



Cisco UCS Manager ファームウェア リリース 4.1 管理ガイド

初版：2020 年 2 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/>

© 2020 Cisco Systems, Inc. All rights reserved.



目 次

はじめに :

はじめに ix

対象読者 ix

表記法 ix

関連 Cisco UCS 資料 xi

マニュアルに関するフィードバック xi

第 1 章

概要 1

概要 1

Cisco UCS Manager ユーザ マニュアル 6

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 7

ファームウェア バージョンの用語 9

バージョンをまたがるファームウェアのサポート 10

サーバ パック 12

軽量アップグレード 13

サービス パック 13

サービス パックのバージョン 14

サービス パックのロールバック 15

サービス パックに関するガイドラインと制約事項 16

FI クラスタ用のファームウェア自動同期 16

ファームウェア アップグレードのオプション 17

サービス パックの更新のオプション 19

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 20

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 21

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	21
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	24
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	25
Cisco UCS Manager リリース 4.1 へのファームウェア アップグレード	27
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	31
ファームウェアのダウングレード	32
Cisco UCS Central のファームウェア管理	34

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	37
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	37
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	39
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	40
ファブリック インターコネクト トラフィックの待避	41
セキュア ファームウェア アップデート	44
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	48
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	51
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	52
アップグレード前検証	53
バックアップ ファイルの作成	54
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	54
完全な状態のコンフィギュレーション バックアップ ファイルの作成	56
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	58
Smart Call Home の無効化	58
ファームウェア アップグレード中のフォールト抑制	59
UCS Manager の障害の表示	59
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ポートによって生成される障害	60
障害のベースライン有効期限の変更	60
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	61

ファブリック フェールオーバー用の vNIC 設定の確認	61
ファブリック インターコネクトの運用性の確認	62
クラスタ設定の高可用性ステータスとロールの確認	62
デフォルト メンテナンス ポリシーの設定	63
管理インターフェイスの無効化	64
I/O モジュールのステータスの確認	65
サーバのステータスの確認	65
シャーシのサーバのアダプタのステータスの確認	66
データ パスの準備が整っていることの確認	67
ダイナミック vNIC が稼働中であることの確認	67
イーサネット データ パスの確認	67
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	69
ファイバ チャネル スイッチ モードのデータ パスの確認	70

第 3 章**Cisco UCS Manager によるファームウェアの管理** 71

Cisco UCS Manager でのファームウェアのダウンロードと管理	71
ファームウェア イメージの管理	71
ファームウェア イメージ ヘッダー	73
ファームウェア イメージ カタログ	73
シスコからのソフトウェア バンドルの入手	74
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	76
ローカルファイル システムからファブリック インターコネクトへのファームウェア イメージのダウンロード	79
イメージ ダウンロードのキャンセル	80
ファームウェア パッケージの内容の判断	80
ファームウェア パッケージの内容の準拠の確認	81
ファブリック インターコネクトの空き領域のチェック	81
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	82
後の直接アップグレード 自動インストール	83
自動内部バックアップ	83

ファームウェアインストールの準備	83
インストールインフラストラクチャ ファームウェア	84
インストール サーバ ファームウェア	85
自動インストール のための必要な手順	85
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	86
ファームウェアインストールの準備	87
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	89
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	93
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	95
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	95
自動インストールによるサーバ ファームウェアのアップグレード	96
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 99	
ホスト ファームウェア パッケージ	99
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	101
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	102
ホスト ファームウェア パッケージの作成	107
ホスト ファームウェア パッケージのアップデート	109
既存のサービス プロファイルへのファームウェア パッケージの追加	111
ファームウェアの自動同期	111
ファームウェア自動同期サーバ ポリシーの設定	112
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	113
直接のファームウェア アップグレードのステージ	114
直接のファームウェア アップグレードの停止の影響	116
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	117
複数のエンドポイントのファームウェアのアップデート	120
Cisco UCS Manager ファームウェア	121
Cisco UCS Manager ソフトウェアのアクティビズ化	122

Cisco UCS Manager ソフトウェアのサービス パックのアクティブ化	123
IOM ファームウェア	124
IOM のファームウェアのアップデート	125
複数の IOM でのファームウェアのアクティブ化	126
IOM でのファームウェアのアクティブ化	127
ファブリック インターコネクトのファームウェア	128
従属ファブリック インターコネクトでのファームウェアのアクティブ化	128
プライマリ ファブリック インターコネクトでのファームウェアのアクティブ化	129
スタンダードアロン ファブリック インターコネクトでのファームウェアのアクティブ化	
130	
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	131
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	133
アダプタ ファームウェア	134
アダプタのファームウェアのアップデート	135
アダプタでのファームウェアのアクティブ化	136
BIOS ファームウェア	136
サーバの BIOS ファームウェアのアップデート	137
サーバの BIOS ファームウェアのアクティブ化	137
CIMC ファームウェア	138
サーバの CIMC ファームウェアのアップデート	138
サーバの CIMC ファームウェアのアクティブ化	139
PSU ファームウェア	140
PSU でのファームウェアのアップデート	140
PSU でのファームウェアのアクティブ化	141
ボード コントローラ ファームウェア	142
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	144
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	145

機能カタログの内容	147
機能カタログの更新	148
機能カタログ更新のアクティブ化	149
機能カタログが最新であることの確認	149
機能カタログ プロバイダーの表示	150
シスコからの機能カタログのアップデートの入手方法	150
リモート ロケーションからの機能カタログの更新	151
ローカル ファイル システムからの機能カタログの更新	151

第 5 章

ファームウェアのトラブルシューティング 153

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	153
ファブリック インターコネクトまたはポ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	153
ポ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	158
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	159
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	160
ファームウェア アップグレード中の I/O モジュールの回復	161
ピア I/O モジュールからの I/O モジュールのリセット	162



はじめに

- ・対象読者 (ix ページ)
- ・表記法 (ix ページ)
- ・関連 Cisco UCS 資料 (xi ページ)
- ・マニュアルに関するフィードバック (xi ページ)

対象読者

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

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

表記法

テキストのタイプ	説明
GUI 要素	タブの見出し、領域名、フィールド ラベルなどの GUI 要素は、イタリック体 (<i>italic</i>) で示しています。 ウィンドウ、ダイアログボックス、ウィザードのタイトルなどのメイン タイトルは、ボールド体 (bold) で示しています。
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 (<i>italic</i>) 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、イタリック体 (<i>thisfont</i>) 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考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

安全上の重要な注意事項

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

これらの注意事項を保管しておいてください。

関連 Cisco UCS 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、以下の 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

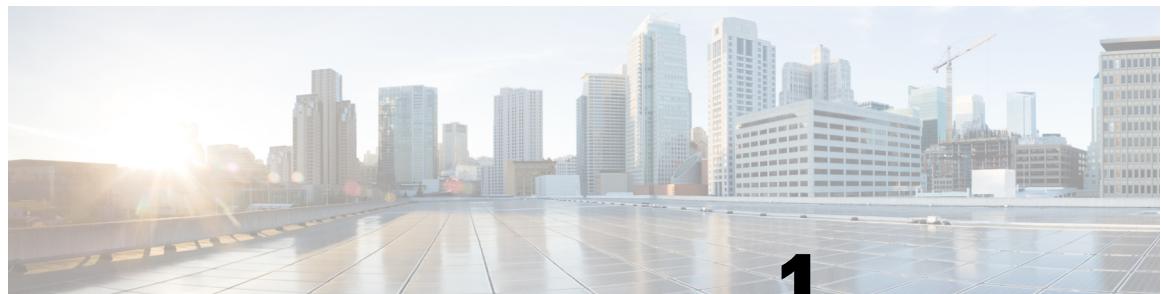
管理用の UCS Manager と統合されたラック サーバでサポートされるファームウェア バージョンとサポートされる UCS Manager バージョンについては、「Release Bundle Contents for Cisco UCS Software」を参照してください。

その他のマニュアル リソース

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

マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、ucs-docfeedback@external.cisco.com までコメントをお送りください。ご協力をよろしくお願ひいたします。



第 1 章

概要

この章は、次の項で構成されています。

- [概要, on page 1](#)
- [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 \(7 ページ\)](#)
- [ファームウェアバージョンの用語, on page 9](#)
- [バージョンをまたがるファームウェアのサポート \(10 ページ\)](#)
- [サーバパック \(12 ページ\)](#)
- [軽量アップグレード \(13 ページ\)](#)
- [FI クラスタ用のファームウェア自動同期 \(16 ページ\)](#)
- [ファームウェアアップグレードのオプション, on page 17](#)
- [Cisco UCS 6200 シリーズファブリックインターフェースから Cisco UCS 6400 シリーズファブリックインターフェースへの移行中のファームウェアアップグレード \(24 ページ\)](#)
- [Cisco UCS Manager リリース 4.1 へのファームウェアアップグレード \(27 ページ\)](#)
- [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 \(31 ページ\)](#)
- [ファームウェアのダウングレード, on page 32](#)
- [Cisco UCS Central のファームウェア管理 \(34 ページ\)](#)

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。

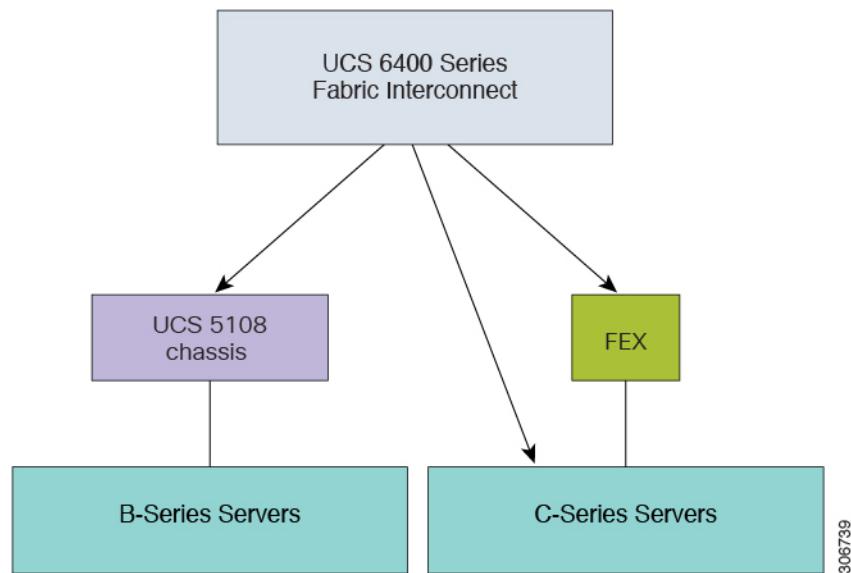
Cisco UCS Manager リリース 4.1(1) では、Cisco UCS 64108 ファブリックインターフェースから Cisco UCS 6400 シリーズファブリックインターフェースを導入します。シスコは Cisco UCS

概要

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



306739

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

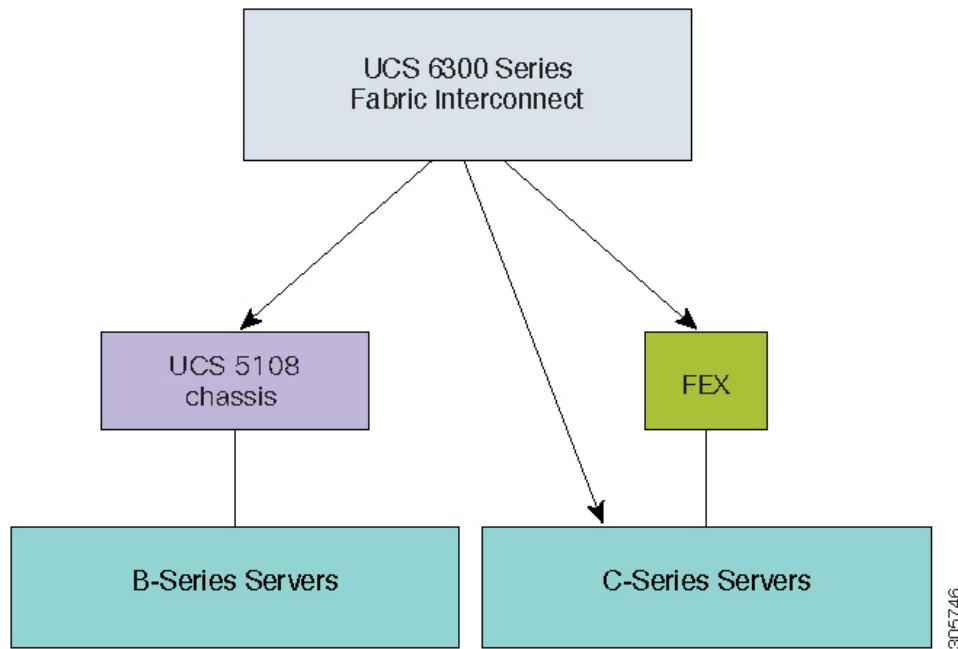
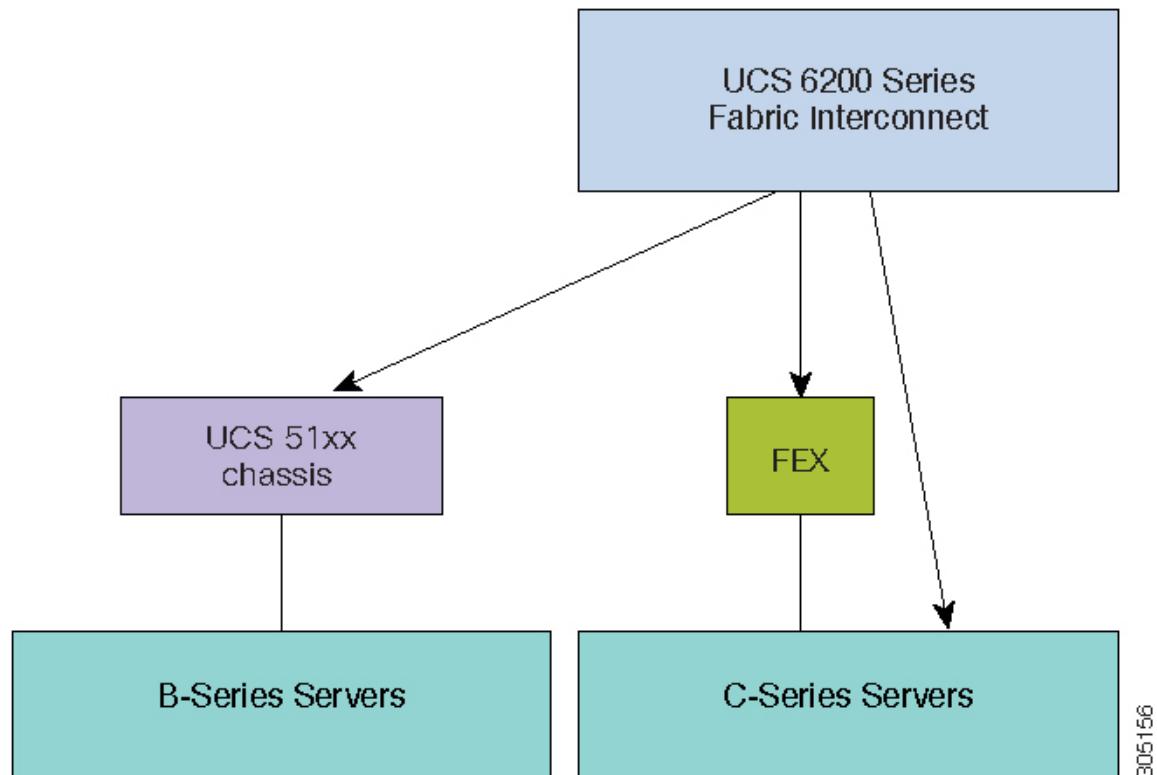
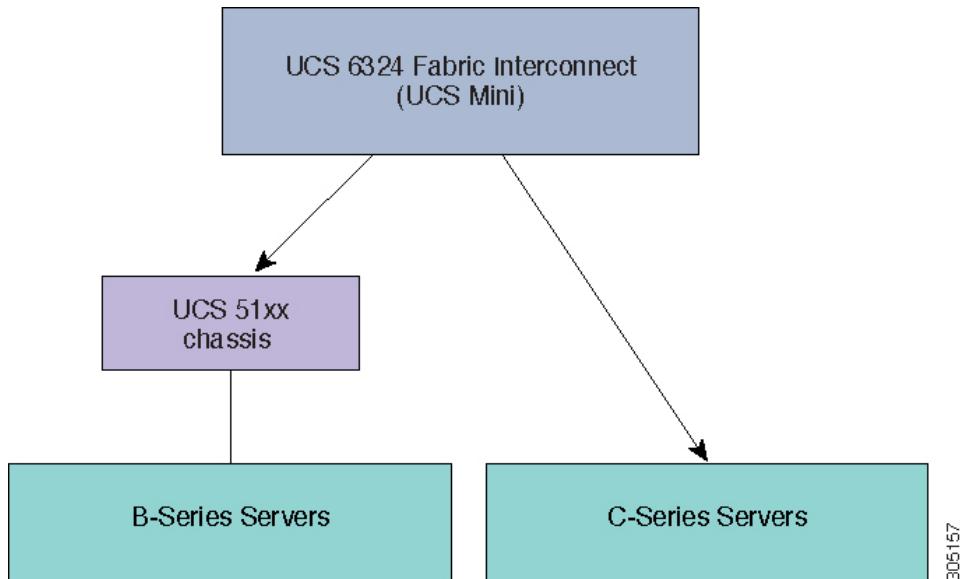


