ガイドラインと前提条件

ファームウェアアップグレードに関するガイドラインとベスト プラクティス

Cisco UCS ドメインのエンドポイントのファームウェアをアップグレードする前に、次の注意事項、ベスト プラクティス、および制約事項を考慮してください。

設定の変更とアップグレードに影響を与える可能性がある設定

Cisco UCS ドメインの設定によっては、アップグレードプロセスで追加の変更が必要な場合があります。

デフォルトのメンテナンス ポリシーの設定を「ユーザ確認応答」にする

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

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

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

注意 Cisco UCS の 1.4 以前のリリースでは、イーサネット VLAN、FCoE VLAN は重複 VLAN ID を持つことができました。しかし、Cisco UCS リリース 2.0 以降では、VLAN ID の重複は許可されません。Cisco UCS Manager は、アップグレードの間に VLAN ID の重複を検出すると、深刻な障害と見なします。VLAN ID を再設定しない場合、Cisco UCS Manager によって重大なエラーが生成され、重複している VLAN からのイーサネット トラフィックが破棄されます。そのため、イーサネットと FCoE の VLAN ID が重複していないことを確認してから、Cisco UCS リリース 3.1 以降にアップグレードすることをお勧めします。

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

Cisco UCS リリース 3.1 以降の新規インストールでは、デフォルトの VLAN ID は次のようになります。

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

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

予約済み範囲の ID を持つ VSAN は正常に動作しない

予約範囲の ID を持つ VSAN は、アップグレード後に正常に動作しません。次を実行して、Cisco UCS Manager で設定されている VSAN が予約済み範囲に含まれないようにします。

- Cisco UCS ドメイン で FC スイッチ モードを使用する予定の場合は、ID が 3040 ～ 4078 の範囲にある VSAN を設定しないでください。
- Cisco UCS ドメイン で FC エンドホスト モードを使用する予定の場合、ID が 3840 ～ 4079 の範囲にある VSAN を設定しないでください。

VSAN に予約済み範囲の ID がある場合は、その VSAN ID を、使用または予約されていない VSAN ID に変更します。

ファームウェアアップグレードに関するハードウェア関連のガイドライン

Cisco UCS ドメイン のハードウェアはアップグレード方法に影響を与えることがあります。エンドポイントをアップグレードする前に、次の注意事項および制約事項を考慮してください。

サーバまたはシャーシのメンテナンスなし

⚠

注意 更新プロセスが完了するまで、エンドポイントがあるハードウェアを取り外したり、そこで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。

アップグレードの実施前や実施中に RAID 構成ハードディスクを交換しない

Cisco UCS インフラストラクチャやサーバ ファームウェアのアップグレードの実施前および実施中は、以下を順守してください。

- サーバのローカル ストレージ（ハード ディスクや SSD）の取り外し、挿入、交換を行わない。
- リビルド、アソシエーション、コピーバック、BGI など、ストレージ操作が実行されていないことを確認する。

サードパーティ アダプタは必ずホスト ファームウェア パッケージによってアップグレードする

サードパーティ アダプタは、エンドポイントから直接アップグレードできません。このようなアダプタのファームウェアは、ホスト ファームウェア パッケージを使用してアップグレードする必要があります。

ファブリック インターコネクトの設定

クラスタ化されたファブリック インターコネクトは、データ パスの冗長性を意図的に提供します。ただし、データ トラフィックが中断されないように、サービス プロファイルに冗長イーサネットおよびストレージ（FC/FCoE）インターフェイスを設定する必要があります。また、対応するオペレーティング システムが 1 つのファブリック パスの停止を処理するように正しく設定されていることを確認する必要があります。

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

アップグレードに関するファームウェアおよびソフトウェア関連のガイドライン

エンドポイントをアップグレードする前に、次の注意事項および制約事項を考慮してください。

各エンドポイントに適したファームウェア アップグレードのタイプの決定

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

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

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

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

使用可能なブートフラッシュおよびワークスペース パーティションの特定

ブートフラッシュ パーティションは、 Cisco UCS Managerによって管理されるファームウェアイメージ専用です。アップグレードまたはダウングレードを開始するには、ブートフラッシュ パーティションの最低 20 % が使用可能である必要があります。ブートフラッシュ パーティションが 70 % を超えると、障害が発生しますが、自動インストールは続行します。ブートフラッシュ パーティションが 80 % を超えると、障害が発生し、自動インストールは続行しません。

ファブリック インターコネクトのワークスペース パーティションに格納されるのは、テクニカル サポート ファイル、コア ファイル、およびデバッグ プラグインです。アップグレードまたはダウングレードを開始するには、ワークスペース パーティションの最低 20 % が使用可能である必要があります。

アダプタおよび I/0 モジュールへのアクティベーションの影響の特定

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

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

I/O モジュールに対して [Set Startup Version Only] を設定した場合、そのデータ パッチ内のファブリック 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。

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

Cisco UCS ドメインをアップグレードすると、アップグレード プロセスを完了するために Cisco UCS Manager によってコンポーネントが再起動されます。この再起動は、Call Home アラートをトリガーする、サービス中断と同様のイベントおよびコンポーネント障害を発生させます。アップグレードを開始する前に Call Home を無効にしない場合、アップグレード関連コンポーネントによってアラートが生成され、Call Home の設定に基づいて再起動と通知が送信されます。

ファブリック インターコネクト トラフィックの待避

リリース 2.2(4) で導入されたファブリック インターコネクト トラフィックの待避は、IOM または FEX を通じてファブリック インターコネクトに接続されているすべてのサーバからファブリック インターコネクトを通過するすべてのトラフィックを待避させる機能です。

システムの下位のファブリック インターコネクトをアップグレードすると、ファブリック インターコネクト上でアクティブなトラフィックが中断されます。このトラフィックは、プライマリ ファブリック インターコネクトにフェールオーバーします。手動によるアップグレード プロセス中は、次のようにファブリック エバキュエーションを使用できます。

1. [Admin Evac Mode] を [On] に設定して、ファブリック インターコネクトでアクティブなすべてのトラフィックを停止します。
2. フェールオーバーが設定されている vNIC に対して、Cisco UCS Manager や vCenter などのツールを使用して、トラフィックがフェールオーバーされたことを確認します。
3. 下位のファブリック インターコネクトをアップグレードします。

