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

	Command or Action	Purpose
ステップ 1	UCS-A# **scope firmware**	ファームウェア モードを開始します。
ステップ 2	UCS-A /firmware # **download image** *URL*	ファームウェア バンドルをダウンロードします。シスコから提供されたダウンロード パスを使用し、次のいずれかの構文で URL を指定します。 • **ftp://** *server-ip-addr* **/** *path* • **scp://**username@server-ip-addr/path • **sftp://**username@server-ip-addr/ **/** *path* • **tftp://**server-ip-addr*:* **:** *port-num* **//** {5}path{5}

	Command or Action	Purpose
		Note [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。 • **usbA:/** *path* • **usbB:/** *path* **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。 **Note** IP アドレスではなくホスト名を使用する場合、Cisco UCS Managerで DNS サーバを設定します。
ステップ 3	リモート サーバのパスワードを入力します。	リモート サーバのユーザ名のパスワード。プロトコルが tfpt の場合、このフィールドは適用されません。
ステップ 4	UCS-A /firmware # **show download-task**	ダウンロード タスクのステータスを表示します。イメージのダウンロードが完了すると、タスク状態が Downloading から Downloaded に変更されます。CLI の表示は自動的には更新されないので、タスクのステータスに Downloaded が表示されるまで何度も **show download-task** コマンドを入力する必要があります。

	Command or Action	Purpose
ステップ 5	すべてのファームウェアバンドルがファブリック インターコネクトにダウンロードされるまで、このタスクを繰り返します。	

Example

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

```
UCS-A# scope firmware
UCS-A /firmware # download image
scp://user1@111.100.10.10/images/ucs-k9-bundle.4.0.1.988.bin
OR
download image usbB:/username/ucs-k9-bundle-b-series.4.0.1a.B.bin
UCS-A /firmware # show download-task
UCS-A /firmware #
```

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。

ファームウェア パッケージのダウンロード ステータスの表示

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

Procedure

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

Example

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

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

Download task:
File Name                                 Protocol   Server            Userid      State
---------                                 --------   ---------------   ---------   -----
ucs-mini-k9-bundle-infra.4.0.1a.A.bin  Scp       100.100.100.10    user1      Downloading

UCS-A /firmware # show download-task

Download task:
File Name                                 Protocol   Server            Userid      State
---------                                 --------   ---------------   ---------   -----
ucs-mini-k9-bundle-infra.4.0.1a.A.bin  Scp       100.100.100.10    user1      Downloading

UCS-A /firmware # show download-task

Download task:
File Name                                 Protocol   Server            Userid      State
---------                                 --------   ---------------   ---------   -----
ucs-mini-k9-bundle-infra.4.0.1a.A.bin  Scp       100.100.100.10    user1      Downloaded
```

イメージ ダウンロードのキャンセル

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

手順

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

例

次の例は、イメージのダウンロードを取り消します。

```
UCS-A# scope firmware
UCS-A /firmware # delete download-task ucs-k9-bundle-b-series.4.0.1a.B.bin
UCS-A /firmware* # commit-buffer
UCS-A /firmware*
```

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

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

Procedure

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

Example

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

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

Name                                       Type                 Version
------------------------------------------ -------------------- -------
ucs-2200.3.2.2cS2.gbin                     Chassis Adaptor      3.2(2cS2)
ucs-2200.4.0.0.46.gbin                     Chassis Adaptor      4.0(0.46)
ucs-3260.3.0.4d.gbin                       Chassis Management Controller
                                                                3.0(4d)
ucs-3260.4.0.0.149.gbin                    Chassis Management Controller
                                                                4.0(0.149)
ucs-3260.4.0.0.155.gbin                    Chassis Management Controller
                                                                4.0(0.155)
```

```
ucs-6100-k9-kickstart.5.0.3.N2.3.22cS2.gbin   Fabric Interconnect Kernel
                                                5.0(3)N2(3.22cS2)
ucs-6100-k9-kickstart.5.0.3.N2.4.00.46.gbin   Fabric Interconnect Kernel
                                                5.0(3)N2(4.00.46)
ucs-6100-k9-system.5.0.3.N2.3.22cS2.gbin      Fabric Interconnect System
                                                5.0(3)N2(3.22cS2)
ucs-6100-k9-system.5.0.3.N2.4.00.46.gbin      Fabric Interconnect System
                                                5.0(3)N2(4.00.46)
ucs-adaptor-pcie-ucsc-pcie-x710ta4.800031CA-1.812.1.gbin
                                              Adapter              800031CA-1.812.1
ucs-adaptor-pcie-ucsc-pcie-xxx710da2.8000364C-1.812.1.gbin
                                              Adapter              8000364C-1.812.1
ucs-bmc-brdprog-S3260M5.2.0.gbin              Board Controller     2.0

...
```

ファブリックインターコネクトの利用可能なすべてのパッケージの表示

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

手順

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

例

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

```
UCS-A# scope firmware
UCS-A /firmware # show package
Name                                       Version
------------------------------------------ -------
ucs-c125-bios.C125.4.0.0.15.0504180159.gbin
ucs-c125-bios.C125.4.0.0.17.0518180446.gbin
ucs-c125-k9-cimc.4.0.0.130.gbin
ucs-c125-k9-cimc.4.0.0.149.gbin
ucs-k9-bundle-c-series.3.1.3h.C.gbin       3.1(3h)C
ucs-k9-bundle-c-series.4.0.0.112.C.gbin    4.0(0.112)C
ucs-k9-bundle-c-series.4.0.0.115.C.gbin    4.0(0.115)C
ucs-k9-bundle-infra.3.2.2eS9.A.gbin        3.2(2eS9)A
ucs-k9-bundle-infra.4.0.0.57.A.gbin        4.0(0.57)A
ucs-manager-k9.4.0.0.8769.gbin
ucs-manager-k9.4.0.0.8777.gbin
ucs-manager-k9.4.0.0.8911.gbin
```

ファームウェア パッケージの内容の判断

手順

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

例

次に、ファームウェア パッケージの内容を表示する例を示します。

```
UCS-A# scope firmware
UCS-A /firmware # show package ucs-k9-bundle-infra.4.0.0.57.A.gbin expand
Package ucs-k9-bundle-infra.4.0.0.57.A.gbin:
    Images:
        ucs-2200.4.0.0.46.gbin
        ucs-6100-k9-kickstart.5.0.3.N2.4.00.46.gbin
        ucs-6100-k9-system.5.0.3.N2.4.00.46.gbin
        ucs-manager-k9.4.0.0.56b.gbin
```

ファブリック インターコネクトの空き領域のチェック

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

手順

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

例

次の例は、ファブリック インターコネクトの空き領域を表示します。

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect # show storage
Storage on local flash drive of fabric interconnect:
    Partition        Size (MBytes)    Used Percentage
    ---------------- ---------------- ---------------
    bootflash        16342            81
    opt              3873             3
    spare            5759             2
    usbdrive         Nothing          Empty
    var_sysmgr       2000             24
    var_tmp          600              2
    volatile         240              Empty
    workspace        3848             6
UCS-A /fabric-interconnect #
```

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（21 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 （29 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。

インフラストラクチャ ファームウェア パックのインストールの準備

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として / を入力します。
ステップ 2	UCS-A /org # **scope fw-infra-pack** *name*	組織インフラストラクチャ ファームウェア ポリシー モードを開始します。
ステップ 3	UCS-A /org/fw-infra-pack # **scope fw-backup-version infra**	インフラストラクチャのバックアップ ファームウェア モードを開始します。
ステップ 4	UCS A/org/fw-infra-pack/fw-backup-version # **set bundle-vers** *firmware_version*	指定のファームウェアバージョンをバックアップ インフラストラクチャ ファームウェアバージョンとして設定します。
ステップ 5	UCS-A /org/fw-infra-pack/fw-backup-version* # **commit-buffer**	トランザクションをコミットします。

例

この例では、バックアップインフラストラクチャ ファームウェアバージョンを設定する方法を示します。

