Cisco UCS M シリーズ GUI ファームウェア管理ガイド リリース 2.5

初版：2015 年 04 月 07 日

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

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

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。 このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。 このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。 添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。 シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。 マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。 説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2015 Cisco Systems, Inc. All rights reserved.

目 次

はじめに vii

対象読者 vii

表記法 vii

Cisco UCS の関連ドキュメント ix

マニュアルに関するフィードバック ix

概要 1

ファームウェアの概要 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 2

ファームウェア バージョン 2

Cisco UCS Manager によるファームウェアの管理 5

Cisco UCS Manager でのファームウェアのダウンロードと管理 7

ファームウェア イメージの管理 7

ファームウェア イメージ ヘッダー 9

ファームウェア イメージ カタログ 9

シスコからの M シリーズ ソフトウェア バンドルの入手 10

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 11

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 12

イメージ ダウンロードのキャンセル 13

ファームウェア パッケージの内容の判断 13

ファブリック インターコネクトの空き領域のチェック 14

自動インストールによるファームウェアのアップグレード 15

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 15

インフラストラクチャ ファームウェアのインストール 16

サーバ ファームウェアのインストール 16

自動インストールのための必要な手順 16
自動インストールによるインフラストラクチャのファームウェアのアップグレード 17
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 19
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 20
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 20
ファームウェア自動同期サーバ ポリシーの使用 25
ファームウェアの自動同期 25
ファームウェア自動同期サーバ ポリシーの設定 26
エンドポイントのファームウェアの直接アップグレード 29
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 30
直接のファームウェア アップグレードのステージ 31
直接のファームウェア アップグレードの停止の影響 32
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 34
シャーシの CMC ファームウェアのアップデート 36
シャーシの CMC ファームウェアのアクティブ化 37
シャーシの共有アダプタ ファームウェアの更新 37
シャーシの共有アダプタ ファームウェアのアクティブ化 38
シャーシのストレージ コントローラ ファームウェアのアクティブ化 39
シャーシのボード コントローラ ファームウェアのアクティブ化 39
サーバの BIOS ファームウェアのアップデート 40
サーバの BIOS ファームウェアのアクティブ化 41
サーバの CIMC ファームウェアのアップデート 41
サーバの CIMC ファームウェアのアクティブ化 42
Cisco UCS Manager ソフトウェアのアクティブ化 43
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 44
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 45
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 46
コンポーネントのファームウェア バージョンの確認 47

サービス プロファイルのファームウェア パッケージによるファームウェアのアップグレード 49
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 49
ホスト ファームウェア パッケージ 50
管理ファームウェア パッケージ 51
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 51
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 52
ホスト ファームウェア パッケージの作成 56
ホスト ファームウェア パッケージのアップデート 57
管理ファームウェア パッケージのアップデート 58
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 59
Cisco UCS Manager での機能カタログの管理 61
機能カタログ 61
機能カタログの内容 61
機能カタログの更新 62
機能カタログ更新のアクティブ化 63
機能カタログが最新であることの確認 63
機能カタログ プロバイダーの表示 64
個別の機能カタログ更新のダウンロード 64
シスコからの機能カタログのアップデートの入手方法 64
リモート ロケーションからの機能カタログの更新 65
ローカル ファイル システムからの機能カタログの更新 65
管理拡張機能の更新 67
Management Extension 67
管理拡張機能のアクティブ化 67
データ パスの準備が整っていることの確認 69
ダイナミック vNIC が稼働中であることの確認 69
イーサネット データ パスの確認 70
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 70

ファイバ チャネル スイッチ モードのデータ パスの確認 71

はじめに

この前書きは、次の項で構成されています。

- 対象読者，vii ページ
- 表記法，vii ページ
- Cisco UCS の関連ドキュメント，ix ページ
- マニュアルに関するフィードバック，ix ページ

対象読者

このガイドは、次の 1 つ以上に責任を持ち、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	用途
GUI 要素	タブの見出し、領域名、フィールドのラベルのようなGUI要素は、[GUI elements] のように示しています。 ウィンドウ、ダイアログボックス、ウィザードのタイトルのようなメイン タイトルは、**[Main titles]** のように示しています。
マニュアルのタイトル	マニュアルのタイトルは、イタリック体（*italic*）で示しています。

テキストのタイプ	用途
TUI 要素	テキストベースのユーザ インターフェイスでは、システムによって表示されるテキストは、courier フォントで示しています。
システム出力	システムが表示するターミナル セッションおよび情報は、courier フォントで示しています。
CLI コマンド	CLI コマンドのキーワードは、ボールド体（**bold**）で示しています。 CLI コマンド内の変数は、イタリック体（*italic*）で示しています。
[ ]	角カッコの中の要素は、省略可能です。
{x | y | z}	必ずいずれか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、このドキュメント以外の参照資料などを紹介しています。

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

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

ワンポイント アドバイス　時間を節約する方法です。 ここに紹介している方法で作業を行うと、時間を短縮できます。

警告　安全上の重要事項

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

これらの注意事項を保管しておいてください。

Cisco UCS の関連ドキュメント

ドキュメント ロードマップ

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

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

M シリーズのすべてのマニュアルのリストについては https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/UCS_M_Series_Servers_Documentation_Roadmap.html、で入手可能な『*Cisco UCS M-Series Servers Documentation Roadmap*』を参照してください。

その他のマニュアル リソース

B シリーズと C シリーズのすべてのドキュメントが格納された ISO ファイルは、次の URL から入手できます。http://www.cisco.com/cisco/software/type.html?mdfid=283853163&flowid=25821 このページで、[Unified Computing System (UCS) Documentation Roadmap Bundle] をクリックします。

ISO ファイルは、ドキュメントのメジャー リリースの後に更新されます。

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、HTML ドキュメント内のフィードバック フォームよりご連絡ください mailto:ucs-docfeedback@cisco.com。 ご協力をよろしくお願いいたします。