4. [Admin Evac Mode] を [Off] に設定して、停止されたすべてのトラフィック フローを再開します。
5. クラスタ リードを下位のファブリック インターコネクトに変更します。
6. ステップ1~4を繰り返し、他のファブリック インターコネクトをアップグレードします。

（注）
- ファブリック インターコネクト トラフィックの待避は、クラスタ設定でのみサポートされます。
- トラフィックの待避は、従属ファブリック インターコネクトからのみ実行できます。
- 待避が設定されているファブリック インターコネクトの IOM または FEX のバックプレーン ポートがダウンし、その状態が [Admin down] として表示されます。手動によるアップグレード プロセス中に、これらのバックプレーン ポートを [Up] 状態に移動させ、トラフィック フローを再開するには、[Admin Evac Mode] を明示的に [Off] に設定する必要があります。

自動インストール でのファブリック エバキュエーション

Cisco UCS Manager リリース 3.1(3) から、自動インストール 中にファブリック エバキュエーションを使用できます。自動インストール の開始時に、ファブリック エバキュエーションを有効にしてから 自動インストール を開始すると、次のイベント シーケンスが開始されます。

1. 下位のファブリック インターコネクト（FI-B）が待避させられ、アクティブ化されます。
2. フェールオーバーが発生し、プライマリ ファブリック インターコネクト（FI-A）が下位のファブリック インターコネクトになります。FI-B がクラスタ リードになります。
3. FI-A は待避させられ、アクティブ化されます。

自動インストール でファブリック エバキュエーションを使用し、ファブリック エバキュエーションが 自動インストール の前にファブリック インターコネクトで有効になっていた場合、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。

プライマリ ファブリック インターコネクトでファブリック エバキュエーションが有効になっている状態で 自動インストール を開始しないでください。ファブリック エバキュエーションを 自動インストール の前にプライマリ ファブリック インターコネクトで手動で有効にした場合は、自動インストール の開始前に手動で無効にする必要があります。

（注）
- ファブリック インターコネクト トラフィックの待避は、クラスタ設定でのみサポートされます。
- トラフィックの待避は、従属ファブリック インターコネクトからのみ実行できます。
- 待避が設定されているファブリック インターコネクトの IOM または FEX のバックプレーン ポートがダウンし、その状態が [Admin down] として表示されます。これらのバックプレーン ポートは、自動インストール の完了後に [Up] 状態に復帰します。

ファブリック インターコネクト トラフィックの待避の設定

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/enable_and_disable_fi_traffic_evacuation.html）の [Play] をクリックしてファブリック インターコネクト トラフィックの待避を有効および無効にする方法を視聴することもできます。

手順

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

ステップ 2 **[Equipment]** > **[Fabric Interconnects]** > ***[Fabric_Interconnect_Name]*** の順に展開します。

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

ステップ 4 [General] タブの [Actions] 領域で、[Configure Evacuation] をクリックします。
[Configure Evacuation] ダイアログボックスが表示されます。

ステップ 5 指定したファブリック インターコネクトを通過するトラフィックの待避を設定するには、[Admin Evac Mode] フィールドにある次のオプション ボタンの 1 つをクリックします。
- [On]：指定したファブリックインターコネクトを通過するアクティブなすべてのトラフィックを停止します。
- [Off]：指定したファブリック インターコネクトを通過するトラフィックを再開します。

ステップ 6 （任意） ファブリック インターコネクトを通過するトラフィックをその現在の待避状態に関係なく待避させるには、[Force] チェックボックスをオンにします。

ステップ 7 [Apply] をクリックします。
警告ダイアログボックスが表示されます。

```
Enabling fabric evacuation will stop all traffic through this Fabric Interconnect from
servers attached through IOM/FEX.
The traffic will fail over to the Primary Fabric Interconnect for fail over vnics.
Are you sure you want to continue?
```

ステップ 8 [OK] をクリックして、ファブリック インターコネクト トラフィックの待避を確定して続行します。

セキュア ファームウェア アップデート

Cisco UCS Managerリリース 3.1(2) では、セキュア ファームウェア アップデートが採用されています。これは、サードパーティの Intel ネットワークおよびストレージ アダプタ用にアダプタのファームウェアを安全に更新できるものです。アダプタのファームウェアをアップグレードまたはダウングレードできるのはサーバ管理者のみです。root 権限を持つ OS 管理者は、アダプタ ファームウェアをダウングレードできません。

次の Cisco UCS サーバがセキュア ファームウェア アップデートをサポートしています。

- Cisco UCS C460 M4 サーバ
- Cisco UCS C240 M4 サーバ および Cisco UCS C240 M5 サーバ
- Cisco UCS C220 M4 サーバ および Cisco UCS C220 M5 サーバ
- Cisco UCS B200 M4 サーバ および Cisco UCS B200 M5 サーバ
- Cisco UCS B480 M5 サーバおよびCisco UCS C480 M5 サーバ

セキュア ファームウェア アップデートをサポートするネットワーク アダプタとストレージ ディスク

Cisco ブレード サーバでサポートされるストレージ ディスク

次の Intel NVMe ストレージ ディスクは Cisco UCS B200 M5 サーバ および Cisco UCS B480 M5 サーバ でのセキュア ファームウェア アップデートをサポートしています。

表 *1:* サポートされる *NVMe* ストレージ ディスク

NVMe ストレージ ディスク
UCSC-NVMEHW-H800
UCSC-NVMEHW-H1600
UCSC-NVMEHW-H3200
UCSC-NVMEHW-H6400
UCSC-NVMEHW-H7680

以下の NVMe ストレージ ディスクは、UCSB-LSTOR-PT ストレージ コントローラが搭載された Cisco UCS B200 M4 サーバ上でセキュア ファームウェア アップデートをサポートしています。

ストレージ ディスク
UCS-PCI25-8003
UCS-PCI25-16003
UCS-PCI25-40010

ストレージ ディスク
UCS-PCI25-80010

（注） Cisco UCS B200 M4 サーバ上では、以下のものに対するセキュア ファームウェア アップデートはサポートされていません。

- SAS ストレージ コントローラを搭載する NVMe ディスク。
- Cisco UCS B200 M4 サーバ上の NVMe ディスクと HDD の組み合わせ。
- ネットワーク アダプタ。

