Cisco UCS Release 1.4(1)/1.4(2) から Release 1.4(3) へのアップグレード

初版：2011 年 06 月 23 日

最終更新：2012 年 02 月 20 日

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

Text Part Number: OL-25310-04-J

【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。

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)

このマニュアルで使用している IP アドレスは、実際のアドレス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、および図は、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。

© 2013 Cisco Systems, Inc. All rights reserved.

目 次

はじめに vii

対象読者 vii

マニュアルの構成 vii

表記法 viii

関連資料 ix

マニュアルに関するフィードバック ix

マニュアルの入手方法およびテクニカル サポート ix

Release 1.4(3) へのアップグレードの概要 1

ファームウェアの概要 1

ファームウェア イメージの管理 2

ファームウェア バージョン 4

Cisco UCS Release 1.4 へのファームウェア アップグレード 5

Release 1.4(1) または 1.4(2) からのアップグレード時に必要な手順 5

Cisco UCS B230 サーバの追加に必要な手順 7

Cisco UCS ラックマウント サーバの統合に必要な手順 7

アップグレードの注意、注意事項、およびベスト プラクティス： Cisco UCS 8

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 8

ファームウェア アップグレードに関するハードウェア関連の注意事項とベスト プラクティス 9

アップグレードに関するファームウェア関連およびソフトウェア関連のベスト プラクティス 11

直接のファームウェア アップグレードの停止の影響 12

ファームウェアのアップグレードの前提条件の実行 15

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 15

すべてのコンフィギュレーション バックアップ ファイルの作成 16

ファブリック インターコネクトの全体のステータスの確認 18

クラスタ設定の高可用性ステータスとロールの確認 18
I/O モジュールのステータスの確認 19
サーバのステータスの確認 20
シャーシのサーバのアダプタのステータスの確認 21
Release 1.4 ファームウェアのダウンロード 23
シスコからのソフトウェア バンドルの取得 23
ファブリック インターコネクトへのファームウェア パッケージのダウンロード 25
ファームウェア パッケージの内容の判断 27
イメージ ダウンロードのキャンセル 27
ファブリック インターコネクトのローカル記憶域のチェック 28
ファブリック インターコネクトの空き領域のチェック 28
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 28
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 29
Release 1.4(3) へのファームウェアのアップグレード 31
Release 1.4(1) または 1.4(2) からのアップグレード時に必要な手順 31
Call Home のディセーブル化 33
アダプタ、CIMC、IOM でのファームウェアのアップデート 33
アダプタおよび CIMC でのファームウェアのアクティブ化 35
サーバのボード コントローラ ファームウェアのアクティブ化 37
Cisco UCS Manager ソフトウェアの Release 1.4 へのアクティブ化 38
IOM のファームウェアの Release 1.4 へのアクティブ化 38
クラスタ設定のファブリック インターコネクト ファームウェアのアクティブ化 40
下位ファブリック インターコネクトのファームウェアの Release 1.4 へのアクティブ化 40
データ パスの準備が整っていることの確認 41
ダイナミック vNIC が稼働中であることの確認 41
イーサネット データ パスの確認 42
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 42
ファイバ チャネル スイッチ モードのデータ パスの確認 43
プライマリ ファブリック インターコネクトのファームウェアの Release 1.4 へのアクティブ化 44

スタンドアロン ファブリック インターコネクトのファームウェアの Release 1.4 へのアクティブ化 45
ホストおよび管理ファームウェア パッケージのアップデート 46
ホスト ファームウェア パッケージおよび管理ファームウェア パッケージへのアップデートの影響 46
管理ファームウェア パッケージのアップデート 50
ホスト ファームウェア パッケージのアップデート 51
Call Home のイネーブル化 53

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
- マニュアルの構成，vii ページ
- 表記法，viii ページ
- 関連資料，ix ページ
- マニュアルに関するフィードバック，ix ページ
- マニュアルの入手方法およびテクニカル サポート，ix ページ

対象読者

このガイドは、主に既存の Cisco Unified Computing System（Cisco UCS）インスタンスをアップグレードする必要があるユーザを対象にしています。

マニュアルの構成

このマニュアルの構成は、次のとおりです。

章	タイトル	説明
第 1 章	概要	UCS Manager GUI を使用して、Cisco UCS を、指定したリリースにアップグレードする概要を説明します。開始する前に知っておく必要があるアップグレード手順やその他の情報などが含まれます。
第 2 章	前提条件の実行	アップグレードの前提条件について説明します。

章	タイトル	説明
第 3 章	ファームウェアのダウンロード	アップグレードに必要なファームウェアがある場所と、それを Cisco UCS Manager にダウンロードする方法について説明します。
第 4 章	ファームウェアのアップグレード	アップグレードを実行するために必要な順序で従う必要がある手順について説明します。

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	用途
bold フォント	コマンド、キーワード、およびユーザが入力したテキストは、**bold** フォントで示しています。
italic フォント	ドキュメント名、新規用語または強調する用語、値を指定するための引数は、*italic* フォントで示しています。
`courier` フォント	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。
[ ]	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。

ヒント 「問題解決に役立つ情報」です。

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 「警告」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。

関連資料

Cisco Unified Computing System（Cisco UCS）B シリーズ ハードウェアおよびソフトウェアに関するすべてのマニュアルを一覧にしたロードマップは、次の URL から入手できます。

http://www.cisco.com/go/unifiedcomputing/b-series-doc

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。 ご協力をよろしくお願いいたします。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカルサポート、その他の有用な情報について、次のURLで、毎月更新される『What's New in Cisco Product Documentation』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。 RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

ドキュメントのアップデート通知を受け取るには、Twitter で Cisco UCS Docs をフォローしてください。

第 1 章

Release 1.4(3) へのアップグレードの概要

この章の内容は、次のとおりです。

- ファームウェアの概要，1 ページ
- ファームウェア イメージの管理，2 ページ
- ファームウェア バージョン，4 ページ
- Cisco UCS Release 1.4 へのファームウェア アップグレード，5 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 インスタンス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、ファームウェアが機能するために必要なインスタンスのコンポーネントです。 Cisco UCS インスタンスのエンドポイントのアップグレード順序は、アップグレード パスによって異なります。次の項目が含まれます。

- Cisco UCS Manager
- I/O モジュール
- ファブリック インターコネクト
- NIC や HBA ファームウェア、サービス プロファイルに含まれているファームウェア パッケージを使用してアップグレードできるオプション ROM（該当する場合）など、アダプタ上に物理的に存在するエンドポイント
- サービス プロファイルに含まれているファームウェア パッケージを使用してアップグレードできる BIOS、ストレージ コントローラ（RAID コントローラ）、Cisco Integrated Management Controller（CIMC）など、サーバ上に物理的に存在するエンドポイント

Cisco UCS インスタンスのエンドポイントをアップグレードする適切な順序を確認するには、アップグレード パスに必要な手順の順序を参照してください。

（注） Cisco UCS Release 1.4(1) 以降では、シスコは 1 つの大きなファームウェア パッケージではなく、複数のバンドルでファームウェア アップグレードをリリースしています。 詳細については、ファームウェア イメージの管理, （2 ページ）を参照してください。

シスコでは、このマニュアルおよびテクニカル ノート『Unified Computing System Firmware Management Best Practices』において、ファームウェア イメージおよびファームウェア アップデートを管理するための一連のベスト プラクティスを保持しています。

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

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。

（注） ファームウェア管理および個別のコンポーネントのアップグレードの詳細については、Cisco UCS Manager コンフィギュレーション ガイドを参照してください。

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、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
- I/O モジュールのファームウェア

Cisco UCS B シリーズ ブレード サーバ ソフトウェア バンドル

このバンドルには、Cisco UCS インスタンスのブレード サーバのファームウェアをアップデートするために必要な次のファームウェア イメージが含まれます。 Cisco UCS Manager で最新のインフラストラクチャ バンドルに含まれていないブレード サーバがサポートされるように、リリースに対して作成されたバンドル以外に次のバンドルもインフラストラクチャ バンドル間でリリースできます。

- CIMC ファームウェア
- BIOS ファームウェア
- アダプタ ファームウェア
- ボード コントローラ ファームウェア
- 新規サーバで必要なサードパーティ製のファームウェア イメージ