第 1 章

概要

この章は、次の内容で構成されています。

- ファームウェアの概要，1 ページ
- 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，2 ページ
- ファームウェア バージョン，2 ページ

ファームウェアの概要

Cisco UCS では、シスコから取得し、シスコによって認定されたファームウェアを使用して、Cisco UCS ドメインのエンドポイントをサポートします。 各エンドポイントは、機能するためにファームウェアが必要な Cisco UCS ドメインのコンポーネントです。

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

アップグレード

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

アップデート

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

アクティブ化

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

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

重要 Cisco UCS Manager リリース 2.5 は Cisco UCS M シリーズ サーバのみをサポートします。 Cisco UCS B シリーズ サーバと Cisco C シリーズ サーバはサポートされません。

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

次のコンポーネントはファームウェア アップグレードをサポートします。

- シャーシ:
  - シャーシ管理コントローラ（CMC）
  - 共有アダプタ
  - ストレージ コントローラ
  - ボード コントローラ
- サーバ：
  - Cisco Integrated Management Controller（CIMC）
  - BIOS

ファームウェア バージョン

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

CIMC、BIOS、CMC と共有アダプタのファームウェア バージョン

CIMC、BIOS、共有アダプタ、CMC のそれぞれには、ファームウェア用フラッシュが 2 つあります。 各スロットに 1 つのバージョンのファームウェアを装着します。 1 つのスロットはアクティブで、他方のスロットはバックアップスロットです。 コンポーネントは、アクティブとして指定されているスロットからブートします。

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

実行されているバージョン

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

スタートアップ バージョン

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

バックアップ バージョン

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

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

ボード コントローラとストレージ コントローラにはバックアップ バージョンがありません。 したがって、実行できるのはアクティブ化だけです。

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

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

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

第 I 部

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，7 ページ
- 自動インストールによるファームウェアのアップグレード，15 ページ
- ファームウェア自動同期サーバ ポリシーの使用，25 ページ
- エンドポイントのファームウェアの直接アップグレード，29 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のアップグレード，49 ページ
- Cisco UCS Manager での機能カタログの管理，61 ページ
- 管理拡張機能の更新，67 ページ
- データ パスの準備が整っていることの確認，69 ページ

第 2 章

Cisco UCS Manager でのファームウェアのダウンロードと管理

この章は、次の内容で構成されています。

- ファームウェア イメージの管理，7 ページ
- ファームウェア イメージ ヘッダー，9 ページ
- ファームウェア イメージ カタログ，9 ページ
- シスコからの M シリーズ ソフトウェア バンドルの入手，10 ページ
- 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，11 ページ
- 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，12 ページ
- イメージ ダウンロードのキャンセル，13 ページ
- ファームウェア パッケージの内容の判断，13 ページ
- ファブリック インターコネクトの空き領域のチェック，14 ページ

ファームウェア イメージの管理

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

Cisco UCS インフラストラクチャ ソフトウェア バンドル

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

- Cisco UCS Manager ソフトウェア
- ファブリック インターコネクトのカーネル ファームウェアとシステム ファームウェア

Cisco UCS M シリーズ モジュラ サーバ ソフトウェア バンドル

このバンドルには、Cisco UCS ドメインのモジュラ サーバのファームウェアをアップデートするために必要な次のファームウェア イメージが含まれます。

- シャーシ:
  - CMC ファームウェア
  - 共有アダプタ ファームウェア
  - ボード コントローラ ファームウェア
  - ストレージ コントローラのファームウェア
- サーバ :
  - CIMC ファームウェア
  - BIOS ファームウェア

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。

M シリーズシャーシコンポーネントのファームウェアのアップグレードをトリガーするには、次の順に実行します。

1. CMC ファームウェアの更新
2. 共有アダプタ ファームウェアの更新
3. CMC ファームウェアのアクティブ化
4. 共有アダプタ ファームウェアのアクティブ化
5. ストレージ コントローラのアクティブ化
6. ボード コントローラのアクティブ化

エンドポイントのファームウェアのアップグレードをトリガーするには、次の順に実行します。

1. CIMC の更新
2. CIMC のアクティブ化
3. BIOS の更新

4 BIOS のアクティブ化

ファームウェア イメージ ヘッダー

すべてのファームウェア イメージに、次の情報を含むヘッダーがあります。

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

ファームウェア イメージ カタログ

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

パッケージ

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

イメージ

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

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

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

シスコからの M シリーズ ソフトウェア バンドルの入手

はじめる前に

手順

ステップ 1 Web ブラウザで、 Cisco.com を参照します。

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

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

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

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

バンドル	ナビゲーション パス
Cisco UCS M シリーズ モジュラ サーバ ソフトウェア バンドル	[Cisco UCS M-Series Modular Server Software] > [Unified Computing System (UCS) Server Software Bundle] をクリックします。

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

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

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

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

b) 次のいずれかのボタンをクリックして、表示される指示に従います。

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

c) メッセージに従ってソフトウェア バンドルのダウンロードを完了します。

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

次の作業

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

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

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

はじめる前に

必要なファームウェア バンドルをシスコから入手します。

手順

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

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

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

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

ステップ 5 [Download Firmware] をクリックします。

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

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

ステップ 8 （任意） [Download Tasks] タブで、ダウンロードのステータスをモニタします。
（注） Cisco UCS Manager によって、ブートフラッシュの領域が不足していることが報告された場合は、[Packages] タブで古いバンドルを削除して、領域を解放します。 ブートフラッシュの空き領域を表示するには、[Equipment] タブのファブリック 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 9 必要なすべてのファームウェアバンドルがファブリックインターコネクトにダウンロードされるまで、このタスクを繰り返します。