```
UCS-A# scope org
UCS-A /org # scope fw-infra-pack default
UCS-A /org/fw-infra-pack # scope fw-backup-version infra
UCS-A /org/fw-infra-pack/fw-backup-version # set bundle-vers 4.0(1a)A
UCS-A /org/fw-infra-pack/fw-backup-version* # commit-buffer
```

シャーシ ファームウェア パックのインストールの準備

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として / を入力します。
ステップ 2	UCS-A /org # **scope fw-chassis-pack** *name*	組織シャーシ ファームウェア ポリシー 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/org/fw-chassis-pack # **scope fw-backup-version chassis**	シャーシのバックアップ ファームウェア モードを開始します。
ステップ 4	UCS-A /org/fw-chassis-pack/fw-backup-version # **set bundle-vers** *firmware_version*	バックアップ シャーシ ファームウェア バージョンとして指定されたファームウェアバージョンを設定します。
ステップ 5	UCS A/org/fw-chassis-pack/fw-backup-バージョン * # **commit-buffer**	トランザクションをコミットします。

例

この例では、バックアップ シャーシ ファームウェアバージョンを設定する方法を示します。

```
UCS-A# scope org
UCS-A /org # scope fw-chassis-pack default
UCS-A /org/fw-chassis-pack # scope fw-backup-version chassis
UCS-A /org/fw-chassis-pack/fw-backup-version # set bundle-vers 4.0(1a)C
UCS-A /org/fw-chassis-pack/fw-backup-version* # commit-buffer
```

インストールのブレードのホスト ファームウェア パックの準備

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として / を入力します。
ステップ 2	UCS-A /org # **scope fw-host-pack** *name*	組織ホスト ファームウェア ポリシー モードを開始します。
ステップ 3	UCS A/org/fw-host-pack # **scope fw-backup-version blade**	ブレード サーバのバックアップ ファームウェア モードを開始します。
ステップ 4	UCS-A /org/fw-host-pack/fw-backup-version # **set bundle-vers** *firmware_version*	ファームウェアバージョン ブレード サーバのバックアップのホストとして指定されたファームウェアバージョンを設定します。
ステップ 5	UCS A/org/fw-host-pack/fw-backup-バージョン * # **commit-buffer**	トランザクションをコミットします。

例

この例では、ブレード サーバのバックアップ ホスト ファームウェアバージョンを設定する方法を示します。

```
UCS-A# scope org
UCS-A /org # scope fw-host-pack default
UCS-A /org/fw-host-pack # scope fw-backup-version blade
UCS-A /org/fw-host-pack/fw-backup-version # set bundle-vers 4.0(1a)B
UCS-A /org/fw-host-pack/fw-backup-version* # commit-buffer
```

インストールのラック ホスト ファームウェア パックの準備

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として **/** を入力します。
ステップ 2	UCS-A /org # **scope fw-host-pack** *name*	組織ホスト ファームウェア ポリシー モードを開始します。
ステップ 3	UCS A/org/fw-host-pack # **scope fw-backup-version rack**	ラックマウント サーバのバックアップ ファームウェア モードを開始します。
ステップ 4	UCS-A /org/fw-host-pack/fw-backup-version # **set bundle-vers** *firmware_version*	ラックマウント サーバのバックアップのホスト ファームウェア バージョンとして指定されたファームウェアバージョンを設定します。
ステップ 5	UCS A/org/fw-host-pack/fw-backup-バージョン * # **commit-buffer**	トランザクションをコミットします。

例

この例では、ラックマウント サーバのバックアップ ホスト ファームウェア バージョンを設定する方法を示します。

```
UCS-A# scope org
UCS-A /org # scope fw-host-pack default
UCS-A /org/fw-host-pack # scope fw-backup-version rack
UCS-A /org/fw-host-pack/fw-backup-version # set bundle-vers 4.0(1a)C
UCS-A /org/fw-host-pack/fw-backup-version* # commit-buffer
```

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 Full State バックアップ ポリシーの構成 で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）は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。インフラストラクチャ ファームウェア パックの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 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。
    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 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 ポリシーの設定には、メンテナンス ポリシーに関する詳細情報と、デフォルトのメンテナンス ポリシーを **[User-Ack]** に設定する方法が掲載されています。
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詳細な情報を提供します。

3. 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（22ページ）
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 （27 ページ） は詳細情報を提供します。
8. 新しい障害を確認します。

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

（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

- にリストされているすべての前提条件を満たす必要があります。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
- 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。インフラストラクチャ ファームウェア パックの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。

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope firmware**	ファームウェア モードを開始します。
ステップ 2	UCS-A /firmware # **scope auto-install**	インフラストラクチャ ファームウェアのアップグレードの自動インストール モードを開始します。
ステップ 3	UCS A/firmware/auto-install # **install infra infra-vers** *infrastructure-bundle-version* **servicepack-vers** *servicepack-bundle-version*[**starttime** *mon dd yyyy hh min sec*[**force**] [**evacuate**] [**skipvalidation**]	インフラストラクチャ ファームウェアおよびサービス パック バンドルを更新してアクティブ化します。 即座にアップグレードを開始したくない場合は、**starttime** を使用してインフラストラクチャ ファームウェアのアップグレードをスケジュールする必要があります。**starttime** を使用する場合は、アップグレードをいつスケジュールするかを

	コマンドまたはアクション	目的
		指定するために、次の情報を入力してください。 • *mon*：jan や feb など目的の月の名前の最初の 3 文字。 • *dd*：月の目的の日（1 ～ 31）。 • *yyyy*：2012 などの目的の年（西暦）。 • *hh*：アップグレードを開始する時刻の時（0 ～ 23）。 • *min*：アップグレードを開始する時刻の分（0 ～ 60）。 • *sec*：アップグレードを開始する時刻の秒（0 ～ 60）。 互換性のない可能性や、現在実行中のタスクに関係なく、ファームウェアをアクティブにするには、**force** キーワードを使用します。 **注意** アップグレードを続行する前に、表示されたチェックリストを見直して、すべての要件が満たされていることを確認します。 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。 **evacuate** キーワードを使用して、自動インストール を経由し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を有効にします。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。

	コマンドまたはアクション	目的
		（注） 自動インストール の間に、ファブリック エバキュエーションを有効にし、ファブリック エバキュエーションが 自動インストール の前にいずれかのファブリック インターコネクトで手動で有効にされていた場合、ファブリック エバキュエーションは 自動インストール が完了した後で無効になります。
ステップ 4	（任意） UCS-A /firmware/auto-install # **install infra servicepack-vers** *servicepack-bundle-version* [**force**]	既存の基本インフラストラクチャ パック上のサービス パック バンドルを更新してアクティブ化します。

例

次に、Cisco UCS インフラストラクチャ ソフトウェア バンドル でインフラストラクチャをファームウェアにアップグレードする例を示します。

```
UCS-A# scope firmware
UCS-A /firmware # scope auto-install
UCS-A /firmware/auto-install # install infra infra-vers 4.0(1a)A
This operation upgrades firmware on UCS Infrastructure Components
(UCS manager, Fabric Interconnects and IOMs).
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup
(3) Check if Management Interface Monitoring Policy is enabled
(4) Check if there is a pending Fabric Interconnect Reboot activitiy
(5) Ensure NTP is configured
(6) Check if any hardware (fabric interconnects, io-modules, servers or adapters) is
unsupported in the target release
Do you want to proceed? (yes/no): yes

Triggering Install-Infra with:
   Infrastructure Pack Version: 4.0(1a)A
UCS-A /firmware/auto-install #
```

次に、**evacuate** オプションが有効になっている Cisco UCS インフラストラクチャ ソフトウェア バンドルでインフラストラクチャをファームウェアにアップグレードする例を示します。

```
UCS-A# scope firmware
UCS-A /firmware # scope auto-install
UCS-A /firmware/auto-install # install infra infra-vers 4.0(1a)A evacuate
```

```
This operation upgrades firmware on UCS Infrastructure Components
(UCS manager, Fabric Interconnects and IOMs).
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup
(3) Check if Management Interface Monitoring Policy is enabled
(4) Check if there is a pending Fabric Interconnect Reboot activitiy
(5) Ensure NTP is configured
(6) Check if any hardware (fabric interconnects, io-modules, servers or adapters) is
unsupported in the target release
Do you want to proceed? (yes/no): yes

Evacuate option: true
Warning: Please note that if fabric evacuation was configured ON manually on any of the
 FIs, it will be turned OFF in the process of Auto Install.