Cisco UCS C シリーズ ラックマウント サーバ ソフトウェア バンドル

このバンドルには、Cisco UCS Manager に統合され、Cisco UCS Manager によって管理されるラックマウント サーバのコンポーネントのアップデートに必要な次のファームウェアイメージが含まれます。

- CIMC ファームウェア
- BIOS ファームウェア
- アダプタ ファームウェア
- ストレージ コントローラのファームウェア

（注） このバンドルは、スタンドアロン C シリーズ サーバには使用できません。 このサーバのファームウェア管理システムでは、Cisco UCS Manager に必要なヘッダーを解釈できません。 スタンドアロン C シリーズ サーバのアップグレード方法については、C シリーズのコンフィギュレーション ガイドを参照してください。

また、シスコではリリース ノートも提供しており、バンドルを取得したのと同じ Web サイトから入手できます。

ファームウェア バージョン

エンドポイントのファームウェア バージョンはエンドポイントのタイプによって異なります。ファブリック インターコネクトに物理的に存在するエンドポイントのバージョンは、サーバまたは I/O モジュールに物理的の存在するバージョンと異なります。

CIMC、I/O モジュール、アダプタのファームウェア バージョン

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

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

実行されているバージョン

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

スタートアップ バージョン

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

バックアップ バージョン

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

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

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

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

ト可能ファブリック インターコネクト イメージは、ファブリック インターコネクトのメモリの空き領域と、そこに保存されるイメージの数によって制限されます。

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

Cisco UCS Release 1.4 へのファームウェア アップグレード

Cisco UCS Release 1.4(2) から Release 1.4(3) へのファームウェア アップグレードは、エンドポイントをアクティブ化し、更新されたホスト ファームウェア パッケージが適用された後にサーバがリブートするために、最大 1 分間のデータの中断に対応する必要がある場合、予定されたメンテナンス ウィンドウで計画する必要があります。

このファームウェアのアップグレードでは、次の方法を組み合わせる必要があります。

- エンドポイントでの直接のアップグレード。 2 つのファブリック インターコネクトによるクラスタ設定の場合、直接のアップグレードによって、データ トラフィックの中断を最小限にすることができます。 ただし、Cisco UCS インスタンスに、直接アップグレードするエンドポイントのファームウェア ポリシーをインクルードしないようにします。 ファブリック インターコネクトが 1 つだけの Cisco UCS インスタンスでは、トラフィックの中断が避けられません。
- ホスト ファームウェア パッケージまたは管理ファームウェア パッケージ、またはその両方を含むサービス プロファイルによって、サーバ エンドポイントをアップグレードします。 この方法はデータ トラフィックを中断させるため、メンテナンス ウィンドウ時に実行する必要があります。

（注） 直接のアップグレードは、サーバ BIOS、ストレージ コントローラ、HBA ファームウェア、HBA オプション ROM 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。

Release 1.4(1) または 1.4(2) からのアップグレード時に必要な手順

（注） この順序に従わないと、ファームウェアのアップグレードが失敗し、サーバで Cisco UCS Manager の通信に問題が発生することがあります。

このマニュアルの手順と推奨されるオプションによって、データ トラフィックの中断を最小限にします。 そのため、Release 1.4 のいずれかのバージョンから Release 1.4 のそれよりも新しいバージョンにアップグレードする場合は、次の順序でコンポーネントをアップグレードします。

1. 次のファームウェア イメージをダウンロードします。
   - Cisco UCS インフラストラクチャ ソフトウェア バンドル：すべての Cisco UCS インスタンスに必要です。
   - Cisco UCS B シリーズ ブレード サーバ ソフトウェア バンドル：ブレード サーバを含むすべての Cisco UCS インスタンスに必要です。
   - Cisco UCS C シリーズ ラックマウント サーバ ソフトウェア バンドル：統合ラックマウント サーバを含む Cisco UCS インスタンスのみに必要です。 このバンドルには、Cisco UCS Manager でこれらのサーバを管理できるようにするファームウェアが含まれます。標準の C シリーズ ラックマウント サーバには適用されません。
2. （任意）Call Home をディセーブルにする：Cisco UCS インスタンスに Call Home または Smart Call Home が含まれている場合、Call Home をディセーブルにして、Cisco UCS Manager がコンポーネントを再始動したときに不要な警告を受け取らないようにします。
3. アダプタ、CIMC、および IOM を更新する：必要に応じて、ホスト ファームウェア パッケージ内のアダプタを最後の更新手順の一部としてアップグレードできます。
4. アダプタをアクティブ化する：この手順を実行するときは、[Ignore Compatibility Check] と [Set Startup Version Only] を選択します。
5. CIMC をアクティブ化する：この手順を実行するときは、[Ignore Compatibility Check] を選択します。
6. Cisco UCS Manager をアクティブ化する：この手順を実行するときは、[Ignore Compatibility Check] を選択します。
7. I/O モジュールをアクティブ化する：この手順を実行するときは、[Ignore Compatibility Check] と [Set Startup Version Only] を選択します。
8. 従属ファブリック インターコネクトをアクティブ化する：この手順を実行するときは、[Ignore Compatibility Check] を選択します。
9. データ パスが復元されたことを確認します。
10. 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：この手順を実行するときは、[Ignore Compatibility Check] を選択します。
11. サーバの管理ファームウェア パッケージを更新する：サーバで CIMC を直接更新およびアクティブ化した場合、この手順を実行する必要はありません。
12. サーバのホスト ファームウェア パッケージを更新する：アップグレードされた最後のファームウェアがある必要があります。 そのファームウェアを持つサーバがさらにリブートされるのを避けるため、この手順の間に、ボード コントローラ ファームウェアをアップグレードすることをお勧めします。 ホスト ファームウェア パッケージ内の次のファームウェアをアップグレードする必要があります。

- BIOS
- ストレージ コントローラ
- 一部のアダプタ

13 （任意）Call Home をイネーブルにする：ファームウェアをアップグレードする前に Call Home をディセーブルにしていた場合、それをイネーブルにします。

Cisco UCS B230 サーバの追加に必要な手順

最初の B230 サーバを追加するとき、Cisco UCS Manager でサーバのサポートを追加するために、次の順序で手順を実行する必要があります。

1 まだ実行していない場合は、Cisco UCS インスタンスを Release 1.4(1) 以降にアップグレードします。

2 サーバのインストレーション ガイドの説明に従って、シャーシにブレード サーバを挿入します。

3 Cisco UCS Manager が新しいサーバを検出するのを待ちます。 数分以内にサーバの検出が開始されない場合は、サーバを確認します。

（注） B230 サーバを追加するために、Management Extension または機能カタログを更新する必要はありません。 必要なサポートは、それぞれの Cisco UCS Release 1.4 インフラストラクチャ バンドルに含まれています。

Cisco UCS ラックマウント サーバの統合に必要な手順

既存のコ Cisco UCS ンポーネントのアップグレードが完了した後、Cisco UCS ラックマウント サーバを統合できます。 ラックマウント サーバを統合するときは、次の順序で手順を実行する必要があります。

1 Cisco UCS Manager でラック サーバ ディスカバリ ポリシーを設定していない場合は、設定を行います。

2 Cisco UCS Manager によって管理されるシステムでのラックマウント サーバのインストールおよび統合については、サーバ インストレーション ガイドの手順に従います。

3 Cisco UCS Manager が新しいサーバを検出するのを待ちます。 数分以内にサーバの検出が開始されない場合は、サーバを確認します。

アップグレードの注意、注意事項、およびベストプラクティス：Cisco UCS

Cisco UCS インスタンスの任意のエンドポイントのファームウェアをアップデートする前に、次の注意、注意事項、およびベスト プラクティスを考慮してください。

設定の変更とアップグレードに影響を与える可能性がある設定

Cisco UCS インスタンスの設定に応じて、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。

vNIC フェールオーバーと NIC チーミングの両方がイネーブルになっている場合、アップグレード時にすべての接続が失われる可能性がある

ホスト オペレーティング システム レベルで、1 つ以上の vNIC で [Enable Failover] を設定し、同時にNICチーミング/ボンディングを設定した場合は、ファームウェアのアップグレード時にすべての接続が失われる可能性があります。 いずれかの方法を使用して可用性を設計します。 両方は使用しないでください。