次の作業

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

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

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

はじめる前に

必要なファームウェア バンドルをシスコから入手します。

手順

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

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

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

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

ステップ 5 [Download Firmware] をクリックします。

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

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

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

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

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

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

次の作業

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

イメージ ダウンロードのキャンセル

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

手順

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

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] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[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 [Packages] サブタブで、パッケージの内容を表示するには、パッケージの横の [+] アイコンをクリックします。

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

a) イメージ名とその内容を含む行を強調表示します。

b) 右クリックし、[Copy] を選択します。

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

ファブリック インターコネクトの空き領域のチェック

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

手順

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

ステップ 2 [Equipment] タブで、[Equipment] > [Fabric Interconnects] を展開します。

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] ペインの [General] タブをクリックします。

ステップ 5 [Local Storage Information] 領域を展開します。
ファームウェア イメージ バンドルをダウンロードする場合、ファブリック インターコネクトに、ファームウェア イメージ バンドルのサイズの少なくとも 2 倍の空き領域が必要です。 ブートフラッシュに十分な領域がない場合は、ファブリック インターコネクトから、古いファームウェア、コア ファイル、その他の不要なオブジェクトを削除してください。

第 3 章

自動インストールによるファームウェアのアップグレード

この章は、次の内容で構成されています。

- 自動インストール によるファームウェア アップグレード，15 ページ
- 自動インストールのための必要な手順，16 ページ
- 自動インストールによるインフラストラクチャのファームウェアのアップグレード, 17 ページ
- 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，19 ページ
- 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，20 ページ
- 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，20 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

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

- インフラストラクチャ ファームウェアのインストール：Cisco UCS インフラストラクチャ ソフトウェア バンドルを使用して、ファブリック インターコネクト、Cisco UCS Manager などのインフラストラクチャ コンポーネントをアップグレードします。
- サーバ ファームウェアのインストール：Cisco UCS M シリーズ 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サーバをアップグレードします。

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

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

インフラストラクチャ ファームウェアのインストール

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

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

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

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

サーバ ファームウェアのインストール

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

- すべてのサーバ用の Cisco UCS M シリーズ サーバ ソフトウェア バンドル。

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

自動インストールのための必要な手順

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

1. インフラストラクチャ ファームウェアのインストール

2 サーバ ファームウェアのインストール

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

自動インストールによるインフラストラクチャのファームウェアのアップグレード

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

はじめる前に

ファームウェアのアップグレードとダウングレードの前提条件に記載のすべての前提条件を満た

はじめる前に

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

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

手順

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

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

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

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

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

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

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

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

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

名前	説明
[Name] フィールド	Cisco UCS によって作成および管理されるインフラストラクチャ パックの名前。 このフィールドのデフォルト名を変更したり、カスタムインフラストラクチャ パックを作成することはできません。
[説明] フィールド	インフラストラクチャ パックのユーザ定義による説明。 このフィールドはデフォルトで入力されています。 ただし、必要に応じて独自の説明を入力することもできます。 256 文字以下で入力します。 次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
[Version] ドロップダウン リスト	インフラストラクチャ コンポーネントのファームウェア アップグレードに使用できるソフトウェア バンドルのリスト。
[Force] チェックボックス	オンにすると、Cisco UCS では、選択したバージョンを前回インストールしようとしたときに失敗または中断した場合でも、インストールを試みます。

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

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

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

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

次の作業

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

プライマリ ファブリック インター コネクトのリブートの確認

⚠

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, （69 ページ）を参照してください。

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

手順

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

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

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

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

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

インフラストラクチャファームウェアのアップグレードのキャンセル

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

手順

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

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

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

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

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

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

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

ステップ 8 [OK] をクリックします。

自動インストールによるサーバ ファームウェアのアップグレード

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

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

はじめる前に

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

手順

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

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

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

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

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

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

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

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

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

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

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

c) Cisco UCS ドメインに M シリーズ サーバが含まれている場合は、[M-Series 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。

d) [Next] をクリックします。

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

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

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

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

c) [Next] をクリックします。

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

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

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

c) 必要に応じて、次のいずれかのカラムにあるリンクをクリックします。

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

d) 次のいずれかを実行します。

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

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

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

b) 影響を受けるエンドポイントのリストを確認します。

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

d) 次のいずれかを実行します。

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

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

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

第 4 章

ファームウェア自動同期サーバ ポリシーの使用

この章は、次の内容で構成されています。

- ファームウェアの自動同期，25 ページ
- ファームウェア自動同期サーバ ポリシーの設定，26 ページ

ファームウェアの自動同期

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

重要 ファームウェアの自動同期はデフォルトのホスト ファームウェア パックに基づいています。 デフォルトのホスト ファームウェア パックを削除すると、Cisco UCS Manager で重大な問題が発生します。 デフォルトのホスト ファームウェアは設定され ているが、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。

- [Auto Acknowledge]：サーバのファームウェアが Cisco UCS Manager により検出された後に自動的に同期されます。 このオプションは、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。

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

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

- サーバまたはサーバのエンドポイントのファームウェア バージョンがデフォルトのホスト ファームウェア パックで設定されているファームウェア バージョンと異なる場合。
- [Firmware Auto Sync Server] ポリシーの値が変更された場合。 たとえば、最初に値を [Auto Acknowledge] に設定し、後から [User Acknowledge] に変更した場合などです。

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

ファームウェア自動同期サーバ ポリシーの設定

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

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

はじめる前に

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

手順

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

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

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

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

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

- [Auto Acknowledge]：サーバのファームウェアが Cisco UCS Manager により検出された後に自動的に同期されます。 このオプションは、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。
- [No Action]：ファームウェアのアップグレードは、サーバで開始されません。