Triggering Install-Infra with:
   Infrastructure Pack Version: 4.0(1a)A
UCS-A /firmware/auto-install #
```

次に、インフラストラクチャをサービス パックのバージョンにアップグレードする例を示します。

```
UCS-A# scope firmware
UCS-A /firmware # scope auto-install
UCS-A /firmware/auto-install # install infra infra-vers 4.0(1a)A servicepack-vers 4.0(1)SP1
 force
This operation upgrades firmware on UCS Infrastructure Components
(UCS manager, Fabric Interconnects and IOMs).
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup
(3) Check if Management Interface Monitoring Policy is enabled
(4) Check if there is a pending Fabric Interconnect Reboot activitiy
(5) Ensure NTP is configured
(6) Check if any hardware (fabric interconnects, io-modules, servers or adapters) is
unsupported in the target release
Do you want to proceed? (yes/no):
```

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

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確認する前に、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

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

例

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

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

インフラストラクチャファームウェアのアップグレードのキャンセル

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

手順

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

例

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

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

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として **/** を入力します。
ステップ 2	UCS-A /org # **scope fw-infra-pack** *name*	組織インフラストラクチャ ファームウェア ポリシー モードを開始します。
ステップ 3	UCS-A /org/fw-infra-pack # **set infra-bundle-version ""**	デフォルトのインフラストラクチャパックおよびサービスパックのスタートアップ バージョンをクリアします。
ステップ 4	（任意） UCS-A /org/fw-infra-pack # **set servicepack-vers ""**	サービス パックのスタートアップ バージョンをクリアします。
ステップ 5	UCS-A /org/fw-infra-pack* # **commit-buffer**	トランザクションをコミットします。

例

次の例では、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 バージョンをクリアする方法を示します。

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

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の FSM ステータスの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope firmware**	ファームウェア モードを開始します。
ステップ 2	UCS-A /firmware # **scope auto-install**	インフラストラクチャ ファームウェアのアップグレードの自動インストール モードを開始します。
ステップ 3	UCS-A /firmware/auto-install # **show fsm status expand**	FSM のステータスを表示します。

例

次に、FSM のステータスを表示する例を示します。

```
UCS-A /firmware/auto-install # show fsm status expand

    FSM Status:

        Affected Object: sys/fw-system/fsm
        Current FSM: Deploy
        Status: Success
        Completion Time: 2017-02-03T18:02:13.699
        Progress (%): 100

        FSM Stage:

        Order  Stage Name                                Status       Try
        ------ ------------------------------------------ ------------ ---
        1      DeployWaitForDeploy                        Success      0
        2      DeployResolveDistributableNames            Skip         0
        3      DeployResolveDistributable                 Skip         0
        4      DeployResolveImages                        Skip         0
        5      DeployDownloadImages                       Skip         0
        6      DeployCopyAllImagesToPeer                  Skip         0
        7      DeployInternalBackup                       Skip         0
        8      DeployPollInternalBackup                   Success      0
        9      DeployActivateUCSM                         Skip         0
        10     DeployPollActivateOfUCSM                   Success      0
        11     DeployUpdateIOM                            Success      0
        12     DeployPollUpdateOfIOM                      Success      0
        13     DeployActivateIOM                          Success      0
        14     DeployPollActivateOfIOM                    Success      0
        15     DeployFabEvacOnRemoteFI                    Skip         0
        16     DeployPollFabEvacOnRemoteFI                Skip         0
        17     DeployActivateRemoteFI                     Success      0
        18     DeployPollActivateOfRemoteFI               Success      0
        19     DeployFabEvacOffRemoteFI                   Skip         0
        20     DeployPollFabEvacOffRemoteFI               Skip         0
        21     DeployWaitForUserAck                       Skip         0
        22     DeployPollWaitForUserAck                   Success      0
```

```
23     DeployFailOverToRemoteFI                Skip         0
24     DeployPollFailOverToRemoteFI            Skip         0
25     DeployActivateLocalFI                   Success      0
26     DeployPollActivateOfLocalFI             Success      0
27     DeployActivateUCSMServicePack           Skip         0
28     DeployPollActivateOfUCSMServicePack     Success      0
```

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 パッケージの作成または更新

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。

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。

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

	Command or Action	Purpose
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、[org-name] に / を入力します。
ステップ 2	UCS A org/ # **create fw-host-pack** パック名	ホストファームウェアパッケージを選択したパッケージ名で作成し、組織ファームウェア ホストパッケージモードを開始します。
ステップ 3	(Optional) UCS-A /org/fw-host-pack # **set descr** *description*	ホストファームウェアパッケージの説明を記入します。 **Note** 説明にスペース、特殊文字、または句読点が含まれている場合、説明を引用符で括る必要があります。引用符は、**show** コマンド出力の説明フィールドには表示されません。

	Command or Action	Purpose
ステップ 4	UCS-A org/fw-host-pack # **create pack-image** "*hw-vendor-name*" "*hw モデル*" {**adapter** |**board-controller** | **cimc** | **graphics-card** |**host-hba** |**host-hba-optionrom** |**host-nic** |**local-disk** |**raid-controller** |**server-bios**}} "*version-num*"	ホスト ファームウェア パッケージのパッケージ イメージを作成し、組織ファームウェア ホスト パッケージ イメージ モードを開始します。*hw-vendor-name* は、ベンダーのフルネームと一致する必要があり、引用符で始まって引用符で終わる必要があります。 *hw-vendor-name* および *hw-model* 値は、 **show image detail** コマンド入力時にパッケージイメージの判別を容易にするラベルです。*version-num* 値は、パッケージのイメージに使用されているファームウェアのバージョン番号を指定します。 モデルとモデル番号（PID）は、このファームウェアパッケージに関連付けられているサーバに一致する必要があります。誤ったモデルまたはモデル番号を選択すると、Cisco UCS Manager はファームウェアアップデートをインストールできません。
ステップ 5	UCS-A org/fw-host-pack # **create exclude-server-component** {**adapter** |**board-controller** |**cimc** |**flexflash-controller** |**graphics-card** |**host-hba** |**host-hba-optionrom** |**host-nic** |**host-nic-optionrom** |**local-disk** |**psu** |**raid-controller** |**sas-expander** |**server-bios** |**unspecified**}	ホストファームウェア パッケージから指定されたコンポーネントを除外します。 **Note** デフォルトでは、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ています。
ステップ 6	Required: UCS-A org/fw-host-pack # **delete exclude-server-component** {**adapter** |**board-controller** |**cimc** |**flexflash-controller** |**graphics-card** |**host-hba** |**host-hba-optionrom** |**host-nic** |**host-nic-optionrom** |**local-disk** |**psu** |**raid-controller** |**sas-expander** |**server-bios** |**unspecified**}	ホストファームウェア パッケージから指定されたコンポーネントを含めます。
ステップ 7	(Optional) UCS-A org/fw-host-pack/pack-image # **set blade-vers** *blade-version-num*	B シリーズ サーバ パッケージ イメージのバージョン番号を指定します。この番号を変更すると、サービス プロファイル経由でファームウェアを使用して、すべての B シリーズ サーバ コ

	Command or Action	Purpose
		ンポーネントのファームウェア更新が実行されます。このステップは、ホストファームウェアパッケージ更新時にのみ使用し、作成時には使用しません。 ホストファームウェアパッケージには複数のパッケージイメージを含めることができます。その他のコンポーネントについて、追加パッケージイメージを作成するには、手順 4 と 5 を繰り返します。
ステップ 8	(Optional) UCS-A org/fw-host-pack/pack-image # **set rack-vers** *rack-version-num*	C シリーズ サーバ パッケージ イメージのバージョン番号を指定します。この番号を変更すると、サービス プロファイル経由でファームウェアを使用して、すべての C シリーズ サーバ コンポーネントのファームウェア更新が実行されます。このステップは、ホストファームウェアパッケージ更新時にのみ使用し、作成時には使用しません。 ホストファームウェアパッケージには複数のパッケージイメージを含めることができます。その他のコンポーネントについて、追加パッケージイメージを作成するには、手順 4 と 5 を繰り返します。
ステップ 9	(Optional) UCS-A org/fw-host-pack/pack-image # **set servicepack-vers** *servicepack-version-num*	サービスパック バージョン番号を指定します。基本のサーバ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。 ホストファームウェアパッケージからサービスパックを削除するには、使用 "" サービスパック バージョン番号として。 サービスパックからのイメージは、ブレード パッケージまたはラック パッケージからのイメージよりも優先されます。

	Command or Action	Purpose
ステップ 10	UCS-A org/fw-host-pack/pack-image # **commit-buffer**	トランザクションをコミットします。 Cisco UCS Manager 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。

Example

次に、app1 ホスト ファームウェア パッケージを作成して、バージョン 02.00.77 ファームウェアでアダプタ パッケージイメージを作成し、トランザクションをコミットする例を示します。