Cisco UCS インスタンスの 1 つ以上の vNIC に対してフェールオーバーをイネーブルにしているかどうかを確認するには、サーバに関連付けられている各サービス プロファイル内で vNIC の設定を確認します。 詳細については、実行しているリリースの Cisco UCS Manager コンフィギュレーション ガイドを参照してください。

VLAN 4048 はリリース 1.4(1) 以降のために予約されている

リリース 1.4(1) 以降では、VLAN 4048 は予約済み VLAN です。 Cisco UCS インスタンスが VLAN 4048 を使用するように設定されている場合、異なる ID を使用するようにこの VLAN を再設定してからアップグレードする必要があります。

Release 1.3(1i) またはそれ以降へのアップグレードによる影響

古い Cisco UCS ファームウェア リリースを Release 1.3(1i) 以降にアップグレードすると、アップグレード後にサーバが初めてサーバプロファイルに関連付けられるとき、ローカルディスク設定ポリシーの Protect Configuration プロパティに次の影響が生じます。

関連付けられていないサーバ

Cisco UCS インスタンスをアップグレードすると、ローカルディスク設定ポリシーがサーバハードウェアと一致するかどうかに関係なく、初期サーバ アソシエーションは設定エラーを生じずに処理が進められます。 Protect Configuration プロパティをイネーブルにしていても、前のサービス プロファイルと新しいサービス プロファイルの間でローカル ディスク設定ポリシーの設定に不一致がある場合、Cisco UCS はサーバ上のユーザ データを保護しません。

（注） Protect Configuration プロパティをイネーブルにした場合、前のサービス プロファイルと新しいサービス プロファイルの間でローカル ディスク設定ポリシーに不一致があると、サーバに対する後続のサービス プロファイル アソシエーションはすべてブロックされます。

関連付けられたサーバ

サービス プロファイルと関連付けられているすべてのサーバは、アップグレード後にリブートしません。 Cisco UCS Managerは、ローカルディスク設定ポリシーとサーバ ハードウェアに不一致があっても、設定エラーを報告しません。

サービス プロファイルがサーバから関連付けを解除され、新しいサービス プロファイルが関連付けられると、新しいサービス プロファイルの Protect Configuration プロパティが優先され、前のサービス プロファイルの設定は上書きされます。

ファームウェアアップグレードに関するハードウェア関連の注意事項とベストプラクティス

Cisco UCS インスタンスのハードウェアはアップグレード方法に影響を与えることがあります。エンドポイントをアップグレードする前に、次の注意事項およびベスト プラクティスを考慮してください。

サーバまたはシャーシのメンテナンスなし

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

アップグレード前に RAID 構成ハード ディスクを交換しない

次の状況では、サービス ファームウェアのアップグレード時に、Cisco UCS Manager によって RAID 同期プロセスの一環としてハード ディスクのすべてのデータにスクラビング処理が行われることがあります。

- サーバのハード ディスクが RAID 用に構成されている。
- サーバの 1 つ以上の RAID 構成ハード ディスクが取り外されている。
- ハード ディスクまたはディスクが既存の RAID で構成されたハード ディスクと交換されたが、このハード ディスクの構成に、サーバのサービス プロファイルに含まれているローカル ディスク構成ポリシーが使用されていない。
- サーバ ファームウェアがアップグレードされたため、サーバがリブートされ、Cisco UCS Manager で RAID 同期プロセスが開始される。

元のハード ディスクに、保持する必要がある重要なデータが含まれている場合は、RAID 用にすでに構成されている新しいハード ディスクを挿入しないでください。

常にホスト ファームウェア パッケージを使用して Cisco UCS Gen-2 アダプタをアップグレードする

Cisco UCS Gen-2 アダプタは、エンドポイントで直接アップグレードすることはできません。 このようなアダプタのファームウェアは、ホスト ファームウェア パッケージを使用してアップグレードする必要があります。

アップグレード不可： Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter

Intel ベースのアダプタ カードである Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter（N20-AI0002）のファームウェアは、製造元でハードウェアに書き込まれます。 このアダプタのファームウェアはアップグレードできません。

ファブリック インターコネクト数

2 つのファブリック インターコネクトのあるクラスタ設定の場合、ファブリック インターコネクト間のフェールオーバーを利用して、データ トラフィックを中断せずに、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できます。 ただし、ホストまたは管理ファームウェア パッケージによってアップグレードする必要があるエンドポイントの場合は、データ トラフィックの中断が避けられません。

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

アップグレードに関するファームウェア関連およびソフトウェア関連のベスト プラクティス

エンドポイントをアップグレードする前に、次の注意事項およびベスト プラクティスを考慮してください。

部分アップグレードなし

Cisco UCS インスタンスのすべてのエンドポイントを、同じファームウェア リリースにアップグレードすることをお勧めします。 あるエンドポイントのファームウェア リリース内の新しい機能および変更は、別のエンドポイント内の同じ機能および変更と依存関係があることがあります。 そのため、ファームウェア リリースを混在させると、通常の使用時に、パフォーマンスの問題やその他の問題を引き起こしたり、アップデートが失敗したりする可能性があります。

各エンドポイントの適切なタイプのファームウェア アップグレードの決定

アダプタやサーバ CIMC などの一部のエンドポイントは、直接のファームウェア アップグレードか、またはサービスプロファイルに含まれるファームウェアパッケージによって、アップグレードできます。 Cisco UCS インスタンスの設定によって、これらのエンドポイントのアップグレード方法が決まります。 サーバに関連付けられているサービス プロファイルに、ホスト ファームウェアパッケージが含まれる場合、ファームウェアパッケージによって、それらのサーバのアダプタをアップグレードします。 同様に、サーバに関連付けられているサービスプロファイルに管理ファームウェア パッケージが含まれる場合、ファームウェア パッケージによって、それらのサーバの CIMC をアップグレードします。

管理ファームウェア パッケージによる CIMC のアップグレードまたは、サーバに関連付けられたサービスプロファイル内のファームウェアパッケージによるアダプタのアップグレードは、直接のファームウェアアップグレードより優先されます。 サーバに関連付けられたサービスプロファイルにファームウェア パッケージが含まれる場合、エンドポイントを直接アップグレードすることはできません。 直接のアップグレードを実行するには、サービス プロファイルからファームウェア パッケージを削除する必要があります。

すべてのエンドポイントを同時にアクティブにしない Cisco UCS Manager GUI

Cisco UCS Manager GUI を使用して、ファームウェアをアップデートする場合、[Activate Firmware] ダイアログボックスの [Filter] ドロップダウン リストで [ALL] を選択して、すべてのエンドポイントを同時にアクティブにしないでください。 多くのファームウェア リリースやパッチには依存関係があるため、ファームウェアの更新を正常に実行するためにエンドポイントを特定の順序でアクティブにする必要があります。 この順序はリリースやパッチの内容によって異なります。 すべてのエンドポイントをアクティブにすると、必要な順序でアップデートが行われることが保証されず、エンドポイント、ファブリック インターコネクト、および Cisco UCS Manager 間の通信が中断することがあります。 特定のリリースやパッチの依存関係については、当該のリリースやパッチに付属のリリース ノートを参照してください。

アダプタおよび I/O モジュールのアクティベーションの影響

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

サーバがサービス プロファイルに関連付けられていない場合、アクティブ化されたファームウェアは pending-next-boot 状態のままになります。 Cisco UCS Manager は、サーバがサービス プロファイルに関連付けられるまで、エンドポイントをリブートせず、ファームウェアをアクティブにしません。 必要に応じて、関連付けられていないサーバを手動でリブートまたはリセットして、ファームウェアをアクティブにできます。

I/O モジュールに対して [Set Startup Version Only] を設定した場合、そのデータ パス内のファブリック インターコネクトがリブートされると、I/O モジュールがリブートされます。 I/O モジュールに対して、[Set Startup Version Only] を設定しない場合、I/O モジュールがリブートし、トラフィックが中断します。 また、Cisco UCS Manager が、ファブリック インターコネクトと I/O モジュールとの間でプロトコルとファームウェア バージョンが一致しないことを検出した場合、Cisco UCS Manager は I/O モジュールをファブリック インターコネクトのファームウェアと同じバージョンに自動的にアップデートし、ファームウェアをアクティブにして I/O モジュールを再度リブートします。

アップグレード時の [Ignore Compatibility Check] の選択

より新しいリリースに直接アップグレードするときは、[Ignore Compatibility Check] を選択することを推奨します。 より新しいリリースには、旧リリースとの互換性がないコードが含まれている場合があります。 このオプションによって、アップグレードが実行され、互換性の問題が回避されます。