ステップ 6 [Save Changes] をクリックします。

第 5 章

エンドポイントのファームウェアの直接アップグレード

この章は、次の内容で構成されています。

- エンドポイントでの直接のファームウェアのアップグレード，30 ページ
- 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，34 ページ
- シャーシの CMC ファームウェアのアップデート，36 ページ
- シャーシの CMC ファームウェアのアクティブ化，37 ページ
- シャーシの共有アダプタ ファームウェアの更新，37 ページ
- シャーシの共有アダプタ ファームウェアのアクティブ化，38 ページ
- シャーシのストレージ コントローラ ファームウェアのアクティブ化，39 ページ
- シャーシのボード コントローラ ファームウェアのアクティブ化，39 ページ
- サーバの BIOS ファームウェアのアップデート，40 ページ
- サーバの BIOS ファームウェアのアクティブ化，41 ページ
- サーバの CIMC ファームウェアのアップデート，41 ページ
- サーバの CIMC ファームウェアのアクティブ化，42 ページ
- Cisco UCS Manager ソフトウェアのアクティブ化，43 ページ
- 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，44 ページ
- 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，45 ページ
- 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，46 ページ
- コンポーネントのファームウェア バージョンの確認，47 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

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

次のエンドポイントのファームウェアを直接アップグレードできます。

- シャーシ:
  - CMC
  - 共有アダプタ
  - ストレージ コントローラ
  - ボード コントローラ
- サーバ：
  - CIMC
  - BIOS
- インフラストラクチャ：
  - ファブリック インターコネクト
  - Cisco UCS Manager

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することもできます。 ホスト ファームウェア パッケージを使用して、このファームウェアをアップグレードする場合、ファームウェアのアップグレード プロセス中に、サーバをリブートする必要がある回数を削減できます。

（注） サーバに関連付けられたサービスプロファイル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。

M シリーズシャーシコンポーネントのファームウェアのアップグレードをトリガーするには、次の順に実行します。

1. CMC ファームウェアの更新
2. 共有アダプタ ファームウェアの更新
3. CMC ファームウェアのアクティブ化
4. 共有アダプタ ファームウェアのアクティブ化
5. ストレージ コントローラのアクティブ化
6. ボード コントローラのアクティブ化

エンドポイントのファームウェアのアップグレードをトリガーするには、次の順に実行します。

1. CIMC の更新
2. CIMC のアクティブ化
3. BIOS の更新
4. BIOS のアクティブ化

直接のファームウェア アップグレードのステージ

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

アップデート

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

アップデート ステージは、次のエンドポイントにのみ適用されます。

- シャーシ:
  - シャーシ管理コントローラ（CMC）
  - 共有アダプタ

- サーバ：
  - Cisco Integrated Management Controller（CIMC）
  - BIOS

⚠

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

アクティブ化

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

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

- Cisco UCS Manager
- ファブリック インターコネクト
- CMC
- 共有アダプタ
- ボード コントローラ
- ストレージ コントローラ
- CIMC
- BIOS

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

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

ファブリック インターコネクト ファームウェア アップグレードの停止の影響

ファブリックインターコネクトのファームウェアをアップグレードするときは、ファブリックインターコネクトをリブートします。

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

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

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

  実行中の保存されていない作業が失われます。

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

CMC ファームウェア アップグレードによる停止の影響

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

共有アダプタ ファームウェア アップグレードによる停止の影響

共有アダプタのファームウェアをアクティブ化する際、次の停止の影響と中断が発生します。

- サーバがリブートします。
- サーバ トラフィックが中断します。
- ストレージ コントローラがリブートします。

ストレージ コントローラのファームウェア アップグレードによる停止の影響

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

- サーバがリブートします。
- サーバ トラフィックが中断します。
- ストレージ コントローラがリブートします。

ボード コントローラのファームウェア アップグレードによる停止の影響

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

- 共有アダプタがリブートします。
- カートリッジとサーバがリブートします。
- サーバ トラフィックが中断します。
- ストレージ コントローラがリブートします。

BIOS ファームウェア アップグレードによる停止の影響

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

CIMC ファームウェア アップグレードの停止の影響

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

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

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

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

複数のエンドポイントのファームウェアのアップデート

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

- BIOS
- CIMC
- CMC
- 共有アダプタ

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

手順

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

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

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

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

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。
共有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 ファームウェアを更新する場合、ドロップダウン リストからそのタイプを選択します。

b) [Select] フィールドで、次のいずれかの手順を実行します。

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

c) [OK] をクリックします。
1 つ以上のエンドポイントを直接アップデートできない場合は、Cisco UCS Manager に通知メッセージが表示されます。 通知メッセージを確認した後、Cisco UCS Manager によって、サーバ上にある直接アップデート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アップデートされます。

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

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

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

次の作業

ファームウェアをアクティブにします。

シャーシの CMC ファームウェアのアップデート

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

手順

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

ステップ 2 [Skip Validation] タブで、[Equipment] > [Chassis] > *[Chassis Number]* を展開します。

ステップ 3 [Installed Firmware] タブで [Chassis Management Controller] を選択し、[Update Firmware] をクリックします。

ステップ 4 [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アップデートできない場合は、Cisco UCS Manager に通知メッセージが表示されます。 通知メッセージを確認した後、Cisco UCS Manager によって、サーバ上にある直接アップデート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アップデートされます。

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

ステップ 5 （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。 [Installed Firmware] タブの [Backup Version] フィールドに、選択したファームウェア パッケージが表示されるまで、ファームウェアをアクティブにしないでください。

次の作業

ファームウェアをアクティブにします。

シャーシの CMC ファームウェアのアクティブ化

手順

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

ステップ 2 [Equipment] タブの [Equipment] > [Chassis] > [Chassis *Number*] を展開します。

ステップ 3 [Installed Firmware] タブで [Chassis Management Controller] を選択し、[Activate Firmware] をクリックします。

ステップ 4 [Activate Firmware] ダイアログボックスで、次の操作を実行します。

a) [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。
1 つ以上の選択したエンドポイントが、バックアップ バージョンとして目的のバージョンで設定されていない場合、Cisco UCS Manager GUI によって、[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) [OK] をクリックします。

