Cisco UCS M シリーズ CLI 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 イメージ ヘッダー 2

ファームウェア イメージ カタログ 2

ファームウェア バージョン 3

ファームウェア アップグレードのオプション 4

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 5

Cisco UCS Manager によるファームウェアの管理 9

Cisco UCS Manager でのファームウェアのダウンロードと管理 11

シスコからの M シリーズ ソフトウェア バンドルの取得 12

M シリーズファームウェアイメージをリモートの場所からファブリック インターコネクトにダウンロードする 13

ファームウェア パッケージのダウンロード ステータスの表示 14

イメージ ダウンロードのキャンセル 15

ファブリック インターコネクトの利用可能なすべてのソフトウェア イメージの表示 16

ファブリック インターコネクトの利用可能なすべてのパッケージの表示 17

ファームウェア パッケージの内容の判断 17

ファブリック インターコネクトの空き領域のチェック 18

ファブリック インターコネクトからのファームウェア パッケージの削除 19

ファブリック インターコネクトからのファームウェア イメージの削除 19
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 21
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 21
インフラストラクチャ ファームウェアのインストール 22
サーバ ファームウェアのインストール 22
自動インストールのための必要な手順 22
自動インストールによるアップグレードに関する注意、ガイドライン、および制約事項 23
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 26
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 28
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 29
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 31
エンドポイントでのファームウェアの直接アップグレード 31
ファームウェアの直接アップグレードのステージ 33
ファームウェアの直接アップグレードの停止の影響 34
シャーシ上の CMC ファームウェアのアップデートとアクティブ化 36
シャーシ上の共有アダプタ ファームウェアのアップデートとアクティブ化 38
シャーシ上のストレージ コントローラ ファームウェアのアクティブ化 41
シャーシ上のボード コントローラ ファームウェアのアクティブ化 42
サーバの BIOS ファームウェアの更新とアクティブ化 42
サーバの CIMC ファームウェアのアップデートおよびアクティブ化 44
Cisco UCS Manager ソフトウェアのアクティブ化 47
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 48
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 51
サービス プロファイルのファームウェア パッケージによるファームウェア アップグレード 51
ホスト ファームウェア パッケージ 52
管理ファームウェア パッケージ 53
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 53

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 54
ホスト ファームウェア パッケージの作成または更新 58
管理ファームウェア パッケージのアップデート 61
Cisco UCS Manager での機能カタログの管理 63
機能カタログ 63
機能カタログの内容 63
機能カタログの更新 64
個別の機能カタログ更新のダウンロード 65
シスコからの機能カタログのアップデートの入手方法 65
リモート ロケーションからの機能カタログの更新 65
機能カタログが最新であることの確認 67
M シリーズの機能カタログ更新のアクティブ化 67
機能カタログ更新のリスタート 68
機能カタログ プロバイダーの表示 69
管理拡張機能の更新 73
Management Extension 73
管理拡張機能のアクティブ化 73

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，3 ページ
- ファームウェア アップグレードのオプション，4 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。

管理拡張機能 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 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。

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。

BIOS、CIMC、CMC、および共有アダプタのファームウェア バージョン

各 CIMC、BIOS、共有アダプタ、および CMC にファームウェア用のフラッシュが 2 つずつ付属します。 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。 そのため、それらをアクティブにすることしかできません。

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

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

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

ファームウェア アップグレードのオプション

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

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

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

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

- 自動インストールによるインフラストラクチャとサーバのアップグレード：このオプションでは、最初の段階ですべてのインフラストラクチャ コンポーネントをアップグレードします。 次の段階で、ホスト ファームウェア パッケージを使用してすべてのサーバ エンドポイントをアップグレードできます。
- サービス プロファイルのファームウェア パッケージを使用してサーバをアップグレード：このオプションを使用すると 1 回のステップですべてのサーバのエンドポイントをアップグレードできるため、サーバのリブートによる中断時間を短くすることができます。 サービス プロファイルの更新の延期導入とこのオプションを組み合わせて、スケジュールされたメンテナンス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とサーバ エンドポイントの直接アップグレード：このオプションでは、ファブリック インターコネクト、共有アダプタ、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 エンドポイントを直接アップグレードできます。 ただし、直接アップグレードは、サーバ BIOS、ストレージ コントローラ、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。

設定の変更とアップグレードに影響を与える可能性がある設定

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

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

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

Cisco UCS Release 2.0(1) のサービス プロファイル全体において、iSCSI vNIC で同じイニシエータ IQN が使用されている場合は、アップグレードすると、サービス プロファイル レベルの重複したイニシエータ IQN が生成されます。 このような構成では、サービス プロファイル レベルで定義された重複イニシエータ IQN を持つ各 iSCSI vNIC に対してエラーが生成されます。 これらのエラーは、サービス プロファイル レベルの重複イニシエータ IQN を変更すると解消されます。 サービス プロファイル関連の操作（ホスト ファームウェア パッケージのアップデートなど）を実行する前に、これらのエラーを解消する必要があります。

デフォルトのメンテナンス ポリシーの設定を「ユーザ確認応答」にする

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

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

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

⚠

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

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

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

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

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

FCoE ストレージ ポートのネイティブ VLAN に VLAN ID 4048 が使用されていた Cisco UCS Release 1.4 からリリース 2.0 にアップグレードした後、デフォルトの VLAN ID は次のようになります。

- デフォルトのイーサネット VLAN ID は 1 です。

- 現在のデフォルトの FCoE VLAN ID が保持されます。 競合するイーサネット VLAN がある場合、Cisco UCS Manager によって重大なエラーが生成されます。 1 つの VLAN ID を、使用または予約されていない VLAN ID に変更する必要があります。

（注） Cisco UCS ドメインでデフォルト VLAN ID の 1 つが使用されているため VLAN のオーバーラップが発生している場合は、1 つ以上のデフォルト VLAN ID を、使用または予約されていない VLAN ID に変更します。 リリース 2.0 以降では ID が 4030 ～ 4047 の VLAN は予約されます。

重要 VSAN、FC、および FCoE は Cisco UCS リリース 2.5 でサポートされていません。

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，11 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，21 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，31 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，51 ページ
- Cisco UCS Manager での機能カタログの管理，63 ページ
- 管理拡張機能の更新，73 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。

- シスコからの M シリーズ ソフトウェア バンドルの取得，12 ページ
- M シリーズ ファームウェア イメージをリモートの場所からファブリック インターコネクトにダウンロードする，13 ページ
- ファームウェア パッケージのダウンロード ステータスの表示，14 ページ
- イメージ ダウンロードのキャンセル，15 ページ
- ファブリック インターコネクトの利用可能なすべてのソフトウェア イメージの表示，16 ページ
- ファブリック インターコネクトの利用可能なすべてのパッケージの表示，17 ページ
- ファームウェア パッケージの内容の判断，17 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，18 ページ
- ファブリック インターコネクトからのファームウェア パッケージの削除，19 ページ
- ファブリック インターコネクトからのファームウェア イメージの削除，19 ページ

