scope psu** *psu-id*	指定した PSU で PSU モードを開始します。
ステップ 3	UCS-A /chassis/psu # **activate firmware** *version-num*	PSUの選択したファームウェアバージョンをアクティブにします。
ステップ 4	必須: UCS-A /chassis/psu # **commit-buffer**	トランザクションをコミットします。 （注） トランザクションのコミットによりエンドポイントがリセットされます。

例

次の例では、PSU ファームウェアをアクティブにし、トランザクションをコミットします。

```
UCS-A# scope chassis 1
UCS-A# /chassis # scope psu 2
UCS-A# /chassis/psu # activate firmware 03.10
Warning: When committed this command will reset the end-point
UCS-A# /chassis/psu* # commit-buffer
UCS-A# /chassis/psu #
```

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

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

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

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

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

機能カタログの更新は、次の手順で適用できます。

1. 2.2(4c) Infra/Catalog または 2.2(5b) Infra/Catalog ソフトウェア バンドルをダウンロードします。
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（165 ページ） は Cisco UCS Manager を使用した機能カタログのアクティブ化についての詳細情報を提供します。
3. 新しく挿入されたブレード サーバを停止します。
4. 以前のボード コントローラ バージョンがあるホスト ファームウェア パック ポリシーにサービス プロファイルを関連付けます。

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

5. **[Save（保存）]** をクリックします。
6. ブレード サーバを再検出します。

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

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

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

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

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

  このアラームが表示されないようにするには、次のいずれかを行います。

  - Cisco UCS Manager 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

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

（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 ファームウェアは、Cisco UCS ドメインのアップグレードの最後の手順として、サーバ BIOS のアップグレードと同時に、サービス プロファイル内のホスト ファームウェア パッケージからアップグレードすることをお勧めします。これにより、アップグレードプロセス中にサーバをリブートしなければならない回数を減らせます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *chassis-id / server-id*	指定サーバーのシャーシ サーバー モードを開始します。
ステップ 2	UCS-A /chassis/server # **scope boardcontroller**	サーバのボード コントローラ モードを開始します。
ステップ 3	（任意） UCS-A /chassis/server/boardcontroller # **show image**	ボード コントローラの利用可能なソフトウェア イメージを表示します。
ステップ 4	（任意） UCS-A /chassis/server/boardcontroller # **show firmware**	ボード コントローラの現在実行中のソフトウェア イメージを表示します。
ステップ 5	UCS-A /chassis/server/boardcontroller # **activate firmware** バージョン番号	サーバのボード コントローラの選択されたファームウェア バージョンをアクティブ化します。
ステップ 6	UCS-A /chassis/server/boardcontroller # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、ボード コントローラのファームウェアをアクティブ化します。

```
UCS-A# scope server 1/1
UCS-A# /chassis/server # scope boardcontroller
UCS-A# /chassis/server/boardcontroller # show image
```

```
Name                                       Type                Version
------------------------------------------ ------------------- -------
ucs-b200-m3-brdprog.15.0.bin               Board Controller    15.0
ucs-b22-m3-brdprog.16.0.bin                Board Controller    16.0
ucs-b420-m3-brdprog.12.0.bin               Board Controller    12.0

UCS-A# /chassis/server/boardcontroller # show firmware
BoardController:
    Running-Vers: 15.0
    Package-Vers: 3.2(1)B
    Activate-Status: Ready

UCS-A# /chassis/server/boardcontroller # activate firmware 15.0
UCS-A# /chassis/server/boardcontroller* # commit-buffer
```

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

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

（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 ファームウェアは、Cisco UCS ドメインのアップグレードの最後の手順として、サーバ BIOS のアップグレードと同時に、サービス プロファイル内のホスト ファームウェア パッケージからアップグレードすることをお勧めします。これにより、アップグレードプロセス中にサーバをリブートしなければならない回数を減らせます。

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

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

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *server-id*	指定サーバのシャーシ サーバ モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /server # **scope boardcontroller**	サーバのボード コントローラ モードを開始します。
ステップ 3	（任意） UCS-A /server/boardcontroller # **show image**	ボード コントローラの利用可能なソフトウェア イメージを表示します。
ステップ 4	（任意） UCS-A /server/boardcontroller # **show firmware**	ボード コントローラの現在実行中のソフトウェア イメージを表示します。
ステップ 5	UCS-A /server/boardcontroller # **activate firmware** *version-num*	サーバのボード コントローラの選択されたファームウェア バージョンをアクティブ化します。
ステップ 6	UCS-A /server/boardcontroller # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