```
UCS-A# scope org
UCS-A /org # create fw-host-pack app1
UCS-A /org/fw-host-pack* # set descr "This is a host firmware package example."
UCS-A /org/fw-host-pack* # create pack-image "Cisco Systems Inc" "N20-AQ0102" adapter
"02.00.77"
UCS-A /org/fw-host-pack/pack-image* # commit-buffer
UCS-A /org/fw-host-pack/pack-image #
```

次に、app1 ホスト ファームウェア パッケージからサーバ BIOS コンポーネントを除外し、トランザクションをコミットする例を示します。

```
UCS-A# scope org
UCS-A /org # enter fw-host-pack app1
UCS-A /org/fw-host-pack* # create exclude-server-component server-bios
UCS-A /org/fw-host-pack/exclude-server-component* # commit-buffer
UCS-A /org/fw-host-pack/exclude-server-component #
```

次の例では、app1 ホスト ファームウェア パッケージにサービス パックを追加し、トランザクションをコミットします。

```
UCS-A# scope org
UCS-A /org # scope fw-host-pack app1
UCS-A /org/fw-host-pack # set servicepack-vers 4.0(1)SP1
UCS-A /org/fw-host-pack* # commit-buffer
UCS-A /org/fw-host-pack #
```

次の例では、app1 ホスト ファームウェア パッケージからサービス パックを削除し、トランザクションをコミットします。

```
UCS-A# scope org
UCS-A /org # scope fw-host-pack app1
UCS-A /org/fw-host-pack # set servicepack-vers ""
UCS-A /org/fw-host-pack* # commit-buffer
UCS-A /org/fw-host-pack #
```

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。

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のファームウェア バージョンの更新時期と更新方法を指定して、デフォルトのホスト ファームウェア パックのファームウェア バージョンと一致させることができます。

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、org-name に / と入力します。
ステップ 2	UCS-A /org # **scope fw-autosync-policy**	ファームウェア自動同期ポリシー モードを開始します。
ステップ 3	UCS-A /org/fw-autosync-policy # **set auto-sync**{*user-acknowledge* | *no-actions*}	次の値のいずれかを指定してポリシーを設定します。 • [user-acknowledge]：管理者が**server** コマンド モードで検出されたサー

	コマンドまたはアクション	目的
		バを確認するまで、サーバのファームウェアは同期されません。 • [no-action]：ファームウェアのアップグレードはサーバで開始されません。 この値は、デフォルトで選択されます。
ステップ 4	UCS-A /org/fw-autosync-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、[Firmware Auto Sync Server] ポリシーを設定し、トランザクションをシステムにコミットする方法を示しています。

```
UCS-A # scope org
UCS-A /org # scope fw-autosync-policy
UCS-A /org/fw-autosync-policy # set auto-sync user-acknowledge
UCS-A /org/fw-autosync-policy* # commit-buffer
UCS-A /org/fw-autosync-policy #
```

次のタスク

値を [user-acknowledge] に設定した場合は、ファームウェアを同期させるために、保留中のサーバ アクティビティを確認する必要があります。

サーバのファームウェア自動同期の確認

ファームウェア自動同期サーバー ポリシーを [User Acknowledge] に設定した場合は、保留中のサーバ アクティビティを確認する必要があります。保留中のサーバ アクティビティを確認しないと、サーバのファームウェア バージョンまたはサーバ内のエンドポイントが更新されず、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 バージョンと一致しなくなります。

始める前に

- 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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	UCS-A /chassis # **scope server** *server ID*	サーバ コマンド モードを開始します。
ステップ 3	UCS-A /chassis/server # **fw-sync** {*acknowledge discard*}	保留中のサーバ ファームウェアの同期を確認または破棄します。
ステップ 4	UCS-A /chassis/server # **commit-buffer**	トランザクションをサーバにコミットします。

例

次の例は、保留中のサーバ ファームウェアの更新を確認して、トランザクションをコミットする方法を示しています。

```
UCS-A # scope chassis
UCS-A /chassis # scope server 1
UCS-A /chassis/server # fw-sync acknowledge
UCS-A /chassis/server* # commit-buffer
UCS-A /chassis/server #
```

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 52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

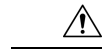
このステージでは、指定したイメージバージョン（通常はバックアップ バージョン）がスタートアップ バージョンとして設定され、[Set Startup Version Only] を指定していない場合、エンドポイントがただちにリブートされます。エンドポイントがリブートされると、バックアップ パーティションがアクティブなパーティションになり、アクティブなパーティションがバックアップ パーティションになります。新しいアクティブなパーティションのファームウェアはスタートアップ バージョンおよび実行されているバージョンになります。

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 Full State バックアップ ポリシーの構成 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）は詳細な情報を提供します。
    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 （54 ページ）
3. IOM ファームウェアをアップデートします。IOM でのファームウェアのアップデートおよびアクティブ化 （58 ページ） は、詳細情報を提供します。
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。
    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。
    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 でのファームウェアのアップデートおよびアクティブ化 （58 ページ） は、詳細情報を提供します。
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 インターコネクトのトラフィックの停止 は、詳細情報を提供します。
    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。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（61 ページ）は、詳細情報を提供します。

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 インターコネクトのトラフィックの再開 は、詳細情報を提供します。
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 は、詳細情報を提供します。

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 （63 ページ） は、詳細情報を提供します。
   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 コネクトのリブートの確認 （27 ページ） は、詳細情報を提供します。
   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。ファブリック インターコネクトのトラフィックの再開 は、詳細情報を提供します。
   6. 新しい障害を確認します。

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

Procedure

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

Example

次に、Cisco UCS Manager をアップグレードして、トランザクションをコミットする例を示します。

```
UCS-A# scope system
UCS-A# /system # show image
Name                                        Type                Version
------------------------------------------- ------------------- -------
ucs-manager-k9.4.0.1.0.bin                  System              4.0(1a)

UCS-A# /system # activate firmware 4.0(1a)
UCS-A# /system* # commit-buffer
UCS-A# /system #
```

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

	Command or Action	Purpose
ステップ 1	UCS-A# **scope firmware**	
ステップ 2	UCS A/firmware # **show image type** mgmt-service-pack	Cisco UCS Manager（システム）の使用可能なイメージを表示します。
ステップ 3	UCS-A /firmware # **exit**	
ステップ 4	UCS-A# **scope system**	システム モードを開始します。
ステップ 5	UCS-A /system # **activate service-pack** *version-num* **module security**	システムの選択されたサービス パック バージョンをアクティブにします。 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。
ステップ 6	UCS-A /system # **commit-buffer**	トランザクションをコミットします。

	Command or Action	Purpose
ステップ 7	(Optional) UCS-A /system # **show version**	システムで、サービス パック バージョンを含む、ファームウェアのバージョンの概要を示しています。

Example

次の例では、Cisco UCS Manager をバージョン 3.1(3)SP2 にアップグレードし、トランザクションをコミットします。

```
UCS-A# scope firmware
UCS-A# /firmware # show image type mgmt-service-pack
Name                                       Type                 Version
------------------------------------------ -------------------- -------
ucs-manager-k9.service-pack.3.1.3.SP1.gbin    Mgmt Service Pack    3.1(3)SP1
ucs-manager-k9.service-pack.3.1.3.SP2.gbin    Mgmt Service Pack    3.1(3)SP2
ucs-manager-k9.service-pack.3.1.4.SP1.gbin    Mgmt Service Pack    3.1(4)SP1
UCS-A# /firmware # exit
UCS-A# scope system
UCS-A# /system # activate service-pack 3.1(3)SP2 module security
As part of activation, all cli sessions will be terminated.
Continue with activation? (yes/no) yes
UCS-A# /system* # commit-buffer
UCS-A# /system # show version
UCSM:
    Running-Vers: 3.1(2.172a)
    Package-Vers: 3.1(2.173)A
    Activate-Status: Ready

UCSM Service Pack:
    Running-Vers: 3.1(3)SP2
    Running-Modules: security
    Package-Vers:
    Activate-Status: Ready


UCS-A# /system #
```

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

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **remove service-pack**	システムからのアクティブ化されたサービス パックを削除します。 システムからサービス パックを削除中には、すべての CLI セッションが終了しました。

	Command or Action	Purpose
ステップ 3	UCS-A /system # **commit-buffer**	トランザクションをコミットします。

Example

次の例では、Cisco UCS Manager からサービス パックを削除し、トランザクションをコミットします。