シスコからの M シリーズ ソフトウェア バンドルの取得

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] の順にクリックします。

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。

M シリーズ ファームウェア イメージをリモートの場所からファブリック インターコネクトにダウンロードする

（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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope firmware**	ファームウェア モードを開始します。
ステップ 2	UCS-A /firmware # **download image** *URL*	ファームウェア バンドルをダウンロードします。 シスコから提供されたダウンロードパスを使用し、次のいずれかの構文で URL を指定します。 • **ftp:**// *server-ip-addr* / *path* • **scp:**// *username@server-ip-addr* / *path* • **sftp:**// *username@server-ip-addr* / *path* • **tftp:**// *server-ip-addr* **:** *port-num* / *path* （注） [TFTP] ではファイル サイズが 32 MB に制限されます。 ファームウェア バンドルはそれよりも大幅にサイズが大きい可能性があるため、ファームウェアのダウンロードに TFTP を選択しないことを推奨します。 IP アドレスではなくホスト名を使用する場合、Cisco UCS Manager で DNS サーバを設定します。
ステップ 3	リモート サーバのパスワードを入力します。	リモート サーバのユーザ名のパスワード。 プロトコルが tfpt の場合、このフィールドは適用されません。

	コマンドまたはアクション	目的
ステップ 4	UCS-A /firmware # **show download-task**	ダウンロード タスクのステータスを表示します。 イメージのダウンロードが完了すると、タスク状態が Downloading から Downloaded に変更されます。 CLI の表示は自動的には更新されないので、タスクのステータスに Downloaded が表示されるまで何度も **show download-task** コマンドを入力する必要があります。
ステップ 5	すべてのファームウェア バンドルがファブリック インターコネクトにダウンロードされるまで、このタスクを繰り返します。	

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

```
UCS-A# scope firmware
UCS-A /firmware # download image
scp://user1@192.168.10.10/images/ucs-k9-bundle-m-series.2.5.0.224.M.bin
UCS-A /firmware # show download-task
UCS-A /firmware #
```

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。

ファームウェア パッケージのダウンロード ステータスの表示

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

手順

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

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

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

Download task:
File Name                                    Protocol     Server          Userid      State
---------                                    --------     --------------- ---------   -----
ucs-k9-bundle-m-series.2.5.0.224.M.bin        Scp          10.193.32.11    user1
Downloading

UCS-A /firmware # show download-task

Download task:
File Name                                    Protocol     Server          Userid      State
---------                                    --------     --------------- ---------   -----
ucs-k9-bundle-m-series.2.5.0.224.M.bin        Scp          10.193.32.11    user1
Downloaded
```

イメージ ダウンロードのキャンセル

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

手順

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

次の例は、イメージのダウンロードを取り消します。

```
UCS-A# scope firmware
UCS-A /firmware # delete download-task ucs-k9-bundle-m-series.2.5.0.202.M.bin
UCS-A /firmware* # commit-buffer
UCS-A /firmware* #
```

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

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

手順

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

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

```
UCS-A# scope firmware
UCS-A /firmware # show image
Name                                          Type                  Version
--------------------------------------------- -------------------- -------
ucs-4308-brdprog.1.0.6.bin                    Board Controller      1.0.6
ucs-4308.2.0.2.45.bin                         Chassis Management Controller
                                                                    2.0(2.45)
ucs-6100-k9-kickstart.5.2.3.N2.2.50.225.bin   Fabric Interconnect Kernel
                                                                    5.2(3)N2(2.50.225)
ucs-6100-k9-system.5.2.3.N2.2.50.225.bin      Fabric Interconnect System
                                                                    5.2(3)N2(2.50.225)
ucsme-142-m4-bios.UCSME.142M4.2.0.100.54.011620150100.bin
                                              Server BIOS
UCSME.142M4.2.0.100.54.011620150100
ucsme-142-m4-k9-cimc.2.0.100.59.bin           CIMC                  2.0(100.59)
```

ファブリックインターコネクトの利用可能なすべてのパッケージの表示

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

手順

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

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

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

ファームウェア パッケージの内容の判断

手順

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

次に、ファームウェア パッケージの内容を表示する例を示します。

```
UCS-A# scope firmware
UCS-A /firmware # show package ucs-k9-bundle-m-series.2.5.0.224.M.bin expand
```

```
Package ucs-k9-bundle-m-series.2.5.0.224.M.bin:

  Images:
      ucs-4308-brdprog.1.0.6.bin
      ucs-4308.2.0.2.45.bin
      ucs-m-lsi-mrsas-9361-8i.24.5.1.9.bin
      ucs-m83-8p40-vic.4.0.2S47.bin
      ucsme-142-m4-bios.UCSME.142M4.2.0.100.54.011620150100.bin
      ucsme-142-m4-k9-cimc.2.0.100.59.bin

UCS-A /firmware #
```

ファブリック インターコネクトの空き領域のチェック

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

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fabric-interconnect** {**a** | **b**}	指定したファブリックのファブリックインターコネクトモードを開始します。
ステップ 2	UCS-A /fabric-interconnect # **show storage** [**detail** | **expand**}	指定したファブリックの空き領域を表示します。 （注） ファームウェアイメージバンドルをダウンロードする場合、ファブリック インターコネクトに、ファームウェア イメージ バンドルのサイズの少なくとも 2 倍の空き領域が必要です。ブートフラッシュに十分な領域がない場合は、ファブリック インターコネクトから、古いファームウェア、コア ファイル、その他の不要なオブジェクトを削除してください。

次の例は、ファブリック インターコネクトの空き領域を表示します。

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect # show storage
Storage on local flash drive of fabric interconnect:
    Partition        Size (MBytes)    Used Percentage
    ---------------- ---------------- ---------------
    bootflash        8658             50
    opt              1917             2
    workspace        277              4
UCS-A /fabric-interconnect #
```

ファブリック インターコネクトからのファームウェア パッケージの削除

パッケージ全体を削除するには、この手順を使用します。 パッケージから 1 つのイメージのみを削除することも可能です。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope firmware**	ファームウェア モードを開始します。
ステップ 2	UCS-A /firmware # **delete package** *package-name*	指定したファームウェアパッケージを削除します。
ステップ 3	UCS-A /firmware # **commit-buffer**	トランザクションをシステムの設定にコミットします。

Cisco UCS Manager によって、選択したパッケージおよび各パッケージに含まれるすべてのイメージが削除されます。

次に、ファームウェア パッケージを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope firmware
UCS-A /firmware # delete package ucs-k9-bundle-infra.2.5.0.224.A.bin
UCS-A /firmware* # commit-buffer
UCS-A /firmware #
```

ファブリック インターコネクトからのファームウェア イメージの削除

この手順は、パッケージから単一のイメージだけを削除する場合に使用します。

手順

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

次に、ファームウェア イメージを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope firmware
UCS-A /firmware # delete image ucs-m-lsi-mrsas-9361-8i.24.5.1.8.bin
UCS-A /firmware* # commit-buffer
UCS-A /firmware #
```