シャーシの共有アダプタ ファームウェアの更新

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

はじめる前に

正常にサーバの電源を切ります。

手順

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

ステップ 2 [Equipment] タブの [Equipment] > [Chassis] > [Chassis *Number*] を展開します。

ステップ 3 [Installed Firmware] タブで [Shared Adapter] を選択し、[Update Firmware] をクリックします。

ステップ 4 [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アップデートできない場合は、Cisco UCS Manager に通知メッセージが表示されます。 通知メッセージを確認した後、Cisco UCS Manager によって、サーバ上にある直接アップデート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アップデートされます。

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

ステップ 5 （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。 [Installed Firmware] タブの [Backup Version] フィールドに、選択したファームウェア パッケージが表示されるまで、ファームウェアをアクティブにしないでください。

次の作業

ファームウェアをアクティブにします。

シャーシの共有アダプタ ファームウェアのアクティブ化

手順

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

ステップ 2 [Equipment] タブの [Equipment] > [Chassis] > [Chassis *Number*] を展開します。

ステップ 3 [Installed Firmware] タブで [Shared Adapter] を選択し、[Activate Firmware] をクリックします。

ステップ 4 [Activate Firmware] ダイアログボックスで、次の操作を実行します。

a) [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。
1 つ以上の選択したエンドポイントが、バックアップ バージョンとして目的のバージョンで設定されていない場合、Cisco UCS Manager GUI によって、[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) [OK] をクリックします。

シャーシのストレージ コントローラ ファームウェアのアクティブ化

手順

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

ステップ 2 [Equipment] タブの [Equipment] > [Chassis] > [Chassis *Number*] を展開します。

ステップ 3 [Installed Firmware] タブで、更新するストレージ コントローラを選択して [Activate Firmware] をクリックします。

ステップ 4 [Activate Firmware] ダイアログボックスで、次の操作を実行します。

a) [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。
1 つ以上の選択したエンドポイントが、バックアップ バージョンとして目的のバージョンで設定されていない場合、Cisco UCS Manager GUI によって、[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) [OK] をクリックします。

シャーシのボード コントローラ ファームウェアのアクティブ化

はじめる前に

正常にサーバの電源を切ります。

手順

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

ステップ 2 [Equipment] タブの [Equipment] > [Chassis] > [Chassis *Number*] を展開します。

ステップ 3 [Installed Firmware] タブで [Board Controller] を選択し、[Activate Firmware] をクリックします。

ステップ 4 [Activate Firmware] ダイアログボックスで、次の操作を実行します。

a) [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。
1 つ以上の選択したエンドポイントが、バックアップ バージョンとして目的のバージョンで設定されていない場合、Cisco UCS Manager GUI によって、[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) [OK] をクリックします。

サーバの BIOS ファームウェアのアップデート

⚠

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

手順

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

ステップ 2 [Equipment] タブの [Equipment] > [Chassis] > [Chassis *Number*] > [Cartridges] > [Cartridge *Number*] > [Servers] を展開します。

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

ステップ 4 [Installed Firmware] タブで [BIOS] を選択し、[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、サーバの BIOS のアップデートの対象となるファームウェア バージョンを選択します。

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

c) [OK] をクリックします。

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

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

次の作業

ファームウェアをアクティブにします。

サーバの BIOS ファームウェアのアクティブ化

手順

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

ステップ 2 [Equipment] タブの [Equipment] > [Chassis] > [Chassis *Number*] > [Cartridges] > [Cartridge *Number*] > [Servers] を展開します。

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

ステップ 4 [Installed Firmware] タブで BIOS を選択し、[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、適切なサーバ BIOS のバージョンを選択します。

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

c) [OK] をクリックします。

サーバの CIMC ファームウェアのアップデート

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

手順

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

ステップ 2 [Equipment] タブの [Equipment] > [Chassis] > [Chassis *Number*] > [Cartridges] > [Cartridge *Number*] > [Servers] を展開します。

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 [Installed Firmware] タブで CIMC コントローラを選択し、[Update Firmware] をクリックします。

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

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

b) [OK] をクリックします。

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

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

次の作業

ファームウェアをアクティブにします。

サーバの CIMC ファームウェアのアクティブ化

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

⚠

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

手順

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

ステップ 2 [Equipment] タブの [Equipment] > [Chassis] > [Chassis *Number*] > [Cartridges] > [Cartridge *Number*] > [Servers] を展開します。

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 [Installed Firmware] タブで [CIMC Controller] を選択し、[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) [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。
1 つ以上の選択したエンドポイントが、バックアップ バージョンとして目的のバージョンで設定されていない場合、Cisco UCS Manager GUI によって、[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) [OK] をクリックします。

Cisco UCS Manager ソフトウェアのアクティブ化

手順

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

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

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

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

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

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

b) [OK] をクリックします。

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

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

従属ファブリックインターコネクトでのファームウェアのアクティブ化

はじめる前に

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

手順

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

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

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

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

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

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

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

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

ステップ 7 [Apply] をクリックします。
Cisco UCS Manager はファームウェアの更新とアクティベーションを実行し、ファブリック インターコネクトと、をリブートして、ファブリック インターコネクトへの双方向のデータ トラフィックを中断します。 しかし、Cisco UCS ドメインはトラフィックとポート フェールオーバーを許可するよう設定されているため、データ トラフィックはプライマリ ファブリック インターコネクトにフェールオーバーし、中断しません。

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

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

次の作業

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

プライマリ ファブリック インターコネクトでのファームウェアのアクティブ化

この手順は、従属ファブリック インターコネクトでのファームウェアのアクティブ化, （44 ページ）から直接続いており、[Firmware Management] タブが表示されていることを前提としています。