```
UCS-A# scope system
UCS-A# /system # remove service-pack
As part of activation, all cli sessions will be terminated.
Continue with activation? (yes/no)yes
UCS-A# /system* # commit-buffer
```

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。

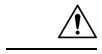
- 各 IOM は、実行中のイメージとバックアップ イメージの 2 つのイメージを格納します。
- 更新操作では、IOM のバックアップ イメージが新しいファームウェア バージョンに置き換えられます。

- 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。

IOM でのファームウェアのアップデートおよびアクティブ化

システムがハイ アベイラビリティ クラスタ設定で稼働している場合は、両方の I/O モジュールをアップデートし、アクティブにする必要があります。



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

	Command or Action	Purpose
ステップ 1	UCS-A # **scope chassis** *chassis-id*	指定したシャーシでシャーシ モードを開始します。
ステップ 2	UCS-A /chassis # **scope iom** *iom-id*	選択した I/O モジュールでシャーシ I/O モジュール モードを開始します。
ステップ 3	UCS-A /chassis/iom # **show image**	I/O モジュールの使用可能なソフトウェア イメージを表示します。

	Command or Action	Purpose
ステップ 4	UCS-A /chassis/iom # **update firmware** *version-num*	I/O モジュールの選択したファームウェア バージョンをアップデートします。
ステップ 5	(Optional) UCS-A /chassis/iom # **commit-buffer**	トランザクションをコミットします。 ステップ 7 でファームウェアをアクティブにする前に、ステップ 6 で **show firmware** コマンドを使用してファームウェアのアップデートが正常に完了したことを確認する場合のみ、このステップを使用します。このステップをスキップして、同じトランザクションで **update-firmware** および **activate-firmware** コマンドをコミットできます。ただし、ファームウェアのアップデートが正常に完了していない場合は、ファームウェアのアクティブ化が開始されません。 Cisco UCS Manager によって、選択したファームウェア イメージがバックアップ メモリ パーティションにコピーされ、そのイメージが破損していないことが確認されます。イメージは、明示的にアクティブにするまで、バックアップ バージョンとして残されます。
ステップ 6	(Optional) UCS-A /chassis/iom # **show firmware**	ファームウェアのアップデートのステータスを表示します。 ファームウェアのアップデートが正常に完了したことを確認する場合にのみ、このステップを使用します。アップデート ステータスが Ready になったら、ファームウェアのアップデートは完了です。CLI の表示は自動的には更新されないため、タスクのステータスが Updating から Ready に変更されるまで何度も **show firmware** コマンドを入力する必要がある場合があります。アップデート ステータスが Ready になったらステップ 7 に進みます。
ステップ 7	UCS-A /chassis/iom # **activate firmware** *version-num* [**set-startup-only**]	I/O モジュールの選択したファームウェア バージョンをアクティブにします。

	Command or Action	Purpose
		ファブリック インターコネクトがそのデータ パスでリブートする場合にのみ I/O モジュールをリブートする場合、**set-startup-only** キーワードを使用します。 **set-startup-only** キーワードを使用しない場合、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。さらに、Cisco UCS Manager は I/O モジュールとの間でプロトコルとファームウェア バージョンの不一致を検出すると、一致するファームウェア バージョンで I/O モジュールをアップデートし、ファームウェアをアクティブにし、再度 I/O モジュールをリブートします。
ステップ 8	UCS-A /chassis/iom # **commit-buffer**	トランザクションをコミットします。
ステップ 9	(Optional) UCS-A /chassis/iom # **show firmware**	ファームウェアのアクティベーションのステータスを表示します。 ファームウェアのアクティベーションが正常に完了したことを確認する場合にのみ、このステップを使用します。CLIの表示は自動的には更新されないため、タスクのステータスが Activating から Ready に変更されるまで何度も **show firmware** コマンドを入力する必要がある場合があります。

Example

次の例では、同じトランザクションで I/O モジュールのファームウェアをアップデートしてアクティブ化します。ファームウェアのアップデートとアクティベーションが正常に完了したかどうかについて確認は行いません。

```
UCS-A# scope chassis 1
UCS-A# /chassis # scope iom 1
UCS-A# /chassis/iom # show image
Name                                       Type                 Version
------------------------------------------ -------------------- -------
ucs-2200.4.0.0.332.bin                     IOM                  4.0(1a)

UCS-A# /chassis/iom # update firmware 4.0(1a)
UCS-A# /chassis/iom* # activate firmware 4.0(1a) set-startup-only
UCS-A# /chassis/iom* # commit-buffer
UCS-A# /chassis/iom #
```

次の例では、I/Oモジュールのファームウェアをアップデートし、アップデートが正常に完了したことを確認してからファームウェアのアクティベーションを開始して、I/Oモジュールのファームウェアをアクティブ化し、アクティベーションが正常に完了したことを確認します。

```
UCS-A# scope chassis 1
UCS-A# /chassis # scope iom 1
UCS-A# /chassis/iom # show image
Name                                       Type                Version
------------------------------------------ ------------------- -------
ucs-2200.4.0.0.332.bin                     IOM                 4.0(1)

UCS-A# /chassis/iom # update firmware 4.0(1)
UCS-A# /chassis/iom* # commit-buffer
UCS-A# /chassis/iom # show firmware
IOM      Fabric ID Running-Vers    Update-Status   Activate-Status
-------- --------- --------------- --------------- ---------------
       1 A         4.0(1)          Updating        Ready

UCS-A# /chassis/iom # show firmware
IOM      Fabric ID Running-Vers    Update-Status   Activate-Status
-------- --------- --------------- --------------- ---------------
       1 A         4.0(1)          Ready           Ready

UCS-A# /chassis/iom # activate firmware 4.0(1) ignorecompcheck
UCS-A# /chassis/iom* # commit-buffer
UCS-A# /chassis/iom # show firmware
IOM      Fabric ID Running-Vers    Update-Status   Activate-Status
-------- --------- --------------- --------------- ---------------
       1 A         4.0(1)          Ready           Activating

UCS-A# /chassis/iom # show firmware
IOM      Fabric ID Running-Vers    Update-Status   Activate-Status
-------- --------- --------------- --------------- ---------------
       1 A         4.0(1)          Ready           Ready
```

ファブリック インターコネクトのファームウェア

ファブリック インターコネクトでのファームウェアのアクティブ化

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

単一のファブリック インターコネクトのスタンドアロン 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

	Command or Action	Purpose
ステップ 1	UCS-A# **scope fabric-interconnect** {**a** | **b**}	指定したファブリック インターコネクトのファブリック インターコネクト モードを開始します。
ステップ 2	UCS-A /fabric-interconnect # **show image**	ファブリック インターコネクトの利用可能なソフトウェア イメージを表示します。
ステップ 3	UCS-A /fabric-interconnect # **activate firmware** {**kernel-version** *kernel-ver-num* | **system-version** *system-ver-num*}	ファブリック インターコネクトの選択されたファームウェア バージョンをアクティブにします。 **Note** kernel-version と system-version は、同じである必要があります。
ステップ 4	UCS-A /fabric-interconnect # **commit-buffer**	トランザクションをコミットします。 Cisco UCS Manager はファームウェアの更新とアクティベーションを実行してから、ファブリックインターコネクトと、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。

Example

次の例では、ファブリック インターコネクトをバージョン 5.0(3)N2(3.10.123) にアップグレードし、トランザクションをコミットします。

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect # show image
Name                                       Type                 Version
------------------------------------------ -------------------- -------
```

```
ucs-6300-k9-kickstart.5.0.3.N2.3.10.123.bin   Fabric Interconnect Kernel
                                                5.0(3)N2(3.10.123)
ucs-6300-k9-system.5.0.3.N2.3.10.123.bin      Fabric Interconnect System
                                                5.0(3)N2(3.10.123)

UCS-A /fabric-interconnect # activate firmware kernel-version 5.0(3)N2(3.10.123)
system-version 5.0(3)N2(3.10.123)
UCS-A /fabric-interconnect* # commit-buffer
UCS-A /fabric-interconnect #
```

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。
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

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope firmware**	
ステップ 2	UCS A/firmware # **show image type** fabric-interconnect-service-pack	ファブリック インターコネクトの使用可能なサービスパックが表示されます。
ステップ 3	UCS-A /firmware # **exit**	
ステップ 4	UCS-A# **scope fabric-interconnect** {**a** | **b**}	fabric-interconnect モードを開始します。
ステップ 5	UCS-A /fabric-interconnect # **activate service-pack** *version-num* [**security**]	システムの選択されたサービス パック バージョンをアクティブにします。