Cisco ラック サーバでサポートされているネットワーク アダプタとストレージ ディスク

次の NVMe ストレージ ディスクは Cisco UCS C220 M5 サーバ サーバ、Cisco UCS C240 M5 サーバ サーバ、および Cisco UCS C480 M5 サーバ サーバでのセキュア ファームウェア アップデートをサポートしています。

表 *2:* サポートされる *NVMe* ストレージ ディスク

NVMe ストレージ ディスク
UCSC-NVMEHW-H800
UCSC-NVMEHW-H1600
UCSC-NVMEHW-H3200
UCSC-NVMEHW-H6400
UCSC-NVMEHW-H7680
UCSC-NVME-H16003 ～ UCSC-F-H16003
UCSC-NVME-H32003
UCSC-NVME-H38401
UCSC-NVME-H64003
UCSC-NVME-H76801

以下の Intel ネットワーク アダプタは、Cisco UCS C460、C240、および C220 M4 サーバ上でセキュア ファームウェア アップデートをサポートしています。

表 *3:* サポートされるネットワーク アダプタ

ネットワーク アダプタ
UCSC-PCIE-IQ10GF
UCSC-PCIE-ID10GF
UCSC-PCIE-ID40GF

次の Intel NVMe ストレージ ディスクは、Cisco UCS C460 M4 サーバ、Cisco UCS C240 M4 サーバ、および Cisco UCS C220 M4 サーバ でのセキュア ファームウェア アップデートをサポートしています。

表 *4:* サポートされる *NVMe* ストレージ ディスク

NVMe ストレージ ディスク	説明
UCS-PCI25-8003	P3600 2.5"
UCS-PCI25-16003	P3600 2.5"
UCS-PCI25-40010	P3700 2.5"
UCS-PCI25-80010	P3700 2.5"
UCSC-F-I80010	P3700 HHHL
UCSC-F-I160010	P3700 HHHL
UCSC-F-I20003	P3600 HHHL

Cisco UCS サーバ上セキュア ファームウェア サポートのガイドライン

Cisco UCS Manager リリース 3.1(2) では、セキュア ファームウェア アップデートのサポートが導入されています。Cisco UCS M5 サーバの場合、安全なファームウェア アップデートがCisco UCS Managerリリース 3.2(2) で導入されています。

重要 CIMC がバージョン 2.0(13) 以降を実行し、Cisco UCS Manager がリリース 3.1(2) 以降のリリースを実行していることを確認します。CIMC が 2.0(13) よりも前のバージョンを実行し、Cisco UCS Manager がリリース 3.1(2) よりも前のリリースを実行している場合、セキュア ファームウェア アップデートを実行できません。

ブレード サーバに対するガイドライン

Cisco UCS B200 M4、B200 M5、B480 M5 サーバでのセキュア ファームウェア アップデートについては、次の手順を実行します。

- Cisco UCS B200 M4 サーバでは、Cisco UCS Manager インフラストラクチャ ソフトウェア バンドルをアップグレードし、B シリーズ サーバ ソフトウェア バンドルを Cisco UCS

Manager リリース 3.1 (2) またはそれ以降のリリースにアップグレードします。Cisco UCS M5サーバの場合は、Cisco UCS Managerリリース 3.2(2) 以降のリリースにアップグレードします。

- Cisco UCS B200 M4、B200 M5 または B480 M5 サーバ上に UCSB-LSTOR-PT ストレージ コントローラを取り付け、NVMe ディスクを挿入します。
- サーバを再認識します。『*Cisco UCS Manager Infrastructure Management Guide, Release 3.2*』の「*Reacknowledging a Blade Server*」セクションを参照してください。

（注） サーバ検出に失敗せず、NVMe ディスクが CIMC および BIOS で認識されることを確認します。サーバがデフォルト ホスト ファームウェア パッケージを使用するサービス プロファイルに関連付けられた後、自動インストールがトリガーされます。NVMeディスクは、自動インストール中に最新のファームウェアで更新できます。

Cisco UCS Manager リリース 3.2(1) は NVMe ブートをサポートしています。

ラック サーバに対するガイドライン

Cisco UCS C460、C240、および C220 M44および M5サーバ、C480 M5 サーバでのセキュア ファームウェア アップデートについては、次の手順を実行します。

- サポートされている Cisco UCS M4 サーバでは、アップグレード、 Cisco UCS Manager インフラストラクチャ ソフトウェア バンドルと C シリーズ サーバ ソフトウェアにバンドル Cisco UCS Manager リリース 3.1 (2) またはそれ以降のリリースです。Cisco UCS M5 サーバをアップグレード Cisco UCS Manager リリース 3.2(2) またはそれ以降のリリースです。
- Cisco UCS サーバを再認識させます。『*Cisco UCS Manager Infrastructure Management Guide, Release 3.2*』の「*Reacknowledging a Rack Server*」セクションを参照してください。

（注） サーバ検出に失敗せず、NVMe ディスクが CIMC および BIOS で認識されることを確認します。サーバがデフォルト ホスト ファームウェア パッケージを使用するサービス プロファイルに関連付けられた後、自動インストールがトリガーされます。NVMeディスクは、自動インストール中に最新のファームウェアで更新できます。

Cisco UCS Manager リリース 3.2(1) は NVMe ブートをサポートしています。

自動インストールによるアップグレードに関する注意事項とガイドライン

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

（注） 次の注意事項は 自動インストール に固有の事項であり、ファームウェア アップグレードに関するガイドラインとベスト プラクティス （1 ページ）の項目と併せて考慮する必要があります。

エンドポイントの状態

アップグレードを開始する前に、影響を受けるすべてのエンドポイントが次のようになっていることが必要です。

- クラスタ設定の場合、ファブリック インターコネクトの高可用性ステータスに、両方が稼働中であると示されていることを確認します。
- スタンドアロン設定の場合、ファブリック インターコネクトの [Overall Status] が [Operable] であることを確認します。
- アップグレードするすべてのエンドポイントについて、動作可能な状態にあることを確認します。
- アップグレードするすべてのサーバについて、すべてのサーバが検出され、検出が失敗しないことを確認します。サーバ エンドポイントがアップグレードできない場合、インストール サーバ ファームウェア が失敗します。
- アップグレードする各サーバについて、ストレージ コントローラとローカル ディスク上で実行されているファームウェアのバージョンを確認し、それらが [Ready] 状態になっていることを確認します。