はじめる前に

下位のファブリック インターコネクトをアクティブにします。

手順

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

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

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

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

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

ステップ 4 [Apply] をクリックします。
Cisco UCS Manager はファームウェアの更新とアクティベーションを実行し、ファブリック インターコネクトと、をリブートし、ファブリックインターコネクトへの双方向のデータ トラフィックを中断します。 しかし、Cisco UCS ドメインはトラフィックとポート フェールオーバーを許可

するよう設定されているため、データ トラフィックはもう一方のファブリック インターコネクトにフェールオーバーし、このファブリック インターコネクトがプライマリとなります。このファブリック インターコネクトが再度稼働状態になると、このファブリック インターコネクトは従属ファブリック インターコネクトになります。

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

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

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

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

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

手順

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

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

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

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

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

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

ステップ 6 [OK] をクリックします。

Cisco UCS Manager はファームウェアをアクティブにし、ファブリック インターコネクトと、 スタンドアロン ファブリック インターコネクトでは、これにより Cisco UCS ドメイン内のすべてのデータ トラフィックが中断します。

コンポーネントのファームウェア バージョンの確認

手順

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

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

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

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

第 6 章

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

この章は、次の内容で構成されています。

- サービス プロファイルのファームウェア パッケージによるファームウェア アップグレード，49 ページ
- ホスト ファームウェア パッケージの作成，56 ページ
- ホスト ファームウェア パッケージのアップデート，57 ページ
- 管理ファームウェア パッケージのアップデート，58 ページ
- 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，59 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

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、サーバのファームウェアをアップグレードできます。そのためには、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。

CMC、共有アダプタ、ストレージ コントローラ、ボード コントローラ、ファブリック インターコネクト、または Cisco UCS Manager のファームウェアについては、サービス プロファイルによるアップグレードはできません。 それらのエンドポイントのファームウェアは直接アップグレードする必要があります。

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

ホスト ファームウェア パッケージ

このポリシーでは、ホスト ファームウェア パッケージ（ホスト ファームウェア パック）を構成するファームウェアバージョンのセットを指定することができます。 ホストファームウェアパッケージには、サーバのエンドポイント用の次のファームウェアが含まれています。

- CIMC
- BIOS

ヒント 同じホスト ファームウェア パッケージに複数のファームウェアを含めることができます。 たとえば、ホストファームウェアパッケージには、BIOS ファームウェアと CIMC ファームウェアの両方を含めることができます。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。

ファームウェアパッケージは、このポリシーが含まれるサービスプロファイルに関連付けられたすべてのサーバにプッシュされます。

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

このポリシーはサービス プロファイルにインクルードする必要があります。また、このサービス プロファイルを有効にするには、サーバに関連付ける必要があります。

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

管理ファームウェア パッケージ

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

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

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

このポリシーはサービス プロファイルにインクルードする必要があります。また、このサービス プロファイルを有効にするには、サーバに関連付ける必要があります。

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

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

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

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

新しいサービス プロファイル

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

ファームウェア パッケージ ポリシーの作成

このステージでは、ホスト ファームウェア パッケージを作成します。

サービス プロファイルのアソシエーション

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

既存のサービス プロファイル

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

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

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

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

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

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

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

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

ホスト ファームウェア パッケージの作成

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

はじめる前に

ファブリック インターコネクトに適切なファームウェアがダウンロードされていることを確認します。

手順

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

ステップ 2 [Servers] タブで、[Servers] > [Policies] を展開します。

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] を右クリックして [Create Host Firmware Package] を選択します。

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

ステップ 6 ホスト ファームウェア パッケージ設定の [Advanced] を選択します。

ステップ 7 各サブタブで、パッケージに含める各タイプのファームウェアに対して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、そのパッケージでアップデートするサーバに情報が一致していることを確認します。
モデルとモデル番号（PID）は、このファームウェア パッケージに関連付けられているサーバに一致する必要があります。 誤ったモデルまたはモデル番号を選択すると、Cisco UCS Manager はファームウェア更新ファイルをインストールできません。

c) [Version] カラムで、ファームウェア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。

ステップ 8 必要なすべてのファームウェアをパッケージに追加したら、[OK] をクリックします。

次の作業

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

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

はじめる前に

ファブリック インターコネクトに適切なファームウェアがダウンロードされていることを確認します。

手順

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

ステップ 2 [Servers] タブで、[Servers] > [Policies] を展開します。

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

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

ステップ 5 [Work] ペインの [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各タイプのファームウェアに対して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、そのパッケージでアップデートするサーバに情報が一致していることを確認します。
モデルとモデル番号（PID）は、このファームウェア パッケージに関連付けられているサーバに一致する必要があります。 誤ったモデルまたはモデル番号を選択すると、Cisco UCS Manager はファームウェア更新ファイルをインストールできません。

c) [Version] カラムで、ファームウェア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。

ステップ 7 [Save Changes] をクリックします。
Cisco UCS Manager はモデル番号とベンダーを、このポリシーが含まれているサービス プロファイルに関連付けられているすべてのサーバと照合します。 モデル番号とベンダーがポリシー内のファームウェア バージョンに一致する場合、Cisco UCS Manager により、サービス プロファイルに含まれているメンテナンス ポリシー内の設定に従ってファームウェアが更新されます。

管理ファームウェア パッケージのアップデート

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

ポリシーが、サーバに関連付けられている 1 つ以上のサービス プロファイルに含まれており、それらのサービスプロファイルにメンテナンスポリシーが含まれていない場合、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と、管理ファームウェアパッケージポリシーを保存するとすぐに、Cisco UCS Manager によってサーバの管理ファームウェアが新しいバージョンで更新およびアクティブ化され、サーバがリブートされます。