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，21 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，26 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，28 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，29 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 インターコネクトなどのインフラストラクチャ コンポーネントと Cisco UCS Manager 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 ドメイン内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 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アップグレードに関する注意、ガイドライン、および制約事項

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

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

エンドポイントの状態

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

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

デフォルトのホスト ファームウェア ポリシーに関する推奨事項

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

サーバ ファームウェアのアップグレード中に、Cisco UCS ドメイン内のサーバのファームウェアをデフォルト ホスト ファームウェア ポリシーに追加できます。アップグレードを完了するには、すべてのサーバをリブートする必要があります。

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

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

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

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

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

必要な権限

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

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

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

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

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

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

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

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

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

新たに追加されたサーバのサーバ ファームウェアのアップグレード

サーバファームウェアのインストールを実行した後、CiscoUCSドメインにサーバを追加すると、新しいサーバのファームウェアはサーバ ファームウェアのインストールによって自動的にアップグレードされません。新しく追加したサーバのファームウェアを、最後にサーバファームウェアのインストールを実行したときに使用したファームウェア バージョンにアップグレードする場合

は、エンドポイントをそのサーバのファームウェアに手動でアップグレードする必要があります。サーバファームウェアのインストールには、ファームウェアバージョンの変更が毎回必要です。サーバを同じファームウェアバージョンにアップグレードするためにサーバファームウェアのインストールを再実行することはできません。

（注） リリース 2.2 へのアップグレードが終了すると、Cisco UCS Manager で [Firmware Auto Sync Server] ポリシーを使用して、新たに検出されたサーバを自動的に更新できます。

インフラストラクチャ ファームウェアのアップグレード

Cisco UCS Manager CLI のリリースが 2.1(1) よりも古い場合、**auto-install** は使用できません。

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope firmware**	ファームウェア モードを開始します。
ステップ 2	UCS-A /firmware # **scope auto-install**	インフラストラクチャ ファームウェアのアップグレードの自動インストール モードを開始します。
ステップ 3	UCS-A /firmware/auto-install # **install infra infra-vers** *infrastructure-bundle-version* [**starttime** *mon dd yyyy hh min sec*] [**force**]	インフラストラクチャ ファームウェアを更新してアクティブにします。 トランザクションをコミットしてすぐにアップグレードを開始したくない場合は、**starttime** を使用してインフラストラクチャ ファームウェアのアップグレードをスケジュールする必要があります。 **starttime** を使用する場合は、アップグレードをいつスケジュールするかを指定するために、次の情報を入力してください。 • *mon*：jan または feb など目的の月の名前の最初の 3 文字。 • *dd*：月の目的の日（1 ～ 31）。

	コマンドまたはアクション	目的
		• *yyyy*：2012 などの目的の年（西暦）。 • *hh*：アップグレードを開始する時刻の時（0～23）。 • *min*：アップグレードを開始する時刻の分（0～60）。 • *sec*：アップグレードを開始する時刻の秒（0～60）。 互換性のない可能性や、現在実行中のタスクに関係なく、ファームウェアをアクティブにするには、**force** キーワードを使用します。 **注意** アップグレードを続行する前に、表示されたチェックリストを見直して、すべての要件が満たされていることを確認します。
ステップ 4	UCS-A /firmware/auto-install # **commit-buffer**	トランザクションをシステムの設定にコミットします。 （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。

次に、Cisco UCS インフラストラクチャ ソフトウェア バンドル でインフラストラクチャをファームウェアにアップグレードして、トランザクションをコミットする例を示します。

```
UCS-A# scope firmware
UCS-A /firmware # scope auto-install
UCS-A /firmware/auto-install # install infra infra-vers ucs-k9-bundle-infra.2.5.0.225.A.bin
This operation upgrades firmware on UCS Infrastructure Components
(UCS manager, Fabric Interconnects and IOMs).
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup
(3) Check if Management Interface Monitoring Policy is enabled
(4) Check if there is a pending Fabric Interconnect Reboot activitiy
(5) Ensure NTP is configured
Do you want to proceed? (yes/no): yes
UCS-A /firmware/auto-install* # commit-buffer
UCS-A /firmware/auto-install #
```

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 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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope firmware**	ファームウェア モードを開始します。
ステップ 2	UCS-A /firmware # **scope auto-install**	インフラストラクチャ ファームウェアのアップグレードの自動インストール モードを開始します。
ステップ 3	UCS-A /firmware/auto-install # **acknowledge primary fabric-interconnect reboot**	プライマリ ファブリック インターコネクトの保留中のリブートを確認します。
ステップ 4	UCS-A /firmware/auto-install # **commit-buffer**	トランザクションをシステムの設定にコミットします。 Cisco UCS Manager によって、即座にプライマリ ファブリック インター コネクトがリブートされます。 トランザクションをコミットした後でこのリブートを停止することはできません。

次に、プライマリ ファブリック インターコネクトのリブートを確認し、トランザクションをコミットする例を示します。

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

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

インフラストラクチャファームウェアのアップグレードのキャンセル

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

手順

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

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

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

第 4 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ファームウェアの直接アップグレード，31 ページ
- シャーシ上の CMC ファームウェアのアップデートとアクティブ化，36 ページ
- シャーシ上の共有アダプタ ファームウェアのアップデートとアクティブ化，38 ページ
- シャーシ上のストレージ コントローラ ファームウェアのアクティブ化，41 ページ
- シャーシ上のボード コントローラ ファームウェアのアクティブ化，42 ページ
- サーバの BIOS ファームウェアの更新とアクティブ化，42 ページ
- サーバの CIMC ファームウェアのアップデートおよびアクティブ化，44 ページ
- Cisco UCS Manager ソフトウェアのアクティブ化，47 ページ
- 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，48 ページ

エンドポイントでのファームウェアの直接アップグレード

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、エンドポイントのファームウェアの直接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

サービス プロファイルのホスト ファームウェア パッケージを使用して、CIMC フォームウェアと BIOS ファームウェアを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 コンポーネント上のファームウェア アップグレードをトリガーするには、次の順序を使用します。

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

エンドポイント上のファームウェア アップグレードをトリガーするには、次の順序を使用します。

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

ファームウェアの直接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。

- Chassis:
  - 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。

ファームウェアの直接アップグレードの停止の影響

エンドポイントで、ファームウェアの直接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、ファブリック インターコネクトがリブートされます。

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

シャーシ内の CMC のファームウェアをアップグレードしても、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にすると、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 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にすると、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 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にすると、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お勧めします。 アクティブ化中にサーバの電源をオフにしなかった場合は、Cisco UCSM がサーバの電源をオフにしようと試みて、最大 16 分間待機します。 この間に Cisco UCSM がサーバの電源がオフになっていないことを検出した場合は、FSM が失敗して、Cisco UCSM は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 がサーバの電源を正常にオフにした場合は、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。

