Cisco UCS Manager によるファームウェアの管理

Cisco UCS Manager でのファームウェアのダウンロードと管理

ファームウェア イメージの管理

シスコでは、イメージのバンドル内の Cisco UCS コンポーネントに、すべてのファームウェア アップデートを提供します。各イメージは、1 つのハードウェア コンポーネントに固有のファームウェア パッケージを表します。たとえば、IOM イメージや Cisco UCS Manager イメージなどです。Cisco UCS ファームウェアのアップデートは、Cisco UCS ドメイン のファブリック インターコネクトに次のバンドルでダウンロードできます。

Cisco UCS インフラストラクチャ ソフトウェア バンドル

Cisco UCS Manager リリース 4.0 以降のリリースには、4 つの個別のインフラストラクチャ バンドルが含まれています。

これらのバンドルには、次のコンポーネントをアップデートするために必要となるファームウェア イメージなどがあります。

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

- I/O モジュールのファームウェア

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

Note あるプラットフォーム用の UCS インフラストラクチャ バンドルは、別のプラットフォームをアクティブ化するために使用できません。たとえば、UCS 6300 シリーズ ファブリック インターコネクトのインフラストラクチャ バンドルを使用して Cisco UCS 6400 シリーズ ファブリック インターコネクト をアクティブにすることはできません。

Cisco UCS B シリーズ ブレード サーバ ソフトウェア バンドル

このバンドルには、Cisco UCS ドメインのブレードサーバのファームウェアをアップデートするために必要となる、次のファームウェアイメージが含まれます。リリース用に作成された最新のバンドルに加えて、最新のインフラストラクチャ バンドルに含まれないブレード サーバに対して Cisco UCS Manager をイネーブルにするために、次のバンドルもリリースされる場合があります。

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

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

このバンドルには、Cisco UCS Manager と統合されその管理を受けているラックマウントサービスのコンポーネントの更新に必要な、次のファームウェアイメージが含まれます。

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

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

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

Caution 自動インストールプロセスを開始する前に、データ パスの準備が整っていることの確認に従ってデータをキャプチャしてください。

- 自動インストール中に保留中のアクティビティを確認する前に、すべての下位 VIF パスが再構築されていることを確認することが重要です。
- UCS VIF パスは、UCS Manager GUI 内の障害からではなく、CLI からのみモニターしてください。
- UCS VIF パスのモニターに失敗すると、部分的または完全な「すべてのパスがダウン」状態になる可能性があります。

両方のファブリック インターコネクトのリブートが必要なプロセスを実行する前に、ガイドラインに従うことを推奨します。

ファームウェア イメージ ヘッダー

すべてのファームウェア イメージに、次の情報を含むヘッダーがあります。

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

ファームウェア イメージ カタログ

Cisco UCS Manager 使用できるすべてのイメージのインベントリを維持します。イメージ カタログには、イメージとパッケージのリストが含まれます。パッケージは、ダウンロードされたときに作成される読み取り専用オブジェクトです。これはディスク領域を占有せず、パッケージのダウンロードの一部として展開されたイメージのリストまたはコレクションを表します。個々のイメージがダウンロードされるときに、パッケージ名はイメージ名と同じままです。

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

パッケージ

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

イメージ

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

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

Tip Cisco UCS Manager によって、ファブリック インターコネクトのブートフラッシュにイメージが保存されます。クラスタ システムでは、すべてのイメージが互いに同期されるので、両方のファブリック インターコネクトにおけるブートフラッシュのスペース使用量は等しくなります。ブートフラッシュ パーティションが 70 % を超え、合計使用スペースが 90 % を超えると、エラーが発生します。Cisco UCS Manager がこのような障害を生成した場合、領域を解放するために古いイメージを削除します。

シスコからのソフトウェア バンドルの入手

Before you begin

Cisco UCS ドメインを更新するには、次のどのソフトウェア バンドルが必要かを判断します。

- Cisco UCS 6400 シリーズ ファブリック インターコネクト、6300 シリーズ ファブリック インターコネクト、6200 シリーズ ファブリック インターコネクト、および 6324 ファブリック インターコネクト用の Cisco UCS インフラストラクチャ ソフトウェア バンドル：すべての Cisco UCS ドメイン で必要です。
- Cisco UCS B シリーズ ブレード サーバ ソフトウェア バンドル：ブレード サーバーを含むすべての Cisco UCS ドメイン に必要。
- Cisco UCS C シリーズ ラックマウント UCS 管理対象サーバ ソフトウェア バンドル：統合ラックマウント サーバーを含む Cisco UCS ドメイン にのみ必要。このバンドルには、Cisco UCS Managerを使用してこれらのサーバーを管理するためのファームウェアが含まれています。このバンドルはスタンドアロンの C シリーズ ラックマウント サーバーには適用できません。

Procedure

ステップ 1 Web ブラウザで、Cisco.com を参照します。

ステップ 2 [サポート（Support）] で [すべてをダウンロード（All Downloads）] をクリックします。

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

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

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

作成	ナビゲーション パス
Cisco UCS 6400 シリーズ ファブリック インターコネクト、6300 シリーズ ファブリック インターコネクト、6200 シリーズ ファブリック インターコネクト、および 6324 ファブリック インターコネクト用の Cisco UCS インフラストラクチャ ソフトウェア バンドル	**[UCS Infrastructure and UCS Manager Software]** > **[Unified Computing System (UCS) Infrastructure Software Bundle]** をクリックします。
Cisco UCS B シリーズ ブレード サーバ ソフトウェア バンドル	**[UCS B-Series Blade Server Software]** > **[Unified Computing System (UCS) Server Software Bundle]** をクリックします。
Cisco UCS C シリーズ ラックマウント UCS 管理対象サーバ ソフトウェア バンドル	**[UCS C-Series Rack-Mount UCS-Managed Server Software]** > **[Unified Computing System (UCS) Server Software Bundle]** をクリックします。

Tip これらのパスからアクセスできる Unified Computing System（UCS）ドキュメント ロードマップ バンドルは、すべての Cisco UCS ドキュメントを含むダウンロード可能な ISO イメージです。

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

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

a) 最新リリースの 4.0 ソフトウェア バンドルのリンクをクリックします。

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

b) 次のいずれかのボタンをクリックして、表示される指示に従います。

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

c) メッセージに従ってソフトウェア バンドルのダウンロードを完了します。

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

What to do next

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

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

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

Before you begin

必要なファームウェア バンドルをシスコから入手します。

Procedure

ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。

ステップ 2 **[機器]** ノードをクリックします。

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

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

ステップ 5 [Download Firmware] をクリックします。

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

名前	説明
[Protocol] フィールド	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** **Note** TFTP ファイルのサイズ上限は 32 MB です。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 の使用はお勧めしません。 • **SCP** • **ステップ** • **[USB A]**：ファブリック インターコネクト A に挿入された USB ドライブ。 • [USB B]：ファブリック インターコネクト B に挿入された USB ドライブ。 **Note** USB A および USB B は、Cisco UCS 6324（UCS Mini）および Cisco UCS 6300 シリーズ ファブリック インターコネクトにのみ適用されます。 Cisco UCS 6300 シリーズ ファブリック インターコネクトでは、2 個のポートのうちの最初のポートのみ検出されます。
[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。 **Note** IPv4 や IPv6 アドレスではなくホスト名を使用する場合、DNS サーバを設定する必要があります。Cisco UCS ドメイン が Cisco UCS Central に登録されていないか、または DNS 管理が [local] に設定されている場合は、Cisco UCS Manager で DNS サーバを設定します。Cisco UCS ドメイン が Cisco UCS Central に登録されていて、DNS 管理が [global] に設定されている場合は、Cisco UCS Central で DNS サーバを設定します。
[Filename] フィールド	ファームウェア ファイルの名前。

名前	説明
[Path] フィールド	リモート サーバー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 サーバーの設定方法の詳細については、システム管理者に問い合わせてください。
[User] フィールド	システムがリモート サーバへのログインに使用する必要のあるユーザ名。プロトコルが TFTP の場合、このフィールドは適用されません。
[Password] フィールド	リモート サーバのユーザ名のパスワード。プロトコルが TFTP の場合、このフィールドは適用されません。

ステップ 7 [OK] をクリックします。

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

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

Note Cisco UCS Manager によって、ブートフラッシュの領域が不足していることが報告された場合は、**[パッケージ（Packages）]** タブで古いバンドルを削除して、領域を解放します。ブートフラッシュの空き領域を表示するには、ファブリック インターコネクトにナビゲートし、**[機器（Equipment）]** タブをクリックして、**[一般（General）]** タブの **[ローカル ストレージ情報（Local Storage Information）]** 領域を展開します。

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

What to do next

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

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

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

始める前に

必要なファームウェア バンドルをシスコから入手します。

手順

ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。

ステップ 2 **[機器]** ノードをクリックします。

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

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

ステップ 5 [Download Firmware] をクリックします。

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

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

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

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

ステップ 8 [OK] をクリックします。

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

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

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

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

次のタスク

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

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。

Procedure

ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。
ステップ 2 [Equipment] ノードを展開します。
ステップ 3 [Work] ペインの [Firmware Management] タブをクリックします。
ステップ 4 [Download Tasks] タブで、キャンセルするタスクを右クリックし、[Delete] を選択します。