	Command or Action	Purpose
		Note 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。
ステップ 6	UCS-A /fabric-interconnect # **commit-buffer**	トランザクションをコミットします。
ステップ 7	(Optional) UCS-A /fabric-interconnect # **show version**	ファブリック インターコネクトで、サービス パック バージョンを含む、ファームウェアのバージョンの概要を示しています。

Example

次に、ファブリック インターコネクトをアップグレードして、トランザクションをコミットする例を示します。

```
UCS-A# scope firmware
UCS-A# /firmware # show image type fabric-interconnect-service-pack
Name                                       Type                  Version
------------------------------------------ --------------------- -------
ucs-6400-servicepack.4.0.1.SP1.gbin        Fabric Interconnect Service Pack
                                                                  4.0(1)SP1
ucs-6400-servicepack.4.0.1.SP2.gbin        Fabric Interconnect Service Pack
                                                                  4.0(1)SP2
ucs-6300-servicepack.4.0.1.SP1.gbin        Fabric Interconnect Service Pack
                                                                  4.0(1)SP1
ucs-6300-servicepack.4.0.1.SP2.gbin        Fabric Interconnect Service Pack
                                                                  4.0(1)SP2
ucs-mini-servicepack.4.0.1.SP1.gbin        Fabric Interconnect Service Pack
                                                                  4.0(1)SP1
ucs-mini-servicepack.4.0.1.SP2.gbin        Fabric Interconnect Service Pack
                                                                  4.0(1)SP2

UCS-A# /firmware # exit
UCS-A# scope fabric-interconnect a
UCS-A# /fabric-interconnect # activate service-pack 4.0(1)SP0 security
UCS-A# /fabric-interconnect* # commit-buffer
UCS-A# /fabric-interconnect # show version
 Fabric Interconnect A:
    Running-Kern-Vers: 7.0(3)N2(4.00.226)
    Running-Sys-Vers: 7.0(3)N2(4.00.226)
    Running-Service-Pack-Vers: 4.0(1)SP0(Default)
    Package-Vers: 4.0(0.147)A
    Package-Service-Pack-Vers:
    Startup-Kern-Vers: 7.0(3)N2(4.00.226)
```

```
Startup-Sys-Vers: 7.0(3)N2(4.00.226)
Startup-Service-Pack-Vers: 4.0(1)SP0(Default)
Act-Kern-Status: Ready
Act-Sys-Status: Ready
Act-Service-Pack-Status: Ready
Bootloader-Vers: v05.28(01/18/2018)
```

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

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。

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope fabric-interconnect** {**a** | **b**}	fabric-interconnect モードを開始します。
ステップ 2	UCS-A /fabric-interconnect # **remove service-pack security**	ファブリック インターコネクトからアクティベート済みサービス パックを削除します。
ステップ 3	UCS-A /fabric-interconnect # **commit-buffer**	トランザクションをコミットします。

Example

次に、ファブリック インターコネクトからサービス パックを削除し、トランザクションをコミットする例を示します。

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

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。

アダプタでのファームウェアのアップデートおよびアクティブ化

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

	Command or Action	Purpose
ステップ 1	UCS-A# **scope adapter** *chassis-id / blade-id / adapter-id*	指定したアダプタでシャーシ サーバ アダプタ モードを開始します。
ステップ 2	UCS-A /chassis/server/adapter # **show image**	アダプタの使用可能なソフトウェア イメージを表示します。
ステップ 3	UCS-A /chassis/server/adapter # **update firmware** *version-num*	アダプタの選択したファームウェアバージョンをアップデートします。
ステップ 4	(Optional) UCS-A /chassis/server/adapter # **commit-buffer**	トランザクションをコミットします。 ステップ 6 でファームウェアをアクティブにする前に、ステップ 5 で **show firmware** コマンドを使用してファームウェアのアップデートが正常に完了したことを確認する場合のみ、このステップを使用します。このステップをスキップして、同じトランザクションで **update-firmware** および **activate-firmware** コマンドをコミットできます。ただし、ファームウェアのアップデートが正常に完了していない場合は、ファームウェアのアクティブ化が開始されません。

	Command or Action	Purpose
		Cisco UCS Manager によって、選択したファームウェア イメージがバックアップ メモリ パーティションにコピーされ、そのイメージが破損していないことが確認されます。イメージは、明示的にアクティブにするまで、バックアップ バージョンとして残されます。
ステップ 5	(Optional) UCS-A /chassis/server/adapter # **show firmware**	ファームウェアのアップデートのステータスを表示します。 ファームウェアのアップデートが正常に完了したことを確認する場合にのみ、このステップを使用します。アップデート ステータスが Ready になったら、ファームウェアのアップデートは完了です。CLI の表示は自動的には更新されないため、タスクのステータスが Updating から Ready に変更されるまで何度も **show firmware** コマンドを入力する必要がある場合があります。アップデート ステータスが Ready になったらステップ 6 に進みます。
ステップ 6	UCS-A /chassis/server/adapter # **activate firmware** *version-num* [**set-startup-only**]	アダプタの選択したファームウェア バージョンをアクティブにします。 アクティブ化したファームウェアを pending-next-boot 状態にし、サーバをただちにリブートしない場合は、**set-startup-only** キーワードを使用します。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は **set-startup-only** キーワードは使用できません。
ステップ 7	UCS-A /chassis/server/adapter # **commit-buffer**	トランザクションをコミットします。 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

	Command or Action	Purpose
		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。
ステップ 8	(Optional) UCS-A /chassis/server/adapter # **show firmware**	ファームウェアのアクティベーションのステータスを表示します。 ファームウェアのアクティベーションが正常に完了したことを確認する場合にのみ、このステップを使用します。CLIの表示は自動的には更新されないため、タスクのステータスが Activating から Ready に変更されるまで何度も **show firmware** コマンドを入力する必要がある場合があります。

Example

次に、ファームウェアのアップデートおよびファームウェアのアクティベーションが正常に完了したことを確認せずに、同じトランザクションでアダプタのファームウェアをバージョン 4.1(0.123) にアップデートし、アクティブ化する例を示します。

```
UCS-A# scope adapter 1/1/1
UCS-A# /chassis/server/adapter # show image
Name                                       Type                Version
------------------------------------------ ------------------- -------
ucs-m82-8p-vic.4.1.0.123.bin               Adapter             4.1(0.123)

UCS-A# /chassis/server/adapter # update firmware 4.1(0.123)
UCS-A# /chassis/server/adapter* # activate firmware 4.1(0.123) set-startup-only
UCS-A# /chassis/server/adapter* # commit-buffer
UCS-A# /chassis/server/adapter #
```

次に、アダプタのファームウェアをバージョン 4.1(0.123) にアップデートし、ファームウェアのアクティベーションを開始する前にファームウェアのアップデートが正常に完了したことを確認し、アダプタのファームウェアをアクティブにし、ファームウェアのアクティベーションが正常に完了したことを確認する例を示します。

```
UCS-A# scope adapter 1/1/1
UCS-A# /chassis/server/adapter # show image
Name                                       Type                Version
------------------------------------------ ------------------- -------
ucs-m82-8p-vic.4.1.0.123.bin               Adapter             4.2(1.13)

UCS-A# /chassis/server/adapter # update firmware 4.2(3.13)
```

```
UCS-A# /chassis/server/adapter* # commit-buffer
UCS-A# /chassis/server/adapter # show firmware
Adapter 1:
    Running-Vers: 4.2(3.13)
    Package-Vers: 4.0(0.128)B
    Update-Status: Updating
    Activate-Status: Ready

UCS-A# /chassis/server/adapter # show firmware
Adapter 1:
    Running-Vers: 4.2(3.13)
    Package-Vers: 4.0(0.128)B
    Update-Status: Ready
    Activate-Status: Ready

UCS-A# /chassis/server/adapter # activate firmware 4.2(3.13)
Warning: When committed this command will reset the end-point
UCS-A# /chassis/server/adapter* # commit-buffer
UCS-A# /chassis/server/adapter # show firmware
Adapter 1:
    Running-Vers: 4.2(3.13)
    Package-Vers: 4.0(0.128)B
    Update-Status: Ready
    Activate-Status: Activating

UCS-A# /chassis/server/adapter # show firmware
Adapter 1:
    Running-Vers: 4.2(3.13)
    Package-Vers: 4.0(0.128)B
    Update-Status: Ready
    Activate-Status: Pending Next Boot

UCS-A# /chassis/server/adapter # exit
UCS-A# /chassis/server # cycle cycle-immediate
UCS-A# /chassis/server* # commit-buffer
UCS-A# /chassis/server # scope adapter 1
UCS-A# /chassis/server/adapter # show firmware
Adapter 1:
    Running-Vers: 4.2(3.13)
    Package-Vers: 4.0(0.128)B
    Update-Status: Ready
    Activate-Status: Ready
UCS-A# /chassis/server/adapter #
```