シャーシ上の CMC ファームウェアのアップデートとアクティブ化

⚠

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope chassis** *chassis-id*	指定サーバのシャーシ サーバ モードを開始します。
ステップ 2	UCS-A /chassis # **scope cmc**	シャーシ CMC モードに入ります。
ステップ 3	UCS-A /chassis/cmc # **update firmware** *version-num*	シャーシの CMC で、選択されたファームウェア バージョンを更新します。
ステップ 4	UCS-A /chassis/cmc # **commit-buffer**	（任意） トランザクションをコミットします。 このステップを使用するのは、ステップ 6 でファームウェアをアクティブにする前に、ファームウェア更新が正常に完了したことを確認するためにステップ 5 で **show update status** コマンドを使用する場合だけです。 このステップをスキップして、同じトランザクションで **update-firmware** および **activate-firmware** コマンドをコミットできます。ただし、ファームウェア更新が正常に完了していない場合は、ファームウェア アクティブ化が開始されません。 Cisco UCS Manager によって、選択したファームウェア イメージがバックアップ メモリ パーティションにコピーされ、そのイメージが破損していないことが確認されます。イメージは、明示的にアクティブにするまで、バックアップ バージョンとして残されます。
ステップ 5	UCS-A /chassis/cmc # **show update status**	（任意） ファームウェアのアップデートのステータスを表示します。 ファームウェアのアップデートが正常に完了したことを確認する場合にのみ、このステップを使用します。 アップデート ステータスが Ready になったら、ファームウェアの

	コマンドまたはアクション	目的
		アップデートは完了です。 CLI は自動的に表示更新されないため、タスクの状態が Updating から Ready に変更されるまで何度も **show update status** コマンドを入力しなければならない場合があります。アップデートステータスが Ready になったらステップ 6 に進みます。
ステップ 6	UCS-A /chassis/cmc # **activate firmware** *version-num*	サーバ内の CMC で、選択されたファームウェア バージョンをアクティブにします。
ステップ 7	UCS-A /chassis/cmc # **commit-buffer**	トランザクションをコミットします。
ステップ 8	UCS-A /chassis/cmc # **show activate status**	（任意） ファームウェアのアクティベーションのステータスを表示します。 ファームウェアのアクティベーションが正常に完了したことを確認する場合にのみ、このステップを使用します。CLI は自動的に表示更新されないため、タスクの状態が Activating から Ready に変更されるまで何度も **show activate status** コマンドを入力しなければならない場合があります。
ステップ 9	CS-A /chassis/cmc # **show firmware**	（任意） 実行中のファームウェアのバージョン、更新ステータス、およびアクティブ化ステータスを表示します。

次の例では、ファームウェア更新とファームウェア アクティブ化が正常に完了したことを確認せずに、同じトランザクション内で CMC ファームウェアをバージョン 2.0(2.30) に更新してアクティブにします。

```
UCS-A# scope chassis 2
UCS-A# /chassis # scope cmc
UCS-A# /chassis/cmc # update firmware 2.0(2.30)
UCS-A# /chassis/cmc* # activate firmware 2.0(2.30)
UCS-A# /chassis/cmc* # commit-buffer
UCS-A# /chassis/cmc # show firmware
CMC:
    Running-Vers: 2.0(2.30)
    Package Vers: 2.5(0.147)M
    Update-Status: Ready
    Activate-Status: Ready
```

次の例では、CMC ファームウェアをバージョン 2.0(2.30) に更新して、ファームウェア更新が正常に完了したことを確認してからファームウェア アクティブ化を開始し、CMC ファームウェアをアクティブにして、ファームウェア アクティブ化が正常に完了したことを確認します。

```
UCS-A# scope chassis 2
UCS-A# /chassis # scope cmc
UCS-A# /chassis/cmc # update firmware 2.0(2.30)
UCS-A# /chassis/cmc* # commit-buffer
UCS-A# /chassis/cmc # show update status
Status: Ready
UCS-A# /chassis/cmc # activate firmware 2.0(2.30)
UCS-A# /chassis/cmc* # commit-buffer
UCS-A# /chassis/cmc # show activate status
Status: Ready
UCS-A# /chassis/cmc # show firmware
CMC:
    Running-Vers: 2.0(2.30)
    Package Vers: 2.5(0.147)M
    Update-Status: Ready
    Activate-Status: Ready
```

シャーシ上の共有アダプタファームウェアのアップデートとアクティブ化

Cisco M シリーズでは、共有アダプタ ファームウェアを更新してアクティブ化すると、シャーシ内のすべてのサーバが影響を受けます。

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。

はじめる前に

正しい手順でサーバの電源をオフにします。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope chassis** *chassis-id*	指定したシャーシでシャーシ モードを開始します。
ステップ 2	UCS-A /chassis # **scope adapter**	シャーシ アダプタ モードに入ります。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /chassis/adapter # **show image**	共有アダプタに使用可能なソフトウェアイメージを表示します。
ステップ 4	UCS-A /chassis/adapter # **update firmware** *version-num*	共有アダプタ上で選択されたファームウェアバージョンを更新します。
ステップ 5	UCS-A /chassis/adapter # **commit-buffer**	（任意） トランザクションをコミットします。 このステップを使用するのは、ステップ 7 でファームウェアをアクティブにする前に、ファームウェア更新が正常に完了したことを確認するためにステップ 6 で **show update status** コマンドを使用する場合だけです。 このステップをスキップして、同じトランザクションで **update-firmware** および **activate-firmware** コマンドをコミットできます。ただし、ファームウェア更新が正常に完了していない場合は、ファームウェアアクティブ化が開始されません。
ステップ 6	UCS-A /chassis/adapter # **show update status**	（任意） ファームウェアのアップデートのステータスを表示します。 ファームウェアのアップデートが正常に完了したことを確認する場合にのみ、このステップを使用します。 アップデートステータスが Ready になったら、ファームウェアのアップデートは完了です。 CLI は自動的に表示更新されないため、タスクの状態が Updating から Ready に変更されるまで何度も **show update status** コマンドを入力しなければならない場合があります。 アップデートステータスが Ready になったらステップ 7 に進みます。
ステップ 7	UCS-A /chassis/adapter # **activate firmware** *version-num*	共有アダプタ上で選択されたファームウェアバージョンをアクティブにします。
ステップ 8	UCS-A /chassis/adapter # **commit-buffer**	トランザクションをコミットします。
ステップ 9	UCS-A /chassis/adapter # **show activate status**	ファームウェアのアクティベーションのステータスを表示します。 ファームウェアのアクティベーションが正常に完了したことを確認する場合にのみ、このステップを使用します。 CLI は自動的に表示更新されないため、タスクの状態が Activating から Ready に変更されるまで何度も **show**

	コマンドまたはアクション	目的
		activate status コマンドを入力しなければならない場合があります。
ステップ 10	UCS-A /chassis/adapter # **show firmware**	（任意） 実行中のファームウェアのバージョン、更新ステータス、およびアクティブ化ステータスを表示します。