デフォルトのホスト ファームウェア ポリシーに関する推奨事項

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

サーバ ファームウェアのアップグレード時に、デフォルトのホスト ファームウェア ポリシーを変更して、Cisco UCS ドメイン 内のブレード サーバおよびラックマウント サーバ用のファームウェアを追加できます。アップグレードを完了するには、すべてのサーバをリブートする必要があります。

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

（注） 2.1(2a) より前のリリースからアップグレードする場合は、CSCup57496 の影響を受ける可能性があります。手動で CIMC をアップグレードしてサービス プロファイルを関連付けたら、管理ファームウェア パックを削除して CIMC のファームウェアをアクティブにします。詳細については、https://tools.cisco.com/bugsearch/bug/CSCup57496 を参照してください。これは Cisco UCS には該当しません。

ファブリック インターコネクトの時刻、日付、およびタイム ゾーンを同一にする

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

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

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

必要な権限

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

権限	実行できるアップグレード作業
admin	• インストール インフラストラクチャ ファームウェアの実行 • インストール サーバ ファームウェアの実行 • ホスト ファームウェア パッケージの追加、削除、および変更

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

インストール サーバ ファームウェア へのホスト ファームウェア パッケージの影響

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

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

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

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

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

新たに追加されたサーバのサーバ ファームウェアのアップグレード

インストール サーバ ファームウェアを実行した後、Cisco UCS ドメインにサーバを追加すると、新しいサーバのファームウェアはインストール サーバ ファームウェアによって自動的にアップグレードされません。新しく追加したサーバのファームウェアを、最後にインストール

サーバ ファームウェアを実行したときに使用したファームウェア バージョンにアップグレードする場合は、エンドポイントを手動でアップグレードしてそのサーバのファームウェアをアップグレードする必要があります。インストール サーバ ファームウェア では、毎回ファームウェア バージョンを変更する必要があります。サーバを同じファームウェア バージョンにアップグレードするためにインストール サーバ ファームウェアを再実行することはできません。

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

Cisco UCS Central のファームウェア管理に関する注意事項、ガイドライン、および制約事項

Cisco UCS Central から Cisco UCS Manager のファームウェアの管理を開始する前に、次の注意、ガイドライン、および制約事項を考慮してください。

- ドメイン グループに定義したファームウェア ポリシーは、このドメイン グループに追加されるすべての新しい Cisco UCS ドメイン に適用されます。ドメイン グループでファームウェア ポリシーが定義されていない場合、Cisco UCS ドメイン は親ドメイン グループからポリシーを継承します。
- グローバル ポリシーは、Cisco UCS Manager が Cisco UCS Central との接続を失った場合でも Cisco UCS Manager にグローバルに残ります。Cisco UCS Manager でグローバルなポリシーのいずれかに変更を適用するには、所有権をグローバルからローカルに変更する必要があります。
- ホスト ファームウェア パッケージを Cisco UCS ドメイン から作成した場合は、これをサービス プロファイルに関連付けて、Cisco UCS Central にアップデートを展開する必要があります。
- Cisco UCS ドメイン でホスト ファームウェア パッケージを変更すると、その変更はホスト ファームウェア アップデートに関連付けられた次のメンテナンス スケジュールの際に Cisco UCS Central に適用されます。
- Cisco UCS ドメイン で定義したホスト ファームウェア メンテナンス ポリシーは、Cisco UCS Central の org-root に適用されます。Cisco UCS Central から Cisco UCS ドメイン のサブ組織に対して別のホスト メンテナンス ポリシーを定義することはできません。
- サービス プロファイルとの関連付けを持たないサーバは、ホスト ファームウェア パックのデフォルト バージョンにアップグレードされます。これらのサーバにはメンテナンス ポリシーがないため、ただちにリブートされます。
- Cisco UCS Manager でメンテナンス ポリシーを指定してユーザの確認応答を有効にし、スケジュールを指定しない場合は、Cisco UCS Central からのみ保留中のタスクに確認応答で

きます。Cisco UCS Central から保留中のアクティビティに確認応答するには、グローバルなスケジューラを使用してメンテナンスをスケジュールし、ユーザの確認応答をイネーブルにする必要があります。

- Cisco UCS Central でメンテナンス ポリシーをスケジュールし、ユーザの確認応答をイネーブルにすると、このタスクは保留中のアクティビティ タブにスケジュールで指定した時刻で表示されます。
- メンテナンス ポリシーの保留中のアクティビティは、ドメイン グループのセクションからのみ表示できます。
- 任意のファームウェアのスケジュールに対するユーザーの確認応答を有効にして、Cisco UCS ドメイン での予期せぬリブートを避けるようにしてください。

（注） Cisco UCS Central のファームウェア管理の詳細については、『*Cisco UCS Central Administration Guide*』および『*Cisco UCS Central CLI Reference Manual*』の「Firmware Management」の章を参照してください。

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

エンドポイントのファームウェアのアップグレードまたはダウングレードを開始するには、Cisco UCS ドメイン のすべてのエンドポイントが完全に機能していて、すべてのプロセスが完了している状態でなければなりません。機能状態でないエンドポイントはアップグレードまたはダウングレードすることはできません。

たとえば、検出されていないサーバのファームウェアはアップグレードまたはダウングレードできません。最大回数の再試行後に失敗した FSM などの未完了のプロセスによって、エンドポイントのアップグレードやダウングレードが失敗する可能性があります。FSM が実行中の場合、Cisco UCS Manager によって、アップデートとアクティベーションがキューに入れられ、FSM が正常に完了すると、それらが実行されます。

[Equipment] タブのコンポーネントの周囲の色付けされたボックスは、そのコンポーネントのエンドポイントがアップグレードまたはダウングレードできないことを示していることがあります。エンドポイントのアップグレードを試みる前に、そのコンポーネントのステータスを確認してください。

（注） Cisco UCS Manager GUI の [インストールされたファームウェア（Installed Firmware）] タブでは、これらの前提条件を実行するための十分な情報を得られません。