ファームウェア パッケージの内容の判断

手順

ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。
ステップ 2 **[機器]** ノードをクリックします。
ステップ 3 [Work] ペインの [Firmware Management] タブをクリックします。
ステップ 4 [Packages] サブタブで、パッケージの内容を表示するには、パッケージの横の [+] アイコンをクリックします。
ステップ 5 パッケージの内容のスナップショットを取得するには、次の手順を実行します。
a) イメージ名とその内容を含む行を強調表示します。

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

ファームウェア パッケージの内容の準拠の確認

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

手順

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

ファブリック インターコネクトの空き領域のチェック

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

手順

ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。
ステップ 2 **[機器]** > **[ファブリックインターコネクト]**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] ペインで、[General] タブをクリックします。
ステップ 5 [Local Storage Information] 領域を展開します。

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

自動インストールによるファームウェアアップグレード

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

- インストール インフラストラクチャ ファームウェア：Cisco UCS インフラストラクチャ ソフトウェア バンドルを使用して、 ファブリック インターコネクト、I/O モジュール、Cisco UCS Managerなど、インフラストラクチャ コンポーネントをアップグレードします。ファームウェア イメージの管理 （1 ページ）はCisco UCS Managerリリース 4.0。の使用可能なインフラストラクチャ ソフトウェア バンドルに関する詳細を提供します。自動インストールによるインフラストラクチャ ファームウェアのアップグレードの推奨プロセス （16 ページ）では、インフラストラクチャ ファームウェアの自動インストールに関して Cisco が推奨するプロセスを説明しています。
- シャーシ ファームウェアのインストール] を使用して、 Cisco UCS C シリーズ ラックマウント UCS 管理対象サーバ ソフトウェア バンドル シャーシのコンポーネントをアップグレードします。
- インストール サーバ ファームウェア：Cisco UCS B シリーズ ブレード サーバ ソフトウェア バンドル を使用して Cisco UCS ドメイン のすべてのブレード サーバをアップグレードしたり、また Cisco UCS C シリーズ ラックマウント UCS 管理対象サーバ ソフトウェア バンドル を使用してすべてのラック サーバをアップグレードすることができます。

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

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

（注） ドメイン内の Cisco UCS Manager が Cisco UCS 2.1(1) より前のリリースである場合は、自動インストールを使用して、Cisco UCS ドメイン内のインフラストラクチャまたはサーバをアップグレードすることはできません。ただし、Cisco UCS Manager を Release 2.1(1) 以降にアップグレードすると、自動インストールを使用して、ファームウェア レベルの最低要件を満たしている Cisco UCS ドメイン内の他のコンポーネントをアップグレードできます。詳細については、自動インストール によるアップグレードに関する注意事項とガイドラインを参照してください。

Cisco UCS Manager リリース 3.1(1l)、3.1(2b)、3.1(2c)、および 3.1(2e) で、[Redundancy] を [Grid] に設定し、[Power Capping] を [No Cap] に設定して電源ポリシーを設定している場合、自動インストール を使用した Cisco UCS Manager ソフトウェアのアクティブ化は失敗します。Cisco UCS Manager リリース 3.1(2b) より前、および 3.1(2e) より後の Cisco UCS Manager リリースでは、自動インストール を使用した Cisco UCS Manager ソフトウェアのアクティブ化は構成された電源ポリシーに基づく失敗がなくなりました。

後の直接アップグレード 自動インストール

自動インストール 中、デフォルト インフラストラクチャ パックのスタートアップ バージョンが設定されます。Cisco UCS Manager後に自動インストール、ファブリック インターコネクト、および IOM の直接アップグレードまたはアクティブ化を正常に完了するには、直接アップグレードまたはアクティブ化を開始する前に、スタートアップ バージョンがクリアされていることを確認します。デフォルト インフラストラクチャ パックのスタートアップ バージョンが構成されている場合、Cisco UCS Manager、ファブリック インターコネクト、および IOM を直接アップグレードまたはアクティブ化することはできません。デフォルトのインフラストラクチャ パックおよびサービス パックのスタートアップ バージョンのクリア （25 ページ） は、スタートアップ バージョンをクリアするための詳細な手順を提供します。

自動内部バックアップ

インフラストラクチャ ファームウェアのアップグレード中に、完全な状態のバックアップ ファイルが自動的に作成されます。Cisco UCS Manager リリース 2.2(4) では、FSM ステータスで表示される 2 つの新しいバックアップ段階が追加されました。これらを次に示します。

1. **InternalBackup**：設定をバックアップします。
2. **PollInternalBackup**：バックアップの完了を待ちます。

バックアップが正常に完了すると、「bkp.*timestamp*.tgz」という名前のバックアップ ファイルが、両方のファブリック インターコネクトの `/workspace/backup` ディレクトリに保存されます。ここには、最新のバックアップ ファイルのみが保存されます。

バックアップが失敗した場合は、「**internal backup failed**」というマイナー エラーがログに記録されます。このエラーは、Cisco UCS Manager リリース 2.2(4) より前のリリースにダウングレードした場合は記録されません。

このバックアップ ファイルからファブリック インターコネクトの設定を復元する前に、local-mgmt から copy コマンドを使用して、バックアップ ファイルをファブリック インターコネクトからファイル サーバにコピーします。

次に、自動内部バックアップ ファイルをファイル サーバにコピーする方法の例を示します。

```
UCS-A# connect local-mgmt
UCS-A (local-mgmt) # copy workspace:/backup/bkp.1429690478.tgz
scp://builds@10.190.120.2://home/builds/
```

ファームウェア インストールの準備

自動インストールを使用して、Cisco UCS ドメインを単一のパッケージに含まれているファームウェア バージョンにアップグレードできます。自動インストールでは、3つの独立した段階でファームウェアをインストールする機能を提供:インフラストラクチャ ファームウェアのイ

ンストール、シャーシ ファームウェアのインストール、およびサーバ ファームウェアのインストール。自動インストール中に、IOM、アダプタ、BIOS、CIMCなどの一部のエンドポイントのファームウェアが最初に更新されてからアクティブになります。

エンドポイントのファームウェアを更新するには、ファームウェアイメージをエンドポイントのバックアップ パーティションにステージングする必要があります。更新フェーズでは、エンドポイントの再起動は不要です。アクティブ化の段階で、バックアップパーティションのファームウェアをエンドポイントのアクティブなファームウェアバージョンとして設定します。アクティベーションには、エンドポイントのリブートが必要な場合やリブートが発生する場合があります。したがって、自動インストールプロセスを完了するのにかかる時間には、次のことを実行するために必要な時間が含まれます。

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

（注） 自動インストール完了に費やされる時間の大半は、この処理です。

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

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

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

インストール インフラストラクチャ ファームウェア

インストール インフラストラクチャ ファームウェア では、Cisco UCS Manager を含む Cisco UCS ドメイン内のすべてのインフラストラクチャ コンポーネントと、すべてのファブリック インターコネクトおよび I/O モジュールをアップグレードします。すべてのコンポーネント

が、選択した Cisco UCS インフラストラクチャ ソフトウェア バンドルに含まれるファームウェア バージョンにアップグレードされます。

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

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

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

インストール サーバ ファームウェア

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

- シャーシ内のすべてのブレード サーバ用の Cisco UCS B シリーズ ブレード サーバ ソフトウェア バンドル。
- Cisco UCS ドメインに統合されているすべてのラックマウント サーバ用の Cisco UCS C シリーズ ラックマウント UCS 管理対象サーバ ソフトウェア バンドル。

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

自動インストール のための必要な手順

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

1. インストール インフラストラクチャ ファームウェア

2. インストール サーバ ファームウェア

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

自動インストールによるインフラストラクチャファームウェアのアップグレードの推奨プロセス

シスコでは、自動インストールによるインフラストラクチャ ファームウェアのアップグレードについて、次のプロセスを推奨します。

1. ソフトウェアをステージングし、アップグレードを準備します。
    1. すべてのコンフィギュレーションファイルと完全な状態のバックアップ ファイル、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、完全な状態のコンフィギュレーション バックアップ ファイルの作成 を作成します。
    2. ファームウェア パッケージをダウンロードします。離れた場所からのファブリック インターコネクトへのファームウェア イメージのダウンロード （6 ページ）、およびローカル ファイル システムからファブリック インターコネクトへのファームウェア イメージのダウンロード （9 ページ）、詳細な情報を提供します。
    3. Cisco UCS Manager リリース 3.2(3) または以降のリリースを使用している場合は、インフラストラクチャのファームウェアをステージングします。ファームウェア インストールの準備 （17 ページ）は、インフラストラクチャ ファームウェアのステージングに関する詳細情報を提供します。