Figure 3: Cisco UCS 6200 シリーズ Fabric Interconnect と Cisco UCS B シリーズ、および C シリーズ サーバ



■ 概要

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



305157

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.4.1.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.4.1.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.4.1.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.4.1.x.xxx.A.bin

- B シリーズ サーバ ソフトウェア バンドル：B バンドルとも呼ばれます。このバンドルには、B シリーズ ブレード サーバが機能するために必要なファームウェア イメージ（アダプタ、BIOS、CIMC、ボード コントローラ ファームウェアなど）が含まれています。

『Release Bundle Contents for Cisco UCS Manager, Release 4.1』には、B シリーズ サーバ ソフトウェア バンドルの内容の詳細が掲載されています。

**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 S3260 ストレージサーバ用のファームウェアイメージも含まれています。『Release Bundle Contents for Cisco UCS Manager リリース 4.1 のリリース バンドルコンテンツ』には、C シリーズ サーバソフトウェア バンドルの内容の詳細が掲載されています。

**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実行されます。このようなアップグレードについては、アップデートまたはアクティブ化のいずれかのみを実行する必要があります。両方の手順を実行する必要はありません。

Cisco UCS Manager ユーザ マニュアル

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

ガイド	説明
Cisco UCS Manager Getting Started Guide	Cisco UCS アーキテクチャのほか、Cisco UCS Manager の初期設定や構成のベストプラクティスなど、稼働前に必要な操作について説明しています。
『Cisco UCS Manager Administration Guide』	パスワード管理、ロールベースアクセスの設定、リモート認証、通信サービス、CIMC セッション管理、組織、バックアップと復元、スケジューリングオプション、BIOS トークン、および遅延展開について説明しています。
Cisco UCS Manager Infrastructure Management Guide	Cisco UCS Manager によって使用および管理される物理インフラストラクチャと仮想インフラストラクチャのコンポーネントについて説明します。
『Cisco UCS Manager Firmware Management Guide』	ファームウェアのダウンロードと管理、自動インストールによるアップグレード、サービスプロファイルによるアップグレード、ファームウェアの自動同期によるエンドポイントでの直接アップグレード、機能カタログの管理、展開シナリオ、およびトラブルシューティングについて説明しています。

ガイド	説明
『Cisco UCS Manager Server Management Guide』	新しいランセンス、Cisco UCS ドメインへの Cisco UCS Central の登録、パワー キヤッピング、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』	Cisco UCS Manager の SAN や VSAN など、ストレージ管理のあらゆる側面について説明しています。
『Cisco UCS Manager Network Management Guide』	Cisco UCS Manager の LAN や VLAN 接続など、ネットワーク管理のあらゆる側面について説明しています。
『Cisco UCS Manager System Monitoring Guide』	Cisco UCS Manager における、システム統計を含むシステムおよびヘルスモニタリングのあらゆる側面について説明しています。
Cisco UCS S3260 サーバと Cisco UCS Manager との統合	Cisco UCS Manager を使用して管理される UCS S シリーズ サーバの管理のあらゆる側面について説明しています。

ファームウェアアップグレードをサポートするコンポーネント

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

- ファブリック インターコネクト :
 - Cisco UCS 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 :

■ 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

- I/O モジュール



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

- 電源装置

- Cisco UCS S3260 シャーシ :

- シャーシ管理コントローラ (CMC)
- シャーシアダプタ
- SAS エクスパンダ
- ボード コントローラ

- サーバ コンポーネント :

- ブレードおよびラック サーバ :
 - アダプタ
 - Cisco Integrated Management Controller (CIMC)
 - BIOS
 - ストレージ コントローラ



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

- ボード コントローラ

- Cisco UCS S3260 ストレージ サーバ ノード :

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

ファームウェアバージョンの用語

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

CIMC、I/Oモジュール、BIOS、CIMC、およびアダプタのファームウェアバージョン

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

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

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、スタートアップバージョンを変更するアクティビ化操作を使用します。

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ビ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、スタートアップバージョンを変更するアクティビ化操作を使用します。

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フェクトおよび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フェクトのファームウェアとファブリックインターフェクト上の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フェクトに保存されるため、ファブリックインターフェクトおよび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フェクトイメージは、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フェクトイメージは、ファブリックインターフェ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フェクトおよび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

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)	2.2(8)	3.1(3)	3.2(3)	4.0(1)	4.0(2)	4.0(4)	4.1(1)
2.2(8)	6200	6200	6200	6200	6200	6200	6200
3.1(3)	—	6200、 6332、 6332-16UP	6200、 6332、 6332-16UP	6200、 6332、 6332-16UP	6200、 6332、 6332-16UP	6200、 6332、 6332-16UP	6200、 6332、 6332-16UP
3.2(3)	—	—	6200、 6332、 6332-16UP	6200、 6332、 6332-16UP	6200、 6332、 6332-16UP	6200、 6332、 6332-16UP	6200、 6332、 6332-16UP
4.0(1)	—	—	—	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
4.0(4)	—	—	—	6200,6332、 6332 16UP、 6454	6200,6332、 6332 16UP、 6454	6200,6332、 6332 16UP、 6454	6200,6332、 6332 16UP、 6454

インフラストラクチャのバージョン (Aバンドル)						
4.1(1)	—	—	—	—	—	—

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

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

インフラストラクチャのバージョン (Aバンドル)						
ホスト FW のバージョン (B または C バンドル)	3.1(3)	3.2(3)	4.0(1)	4.0(2)	4.0(4)	4.1(1)
3.1(3)	6324	6324	6324	6324	6324	6324
3.2(3)	—	6324	6324	6324	6324	6324
4.0(1)	—	—	6324	6324	6324	6324
4.0(2)	—	—	6324	6324	6324	6324
4.0(4)	—	—	6324	6324	6324	6324
4.1(1)	—	—	—	—	—	6324

次の表に、4.1(x)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: 4.1(x)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)	4.1(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
2.2(8) (B、C バンドル)	対応	—	—	—

■ サーバパック

インフラストラクチャのバージョン (Aバンドル)				
3.1(3) (B、C バンドル)	あり	あり	あり	—
3.2(3) (B、C バンドル)	あり	あり	あり	—
4.0(1)、4.0(2)、4.0(4) (B、C バンドル)	あり	あり	あり	あり
4.1(1)	あり	あり	あり	あり



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

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。

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

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

軽量アップグレード

Cisco UCS Manager リリース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ビ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フェイス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フェイストの再起動なしで時々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。

■ サービス パックのバージョン

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トIME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。

■ サービス パックに関するガイドラインと制約事項

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 を強制的にスタンダー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ます、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。

■ ファームウェア アップグレードのオプション

- 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フェース、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フェース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フェクト、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フェ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

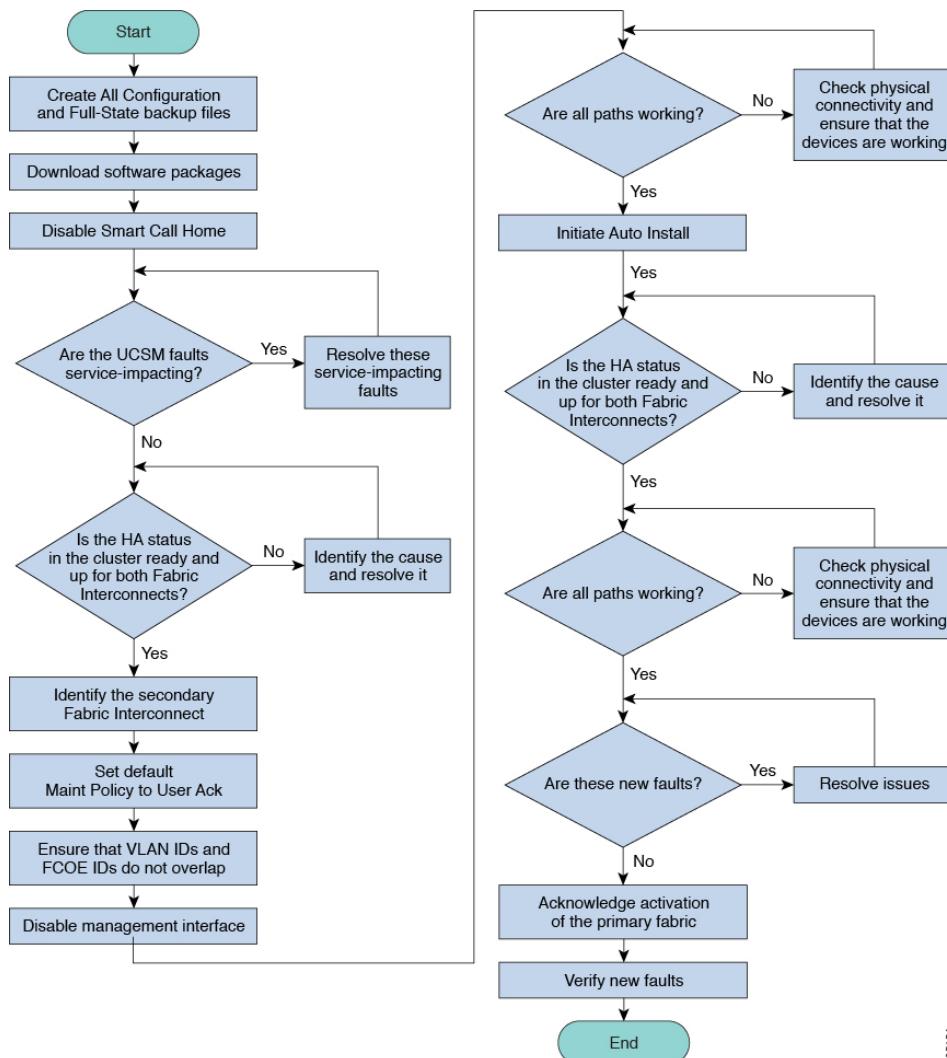
自動インストールによるファームウェアアップグレード

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を使用して、Cisco UCS インフラストラクチャソフトウェアバンドル、ファブリックインターフェクト、I/O モジュールなど、インフラストラクチャのコンポーネントをアップグレードして Cisco UCS Manager。

[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 \(20 ページ\)](#) は自動的にインフラストラクチャのファームウェアをインストールする推奨のプロセスフローを示しています。

図 5: インフラストラクチャファームウェアの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。

305154

- インストールサーバファームウェア：必要に応じて、Cisco UCSB 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止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。

■ 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

インフラストラクチャ	UCS 5108 シャーシ	UCS ラックサーバ	Cisco UCS S3260 シャーシ
<ul style="list-style-type: none"> • Cisco UCS Manager • ファブリックインターフェース <p>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フェースをアップグレードしてください。</p>	<ul style="list-style-type: none"> • I/O モジュール • 電源装置 • サーバー: <ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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 • サーバー: <ul style="list-style-type: none"> • CIMC • BIOS • ボードコントローラ • ストレージコントローラ

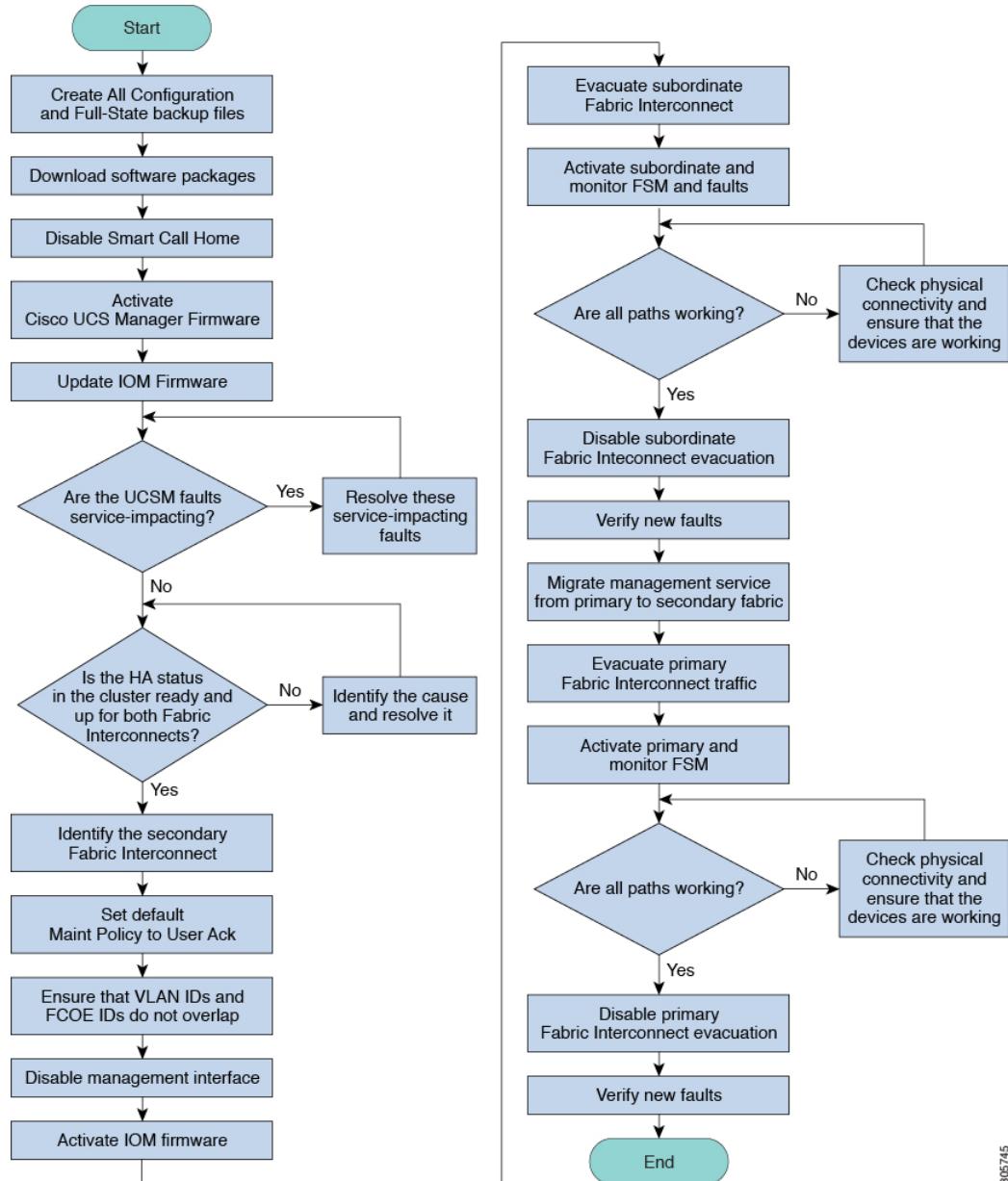


Note

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



305745

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。

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



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、ダウントIME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止が発生します。
- 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 Fabric Interconnect 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 10/25G 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検出ポリシー : 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 モードでシャーシの接続ポリシー : 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 によるサービス 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。