はじめる前に

ファブリック インターコネクトに適切なファームウェアがダウンロードされていることを確認します。

手順

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

ステップ 2 [Servers] タブで、[Servers] > [Policies] を展開します。

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

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

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

ステップ 6 ファームウェア テーブルで、次の手順を実行します。

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

b) [Vendor]、[Model]、および [PID] カラムで、そのパッケージでアップデートするサーバに情報が一致していることを確認します。
モデルとモデル番号（PID）は、このファームウェア パッケージに関連付けられているサーバに一致する必要があります。 誤ったモデルまたはモデル番号を選択すると、Cisco UCS Manager はファームウェア更新ファイルをインストールできません。

c) [Version] カラムで、ファームウェア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。

ステップ 7 [Save Changes] をクリックします。
Cisco UCS Manager はモデル番号とベンダーを、このポリシーが含まれているサービス プロファイルに関連付けられているすべてのサーバと照合します。 モデル番号とベンダーがポリシー内のファームウェア バージョンに一致する場合、Cisco UCS Manager により、サービス プロファイルに含まれているメンテナンス ポリシー内の設定に従ってファームウェアが更新されます。

既存のサービス プロファイルへのファームウェア パッケージの追加

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

手順

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

ステップ 2 [Servers] タブで、[Servers] > [Service Profiles] を展開します。

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

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

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

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

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

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

ステップ 9 [Save Changes] をクリックします。

第 7 章

Cisco UCS Manager での機能カタログの管理

この章は、次の内容で構成されています。

- 機能カタログ，61 ページ
- 機能カタログ更新のアクティブ化，63 ページ
- 機能カタログが最新であることの確認，63 ページ
- 機能カタログ プロバイダーの表示，64 ページ
- 個別の機能カタログ更新のダウンロード，64 ページ

機能カタログ

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

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

機能カタログの内容

機能カタログの内容は次のとおりです。

実装固有の調整可能なパラメータ

- 電力および熱に関する制約
- スロット範囲および番号
- アダプタ機能

ハードウェア固有のルール

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

ユーザ表示文字列

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

機能カタログの更新

機能カタログのアップデートは、各 Cisco UCS インフラストラクチャ ソフトウェア バンドルに含まれています。 Cisco TAC から特に指示された場合を除いて、Cisco UCS インフラストラクチャ ソフトウェア バンドルをダウンロードし、アップデートし、アクティブ化した後に、機能カタログのアップデートをアクティブ化する必要があるだけです。

機能カタログのアップデートをダウンロードすると、Cisco UCS によってすぐに新しいベースライン カタログに更新されます。 それ以外の作業は行う必要がありません。 機能カタログの更新では、Cisco UCS ドメイン内のコンポーネントをリブートや再インストールを行う必要はありません。

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

（注） 機能カタログのバージョンは、使用している Cisco UCS のバージョンによって決まります。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、『*Release Notes for Cisco UCS Administration Software*』を参照してください。

機能カタログ更新のアクティブ化

手順

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

ステップ 2 [Admin] タブで [All] を展開します。

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

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

ステップ 5 [Activate Catalog] をクリックします。

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

ステップ 7 [OK] をクリックします。

機能カタログが最新であることの確認

はじめる前に

手順

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

ステップ 2 [Admin] タブで [All] を展開します。

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

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

ステップ 5 Cisco.com で、機能カタログの利用可能な最新リリースを確認します。
機能カタログのアップデートの場所については、シスコからの機能カタログのアップデートの入手方法, （64 ページ）を参照してください。

ステップ 6 より新しいバージョンの機能カタログを Cisco.com で入手できる場合は、そのバージョンを使用して機能カタログをアップデートします。

機能カタログ プロバイダーの表示

手順

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

ステップ 2 [Admin] タブで、[All] > [Capability Catalog] を展開します。

ステップ 3 [Work] ペインで、表示するプロバイダーのタブをクリックします。

ステップ 4 プロバイダーの詳細情報を表示するには、次の手順を実行します。

a) テーブルで、表示するプロバイダーのベンダー、モデル、リビジョンの行をクリックします。

b) 見出しの右側にある [Expand] アイコンをクリックし、次の領域のプロパティを表示します。

- [Equipment Manufacturing] 領域
- [Form Factor] 領域

個別の機能カタログ更新のダウンロード

シスコからの機能カタログのアップデートの入手方法

手順

ステップ 1 Web ブラウザで、 Cisco.com を参照します。

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

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

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

ステップ 5 右側のペインで、[Cisco UCS Infrastructure and UCS Manager Software] > [Unified Computing System (UCS) Manager Capability Catalog] をクリックします。

ステップ 6 機能カタログの最新リリースのリンクをクリックします。

ステップ 7 次のいずれかのボタンをクリックして、表示される指示に従います。

- [Download Now]：カタログのアップデートをただちにダウンロードできます。

- [Add to Cart]：後でダウンロードできるよう、カタログのアップデートをカートに入れます。

ステップ 8 プロンプトに従い、カタログのアップデートのダウンロードを完了します。

次の作業

機能カタログをアップデートします。

リモート ロケーションからの機能カタログの更新

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

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

手順

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

ステップ 2 [Admin] タブで [All] を展開します。

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

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

ステップ 5 [Update Catalog] をクリックします。

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

ステップ 7 [OK] をクリックします。

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

次の作業

機能カタログの更新をアクティブ化します。

ローカル ファイル システムからの機能カタログの更新

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

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

手順

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

ステップ 2 [Admin] タブで [All] を展開します。

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

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

ステップ 5 [Update Catalog] をクリックします。

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

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

ステップ 8 [OK] をクリックします。

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

次の作業

機能カタログの更新をアクティブ化します。

第 8 章

管理拡張機能の更新

この章は、次の内容で構成されています。

- Management Extension, 67 ページ
- 管理拡張機能のアクティブ化, 67 ページ

Management Extension

管理拡張機能の更新は各 Cisco UCS Manager のアップデートに含まれています。 シスコのテクニカル サポートから指示された場合を除いて、Cisco UCS インフラストラクチャ ソフトウェア バンドルをダウンロードし、更新し、アクティブ化した後に、管理拡張機能の更新をアクティブ化する必要があるだけです。