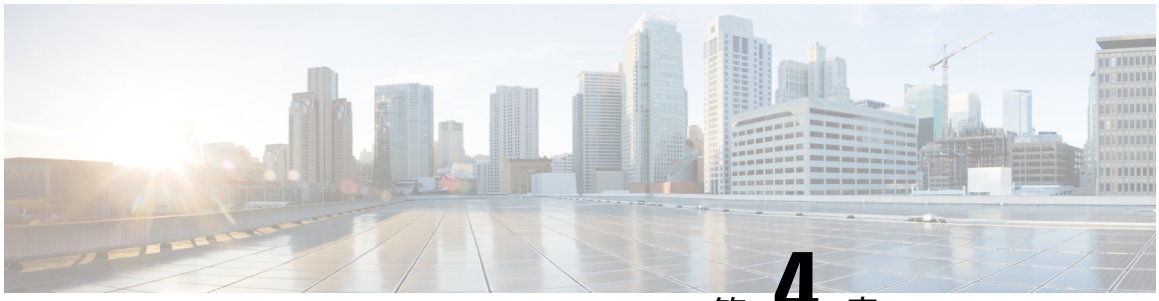
次の例では、ボード コントローラのファームウェアをアクティブ化します。

```
UCS-A# scope server 7
UCS-A# /server # scope boardcontroller
UCS-A# /server/boardcontroller # show image
Name                                     Type               Version     State
---------------------------------------- ------------------ ---------   -----
ucs-c220-m3-brdprog.3.0.bin              Board Controller    3.0      Active
ucs-c220-m3-brdprog.3.0.bin              Board Controller    3.0       Active

UCS-A# /server/boardcontroller # show firmware
BoardController:
    Running-Vers: N/A
    Package-Vers:
    Activate-Status: Ready

UCS-A# /server/boardcontroller # activate firmware 3.0 force
Warning: When committed this command will reset the end-point.

UCS-A# /server/boardcontroller* # commit-buffer
```



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
- アダプタの機能

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 からの指示がない限り、必要なのは Cisco UCS インフラストラクチャ ソフトウェア バンドル のダウンロード、更新、アクティブ化の後に機能カタログ更新をアクティブ化にするだけです。

機能カタログ更新をアップデートすると、Cisco UCS はすぐに新しいベースライン カタログに更新します。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。たとえば、Cisco UCS 4.0(1) リリースは、4.0(2) リリースの機能カタログで動作しますが、3.2、3.1、3.0 またはそれ以前のリリースのバージョンでは動作しません。同様に、3.2(1) システムにはリリース 3.2(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、『*Cisco UCS B-Series Servers Documentation Roadmap*』（URL:http://www.cisco.com/go/unifiedcomputing/b-series-doc）にある『*Release Notes for Cisco UCS Administration Software*』を参照してください。

機能カタログ更新のアクティブ化

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope capability**	システム機能モードを開始します。
ステップ 3	UCS-A /system/capability # **activate firmware** *firmware-version*	指定の機能カタログのバージョンをアクティブにします。
ステップ 4	UCS-A /system/capability # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、機能カタログの更新をアクティブにし、トランザクションをコミットします。

```
UCS-A# scope system
UCS-A /system # scope capability
UCS-A /system/capability # activate firmware 4.x(xx)T
UCS-A /system/capability* # commit-buffer
UCS-A /system/capability #
```

機能カタログが最新であることの確認

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope capability**	システム機能モードを開始します。
ステップ 3	UCS-A /system/capability # **show version**	現在の機能カタログのバージョンを表示します。

	コマンドまたはアクション	目的
ステップ 4	Cisco.com で、入手可能な機能カタログの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（169 ページ）を参照してください。
ステップ 5	より新しいバージョンの機能カタログを Cisco.com で入手できる場合は、そのバージョンを使用して機能カタログをアップデートします。	

例

次に、現在の機能カタログのバージョンを表示する例を示します。

```
UCS-A# scope system
UCS-A /system # scope capability
UCS-A /system/capability # show version
Catalog:
    Running-Vers: 4.x(x)T
     Package-Vers: 4.x(x)A
    Activate-Status: Ready
UCS-A /system/capability #
```