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

- 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) に関する設定をサポートしません。

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 カウントを使用した PV カウントの最適化の無効化	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 の制限事項 : 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 4.1へのファームウェア アップグレード

Cisco UCS Manager リリース 4.1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 4.1(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 2.2(8)、3.1(3)、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 4.1(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 3.1(3) および 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。

表 4: リリース 4.1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	4.1(x)	<p>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。</p> <ol style="list-style-type: none"> リリース 2.2(8) 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 2.2(8) には、B、および C のバンドルのすべてのサーバをアップグレードします。 リリース 3.2(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。

Cisco UCS Manager リリース 4.1へのファームウェア 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
2.2(1)、2.2(2)、2.2(3)、2.2(4)、2.2(5)、2.2(6)、2.2(7)	4.1(x)	<p>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。</p> <ol style="list-style-type: none"> リリース 2.2(8)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 2.2(8)には、B、および C のバンドルのすべてのサーバをアップグレードします。 リリース 3.2(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)	4.1(x)	リリース 4.0(x)に直接アップグレードします。
3.0(x)	4.1(x)	<p>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。</p> <ol style="list-style-type: none"> リリース 3.1(3)または 3.2(3)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(3)または 3.2(3)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。 リリース 4.1(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 (1)、3.1 (2)	4.1(x)	<p>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。</p> <ol style="list-style-type: none"> リリース 3.1(3) または 3.2(3) 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(3) または 3.2(3) 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。 リリース 4.1(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(3)	4.1(x)	リリース 4.0(x)に直接アップグレードします。
3.2(1)、3.2(2)	4.1(x)	<p>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。</p> <ol style="list-style-type: none"> 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。 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。 リリース 3.2(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)	4.1(x)	リリース 4.0(x)に直接アップグレードします。
4.0(x)	4.1(x)	リリース 4.0(x)に直接アップグレードします。

**重要**

クラスタ内の FI を Cisco UCS Manager リリース 2.1(2) 以降のリリースで実行される FI に置き換えてから、自動同期機能を使用することで、この FI を直接 3.2(x) リリースにアップグレードできます。このようなシナリオでは、2.2(8) にまずアップグレードしてから 3.2(x) リリースにアップグレードする必要はありません。

Cisco UCS Manager リリース 4.1へのアップグレード条件

- Cisco UCS Manager リリース 4.1 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りますことを確認してください。
 - Cisco UCS Manager リリース 2.2(8)
 - Cisco UCS Manager リリース 3.1 (3)
 - 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 3.1(3)、3.2(x)、または 4.0(x) リリースから Cisco UCS Manager リリース 4.1 にアップグレードできます。

- Cisco UCS Manager リリース 4.1 にアップグレードする前に、以下を実行して、使用中のキー リングが 2048 ビット以上のモジュラス サイズを備えているか確認してください。

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

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

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

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

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



(注)

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

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

Cisco UCS Manager リリース 4.1 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 4.1 へのアップグレードが失敗し、Cisco UCS Manager は以前のバージョンにロールバックします。

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

アップグレード中の SNMP の自動的な無効化

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



重要

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

マイナーまたはパッチ リリースへのファームウェア アップグレード

Cisco UCS Manager ソフトウェアのリリース番号は、メジャー リリース識別番号、マイナー リリース識別番号、およびパッチ リリース識別番号で構成されます。マイナー リリース識別番号とパッチ リリース識別番号は、カッコ内に列挙されます。たとえば、ソフトウェアバージョン番号が **4.1(2a)** の場合は、次の構成になります。

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

つまり、これらは**4.1** リリーストレインの **first** マイナー リリースの **a** パッチを示しています。

■ ファームウェアのダウングレード

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

Cisco UCS Manager リリース 4.1 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 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を提供します。

- **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 ドメインは、グループ内に定義されている任意のホスト ファームウェア ポリシーを選択できます。Cisco UCS Central を使用すると、ホスト ファームウェアをドメイン グループ内のすべての Cisco UCS ドメインに同時にグローバルにアップグレードすることができます。



(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。

Cisco UCS Central のファームウェア管理



第 2 章

ガイドラインと前提条件

- フームウェア 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）
- Cisco UCS Central のフ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（51 ページ）
- フ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（52 ページ）
- アップグレード前検証（53 ページ）
- データ パスの準備が整っていることの確認（67 ページ）

フ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。

■ 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

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 ブラケットの設定で 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止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 は次のようにになります。

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



(注)

Cisco UCS ドメインでデフォルト VLAN ID の 1 つが使用されているため VLAN のオーバーラップが発生している場合は、1 つ以上のデフォルト VLAN ID を、使用または予約されていない VLAN ID に変更します。リリース 2.0 以降では ID が 4030～4047 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、エンドポイントがあるハードウェアを取り外したり、そこで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フェクトの設定

クラスタ化されたファブリックインターフェクトは、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フェクトのスタンダー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止を最小にできます。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フェクトをリブートする必要があるため、トラフィックの中止は避けられません。

■ 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

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 すべてのエンドポイントを同時にアクティブにしない

Cisco UCS Manager GUIを使用して、ファームウェアをアップデートする場合、[Activate Firmware] ダイアログボックスの [Filter] ドロップダウンリストで [ALL] を選択して、すべてのエンドポイントを同時にアクティブにしないでください。多くのファームウェアリリースやパッチには依存関係があるため、ファームウェアの更新を正常に実行するためにエンドポイントを特定の順序でアクティブにする必要があります。この順序はリリースやパッチの内容によって異なります。すべてのエンドポイントをアクティブにすると、必要な順序でアップデートが行われることが保証されず、エンドポイント、ファブリックインターフェース、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最低 20 % が使用可能である必要があります。ブートフラッシュパーティションが 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フェースのワークスペースパーティションに格納されるのは、テクニカルサポートファイル、コアファイル、およびデバッグプラグインです。アップグレードまたはダウングレードを開始するには、ワークスペースパーティションの最低 20 % が使用可能である必要があります。

アダプタおよびI/O モジュール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、アクティビ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。アクティビ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、アクティビ化されたファームウェアは pending-next-boot 状態のままでです。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したり、ファームウェアをアクティビ化したりしません。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ビにできます。

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ビ化して、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ビ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ビ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。

■ ファブリック インターコネクト トラフィックの待避

4. [Admin Evac Mode] を [Off] に設定して、停止されたすべてのトラフィック フローを再開します。
5. クラスタ リードを下位のファブリック インターコネクトに変更します。
6. ステップ1~4を繰り返し、他のファブリック インターコネクトをアップグレードします。



(注)

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

自動インストールでのファブリック エバキュエーション

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

1. 下位のファブリック インターコネクト (FI-B) が待避させられ、アクティブ化されます。
2. フェールオーバーが発生し、プライマリ ファブリック インターコネクト (FI-A) が下位のファブリック インターコネクトになります。FI-B がクラスタ リードになります。
3. FI-A は待避させられ、アクティブ化されます。

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

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



(注)

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

ファブリック インターコネクト トラフィックの待避の設定

ここで説明する手順を使用することも、この[ビデオ](#)

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

手順

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

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

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

ステップ4 [General] タブの [Actions] 領域で、[Configure Evacuation] をクリックします。
[Configure Evacuation] ダイアログボックスが表示されます。

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

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

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

ステップ7 [Apply] をクリックします。

警告ダイアログボックスが表示されます。

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

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

セキュア フームウェア アップデート

セキュア フームウェア 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 フームウェアを安全に更新できるものです。アダプタの フ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

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、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になっていることが必要です。

- ・クラスタ設定の場合、ファブリックインターフェースの高可用性ステータスに、両方が稼働中であると示されていることを確認します。
- ・スタンドアロン設定の場合、ファブリックインターフェースの [Overall Status] が [Operable] であることを確認します。
- ・アップグレードするすべてのエンドポイントについて、動作可能な状態にあることを確認します。
- ・アップグレードするすべてのサーバについて、すべてのサーバが検出され、検出が失敗しないことを確認します。サーバ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か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 ファームウェアと一緒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	<ul style="list-style-type: none"> ・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

■ 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

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では、毎回ファームウェアバージョンを変更する必要があります。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

■ 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

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なると、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には、Cisco UCS ドメインのすべてのエンドポイントが完全に機能していて、すべてのプロセスが完了している状態でなければなりません。機能状態でないエンドポイントはアップグレードまたはダウングレードすることはできません。

たとえば、検出されていないサーバのファームウェアはアップグレードまたはダウングレードできません。最大回数の再試行後に失敗した FSM などの未完了のプロセスによって、エンドポイントのアップグレードやダウングレードが失敗する可能性があります。FSM が実行中の場合、Cisco UCS Manager によって、アップデートとアクティベーションがキューに入れられ、FSM が正常に完了すると、それらが実行されます。

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



(注) Cisco UCS Manager GUI の [インストールされたファームウェア (Installed Firmware)] タブでは、これらの前提条件を実行するための十分な情報を得られません。

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

- リリース ノートの内容を確認します。
- 適切な『[Hardware and Software Interoperability Matrix](#)』を参照し、すべてのサーバのオペレーティングシステム ドライバのレベルがアップグレード予定の Cisco UCS のリリースに適切なレベルであることを確認します。
- 設定を All Configuration バックアップ ファイルにバックアップします。
- クラスタ設定の場合、ファブリック インターコネクトの高可用性ステータスに、両方が稼働中であると示されていることを確認します。
- スタンドアロン設定の場合、ファブリック インターコネクトの [Overall Status] が [Operable] であることを確認します。
- データパスが稼働中であることを確認します。詳細については、[データパスの準備が整っていることの確認（67 ページ）](#) を参照してください。
- すべてのサーバ、I/O モジュール、アダプタが完全に機能することを確認します。動作不能なサーバはアップグレードできません。
- Cisco UCS ドメインに致命的または重大な障害がないことを確認します。このような障害がある場合は解決してから、システムをアップグレードしてください。致命的または重大な障害があると、アップグレードが失敗する可能性があります。
- すべてのサーバが検出されていることを確認します。サーバの電源を入れる必要はありません。また、サーバをサービス プロファイルと関連付ける必要もありません。
- ラックマウント サーバを Cisco UCS ドメインに統合する場合、Cisco UCS Manager で管理するシステムにラックマウント サーバを設置および統合する方法については、該当する [C シリーズ ラックマウント サーバのインストール ガイド](#) [英語] 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 に表示されるように、各ネットワーク ストレージ デバイスで対応する IQN 発信側名を変更します。

アップグレード前検証

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

■ バックアップファイルの作成

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イ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

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

ステップ2 [All] ノードをクリックします。

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

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

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

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

a) 次のフィールドに入力します。

- [Admin State] フィールド : [Enabled] オプションボタンをクリックすると、[OK] をクリックしてすぐに、バックアップ操作が実行されます。

- [Type] フィールド : [All Configuration] オプションボタンをクリックすると、すべてのシステムおよび論理設定情報を含む XML バックアップファイルが作成されます。

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

- [Preserve Identities] チェック ボックス : Cisco UCS ドメインに、プールから取得され、保存する必要がある ID が含まれる場合、このチェックボックスをオンにします。

[Logical Configuration] タイプのバックアップ操作でこのチェックボックスが選択されている場合、バックアップファイルはプールから取得したすべてのアイデンティティ (vHBA、WWPN、WWNN、vNIC、MAC、UUID を含む) を保存します。

(注) このチェックボックスが選択されていない状態で復元を行うと、アイデンティティが再割り当てされ、ユーザラベルが失われます。

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

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

- [Filename] フィールド：ローカルファイルシステム内の新しい場所にナビゲートするには、[Browse] をクリックします。
- **[Protocol]** フィールド：ファイルをバックアップサーバに転送するために使用するプロトコルを指示する場合に、次のいずれかのオプションボタンをクリックします。
 - **FTP**
 - **TFTP**
 - **SCP**
 - **SFTP**
- **[Hostname]** フィールド：バックアップファイルを格納する場所の IP アドレスまたはホスト名を入力します。これは、サーバ、ストレージアレイ、ローカル ドライブ、またはファブリックインターフェクトがネットワーク経由でアクセス可能な任意の読み取り/書き込みメディアなどがあります。ホスト名を使用する場合、Cisco UCS Manager で DNS サーバを使用するように設定する必要があります。
- **[Remote File]** フィールド：バックアップコンフィギュレーションファイルのフルパスを入力します。このフィールドには、ファイル名とパスを含めることができます。ファイル名を省略すると、バックアップ手順によって、ファイルに名前が割り当てられます。
- **[User]** フィールド：Cisco UCS Manager がバックアップ場所へのログインに使用する必要のあるユーザ名を入力します。プロトコルに TFTP を選択した場合は、このフィールドに入力する必要はありません。
- **[Password]** フィールド：ユーザ名に関連付けられたパスワードを入力します。プロトコルに TFTP を選択した場合は、このフィールドに入力する必要はありません。

- b) [OK] をクリックします。

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

■ 完全な状態のコンフィギュレーションバックアップファイルの作成

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

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

- [Properties] 領域に操作が表示されない場合、[Backup Operations] テーブルの操作をクリックします。
 - [Properties] 領域で、[FSM Details] パーの下矢印をクリックします。
- [FSM Details] 領域が展開され、操作のステータスが表示されます。

ステップ9 [OK] をクリックし、[Backup Configuration] ダイアログボックスを閉じます。

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

完全な状態のコンフィギュレーションバックアップファイルの作成

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

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

ステップ2 [All] ノードをクリックします。

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

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

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

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

- 次のフィールドに入力します。

- **[Admin State]** フィールド : **[Enabled]** オプションボタンをクリックすると、[OK] をクリックしてすぐに、バックアップ操作が実行されます。
- **[Type]** フィールド : システム全体のスナップショットが含まれるバイナリファイルを作成するには、**[Full State]** オプションボタンをクリックします。
- **[Preserve Identities]** チェック ボックス : Cisco UCS ドメインに、プールから取得され、保存する必要がある ID が含まれる場合、このチェックボックスをオンにします。