不要なアラートを回避するためのアップグレード前の Call Home のディセーブル化（任意）

Cisco UCS インスタンスをアップグレードすると、Cisco UCS Manager によってコンポーネントが再起動され、アップグレードプロセスが完了します。 この再起動によって、サービスの中断およびコンポーネントの障害と同じイベントが発生し、Call Home アラートの送信がトリガーされます。 アップグレードの開始前に Call Home をディセーブルにしない場合は、アップグレードに関連したコンポーネントの再起動によって生成されるアラートを無視してください。

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 インスタンスで、1 つ以上のエンドポイントでトラフィックの中断や、停止が発生することがあります。

ファブリック インターコネクト ファームウェア アップグレードの停止の影響

ファブリック インターコネクトのファームウェアをアップグレードする場合、次の停止の影響や中断が発生します。

- ファブリック インターコネクトがリブートします。
- 対応する I/O モジュールがリブートします。

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

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

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

  実行中の保存されていない作業が失われます。
- Cisco UCS Manager CLI：telnet によってログインしているすべてのユーザがログアウトされ、それらのセッションが終了します。 コンソール セッションは終了しません。

I/O モジュール ファームウェア アップグレードの停止の影響

I/O モジュールのファームウェアをアップグレードする場合、次の停止の影響と中断が発生します。

- 単一のファブリック インターコネクトのスタンドアロン設定の場合、I/O モジュールのリブート時にデータ トラフィックが中断されます。 2 つのファブリック インターコネクトのクラスタ設定の場合、データ トラフィックは他方の I/O モジュールおよびそのデータ パス内のファブリック インターコネクトにフェールオーバーします。
- 新しいファームウェアをスタートアップ バージョンとしてのみアクティブにした場合、対応するファブリック インターコネクトがリブートされると、I/O モジュールがリブートします。
- 新しいファームウェアを実行されているバージョンおよびスタートアップ バージョンとしてアクティブにした場合、I/O モジュールがただちにリブートします。
- ファームウェアのアップグレード後に、I/O モジュールを使用できるようになるまで最大 10 分かかります。

CIMC ファームウェア アップグレードの停止の影響

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

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

アダプタ ファームウェア アップグレードの停止の影響

アダプタのファームウェアをアクティブにし、[Set Startup Version Only] オプションを設定していない場合、次の停止の影響と中断が発生します。

- サーバがリブートします。

- サーバ トラフィックが中断します。

第 2 章

ファームウェアのアップグレードの前提条件の実行

この章の内容は、次のとおりです。

- ファームウェアのアップグレードとダウングレードの前提条件，15 ページ
- すべてのコンフィギュレーション バックアップ ファイルの作成，16 ページ
- ファブリック インターコネクトの全体のステータスの確認，18 ページ
- クラスタ設定の高可用性ステータスとロールの確認，18 ページ
- I/O モジュールのステータスの確認，19 ページ
- サーバのステータスの確認，20 ページ
- シャーシのサーバのアダプタのステータスの確認，21 ページ

ファームウェアのアップグレードとダウングレードの前提条件

Cisco UCS インスタンスのすべてのエンドポイントが完全に機能し、それらのエンドポイントのファームウェアのアップグレードまたはダウングレードを開始する前に、すべてのプロセスが完了している必要があります。 機能状態でないエンドポイントはアップグレードまたはダウングレードすることはできません。 たとえば、検出されていないサーバのファームウェアはアップグレードまたはダウングレードできません。 最大回数の再試行後に失敗した FSM などの未完了のプロセスによって、エンドポイントのアップグレードやダウングレードが失敗する可能性があります。 FSM が実行中の場合、Cisco UCS Manager によって、アップデートとアクティベーションがキューに入れられ、FSM が正常に完了すると、それらが実行されます。

Cisco UCS インスタンスのファームウェアをアップグレードまたはダウングレードする前に、次の前提条件を実行します。

- リリース ノートの内容を確認します。
- 設定を All Configuration バックアップ ファイルにバックアップします。
- クラスタ設定の場合、ファブリック インターコネクトの高可用性ステータスに、両方が稼働中であると示されていることを確認します。
- スタンドアロン設定の場合、ファブリック インターコネクトの [Overall Status] が [Operable] であることを確認します。
- すべてのサーバ、I/O モジュール、アダプタが完全に機能することを確認します。 動作不能なサーバはアップグレードできません。
- Cisco UCS インスタンスに致命的または重大な障害がないことを確認します。 このような障害がある場合は解決してから、システムをアップグレードしてください。 致命的または重大な障害があると、アップグレードが失敗する可能性があります。
- すべてのサーバが検出されていることを確認します。 サーバの電源を入れる必要はありません。また、サーバをサービス プロファイルと関連付ける必要もありません。

すべてのコンフィギュレーションバックアップファイルの作成

この手順は、All Configuration バックアップ ファイルの既存のバックアップ操作がないことを前提としています。

Cisco UCS インスタンスのバックアップの詳細については、『*Cisco UCS Manager GUI Configuration Guide*』および『*Cisco UCS Manager CLI Configuration Guide*』を参照してください。

はじめる前に

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

手順

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

ステップ 2 [All] ノードをクリックします。

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

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

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

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

a) 次のフィールドに入力します。

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

- [Type] フィールド：[All Configuration] オプション ボタンをクリックすると、すべてのシステムおよび論理設定情報を含む XML バックアップ ファイルが作成されます。
- [Preserve Identities] チェックボックス：Cisco UCS インスタンスに、プールから取得され、保存する必要がある ID が含まれる場合、このチェックボックスをオンにします。

  MAC アドレス、WWNN、WWPN、UUIDS などの ID は実行時に割り当てられます。 バックアップ ファイルのインポート後に、これらの ID を変更しない場合は、このチェックボックスをオンにする必要があります。 このチェックボックスをオンにしない場合、インポートおよび PXE ブートや SAN ブートなどの操作が機能しなくなると、これらの ID が変更されることがあります。
- [Protocol] フィールド：ファイルをバックアップ サーバに転送するために使用するプロトコルを指示する場合に、次のいずれかのオプション ボタンをクリックします。
  - FTP
  - TFTP
  - SCP
  - SFTP
- [Hostname] フィールド：バックアップ ファイルを格納する場所の IP アドレスまたはホスト名を入力します。 これは、サーバ、ストレージ アレイ、ローカル ドライブ、またはファブリック インターコネクトがネットワーク経由でアクセス可能な任意の読み取り/書き込みメディアなどがあります。 ホスト名を使用する場合、Cisco UCS Manager で DNS サーバを使用するように設定する必要があります。
- [Remote File] フィールド：バックアップ コンフィギュレーション ファイルのフル パスを入力します。 このフィールドには、ファイル名とパスを含めることができます。 ファイル名を省略すると、バックアップ手順によって、ファイルに名前が割り当てられます。
- [User] フィールド：Cisco UCS Manager がバックアップ場所へのログインに使用する必要のあるユーザ名を入力します。 プロトコルに TFTP を選択した場合は、このフィールドに入力する必要はありません。
- [Password] フィールド：ユーザ名に関連付けられたパスワードを入力します。 プロトコルに TFTP を選択した場合は、このフィールドに入力する必要はありません。

b) [OK] をクリックします。

ステップ 7 Cisco UCS Manager に確認ダイアログボックスが表示されたら、[OK] をクリックします。
[Admin State] フィールド をイネーブルに設定すると、Cisco UCS Manager によって、選択した設定タイプのスナップショットが取得され、ファイルがネットワークの場所にエクスポートされます。 [Backup Configuration] ダイアログボックスの [Backup Operations] テーブルに、バックアップ操作が表示されます。

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

a) [Properties] 領域に操作が表示されない場合、[Backup Operations] テーブルの操作をクリックします。

b) [Properties] 領域で、[FSM Details] バーの下矢印をクリックします。

[FSM Details] 領域が展開され、操作のステータスが表示されます。

ステップ 9 [OK] をクリックし、[Backup Configuration] ダイアログボックスを閉じます。
バックアップ操作は完了するまで実行し続けます。 進捗を表示するには、[Backup Configuration] ダイアログボックスを再度開きます。