機能カタログ更新のリスタート

必要に応じてアップデートパラメータを変更し、失敗した機能カタログファイルのアップデートを再開できます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム コマンド モードを開始します。
ステップ 2	UCS-A /system # **scope capability**	機能コマンド モードを開始します。
ステップ 3	UCS-A /system/capability # **show cat-updater** [*filename*]	（オプション）機能カタログファイルのアップデート操作の更新履歴を表示します。
ステップ 4	UCS-A /system/capability # **scope cat-updater** *filename*	機能カタログファイルのアップデート操作のコマンドモードを開始します。
ステップ 5	UCS-A /system/capability/cat-updater # **set userid** *username*	（オプション）リモートサーバのユーザ名を指定します。

	コマンドまたはアクション	目的
ステップ 6	UCS-A /system/capability/cat-updater # **set password** *password*	（オプション）リモートサーバのユーザ名のパスワードを指定します。 パスワードが設定されていない場合、アップデートを開始するときに、パスワードの入力を求められます。
ステップ 7	UCS-A /system/capability/cat-updater # **set protocol** {**ftp** | **scp** | **sftp** | **tftp** | **usbA** | **usbB**}	（オプション）リモートサーバのファイル転送プロトコルを指定します。 （注） [TFTP] ではファイル サイズが 32 MB に制限されます。カタログイメージはこれよりも大きくなる可能性があるため、カタログ イメージのダウンロードに TFTP を使用しないことを推奨します。
ステップ 8	UCS-A /system/capability/cat-updater # **set server** {*hostname* | *ip-address*}	（オプション）リモートサーバのホスト名またはIPアドレスを指定します。
ステップ 9	UCS-A /system/capability/cat-updater # **set path** *pathname/filename*	（オプション）リモートサーバにある機能カタログ ファイルのパスおよびファイル名を指定します。
ステップ 10	UCS-A /system/capability/cat-updater # **restart**	機能カタログ ファイルのアップデート操作を再開します。

例

次に、サーバのIPアドレスを変更し、機能カタログ ファイルのアップデート操作を再開する例を示します。

```
UCS-A# scope system
UCS-A /system # scope capability
UCS-A /system/capability # show cat-updater ucs-catalog.4.x.xx.T.bin

Catalog Updater:
    File Name                 Protocol Server          Userid          Status
    ---------                 -------- --------------- --------------- ------
    ucs-catalog.4.x.xx.T.bin  Scp      100.0.2.111     user1           Applied

UCS-A /system/capability # scope cat-updater ucs-catalog.4.x.xx.T.bin
UCS-A /system/capability/cat-updater # set server 100.0.2.112
UCS-A /system/capability/cat-updater # restart
UCS-A /system/capability/cat-updater #
```

機能カタログ プロバイダーの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム コマンド モードを開始します。
ステップ 2	UCS-A /system # **scope capability**	機能コマンド モードを開始します。
ステップ 3	UCS-A /system/capability # **show** {**chassis** |**cpu** |**disk** |**fan** |**fru** |**iom** |**memory** |**psu** |**server**} [*vendor model revision*] [**detail** |**expand**]	指定したコンポーネント カテゴリ内のすべてのコンポーネントのベンダー、モデル、およびリビジョン情報を表示します。 特定のコンポーネントの製造およびフォーム ファクタの詳細を表示するには、**expand** キーワードとともに *vendor* 、 *model* 、および *revision* を指定します。これらのフィールドのいずれかにスペースが含まれている場合は、引用符でフィールドを囲む必要があります。

（注） ハード ディスク ドライブやソリッド ステート ドライブなど、1 つ以上の SATA デバイス サーバが含まれている場合、 **show disk** コマンドによって Vendor フィールドに ATA が表示されます。 **expand** キーワードを使用して、ベンダーの詳細情報を表示します。