（注） この手順はオプションですが、これもお勧めします。

    4. Smart Call Home を無効にします。Smart Call Home の無効化 には、Smart Call Home の無効化に関する詳細情報が掲載されています。
2. ファブリック アップグレードを準備します。
    1. Cisco UCS Manager障害を確認し、サービスに影響を与える障害を解決します。 障害の検証に関する詳細情報を提供します。UCS Manager の障害の表示は、障害の検証に関する詳細情報を提供します。
    2. 高可用性ステータスを確認し、セカンダリ ファブリック インターコネクトを特定します。クラスタ設定の高可用性ステータスとロールの確認 は、障害の確認に関する詳細情報を提供します。
    3. デフォルトのメンテナンス ポリシーを設定します。デフォルト メンテナンス ポリシーの設定は詳細な情報を提供します。また、このビデオ（http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/configure_the_default_maintenance_policy.html）

の [Play] をクリックして、デフォルトのメンテナンス ポリシーを [User Ack] として設定する方法を視聴することもできます。

4. VLAN と FCOE ID が重複していないことを確認します。
5. 管理インターフェイスを無効にします。管理インターフェイスの無効化 には、セカンダリ ファブリック インターコネクトの管理インターフェイスの無効化に関する詳細情報が掲載されています。
6. すべてのパスが機能していることを確認します。データ パスの準備が整っていることの確認は詳細な情報を提供します。

3. 自動インストールによってインフラストラクチャ ファームウェアをアップグレードします。自動インストールによるインフラストラクチャ ファームウェアのアップグレード（19 ページ） は詳細情報を提供します。また、このビデオ（http://www.cisco.com/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/upgrade_the_infrastructure_firmware_with_auto_install.html）の **[Play]** をクリックして、自動インストール でインフラストラクチャ ファームウェアをアップグレードする方法を視聴することもできます。

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

4. クラスタの高可用性ステータスを確認します。
5. すべてのパスが動作していることを確認します。
6. 新しい障害を確認します。ファブリック インターコネクトのアップグレード中に生成される障害の表示 には、障害の確認に関する詳細が掲載されています。
7. プライマリ ファブリックのアクティブ化を確認します。プライマリ ファブリック インターコネクトのリブートの確認 （23 ページ） は詳細情報を提供します。また、このビデオ（http://www.cisco.com/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/acknowledge_pending_reboot_of_the_primary_fabric_interconnect.html）の [Play] をクリックして、プライマリ ファブリック インターコネクトのリブートを確認する方法を視聴することもできます。
8. 新しい障害を確認します。

ファームウェア インストールの準備

手順

ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。
ステップ 2 **[機器]** ノードをクリックします。

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

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

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

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

a) Cisco UCS ドメインのインフラストラクチャ コンポーネントを更新するには、 **[A-Series Infrastructure Firmware]**領域で**[New Version]** ドロップダウン リストからアップグレードするソフトウェア バンドルを選択します。

b) Cisco UCS ドメイン のブレード サーバを更新するには、**[B-Series Blade Server Firmware]** 領域の **[New Version]** ドロップダウン リストからアップグレードするソフトウェア バンドルを選択します。

c) にCisco UCS ドメインのラックマウント サーバと S3260 シャーシを更新するには、**[C-Series Chassis/Rack-Mount Server Firmware]** 領域の **[New Version]** ドロップダウン リストからアップグレードするソフトウェア バンドルを選択します。

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

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

d) [Next] をクリックします。

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

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

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

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

c) [Next] をクリックします。

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

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

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

c) 必要に応じて、次のいずれかのカラムにあるリンクをクリックします。

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

d) 次のいずれかを実行します。

- 選択したファームウェア パッケージを 1 つ以上変更する場合は、**[Prev]** をクリックします。
- 適切なファームウェアパッケージを選択済みで、エンドポイントのファームウェアの更新の影響を確認する場合は、**[Next]** をクリックします。
- ファームウェアの更新をすぐに開始するには、**[Update]**をクリックします。

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

a) **[UCS Firmware Pack Endpoints]** 表で結果をフィルタリングするには、該当するチェックボックスをオンにします。

エンドポイントのタイプによって、結果をフィルタ リングできます。

b) 影響を受けるエンドポイントのリストを確認します。

c) 次のいずれかを実行します。

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

自動インストールによるインフラストラクチャファームウェアのアップグレード

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

（注） ドメイン内の Cisco UCS Manager が Cisco UCS Manager 2.1(1) より前のリリースである場合は、自動インストールを使用して、Cisco UCS ドメイン内のインフラストラクチャまたはサーバをアップグレードすることはできません。ただし、Cisco UCS Manager を Release 2.1(1) 以降にアップグレードすると、自動インストールを使用して、ファームウェア レベルの最低要件を満たしている Cisco UCS ドメイン内の他のコンポーネントをアップグレードできます。詳細については、自動インストールによるアップグレードに関する注意事項とガイドラインおよび該当する『Cisco UCS upgrade guide』を参照してください。

Cisco UCS Manager リリース 3.1(3) から、自動インストール を使用して Cisco UCS Manager および両方のファブリック インターコネクトにサービス パックをインストールできます。基本のインフラストラクチャ パックにサービス パックを適用することはできますが、個別にサービス パックをインストールすることはできません。

インフラストラクチャ パックをアップグレードせずに、互換性のあるサービス パックを 自動インストール 経由でインストールできます。これにより、両方のファブリック インターコネクトでサービス パックのインストールがトリガーされます。特定のサービス パックをインストールするには、ファブリック インターコネクトを再ロードする必要があります。

サービス パックを使用するインフラストラクチャ ファームウェアの 自動インストール は、すべてのインフラストラクチャ コンポーネントが Cisco UCS Manager リリース 3.1(3) 以降のリリースである場合にのみサポートされます。

始める前に

- ファームウェアのアップグレードとダウングレードの前提条件に記載のすべての前提条件を満たす必要があります。
- Cisco UCS Manager リリース 3.2(3) または以降のリリースを使用している場合は、インフラストラクチャのファームウェアを準備します。ファームウェア インストールの準備 （17 ページ） は、インフラストラクチャ ファームウェアのステージングに関する詳細情報を提供します。

（注） オプションですが、これもお勧めします。

Cisco UCS ドメインで NTP サーバを使用して時刻を設定しない場合、プライマリ ファブリック インターコネクトとセカンダリ ファブリック インターコネクトのクロックを必ず同期させてください。Cisco UCS Manager で NTP サーバを設定するか、時間を手動で同期することによってこれを行うことができます。

手順

ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。

ステップ 2 **[機器]** ノードをクリックします。

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

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

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

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

警告は次のカテゴリに分類されています。

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

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

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

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

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

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

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

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

ステップ 9 [OK] をクリックします。

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

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

次のタスク

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

特定のサービス パックをインストールするには、ファブリック インターコネクトを再ロードする必要があります。このようなシナリオでは、サービスパックのインストールを完了させるためにプライマリ ファブリック インターコネクトの再起動を確認する必要があります。

プライマリ ファブリック インター コネクトのリブートの確認

ここで説明する手順を使用することも、このビデオ（http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/acknowledge_pending_reboot_of_the_primary_fabric_interconnect.html）の [Play] をクリックしてプライマリ ファブリック インターコネクトのリブートを確認する方法を視聴することもできます。

始める前に

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

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

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

手順

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

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

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

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

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

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

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

インフラストラクチャファームウェアのアップグレードのキャンセル

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

手順

ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。

ステップ 2 **[機器]** ノードをクリックします。

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

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

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

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

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

ステップ 8 [OK] をクリックします。

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

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

手順

ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。

ステップ 2 **[機器]** ノードをクリックします。

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

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

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

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

ステップ 7 [OK] をクリックします。

自動インストールによるサーバ ファームウェアのアップグレード

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

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

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

この段階を完了すると再起動します。

（注） ドメイン内の Cisco UCS Manager が Cisco UCS Manager 2.1(1) より前のリリースである場合は、自動インストールを使用して、Cisco UCS ドメイン内のインフラストラクチャまたはサーバをアップグレードすることはできません。ただし、Cisco UCS Manager を Release 2.1(1) 以降にアップグレードすると、自動インストールを使用して、ファームウェア レベルの最低要件を満たしている Cisco UCS ドメイン内の他のコンポーネントをアップグレードできます。詳細については、自動インストールによるアップグレードに関する注意事項とガイドラインおよび該当する『Cisco UCS upgrade guide』を参照してください。

（注） **Install Server Firmware** ウィザードの設定が完了した後で、サーバ ファームウェアのアップグレード プロセスをキャンセルすることはできません。Cisco UCS Manager は、変更を即座に反映します。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。

始める前に

- ファームウェアのアップグレードとダウングレードの前提条件に記載のすべての前提条件を満たす必要があります。
- Cisco UCS Manager リリース 3.2(3) または以降のリリースを使用している場合は、サーバのファームウェアをステージングします。ファームウェア インストールの準備 （17 ページ）は、サーバーファームウェアのステージングに関する詳細情報を提供します。

（注） オプションですが、これもお勧めします。

手順

ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。

ステップ 2 **[機器]** ノードをクリックします。

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

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

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

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

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

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

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

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

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

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

c) サーバをサービス パックのファームウェア バージョンにアップグレードするには、[Service-Pack Firmware] 領域の **[New Version]** ドロップダウン リストからこれらのサーバをアップグレードするサービス パックを選択します。

d) [Next] をクリックします。

ステップ 8 **[Install Server Firmware]** ウィザードの **lSe[ect Firmware Packages]** ページで、次を実行します。