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 ファームウェアの更新とアクティブ化

重要 すべての M3 世代以降のサーバで、Cisco UCS Manager CLI を使用し、サーバの BIOS ファームウェアを更新してアクティブ化できます。以前のサーバでは、Cisco UCS Manager CLI による BIOS ファームウェアの更新はサポートされていません。

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *chassis-id* / *blade-id*	指定サーバーのシャーシ サーバー モードを開始します。
ステップ 2	UCS-A /chassis/server # scope bios	シャーシ サーバ BIOS モードを開始します。
ステップ 3	UCS-A /chassis/server/bios # **show image**	使用可能な BIOS ファームウェア イメージを表示します。
ステップ 4	UCS-A /chassis/server/bios # **update firmware** バージョン番号	サーバの選択した BIOS ファームウェアを更新します。
ステップ 5	（任意） UCS-A /chassis/server/bios # **commit-buffer**	トランザクションをコミットします。 ステップ 7 でファームウェアをアクティブにする前に、ステップ 6 で **show firmware** コマンドを使用してファームウェアのアップデートが正常に完了したことを確認する場合のみ、このステップを使用します。このステップをスキップして、同じトランザクションで **update-firmware** および **activate-firmware** コマンドをコミットできます。ただし、ファームウェアのアップデートが正常に完了していない場合は、ファームウェアのアクティブ化が開始されません。

	コマンドまたはアクション	目的
		Cisco UCS Manager によって、選択したファームウェア イメージがバックアップ メモリ パーティションにコピーされ、そのイメージが破損していないことが確認されます。イメージは、明示的にアクティブにするまで、バックアップ バージョンとして残されます。
ステップ 6	（任意） UCS-A /chassis/server/bios # **show firmware**	ファームウェアのアップデートのステータスを表示します。 ファームウェアのアップデートが正常に完了したことを確認する場合にのみ、このステップを使用します。アップデート ステータスが Ready になったら、ファームウェアのアップデートは完了です。CLI の表示は自動的には更新されないため、タスクのステータスが Updating から Ready に変更されるまで何度も **show firmware** コマンドを入力する必要がある場合があります。アップデート ステータスが Ready になったらステップ 7 に進みます。
ステップ 7	UCS-A /chassis/server/bios # **activate firmware** バージョン番号	選択したサーバ BIOS ファームウェア バージョンをアクティブにします。
ステップ 8	UCS-A /chassis/server/bios # **commit-buffer**	トランザクションをコミットします。
ステップ 9	（任意） UCS A/シャーシ/bios #**show firmware**	ファームウェアのアクティベーションのステータスを表示します。 ファームウェアのアクティベーションが正常に完了したことを確認する場合にのみ、このステップを使用します。CLI の表示は自動的には更新されないため、タスクのステータスが Activating から Ready に変更されるまで何度も **show firmware** コマンドを入力する必要がある場合があります。

例

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

```
UCS-A# scope server 1/1
UCS-A# /chassis/server # scope bios
UCS-A# /chassis/server/bios # show image
Name                                        Type                Version
------------------------------------------- ------------------- -------
ucs-b200-m2-bios.S5500.2.1.3c.0.081120151437.bin
                                            Server BIOS
S5500.2.1.3c.0.081120151437
ucs-b200-m3-bios.B200M3.2.2.6c.0.110420151250.bin
                                            Server BIOS
B200M3.2.2.6c.0.110420151250
ucs-b200-m4-bios.B200M4.3.1.0.4.113020151739.bin
                                            Server BIOS
B200M4.3.1.0.4.113020151739

UCS-A# /chassis/server/bios # update firmware B200M4.3.1.0.4.113020151739
UCS-A# /chassis/server/bios* # activate firmware B200M4.3.1.0.4.113020151739
UCS-A# /chassis/server/bios* # commit-buffer
UCS-A# /chassis/server/bios #
```

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およびアクティブ化

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

	Command or Action	Purpose
ステップ 1	UCS-A# **scope server** *chassis-id* / *blade-id*	指定サーバーのシャーシ サーバー モードを開始します。
ステップ 2	UCS-A /chassis/server # **scope cimc**	シャーシ サーバー CIMC モードを開始します。
ステップ 3	UCS-A /chassis/server/cimc # **show image**	アダプタの使用可能なソフトウェア イメージを表示します。
ステップ 4	UCS-A /chassis/server/cimc # **update firmware** バージョン番号	サーバの CIMC の選択したファームウェア バージョンをアップデートします。
ステップ 5	(Optional) UCS-A /chassis/server/cimc # **commit-buffer**	トランザクションをコミットします。 ステップ 7 でファームウェアをアクティブにする前に、ステップ 6 で **show firmware** コマンドを使用してファームウェアのアップデートが正常に完了したことを確認する場合のみ、このステップを使用します。このステップをスキップして、同じトランザクションで **update-firmware** および **activate-firmware** コマンドをコミットできます。ただし、ファームウェアのアップデートが正常に完了していない場合は、ファームウェアのアクティブ化が開始されません。 Cisco UCS Manager によって、選択したファームウェア イメージがバックアップ メモリ パーティションにコピーされ、そのイメージが破損していないことが確認されます。イメージは、明示的にアクティブにするまで、バックアップ バージョンとして残されます。
ステップ 6	(Optional) UCS-A /chassis/server/cimc # **show firmware**	ファームウェアのアップデートのステータスを表示します。 ファームウェアのアップデートが正常に完了したことを確認する場合にのみ、このステップを使用します。アップデート ステータスが Ready になったら、ファームウェアのアップデートは完了です。CLI の表示は自動的には更新されないた

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

Example

次の例では、同じトランザクションで CIMC のファームウェアをアップデートしてアクティブ化します。ファームウェアのアップデートとアクティベーションが正常に完了したかどうかについて確認は行いません。

```
UCS-A# scope server 1/1
UCS-A# /chassis/server # scope cimc
UCS-A# /chassis/server/cimc # show image
Name                                       Type                Version
------------------------------------------ ------------------- -------
ucs-b200-m3-k9-cimc.4.0.1.bin              CIMC                4.0(1)
ucs-b200-m3-k9-cimc.4.0.1.bin              CIMC                4.0(1)
ucs-b200-m4-k9-cimc.4.0.1.bin              CIMC                4.0(1)
ucs-b200-m5-k9-cimc.4.0.1.bin              CIMC                4.0(1)
ucs-b22-m3-k9-cimc.4.0.1.bin               CIMC                4.0(1)

...

UCS-A# /chassis/server/cimc # update firmware 4.0(1)
UCS-A# /chassis/server/cimc* # activate firmware 4.0(1) set-startup-only
UCS-A# /chassis/server/cimc* # commit-buffer
UCS-A# /chassis/server/cimc #
```

次の例では、CIMC のファームウェアをアップデートし、アップデートが正常に完了したことを確認してからファームウェアのアクティベーションを開始して、CIMC のファームウェアをアクティブ化し、アクティベーションが正常に完了したことを確認します。

```
UCS-A# scope server 1/1
UCS-A# /chassis/server # scope cimc
UCS-A# /chassis/server/cimc # show image
Name                                        Type              Version
------------------------------------------- ----------------- -------------
ucs-b200-m1-k9-cimc.4.0.1.bin               CIMC                 4.0(1)
ucs-b200-m1-k9-cimc.4.0.1.bin               CIMC                 4.0(1)
ucs-b200-m1-k9-cimc.4.0.1.bin               CIMC                 4.0(1)
ucs-b200-m3-k9-cimc.4.0.1.bin               CIMC                 4.0(1)
...

UCS-A# /chassis/server/cimc # update firmware 4.0(1)
UCS-A# /chassis/server/cimc* # commit-buffer
UCS-A# /chassis/server/cimc # show firmware
Running-Vers    Update-Status   Activate-Status
--------------- --------------- ---------------
4.0(1)          Updating        Ready

UCS-A# /chassis/server/cimc # show firmware
Running-Vers    Update-Status   Activate-Status
--------------- --------------- ---------------
4.0(1)          Ready           Ready

UCS-A# /chassis/server/cimc # activate firmware 4.0(1)
UCS-A# /chassis/server/cimc* # commit-buffer
UCS-A# /chassis/server/cimc # show firmware
Running-Vers    Update-Status   Activate-Status
--------------- --------------- ---------------
4.0(1)          Ready           Activating

UCS-A# /chassis/server/cimc # show firmware
Running-Vers    Update-Status   Activate-Status
--------------- --------------- ---------------
4.0(1)          Ready           Ready
```