[Logical Configuration] タイプのバックアップ操作でこのチェックボックスが選択されている場合、バックアップファイルはプールから取得したすべてのアイデンティティ (vHBA、WWPN、WWNN、vNIC、MAC、UUID を含む) を保存します。

(注) このチェックボックスが選択されていない状態で復元を行うと、アイデンティティが再割り当てされ、ユーザラベルが失われます。

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

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

- [Filename] フィールド：ローカルファイルシステム内の新しい場所にナビゲートするには、[Browse] をクリックします。
- **[Protocol]** フィールド：ファイルをバックアップサーバに転送するために使用するプロトコルを指示する場合に、次のいずれかのオプションボタンをクリックします。
 - **FTP**
 - **TFTP**
 - **SCP**
 - **SFTP**
- **[Hostname]** フィールド：バックアップファイルを格納する場所の IP アドレスまたはホスト名を入力します。これは、サーバ、ストレージアレイ、ローカル ドライブ、またはファブリックインターフェクトがネットワーク経由でアクセス可能な任意の読み取り/書き込みメディアなどがあります。ホスト名を使用する場合、Cisco UCS Manager で DNS サーバを使用するように設定する必要があります。
- **[Remote File]** フィールド：バックアップコンフィギュレーションファイルのフルパスを入力します。このフィールドには、ファイル名とパスを含めることができます。ファイル名を省略すると、バックアップ手順によって、ファイルに名前が割り当てられます。
- **[User]** フィールド：Cisco UCS Manager がバックアップ場所へのログインに使用する必要のあるユーザ名を入力します。プロトコルに TFTP を選択した場合は、このフィールドに入力する必要はありません。
- **[Password]** フィールド：ユーザ名に関連付けられたパスワードを入力します。プロトコルに TFTP を選択した場合は、このフィールドに入力する必要はありません。

- b) [OK] をクリックします。

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

■ 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

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

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

- [Properties] 領域に操作が表示されない場合、[Backup Operations] テーブルの操作をクリックします。
 - [Properties] 領域で、[FSM Details] パーの下矢印をクリックします。
- [FSM Details] 領域が展開され、操作のステータスが表示されます。

ステップ9 [OK] をクリックし、[Backup Configuration] ダイアログボックスを閉じます。

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

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

Cisco Smart Call Home は、Cisco UCS の Call Home 機能を強化する Web アプリケーションです。Smart Call Home により、予防的な診断および重要なシステム イベントのリアルタイムの電子メールアラートが提供されます。それにより、ネットワークの可用性が高まり、運用効率が向上します。Smart Call Home は、Cisco UCS の Cisco Unified Computing Support サービスと Cisco Unified Computing Mission Critical Support サービスによって提供されるセキュア接続のサービスです。『Cisco UCS Manager Administration Management Guide』には、Smart Call Home の設定に関する詳細情報が掲載されています。

ファームウェアをアップグレードすると、Cisco UCS Manager によってコンポーネントが再起動され、アップグレードプロセスが完了します。この再起動によって、電子メールアラートがトリガーされる可能性があります。Smart Call Home を無効にすることで、ファームウェアアップグレードプロセス中にこのようなアラートや TAC への自動サポートケースを回避できます。

Smart Call Home の無効化

始める前に

Smart Call Home がすでに有効になっている必要があります。

手順

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

ステップ2 [All] > [Communication Management] > [Call Home] の順に展開します。

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

ステップ4 [Admin] 領域で次の作業を行い、Smart Call Home を無効にします。

- a) [State] フィールドで、[Off] をクリックします。

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

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

ファームウェアアップグレード中のフォールト抑制

障害抑制によって、予定されたメンテナンス時間中に SNMP トランプおよび 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た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フェイク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フェイクによってトリガーされたすべての障害は表示されません。

UCS Manager の障害の表示

手順

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

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

ステップ3 [Faults] をクリックします。

ステップ4 [Work] ペインで、[All] チェックボックスをオンにします。

ステップ5 サービスに影響を及ぼす障害が存在しないことを確認してください。

■ ファブリックインターネッ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ネッ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ネッ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ネッ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求められます。

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ネッ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ネットを再起動する前に、未解決の障害のベースラインを作成します。ファブリックインターネッ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、「ベースラインの有効期限間隔」と呼ばれます。[障害のベースライン有効期限の変更（60ページ）](#)、ベースライン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 Cisco UCS Manager。

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

障害のベースライン有効期限の変更

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

手順

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

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

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

ステップ 4 [Baseline Expiration Interval] 領域で、[dd:hh:mm:ss] フィールドを更新します。

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

デフォルトのベースライン有効期限は 24 時間です。

ステップ 5 [Save Changes] をクリックします。

ファブリック インターコネクトのアップグレード中に生成される障害の表示

手順

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

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

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

ベースラインを作成した後に生成されたすべての障害が表示されます。

ファブリック フェールオーバー用の vNIC 設定の確認

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

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

冗長ハードウェアが設置されており、vNIC がフェールオーバー用に設定されている場合、ファブリック障害によってファブリック フェールオーバーが発生します。ファームウェアをアップグレードする前に、vNIC がファブリック フェールオーバー用に設定されていることを確認してください。

手順

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

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

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

ステップ4 [vNICs] を展開し、指定されたサービスプロファイルの最初の vNIC を選択します。

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

ステップ6 [Properties] 領域で、[Fabric ID] が [Fabric A] であり、[Enable Failover] チェックボックスがオンになっていることを確認します。

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

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

■ ファブリック インターコネクトの運用性の確認

ステップ 9 [Properties] 領域で、[Fabric ID] が [Fabric B] であり、[Enable Failover] チェックボックスがオンになっていることを確認します。

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

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

ファブリック B

ファブリック インターコネクトの運用性の確認

手順

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

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

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

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

ステップ 5 [Status] 領域で、[Overall Status] が [operable] であることを確認します。

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

クラスタ設定の高可用性ステータスとロールの確認

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

手順

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

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

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

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

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

ステップ 6 次のフィールドに次の値が表示されることを確認します。

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

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

ステップ1 [Leadership] フィールドの値に注意して、ファブリックインターフェースがプライマリユニットであるか、従属ユニットであるかを判断します。

この情報は、ファブリックインターフェースのファームウェアをアップグレードするために知っておく必要があります。

デフォルトメンテナンスポリシーの設定

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

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

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

ここで説明する手順を使用することも、この[ビデオ](#)

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

手順

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

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

ステップ3 ポリシーを作成する組織のノードを展開します。

■ 管理インターフェイスの無効化

システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ4 [Maintenance Policies] を展開し、[default] をクリックします。

ステップ5 [Work] ペインの [Main] タブをクリックします。

ステップ6 [Properties] 領域で、[Reboot Policy] として [User Ack] を選択します。

[On Next Boot] チェックボックスが表示されます。

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

ステップ7 (任意) [On Next Boot] オプションを有効にするには、[On Next Boot] チェックボックスをオンにします。

[On Next Boot] オプションが有効な場合、ホストOSのリブート、シャットダウン、リセット、またはサーバリセットとシャットダウンにより、[User Ack] メンテナンスウィンドウを待っている変更を適用するために、関連 FSM もトリガーされます。

ステップ8 [Save Changes] をクリックします。

管理インターフェイスの無効化

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

Cisco UCS Manager によって管理インターフェイスの障害が検出されると、障害レポートが生成されます。障害レポートの数が設定された数に達した場合、システムは管理インターフェイスが使用不能であると見なし、障害を生成します。デフォルトでは、管理インターフェイスモニタリングポリシーは有効です。『Cisco UCS Manager システムモニタリングガイド』には、管理インターフェイス モニタリングポリシーに関する詳細が掲載されています。

手順

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

ステップ2 [All] > [Communication Management] の順に展開します。

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

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

ステップ5 [Management Interfaces Monitoring Policy] タブをクリックし、[Admin Status] フィールドで [Enabled] オプション ボタンをクリックして、管理インターフェイスのモニタリングポリシーを有効にします。

Cisco UCS Manager によって管理インターフェイスの障害が検出されると、障害レポートが生成されます。

- ステップ6** ファブリックインターネットに接続されているアップストリームスイッチへの Telnet セッションを開きます。
- ステップ7** ファブリックインターネットの管理ポートが接続されているインターフェイスの設定を確認し、スイッチの **shut** コマンドを使用して無効にします。
- このインターフェイスを通じて開いているすべての KVM セッションが終了します。
- ステップ8** KVM セッションを再接続して、これらのセッションがセカンダリファブリックインターネットのアップグレードの影響を受けないようにします。

I/O モジュールのステータスの確認

手順

- ステップ1** [Navigation] ペインで [Equipment] をクリックします。
- ステップ2** [Equipment] > [Chassis] の順に展開します。
- ステップ3** I/O モジュールのステータスを確認するシャーシをクリックします。
- ステップ4** [Work] ペインの [IO Modules] タブをクリックします。
- ステップ5** 各 I/O モジュールについて、次のカラムに次の値が表示されることを確認します。

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

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

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

サーバのステータスの確認

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

■ シャーシのサーバのアダプタのステータスの確認

手順

- ステップ1** [Navigation] ペインで [Equipment] をクリックします。
- ステップ2** [Work] ペインの [Servers] タブをクリックして、すべてのシャーシのすべてのサーバのリストを表示します。
- ステップ3** 各サーバについて、次のカラムに次の値が表示されることを確認します。

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

- ステップ4** サーバが検出されていることを確認する必要がある場合、次の手順を実行します。
- 検出のステータスを確認するサーバを右クリックし、[Show Navigator] を選択します。
 - [General] タブの [Status Details] 領域で、[Discovery State] フィールドによって、[complete] の値が表示されていることを確認します。
- [Status Details] 領域のフィールドが表示されない場合は、見出しの右側の [Expand] アイコンをクリックします。

シャーシのサーバのアダプタのステータスの確認

手順

- ステップ1** [Navigation] ペインで [Equipment] をクリックします。
- ステップ2** [Equipment] > [Chassis] > [Chassis Number] > [Servers] の順に展開します。
- ステップ3** アダプタのステータスを確認するサーバをクリックします。
- ステップ4** [Work] ペインの [Inventory] タブをクリックします。
- ステップ5** [Inventory] タブの [Adapters] サブタブをクリックします。
- ステップ6** 各アダプタについて、次のカラムに次の値が表示されることを確認します。

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

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

データ パスの準備が整っていることの確認

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

ダイナミック vNIC が稼働中であることの確認

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

この手順は Cisco UCS Manager GUI で実行します。

手順

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

ステップ 2 [All] > [VMware] > [Virtual Machines] を展開します。

ステップ 3 ダイナミック vNIC を確認する仮想マシンを展開し、ダイナミック vNIC を選択します。

ステップ 4 [Work] ペインで、[VIF] タブをクリックします。

ステップ 5 [VIF] タブで、各 VIF の [Status] カラムが [Online] であることを確認します。

ステップ 6 すべての仮想マシンですべてのダイナミック vNIC の VIF のステータスが [Online] であることを確認するまで、ステップ 3 ~ 5 を繰り返します。

イーサネット データ パスの確認

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A /fabric-interconnect # connect nxos {a b}	ファブリック インターコネクトの NX-OS モードを開始します。
ステップ 2	UCS-A(nxos)# show int br grep -v down wc -l	アクティブなイーサネットインターフェイスの数を返します。

	コマンドまたはアクション	目的								
		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。	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。								
	<table border="1"> <thead> <tr> <th>オプション</th> <th>説明</th> </tr> </thead> <tbody> <tr> <td>show platform fwm info hw-stm grep '1.' wc -l</td> <td>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。</td> </tr> <tr> <td>show hardware internal libsdk mtc l2 mac-table-ce valid-only egrep "^[0-9]" wc -l</td> <td>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。</td> </tr> <tr> <td>show hardware mac address-table 1 wc -l</td> <td>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。</td> </tr> </tbody> </table>	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。	
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。									

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、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フェ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フェクトの 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フェ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フェクト 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フェ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

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、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フェースをアクティビ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

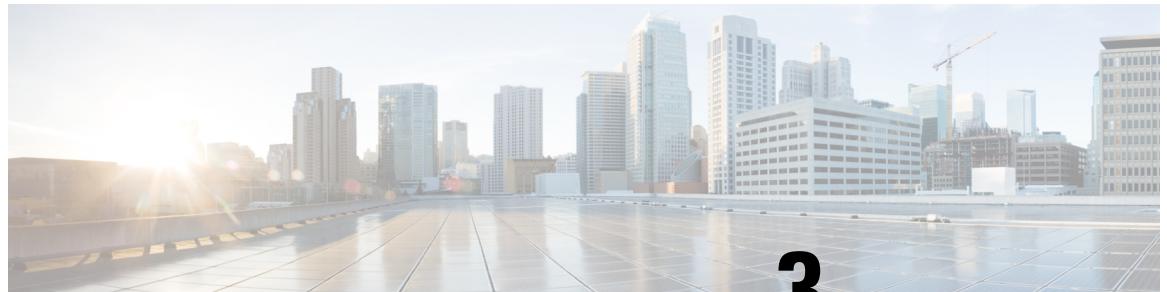
	コマンドまたはアクション	目的
ステップ1	UCS-A /fabric-interconnect # connect nxos {a b}	ファブリックインターフェースのNX-OS モードを開始します。
ステップ2	UCS-A(nxos)# show flogi database	flogi セッションのテーブルを表示します。
ステップ3	UCS-A(nxos)# show flogi database grep -I fc wc -l	ファブリックインターフェースにログインしたサーバの数を返します。 出力は、アップグレードの開始前にこの確認を行ったときに受け取った出力と一致している必要があります。

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フェース 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フェース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 (71 ページ)
- 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 (82 ページ)
- 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, on page 99
- ファームウェアの自動同期 (111 ページ)
- 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, on page 113

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 ドメインのアプリックインターフェース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
- アプリックインターフェースのカーネル ファームウェアとシステム ファームウェア

■ ファームウェア イメージの管理

- 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フェースには、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ビ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フェース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フェースをアクティビ化することはできません。

Cisco UCS B シリーズ ブレードサーバソフトウェアバンドル

このバンドルには、Cisco UCS ドメインのブレードサーバのファームウェアをアップデートするために必要となる、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。

シスコからのソフトウェアバンドルの入手



Tip Cisco UCS Manager によって、ファブリック インターコネクトのポ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ポートフラッシュのスペース使用量は等しくなります。ポ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 [Support] で [All Downloads] をクリックします。

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

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

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

Bundle	ナビゲーションパス
Cisco UCS 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。

Bundle	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、[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。

- [Download Now] : ソフトウェア バンドルをすぐにダウンロードできます。

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

c) メッセージに従ってソフトウェア バンドルのダウンロードを完了します。

ステップ 8 Cisco UCS ドメインをアップグレードする前にリリース ノートをお読みください。

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ネットへのファームウェアイメージのダウンロード

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

**Note**

クラスタ構成では、どちらのファブリックインターネットを使用してダウンロードを開始しても、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ネットにダウンロードされます。Cisco UCS Managerにより、両方のファブリックインターネットのすべてのファームウェアパッケージとイメージは同期状態に保たれます。ファブリックインターネットの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ネットに同期されます。