次の例では、ファームウェア更新とファームウェア アクティブ化が正常に完了したかどうかを確認せずに、同じトランザクション内で共有アダプタ ファームウェアをバージョン 4.0(2S33) に更新してアクティブにします。

```
UCS-A# scope chassis 1
UCS-A# /chassis # scope adapter
UCS-A# /chassis/adapter # show image
Name                                        Type                Version
------------------------------------------- ------------------- -------
ucs-m83-8p40-vic.4.0.2S12.bin               IOM                 4.0(2S12)
ucs-m83-8p40-vic.4.0.2S17.bin               IOM                 4.0(2S17)
ucs-m83-8p40-vic.4.0.2S22.bin               IOM                 4.0(2S22)
ucs-m83-8p40-vic.4.0.2S27.bin               IOM                 4.0(2S27)
ucs-m83-8p40-vic.4.0.2S33.bin               IOM                 4.0(2S33)

UCS-A# /chassis/adapter # update firmware 4.0(2S33)
UCS-A# /chassis/adapter* # activate firmware 4.0(2S33)
UCS-A# /chassis/adapter* # commit-buffer
UCS-A# /chassis/adapter # show firmware
Adapter:
    Running-Vers: 4.0(2S33)
    Package-Vers: 2.5(0.210)M
    Update-Status: Ready
    Activate-Status: Ready
```

次の例では、共有アダプタ ファームウェアをバージョン 4.0(2S33) に更新して、更新が正常に完了したことを確認してからファームウェアアクティブ化を開始し、共有アダプタ ファームウェアをアクティブにして、ファームウェア アクティブ化が正常に完了したことを確認します。

```
UCS-A# scope chassis 1
UCS-A# /chassis # scope adapter
UCS-A# /chassis/adapter # show image
Name                                        Type                Version
------------------------------------------- ------------------- -------
ucs-m83-8p40-vic.4.0.2S12.bin               IOM                 4.0(2S12)
ucs-m83-8p40-vic.4.0.2S17.bin               IOM                 4.0(2S17)
ucs-m83-8p40-vic.4.0.2S22.bin               IOM                 4.0(2S22)
ucs-m83-8p40-vic.4.0.2S27.bin               IOM                 4.0(2S27)
ucs-m83-8p40-vic.4.0.2S33.bin               IOM                 4.0(2S33)

UCS-A# /chassis/adapter # update firmware 4.0(2S33)
UCS-A# /chassis/adapter* # commit-buffer
UCS-A# /chassis/adapter # show update status
Status: Ready
UCS-A# /chassis/adapter # activate firmware 4.0(2S33)
UCS-A# /chassis/adapter* # commit-buffer
UCS-A# /chassis/adapter # show activate status
Status: Ready
```

```
UCS-A# /chassis/adapter # show firmware
Adapter:
    Running-Vers: 4.0(2S33)
    Package-Vers: 2.5(0.210)M
    Update-Status: Ready
    Activate-Status: Ready
```

シャーシ上のストレージ コントローラ ファームウェアのアクティブ化

はじめる前に

正しい手順でサーバの電源をオフにします。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope chassis** *chassis-id*	指定したシャーシでシャーシ モードを開始します。
ステップ 2	UCS-A /chassis # **scope raid-controller** *raid-id* {**sas** | **sd** | **flash** | **sata** | **unknown**	シャーシでストレージ コントローラ モードに入ります。
ステップ 3	UCS-A /chassis/raid-controller # **activate firmware** *version-num*	シャーシ内のストレージ コントローラ上で指定されたファームウェア バージョンをアクティブにします。
ステップ 4	UCS-A /chassis/raid-controller # **commit-buffer**	トランザクションをシステムの設定にコミットします。
ステップ 5	UCS-A /chassis/raid-controller # **show activate status**	ファームウェアのアクティベーションのステータスを表示します。

次に、ストレージ コントローラ ファームウェアをアクティブにする例を示します。

```
UCS-A# scope chassis 1
UCS-A# /chassis # scope raid-controller 1 sas
UCS-A# /chassis/raid-controller # activate firmware 24.5.1.1
Warning: When committed, this command will soft shutdown the servers and reset the endpoint.
Associated servers power state will be restored after endpoint reset.
UCS-A# /chassis/raid-controller* # commit-buffer
UCS-A# /chassis/raid-controller* # show activate status
Activate-Status: Ready
```

シャーシ上のボード 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

正しい手順でサーバの電源をオフにします。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope chassis** *chassis-id*	指定したシャーシでシャーシ モードを開始します。
ステップ 2	UCS-A /chassis #**scope boardcontroller**	シャーシのボードコントローラモードに入ります。
ステップ 3	UCS-A /chassis/boardcontroller # **activate firmware** *version-num*	シャーシのボード コントローラ上で選択されたファームウェア バージョンをアクティブにします。
ステップ 4	UCS-A /chassis/boardcontroller # **commit-buffer**	トランザクションをシステムの設定にコミットします。
ステップ 5	UCS-A /chassis/boardcontroller # **show firmware**	実行中のファームウェアのバージョンとそのアクティブ化ステータスを表示します。

次に、シャーシ上のボード コントローラ ファームウェアをアクティブにする例を示します。

```
UCS-A# scope chassis 1
UCS-A /chassis # scope boardcontroller
UCS-A /chassis/boardcontroller # activate firmware 1.0.4
Warning: When committed, this command will soft shutdown the servers and may power cycle
the chassis while activating the board controller.
Associated servers power state will be restored after chassis power cycle.
UCS-A# /chassis/boardcontroller # commit-buffer
UCS-A /chassis/boardcontroller* # show firmware
Board Controller:
    Running-Vers: 1.0.4
    Package-Vers: 2.5(0.210)M
    Activate-Status: Ready
UCS-A /chassis/boardcontroller* #
```

サーバの BIOS ファームウェアの更新とアクティブ化

重要 Cisco UCS Manager CLI を使用して、サーバ上の BIOS ファームウェアを更新してアクティブにすることができます。

⚠

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *chassis-id / cartridge-id / server-id*	指定サーバのシャーシ サーバ モードを開始します。
ステップ 2	UCS-A /chassis/cartridge/server # **scope bios**	シャーシ サーバ BIOS モードを開始します。
ステップ 3	UCS-A /chassis/cartridge/server/bios # **update firmware** *version-num*	サーバの選択した BIOS ファームウェアを更新します。
ステップ 4	UCS-A /chassis/cartridge/server/bios # **commit-buffer**	（任意） トランザクションをコミットします。 このステップを使用するのは、ステップ 6 でファームウェアをアクティブにする前に、ファームウェア更新が正常に完了したことを確認するためにステップ 5 で **show firmware** コマンドを使用する場合だけです。 このステップをスキップして、同じトランザクションで **update-firmware** および activate-firmware コマンドをコミットできます。ただし、ファームウェア更新が正常に完了していない場合は、ファームウェア アクティブ化が開始されません。 Cisco UCS Manager によって、選択したファームウェア イメージがバックアップ メモリ パーティションにコピーされ、そのイメージが破損していないことが確認されます。 イメージは、明示的にアクティブにするまで、バックアップ バージョンとして残されます。
ステップ 5	UCS-A /chassis/cartridge/server/bios # **show firmware**	（任意） ファームウェアのアップデートのステータスを表示します。 ファームウェアのアップデートが正常に完了したことを確認する場合にのみ、このステップを使用します。 アッ