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

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

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

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

c) [Next] をクリックします。

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

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

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

d) 次のいずれかを実行します。

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

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

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

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

b) 影響を受けるエンドポイントのリストを確認します。
c) 必要に応じて、 **[Maintenance Policy]** カラムのリンクをクリックして、そのポリシーのナビゲータを開きます。
d) 次のいずれかを実行します。

- 選択したホスト ファームウェア パッケージを 1 つ以上変更する場合は、[Prev] をクリックします。

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

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

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

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

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

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

ホスト ファームウェア パッケージ

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

- **アダプタ**
- **BIOS**
- **CIMC**

Note ラック マウント サーバでは、ホスト ファームウェア パックから CIMC を除外し、ボード コントローラをアップグレードまたはダウングレードすると、アップグレードまたはダウングレードが失敗する可能性があります。これは、CIMC ファームウェアのバージョンとボード コントローラ ファームウェアのバージョンに互換性がない可能性があるためです。

- ボード コントローラ

- **Flex Flash コントローラ**
- **GPU**
- **FC アダプタ**
- **HBA Option ROM**
- **ホスト NIC**
- **ホスト NIC オプション ROM**
- **ローカル ディスク**

Note **ローカル ディスク**は、デフォルトでホスト ファームウェア パックから除外されます。

Cisco UCS Manager リリース 3.1(1) で、ローカル ディスク ファームウェアを更新するには、ホスト ファームウェア パッケージに**ブレードパッケージ**を必ず含めます。ブレードパッケージには、ブレード サーバとラック サーバのローカル ディスク ファームウェアが含まれています。Cisco UCS Manager リリース 3.1(2) から、ローカル ディスクおよびその他の共通エンドポイント用のファームウェアは、ブレード パッケージとラック パッケージの両方で入手できます。

- **PSU**
- **SAS エクスパンダ**
- **ストレージ コントローラ**
- **ストレージ コントローラのオンボード デバイス**
- **ストレージ コントローラのオンボード デバイス Cpld**
- **ストレージ デバイスのブリッジ**

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

また、新しいホスト ファームウェア パッケージを作成するとき、または既存のホスト ファームウェア パッケージを変更するときに、ホスト ファームウェア パッケージから特定のコンポーネントのファームウェアを除外できます。たとえば、ホスト ファームウェア パッケージによっ

てBIOSファームウェアをアップグレードしない場合は、ファームウェア パッケージ コンポーネントのリストから BIOS ファームウェアを除外できます。

Important 各ホスト ファームウェア パッケージは、すべてのファームウェア パッケージ（ブレードおよびラック）に共通の除外されたコンポーネントの1つのリストに関連付けられます。ファームウェア パッケージ タイプごとに別の除外リストを設定するには、別のホスト ファームウェア パッケージを使用します。

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

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

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

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

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

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

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

新しいサービス プロファイル

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

ファームウェア パッケージ ポリシーの作成

このステージでは、ホスト ファームウェア パッケージを作成します。

サービス プロファイルのアソシエーション

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

既存のサービス プロファイル

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

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

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

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

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

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

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

サービス プロファイル	メンテナンス ポリシー	アップグレード処理
ファームウェア パッケージが 1 つ以上のサービス プロファイルに含まれており、このサービス プロファイルが 1 つ以上のサーバに関連付けられている。 または ファームウェア パッケージがアップデート中のサービス プロファイル テンプレートに含まれており、このテンプレートから作成されたサービス プロファイルが 1 つ以上のサーバに関連付けられている。	[On Next Boot] オプションでユーザ確認応答に関して設定済み	ファームウェア パッケージをアップデートすると、次のようになります。 **1.** Cisco UCS によって、変更を確認するように要求され、ユーザ確認応答済みのサーバのリブートが必要であることが通知されます。 **2.** リブートして新しいファームウェアを適用するには、次のいずれかの手順を実行します。 • 点滅している [Pending Activities] ボタンをクリックし、リブートして新規ファームウェアを適用するサーバを選択します。 • 手動でサーバをリブートします。 **3.** Cisco UCS によって、このポリシーをインクルードしているサービス プロファイルに関連付けられているすべてのサーバに照らして、モデル番号とベンダーが検証されます。モデル番号とベンダーがポリシーのファームウェア バージョンと一致する場合は、Cisco UCS によりサーバがリブートされ、ファームウェアがアップデートされます。 サーバを手動でリブートすると、Cisco UCS によってファームウェア パッケージが適用されます。これは、[On Next Boot] オプションによって有効になります。

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

ホスト ファームウェア パッケージの作成

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

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

Important 各ホスト ファームウェア パッケージは、すべてのファームウェア パッケージ（ブレードおよびラック）に共通の除外されたコンポーネントの1つのリストに関連付けられます。ファームウェア パッケージ タイプごとに別の除外リストを設定するには、別のホスト ファームウェア パッケージを使用します。

Before you begin

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

Procedure

ステップ 1 [ナビゲーション]ペインで、[サーバ]をクリックします。

ステップ 2 **[サーバ]** > **[ポリシー]**を展開します。

ステップ 3 ポリシーを作成する組織のノードを展開します。

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

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

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

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

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

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

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

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

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

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

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

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

b) **[Vendor]**、**[Model]**、および**[PID]**カラムの情報が、このパッケージを使用して更新するサーバの情報と一致していることを確認します。

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

c) **[Version]** カラムで、ファームウェアのアップデート バージョンを選択します。

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

What to do next

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

ホスト ファームウェア パッケージのアップデート

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

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

Important 各ホスト ファームウェア パッケージは、すべてのファームウェア パッケージ（ブレードおよびラック）に共通の除外されたコンポーネントの 1 つのリストに関連付けられます。ファームウェア パッケージ タイプごとに別の除外リストを設定するには、別のホスト ファームウェア パッケージを使用します。

Before you begin

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

Procedure

ステップ 1 [ナビゲーション]ペインで、[サーバ]をクリックします。

ステップ 2 **[サーバ]** > **[ポリシー]**を展開します。

ステップ 3 アップデートするポリシーを含む組織のノードを展開します。

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

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

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

ステップ 6 各サブタブで、パッケージに含めるファームウェア タイプごとに次の手順を実行します。

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

b) **[Vendor]**、**[Model]**、および **[PID]** カラムの情報が、このパッケージを使用して更新するサーバの情報と一致していることを確認します。

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

c) **[Version]** カラムで、ファームウェアのアップデート バージョンを選択します。

ステップ 7 ホスト ファームウェア パッケージのコンポーネントを変更するには、[Modify Package Versions] をクリックします。

[Modify Package Versions] ウィンドウが表示されます。

ステップ 8 ブレード パッケージを変更するには、[Blade Package] ドロップダウン リストから、ブレード パッケージのバージョンを選択します。

ステップ 9 ラック パッケージを変更するには、[Rack Package] ドロップダウン リストから、ラック パッケージのバージョンを選択します。

ステップ 10 サービス パックを変更するには、[Service Pack] ドロップダウン リストから、サービス パックのバージョンを選択します。

サービス パックを削除するには、[<not set>] を選択します。

ステップ 11 [Excluded Components] 領域で、このホスト ファームウェア パッケージから除外するコンポーネントに対応するチェックボックスをオンにします。

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

ステップ 12 [OK] をクリックします。

Cisco UCS Manager によって、このポリシーをインクルードしているサービス プロファイルに関連付けられているすべてのサーバに照らして、モデル番号とベンダーが検証されます。モデル番号とベンダーがポリシー内のファームウェア バージョンに一致する場合、Cisco UCS Manager は、サービス プロファイルに含まれているメンテナンス ポリシー内の設定に従ってファームウェアを更新します。

既存のサービス プロファイルへのファームウェア パッケージの追加

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

手順

ステップ 1 [ナビゲーション]ペインで、[サーバ]をクリックします。

ステップ 2 **[サーバ]** > **[サービスプロファイル]**を展開します。

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

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

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

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

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

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

ステップ 8 **[Save Changes]**をクリックします。

ファームウェアの自動同期

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

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

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

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

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

  この値は、デフォルトで選択されます。

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

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

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

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

ファームウェア自動同期サーバ ポリシーの設定

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

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

始める前に

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

手順

ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。

ステップ 2 **[機器]** ノードをクリックします。

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

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

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

- [No Action]：ファームウェアのアップグレードはサーバで開始されません。
- [User Acknowledge]：[Pending Activities] ダイアログボックスで管理者がアップグレードを確認するまでサーバのファームウェアは同期されません。

  このオプションは、デフォルトで選択されます。

ステップ 6 **[Save Changes]**をクリックします。

エンドポイントでの直接のファームウェアのアップグレード

正しい手順に従って、正しい順序でアップグレードを適用すれば、エンドポイントの直接のファームウェア アップグレードと新しいファームウェア バージョンのアクティブ化による、Cisco UCS ドメインのトラフィックの中断を最小限に留めることができます。エンドポイントでのインフラストラクチャ ファームウェアの直接アップグレードの推奨プロセス, on page 48は、エンドポイントでインフラストラクチャ ファームウェアをアップグレードする際に、Cisco が推奨するプロセスを説明しています。