Cisco UCS ドメイン のファームウェアをアップグレードまたはダウングレードする前に、次の作業を実行します。

- リリース ノートの内容を確認します。
- 適切な『Hardware and Software Interoperability Matrix』を参照し、すべてのサーバのオペレーティング システム ドライバのレベルがアップグレード予定の Cisco UCS のリリースに適切なレベルであることを確認します。
- 設定を All Configuration バックアップ ファイルにバックアップします。
- クラスタ設定の場合、ファブリック インターコネクトの高可用性ステータスに、両方が稼働中であると示されていることを確認します。
- スタンドアロン設定の場合、ファブリック インターコネクトの [Overall Status] が [Operable] であることを確認します。
- データ パスが稼働中であ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 （31 ページ）を参照してください。
- すべてのサーバ、I/O モジュール、アダプタが完全に機能することを確認します。動作不能なサーバはアップグレードできません。
- Cisco UCS ドメイン に致命的または重大な障害がないことを確認します。このような障害がある場合は解決してから、システムをアップグレードしてください。致命的または重大な障害があると、アップグレードが失敗する可能性があります。
- すべてのサーバが検出されていることを確認します。サーバの電源を入れる必要はありません。また、サーバをサービス プロファイルと関連付ける必要もありません。
- ラックマウント サーバを Cisco UCS ドメイン に統合する場合、Cisco UCS Manager で管理するシステムにラックマウント サーバを設置および統合する方法については、該当する C シリーズ ラックマウント サーバのインストール ガイド [英語] の手順を参照してください。
- iSCSI ブート用に設定されている Cisco UCS ドメイン の場合、次の操作を行ってから、Cisco UCS リリース 3.1(1) 以降にアップグレードしてください。
  - 複数のサービス プロファイルで使用されているすべての iSCSI vNIC に、一意のイニシエータ名が指定されていることを確認します。
  - いずれかの iSCSI vNIC にサーバ プロファイルと同じイニシエータ名が指定されている場合、Cisco UCS は、1 つの一意のイニシエータ名を持つようにサービス プロファイルを再構成します。
  - ブート LUN が新しい IQN に表示されるように、各ネットワーク ストレージ デバイスで対応する IQN 発信側名を変更します。

アップグレード前検証

ファームウェアをインストールする前に、次のアップグレード前検証を実行してください。

バックアップ ファイルの作成

Cisco UCS Manager からバックアップを実行する場合は、システム設定全体またはその一部のスナップショットを作成し、ファイルをネットワーク上の場所にエクスポートします。バックアップは、システムが起動されて動作している間に実行できます。バックアップ操作では、管理プレーンからの情報だけが保存されます。バックアップは、サーバまたはネットワーク トラフィックには影響しません。

シスコでは、Cisco UCS ファームウェア アップグレードを開始する前に、次のバックアップ ファイルを作成することを推奨します。

- [All Configuration] バックアップ ファイル：すべてのシステムおよび論理設定の XML バックアップ
- [Full State] バックアップ ファイル：システム全体のバイナリ スナップショット

すべてのコンフィギュレーション バックアップ ファイルの作成

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

始める前に

バックアップ サーバの IPv4 アドレスまたは IPv6 アドレスおよび認証クレデンシャルを取得します。

手順

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

ステップ 2 [All] ノードをクリックします。

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

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

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

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

a) 次のフィールドに入力します。

- **[Admin State]** フィールド：**[Enabled]** オプション ボタンをクリックすると、[OK] をクリックしてすぐに、バックアップ操作が実行されます。
- **[Type]** フィールド：**[All Configuration]** オプション ボタンをクリックすると、すべてのシステムおよび論理設定情報を含む XML バックアップ ファイルが作成されます。

  システム全体のスナップショットが含まれるバイナリ ファイルを作成するには、[Full State] オプション ボタンをクリックします。
- **[Preserve Identities]** チェック ボックス：Cisco UCS ドメイン に、プールから取得され、保存する必要がある ID が含まれる場合、このチェックボックスをオンにします。

[Logical Configuration] タイプのバックアップ操作でこのチェックボックスが選択されている場合、バックアップ ファイルはプールから取得したすべてのアイデンティティ (vHBA、WWPN、WWNN、vNIC、MAC、UUID を含む) を保存します。

（注） このチェックボックスが選択されていない状態で復元を行うと、アイデンティティが再割り当てされ、ユーザ ラベルが失われます。

- **[Location of the Backup File]** フィールド：ローカル ファイル システムにバックアップ ファイルを保存するには、[Local File System] オプション ボタンをクリックします。リモート ファイル システムにバックアップ ファイルを保存するには、[Local File System] オプション ボタンをクリックします。

  場所が **[Local File System]** に設定されている場合、Cisco UCS Manager GUI によって **[Filename]** フィールドが表示されます。**[Remote File System]** に設定されている場合、Cisco UCS Manager GUI に次に説明する残りのフィールドが表示されます。

- [Filename] フィールド：ローカル ファイル システム内の新しい場所にナビゲートするには、[Browse] をクリックします。

- **[Protocol]** フィールド：ファイルをバックアップ サーバに転送するために使用するプロトコルを指示する場合に、次のいずれかのオプション ボタンをクリックします。
  - **FTP**
  - **TFTP**
  - **SCP**
  - **SFTP**

- **[Hostname]** フィールド：バックアップ ファイルを格納する場所の IP アドレスまたはホスト名を入力します。これは、サーバ、ストレージ アレイ、ローカル ドライブ、またはファブリック インターコネクトがネットワーク経由でアクセス可能な任意の読み取り/書き込みメディアなどがあります。ホスト名を使用する場合、Cisco UCS Manager で DNS サーバを使用するように設定する必要があります。

- **[Remote File]** フィールド：バックアップ コンフィギュレーション ファイルのフル パスを入力します。このフィールドには、ファイル名とパスを含めることができます。ファイル名を省略すると、バックアップ手順によって、ファイルに名前が割り当てられます。

- **[User]** フィールド：Cisco UCS Manager がバックアップ場所へのログインに使用する必要のあるユーザ名を入力します。プロトコルに TFTP を選択した場合は、このフィールドに入力する必要はありません。