	コマンドまたはアクション	目的
		プデート ステータスが Ready になったら、ファームウェアのアップデートは完了です。 CLI の表示は自動的には更新されないので、タスクの状態が [Updating] から [Ready] に変わるまで何度も **show firmware** コマンドを入力する必要があります。 アップデート ステータスが Ready になったらステップ 6 に進みます。
ステップ 6	UCS-A /chassis/cartridge/server/bios # **activate firmware** *version-num*	選択したサーバ BIOS ファームウェア バージョンをアクティブにします。
ステップ 7	UCS-A /chassis/cartridge/server/bios # **commit-buffer**	トランザクションをコミットします。
ステップ 8	UCS-A /chassis/cartridge/server/bios # **show firmware**	（任意） ファームウェアのアクティベーションのステータスを表示します。 ファームウェアのアクティベーションが正常に完了したことを確認する場合にのみ、このステップを使用します。CLI の表示は自動的には更新されないので、タスクの状態が [Activating] から [Ready] に変わるまで何度も **show firmware** コマンドを入力する必要があります。

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

```
UCS-A# scope server 1/2/1
UCS-A# /chassis/cartridge/server # scope bios
UCS-A# /chassis/cartridge/server/bios # update firmware UCSME.142M4.2.0.100.52.122920140321
UCS-A# /chassis/cartridge/server/bios # activate firmware UCSME.142M4.2.0.100.52.122920140321
UCS-A# /chassis/cartridge/server/bios* # commit-buffer
```

サーバの CIMC ファームウェアのアップデートおよびアクティブ化

CIMC のファームウェアのアクティベーションによって、データ トラフィックは中断されませんが、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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *chassis-id* / *cartridge-id* / *server-id*	指定サーバのシャーシ サーバ モードを開始します。
ステップ 2	UCS-A /chassis/cartridge/server # **scope cimc**	シャーシ サーバ CIMC モードを開始します。
ステップ 3	UCS-A /chassis/cartridge/server/cimc # **show image**	アダプタの使用可能なソフトウェアイメージを表示します。
ステップ 4	UCS-A /chassis/cartridge/server/cimc # **update firmware** *version-num*	サーバの CIMC の選択したファームウェア バージョンをアップデートします。
ステップ 5	UCS-A /chassis/cartridge/server/cimc # **commit-buffer**	（任意） トランザクションをコミットします。 ステップ 7 でファームウェアをアクティブにする前に、ステップ 6 で **show firmware** コマンドを使用して、ファームウェアのアップデートが正常に完了したことを確認する場合のみこのステップを使用します。 このステップをスキップし、同じトランザクションで **update-firmware** および **activate-firmware** コマンドをコミットできます。 ただし、ファームウェアのアップデートが正常に完了していない場合、ファームウェアのアクティベーションは開始されません。 Cisco UCS Manager によって、選択したファームウェア イメージがバックアップ メモリ パーティションにコピーされ、そのイメージが破損していないことが確認されます。 イメージは、明示的にアクティブにするまで、バックアップ バージョンとして残されます。

	コマンドまたはアクション	目的
ステップ 6	UCS-A /chassis/cartridge/server/cimc # **show firmware**	（任意） ファームウェアのアップデートのステータスを表示します。 ファームウェアのアップデートが正常に完了したことを確認する場合にのみ、このステップを使用します。アップデートステータスがReadyになったら、ファームウェアのアップデートは完了です。CLIの表示は自動的には更新されないため、タスクのステータスがUpdatingからReady に変更されるまで何度も **show firmware** コマンドを入力する必要がある場合があります。アップデートステータスが Ready になったらステップ 7 に進みます。
ステップ 7	UCS-A /chassis/cartridge/server/cimc # **activate firmware** *version-num*	サーバのCIMCの選択したファームウェアバージョンをアクティブにします。
ステップ 8	UCS-A /chassis/cartridge/server/cimc # **commit-buffer**	トランザクションをコミットします。
ステップ 9	UCS-A /chassis/cartridge/server/cimc # **show firmware**	（任意） ファームウェアのアクティベーションのステータスを表示します。 ファームウェアのアクティベーションが正常に完了したことを確認する場合にのみ、このステップを使用します。CLIの表示は自動的には更新されないため、タスクのステータスが Activating から Ready に変更されるまで何度も **show firmware** コマンドを入力する必要がある場合があります。

次の例では、ファームウェア更新とファームウェア アクティブ化が正常に完了したことを確認せずに、同じトランザクションで CIMC ファームウェアをバージョン 2.0(100.46) に更新してアクティブにします。

```
UCS-A# scope server 1/2/1
UCS-A# /chassis/cartridge/server # scope cimc
UCS-A# /chassis/cartridge/server/cimc # update firmware 2.0(100.46)
UCS-A# /chassis/cartridge/server/cimc* # activate firmware 2.0(100.46)
UCS-A# /chassis/cartridge/server/cimc* # commit-buffer
UCS-A# /chassis/cartridge/server/cimc #
```

次の例では、CIMC ファームウェアをバージョン 2.0(100.46) に更新し、ファームウェア更新が正常に完了したことを確認してからファームウェア アクティブ化を開始し、CIMC ファームウェアをアクティブにして、ファームウェア アクティブ化が正常に完了したことを確認します。

```
UCS-A# scope server 1/1
UCS-A# /chassis/cartridge/server # scope cimc
UCS-A# /chassis/cartridge/server/cimc # update firmware 2.0(100.46)
UCS-A# /chassis/cartridge/server/cimc* # commit-buffer
UCS-A# /chassis/cartridge/server/cimc # show firmware
Running-Vers    Update-Status   Activate-Status
--------------- --------------- ---------------
2.0(100.46)     Updating        Ready

UCS-A# /chassis/cartridge/server/cimc # show firmware
Running-Vers    Update-Status   Activate-Status
--------------- --------------- ---------------
2.0(100.46)     Ready           Ready

UCS-A# /chassis/cartridge/server/cimc # activate firmware 2.0(100.46)
UCS-A# /chassis/cartridge/server/cimc* # commit-buffer
UCS-A# /chassis/cartridge/server/cimc # show firmware
Running-Vers    Update-Status   Activate-Status
--------------- --------------- ---------------
2.0(100.46)     Ready           Activating

UCS-A# /chassis/cartridge/server/cimc # show firmware
Running-Vers    Update-Status   Activate-Status
--------------- --------------- ---------------
2.0(100.46)     Ready           Ready
```

Cisco UCS Manager ソフトウェアのアクティブ化

手順

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

	コマンドまたはアクション	目的
		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スケジュールします。