ファブリックインターコネクトの全体のステータスの確認

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] タブで、[Equipment] > [Fabric Interconnects] を展開します。

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

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

ステップ 5 [Status] 領域で、[Overall Status] が [operable] であることを確認します。
ステータスが [operable] でない場合は、テクニカル サポート ファイルを作成およびダウンロードして、シスコのテクニカル サポートに問い合わせてください。 ファームウェア アップグレードに進まないでください。 テクニカル サポート ファイルの詳細については、『*Cisco UCS Manager B-Series Troubleshooting Guide*』を参照してください。

クラスタ設定の高可用性ステータスとロールの確認

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

手順

ステップ 1 [Navigation] ペインの [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 クラスタのいずれかのファブリック インターコネクトのノードをクリックします。

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

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

ステップ 6 次のフィールドに次の値が表示されることを確認します。

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

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

ステップ 7 [Leadership] フィールドの値に注意して、ファブリック インターコネクトがプライマリであるか、下位であるかを判断します。
この情報は、ファブリック インターコネクトのファームウェアをアップグレードするために知っておく必要があります。

I/O モジュールのステータスの確認

手順

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

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

ステップ 3 I/O モジュールのステータスを確認するシャーシをクリックします。

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

ステップ 5 各 I/O モジュールについて、次のカラムに次の値が表示されることを確認します。

フィールド名	必要な値
[Overall Status] カラム	ok

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

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

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

サーバのステータスの確認

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

手順

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

ステップ 2 [Equipment] タブの [Equipment] をクリックします。

ステップ 3 [Work] ペインの [Servers] タブをクリックして、すべてのシャーシのすべてのサーバのリストを表示します。

ステップ 4 各サーバについて、次のカラムに次の値が表示されることを確認します。

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

ステップ 5 サーバが検出されていることを確認する必要がある場合、次の手順を実行します。

a) 検出のステータスを確認するサーバを右クリックし、[Show Navigator] を選択します。

b) [General] タブの [Status Details] 領域で、[Discovery State] フィールド によって、[complete] の値が表示されていることを確認します。

[Status Details] 領域のフィールドが表示されない場合は、見出しの右側の [Expand] アイコンをクリックします。

シャーシのサーバのアダプタのステータスの確認

手順

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

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

ステップ 3 アダプタのステータスを確認するサーバをクリックします。

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

ステップ 5 [Inventory] タブの [Adapters] サブタブをクリックします。

ステップ 6 各アダプタについて、次のカラムに次の値が表示されることを確認します。

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

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

第 3 章

Release 1.4 ファームウェアのダウンロード

この章の内容は、次のとおりです。

- シスコからのソフトウェア バンドルの取得，23 ページ
- ファブリック インターコネクトへのファームウェア パッケージのダウンロード，25 ページ
- ファームウェア パッケージの内容の判断，27 ページ
- イメージ ダウンロードのキャンセル，27 ページ
- ファブリック インターコネクトのローカル記憶域のチェック，28 ページ

シスコからのソフトウェア バンドルの取得

はじめる前に

Cisco UCS インスタンスを更新するために、つぎのどのソフトウェア バンドルが必要かを判別します。

- Cisco UCS インフラストラクチャ ソフトウェア バンドル：すべての Cisco UCS インスタンスに必要です。
- Cisco UCS B シリーズ ブレード サーバ ソフトウェア バンドル：ブレード サーバを含むすべての Cisco UCS インスタンスに必要です。
- Cisco UCS C シリーズ ラックマウント サーバ ソフトウェア バンドル：統合ラックマウント サーバを含む Cisco UCS インスタンスのみに必要です。 このバンドルには、Cisco UCS Manager でこれらのサーバを管理できるようにするファームウェアが含まれます。標準の C シリーズ ラックマウント サーバには適用されません。

手順

ステップ 1 Web ブラウザで、Cisco.com に移動します。

ステップ 2 [Support] の下で、[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 プロンプトが出されたら、Cisco.com 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、以下に示す、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 インフラストラクチャ ソフトウェア バンドル	[Cisco UCS Infrastructure and UCS Manager Software] > [Unified Computing System (UCS) Infrastructure Software Bundle] をクリックします。
Cisco UCS B シリーズ ブレード サーバ ソフトウェア バンドル	[Cisco UCS B-Series Blade Server Software] > [Unified Computing System (UCS) Server Software Bundle] をクリックします。
Cisco UCS C シリーズ ラックマウント サーバ ソフトウェア バンドル	[Cisco UCS C-Series Rack-Mount UCS-Managed Server Software] > [Unified Computing System (UCS) Server Software Bundle] をクリックします。

ヒント このパスでアクセスできる Unified Computing System (UCS) Documentation Roadmap Bundle は、すべての Cisco UCS マニュアル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、最新版のリリース ノート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 バンドルに対して、次の作業を行います。

a) 次のリンクをクリックします。
リリース番号の後に括弧に入れられた数字と文字が表示されます。 この番号はメンテナンス リリース レベルを識別し、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 リリースとパッチに含まれているものについての詳細は、最新版のリリース 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) プロンプトに従って、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 インスタンスをアップグレードする前に、リリース ノートをお読みください。

次の作業

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

ファブリックインターコネクトへのファームウェアパッケージのダウンロード

同じ手順で、1 つのファームウェア イメージをファブリック インターコネクトにダウンロードできます。

（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された状態に保ちます。 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

シスコから必要なファームウェア バンドルを取得します。

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] ノードをクリックします。

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

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

ステップ 5 [Download Firmware] をクリックします。

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

名前	説明
[Protocol] フィールド	リモート サーバとの通信時に使用するプロトコル。 次のいずれかになります。 • FTP • TFTP • SCP • SFTP （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。

名前	説明
[Server] フィールド	ファイルがリモート サーバのファイルである場合は、ファイルが存在するリモート サーバの IP アドレスまたはホスト名。 ファイルがローカル ソースのファイルである場合、このフィールドには「local」が表示されます。 （注） 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 サーバを設定する必要があります。
[Filename] フィールド	ファームウェア ファイルの名前。
[Path] フィールド	リモート サーバ上のファイルへの絶対パス。 SCP を使用する場合、絶対パスは常に必要です。 他のプロトコルを使用する場合は、ファイルがデフォルトのダウンロード フォルダにあれば、リモート パスを指定する必要はありません。 ファイル サーバの設定方法の詳細については、システム管理者に問い合わせてください。
[User] フィールド	システムがリモート サーバへのログインに使用する必要のあるユーザ名。 プロトコルが TFTP の場合、このフィールドは適用されません。
[Password] フィールド	リモート サーバのユーザ名のパスワード。 プロトコルが TFTP の場合、このフィールドは適用されません。

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 7 [OK] をクリックします。

ステップ 8 （任意） [Download Tasks] タブで、イメージ 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、古いイメージを削除して、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。

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 ポイントの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。

イメージ ダウンロードのキャンセル

ダウンロード タスクの実行中にのみ、イメージのダウンロード タスクを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。 イメージのダウンロード タスクに関連する 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。

ファブリック インターコネクトのローカル記憶域のチェック

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。

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

この手順は、ファームウェアパッケージまたはバンドル全体を削除する場合に使用します。 必要な場合は、パッケージ内の 1 つ以上の個々のイメージを削除することもできます。

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 [Firmware Management] タブで、[Packages] タブをクリックします。

ステップ 5 テーブルで、削除するパッケージをクリックします。
Shift キーまたは Ctrl キーを使用して、複数のエントリを選択できます。

ステップ 6 1 つまたは複数の強調表示されたパッケージを右クリックし、[Delete] 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。

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。

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

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 [Firmware Management] タブで、[Images] タブをクリックします。

ステップ 5 表で、削除するイメージをクリックします。
Shift キーまたは Ctrl キーを使用して、複数のエントリを選択できます。

ステップ 6 強調表示されたイメージを右クリックし、[Delete] を選択します。

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。

第 4 章

Release 1.4(3) へのファームウェアのアップグレード

この章の内容は、次のとおりです。

- Release 1.4(1) または 1.4(2) からのアップグレード時に必要な手順，31 ページ
- Call Home のディセーブル化，33 ページ
- アダプタ、CIMC、IOM でのファームウェアのアップデート，33 ページ
- アダプタおよび CIMC でのファームウェアのアクティブ化，35 ページ
- サーバのボード コントローラ ファームウェアのアクティブ化，37 ページ
- Cisco UCS Manager ソフトウェアの Release 1.4 へのアクティブ化，38 ページ
- IOM のファームウェアの Release 1.4 へのアクティブ化，38 ページ
- クラスタ設定のファブリック インターコネクト ファームウェアのアクティブ化，40 ページ
- スタンドアロン ファブリック インターコネクトのファームウェアの Release 1.4 へのアクティブ化，45 ページ
- ホストおよび管理ファームウェア パッケージのアップデート，46 ページ
- Call Home のイネーブル化，53 ページ