- [Password] フィールド：ユーザ名に関連付けられたパスワードを入力します。プロトコルに TFTP を選択した場合は、このフィールドに入力する必要はありません。

b) [OK] をクリックします。

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

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

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

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

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

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

ステップ 9 [OK] をクリックし、[Backup Configuration] ダイアログボックスを閉じます。

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

完全な状態のコンフィギュレーション バックアップ ファイルの作成

始める前に

バックアップ サーバの IPv4 アドレスまたは IPv6 アドレスおよび認証クレデンシャルを取得します。

手順

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

ステップ 2 [All] ノードをクリックします。

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

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

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

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

a) 次のフィールドに入力します。

- **[Admin State]** フィールド：**[Enabled]** オプション ボタンをクリックすると、[OK] をクリックしてすぐに、バックアップ操作が実行されます。
- **[Type]** フィールド：システム全体のスナップショットが含まれるバイナリ ファイルを作成するには、**[Full State]** オプション ボタンをクリックします。
- **[Preserve Identities]** チェック ボックス：Cisco UCS ドメイン に、プールから取得され、保存する必要がある ID が含まれる場合、このチェックボックスをオンにします。

[Logical Configuration] タイプのバックアップ操作でこのチェックボックスが選択されている場合、バックアップ ファイルはプールから取得したすべてのアイデンティティ (vHBA、WWPN、WWNN、vNIC、MAC、UUID を含む) を保存します。

（注） このチェックボックスが選択されていない状態で復元を行うと、アイデンティティが再割り当てされ、ユーザ ラベルが失われます。

- **[Location of the Backup File]** フィールド：ローカル ファイル システムにバックアップ ファイルを保存するには、[Local File System] オプション ボタンをクリックします。リモート ファイル システムにバックアップ ファイルを保存するには、[Remote File System] オプション ボタンをクリックします。

  場所が **[Local File System]** に設定されている場合、Cisco UCS Manager GUI によって **[Filename]** フィールドが表示されます。**[Remote File System]** に設定されている場合、Cisco UCS Manager GUI に次に説明する残りのフィールドが表示されます。

- [Filename] フィールド：ローカル ファイル システム内の新しい場所にナビゲートするには、[Browse] をクリックします。

- **[Protocol]** フィールド：ファイルをバックアップ サーバに転送するために使用するプロトコルを指示する場合に、次のいずれかのオプション ボタンをクリックします。
  - **FTP**
  - **TFTP**
  - **SCP**
  - **SFTP**

- **[Hostname]** フィールド：バックアップ ファイルを格納する場所の IP アドレスまたはホスト名を入力します。これは、サーバ、ストレージ アレイ、ローカル ドライブ、またはファブリック インターコネクトがネットワーク経由でアクセス可能な任意の読み取り/書き込みメディアなどがあります。ホスト名を使用する場合、Cisco UCS Manager で DNS サーバを使用するように設定する必要があります。

- **[Remote File]** フィールド：バックアップ コンフィギュレーション ファイルのフル パスを入力します。このフィールドには、ファイル名とパスを含めることができます。ファイル名を省略すると、バックアップ手順によって、ファイルに名前が割り当てられます。

- **[User]** フィールド：Cisco UCS Manager がバックアップ場所へのログインに使用する必要のあるユーザ名を入力します。プロトコルに TFTP を選択した場合は、このフィールドに入力する必要はありません。

- [Password] フィールド：ユーザ名に関連付けられたパスワードを入力します。プロトコルに TFTP を選択した場合は、このフィールドに入力する必要はありません。

b) [OK] をクリックします。

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

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

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

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

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

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

ステップ 9 [OK] をクリックし、[Backup Configuration] ダイアログボックスを閉じます。

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

ファームウェア アップグレードのための Cisco Smart Call Home の設定

Cisco Smart Call Home は、Cisco UCS の Call Home 機能を強化する Web アプリケーションです。Smart Call Home により、予防的な診断および重要なシステム イベントのリアルタイムの電子メールアラートが提供されます。それにより、ネットワークの可用性が高まり、運用効率が向上します。Smart Call Home は、Cisco UCS の Cisco Unified Computing Support サービスと Cisco Unified Computing Mission Critical Support サービスによって提供されるセキュア接続のサービスです。『*Cisco UCS Manager Administration Management Guide*』には、Smart Call Home の設定に関する詳細情報が掲載されています。

ファームウェアをアップグレードすると、Cisco UCS Manager によってコンポーネントが再起動され、アップグレード プロセスが完了します。この再起動によって、電子メール アラートがトリガーされる可能性があります。Smart Call Home を無効にすることで、ファームウェア アップグレード プロセス中にこのようなアラートや TAC への自動サポート ケースを回避できます。

Smart Call Home の無効化

始める前に

Smart Call Home がすでに有効になっている必要があります。

手順

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

ステップ 2 **[All]** > **[Communication Management]** > **[Call Home]** の順に展開します。

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

ステップ 4 [Admin] 領域で次の作業を行い、Smart Call Home を無効にします。

a) [State] フィールドで、[Off] をクリックします。

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

Call Home アラートは、Smart Call Home を再度有効にするまで生成されません。

ファームウェア アップグレード中のフォールト抑制

障害抑制によって、予定されたメンテナンス時間中に SNMP トラップおよび Call Home 通知を抑制することができます。障害抑制タスクを作成し、一時的な障害が発生またはクリアされるたびに通知が送信されることを防止できます。

障害は、期限切れになるか、障害抑制タスクがユーザによって手動で停止されるまで抑制されたままになります。フォールト抑制が終了した後に、Cisco UCS Manager がクリアされていない未処理の抑制された障害の通知を送信します。

ファームウェア アップグレード中のすべてのコンポーネントのフォールト抑制を有効にすると、期限切れになるか、またはアップグレード後にコンポーネントが再稼働状態になるまで、そのコンポーネントに関連するエラーが抑制されます。たとえば、ファブリックインターコネクト障害がファームウェアアップグレード中に抑制されるように設定されている場合、アップグレード中にそのファブリックインターコネクトによってトリガーされたすべての障害は表示されません。

UCS Manager の障害の表示

手順

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

ステップ 2 **[All]** > **[Faults, Events, and Audit Log] の順に展開します。**

ステップ 3 [Faults] をクリックします。

ステップ 4 [Work] ペインで、[All] チェックボックスをオンにします。

ステップ 5 サービスに影響を及ぼす障害が存在しないことを確認してください。

ファブリックインターコネクトのアップグレード中のリブートによって生成される障害

ファブリック インターコネクトが再起動するときにダウンするポート設定とサービスは、ファブリック インターコネクトがアップ状態に戻ったときに再確立されるようにすることがきわめて重要です。