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

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

ステップ2 [Equipment] ノードをクリックします。

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

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

ステップ5 [Download Firmware] をクリックします。

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

名前	説明
[Protocol] フィールド	<p>リモートサーバとの通信時に使用するプロトコル。次のいずれかになります。</p> <ul style="list-style-type: none"> • FTP • TFTP <p>Note TFTP ファイルサイズの限度は 32 MB です。ファームウェア バンドルは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。</p> <ul style="list-style-type: none"> • SCP • SFTP <ul style="list-style-type: none"> • [USB A] : ファブリック インターコネクト A に挿入された USB ドライブ。 • [USB B] : ファブリック インターコネクト B に挿入された USB ドライブ。 <p>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。</p> <p>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。</p>
[Server] フィールド	<p>ファイルがリモートサーバのファイルである場合は、ファイルが存在するリモートサーバの IP アドレスまたはホスト名。ファイルがローカルソースのファイルである場合、このフィールドには「local」が表示されます。</p> <p>Note 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 [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 [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。</p>
[Filename] フィールド	ファームウェア ファイルの名前。

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

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

ステップ 7 [OK] をクリックします。

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

ステップ 8 (Optional) [Download Tasks] タブで、ダウンロードのステータスをモニタします。

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

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

What to do next

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

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



(注)

クラスタ構成では、どちらのファブリック インターコネクトを使用してダウンロードを開始しても、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により、両方のファブリック インターコネクトのすべてのファームウェア パッケージとイメージは同期状態に保たれます。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。

始める前に

必要なファームウェア バンドルをシスコから入手します。

手順

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

ステップ2 [Equipment] ノードをクリックします。

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

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

ステップ5 [Download Firmware] をクリックします。

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

ステップ7 [Filename] フィールドに、イメージ ファイルのフルパスと名前を入力します。

ファームウェア イメージ ファイルが配置されているフォルダへの正確なパスがわからない場合は、[Browse] をクリックしてファイルにナビゲートします。

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

ステップ8 [OK] をクリックします。

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

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

■ イメージダウンロードのキャンセル

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

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

次のタスク

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

イメージダウンロードのキャンセル

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

Procedure

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

ステップ 2 [Equipment] ノードを展開します。

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

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

ファームウェア パッケージの内容の判断

手順

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

ステップ 2 [Equipment] ノードをクリックします。

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

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

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

a) イメージ名とその内容を含む行を強調表示します。

- b) 右クリックし、[Copy] を選択します。
 - c) クリップボードの内容をテキストファイルまたは他のドキュメントに貼り付けます。
-

ファームウェア パッケージの内容の準拠の確認

適合チェック機能を使用して、選択したバンドルに対して、すべてのコンポーネントが正しいファームウェア バージョンを実行していることを確認できます。これは、ファームウェアのアップグレードを実行する前で、アップグレードが完了した後に使用しないでください。

手順

- ステップ1** [Navigation] ペインで [Equipment] をクリックします。
 - ステップ2** [Equipment] ノードをクリックします。
 - ステップ3** [Work] ペインの [Firmware Management] タブをクリックします。
 - ステップ4** [Packages] サブタブでは、適合性を確認するパッケージを選択します。
 - ステップ5** [Check Conformance]] をクリックします。
 - ステップ6** 表示されるダイアログボックスの [Message] カラムには、各コンポーネントがファームウェア パッケージに適合しているかどうかが表示されます。
-

ファブリック インターコネクトの空き領域のチェック

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

手順

- ステップ1** [Navigation] ペインで [Equipment] をクリックします。
- ステップ2** [Equipment] > [Fabric Interconnects] の順に展開します。
- ステップ3** 空き領域をチェックするファブリック インターコネクトをクリックします。
- ステップ4** [Work] ペインで、[General] タブをクリックします。
- ステップ5** [Local Storage Information] 領域を展開します。

ファームウェアイメージバンドルをダウンロードする場合、ファブリック インターコネクトに、ファームウェアイメージバンドルのサイズの少なくとも2倍の空き領域が必要です。ブート フラッシュに十分な領域がない場合は、ファブリック インターコネクトから、古いファームウェア、コア ファイル、およびテクニカル サポート ファイルを削除してください。

自動インストールによるファームウェアアップグレード

自動インストールでは、次の段階によって、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 \(71 ページ\)](#) 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 \(86 ページ\)](#) 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 \(48 ページ\)](#) 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フェイク、およびIOMの直接アップグレードまたはアクティビティ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ビティ化を開始する前に、スタートアップバージョンがクリアされていることを確認します。デフォルトインフラストラクチャパックのスタートアップバージョンが設定されている場合、Cisco UCS Manager、ファブリックインターフェイク、およびIOMを直接アップグレードまたはアクティビティ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（95ページ）](#)は、スタートアップバージョンのクリアリングに関する詳細な手順を説明します。

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フェイクの /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フェイク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フェイク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

■ インストールインフラストラクチャ ファームウェア

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フェクトおよび 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、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 は変更をただちに適用します。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

■ 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

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、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 (54 ページ)、完全な状態のコンフィギュレーション バックアップファイルの作成 (56 ページ) を作成します。
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 (76 ページ)、およびローカル ファイル システムからファブリック インターコネクトへのファームウェア イメージのダウンロード (79 ページ)、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。ファームウェア インストールの準備 (87 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 (58 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 故障を確認し、サービスに影響を与える故障を解決します。故障の検証に関する詳細情報を提供します。UCS Manager の障害の表示 (59 ページ) は、故障の検証に関する詳細情報を提供します。
 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 (62 ページ) は、故障の確認に関する詳細情報を提供します。
 3. デフォルトのメンテナンス ポリシーを設定します。デフォルト メンテナンス ポリシーの設定 (63 ページ) は詳細な情報を提供します。また、このビデオ

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

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（64 ページ）](#) には、セカンダリファブリックインターフェイスク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（67 ページ）](#) は詳細な情報を提供します。
3. 自動インストールによってインフラストラクチャ ファームウェアをアップグレードします。 [自動インストールによるインフラストラクチャ ファームウェアのアップグレード（89 ページ）](#) は詳細情報を提供します。また、このビデオ (http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/upgrade_the_infrastructure_firmware_with_auto_install.html) の [Play] をクリックして、自動インストールでインフラストラクチャ ファームウェアをアップグレードする方法を視聴することもできます。



(注)

[Prepare for Firmware Install] を使用してインフラストラクチャ ファームウェアをステージングした場合、再起動が必要な場合は、この手順には再起動を伴うアクティブ化のみが含まれます。

4. クラスタの高可用性ステータスを確認します。
5. すべてのパスが動作していることを確認します。
6. 新しい障害を確認します。 [ファブリックインターフェイスクのアップグレード中に生成される障害の表示（61 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フェイスクのリブートの確認（93 ページ）](#) は詳細情報を提供します。また、このビデオ (http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/acknowledge_pending_reboot_of_the_primary_fabric_interface.html) の [Play] をクリックして、プライマリファブリックインターフェイスクのリブートを確認する方法を視聴することもできます。
8. 新しい障害を確認します。

ファームウェアインストールの準備

手順

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

■ ファームウェアインストールの準備

ステップ2 [Equipment] ノードをクリックします。

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

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

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

ステップ6 [Install Server Firmware] ウィザードの [Prepare for Firmware Install] ページで、次の手順を実行します。

- Cisco UCS ドメインのインフラストラクチャコンポーネントを更新するには、[A-Series Infrastructure Firmware] 領域で [New Version] ドロップダウンリストからアップグレードするソフトウェアバンドルを選択します。
- Cisco UCS ドメインのブレードサーバを更新するには、[B-Series Blade Server Firmware] 領域の [New Version] ドロップダウンリストからアップグレードするソフトウェアバンドルを選択します。
- にCisco UCS ドメインのラックマウントサーバと S3260 シャーシを更新するには、[C-Series Chassis/Rack-Mount Server Firmware] 領域の [New Version] ドロップダウンリストからアップグレードするソフトウェアバンドルを選択します。

Cisco UCS ドメインにブレードサーバとラックサーバの両方が含まれている場合は、[Select Package Versions] ページで B シリーズブレードサーバおよび C シリーズラックマウントサーバの新しいファームウェアバージョンを選択して、ドメイン内のすべてのサーバをアップグレードすることを推奨します。

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

- [Next] をクリックします。

ステップ7 [Prepare for Firmware Install] ウィザードの [Select Firmware Packages] ページで、次を実行します。

- 選択したソフトウェアで更新するファームウェアパッケージが含まれる各組織のノードを展開します。
- 更新する各ファームウェアパッケージの名前の隣にあるチェックボックスをオンにします。

この手順によって、選択したすべてのインフラ、ホスト、シャーシファームウェアパッケージを新しいファームウェアバージョンに変更します。

- [Next] をクリックします。

ステップ8 [Prepare for Firmware Install] ウィザードの [Firmware Package Dependencies] ページで、次を実行します。

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

- b) ホストまたはシャーシ ファームウェア パッケージが含まれるサービスまたはシャシープロファイルのリストを確認します。
- c) 必要に応じて、次のいずれかのカラムにあるリンクをクリックします。
 - [Host/Chassis Pack DN] カラム：ホストまたはシャーシ ファームウェア パッケージのナビゲータを開きます。
 - [Service/Chassis Profile DN] カラム: サービスまたはシャシープロファイルのナビゲータを開きます。
- d) 次のいずれかを実行します。
 - 選択したファームウェア パッケージを 1 つ以上変更する場合は、[Prev] をクリックします。
 - 適切なファームウェア パッケージを選択済みで、エンドポイントのファームウェアの更新の影響を確認する場合は、[Next] をクリックします。
 - ファームウェアの更新をすぐに開始するには、[Update]をクリックします。

ステップ 9 [Prepare for Firmware Install] ウィザードの [Endpoints Summary] ページで、次の手順を実行します。

- a) [UCS Firmware Pack Endpoints] 表で結果をフィルタリングするには、該当するチェックボックスをオンにします。
エンドポイントのタイプによって、結果をフィルタリングできます。
- b) 影響を受けるエンドポイントのリストを確認します。
- c) 次のいずれかを実行します。
 - 選択したファームウェア パッケージを 1 つ以上変更する場合は、[Prev] をクリックします。
 - 適切なファームウェア パッケージを選択済みで、サーバのアップグレードを開始する場合は、[Update]をクリックします。

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

■ 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



(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（48 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

- ・ [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（52 ページ）](#) に記載のすべての前提条件を満たす必要があります。
- ・ Cisco UCS 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準備します。 [ファームウェアインストールの準備（87 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) 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

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

ステップ2 [Equipment] ノードをクリックします。

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

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

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

ステップ6 [Install Infrastructure] ダイアログ ボックスの [Prerequisites] ページで、先に進む前に警告に対処します。

警告は次のカテゴリに分類されています。

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

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

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

名前	説明
[Name] フィールド	Cisco UCS によって作成および管理されるインフラストラクチャ パックの名前。このフィールドのデフォルト名を変更したり、カスタムインフラストラクチャ パックを作成することはできません。
[Description] フィールド	インフラストラクチャ パックのユーザ定義による説明。このフィールドはデフォルトで入力されています。ただし、必要に応じて独自の説明を入力することもできます。 256 文字以下で入力します。任意の文字またはスペースを使用できます。ただし、' (アクセント記号) 、\ (バックスラッシュ) 、^ (キャラット) 、" (二重引用符) 、= (等号) 、> (大なり) 、< (小なり) 、または' (一重引用符) は使用できません。
[Backup Version] フィールド	[Prepare for Firmware Install] を介してファームウェアのインストールのステージング ファームウェア バージョンがステージングされていない場合、このフィールドは空です。

■ 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

名前	説明
[Infra Pack] ドロップダウンリスト	<p>インフラストラクチャ コンポーネントのファームウェア アップグレードに使用できるソフトウェア バンドルのリスト。</p> <p>インフラパックバージョンがバックアップバージョンと異なる場合、ダウンタイムには準備の時間を含み、選択されたインフラパックバージョンをアクティブにします。</p> <p>インフラパックバージョンがバックアップバージョンと同じ場合、ダウンタイムには選択されたインフラパックバージョンをアクティブにする時間を含みます。</p>
[Service Pack] ドロップダウンリスト	<p>インフラストラクチャ コンポーネントのファームウェアのアップグレードに使用できるサービスパックバンドルのリスト。</p> <p>基本のインフラパックを選択せずに直接サービスパックにアップグレードすることはできません。</p> <p>(注) サービスパックは基本のメンテナンスリリースにのみ適用できます。たとえば、サービスパック 3.1(3)SP2 は 3.1(3) リリースにのみ適用できます。3.1(4) リリースに適用することはできません。</p> <p>[Service Pack] を [<not set>] に設定すると、サービスパックがファームウェア パッケージから削除されます。</p>
[Force] チェックボックス	オンにすると、Cisco UCSでは、選択したバージョンを前回インストールしようとしたときに失敗または中断した場合でも、インストールを試みます。
[Evacuate] チェックボックス	オンにすると、自動インストールによってアップグレードされている各ファブリックインターフェイスクエニクト上でファブリックエバキュエーションが有効になります。両方のファブリックインターフェイスクエニクトが待避させられますが、同時にではありません。

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

オプション	説明
[Start Time] フィールド	<p>オカレンスが実行される日時。</p> <p>フィールドの端にある下矢印をクリックして、カレンダーから日付を選択します。</p>

オプション	説明
[Upgrade Now] チェック ボックス	オンにすると、Cisco UCS Manager は [Start Time] フィールドを無視して、[OK] がクリックされるとすぐにインフラストラクチャ ファームウェアをアップグレードします。

ステップ9 [OK] をクリックします。

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

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

次のタスク

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

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/en/ustd/docs/unified_computing/ucs_manager/videos/3-1/acknowledge_pending_reboot_of_the_primary_fabric_interconnect.html) の [Play] をクリックしてプライマリ ファブリック インターコネクトのリブートを確認する方法を視聴することもできます。

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承認する前に、セカンダリ ファブリック インターコネクトからデータ パスが正常に復元されていることを確認します。
詳細については、[データ パスの準備が整っていることの確認（67 ページ）](#) を参照してください。

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

手順

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

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

ステップ3 [Fabric Interconnects] サブタブをクリックし、[Reboot now] をクリックします。

ステップ4 表示される警告ダイアログボックスで [Yes] をクリックします。

警告ダイアログボックスには、最後のリブート後に未確認の障害があることが示され、続行するかどうかを尋ねられます。

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

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

インフラストラクチャ ファームウェアのアップグレードのキャンセル



(注)

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

手順

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

ステップ2 [Equipment] ノードをクリックします。

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

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

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

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

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

ステップ8 [OK] をクリックします。

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

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

手順

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

ステップ2 [Equipment] ノードをクリックします。

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

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

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

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

ステップ7 [OK] をクリックします。

■ 自動インストールによるサーバ ファームウェアのアップグレード

この手順で、ブレード サーバまたはラック マウント サーバの一括アップグレードを実行できます。

Prepare for Firmware Installでサーバ ファームウェアをステージングした場合、そのバックアップ バージョンがこの手順で選択したサーバ ファームウェア バージョンと同じであれば、そのバックアップ 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ます。

以前にバックアップ バージョンを設定していない場合は、選択したファームウェア バージョンがバックアップ バージョンとして設定されます。このバージョンが起動バージョンとして設定されます。

この段階を完了すると再起動します。



- (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（48 ページ）](#) および該当する『Cisco UCS upgrade guide』を参照してください。



- (注) [Install Server Firmware] ウィザードの設定が完了した後で、サーバ ファームウェアのアップグレード プロセスをキャンセルすることはできません。Cisco UCS Manager は変更をただちに適用します。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。