管理拡張機能を使用すると、以前はサポートされていなかったサーバや他のハードウェアのサポートを Cisco UCS Manager に追加することができます。 たとえば、以前はサポートされていなかった新しいサーバを既存の Cisco UCS ドメインに追加する場合は、管理拡張機能をアクティブ化する必要があります。

管理拡張機能のイメージには、Cisco UCS Manager で新しいハードウェアを管理するために必要なイメージ、情報、ファームウェアが含まれています。

Cisco UCS Manager をアクティブにすると、管理拡張機能にアクセスする必要が生じる場合があります。 このため、管理拡張機能は有効化と更新の処理中はロックされます。

管理拡張機能のアクティブ化

Management Extension は、すでにダウンロードしたサーバ バンドルに含まれています。 Management Extension を個別にダウンロードする必要はありません。

手順

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

ステップ 2 [Admin] タブで [All] を展開します。

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

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

ステップ 5 [Actions] 領域で、[Activate Management Extension] をクリックします。

ステップ 6 [Activate Management Extension] 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管理拡張機能を選択します。

ステップ 7 [OK] をクリックします。

第 9 章

データ パスの準備が整っていることの確認

この章は、次の内容で構成されています。

- ダイナミック vNIC が稼働中であることの確認，69 ページ
- イーサネット データ パスの確認，70 ページ
- 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，70 ページ
- ファイバ チャネル スイッチ モードのデータ パスの確認，71 ページ

ダイナミック vNIC が稼働中であることの確認

ダイナミック vNIC、および VMware vCenter との統合を含む Cisco UCS をアップグレードする場合、データ パスの中断を回避するために、以前のプライマリ ファブリック インターコネクトで新しいソフトウェアをアクティブにする前に、すべてのダイナミック vNIC が新しいファブリック インターコネクトで稼働中であることを確認する必要があります。

この手順は Cisco UCS Manager GUI で実行します。

手順

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

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

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

ステップ 4 [Work] ペインで、[VIF] タブをクリックします。

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

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

イーサネット データ パスの確認

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A /fabric-interconnect # **connect nxos** {**a** | **b**}	ファブリック インターコネクトのNX-OSモードを開始します。
ステップ 2	UCS-A(nxos)# **show int br | grep -v down | wc –l**	アクティブなイーサネット インターフェイスの数を返します。 この数がアップグレードの前に稼働していたイーサネット インターフェイスの数と一致することを確認します。
ステップ 3	UCS-A(nxos)# **show platform fwm info hw-stm | grep '1.' | wc –l**	MAC アドレスの合計数を返します。 この数がアップグレード前のMACアドレスの数と一致することを確認します。

次の例では、従属ファブリック インターコネクト A のアクティブなイーサネット インターフェイスおよび MAC アドレスの数が返され、ファブリック インターコネクトのイーサネット データ パスが稼働していることを確認できます。

```
UCS-A /fabric-interconnect # connect nxos a
UCS-A(nxos)# show int br | grep -v down  | wc -l
86
UCS-A(nxos)# show platform fwm info hw-stm | grep '1.' | wc -l
80
```

ファイバ チャネル エンドホスト モードのデータ パスの確認

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

手順

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

	コマンドまたはアクション	目的
ステップ 2	UCS-A(nxos)# **show npv flogi-table**	flogi セッションのテーブルを表示します。
ステップ 3	UCS-A(nxos)# **show npv flogi-table | grep fc | wc -l**	ファブリック インターコネクトにログインしたサーバの数を返します。 出力は、アップグレードの開始前にこの確認を行ったときに受け取った出力と一致している必要があります。

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

```
UCS-A /fabric-interconnect # connect nxos a
UCS-A(nxos)# show npv flogi-table
--------------------------------------------------------------------------------
SERVER                                                                 EXTERNAL
INTERFACE VSAN FCID            PORT NAME               NODE NAME       INTERFACE
--------------------------------------------------------------------------------
vfc705    700  0x69000a 20:00:00:25:b5:27:03:01 20:00:00:25:b5:27:03:00 fc3/1
vfc713    700  0x690009 20:00:00:25:b5:27:07:01 20:00:00:25:b5:27:07:00 fc3/1
vfc717    700  0x690001 20:00:00:25:b5:27:08:01 20:00:00:25:b5:27:08:00 fc3/1

Total number of flogi = 3.

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

ファイバ チャネル スイッチ モードのデータ パスの確認

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

手順

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

	コマンドまたはアクション	目的
		出力は、アップグレードの開始前にこの確認を行ったときに受け取った出力と一致している必要があります。

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

```
UCS-A /fabric-interconnect # connect nxos a
UCS-A(nxos)# show flogi database
--------------------------------------------------------------------------------
INTERFACE        VSAN    FCID           PORT NAME               NODE NAME
--------------------------------------------------------------------------------
vfc726           800   0xef0003  20:00:00:25:b5:26:07:02 20:00:00:25:b5:26:07:00
vfc728           800   0xef0007  20:00:00:25:b5:26:07:04 20:00:00:25:b5:26:07:00
vfc744           800   0xef0004  20:00:00:25:b5:26:03:02 20:00:00:25:b5:26:03:00
vfc748           800   0xef0005  20:00:00:25:b5:26:04:02 20:00:00:25:b5:26:04:00
vfc764           800   0xef0006  20:00:00:25:b5:26:05:02 20:00:00:25:b5:26:05:00
vfc768           800   0xef0002  20:00:00:25:b5:26:02:02 20:00:00:25:b5:26:02:00
vfc772           800   0xef0000  20:00:00:25:b5:26:06:02 20:00:00:25:b5:26:06:00
vfc778           800   0xef0001  20:00:00:25:b5:26:01:02 20:00:00:25:b5:26:01:00

Total number of flogi = 8.
UCS-A(nxos)# show flogi database | grep fc | wc -l
8
```