Cisco UCS Managerリリース 3.1 以降、Cisco UCS Managerはファブリックインターコネクトの最後の再起動後に再確立されていないサービスをすべて表示します。Cisco UCS Managerは、ファブリックインターコネクトを再起動する前に、未解決の障害のベースラインを作成します。ファブリック インターコネクトがリブートして再稼働状態に復帰したら、最後のベースライン以降に生成された新しい障害を確認して、ファブリックのリブートによってダウンしたサービスを特定できます。

Cisco UCS Manager が未処理の障害のベースラインを作成してから特定の期間が経過すると、ベースラインはクリアされ、すべての障害が新しい障害として表示されます。この間隔は、「ベースラインの有効期限間隔」と呼ばれます。障害のベースライン有効期限の変更 （24ページ）、ベースラインの有効期限間隔を変更することに関する詳細情報を提供Cisco UCS Manager。

シスコでは、ファブリック インターコネクトのリブートまたは待避を実行する前に、サービスに影響する障害を解決することを推奨します。

障害のベースライン有効期限の変更

Cisco UCS Managerでは、ベースラインの有効期限を変更できます。

手順

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

ステップ 2 **[All]** > **[Faults, Events, and Audit Log]** の順に展開します。

ステップ 3 [Work] ペインの [Settings] タブをクリックし、[Global Fault Policy] サブタブをクリックします。

ステップ 4 [Baseline Expiration Interval] 領域で、[dd:hh:mm:ss] フィールドを更新します。

[dd:hh:mm:ss] フィールドには、Cisco UCS Manager が障害のベースラインをクリアするまでに経過する必要がある日数、時間数、分数、および秒数を指定します。

デフォルトのベースライン有効期限は 24 時間です。

ステップ 5 [Save Changes] をクリックします。

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

手順

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

ステップ 2 **[All]** > **[Faults, Events, and Audit Log]** の順に展開します。

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

ベースラインを作成した後に生成されたすべての障害が表示されます。

ファブリック フェールオーバー用の vNIC 設定の確認

Cisco UCS システムでは、次のいずれかが発生するとファブリック障害が発生する場合があります。

- ファブリック インターコネクトで障害が発生し、その結果、そのファブリック インターコネクトに接続されているすべてのシャーシでファブリック障害が発生する。
- FEX で障害が発生し、その結果、その FEX に接続されているシャーシでファブリック障害が発生する。
- ファブリック インターコネクトと FEX 間のリンクで障害が発生し、その結果、特定の FEX に接続されているシャーシ内のサーバの一部でファブリック障害が発生する。
- CNA ポートで障害が発生し、その結果、サーバでファブリック障害が発生する。

冗長ハードウェアが設置されており、vNICがフェールオーバー用に設定されている場合、ファブリック障害によってファブリック フェールオーバーが発生します。ファームウェアをアップグレードする前に、vNIC がファブリック フェールオーバー用に設定されていることを確認してください。

手順

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

ステップ 2 **[Servers]** > **[Service Profiles]** > **[Service_Profile_Name]** の順に展開します。

ステップ 3 指定されたサービス プロファイルを展開し、[vNICs] を選択します。

ステップ 4 [vNICs] を展開し、指定されたサービス プロファイルの最初の vNIC を選択します。

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

ステップ 6 [Properties] 領域で、[Fabric ID] が [Fabric A] であり、[Enable Failover] チェックボックスがオンになっていることを確認します。

ステップ 7 [Navigation] ペインで、指定されたサービス プロファイルの次の vNIC を選択します。

ステップ 8 [Work] ペインで、[General] タブをクリックします。

ステップ 9 [Properties] 領域で、[Fabric ID] が [Fabric B] であり、[Enable Failover] チェックボックスがオンになっていることを確認します。

ステップ 10 指定されたサービス プロファイルのすべての vNICs を確認するまで、ステップ 4 ～ 9 を繰り返します。

重要 フェールオーバーが確実に発生するようにするために、代替 vNIC が Fabric A と Fabric B に固定されていることを確認します。

ファブリック B

ファブリック インターコネクトの運用性の確認

手順

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

ステップ 2 **[Equipment]** > **[Fabric Interconnects]** の順に展開します。

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

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

ステップ 5 [Status] 領域で、[Overall Status] が [operable] であることを確認します。

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

クラスタ設定の高可用性ステータスとロールの確認

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

手順

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

ステップ 2 **[Equipment]** > **[Fabric Interconnects]** の順に展開します。

ステップ 3 クラスタのいずれかのファブリック インターコネクトのノードをクリックします。

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

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

ステップ 6 次のフィールドに次の値が表示されることを確認します。

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

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

ステップ 7 [Leadership] フィールドの値に注意して、ファブリック インターコネクトがプライマリ ユニットであるか、従属ユニットであるかを判断します。

この情報は、ファブリック インターコネクトのファームウェアをアップグレードするために知っておく必要があります。

デフォルト メンテナンス ポリシーの設定

サービス プロファイルの変更の一部、またはサービス プロファイル テンプレートの更新は、中断をともなうことや、サーバのリブートが必要になることがあります。メンテナンス ポリシーは、サーバに関連付けられたサービス プロファイル、または1つ以上のサービス プロファイルに関連付けられた更新中のサービス プロファイルに対して、サーバのリブートが必要になるような変更が加えられた場合の Cisco UCS Manager の対処方法を定義します。

メンテナンス ポリシーは、Cisco UCS Manager でのサービス プロファイルの変更の展開方法を指定します。展開は、次のいずれかの方法で実行されます。

- 即時
- ユーザが管理者権限で承認したときに実行する
- スケジュールで指定された時間に自動的に実行する
- サーバをリブートしたときに実行する

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

手順

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

ステップ 2 **[Servers]** > **[Policies]** の順に展開します。

ステップ 3 ポリシーを作成する組織のノードを展開します。

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

ステップ 4 [Maintenance Policies] を展開し、[default] をクリックします。

ステップ 5 [Work] ペインの [Main] タブをクリックします。

ステップ 6 [Properties] 領域で、[Reboot Policy] として [User Ack] を選択します。

[On Next Boot] チェックボックスが表示されます。

サービスプロファイルの関連付けが完了するか、変更が加えられたときは、サーバを手動でリブートする必要があります。

ステップ 7 （任意） [On Next Boot] オプションを有効にするには、[On Next Boot] チェックボックスをオンにします。

[On Next Boot] オプションが有効な場合、ホスト OS のリブート、シャットダウン、リセット、またはサーバリセットとシャットダウンにより、[User Ack] メンテナンス ウィンドウを待っている変更を適用するために、関連 FSM もトリガーされます。