Release 1.4(1) または 1.4(2) からのアップグレード時に必要な手順

（注） この順序に従わないと、ファームウェアのアップグレードが失敗し、サーバで Cisco UCS Manager の通信に問題が発生することがあります。

このマニュアルの手順と推奨されるオプションによって、データ トラフィックの中断を最小限にします。 そのため、Release 1.4 のいずれかのバージョンから Release 1.4 のそれよりも新しいバージョンにアップグレードする場合は、次の順序でコンポーネントをアップグレードします。

1. 次のファームウェア イメージをダウンロードします。
   - Cisco UCS インフラストラクチャ ソフトウェア バンドル：すべての Cisco UCS インスタンスに必要です。
   - Cisco UCS B シリーズ ブレード サーバ ソフトウェア バンドル：ブレード サーバを含むすべての Cisco UCS インスタンスに必要です。
   - Cisco UCS C シリーズ ラックマウント サーバ ソフトウェア バンドル：統合ラックマウント サーバを含む Cisco UCS インスタンスのみに必要です。 このバンドルには、Cisco UCS Manager でこれらのサーバを管理できるようにするファームウェアが含まれます。標準の C シリーズ ラックマウント サーバには適用されません。
2. （任意）Call Home をディセーブルにする：Cisco UCS インスタンスに Call Home または Smart Call Home が含まれている場合、Call Home をディセーブルにして、Cisco UCS Manager がコンポーネントを再始動したときに不要な警告を受け取らないようにします。
3. アダプタ、CIMC、および IOM を更新する：必要に応じて、ホスト ファームウェア パッケージ内のアダプタを最後の更新手順の一部としてアップグレードできます。
4. アダプタをアクティブ化する：この手順を実行するときは、[Ignore Compatibility Check] と [Set Startup Version Only] を選択します。
5. CIMC をアクティブ化する：この手順を実行するときは、[Ignore Compatibility Check] を選択します。
6. Cisco UCS Manager をアクティブ化する：この手順を実行するときは、[Ignore Compatibility Check] を選択します。
7. I/O モジュールをアクティブ化する：この手順を実行するときは、[Ignore Compatibility Check] と [Set Startup Version Only] を選択します。
8. 従属ファブリック インターコネクトをアクティブ化する：この手順を実行するときは、[Ignore Compatibility Check] を選択します。
9. データ パスが復元されたことを確認します。
10. 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：この手順を実行するときは、[Ignore Compatibility Check] を選択します。
11. サーバの管理ファームウェア パッケージを更新する：サーバで CIMC を直接更新およびアクティブ化した場合、この手順を実行する必要はありません。
12. サーバのホスト ファームウェア パッケージを更新する：アップグレードされた最後のファームウェアがある必要があります。 そのファームウェアを持つサーバがさらにリブートされるのを避けるため、この手順の間に、ボード コントローラ ファームウェアをアップグレードすることをお勧めします。 ホスト ファームウェア パッケージ内の次のファームウェアをアップグレードする必要があります。

- BIOS
- ストレージ コントローラ
- 一部のアダプタ

13 （任意）Call Home をイネーブルにする：ファームウェアをアップグレードする前に Call Home をディセーブルにしていた場合、それをイネーブルにします。

Call Home のディセーブル化

この手順は任意です。

Cisco UCS インスタンスをアップグレードすると、Cisco UCS Manager によってコンポーネントが再起動され、アップグレードプロセスが完了します。 この再起動によって、サービスの中断およびコンポーネントの障害と同じイベントが発生し、Call Home アラートの送信がトリガーされます。 アップグレードの開始前に Call Home をディセーブルにしない場合は、アップグレードに関連したコンポーネントの再起動によって生成されるアラートを無視してください。

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] > [Communication Management] > [Call Home]を展開します。

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

ステップ 4 [Admin] 領域の [State] フィールドで、[off] をクリックします。

（注） このフィールドが [off] に設定されている場合、Cisco UCS Manager ではこのタブの残りのフィールドが表示されません。

ステップ 5 [Save Changes] をクリックします。

アダプタ、CIMC、IOM でのファームウェアのアップデート

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

はじめる前に

ここでは、Cisco UCS システムのすべてのエンドポイント上のファームウェアを、同時にアップデートする方法について説明します。この手順を開始する前に、これらの各エンドポイントに対する適切なアップグレードの種類を判別するために、次の質問に回答してください。

- すべてのエンド ポイントが同じバックアップ バージョンで設定されていますか。「はい」の場合は、次の質問に進みます。「いいえ」の場合は、続行する前に、すべてのバックアップ バージョンを同じファームウェア バージョンに更新してください。
- 1 つ以上のサーバに関連付けられたサービス プロファイルに、ホストまたは管理ファームウェア パッケージが含まれていますか。「はい」の場合は、ファームウェア パッケージを使用してそのサーバのファームウェアを更新します。この手順によって、他のファームウェアとサーバをすべて更新できます。「いいえ」の場合は、次の質問に進みます。

  サーバのファームウェアを直接更新する場合、関連付けられたサービスプロファイルからすべてのホストと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。ホストまたは管理ファームウェアパッケージからファームウェアを削除しても、直接更新することはできません。
- サーバに Cisco UCS 第 2 世代のアダプタがありますか。「はい」の場合は、ホスト ファームウェア パッケージを使用してそのサーバのアダプタ ファームウェアを更新する必要があります。「いいえ」の場合は、そのサーバに対してこの手順を使用できます。

前述の最後の 2 つの質問の回答が「はい」であった場合でも、この手順を使用して、I/O モジュールおよび「いいえ」と回答したサーバをアップデートすることができます。

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 [Installed Firmware] サブタブの [Update Firmware] をクリックします。
Cisco UCS Manager GUI によって、[Update Firmware] ダイアログボックスが開き、Cisco UCS インスタンス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。
特定のタイプのエンドポイントを一度にアップデートする場合は、[Filter] ドロップダウン リストからそのエンドポイントを選択します。

b) メニュー バーの [Set Version] ドロップダウン リストから、Release 1.4(3) ファームウェア バンドルに含まれるファームウェア バージョンを選択します。

c) [Apply] をクリックしてアップデートを開始し、各エンドポイントのアップデートの進捗をモニタできるようにダイアログボックスを開いたままにしておきます。

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 すべてのアップデートが完了したら、[OK] をクリックします。

次の作業

ファームウェアをアクティブにします。

アダプタおよび CIMC でのファームウェアのアクティブ化

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

⚠

注意 [Activate Firmware] ダイアログボックスの [Filter] ドロップダウン リストで [ALL] を選択しないでください。選択すると、すべてのエンドポイントが同時にアクティブになります。 多くのファームウェア リリースやパッチには依存関係があるため、ファームウェアの更新を正常に実行するためにエンドポイントを特定の順序でアクティブにする必要があります。 この順序はリリースやパッチの内容によって異なります。 すべてのエンドポイントをアクティブにしても、更新が目的の順序で実行される保証はなく、エンドポイント、ファブリック インターコネクト、Cisco UCS Manager の間での通信が損なわれる可能性があります。 特定のリリースやパッチの依存関係については、当該のリリースやパッチに付属のリリース ノートを参照してください。

この手順は、前の手順から直接続いており、[Firmware Management] タブを表示していることを前提としています。

手順

ステップ 1 [Installed Firmware] タブの [Activate Firmware] をクリックします。
1 つ以上の選択したエンドポイントが、バックアップ バージョンとして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。