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope chassis** *chassis-id*	指定したシャーシでシャーシ モードを開始します。
ステップ 2	UCS-A /chassis # **scope psu** *psu-id*	指定した PSU で PSU モードを開始します。
ステップ 3	UCS-A /chassis/psu # **show detail**	PSU の使用可能なソフトウェア イメージを表示します。
ステップ 4	UCS-A /chassis/psu # **update firmware** *version-num* [**force**]	PSUの選択したファームウェアバージョンを更新します。 互換性のない可能性や、現在実行中のタスクに関係なく、ファームウェアをアクティブにするには、オプションの **force** キーワードを使用できます。 **注意** アップグレードを続行する前に、表示されたチェックリストを見直して、すべての要件が満たされていることを確認します。
ステップ 5	（任意） UCS-A /chassis/psu # **commit-buffer**	トランザクションをコミットします。 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。

例

次の例では、PSU ファームウェアを更新し、トランザクションをコミットする方法を示します。

```
UCS-A# scope chassis 1
UCS-A# /chassis # scope psu 2
UCS-A# /chassis/psu # show detail
PSU:
    PSU: 2
    Overall Status: Operable
    Operability: Operable
    Threshold Status: OK
```

```
    Power State: On
    Presence: Equipped
    Thermal Status: OK
    Voltage Status: OK
    Product Name: Platinum II AC Power Supply for UCS 5108 Chassis
    PID: UCSB-PSU-2500ACDV
    VID: V01
    Part Number: 341-0571-01
    Vendor: Cisco Systems Inc
    Serial (SN): DTM190304FD
    HW Revision: 0
    Firmware Version: 05.10
    Type: DV
    Wattage (W): 2500
    Input Source: 210AC 50 380DC
    Current Task:
UCS-A# /chassis/psu # update firmware 05.10
UCS-A# /chassis/psu* # commit-buffer
UCS-A# /chassis/psu #
```

PSU でのファームウェアのアクティブ化

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope chassis** *chassis-id*	指定したシャーシでシャーシ モードを開始します。
ステップ 2	UCS-A /chassis # **scope psu** *psu-id*	指定した PSU で PSU モードを開始します。
ステップ 3	UCS-A /chassis/psu # **activate firmware** *version-num*	PSU の選択したファームウェア バージョンをアクティブにします。
ステップ 4	必須: UCS-A /chassis/psu # **commit-buffer**	トランザクションをコミットします。 （注） トランザクションのコミットによりエンドポイントがリセットされます。

例

次の例では、PSU ファームウェアをアクティブにし、トランザクションをコミットします。

```
UCS-A# scope chassis 1
UCS-A# /chassis # scope psu 2
UCS-A# /chassis/psu # activate firmware 03.10
Warning: When committed this command will reset the end-point
UCS-A# /chassis/psu* # commit-buffer
UCS-A# /chassis/psu #
```

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 および M4 ブレード サーバのボード コントローラ ファームウェアのアクティブ化に関する注意事項

次の注意事項は、Cisco UCS B シリーズ M3 および M4 ブレード サーバのボード コントローラ ファームウェアに適用されます。

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

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

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

機能カタログの更新は、次の手順で適用できます。

1. 2.2(4c) Infra/Catalog または 2.2(5b) Infra/Catalog ソフトウェア バンドルをダウンロードします。
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 および M4 ラック サーバのボード コントローラ ファームウェアのアクティ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 および M4 ラック サーバのボード コントローラ ファームウェアに適用されます。

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

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

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

  このアラームが表示されないようにするには、次のいずれかを行います。

  - Cisco UCS Manager カスタム ホスト ファームウェア パッケージを作成して、ボード コントローラ ファームウェアを Cisco UCS Manager 2.2(6c) への更新から除外し、古いバージョンを保持します。
  - Cisco UCS Manager インフラストラクチャ（A バンドル）をリリース 2.2(6c) にアップグレードし、『*Release Notes for Cisco UCS Manager, Release 2.2*』の表 2 の混在ファー

ムウェア サポート マトリックスに従って、すべての Cisco UCS C220 M4 または C240 M4 サーバ上でホスト ファームウェア（C バンドル）を引き続き古いバージョンで実行します。

（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

ボード コントローラ ファームウェアは、eUSB、LED、I/O コネクタなど、サーバの多くの機能を制御します。

（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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *chassis-id / server-id*	指定サーバーのシャーシ サーバー モードを開始します。
ステップ 2	UCS-A /chassis/server # **scope boardcontroller**	サーバのボード コントローラ モードを開始します。
ステップ 3	（任意） UCS-A /chassis/server/boardcontroller # **show image**	ボード コントローラの利用可能なソフトウェア イメージを表示します。
ステップ 4	（任意） UCS-A /chassis/server/boardcontroller # **show firmware**	ボード コントローラの現在実行中のソフトウェア イメージを表示します。

	コマンドまたはアクション	目的
ステップ 5	UCS-A /chassis/server/boardcontroller # **activate firmware** バージョン番号	サーバのボード コントローラの選択されたファームウェア バージョンをアクティブ化します。
ステップ 6	UCS-A /chassis/server/boardcontroller # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、ボード コントローラのファームウェアをアクティブ化します。

```
UCS-A# scope server 1/1
UCS-A# /chassis/server # scope boardcontroller
UCS-A# /chassis/server/boardcontroller # show image
Name                                       Type                Version
------------------------------------------ ------------------- -------
ucs-b200-m3-brdprog.15.0.bin               Board Controller    15.0
ucs-b22-m3-brdprog.16.0.bin                Board Controller    16.0
ucs-b420-m3-brdprog.12.0.bin               Board Controller    12.0

UCS-A# /chassis/server/boardcontroller # show firmware
BoardController:
    Running-Vers: 15.0
    Package-Vers: 3.2(1)B
    Activate-Status: Ready

UCS-A# /chassis/server/boardcontroller # activate firmware 15.0
UCS-A# /chassis/server/boardcontroller* # commit-buffer
```

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

ボード コントローラ ファームウェアは、eUSB、LED、I/O コネクタなど、サーバの多くの機能を制御します。

（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。

M3 以降のボード コントローラ ファームウェアには次のような制限があります。

- Cisco UCS ManagerRelease 2.2(1a) 以降を使用している必要がある。

- 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。
- 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。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *server-id*	指定サーバのシャーシ サーバ モードを開始します。
ステップ 2	UCS-A /server # **scope boardcontroller**	サーバのボード コントローラ モードを開始します。
ステップ 3	（任意） UCS-A /server/boardcontroller # **show image**	ボード コントローラの利用可能なソフトウェア イメージを表示します。
ステップ 4	（任意） UCS-A /server/boardcontroller # **show firmware**	ボード コントローラの現在実行中のソフトウェア イメージを表示します。
ステップ 5	UCS-A /server/boardcontroller # **activate firmware** *version-num*	サーバのボード コントローラの選択されたファームウェア バージョンをアクティブ化します。
ステップ 6	UCS-A /server/boardcontroller # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、ボード コントローラのファームウェアをアクティブ化します。

```
UCS-A# scope server 7
UCS-A# /server # scope boardcontroller
UCS-A# /server/boardcontroller # show image
Name                                     Type              Version     State
---------------------------------------- ----------------- ---------   -----
ucs-c220-m3-brdprog.3.0.bin           Board Controller    3.0      Active
ucs-c220-m3-brdprog.3.0.bin           Board Controller    3.0       Active

UCS-A# /server/boardcontroller # show firmware
BoardController:
    Running-Vers: N/A
    Package-Vers:
    Activate-Status: Ready

UCS-A# /server/boardcontroller # activate firmware 3.0 force
Warning: When committed this command will reset the end-point.
```

```
UCS-A# /server/boardcontroller* # commit-buffer
```

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。