ステップ 8 [Save Changes] をクリックします。

管理インターフェイスの無効化

ファームウェアをアップグレードする前に、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をシャットダウンします。これにより、サーバと管理インターフェイス間のアクティブな KVM 接続がすべてリセットされます。GUI フローがプライマリ ファブリック インターコネクトにフェールオーバーされるため、GUI から切断される時間が短縮されます。

Cisco UCS Manager によって管理インターフェイスの障害が検出されると、障害レポートが生成されます。障害レポートの数が設定された数に達した場合、システムは管理インターフェイスが使用不能であると見なし、障害を生成します。デフォルトでは、管理インターフェイス モニタリング ポリシーは有効です。『*Cisco UCS Manager* システム モニタリング ガイド』には、管理インターフェイス モニタリング ポリシーに関する詳細が掲載されています。

手順

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

ステップ 2 **[All]** > **[Communication Management]** の順に展開します。

ステップ 3 [Management Interfaces] をクリックします。

ステップ 4 [Work] ペインで、[Management Interfaces] タブをクリックして、ファブリック インターコネクトの管理 IP アドレスを確認します。

ステップ 5 [Management Interfaces Monitoring Policy] タブをクリックし、[Admin Status] フィールドで [Enabled] オプション ボタンをクリックして、管理インターフェイスのモニタリング ポリシーを有効にします。

Cisco UCS Manager によって管理インターフェイスの障害が検出されると、障害レポートが生成されます。

ステップ 6 ファブリック インターコネクトに接続されているアップストリーム スイッチへの Telnet セッションを開きます。

ステップ 7 ファブリック インターコネクトの管理ポートが接続されているインターフェイスの設定を確認し、スイッチの **shut** コマンドを使用して無効にします。

このインターフェイスを通じて開いているすべての KVM セッションが終了します。

ステップ 8 KVM セッションを再接続して、これらのセッションがセカンダリ ファブリック インターコネクトのアップグレードの影響を受けないようにします。

I/O モジュールのステータスの確認

手順

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

ステップ 2 **[Equipment]** > **[Chassis]** の順に展開します。

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

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

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

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

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

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

サーバのステータスの確認

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

手順

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

ステップ 2 [Work] ペインの [Servers] タブをクリックして、すべてのシャーシのすべてのサーバのリストを表示します。

ステップ 3 各サーバについて、次のカラムに次の値が表示されることを確認します。

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

ステップ 4 サーバが検出されていることを確認する必要がある場合、次の手順を実行します。

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

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

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

シャーシのサーバのアダプタのステータスの確認

手順

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

ステップ 2 **[Equipment]** > **[Chassis]** > ***[Chassis Number]*** > **[Servers]** の順に展開します。

ステップ 3 アダプタのステータスを確認するサーバをクリックします。

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

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

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

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

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

データ パスの準備が整っていることの確認

以下の項では、データ パスの準備ができていることを確認する手順を説明します。

ダイナミック vNIC が稼働中であることの確認

ダイナミック vNIC および VMware vCenter との統合を含む Cisco UCS をアップグレードするとき、すべてのダイナミック vNIC が新しいプライマリ ファブリック インターコネクトで動作中であることを確認する必要があります。データ パスの中断を避けるため、以前のプライマリ ファブリック インターコネクト上で新しいソフトウェアを有効にする前に、vNIC が動作中であることを確認します。

この手順は Cisco UCS Manager GUI で実行します。

手順

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

ステップ 2 **[All]** > **[VMware]** > **[Virtual Machines]**を展開します。

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

ステップ 4 [Work] ペインで、[VIF] タブをクリックします。

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

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

イーサネット データ パスの確認

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A /fabric-interconnect # **connect nxos** {**a** | **b**}	ファブリック インターコネクトの NX-OS モードを開始します。
ステップ 2	UCS-A(nxos)# **show int br | grep -v down | wc –l**	アクティブなイーサネットインターフェイスの数を返します。

<table>
<tr><th></th><th>コマンドまたはアクション</th><th>目的</th></tr>
<tr><td></td><td></td><td>この数がアップグレードの前に稼働していたイーサネット インターフェイスの数と一致することを確認します。</td></tr>
<tr><td>ステップ 3</td><td>ファブリック インターコネクトに基づいて、次のいずれかを実行します。
<table>
<tr><th>オプション</th><th>説明</th></tr>
<tr><td>show platform fwm info hw-stm | grep '1.' | wc –l</td><td>UCS 6200 シリーズ、UCS 6332、および UCS 6332-16UP ファブリック インターコネクトの MAC アドレスの合計数を返します。</td></tr>
<tr><td>show hardware internal libsdk mtc l2 mac-table-ce valid-only | egrep "^ *[0-9]" | wc -l</td><td>UCS 6324 (UCS ミニ) ファブリック インターコネクトの MAC アドレスの合計数を返します。</td></tr>
<tr><td>show hardware mac address-table 1 | wc -l</td><td>UCS 6400 シリーズ ファブリック インターコネクトの MAC アドレスの合計数を返します。</td></tr>
</table></td><td>この数がアップグレード前の MAC アドレスの数と一致することを確認します。</td></tr>
</table>

例

次の例では、従属 UCS 6332 ファブリック インターコネクト A のアクティブなイーサネット インターフェイスおよび MAC アドレスの数が返され、ファブリック インターコネクトのイーサネット データ パスが稼働していることを確認できます。

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

次の例では、従属 UCS 6400 シリーズ ファブリック インターコネクト A のアクティブなイーサネット インターフェイスおよび MAC アドレスの数が返され、ファブリック インターコネクトのイーサネット データ パスが稼働していることを確認できます。

```
UCS-A /fabric-interconnect # connect nxos a
UCS-A(nxos)# show int br | grep -v down  | wc -l
86
UCS-A(nxos)# show hardware mac address-table 1 | wc -l
80
```

ファイバ チャネル エンドホスト モードのデータ パスの確認

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

手順

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

例

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

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

Total number of flogi = 3.

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

ファイバ チャネル スイッチ モードのデータ パスの確認

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

手順

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

例

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

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

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