次のコンポーネントのファームウェアを直接アップグレードできます。

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

• Cisco UCS Manager
• ファブリック インターコネクト
 	
必ず Cisco UCS Manager をアップグレードしてからファブリック インターコネクトをアップグレードしてください。
	• I/O モジュール
	• 電源装置
	• サーバ：
	  • アダプタ
	  • CIMC
	  • BIOS
	  • ストレージ コントローラ
	  • ボード コントローラ
		• アダプタ
		• CIMC
		• BIOS
		• ストレージ コントローラ
		• ボード コントローラ
			• CMC
			• シャーシ アダプタ
			• SAS エクスパンダ
			• シャーシ ボード コントローラ
			• サーバ：
			  • CIMC
			  • BIOS
			  • ボード コントローラ
			  • ストレージ コントローラ

Cisco UCS C3260 シャーシの場合、シャーシ プロファイル内のシャーシ ファームウェア パッケージを通じて、CMC、シャーシ アダプタ、シャーシ ボード コントローラ、SAS エクスパンダ、およびローカル ディスクのファームウェアをアップグレードできます。『*Cisco UCS S3260 Server Integration with Cisco UCS Manager, Release 4.0*』には、シャーシ プロファイルとシャーシ ファームウェア パッケージに関する詳細情報が記載されています。

アダプタ、ボード コントローラ、CIMC、および BIOS ファームウェアは、サービス プロファイル内のホスト ファームウェア パッケージによってアップグレードできます。ホスト ファームウェア パッケージを使用して、このファームウェアをアップグレードする場合、ファームウェアのアップグレード プロセス中に、サーバをリブートする必要がある回数を削減できます。

Important すべてのサーバ コンポーネントは、同じリリース レベルで維持する必要があります。これらのコンポーネントはリリースごとに同時にテストされているので、互いのバージョンが一致していないと、予期しないシステム動作が発生する可能性があります。

直接のファームウェア アップグレードのステージ

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

アップデート

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

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

- アダプタ
- CIMC
- I/O モジュール

Cisco UCS C3260 高密度ストレージ ラック サーバ シャーシでは、アップデートの段階は以下のエンドポイントのみに適用されます。

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

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

アクティブ化

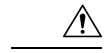
このステージでは、指定したイメージバージョン（通常はバックアップ バージョン）がスタートアップ バージョンとして設定され、[Set Startup Version Only] を指定していない場合、エンドポイントがただちにリブートされます。エンドポイントがリブートされると、バックアップ パーティションがアクティブなパーティションになり、アクティブなパーティションがバックアップ パーティションになります。新しいアクティブなパーティションのファームウェアはスタートアップ バージョンおよび実行されているバージョンになります。

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

- Cisco UCS Manager

- ファブリック インターコネクト
- それらをサポートするサーバ上のボード コントローラ
- Cisco UCS C3260 高密度ストレージ ラック サーバ シャーシ：
  - CMC
  - 共有アダプタ
  - シャーシとサーバのボード コントローラ
  - SAS エクスパンダ
  - ストレージ コントローラ
  - BIOS
  - CIMC

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



Caution I/O モジュールに対して [Set Startup Version Only] を設定した場合、そのデータ パス内のファブリック インターコネクトがリブートされると、I/O モジュールがリブートされます。I/O モジュールに対して、[Set Startup Version Only] を設定しない場合、I/O モジュールがリブートし、トラフィックが中断します。また、ファブリック インターコネクトと I/O モジュール間でプロトコルとファームウェア バージョンの不一致が Cisco UCS Manager で検出された場合、Cisco UCS Managerは、ファブリック インターコネクトのファームウェアと一致するファームウェア バージョンを使用して I/O モジュールを自動的に更新し、ファームウェアをアクティブ化して、I/O モジュールを再度リブートします。

直接のファームウェア アップグレードの停止の影響

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

ファブリック インターコネクト ファームウェア アップグレードの停止の影響

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

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

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

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

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

  実行中の保存されていない作業が失われます。

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

I/O モジュール ファームウェア アップグレードの停止の影響

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

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

CIMC ファームウェア アップグレードの停止の影響

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

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

アダプタ ファームウェア アップグレードの停止の影響

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

- サーバがリブートします。
- サーバ トラフィックが中断します。

エンドポイントでのインフラストラクチャファームウェアの直接アップグレードの推奨プロセス

シスコでは、エンドポイントでのインフラストラクチャ ファームウェアの直接アップグレードについて、次のプロセスを推奨します。

1. ソフトウェアをステージングし、アップグレードを準備します。
    1. すべての構成ファイルと完全な状態のバックアップファイルを作成します。すべてのコンフィギュレーション バックアップ ファイルの作成 と 完全な状態のコンフィギュレーション バックアップ ファイルの作成 は、詳細情報を提供します。
    2. ファームウェア パッケージをダウンロードします。離れた場所からのファブリック インターコネクトへのファームウェア イメージのダウンロード （6 ページ） と ローカル ファイル システムからファブリック インターコネクトへのファームウェア イメージのダウンロード （9 ページ） は、詳細情報を提供します。
    3. Smart Call Home を無効にします。Smart Call Home の無効化 は、詳細情報を提供します。
2. Cisco UCS Manager ソフトウェアのアクティブ化Cisco UCS Manager ソフトウェアのアクティブ化 （52 ページ） は、詳細情報を提供します。また、このビデオ（http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/activate_ucsm.html）の **[Play]** をクリックして、Cisco UCS Manager ソフトウェアをアクティブ化する方法を視聴することもできます。
3. IOM ファームウェアをアップデートします。IOM （56 ページ） は、詳細情報を提供します。また、このビデオ（http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/update_and_activate_iom.html）の [Play] をクリックして、IOM ファームウェアを更新する方法を視聴することもできます。
4. ファブリック アップグレードを準備します。
    1. UCS Manager の障害を確認し、サービスに影響を及ぼす障害を解決します。UCS Manager の障害の表示 は、詳細情報を提供します。
    2. 高可用性ステータスを確認し、セカンダリ ファブリック インターコネクトを特定します。クラスタ設定の高可用性ステータスとロールの確認 は、詳細情報を提供します。
    3. デフォルトのメンテナンス ポリシーを構成します。デフォルト メンテナンス ポリシーの設定 は、詳細情報を提供します。また、このビデオ（http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/configure_the_default_maintenance_policy.html）の [Play] をクリックして、デフォルトのメンテナンス ポリシーを [User Ack] として設定する方法を視聴することもできます。
    4. VLAN と FCOE ID が重複していないことを確認します。
    5. 管理インターフェイスを無効にします。管理インターフェイスの無効化 は、詳細情報を提供します。

6. IOM ファームウェアをアクティブ化します。IOM （58 ページ） は、詳細情報を提供します。また、このビデオ（http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/update_and_activate_iom.html）の [Play] をクリックして、IOM ファームウェアをアクティブ化する方法を視聴することもできます。

5. 従属ファブリック インターコネクトをアクティブにします。

   1. 従属ファブリック インターコネクトのトラフィックを待避させます。ファブリック インターコネクト トラフィックの待避の設定は、詳細情報を提供します。また、このビデオ（http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/enable_and_disable_fi_traffic_evacuation.html）の [Play] をクリックして、ファブリック インターコネクト トラフィックを待避させる方法を視聴することもできます。

   2. 従属ファブリック インターコネクト（FI-B）をアクティブにし、FSM をモニタします。従属ファブリック インターコネクトでのファームウェアのアクティブ化 （58 ページ） は、詳細情報を提供します。また、このビデオ（http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/activate_the_firmware_on_a_subordinate_fabric_interconnect.html）の [Play] をクリックして、従属ファブリック インターコネクトでファームウェアをアクティブ化する方法を視聴することもできます。

   3. すべてのパスが動作していることを確認します。データ パスの準備が整っていることの確認 は、詳細情報を提供します。

   4. 従属ファブリック インターコネクトのトラフィック待避を無効にします。ファブリック インターコネクト トラフィックの待避の設定 は、詳細情報を提供します。また、このビデオ（http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/enable_and_disable_fi_traffic_evacuation.html）の [Play] をクリックして、ファブリック インターコネクトのトラフィック待避を無効にする方法を視聴することもできます。

   5. 新しい障害を確認します。ファブリック インターコネクトのアップグレード中に生成される障害の表示。

6. プライマリ ファブリック インターコネクト（FI-A）をアクティブにします。

   1. 管理サービスをプライマリ ファブリック インターコネクトからセカンダリ ファブリック インターコネクトに移行し、クラスタ リードをセカンダリ ファブリック インターコネクトに変更します。ファブリック インターコネクト クラスタ リードのスイッチオーバー （62 ページ） は、詳細情報を提供します。また、このビデオ（http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/switch_over_fabric_interconnect_cluster_lead.html）の [Play] をクリックして、あるファブリック インターコネクトから別のファブリック インターコネクトにクラスタ リードをスイッチオーバーする方法を視聴することもできます。