例

次に、設置済みファンをリストし、機能カタログから特定のファンに関する詳細情報を表示する例を示します。

```
UCS-A# scope system
UCS-A /system # scope capability
UCS-A /system/capability # show fan

Fan Module:
    Vendor                   Model                    HW Revision
    ------------------------ ------------------------ ------------
    Cisco Systems, Inc.      N20-FAN5                 0
    Cisco Systems, Inc.      N10-FAN1                 0
    Cisco Systems, Inc.      N10-FAN2                 0
    Cisco Systems, Inc.      N5K-C5548P-FAN           0
    Cisco Systems, Inc.      N5K-C5596P-FAN           0
    Cisco Systems, Inc.      UCS-FAN-6248UP           0
    Cisco Systems, Inc.      UCS-FAN-6296UP           0
```

```
UCS-A /system/capability # show fan "Cisco Systems, Inc." N10-FAN1 0 expand

Fan Module:
    Vendor: Cisco Systems, Inc.
    Model: N10-FAN1
    Revision: 0

    Equipment Manufacturing:
        Name: Fan Module for UCS 6140 Fabric Interconnect
        PID: N10-FAN1
        VID: NA
        Caption: Fan Module for UCS 6140 Fabric Interconnect
        Part Number: N10-FAN1
        SKU: N10-FAN1
        CLEI:
        Equipment Type:

    Form Factor:
        Depth (C): 6.700000
        Height (C): 1.600000
        Width (C): 4.900000
        Weight (C): 1.500000

UCS-A /system/capability #
```

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。

次のタスク

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。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム コマンド モードを開始します。
ステップ 2	UCS-A /system # **scope capability**	機能コマンド モードを開始します。
ステップ 3	UCS-A /system/capability # **update catalog** *URL*	指定した機能カタログ ファイルをインポートし、適用します。次のいずれかの構文を使用して、操作の URL を指定します。 • **ftp:**// *username***@***hostname* / *path* • **scp:**// *username@hostname* / *path* • **sftp:**// *username@hostname* / *path* • **tftp:**// *hostname* **:** *port-num* / *path* • **usbA:**/ *path* • **usbB:**/ *path* ユーザ名を指定すると、パスワードの入力を求められます。
ステップ 4	UCS-A /system/capability # **show version**	（オプション）カタログ アップデート バージョンを表示します。
ステップ 5	UCS-A /system/capability # **show cat-updater** [*filename*]	（オプション）指定した機能カタログ ファイルまたはすべての機能カタログ ファイルの更新操作の更新履歴を表示します。

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。

例

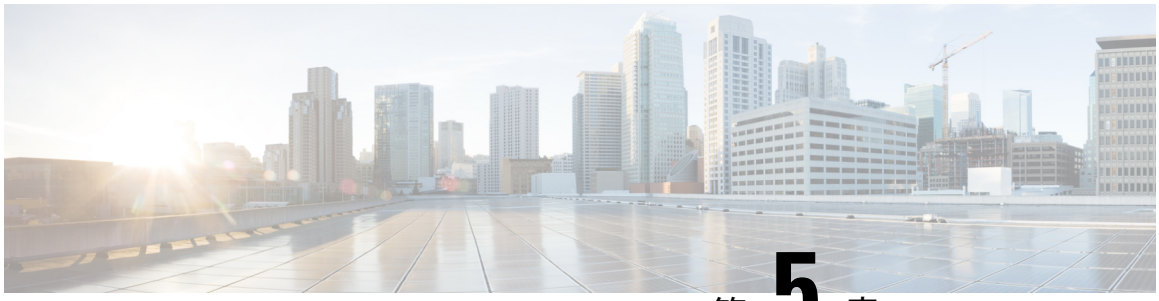
次に、SCP を使用して機能カタログ ファイルをインポートする例を示します。

```
UCS-A# scope system
UCS-A /system # scope capability
UCS-A /system/capability # update catalog
scp://user1@192.0.2.111/catalogs/ucs-catalog.3.1.1a.T.bin
Password:
UCS-A /system/capability # show version
Catalog:
    Update Version: 3.1(1a)T

UCS-A /system/capability # show cat-updater ucs-catalog.3.1.1a.T.bin

Catalog Updater:
    File Name                 Protocol Server          Userid          Status
    ---------                 -------- --------------- --------------- ------
    ucs-catalog.3.1.1a.T.bin  Scp      192.0.2.111     user1           Success

UCS-A /system/capability #
```



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** 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 必須: 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] > [prompt] 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** 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** 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** 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) システムの mgmt0 インターフェイスを有効にするために**no shutdown**コマンドを入力して下さい。

例：

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

d) **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。

始める前に

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 [ナビゲーション]ペインで、[機器]をクリックします。

ステップ 2 **[機器（Equipment）] > [シャーシ（Chassis）] > *[シャーシ番号（Chassis Number）]* > [IO モジュール（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。

翻訳について
このドキュメントは、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。