ステップ 2 アダプタ ファームウェアが、サービス プロファイルのホスト ファームウェア パッケージによってアップデートされていない場合は、[Activate Firmware] ダイアログボックスで、次の手順を実行して、アダプタ ファームウェアをアクティブにします。

a) [Filter] ドロップダウン リストから、[Adapters] を選択します。
b) [Set Version] ドロップダウン リストから、Release 1.4(3) ファームウェア バンドルに含まれるファームウェア バージョンを選択します。
c) [Ignore Compatibility Check] チェックボックスをオンにします。
このリリースのファームウェアは以前のリリースと互換性がありません。 そのため、アクティベーションを成功させるために、[Ignore Compatibility Check] チェックボックスをオンにする必要があります。
d) [Set Startup Version Only] チェックボックスをオンにします。
（注） 直接のアップグレード時に、アダプタに [Set Startup Version Only] を設定する必要があります。 この設定では、アクティブ化されたファームウェアが pending-next-boot 状態に移行し、サーバがすぐにリブートしません。 アクティブ化されたファームウェアは、サーバがリブートされるまで、アダプタで実行されているバージョンのファームウェアになりません。 ホスト ファームウェア パッケージのアダプタに [Set Startup Version Only] を設定することはできません。
e) [Apply] をクリックします。
すべてのアダプタの [Activate Status] カラムに [pending-next-boot] または [ready] が表示されている場合は、ステップ 3 に進みます。

ステップ 3 CIMC ファームウェアが、サービス プロファイルの管理ファームウェア パッケージによってアップデートされていない場合は、[Activate Firmware] ダイアログボックスで次の手順を実行して、CIMC ファームウェアをアクティブにします。

a) [Filter] ドロップダウン リストから、[CIMC] を選択します。
b) [Set Version] ドロップダウン リストから、Release 1.4(3) ファームウェア バンドルに含まれるファームウェア 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。
c) [Ignore Compatibility Check] チェックボックスをオンにします。
d) [Apply] をクリックします。

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

すべての CIMC コンポーネントの [Activate Status] カラムに [ready] が表示されている場合は、ステップ 4 に進みます。

ステップ 4 [OK] をクリックします。

サーバのボードコントローラファームウェアのアクティブ化

ボード コントローラ ハードウェアがあるのは、Cisco UCS B440 High Performance ブレード サーバや Cisco UCS B230 ブレード サーバなどの一部サーバだけです。 ボード コントローラ ファームウェアは eUSB、LED、および I/O コネクタなど、多数のサーバ機能を制御します。

この手順は、前の手順から続いており、[Installed Firmware] タブを表示していることを前提としています。

（注） このアクティベーションを実行すると、サーバはリブートします。 サーバに関連付けられたサービス プロファイルにメンテナンス ポリシーが含まれているかどうかによって、リブートがただちに実行される場合があります。 アップグレード中にサーバがリブートする回数を抑えるため、ボード コントローラ ファームウェアのアップグレードはサービス プロファイルのホスト ファームウェア パッケージから行うことを推奨します。

手順

ステップ 1 [Installed Firmware] サブタブの [Activate 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 インスタンス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 [Activate Firmware] ダイアログボックスのメニュー バーにある [Filter] ドロップダウン リストから、[Board Controller] を選択します。
Cisco UCS Manager GUI によって、[Activate Firmware] ダイアログボックスにボード コントローラを備えたすべてのサーバが表示されます。

ステップ 3 [Activate Firmware] ダイアログボックスのメニュー バーの [Set Version] ドロップダウン リストから、Release 1.4(3) ファームウェア バンドルに含まれるボード コントローラ ファームウェア バージョンを選択します。

ステップ 4 [Ignore Compatibility Check] 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 ソフトウェアの Release 1.4 へのアクティブ化

この手順は、前の手順から直接続いており、[Firmware Management] タブを表示していることを前提としています。

手順

ステップ 1 [Installed Firmware] サブタブの [Activate 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 インスタンス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 [Filter] ドロップダウン リストから、[UCS Manager] を選択します。

ステップ 3 [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、Release 1.4 ファームウェア バンドルに含まれているファームウェア バージョンを選択します。

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

ステップ 4 [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、その後で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。

IOM のファームウェアの Release 1.4 へのアクティブ化

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

⚠

注意 [Activate Firmware] ダイアログボックスの [Filter] ドロップダウン リストで [ALL] を選択しないでください。選択すると、すべてのエンドポイントが同時にアクティブになります。 多くのファームウェア リリースやパッチには依存関係があるため、ファームウェアの更新を正常に実行するためにエンドポイントを特定の順序でアクティブにする必要があります。 この順序はリリースやパッチの内容によって異なります。 すべてのエンドポイントをアクティブにしても、更新が目的の順序で実行される保証はなく、エンドポイント、ファブリック インターコネクト、Cisco UCS Manager の間での通信が損なわれる可能性があります。 特定のリリースやパッチの依存関係については、当該のリリースやパッチに付属のリリース ノートを参照してください。

この手順は、前の手順から直接続いており、[Firmware Management] タブを表示していることを前提としています。

手順

ステップ 1 [Installed Firmware] タブの [Activate Firmware] をクリックします。
1 つ以上の選択したエンドポイントが、バックアップ バージョンとして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。

ステップ 2 IOM ファームウェアをアクティブにするには、[Activate Firmware] ダイアログボックスで、次の手順を実行します。

a) [Filter] ドロップダウン リストから、[IO Modules] を選択します。
b) [Set Version] ドロップダウン リストから、Release 1.4 ファームウェア バンドルに含まれるファームウェア バージョンを選択します。
c) [Ignore Compatibility Check] チェックボックスをオンにします。
d) [Set Startup Version Only] チェックボックスをオンにします。

重要 I/O モジュールに対して [Set Startup Version Only] を設定した場合、そのデータ パス内のファブリック インターコネクトがリブートされると、I/O モジュールがリブートされます。 I/O モジュールに対して、[Set Startup Version Only] を設定しない場合、I/O モジュールがリブートし、トラフィックが中断します。 また、Cisco UCS Manager が、ファブリック インターコネクトと I/O モジュールとの間でプロトコルとファームウェア バージョンが一致しないことを検出した場合、Cisco UCS Manager は I/O モジュールをファブリック インターコネクトのファームウェアと同じバージョンに自動的にアップデートし、ファームウェアをアクティブにして I/O モジュールを再度リブートします。

e) [Apply] をクリックします。

ステップ 3 すべての IOM の [Activate Status] カラムに [pending-next-boot] が表示されている場合は、[OK] をクリックします。

クラスタ設定のファブリックインターコネクトファームウェアのアクティブ化

下位ファブリック インターコネクトのファームウェアの Release 1.4 へのアクティブ化

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。 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, （18 ページ）を参照してください。

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] サブタブの [Activate 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 インスタンス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 メニュー バーで、[Ignore Compatibility Check] チェックボックスをオンにします。

ステップ 7 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、Release 1.4 ファームウェア バンドルに含まれるファームウェア 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、Release 1.4 ファームウェア バンドルに含まれるファームウェア バージョンを選択します。

ステップ 8 [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てから、ファブリックインターコネクトと、そのファブリックインターコネクトへのデータ パスにある、ファブリックインターコネクトへのデータ トラフィックを中断するすべての I/O モジュールをリブートします。しかし、Cisco UCS インスタンス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 9 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。

（注） 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。

データ パスの準備が整っていることの確認

アップグレードの次の手順に進む前に、新しいプライマリ ファブリック インターコネクトのデータ パスが復元され、データ トラフィックを処理する準備が整っていることを確認します。

ダイナミック vNIC が稼働中であることの確認

ダイナミック vNIC、および VMware vCenter との統合を含む Cisco UCS をアップグレードする場合、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 –1**	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 –1**	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 インスタンスのアップグレード時に最適な結果を得るためには、アップグレードを開始する前、および従属ファブリック インターコネクトをアクティブ化した後にこのタスクを実行し、2 つの結果を比較することを推奨します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A /fabric-interconnect # **connect nxos** {**a** | **b**}	ファブリック インターコネクトの NX-OS モードを開始します。
ステップ 2	UCS-A(nxos)# **show npv flogi-table**	flogi セッションのテーブルを表示します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A(nxos)# **show npv flogi-table | grep fc | wc -1**	ファブリック インターコネクトにログインしたサーバの数を返します。 出力は、アップグレードの開始前にこの確認を行ったときに受け取った出力と一致している必要があります。