   2. プライマリ ファブリック インターコネクトのトラフィックを待避させます。

3. プライマリ ファブリック インターコネクト（FI-A）をアクティブにし、FSM をモニタします。プライマリ ファブリック インターコネクトでのファームウェアのアクティブ化 （60 ページ） は、詳細情報を提供します。また、このビデオ（http://www.cisco.com/en/us/docs/unified_computing/ucs/ucs-manager/videos/3-1/activate_the_firmware_on_a_primary_fabric_interconnect.html）の [Play] をクリックして、プライマリ ファブリック インターコネクトでファームウェアをアクティブ化する方法を視聴することもできます。
4. すべてのパスが動作していることを確認します。
5. プライマリ ファブリック インターコネクトのトラフィック待避を無効にします。
6. 新しい障害を確認します。

複数のエンドポイントのファームウェアのアップデート

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

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

Procedure

ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。

ステップ 2 **[機器]** ノードをクリックします。

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

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

Cisco UCS Manager GUI によって [ファームウェアの更新（Update Firmware）] ダイアログボックスが開かれ、Cisco UCS ドメイン内のすべてのエンドポイントのファームウェア バージョンが検証されます。この手順は、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。

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

b) [選択（Select）] フィールドで、次のいずれかの手順を実行します。

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

c) [OK] をクリックします。

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

Cisco UCS Manager 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、アクティブにするまでは、バックアップ バージョンの状態のままに保たれます。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、アップデートごとに完了時間は異なります。

[ファームウェアの更新（Update Firmware）] ダイアログボックスで、すべてのアップデート エンドポイントの **[ステータスの更新（Update Status）]** カラムに **[ready]** と表示されると、アップデートは完了です。

ステップ 6 (Optional) 各エンドポイントのアップデート状況をモニタするには、該当するエンドポイントを右クリックして、[Show Navigator] を選択します。

Cisco UCS Manager によって、**[全般（General）]** タブの **[ステータスの更新（Update Status）]** 領域に進捗が表示されます。ナビゲータに **[FSM]** タブがある場合は、このタブでも進捗をモニタできます。**[再試行#]** フィールドに、アップデートが失敗したことが示されないことがあります。再試行回数には、Cisco UCS Manager が更新ステータスを取得するときに発生する再試行も含まれます。

What to do next

ファームウェアをアクティブにします。

Cisco UCS Manager ファームウェア

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

- クラスタ設定の場合、両方のファブリック インターコネクトの Cisco UCS Manager は同じバージョンを実行する必要があります。
- Cisco UCS Manager アクティブ化により、管理機能が短期間にわたってダウンします。すべての仮想シェル（VSH）接続が切断されます。
- クラスタ設定の場合、両方のファブリック インターコネクトの Cisco UCS Manager がアクティブ化されます。
- ファブリック インターコネクトをリセットする必要がないため、Cisco UCS Manager の更新はサーバ アプリケーション I/O に影響を与えません。
- 従属ファブリック インターコネクトがダウンしている間に Cisco UCS Manager が更新された場合、従属ファブリック インターコネクトは復帰時に自動的に更新されます。

アップグレードの検証

Cisco UCS Manager は、アップグレードまたはダウングレード プロセスを検証し、すべてのファームウェア アップグレードの検証エラー（非推奨のハードウェアなど）を **[Upgrade Validation]** タブに表示します。アップグレードの検証エラーがある場合、アップグレードは失敗し、Cisco UCS Manager は以前のリリースにロールバックします。これらのエラーを解決し、[Force] オプションを使用してアップグレードを続行する必要があります。

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

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

Cisco UCS Manager ソフトウェアのアクティブ化

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

Procedure

ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。

ステップ 2 **[機器]** ノードをクリックします。

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

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

Cisco UCS Manager GUI によって [ファームウェアのアクティブ化（Activate Firmware）] ダイアログボックスが開かれ、Cisco UCS ドメイン 内のすべてのエンドポイントのファームウェア バージョンが検証されます。この手順は、シャーシとサーバの数によって、数分かかることがあります。

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

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

b) [OK] をクリックします。

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

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

Cisco UCS Manager ソフトウェアのサービス パックのアクティブ化

ここで説明する手順を使用して、Cisco UCS Manager ソフトウェアのサービス パックをアクティブ化することができます。このプロセスでは、ファブリック インターコネクトのアップグレードまたは再起動は必要ありません。

Procedure

ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。

ステップ 2 **[機器]** ノードをクリックします。

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

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

Cisco UCS Manager GUI によって [ファームウェアのアクティブ化（Activate Firmware）] ダイアログボックスが開かれ、Cisco UCS ドメイン 内のすべてのエンドポイントのファームウェア バージョンが検証されます。この手順は、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、[UCS Manager] を選択します。

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

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

b) [OK] をクリックします。

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

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

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

Procedure

ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。

ステップ 2 **[機器]** ノードをクリックします。

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

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

Cisco UCS Manager GUI によって [ファームウェアのアクティブ化（Activate Firmware）] ダイアログボックスが開かれ、Cisco UCS ドメイン 内のすべてのエンドポイントのファームウェア バージョンが検証されます。この手順は、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、[UCS Manager] を選択します。

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

ステップ 7 [OK] をクリックします。

IOM および IFM（Cisco UCS X シリーズ サーバーの IOM） ファームウェア

Cisco UCS I/O モジュール（IOM）は、ブレード サーバ エンクロージャにユニファイド ファブリック テクノロジーを組み込みます。これにより、ブレード サーバとファブリック インターコネクト間の複数の 10 ギガビット イーサネット接続を提供し、診断、配線、管理を簡素化します。IOM により、ファブリック インターコネクトとブレード サーバ シャーシ間での I/O ファブリックが拡張され、すべてのブレードおよびシャーシを 1 つに接続する、損失のない確実な Fibre Channel over Ethernet（FCoE）ファブリックを使用できます。

IOM は分散ライン カードと同様であるため、スイッチングを実行せず、ファブリック インターコネクトの拡張として管理されます。このようなアプローチを取ることで、ブレード シャーシ

から各種スイッチが取り払われ、システム全体構造の複雑さが低減します。また、Cisco UCS の規模を拡大してシャーシの数を増やしても、必要なスイッチの数が増えることはありません。これにより、すべてのシャーシを可用性の高い1つの管理ドメインとして扱うことが可能になります。

IMO では、ファブリック インターコネクトと併せてシャーシ環境（電源、ファン、ブレードを含む）も管理できます。したがって、個別のシャーシ管理モジュールは必要ありません。IMO は、ブレード サーバ シャーシの背面に設置します。各ブレード シャーシは最大 2 つの IOM をサポートできるため、容量と冗長性を向上させることができます。

IOM ファームウェアの更新およびアクティブ化に関するガイドライン

IOM でファームウェアを更新およびアクティブ化するときには、次のガイドラインとベストプラクティスを考慮してください。

- 各 IOM は、実行中のイメージとバックアップ イメージの 2 つのイメージを格納します。
- 更新操作では、IOM のバックアップ イメージが新しいファームウェア バージョンに置き換えられます。
- アクティブ化操作では、現在の起動イメージがバックアップイメージに降格します。新しい起動イメージが代わりに配置され、このバックアップイメージから起動するようにシステムが設定されます。
- アクティブなイメージのみを設定するには、[Set Startup Version Only] チェックボックスをオンにします。リセットは実行されません。このプロセスを使用すると、複数の IOM をアップグレードし、同時にリセットできます。ファブリックインターコネクトが更新およびアクティブ化されると、ファブリックインターコネクトは対応するIOMをリブートし、ダウンタイムを低減します。
- IOM とファブリック インターコネクトは、互いに互換性がある必要があります。
- ファブリックインターコネクトで実行されるソフトウェアが互換性のないバージョンを実行する IOM を検出した場合、ファブリック インターコネクトのシステム ソフトウェアと同じバージョンにするために IOM の自動更新を実行します。

  Cisco UCS Manager この状況を通知するために障害を生成します。また、自動更新の進行中、IOM の検出状態は [Auto updating] を示します。
- Cisco UCS Manager では、**[Installed Firmware]** タブで IOM ファームウェアをシャーシ レベルで確認できます。

次の項で詳しく説明する手順を使用するか、またはこのビデオ（http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/update_and_activate_iom.html）の [Play] をクリックして、IOM ファームウェアを更新およびアクティブ化する方法を視聴できます。

IOM

⚠

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

Procedure

ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。

ステップ 2 **[機器（Equipment）] > [シャーシ（Chassis）] > *[シャーシ番号（Chassis Number）]* > [IO モジュール（IO Modules）]** の順に展開します。