始める前に

- ・[ファームウェアのアップグレードとダウングレードの前提条件（52 ページ）](#) に記載のすべての前提条件を満たす必要があります。
- ・Cisco UCS 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、サーバのファームウェアをステージングします。[ファームウェアインストールの準備（87 ページ）](#) は、サーバー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) オプションですが、これもお勧めします。

手順

- ステップ1** [Navigation] ペインで [Equipment] をクリックします。
- ステップ2** [Equipment] ノードをクリックします。
- ステップ3** [Work] ペインの [Firmware Management] タブをクリックします。
- ステップ4** [Work] ペインの [Firmware Auto Install] タブをクリックします。
- ステップ5** [Actions] 領域で、[Install Server Firmware] をクリックします。
- ステップ6** [Install Server Firmware] ウィザードの [Prerequisites] ページで、このページに一覧されている前提条件とガイドラインを慎重に確認してから、次のいずれかを実行してください。
- 前提条件をすべて満たしている場合は、[Next] をクリックします。
 - 前提条件をすべて満たしていない場合は [Cancel] をクリックして、サーバのファームウェアをアップグレードする前に前提条件を満たしてください。
- ステップ7** [Install Server Firmware] ウィザードの [Select Package Versions] ページで、次の手順を実行します。
- a) Cisco UCS ドメインにブレードサーバが含まれている場合は、[B-Series Blade Server Software] 領域の [New Version] ドロップダウンリストから、これらのサーバをアップグレードするソフトウェアバンドルを選択します。
 - b) Cisco UCS ドメインにラックマウントサーバが含まれている場合は、[C-Series Rack-Mount Server Software] 領域の [New Version] ドロップダウンリストから、これらのサーバをアップグレードするソフトウェアバンドルを選択します。
- Cisco UCS ドメインにブレードサーバとラックサーバの両方が含まれている場合は、[Select Package Versions] ページで B シリーズブレードサーバおよび C シリーズラックマウントサーバの新しいファームウェアバージョンを選択して、ドメイン内のすべてのサーバをアップグレードすることを推奨します。
- (注) デフォルトのホストファームウェアパッケージを更新すると、関連付けられていないサーバと、ホストファームウェアパッケージを含まないサービスプロファイルが関連付けられたサーバで、ファームウェアがアップグレードされることがあります。このファームウェアアップグレードにより、サービスプロファイルで定義されたメンテナンスポリシーに従ってこれらのサーバのリポートが発生する可能性があります。
- c) サーバをサービスパックのファームウェアバージョンにアップグレードするには、[Service-Pack Firmware] 領域の [New Version] ドロップダウンリストからこれらのサーバをアップグレードするサービスパックを選択します。
 - d) [Next] をクリックします。
- ステップ8** [Install Server Firmware] ウィザードの [Select Firmware Packages] ページで、次を実行します。
- a) 選択したソフトウェアで更新するホストファームウェアパッケージが含まれる各組織のノードを展開します。

■ 自動インストールによるサーバ ファームウェアのアップグレード

ホスト ファームウェア パッケージのファームウェア バージョンがステージングされている場合は、ホスト ファームウェア パッケージの名前と共に**[Backup Version]** フィールドに表示されます。

- 更新する各ホスト ファームウェア パッケージの名前の隣にあるチェックボックスをオンにします。

この手順によって、選択したホスト ファームウェア パッケージが新しいバージョンの ファームウェアによって更新されます。すべてのサーバを更新するには、Cisco UCS ドメインのすべてのサーバに関連付けられたサービス プロファイルに含まれているホスト ファームウェア パッケージを選択する必要があります。

- [Next] をクリックします。

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

- テーブルに表示される各ホスト ファームウェア パッケージのノードを展開します。
- ホスト ファームウェア パッケージが含まれるサービス プロファイルのリストを確認します。
- 必要に応じて、次のいずれかのカラムにあるリンクをクリックします。

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

- 次のいずれかを実行します。

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

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

- [Impacted Endpoints] テーブルで結果をフィルタリングするには、該当するチェックボックスをオンにします。

結果は、エンドポイントのタイプや、アップグレードの影響が重大であるかどうかによってフィルタリングできます。

- 影響を受けるエンドポイントのリストを確認します。
- 必要に応じて、**[Maintenance Policy]** カラムのリンクをクリックして、そのポリシーのナビゲータを開きます。
- 次のいずれかを実行します。
 - 選択したホスト ファームウェア パッケージを 1 つ以上変更する場合は、[Prev] をクリックします。

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

ステップ 11 (任意) サーバ ファームウェアのアップグレードの進行状況をチェックするには、アップグレードする各サーバの [FSM] タブをチェックします。

[Firmware Auto Install] タブの [Firmware Installer] フィールドには、インフラストラクチャ ファームウェアのアップグレードのステータスだけが表示されます。

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

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

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

ホスト ファームウェア パッケージ

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

- アダプタ
- BIOS
- CIMC



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

■ ホストファームウェアパッケージ

- **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ケージから除外されます。

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つ

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 トランザクションが中断します。

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。

■ 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

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
<p>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。</p> <p>または</p> <p>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。</p>	メンテナンス ポリシーなし	<p>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。</p> <ul style="list-style-type: none"> 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。 <ol style="list-style-type: none"> 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。 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。 サーバを新規サービス プロファイルと関連付けます。 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。 <p>注意 元のサービス プロファイルにスクラップ 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。</p>

■ 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	メンテナンス ポリシー	アップグレード処理
<p>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。</p> <p>または</p> <p>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。</p>	<p>メンテナンス ポリシーなし</p> <p>または</p> <p>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。</p>	<p>ファームウェア パッケージをアップデートすると、次のようにになります。</p> <ol style="list-style-type: none"> 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。 <p>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。</p>

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
<p>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。</p> <p>または</p> <p>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。</p>	<p>ユーザ確認応答に関して設定済み</p>	<p>ファームウェア パッケージをアップデートすると、次のようにになります。</p> <ol style="list-style-type: none"> Cisco UCS によって、変更を確認するよう要求され、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。 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。 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。 <p>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。</p>

■ 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	メンテナンス ポリシー	アップグレード処理
<p>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。</p> <p>または</p> <p>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。</p>	[On Next Boot] オプションでユーザ確認応答に関して設定済み	<p>ファームウェア パッケージをアップデートすると、次のようにになります。</p> <ol style="list-style-type: none"> 1. Cisco UCSによって、変更を確認するようい要求され、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。 <ul style="list-style-type: none"> 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。 <p>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。</p>

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
<p>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。</p> <p>または</p> <p>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。</p>	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する設定済み。	<p>ファームウェア パッケージをアップデートすると、次のようにになります。</p> <ol style="list-style-type: none"> 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。 <p>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。</p>

ホスト ファームウェア パッケージの作成



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。

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

**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フェース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

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

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

ステップ3 ポリシーを作成する組織のノードを展開します。

システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

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

ステップ5 [Create Host Firmware Package] ダイアログボックスで、パッケージの一意の名前と説明を入力します。

この名前には、1～32文字の英数字を使用できます。- (ハイフン)、_ (アンダースコア)、: (コロン)、および (ピリオド) は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後にこの名前を変更することはできません。

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

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

[Service Pack] からのイメージは、[Blade Package] または [Rack Package] のイメージよりも優先されます。

ステップ8 [Excluded Components] 領域で、このホストファームウェアパッケージから除外するコンポーネントに対応するチェックボックスをオンにします。

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

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

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

- a) [Select] カラムで、該当する行のチェックボックスがオンになっていることを確認します。
- b) [Vendor]、[Model]、および[PID] カラムで、情報がこのパッケージを使用して更新するサーバに一致していることを確認します。

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

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

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

What to do next

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

ホスト ファームウェア パッケージのアップデート

ポリシーが、メンテナンス ポリシーを含まない1つ以上のサービス プロファイルに含まれている場合、Cisco UCS Managerはサーバ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。また、メンテナンス ウィンドウを設定およびスケジュールしていない場合、ホスト ファームウェア パッケージ ポリシーを保存するときに Cisco UCS Managerによってサーバがリブートされます。

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



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

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

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

ステップ3 アップデートするポリシーを含む組織のノードを展開します。

■ ホストファームウェアパッケージのアップデート

システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

- ステップ 4** [Host Firmware Packages] を展開し、アップデートするポリシーを選択します。
 - ステップ 5** [Work] ペインで、[General] タブをクリックします。
 - ステップ 6** 各サブタブで、パッケージに含めるファームウェアのタイプごとに次の手順を実行します。
 - a) [Select] カラムで、該当する行のチェックボックスがオンになっていることを確認します。
 - b) [Vendor]、[Model]、および[PID] カラムで、情報がこのパッケージを使用して更新するサーバに一致していることを確認します。
 - c) 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 7** 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 8** 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 9** 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 10** 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 11** 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 12** [OK] をクリックします。
- 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。

既存のサービス プロファイルへのファームウェア パッケージの追加

メンテナンス ポリシーを含まないサービス プロファイルがサーバに関連付けられている場合、Cisco UCS Managerはサーバのファームウェアを新しいバージョンに更新してアクティブ化し、サービス プロファイルの変更が保存されるとただちにサーバをリブートします。

手順

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

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

ステップ3 アップデートするサービス プロファイルが含まれている組織のノードを展開します。

システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

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

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

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

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

ステップ8 [Save Changes] をクリックします。

ファームウェアの自動同期

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



重要

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

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

- [No Action] : ファームウェアのアップグレードはサーバで開始されません。

■ ファームウェア自動同期サーバポリシーの設定

この値は、デフォルトで選択されます。

- [User Acknowledge] : [Pending Activities] ダイアログボックスで管理者がアップグレードを確認するまでサーバのファームウェアは同期されません。

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

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



重要

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

ファームウェア自動同期サーバポリシーの設定

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

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

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

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

ステップ2 [Equipment] ノードをクリックします。

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

ステップ4 [Global Policies] サブタブをクリックします。

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

- [No Action] : ファームウェアのアップグレードはサーバで開始されません。
- [User Acknowledge] : [Pending Activities] ダイアログボックスで管理者がアップグレードを確認するまでサーバのファームウェアは同期されません。
このオプションは、デフォルトで選択されます。

ステップ6 [Save Changes] をクリックします。

エンドポイントでの直接のファームウェアのアップグレード

正しい手順に従って、正しい順序でアップグレードを適用すれば、エンドポイントの直接のファームウェアアップグレードと新しいファームウェアバージョンのアクティビ化による、Cisco UCS ドメインのトラフィックの中止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 117 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 S3260 シャーシ
<ul style="list-style-type: none"> • Cisco UCS Manager • ファブリックインターフェース <p>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フェースをアップグレードしてください。</p>	<ul style="list-style-type: none"> • I/O モジュール • 電源装置 • サーバ : <ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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 : <ul style="list-style-type: none"> • CIMC • BIOS • ボードコントローラ • ストレージコントローラ

Cisco UCS S3260 シャーシの場合、シャーシプロファイル内のシャーシファームウェアパッケージを通じて、CMC、シャーシアダプタ、シャーシボードコントローラ、SAS エクスパン

直接のファームウェア アップグレードのステージ

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ることなく、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 インターフェクトから、エンドポイントのバックアップアップデータイシヨンにコピーされ、ファームウェアイメージが破損していないことが確認されます。アップデートプロセスでは、常にバックアップスロットのファームウェアが上書きされます。

アップデートステージは、UCS 5108 シャーシの次のエンドポイントにのみ適用されます。

- アダプタ
- CIMC
- I/O モジュール

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

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

- ・アダプタ

**Caution**

更新プロセスが完了するまで、エンドポイントがあるハードウェアを取り外したり、そこで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 S3260 高密度ストレージラック サーバ シャーシ：
 - CMC
 - 共有アダプタ
 - シャーシとサーバのボード コントローラ
 - SAS エクスパンダ
 - ストレージ コントローラ
 - BIOS
 - CIMC

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

直接のファームウェアアップグレードの停止の影響



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ビ化して、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止や、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止が発生します。

- 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、次の停止が発生します。

- 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止が発生します。

- 単一のファブリック インターコネクトのスタンダー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 トラフィックが中止されます。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。

- 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。
 - 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、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 (54 ページ)、完全な状態のコンフィギュレーションバックアップファイルの作成 (56 ページ) を作成します。
 - 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 (76 ページ)、およびローカル ファイル システムからファブリック インターコネクトへのファームウェアイメージのダウンロード (79 ページ)、詳細な情報を提供します。

■ 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

3. Smart Call Home Smart Call Home の無効化（58 ページ）を無効にして、詳細情報を提供します。
2. Cisco UCS Manager ソフトウェアを有効にします。Cisco UCS Manager ソフトウェアのアクティビティ化（122 ページ）、詳細な情報を提供します。また、このビデオ (http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/activate_ucsrm.html) の [Play] をクリックして、Cisco UCS Manager ソフトウェアをアクティビティ化する方法を視聴することもできます。
3. IOM ファームウェアを更新します。IOM のファームウェアのアップデート（125 ページ）、詳細な情報を提供します。また、このビデオ (http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/update_and_activate_iom.html) の [Play] をクリックして、IOM ファームウェアを更新する方法を視聴することもできます。
4. ファブリック アップグレードを準備します。
 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。UCS Manager の障害の表示（59 ページ）は詳細情報を提供します。
 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フェイスクエートを特定します。クラスタ設定の高可用性ステータスとロールの確認（62 ページ）は、障害の確認に関する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設定します。デフォルトメンテナンスポリシーの設定（63 ページ）は詳細な情報を提供します。また、このビデオ (http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/configure_the_default_maintenance_policy.html) の [Play] をクリックして、デフォルトのメンテナンスポリシーを [User Ack] として設定する方法を視聴することもできます。
 4. VLAN と FCOE ID が重複していないことを確認します。
 5. 詳細な管理インターフェイス情報を表示します。管理インターフェイスの無効化（64 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にします。IOM でのファームウェアのアクティビティ化（127 ページ）は詳細な情報を提供します。また、このビデオ (http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/update_and_activate_iom.html) の [Play] をクリックして、IOM ファームウェアをアクティビティ化する方法を視聴することもできます。
5. 従属ファブリックインターフェイスクエートをアクティブにします。
 1. 従属ファブリックインターフェイスクエー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フェイスクエート トラフィックの待避の設定（43 ページ）は詳細情報を提供します。また、このビデオ (http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/enable_and_disable_fi_traffic_evacuation.html) の [Play] をクリックして、ファブリックインターフェイスクエート トラフィックを待避させる方法を視聴することもできます。

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。従属ファブリック インターコネクトでのファームウェアのアクティビ化 (128 ページ) は詳細情報を提供します。また、このビデオ (http://www.cisco.com/en/ustd/docs/unified_computing/ucs/ucs-manager/videos/3-l/activate_the_firmware_on_a_subordinate_fabric_interconnect.html) の [Play] をクリックして、従属ファブリック インターコネクトでファームウェアをアクティビ化する方法を視聴することもできます。
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 (67 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 トラフィックの待避の設定 (43 ページ) は詳細情報を提供します。また、このビデオ (http://www.cisco.com/en/ustd/docs/unified_computing/ucs/ucs-manager/videos/3-l/enable_and_disable_fi_traffic_evacuation.html) の [Play] をクリックして、ファブリック インターコネクトのトラフィック待避を無効にする方法を視聴することもできます。
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 (61 ページ)。
6. プライマリ ファブリック インターコネクト (FI-A) をアクティブにします。
 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 (131 ページ) は詳細情報を提供します。また、このビデオ (http://www.cisco.com/en/ustd/docs/unified_computing/ucs/ucs-manager/videos/3-l/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。
 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 インターコネクトでのファームウェアのアクティビ化 (129 ページ) は詳細情報を提供します。また、このビデオ (http://www.cisco.com/en/ustd/docs/unified_computing/ucs/ucs-manager/videos/3-l/activate_the_firmware_on_a_primary_fabric_interconnect.html) の [Play] をクリックして、プライマリ ファブリック インターコネクトでファームウェアをアクティビ化する方法を視聴することもできます。
 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。
 6. 新しい障害を確認します。