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

手順

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

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
```

プライマリファブリックインターコネクトのファームウェアのRelease 1.4 へのアクティブ化

この手順は、前の手順から直接続いており、[Firmware Management] タブを表示し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] サブタブの [Activate 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 インスタンス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 メニュー バーで、[Ignore Compatibility Check] チェックボックスをオンにします。

ステップ 4 プライマリ 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、Release 1.4 ファームウェア バンドルに含まれるファームウェア 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、Release 1.4 ファームウェア バンドルに含まれるファームウェア バージョンを選択します。

ステップ 5 [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てから、ファブリック インターコネクトと、そのファブリック インターコネクトへのデータ パスにある、ファブリック インターコネクトへのデータ トラフィックを中断するすべての I/O モジュールをリブートします。しかし、Cisco UCS インスタンス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 6 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。
（注） 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のファームウェアの Release 1.4 へのアクティブ化

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。

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] サブタブの [Activate 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 インスタンス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 [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 メニュー バーで、[Ignore Compatibility Check] チェックボックスをオンにします。

ステップ 7 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、Release 1.4 ファームウェア バンドルに含まれるファームウェア 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、Release 1.4 ファームウェア バンドルに含まれるファームウェア バージョンを選択します。

ステップ 8 [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てから、ファブリック インターコネクトと、そのファブリック インターコネクトへのデータ パスにあるすべての I/O モジュールをリブートします。 スタンドアロン ファブリック インターコネクトでは、これにより Cisco UCS インスタンス内のすべてのデータ トラフィックが中断します。

ホストおよび管理ファームウェア パッケージのアップデート

ホストファームウェアパッケージおよび管理ファームウェアパッケージへのアップデートの影響

ホスト ファームウェア パッケージまたは管理ファームウェア 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。ホスト ファームウェア パッケージまたは管理ファームウェア パッケージへの変更を保存した後の動作は、Cisco UCS インスタンスの設定によって異なります。

次の表に、ホスト ファームウェア パッケージまたは管理ファームウェア パッケージを使用したサーバのアップグレードにおける最も一般的なオプションを示します。

（注） メンテナンス ポリシーは、Cisco UCS Release 1.4 以降で使用可能です。

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
ホスト ファームウェア パッケージまたは管理ファームウェア 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、該当するリリースの Cisco UCS Manager コンフィギュレーション ガイドの手順に従い、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、この手順によって、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
ホストファームウェアパッケージまたは管理ファームウェア 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 ホストファームウェアパッケージまたは管理ファームウェア 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 Manager はモデル番号とベンダーを、このポリシーがインクルードされているサービス プロファイルに関連付けられているすべてのサーバと照合します。モデル番号とベンダーがポリシーのファームウェア バージョンと一致する場合は、Cisco UCS Manager 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
ホストファームウェアパッケージまたは管理ファームウェア 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 ホストファームウェアパッケージまたは管理ファームウェア 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 Manager 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 Manager はモデル番号とベンダーを、このポリシーがインクルードされているサービス プロファイルに関連付けられているすべてのサーバと照合します。モデル番号とベンダーがポリシーのファームウェア バージョンと一致する場合は、Cisco UCS Manager 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 Manager によってファームウェア パッケージが適用されず、保留中のアクティビティがキャンセルされません。 [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
ホストファームウェア パッケージまたは管理ファームウェア 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 ホストファームウェア パッケージまたは管理ファームウェア 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 Manager 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 Manager はモデル番号とベンダーを、このポリシーがインクルードされているサービス プロファイルに関連付けられているすべてのサーバと照合します。モデル番号とベンダーがポリシーのファームウェア バージョンと一致する場合は、Cisco UCS Manager 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 Manager によってファームウェア パッケージが適用されず、予定されたメンテナンスアクティビティがキャンセルされません。

管理ファームウェア 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た 1 つ以上のサービス プロファイルに含まれており、これらのサービス プロファイルにメンテナンス ポリシーが含まれていない場合、Cisco UCS Manager では、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、新しいバージョンを使用して管理サーバでファームウェアが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 右側の表で、次の手順を実行して、アップデートするファームウェアの既存のエントリを削除します。

a) 表の、変更するファームウェア バージョンの行を選択します。
b) 右クリックし、[Delete] を選択します。
c) [Yes] をクリックして、そのエントリを削除することを確認します。

ステップ 7 左側の [CIMC Firmware Packages] セクションで、次の手順を実行します。

a) 下矢印をクリックしてセクションを展開します。
デフォルトでは、セクション内のエントリはベンダー名でソートされます。エントリをソートするには、カラム見出しをクリックします。

b) ファームウェア パッケージに追加するリリースのファームウェア バージョンがリストされたテーブルの行を選択します。
ファームウェア バージョンは、このファームウェア パッケージに関連付けられたサーバのモデル番号（PID）と一致する必要があります。誤ったモデル番号のファームウェア バージョンを選択すると、Cisco UCS Manager はファームウェア更新をインストールできません。

c) 行を右側の表にドラッグします。
d) [Yes] をクリックして、正しいバージョンを選択したことを確認します。

ステップ 8 この管理ファームウェア パッケージに、異なるモデル番号（PID）を持つサーバの CIMC ファームウェアをインクルードする必要がある場合は、ステップ 6 を繰り返します。

ステップ 9 [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、このポリシーがインクルードされているサービス プロファイルに関連付けられているすべてのサーバと照合します。モデル番号とベンダーがポリシーのファームウェア バージョンと一致していれば、Cisco UCS Manager はサービス プロファイルに含まれているメンテナンス ポリシーの設定に従って、ファームウェアを更新します。

ホスト ファームウェア パッケージのアップデート

Release 1.4(3) にアップグレードする場合、ホスト ファームウェア パッケージによって BIOS とストレージ コントローラのファームウェアをアップグレードする必要があります。それらのパッ

ケージをアップグレードしないと、サーバで、Cisco UCS Manager および CIMC の通信に問題が発生することがあります。

⚠

注意 ポリシーがサーバに関連付けられた 1 つ以上のサービス プロファイルに含まれており、これらのサービスプロファイルにメンテナンス ポリシーが含まれていない場合、Cisco UCS Manager では、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、新しいバージョンを使用してサーバおよびアダプタでファームウェアが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。

この手順では、ホスト ファームウェア パッケージがすでに存在し、Cisco UCS Manager を現在の Release 1.4(2) にアップグレードしていることを前提としています。 ホスト ファームウェア パッケージの作成方法または以前のリリースの既存パッケージをアップデートする方法については、Cisco UCS Manager が実行されているリリースの該当する『*Cisco UCS Manager GUI Configuration Guide*』を参照してください。

はじめる前に

ホスト ファームウェア パッケージをアップデートする前に、次の手順を実行します。

- Cisco UCS Manager およびファブリック インターコネクトをアップグレードします。
- 適切なメンテナンス ウィンドウを判断し、サーバのリブート時のデータ トラフィックの中断の影響を緩和します。
- サーバのファームウェア バージョンとモデル番号（PID）を知っ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 [General] タブの各サブタブで、パッケージに含めるファームウェアのタイプごとに次の操作を実行します。

a) [Select] 列で、適切な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] 列の情報が、このパッケージでアップデートするサーバの情報と一致す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たサーバと一致している必要があります。 誤ったモデルまたは型番を選択した場合、Cisco UCS Manager はファームウェア アップデートをインストールできません。

c) [Version] カラムで、Release 1.4(3) ファームウェア イメージからファームウェア バージョンを選択します。

ステップ 6 [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、このポリシーがインクルードされているサービス プロファイルに関連付けられているすべてのサーバと照合します。 モデル番号とベンダーがポリシーのファームウェア バージョンと一致していれば、Cisco UCS Manager はサービス プロファイルに含まれているメンテナンス ポリシーの設定に従って、ファームウェアを更新します。

次の作業

ホスト ファームウェア パッケージに含まれるエンドポイントのファームウェアが Release 1.4(3) にアップデートされたことを確認します。 ファームウェアがアップデートされていない場合は、ホストファームウェアパッケージのモデル番号とベンダーをアップデートされたエンドポイントのそれらと照らして確認します。

Call Home のイネーブル化

この手順は任意です。 ファームウェアのアップグレードを開始する前に Call Home をディセーブルにした場合にのみ、イネーブルにする必要があります。

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] > [Communication Management] > [Call Home]を展開します。

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

ステップ 4 [Admin] 領域の [State] フィールドで、[on] をクリックします。

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

ステップ 5 [Save Changes] をクリックします。