ステップ 3 アップデートする I/O モジュールをクリックします。

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

ステップ 5 **[ファームウェアの更新（Update Firmware）]** ダイアログボックスで、次の操作を実行します。

a) **[バージョン（Version）]** ドロップダウン リストで、ファームウェア バージョンを選択してエンドポイントを更新します。

b) **[OK]** をクリックします。

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

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

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

What to do next

ファームウェアをアクティブにします。

複数の IOM でのファームウェアのアクティブ化

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

⚠

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

Procedure

ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。

ステップ 2 **[機器]** ノードをクリックします。

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

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

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

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

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

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

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

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

Important I/O モジュールに対して [Set Startup Version Only] を設定した場合、そのデータパス内のファブリック インターコネクトがリブートされると、I/O モジュールがリブートされます。I/O モジュールに対して、[Set Startup Version Only] を設定しない場合、I/O モジュールがリブートし、トラフィックが中断します。また、ファブリック インターコネクトと I/O モジュール間でプロトコルとファームウェア バージョンの不一致が Cisco UCS Manager で検出された場合、Cisco UCS Managerは、ファブリック インターコネクトのファームウェアと一致するファームウェアバージョンを使用してI/Oモジュールを自動的に更新し、ファームウェアをアクティブ化して、I/O モジュールを再度リブートします。

e) [Apply] をクリックします。

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

ステップ 6 [OK] をクリックします。

IOM

Procedure

ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。

ステップ 2 **[機器（Equipment）] > [シャーシ（Chassis）] > *[シャーシ番号（Chassis Number）]* > [IO モジュール（IO Modules）]** の順に展開します。

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

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

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

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

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

b) スタートアップバージョンを設定し、エンドポイントで実行中のバージョンを変更しない場合、**[スタートアップ バージョンのみを設定（Set Startup Version Only）]** チェックボックスをオンにします。

[スタートアップ バージョンのみを設定する（Set Startup Version Only）] を設定した場合、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、エンドポイントはすぐにはリブートされません。アクティブ化されたファームウェアは、エンドポイントがリブートされるまで、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。

c) [OK] をクリックします。

ファブリック インターコネクトのファームウェア

従属ファブリック インターコネクトでのファームウェアのアクティブ化

ここで説明する手順を使用することも、このビデオ（http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/activate_the_firmware_on_a_subordinate_fabric_interconnect.html）の [Play] をクリックして従属ファブリックインターコネクトのファームウェアをアクティブ化する方法を視聴することもできます。

始める前に

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

手順

ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。

ステップ 2 **[機器]** ノードをクリックします。

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

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

Cisco UCS Manager GUI によって [ファームウェアのアクティブ化（Activate Firmware）] ダイアログボックスが開かれ、Cisco UCS ドメイン 内のすべてのエンドポイントのファームウェア バージョンが検証されます。この手順は、シャーシとサーバの数によって、数分かかることがあります。

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

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

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

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

ステップ 7 [Apply] をクリックします。

Cisco UCS Manager はファームウェアをアップデートしてアクティブにし、ファブリック インターコネクトとそのファブリック インターコネクトへのデータ パスにあるすべての I/O モジュールをリブートするため、そのファブリックインターコネクトとの間のデータ トラフィックが中断します。ただし、トラフィックおよびポートフェールオーバーを許可するようにCisco UCS ドメインが設定されている場合、データ トラフィックはプライマリ ファブリック インターコネクトにフェールオーバーし、中断されません。

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

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

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

次のタスク

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

プライマリ ファブリック インターコネクトでのファームウェアのアクティブ化

この手順は、従属ファブリック インターコネクトでのファームウェアのアクティブ化 （58 ページ）から直接続いており、[Firmware Management] タブが表示されていることを前提としています。ここで説明する手順を使用することも、このビデオ（http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/activate_the_firmware_on_a_primary_fabric_interconnect.html）の [Play] をクリックしてプライマリ ファブリック インターコネクトのファームウェアをアクティブ化する方法を視聴することもできます。

始める前に

下位のファブリック インターコネクトをアクティブにします。

手順

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

Cisco UCS Manager GUI によって [ファームウェアのアクティブ化（Activate Firmware）] ダイアログボックスが開かれ、Cisco UCS ドメイン 内のすべてのエンドポイントのファームウェア バージョンが検証されます。この手順は、シャーシとサーバの数によって、数分かかることがあります。

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

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

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

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

ステップ 4 [Apply] をクリックします。

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

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

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

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

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

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

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

Procedure

ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。

ステップ 2 **[機器]** ノードをクリックします。

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

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

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

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

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

ステップ 6 [OK] をクリックします。

Cisco UCS Manager はファームウェアをアクティベートして、そのファブリック インターコネクトへのデータ パスでファブリック インターコネクトおよびI/Oモジュールを再起動します。. スタンドアロン インターコネクトでは、これにより、Cisco UCS ドメイン のすべてのデータ トラフィックが中断します。

ファブリック インターコネクト クラスタ リードのスイッチオーバー

この操作は Cisco UCS Manager CLIでのみ実行できます。ここで説明する手順を使用することも、このビデオ（http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/videos/3-1/switch_over_fabric_interconnect_cluster_lead.html）の [Play] をクリックして、あるファブリック インターコネクトから別のファブリック インターコネクトにクラスタ リードをスイッチオーバーする方法を視聴することもできます。

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

手順

	コマンドまたはアクション	目的
ステップ 1	（任意） UCS-A# **show cluster state**	クラスタ内のファブリック インターコネクトの状態と、クラスタがHA レディであるかどうかを表示します。
ステップ 2	UCS-A# **connect local-mgmt**	クラスタのローカル管理モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A (local-mgmt) # **cluster** {**force** **primary** | **lead** {**a** | **b**}}	次のいずれかのコマンドを使用して、従属ファブリック インターコネクトをプライマリに変更します。 **force** ローカル ファブリック インターコネクトがプライマリになるように強制します。 **lead** 指定した従属ファブリック インターコネクトをプライマリにします。

例

次に、ファブリック インターコネクト B を従属からプライマリに変更する例を示します。

```
UCS-A# show cluster state
Cluster Id: 0xfc436fa8b88511e0-0xa370000573cb6c04

A: UP, PRIMARY
B: UP, SUBORDINATE

HA READY
UCS-A# connect local-mgmt
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2011, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

UCS-A(local-mgmt)# cluster lead b
UCS-A(local-mgmt)#
```

ファブリック インターコネクトでのサービス パックの有効化

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

手順

ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。

ステップ 2 **[機器]** ノードをクリックします。

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

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

Cisco UCS Manager GUI によって [ファームウェアのアクティブ化（Activate Firmware）] ダイアログボックスが開かれ、Cisco UCS ドメイン 内のすべてのエンドポイントのファームウェア バージョンが検証されます。この手順は、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 ファブリック インターコネクトの [Activate Firmware] ダイアログボックスの [Service Pack] の行で、[スタートアップ バージョン（Startup Version）] カラム のドロップダウンリストからアップグレードするサービス パックのバージョンを選択します。

ステップ 7 [OK] をクリックします。

Cisco UCS Manager ファームウェアをアクティブにします。場合によっては、Cisco UCS Manager によってファブリック インターコネクトが再起動され、そのファブリック インターコネクトに対するデータ トラフィックが中断されます。

ファブリック インターコネクトからのサービス パックの削除

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

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

手順

ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。

ステップ 2 **[機器]** ノードをクリックします。

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

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

Cisco UCS Manager GUI によって [ファームウェアのアクティブ化（Activate Firmware）] ダイアログボックスが開かれ、Cisco UCS ドメイン 内のすべてのエンドポイントのファームウェア バージョンが検証されます。この手順は、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 ファブリック インターコネクトの [Activate Firmware] ダイアログボックスの [Service Pack] の行で、[スタートアップ バージョン（Startup Version）] カラム のドロップダウン リストからサービス パックのバージョンとして [<not set>] を選択します。

ステップ 7 [OK] をクリックします。

アダプタ ファームウェア

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

すべての Cisco UCS ネットワーク アダプタ：

- 必要なネットワーク インターフェイス カードとホスト バス アダプタの数を削減可能
- Cisco UCS Managerソフトウェアを使用した管理
- 2 つのファブリック エクステンダと 2 つのファブリック インターコネクトを備えた冗長構成で使用可能
- 配線は初回のみ、その後はソフトウェアで機能の有効化や設定が行える「ワイヤワンス（wire-once）」アーキテクチャに対応
- ファイバ チャネル マルチパスをサポート

シスコ仮想インターフェイス カード（VIC）は、256 の仮想インターフェイスを提供し、Cisco VM-FEX テクノロジーをサポートします。Cisco VIC は、仮想化環境の実際のワークロード モビリティを実現するための I/O ポリシーの整合性と可視性を提供します。Cisco VIC は、B シリーズ ブレード サーバおよびC シリーズ ラック サーバのフォーム ファクタで使用できます。

アダプタのファームウェアのアップデート

⚠

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

Procedure

ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。

ステップ 2 **[機器（Equipment）] > [シャーシ（Chassis）] > *[シャーシ番号（Chassis Number）]* > [サーバ（Servers）]** の順に展開します。

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

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

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

ステップ 6 **[ファームウェアの更新（Update Firmware）]** ダイアログボックスで、次の操作を実行します。

a) **[バージョン（Version）]** ドロップダウン リストで、ファームウェア バージョンを選択してエンドポイントを更新します。

b) **[OK]** をクリックします。

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

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

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

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

What to do next

ファームウェアをアクティブにします。

アダプタでのファームウェアのアクティブ化

Procedure

ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。

ステップ 2 **[機器（Equipment）]** > **[シャーシ（Chassis）]** > ***[シャーシ番号（Chassis Number）]*** > **[サーバ（Servers）]** の順に展開します。