次に、Cisco UCS Manager をバージョン 2.5(0.225) にアップグレードして、トランザクションをコミットする例を示します。

```
UCS-A# scope system
UCS-A# /system # show image
Name                                                Type              Version
--------------------------------------------------- ----------------- -----------
ucs-manager-k9.2.5.0.225.bin                        System            2.5(0.225)

UCS-A# /system # activate firmware 2.5(0.225)
UCS-A# /system* # commit-buffer
UCS-A# /system #
```

ファブリック インターコネクトでのファームウェアのアクティブ化

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

単一のファブリック インターコネクトのスタンドアロン設定の場合、エンドポイントのファームウェアの直接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

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

	コマンドまたはアクション	目的
ステップ 2	UCS-A /fabric-interconnect # **show image**	ファブリック インターコネクトの利用可能なソフトウェア イメージを表示します。
ステップ 3	UCS-A /fabric-interconnect # **activate firmware** {**kernel-version** *kernel-ver-num* | **system-version** *system-ver-num*}	ファブリック インターコネクトの選択されたファームウェア バージョンをアクティブにします。
ステップ 4	UCS-A /fabric-interconnect # **commit-buffer**	トランザクションをコミットします。 Cisco UCS Manager はファームウェアの更新とアクティベーションを実行してから、ファブリック インターコネクトと、、ファブリック インターコネクトへのデータ トラフィックを中断するすべての I/O モジュールをリブートします。

次の例では、ファブリック インターコネクトをバージョン 5.2(3)N2(2.21.92) にアップグレードし、トランザクションをコミットします。

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect # show image
Name                                          Type                  Version
--------------------------------------------- --------------------- -----------------
ucs-6100-k9-kickstart.5.2.3.N2.2.50.225.bin   Fabric Interconnect Kernel
                                                                    5.2(3)N2(2.50.225)
ucs-6100-k9-system.5.2.3.N2.2.50.225.bin      Fabric Interconnect System
                                                                    5.2(3)N2(2.50.225)

UCS-A /fabric-interconnect # activate firmware kernel-version 5.2(3)N2(2.50.224)
system-version 5.2(3)N2(2.50.224)
UCS-A /fabric-interconnect* # commit-buffer
UCS-A /fabric-interconnect #
```

第 5 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，51 ページ
- ホスト ファームウェア パッケージの作成または更新，58 ページ
- 管理ファームウェア パッケージのアップデート，61 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、ホスト ファームウェア ポリシーを定義し、サーバに関連付けられたサービス プロファイルにそれを追加することによって、サーバ上の BIOS を含むサーバ ファームウェアをアップグレードできます。

サービス プロファイルを通して、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 のファームウェアをアップグレードすることはできません。 それらのエンドポイントのファームウェアは直接アップグレードする必要があります。

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

ホスト ファームウェア パッケージ

このポリシーでは、ホスト ファームウェア パッケージ（ホスト ファームウェア パック）を構成するファームウェアバージョンのセットを指定することができます。 ホストファームウェアパッケージには、サーバ エンドポイント エンドポイント用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、エンドポイントに必要なファームウェアバージョンを認識して、それ以外のファームウェア バージョンを無視します。

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 パッケージの作成または更新

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。

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。 ルート組織モードに入るには、「/」を *org-name* として入力します。
ステップ 2	UCS-A org/ # **create fw-host-pack** *pack-name*	ホスト ファームウェア パッケージを選択したパッケージ名で作成し、組織ファームウェア ホスト パッケージ モードを開始します。
ステップ 3	UCS-A /org/fw-host-pack # **set descr** *description*	（任意） ホスト ファームウェア パッケージの説明を記入します。 （注）　説明にスペース、特殊文字、または句読点が含まれている場合、説明を引用符で括る必要があります。 引用符は、**show** コマンド出力の説明フィールドには表示されません。
ステップ 4	UCS-A org/fw-host-pack # **create pack-image** *hw-vendor-name hw-model* {**adapter** | **board-controller** | **cimc** | **graphics-card** | **host-hba** | **host-hba-optionrom** | **host-nic** | **local-disk** | **raid-controller** | **server-bios**} *version-num*	ホスト ファームウェア パッケージのパッケージ イメージを作成し、組織ファームウェア ホスト パッケージ イメージ モードを開始します。 *hw-vendor-name* は、ベンダーのフルネームと一致する必要があり、引用符で始まって引用符で終わる必要があります。 *hw-vendor-name* および *hw-model* 値は、**show image detail** コマンド入力時にパッケージ イメージの判別を容易にするラベルです。 *version-num* 値は、パッケージのイメージに使用されているファームウェアのバージョン番号を指定します。 重要　**host-hba** オプションと **host-hba-optionrom** オプションは、Cisco UCS M シリーズ サーバでサポートされていません。

	コマンドまたはアクション	目的
		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。 （注） パック項目作成に使用できるのは、CIMC ファームウェアと BIOS ファームウェアだけです。
ステップ 5	UCS-A org/fw-host-pack/pack-image # **set version** *version-num*	（任意） パッケージイメージのバージョン番号を指定します。 この番号を変更すると、サービス プロファイル経由でファームウェアを使用して、すべてのコンポーネントのファームウェア更新が実行されます。 このステップは、ホスト ファームウェア パッケージ更新時にのみ使用し、作成時には使用しません。 （注） ホストファームウェアパッケージには複数のパッケージ イメージを含めることができます。 その他のコンポーネントについて、追加パッケージイメージを作成するには、4 と 5 を繰り返します。
ステップ 6	UCS-A org/fw-host-pack/pack-image # **commit-buffer**	トランザクションをコミットします。 Cisco UCS Manager 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。

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

```
UCS-A# scope org /
UCS-A /org # create fw-host-pack app1
UCS-A /org/fw-host-pack* # set descr "This is a host firmware package example."
UCS-A /org/fw-host-pack* # create pack-image "Cisco Systems Inc" N20-AQ0102 bios
UCSME.142M4.2.0.100.52.122920140321
UCS-A /org/fw-host-pack/pack-image* # commit-buffer
UCS-A /org/fw-host-pack/pack-image #
```

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。

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。 ルート組織モードに入るには、「/」を *org-name* として入力します。
ステップ 2	UCS-A org/ # **scope fw-mgmt-pack** *pack-name*	指定したパッケージ名で管理ファームウェア パッケージを作成し、組織ファームウェア管理パッケージ モードを開始します。
ステップ 3	UCS-A /org/fw-mgmt-pack # **set descr** *description*	（任意） 管理ファームウェア パッケージの説明を記入します。 （注） 説明にスペース、特殊文字、または句読点が含まれている場合、説明を引用符で括る必要があります。 引用符は、**show** コマンド出力の説明フィールドには表示されません。
ステップ 4	UCS-A org/fw-mgmt-pack # **create pack-image** "*hw-vendor-name*" "*hw-model*" **cimc** "*version-num*"	管理ファームウェア パッケージのパッケージイメージを作成し、組織ファームウェア管理パッケージ イメージ モードを開始します。 *hw-vendor-name* および *hw-model* 値は、**show image detail** コマンド入力時にパッケージ イメージの判別を容易にするラベルです。 *version-num* 値は、パッケージのイメージに使用されているファームウェアのバージョン番号を指定します。

	コマンドまたはアクション	目的
		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。
ステップ 5	UCS-A org/fw-mgmt-pack/pack-image # **set version** *version-num*	（任意） パッケージイメージのバージョン番号を指定します。 この番号を変更すると、サービスプロファイル経由でファームウェアを使用して、すべてのコンポーネントのファームウェア更新が実行されます。 このステップは、ファームウェア パッケージ更新時にのみ使用し、作成時には使用しません。
ステップ 6	UCS-A org/fw-mgmt-pack/pack-image # **commit-buffer**	トランザクションをコミットします。 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。

次に、cimc1 ホスト ファームウェア パッケージを更新して、バージョン 1.0(0.988) のファームウェアを持つ CIMC パッケージ イメージを作成し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # scope fw-mgmt-pack cimc1
UCS-A /org/fw-mgmt-pack* # set descr "This is a management firmware package example."
UCS-A /org/fw-mgmt-pack* # create pack-image "Cisco Systems Inc" "SB-1600-CTRL" cimc
"2.3(200.166)"
UCS-A /org/fw-mgmt-pack/pack-image* # commit-buffer
UCS-A /org/fw-mgmt-pack/pack-image #
```