複数のエンドポイントのファームウェアのアップデート

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



Caution

更新プロセスが完了するまで、エンドポイントがあるハードウェアを取り外したり、そこで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

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

ステップ2 [Equipment] ノードをクリックします。

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

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

Cisco UCS Manager GUI によって [Update Firmware] ダイアログボックスが表示され、Cisco UCS ドメイン内のすべてのエンドポイントのファームウェアバージョンが検証されます。このステップは、シャーシとサーバの数に基づいて数分かかる場合があります。

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

a) メニューバーの [Filter] ドロップダウンリストから [ALL] を選択します。

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

b) [Select] フィールドで、次のいずれかの手順を実行します。

- すべてのエンドポイントと同じバージョンにアクティビ化するには、[Version] オプションボタンをクリックし、[Set Version] ドロップダウンリストから適切なバージョンを選択します。

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

c) [OK] をクリックします。

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

Cisco UCS Manager 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。このイメージは、アクティブ化されるまでバックアップバージョンとして保持されます。Cisco UCS Managerは、すべてのアップデートを同時に開始します。ただし、アップデートによって、完了する時間が異なることがあります。

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

ステップ 6 (Optional) 特定のエンドポイントのアップデートの進捗をモニタするには、エンドポイントを右クリックし、[Show Navigator] を選択します。

Cisco UCS Managerによって、[General] タブの [Update Status] 領域に進捗が表示されます。ナビゲータに[FSM] タブがある場合は、そこでも進捗をモニタできます。[Retry#] フィールドのエントリが、アップデートが失敗したことを示していない場合があります。再試行回数には、Cisco UCS Manager が更新ステータスを取得するときに発生する再試行も含まれます。

What to do next

ファームウェアをアクティブにします。

Cisco UCS Manager ファームウェア

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

- クラスタ設定の場合、両方のファブリックインターフェースの 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フェースの Cisco UCS Manager がアクティブ化されます。
- ファブリックインターフェース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フェース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フェース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]

Cisco UCS Manager ソフトウェアのアクティブ化

Validation] タブに表示します。アップグレードの検証エラーがある場合、アップグレードは失敗し、Cisco UCS Manager は以前のリリースにロールバックします。これらのエラーを解決し、[Force] オプションを使用してアップグレードを続行する必要があります。

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

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

Cisco UCS Manager ソフトウェアのアクティブ化

ここで説明する手順を使用することも、この**ビデオ**

(http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/activate_ucsm.html) の**[Play]** をクリックして Cisco UCS Manager ソフトウェアをアクティブ化する方法を視聴することもできます。

Procedure

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

ステップ 2 [Equipment] ノードをクリックします。

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

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

Cisco UCS Manager GUI によって [フームウェアのアクティブ化 (Activate Firmware)] ダイアログボックスが開かれ、Cisco UCS ドメイン内のすべてのエンドポイントのフームウェアバージョンが検証されます。このステップは、シャーシとサーバの数に基づいて数分かかる場合があります。

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

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

b) [OK] をクリックします。

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

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

Cisco UCS Manager ソフトウェアのサービスパックのアクティベーション

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ベーション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フェースのアップグレードまたは再起動は必要ありません。

Procedure

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

ステップ2 [Equipment] ノードをクリックします。

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

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

Cisco UCS Manager GUI によって [ファームウェアのアクティベーション (Activate Firmware)] ダイアログボックスが開かれ、Cisco UCS ドメイン内のすべてのエンドポイントのファームウェアバージョンが検証されます。このステップは、シャーシとサーバの数に基づいて数分かかる場合があります。

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

ステップ6 [Activate Firmware] ダイアログボックスの [UCS Manager] 行で、次の手順を実行します。

- [UCS Manager Service Pack] 行で、[Startup Version] カラムのドロップダウンリストからアップグレードするサービスパックのバージョンを選択します。
- [OK] をクリックします。

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

Cisco UCS Manager ソフトウェアからのサービスパックの削除

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

Procedure

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

ステップ2 [Equipment] ノードをクリックします。

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

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

Cisco UCS Manager GUI によって [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が開かれ、Cisco UCS ドメイン内のすべてのエンドポイントのファームウェアバージョンが検証されます。このステップは、シャーシとサーバの数に基づいて数分かかる場合があります。

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

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

ステップ7 [OK] をクリックします。

IOM ファームウェア

Cisco UCS I/O モジュール (IOM) は、ブレードサーバエンクロージャにユニファイドファブリック テクノロジーを組み込みます。これにより、ブレードサーバとファブリックインターフェイスクロネクト間の複数の 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フェイスクロ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フェイスクロ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扱われ、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。

IOM では、ファブリックインターフェイスクロ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。IOM 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フェースが更新およびアクティビ化されると、ファブリックインターフェースは対応する 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フェースは、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フェース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フェース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。

次の項で詳しく説明する手順を使用するか、またはこの[ビデオ](#)

(http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/update_and_activate_iom.html) の [Play] をクリックして、IOM ファームウェアを更新およびアクティビ化する方法を視聴できます。

IOM のファームウェアのアップデート



Caution

更新プロセスが完了するまで、エンドポイントがあるハードウェアを取り外したり、そこで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、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

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

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

ステップ3 アップデートする I/O モジュールをクリックします。

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

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

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

b) [OK] をクリックします。

Cisco UCS Manager 選択したファームウェアパッケージがバックアップメモリスロットにコピーされ、アクティビ化されるまで保持されます。

ステップ6 (Optional) [Update Status] 領域でアップデートのステータスをモニタします。

複数の IOM でのファームウェアのアクティブ化

アップデートプロセスは数分かかることがあります。[General] タブの[Firmware] 領域の[Backup Version] フィールドに、選択したファームウェアパッケージが表示されるまで、ファームウェアをアクティブにしないでください。

What to do next

ファームウェアをアクティブにします。

複数の IOM でのファームウェアのアクティブ化

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



Caution

[Activate Firmware] ダイアログボックスの[Filter] ドロップダウンリストで [ALL] を選択しないでください。選択すると、すべてのエンドポイントが同時にアクティブになります。多くのファームウェアリリースやパッチには依存関係があるため、ファームウェアの更新を正常に実行するためにエンドポイントを特定の順序でアクティブにする必要があります。この順序はリリースやパッチの内容によって異なります。すべてのエンドポイントをアクティブにすると、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フェース、および Cisco UCS Manager 間の通信が中断される可能性があります。特定のリリースやパッチの依存関係については、当該のリリースやパッチに付属のリリースノートを参照してください。

Procedure

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

ステップ 2 [Equipment] ノードをクリックします。

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

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

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

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

a) [Filter] ドロップダウンリストから、[IO Modules] を選択します。

b) [Set Version] ドロップダウンリストから、現在の 2.0 リリースのバージョンを選択します。

c) [Ignore Compatibility Check] チェックボックスをオンにします。

- d) [Set Startup Version Only] チェックボックスをオンにします。

Important 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フェース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、トライフィックが中断します。また、ファブリックインターフェースと 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フェース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ビ化して、I/O モジュールを再度リブートします。

- e) [Apply] をクリックします。

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

ステップ 6 [OK] をクリックします。

IOMでのファームウェアのアクティビ化

Procedure

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

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

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

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

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

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

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

- b) スタートアップバージョンを設定し、エンドポイントで実行しているバージョンを変更しない場合、[Set Startup Version Only] チェックボックスをオンにします。

[Set Startup Version Only] を設定した場合は、アクティビ化されたファームウェアが pending-next-reboot 状態に移行して、エンドポイントがすぐにリブートしません。有効化されたファームウェアは、エンドポイントがリブートするまで、実行中のファームウェアのバージョンになりません。

■ ファブリック インターコネクトのファームウェア

- c) [OK] をクリックします。
-

ファブリック インターコネクトのファームウェア

従属ファブリック インターコネクトでのファームウェアのアクティビズム

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/en/ust/docs/unified_computing/ucs/ucs_manager/videos/3-1/activate_the_firmware_on_a_subordinate_fabric_interconnect.html) の[Play]をクリックして従属ファブリック インターコネクトのファームウェアをアクティビズム化する方法を視聴することもできます。

始める前に

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

手順

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

ステップ2 [Equipment] ノードをクリックします。

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

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

Cisco UCS Manager GUI によって [ファームウェアのアクティビズム (Activate Firmware)] ダイアログボックスが開かれ、Cisco UCS ドメイン内のすべてのエンドポイントのファームウェアバージョンが検証されます。このステップは、シャーシとサーバの数に基づいて数分かかる場合があります。

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

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

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

ステップ7 [Apply] をクリックします。

Cisco UCS Manager はファームウェアをアップデートしてアクティビズムにし、ファブリック インターコネクトとそのファブリック インターコネクトへのデータパスにあるすべての I/O モジュールをリブートするため、そのファブリック インターコネクトとの間のデータ トラフィックが中断します。ただし、トラフィックおよびポートフェールオーバーを許可するように Cisco

UCS ドメインが設定されている場合、データ トラフィックはプライマリ ファブリック インターコネクトにフェールオーバーし、中断されません。

ステップ8 下位ファブリック インターコネクトの高可用性ステータスを確認します。

ファブリック インターコネクトの [High Availability Details] 領域に次の値が表示されない場合は、シスコのテクニカルサポートに問い合わせてください。プライマリ ファブリック インターコネクトのアップデートに進まないでください。

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

次のタスク

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

プライマリ ファブリック インターコネクトでのファームウェアのアクティビゼーション

この手順は、[従属ファブリック インターコネクトでのファームウェアのアクティビゼーション \(128 ページ\)](#) から直接続いており、[Firmware Management] タブが表示されていることを前提としています。ここで説明する手順を使用することも、この[ビデオ](#) (http://www.cisco.com/c/en/us/d/docs/unified_computing/ucsmanager/videos/3-1/activate_the_firmware_on_a_primary_fabric_interconnect.html) の [Play] をクリックしてプライマリ ファブリック インターコネクトのファームウェアをアクティビゼーションする方法を視聴することもできます。

始める前に

下位のファブリック インターコネクトをアクティビゼーションします。

手順

ステップ1 [Installed Firmware] タブの [Activate Firmware] をクリックします。

Cisco UCS Manager GUI によって [ファームウェアのアクティビゼーション (Activate Firmware)] ダイアログボックスが開かれ、Cisco UCS ドメイン内のすべてのエンドポイントのファームウェアバージョンが検証されます。このステップは、シャーシとサーバの数に基づいて数分かかる場合があります。

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

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

■ スタンドアロン ファブリック インターコネクトでのファームウェアのアクティブ化

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

ステップ4 [Apply] をクリックします。

Cisco UCS Manager はファームウェアをアップデートしてアクティブにし、ファブリック インターコネクトとそのファブリック インターコネクトへのデータパスにあるすべての I/O モジュールをリブートするため、そのファブリック インターコネクトとの間のデータ トラフィックが中断します。ただし、トラフィックおよびポートフェールオーバーを許可するように Cisco UCS ドメインが設定されている場合、データ トラフィックはもう1つのファブリック インターコネクトにフェールオーバーし、それがプライマリになります。このファブリック インターコネクトが再度稼働状態になると、このファブリック インターコネクトは従属ファブリック インターコネクトになります。

ステップ5 ファブリック インターコネクトの高可用性ステータスを確認します。

ファブリック インターコネクトの [High Availability Details] 領域に次の値が表示されない場合は、シスコのテクニカルサポートに問い合わせてください。

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

スタンドアロン ファブリック インターコネクトでのファームウェアのアクティブ化

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



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

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

ステップ2 [Equipment] ノードをクリックします。

ステップ3 [Fabric Interconnects] ノードを展開して、スタンダードアロン ファブリックインターネットをクリックします。

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

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

名前	説明
[Kernel Version] ドロップダウンリスト	カーネルとして使用するバージョンを選択します。
[Force] チェックボックス	オンにすると、Cisco UCSでは、選択したバージョンを前回インストールしようとしたときに失敗または中断した場合でも、インストールを試みます。
[System Version] ドロップダウンリスト	システムとして使用するバージョンを選択します。
[Force] チェックボックス	オンにすると、Cisco UCSでは、選択したバージョンを前回インストールしようとしたときに失敗または中断した場合でも、インストールを試みます。
[Service Pack Version] ドロップダウンリスト	適用するサービスパックのバージョンを選択します。 Note サービスパックは基本のメンテナンスリリースにのみ適用できます。たとえば、サービスパック 3.1(3)SP2 は 3.1(3) リリースにのみ適用できます。3.1(4) リリースに適用することはできません。 [Service Pack] を [<not set>] に設定すると、サービスパックがファブリックインターネットから削除されます。

ステップ6 [OK] をクリックします。

Cisco UCS Manager activates the firmware and reboots the fabric interconnect and any I/O module in the data path to that fabric interconnect. スタンダードアロン ファブリックインターネットでは、これにより、Cisco UCS ドメインのすべてのデータ トライフィックが中断します。

ファブリックインターネッ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ネットから別のファブリックインターネッ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。

■ 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



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}}	<p>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。</p> <p>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。</p> <p>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。</p>

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

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

手順

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

ステップ2 [Equipment] ノードをクリックします。

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

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

Cisco UCS Manager GUI によって [ファームウェアのアクティビ化 (Activate Firmware)] ダイアログボックスが開かれ、Cisco UCS ドメイン内のすべてのエンドポイントのファームウェアバージョンが検証されます。このステップは、シャーシとサーバの数に基づいて数分かかる場合があります。

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

ステップ6 ファブリック インターコネクトの [Activate Firmware] ダイアログボックスの [Service Pack] の行で、[Startup Version] カラムのドロップダウンリストからアップグレードするサービス パックのバージョンを選択します。

ステップ7 [OK] をクリックします。

Cisco UCS Manager 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 トライフックが中断されます。

ファブリック インターコネクトからのサービス パックの削除

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

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

手順

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

ステップ2 [Equipment] ノードをクリックします。

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

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

Cisco UCS Manager GUI によって [ファームウェアのアクティビ化 (Activate Firmware)] ダイアログボックスが開かれ、Cisco UCS ドメイン内のすべてのエンドポイントのファームウェアバージョンが検証されます。このステップは、シャーシとサーバの数に基づいて数分かかる場合があります。

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

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

ステップ7 [OK] をクリックします。

アダプタ ファームウェア

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

すべての Cisco UCS ネットワーク アダプタ :

- 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акタで使用できます。

アダプタのファームウェアのアップデート


Caution

更新プロセスが完了するまで、エンドポイントがあるハードウェアを取り外したり、そこで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

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

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

ステップ3 アップデートするアダプタを搭載しているサーバのノードを展開します。

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

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

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

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

b) [OK] をクリックします。

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

Cisco UCS Manager 選択したファームウェアパッケージがバックアップメモリースロットにコピーされ、アクティブ化されるまで保持されます。

ステップ7 (Optional) [Update Status] 領域でアップデートのステータスをモニタします。

アップデートプロセスは数分かかることがあります。[General] タブの [Firmware] 領域の [Backup Version] フィールドに、選択したファームウェアパッケージが表示されるまで、ファームウェアをアクティブにしないでください。