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

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

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

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

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

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

b) スタートアップバージョンを設定し、エンドポイントで実行中のバージョンを変更しない場合、**[スタートアップ バージョンのみを設定（Set Startup Version Only）]** チェックボックスをオンにします。

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

サーバがサービスプロファイルに関連付けられていない場合、アクティブ化されたファームウェアは pending-next-boot 状態のままになります。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。

c) [OK] をクリックします。

BIOS ファームウェア

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

サーバの BIOS ファームウェアのアップデート

⚠

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

手順

ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。

ステップ 2 **[機器（Equipment）]** > **[シャーシ（Chassis）]** > ***[シャーシ番号（Chassis Number）]*** > **[サーバ（Servers）]** の順に展開します。

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

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

ステップ 5 [Motherboard] タブをクリックします。

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

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

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

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

c) [OK] をクリックします。

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

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

次のタスク

ファームウェアをアクティブにします。

サーバの BIOS ファームウェアのアクティブ化

手順

ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。

ステップ 2 **[機器（Equipment）] > [シャーシ（Chassis）] > *[シャーシ番号（Chassis Number）]* > [サーバ（Servers）]** の順に展開します。

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

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

ステップ 5 [Motherboard] タブをクリックします。

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

ステップ 7 **[ファームウェアのアクティベート（Activate Firmware）]** ダイアログボックスで、次の操作を実行します。

a) **[アクティベートするバージョン（Version To Be Activated）]** ドロップダウン リストから、適切なサーバ BIOS のバージョンを選択します。

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

[スタートアップ バージョンのみを設定（Set Startup Version Only）] を設定した場合は、アクティブ化されたファームウェアが pending-next-boot 状態に移行し、サーバはすぐにはリブートされません。アクティブ化されたファームウェアは、サーバがリブートされるまでは、実行バージョンのファームウェアになりません。

c) [OK] をクリックします。

CIMC ファームウェア

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

サーバの CIMC ファームウェアのアップデート

⚠

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

Procedure

ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。

ステップ 2 **[機器（Equipment）] > [シャーシ（Chassis）] > *[シャーシ番号（Chassis Number）]* > [サーバ（Servers）]** の順に展開します。

ステップ 3 CIMC をアップデートするサーバのノードを展開します。

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

ステップ 5 [CIMC] タブをクリックします。

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

ステップ 7 **[ファームウェアの更新（Update Firmware）]** ダイアログボックスで、次の操作を実行します。

a) **[バージョン（Version）]** ドロップダウン リストで、ファームウェア バージョンを選択してエンドポイントを更新します。

b) **[OK]** をクリックします。

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

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

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

What to do next

ファームウェアをアクティブにします。

サーバの CIMC ファームウェアのアクティブ化

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

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

Procedure

ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。

ステップ 2 **[機器（Equipment）]** > **[シャーシ（Chassis）]** > ***[シャーシ番号（Chassis Number）]*** > **[サーバ（Servers）]** の順に展開します。

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

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

ステップ 5 [CIMC] タブをクリックします。

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

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

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

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

b) スタートアップバージョンを設定し、エンドポイントで実行中のバージョンを変更しない場合、**[スタートアップ バージョンのみを設定（Set Startup Version Only）]** チェックボックスをオンにします。

[スタートアップ バージョンのみを設定する（Set Startup Version Only）] を設定した場合、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、エンドポイントはすぐにはリブートされません。アクティブ化されたファームウェアは、エンドポイントがリブートされるまで、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。

c) [OK] をクリックします。

PSU ファームウェア

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

PSU でのファームウェアのアップデート

⚠

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

手順

ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。

ステップ 2 **[機器]** > **[シャーシ]**を展開します。

ステップ 3 管理する PSU に対応するシャーシを選択します。

ステップ 4 [Work] ペインの [PSUs] をクリックします。

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

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

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

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

b) **[OK]** をクリックします。

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

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

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

次のタスク

ファームウェアをアクティブにします。

PSU でのファームウェアのアクティブ化

手順

ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。

ステップ 2 **[機器]** > **[シャーシ]**を展開します。

ステップ 3 管理する PSU に対応するシャーシを選択します。

ステップ 4 [Work] ペインの [PSUs] をクリックします。

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

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

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

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

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

b) スタートアップ バージョンを設定し、エンドポイントで実行中のバージョンを変更しない場合、**[スタートアップ バージョンのみを設定（Set Startup Version Only）]** チェックボックスをオンにします。

[スタートアップ バージョンのみを設定する（Set Startup Version Only）] を設定した場合、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、エンドポイントはすぐにはリブートされません。アクティブ化されたファームウェアは、エンドポイントがリブートされるまで、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。

c) [OK] をクリックします。

ボード コントローラ ファームウェア

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

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

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

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

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

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

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

機能カタログの更新は、次の手順で適用できます。

1. 2.2(4c) インフラ/カタログまたは 2.2(5b) インフラ/カタログ ソフトウェア バンドルをダウンロードします。シスコからのソフトウェア バンドルの入手 （4 ページ） は、ソフトウェア バンドルのダウンロードに関する詳細情報を提供します。
2. カタログ バージョン 2.2(4c)T または 2.2(5b)T（または含まれているカタログ バージョン）をロードしてカタログをアクティブにします。機能カタログ更新のアクティブ化 は Cisco UCS Manager を使用した機能カタログのアクティブ化についての詳細情報を提供します。

3. 新しく挿入されたブレード サーバを停止します。
4. 以前のボード コントローラ バージョンがあるホスト ファームウェア パック ポリシーにサービス プロファイルを関連付けます。

   サービス プロファイルが更新されたホスト ファームウェア パック ポリシーに関連付けられると、誤った不一致アラート（CSCuu15465 のバグによるものなど）は発生しなくなります。
5. **[Save（保存）]** をクリックします。
6. ブレード サーバを再検出します。

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

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

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

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

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

  このアラームが表示されないようにするには、次のいずれかを行います。

  - Cisco UCS Manager カスタム ホスト ファームウェア パッケージを作成して、ボード コントローラ ファームウェアを Cisco UCS Manager 2.2(6c) への更新から除外し、古いバージョンを保持します。
  - Cisco UCS Manager インフラストラクチャ（A バンドル）をリリース 2.2(6c) にアップグレードし、『*Release Notes for Cisco UCS Manager, Release 2.2*』の表 2 の混在ファームウェア サポート マトリックスに従って、すべての Cisco UCS C220 M4 または C240 M4 サーバ上でホスト ファームウェア（C バンドル）を引き続き古いバージョンで実行します。

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

- ボード コントローラのアップグレード後に、ボード コントローラのアクティブ化ステータスに [Pending Power Cycle] が表示される場合、手動による電源の再投入が必要です。ま

た、エラーも生成されます。電源の再投入後、エラーはクリアされ、ボードコントローラのアクティブ化ステータスに [Ready] が表示されます。

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

（注） このアクティブ化手順を実行すると、サーバはリブートされます。サーバに関連付けられているサービス プロファイルにメンテナンス ポリシーが含まれているかどうかに応じて、リブートはただちに行われることがあります。ボードコントローラ ファームウェアは、Cisco UCS ドメインのアップグレードの最後の手順として、サーバ BIOS のアップグレードと同時に、サービス プロファイル内のホスト ファームウェア パッケージからアップグレードすることをお勧めします。これにより、アップグレードプロセス中にサーバをリブートしなければならない回数を減らせます。

手順

ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。

ステップ 2 **[機器]** ノードをクリックします。

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

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

Cisco UCS Manager GUI によって [ファームウェアのアクティブ化（Activate Firmware）] ダイアログボックスが開かれ、Cisco UCS ドメイン 内のすべてのエンドポイントのファームウェア バージョンが検証されます。この手順は、シャーシとサーバの数によって、数分かかることがあります。

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

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

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

ステップ 7 [OK] をクリックします。

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

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

（注） このアクティブ化手順を実行すると、サーバはリブートされます。サーバに関連付けられているサービス プロファイルにメンテナンス ポリシーが含まれているかどうかに応じて、リブートはただちに行われることがあります。ボードコントローラ ファームウェアは、Cisco UCS ドメインのアップグレードの最後の手順として、サーバ BIOS のアップグレードと同時に、サービス プロファイル内のホスト ファームウェア パッケージからアップグレードすることをお勧めします。これにより、アップグレードプロセス中にサーバをリブートしなければならない回数を減らせます。

手順

ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。

ステップ 2 **[機器]** ノードをクリックします。

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

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

Cisco UCS Manager GUI によって [ファームウェアのアクティブ化（Activate Firmware）] ダイアログボックスが開かれ、Cisco UCS ドメイン 内のすべてのエンドポイントのファームウェア バージョンが検証されます。この手順は、シャーシとサーバの数によって、数分かかることがあります。

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

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

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

ステップ 7 [OK] をクリックします。

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

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。