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。

第 6 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，63 ページ
- 個別の機能カタログ更新のダウンロード，65 ページ
- 機能カタログが最新であることの確認，67 ページ
- M シリーズの機能カタログ更新のアクティブ化，67 ページ
- 機能カタログ更新のリスタート，68 ページ
- 機能カタログ プロバイダーの表示，69 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 コンポーネントで分割されます。 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 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。

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。

手順

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

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

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

```
UCS-A# scope system
UCS-A /system # scope capability
UCS-A /system/capability # update catalog
scp://user1@192.0.2.111/catalogs/ucs-catalog.2.5.0.233.T.bin
Warning: This command is deprecated and will be removed in a future release. Replaced by:
activate catalog
Password:
UCS-A /system/capability # show version
Catalog:
    Running-Vers: 2.5(0.233)T
    Package-Vers:
    Activate-Status: Ready

UCS-A /system/capability # show cat-updater ucs-catalog.2.5.0.233.T.bin

Catalog Updater:
    File Name Protocol Server          Userid          Status
```

```
    --------- -------- --------------- --------------- ------
    ucs-catalog.2.5.0.233.T.bin
              Scp      192.0.2.111     user1           Success
UCS-A /system/capability #
```

機能カタログが最新であることの確認

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope capability**	システム機能モードを開始します。
ステップ 3	UCS-A /system/capability # **show version**	現在の機能カタログのバージョンを表示します。
ステップ 4	Cisco.com で、入手可能な機能カタログの最新リリースを確認します。	機能カタログのアップデートの場所については、シスコからの機能カタログのアップデートの入手方法, （65 ページ）を参照してください。
ステップ 5	より新しいバージョンの機能カタログを Cisco.com で入手できる場合は、そのバージョンを使用して機能カタログをアップデートします。	

次に、現在の機能カタログのバージョンを表示する例を示します。

```
UCS-A# scope system
UCS-A /system # scope capability
UCS-A /system/capability # show version
Catalog:
    Running-Vers: 1.0(8.35)
    2.5(0.233)
    Activate-Status: Ready
UCS-A /system/capability #
```

M シリーズの機能カタログ更新のアクティブ化

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。

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

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

```
UCS-A# scope system
UCS-A /system # scope capability
UCS-A /system/capability # activate firmware 2.5(0.233)
UCS-A /system/capability* # commit-buffer
UCS-A /system/capability #
```

機能カタログ更新のリスタート

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

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム コマンド モードを開始します。
ステップ 2	UCS-A /system # **scope capability**	機能コマンド モードを開始します。
ステップ 3	UCS-A /system/capability # **show cat-updater** [*filename*]	（オプション）機能カタログ ファイルのアップデート操作の更新履歴を表示します。
ステップ 4	UCS-A /system/capability # **scope cat-updater** *filename*	機能カタログ ファイルのアップデート操作のコマンド モードを開始します。
ステップ 5	UCS-A /system/capability/cat-updater # **set userid** *username*	（オプション）リモート サーバのユーザ名を指定します。
ステップ 6	UCS-A /system/capability/cat-updater # **set password** *password*	（オプション）リモート サーバのユーザ名のパスワードを指定します。 パスワードが設定されていない場合、アップデートを開始するときに、パスワードの入力を求められます。

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

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

```
UCS-A# scope system
UCS-A /system # scope capability
UCS-A /system/capability # show cat-updater ucs-catalog.1.0.0.4.binshow cat-updater
ucs-catalog.2.5.0.233.T.bin

Catalog Updater:
    File Name                Protocol Server          Userid          Status
    ---------                -------- --------------- --------------- ------
    ucs-catalog.1.0.0.4.binucs-catalog.2.5.0.233.T.bin   Scp      192.0.2.111     user1
        Applied

UCS-A /system/capability # scope cat-updater ucs-catalog.1.0.0.4.binscope cat-updater
ucs-catalog.2.5.0.233.T.bin
UCS-A /system/capability/cat-updater # set server 192.0.2.112
UCS-A /system/capability/cat-updater # restart
UCS-A /system/capability/cat-updater #
```

機能カタログ プロバイダーの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム コマンド モードを開始します。

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

（注） ハード ディスク ドライブやソリッド ステート ドライブなど、1 つ以上の SATA デバイスがサーバに含まれる場合、**show disk** コマンドにより [Vendor] フィールドに ATA が表示されます。 ベンダーの追加情報を表示するには、 **expand** キーワードを使用します。

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

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

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

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

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

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

    Form Factor:
        Depth (C): 6.700000
```

```
        Height (C): 1.600000
        Width (C): 4.900000
        Weight (C): 1.500000

UCS-A /system/capability #
```

第 7 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, 73 ページ
- 管理拡張機能のアクティブ化, 73 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

管理拡張機能は、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。 管理拡張機能を個別にダウンロードする必要はありません。

管理拡張バージョンを確認するには、**show version** コマンドを発行します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **scope management-extension**	システムの管理拡張モードを開始します。
ステップ 3	UCS-A /system/management-extension # **activate firmware** *firmware-version* **[force-activation]**	指定した管理拡張機能をアクティブにします。 互換性のない可能性や、現在実行中のタスクに関係なく、ファームウェアをアクティブにするには、**force-activation** キーワードを使用します。
ステップ 4	UCS-A /system/management-extension # **commit-buffer**	トランザクションをシステムの設定にコミットします。

次の例では、管理拡張機能をアクティブにし、トランザクションをコミットします。

```
UCS-A# scope system
UCS-A /system # scope management-extension
UCS-A /system/management-extension # activate firmware 2.5(0.136)
CS-A /system/management-extension* # commit-buffer
```