What to do next

ファームウェアをアクティブにします。

Procedure

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

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

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

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

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

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

- [Version To Be Activated] ドロップダウンリストから、適切なバージョンを選択します。

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

- スタートアップバージョンを設定し、エンドポイントで実行しているバージョンを変更しない場合、[Set Startup Version Only] チェックボックスをオンにします。

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

サーバがサービスプロファイルに関連付けられていない場合、アクティブ化されたファームウェアは pending-next-boot 状態のままでです。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したり、ファームウェアをアクティブ化したりしません。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。

- [OK] をクリックします。

BIOS ファームウェア

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

サーバの BIOS ファームウェアのアップデート



注意 更新プロセスが完了するまで、エンドポイントがあるハードウェアを取り外したり、そこで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

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

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

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

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

ステップ5 [Motherboard] タブをクリックします。

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

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

- [Version] ドロップダウンリストから、サーバ BIOS をアップデートするファームウェアバージョンを選択します。
- (任意) 互換性のない可能性や、現在実行中のタスクに関係なく、ファームウェアをアップデートする場合は、[Force] チェックボックスをオンにします。
- [OK] をクリックします。

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

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

次のタスク

ファームウェアをアクティブにします。

サーバの BIOS ファームウェアのアクティブ化

手順

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

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

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

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

ステップ 5 [Motherboard] タブをクリックします。

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

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

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

b) スタートアップバージョンを設定し、サーバで実行しているバージョンを変更しない場合は、[Set Startup Version Only] チェックボックスをオンにします。

[Set Startup Version Only] を設定した場合は、アクティビ化されたファームウェアが pending-next-boot 状態に移行し、サーバはすぐにはリブートされません。アクティビ化されたファームウェアは、サーバがリブートされるまでは、実行されているバージョンのファームウェアになりません。

c) [OK] をクリックします。

CIMC ファームウェア

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

サーバの CIMC ファームウェアのアップデート



Caution

更新プロセスが完了するまで、エンドポイントがあるハードウェアを取り外したり、そこで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、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

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

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

ステップ3 CIMC をアップデートするサーバのノードを展開します。

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

ステップ5 [CIMC] タブをクリックします。

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

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

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

- [OK] をクリックします。

Cisco UCS Manager 選択したファームウェア パッケージがバックアップ メモリ スロットにコピーされ、アクティブ化されるまで保持されます。

ステップ8 (Optional) [Update Status] 領域でアップデートのステータスをモニタします。

アップデートプロセスは数分かかることがあります。[General] タブの [Firmware] 領域の [Backup Version] フィールドに、選択したファームウェア パッケージが表示されるまで、ファームウェアをアクティブにしないでください。

What to do next

ファームウェアをアクティブにします。

サーバの CIMC ファームウェアのアクティブ化

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



Caution

更新プロセスが完了するまで、エンドポイントがあるハードウェアを取り外したり、そこで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、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

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

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

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

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

ステップ5 [CIMC] タブをクリックします。

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

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

- [Version To Be Activated] ドロップダウンリストから、適切なバージョンを選択します。

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

- スタートアップバージョンを設定し、エンドポイントで実行しているバージョンを変更しない場合、[Set Startup Version Only] チェックボックスをオンにします。

[Set Startup Version Only] を設定した場合は、アクティブ化されたファームウェアが pending-next-reboot 状態に移行して、エンドポイントがすぐにリブートしません。有効化されたファームウェアは、エンドポイントがリブートするまで、実行中のファームウェアのバージョンになりません。

- [OK] をクリックします。

PSU ファームウェア

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

PSU でのファームウェアのアップデート



注意

更新プロセスが完了するまで、エンドポイントがあるハードウェアを取り外したり、そこで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、他のメンテナンス作業により使用できない場合、ファームウェアの更新は失敗します。この失敗により、バックアップパーティションが破損する場合があります。バックアップパーティションが破損しているエンドポイントではファームウェアを更新できません。

手順

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

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

ステップ3 管理する PSU に対応するシャーシを選択します。

ステップ4 [Work] ペインの [PSUs] をクリックします。

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

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

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

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

Cisco UCS Manager 選択したファームウェア パッケージがバックアップ メモリ スロットにコピーされ、明示的にアクティブ化されるまでそれが保持されます。

ステップ8 (任意) [Update Status] 領域でアップデートのステータスをモニタします。

アップデートプロセスは数分かかることがあります。[General] タブの [Firmware] 領域の [Backup Version] フィールドに、選択したファームウェア パッケージが表示されるまで、ファームウェアをアクティブにしないでください。

次のタスク

ファームウェアをアクティブにします。

PSUでのファームウェアのアクティブ化

手順

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

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

ステップ3 管理する PSU に対応するシャーシを選択します。

ステップ4 [Work] ペインの [PSUs] をクリックします。

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

ステップ6 [General] タブの [Activate Firmware] をクリックします。

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

- [Version To Be Activated] ドロップダウンリストから、適切なバージョンを選択します。

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

- スタートアップバージョンを設定し、エンドポイントで実行しているバージョンを変更しない場合、[Set Startup Version Only] チェックボックスをオンにします。

[Set Startup Version Only] を設定した場合は、アクティブ化されたファームウェアが pending-next-reboot 状態に移行して、エンドポイントがすぐにリブートしません。有効化されたファームウェアは、エンドポイントがリブートするまで、実行中のファームウェアのバージョンになりません。

- c) [OK] をクリックします。

ボードコントローラ ファームウェア

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

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

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

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

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

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



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

機能カタログの更新は、次の手順で適用できます。

1. 2.2(4c) インフラ/カタログまたは 2.2(5b) インフラ/カタログ ソフトウェア バンドルをダウンロードします。[シスコからのソフトウェアバンドルの入手 \(74ページ\)](#) は、ソフトウェア バンドルのダウンロードに関する詳細情報を提供します。

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ビ化 (149ページ) は Cisco UCS Manager を使用した機能カタログのアクティビ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 以降のラック サーバのボードコントローラ ファームウェアのアクティビ化に関する注意事項

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

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

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

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

このアラームが表示されないようにするには、次のいずれかを行います。

- Cisco UCS Manager 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。

Cisco UCS B シリーズ M3 以降のブレード サーバでのボードコントローラ ファームウェアのアクティブ化

(注)

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

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

Cisco UCS B シリーズ M3 以降のブレード サーバでのボードコントローラ ファームウェアのアクティブ化

(注)

このアクティブ化手順を実行すると、サーバはリブートされます。サーバに関連付けられているサービスプロファイルにメンテナンス ポリシーが含まれているかどうかに応じて、リブートはただちに行われることがあります。ボードコントローラ ファームウェアは、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一緒に、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。これによって、アップグレード プロセス中にサーバをリブートする回数を低減できます。

手順

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

ステップ 2 [Equipment] ノードをクリックします。

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

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

Cisco UCS Manager GUI によって [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が開かれ、Cisco UCS ドメイン内のすべてのエンドポイントのファームウェア バージョンが検証されます。このステップは、シャーシとサーバの数に基づいて数分かかる場合があります。

ステップ 5 [Activate Firmware] ダイアログボックスのメニュー バーにある [Filter] ドロップダウン リストから、[Board Controller] を選択します。

Cisco UCS Manager GUI によって、[Activate Firmware] ダイアログボックスにボードコントローラを備えたすべてのサーバが表示されます。

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

ステップ 7 [OK] をクリックします。

ステップ8 (任意) 異なるアーキテクチャのCPUにアップグレードする場合には、[Force Board Controller Activation] オプションを使用してファームウェアバージョンを更新することもできます。

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



(注)

このアクティビ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。これによって、アップグレードプロセス中にサーバをリブートする回数を低減できます。

手順

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

ステップ2 [Equipment] ノードをクリックします。

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

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

Cisco UCS Manager GUI によって [ファームウェアのアクティビ化 (Activate Firmware)] ダイアログボックスが開かれ、Cisco UCS ドメイン内のすべてのエンドポイントのファームウェアバージョンが検証されます。このステップは、シャーシとサーバの数に基づいて数分かかる場合があります。

ステップ5 [Activate Firmware] ダイアログボックスのメニュー バーにある [Filter] ドロップダウンリストから、[Board Controller] を選択します。

Cisco UCS Manager GUI によって、[Activate Firmware] ダイアログボックスにボードコントローラを備えたすべてのサーバが表示されます。

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

ステップ7 [OK] をクリックします。

ステップ8 (任意) 異なるアーキテクチャのCPUにアップグレードする場合には、[Force Board Controller Activation] オプションを使用してファームウェアバージョンを更新することもできます。

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



第 4 章

Cisco UCS Manager での機能力タログの管理

- [機能カタログ \(147 ページ\)](#)
- [機能カタログ更新のアクティブ化 \(149 ページ\)](#)
- [機能カタログが最新であることの確認 \(149 ページ\)](#)
- [機能カタログプロバイダーの表示 \(150 ページ\)](#)
- [シスコからの機能カタログのアップデートの入手方法 \(150 ページ\)](#)
- [リモートロケーションからの機能カタログの更新 \(151 ページ\)](#)
- [ローカルファイルシステムからの機能カタログの更新 \(151 ページ\)](#)

機能力タログ

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、Cisco UCS は、新しく資格を得たサーバの 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するために使用されます。

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。

機能力タログの内容

機能カタログの内容は次のとおりです。

■ 機能カタログの更新

実装固有の調整可能なパラメータ

- 電力および熱に関する制約
- スロット範囲および番号
- アダプタ機能

ハードウェア固有のルール

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

ユーザ表示文字列

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

機能カタログの更新

Cisco UCS インフラストラクチャソフトウェアバンドルには、機能カタログの更新が含まれています。Cisco Technical Assistance Center からの指示がない限り、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、アクティビ化の後に機能カタログ更新をアクティビ化にするだけです。

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入手できるようにする場合があります。



(注)

機能カタログのバージョンは、使用している Cisco UCS のバージョンによって決まります。同じメジャーリリースバージョン内で機能カタログをアップグレードできます。Cisco UCS 4.0(x) リリースは、4.0(x) 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。たとえば、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、<http://www.cisco.com/go/unifiedcomputing/b-series-doc> で入手可能な「Cisco UCS B-Series Servers Documentation Roadmap」にある『Release Notes for Cisco UCS Software』を参照してください。

機能カタログ更新のアクティブ化

手順

-
- ステップ1 [Navigation] ペインで [Admin] をクリックします。
 - ステップ2 [All] > [Capability Catalog] の順に展開します。
 - ステップ3 [Capability Catalog] ノードをクリックします。
 - ステップ4 [Work] ペインで [Catalog Update Tasks] タブをクリックします。
 - ステップ5 [Activate Catalog] をクリックします。
 - ステップ6 [Activate Catalog] ダイアログボックスで、[Version to be Activated] ドロップダウンリストからアクティブ化する機能カタログの更新を選択します。
 - ステップ7 [OK] をクリックします。
-

機能カタログが最新であることの確認

手順

-
- ステップ1 [Navigation] ペインで [Admin] をクリックします。
 - ステップ2 [All] > [Capability Catalog] の順に展開します。
 - ステップ3 [Capability Catalog] ノードをクリックします。
 - ステップ4 [Work] ペインで [Catalog Update Tasks] タブをクリックします。
機能カタログの最新バージョンは、このタブの右上にあります。
 - ステップ5 <http://www.cisco.com/> で、機能カタログの利用可能な最新リリースを確認します。
機能カタログのアップデートの場所については、シスコからの機能カタログのアップデートの入手方法（150 ページ）を参照してください。
 - ステップ6 より新しいバージョンの機能カタログを <http://www.cisco.com/> で入手できる場合は、そのバージョンを使用して機能カタログをアップデートします。
-

■ 機能力カタログ プロバイダーの表示

機能力カタログ プロバイダーの表示

手順

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

ステップ2 [All] > [Capability Catalog] の順に展開します。

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

ステップ4 [Work] ペインで、表示するプロバイダーのタブをクリックします。

ステップ5 プロバイダーの詳細情報を表示するには、次の手順を実行します。

- a) テーブルで、表示するプロバイダーのベンダー、モデル、リビジョンの行をクリックします。
 - b) 見出しの右側にある [Expand] アイコンをクリックし、次の領域のプロパティを表示します。
 - [Equipment Manufacturing] 領域
 - [Form Factor] 領域
-

シスコからの機能力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 機能力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

機能力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力タログの更新

機能力タログの一部分のみの更新はできません。機能力タログを更新すると、カタログイメージ内のコンポーネントがすべて更新されます。

B-Series サーババンドルには、そのサーバの機能力タログの更新が含まれています。個別の機能力タログの更新をダウンロードする必要はありません。機能力タログの更新をアクティブ化するだけです。

手順

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

ステップ2 [All] > [Capability Catalog] の順に展開します。

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

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

ステップ5 [Update Catalog] をクリックします。

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

ステップ7 [OK] をクリックします。

Cisco UCS Manager イメージをダウンロードし、機能力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。

ローカル ファイル システムからの機能力タログの更新

機能力タログの一部分のみの更新はできません。機能力タログを更新すると、カタログイメージ内のコンポーネントがすべて更新されます。

B-Series サーババンドルには、そのサーバの機能力タログの更新が含まれています。個別の機能力タログの更新をダウンロードする必要はありません。機能力タログの更新をアクティブ化するだけです。

手順

-
- ステップ1 [Navigation] ペインで [Admin] をクリックします。
 - ステップ2 [All] > [Capability Catalog] の順に展開します。
 - ステップ3 [Capability Catalog] ノードをクリックします。
 - ステップ4 [Work] ペインで [Catalog Update Tasks] タブをクリックします。
 - ステップ5 [Update Catalog] をクリックします。
 - ステップ6 [Download Firmware] ダイアログボックスで、[Location of the Image File] フィールドの [Local File System] オプションボタンをクリックします。
 - ステップ7 [Filename] フィールドに、イメージファイルのフルパスと名前を入力します。
 ファームウェアイメージファイルが配置されているフォルダへの正確なパスがわからない場合は、[Browse] をクリックしてファイルにナビゲートします。
 - ステップ8 [OK] をクリックします。
-

Cisco UCS Manager イメージをダウンロードし、機能力タログを更新します。ハードウェアコンポーネントをリブートする必要はありません。



第 5 章

ファームウェアのトラブルシューティング

- ・アップグレード中のファブリック インターコネクトの回復（153 ページ）
- ・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（161 ページ）

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。

■ 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

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ぬ場合があります。

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 :

■ 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

```
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 nova-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。

nova-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
nova-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
nova-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ビ化します。

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

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フェース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ぬ場合があります。

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 nova-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。

novasim-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 nova-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。

■ 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

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 activity
(5) Ensure NTP is configured
(6) Check if any hardware (fabric interconnects, io-modules, servers or adapters) is
unsupported in the target release
Do you want to proceed? (yes/no): yes
Triggering Install-Infra with:
Infrastructure Pack Version: 3.1(3a)A

```

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

例 :

```

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

```

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

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

例 :

```

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

```

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

例 :

```

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

```

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

ファームウェアアップグレード中のIOモジュールの回復

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

ピア I/O モジュールからの I/O モジュールのリセット

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

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

手順

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

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

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

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

ステップ 5 [Actions] 領域で、[Reset Peer IO Module] をクリックします。