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 4043 ～ 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 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。

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更新する場合、[ファームウェアのアクティブ化（Activate Firmware）] ダイアログボックスの [フィルタ（Filter）] ドロップダウン リストで[すべて（ALL）] を選択し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20%以上が使用可能でなければなりません。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 インターコネクト上のワークスペース パーティションには、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 プラグインが格納されます。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 20% 以上が使用可能でなければなりません。

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

I/O モジュールに対して [Set Startup Version Only] を設定した場合、そのデータ パ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。

重要

- 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。

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。

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 インターコネクトのトラフィックの停止

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope fabric-interconnect** {**a** | **b**}	指定したファブリック インターコネクトのファブリック インターコネクト モードを開始します。
ステップ 2	UCS-A /fabric-interconnect # **stop server traffic** [**force**]	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。 ファブリック インターコネクトの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** オプションを使用します。
ステップ 3	UCS-A /fabric-interconnect # **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、ファブリック インターコネクト B を通過するアクティブなすべてのトラフィックを停止する方法を示します。

```
UCS-A# scope fabric-interconnect b
UCS-A /fabric-interconnect # stop server traffic
Warning: 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.
UCS-A /fabric-interconnect # commit-buffer
```

ファブリック インターコネクトのトラフィックの再開

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope fabric-interconnect** {**a** | **b**}	指定したファブリック インターコネクトのファブリック インターコネクト モードを開始します。
ステップ 2	UCS-A /fabric-interconnect # **start server traffic**	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 3	UCS-A /fabric-interconnect # **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、ファブリック インターコネクト B を通過するトラフィックを再開する方法を示します。

```
UCS-A# scope fabric-interconnect b
UCS-A /fabric-interconnect # start server traffic
Warning: Resetting fabric evacuation will cause server traffic that failed over to the
Primary Fabric Interconnect to fail back to this Fabric Interconnect.
UCS-A /fabric-interconnect # commit-buffer
```

ファブリックの退避の確認

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **show service-profile circuit server** *server-id*	指定されたサーバに関連付けられたサービス プロファイル用のネットワーク回路情報を表示します。

例

次の例は、ファブリック退避前の VIF パスを示しています。

（注）
- ファブリック インターコネクト A の VIF は、トラフィックがファブリック インターコネクトによって最初にアクティブであることを示します。
- ファブリック インターコネクト B の VIF は、退避前にパッシブです。

```
UCS-A# show service-profile circuit server 1/6
Service Profile: test1
Server: 1/6
    Fabric ID: A
        Path ID: 1
        VIF        vNIC            Link State  Oper State Prot State    Prot Role   Admin
 Pin  Oper Pin   Transport
        ---------- --------------- ----------- ---------- ------------- -----------
---------- ---------- ---------
               692 eth0             Up          Active     Active        Primary     0/0
        1/15       Ether
    Fabric ID: B
        Path ID: 1
        VIF        vNIC            Link State  Oper State Prot State    Prot Role   Admin
 Pin  Oper Pin   Transport
        ---------- --------------- ----------- ---------- ------------- -----------
---------- ---------- ---------
               693 eth0             Up          Active     Passive       Backup      0/0
        1/15       Ether
UCS-A#
```

次の例は、ファブリック インターコネクト A 退避後の VIF パスを示しています。

（注）
- フェールオーバー後、ファブリック インターコネクト A の VIF 状態はエラーになります。
- ファブリック インターコネクト B の VIF がアクティブとして引き継ぎます。

```
UCS-A# show service-profile circuit server 1/6
Service Profile: test1
Server: 1/6
    Fabric ID: A
        Path ID: 1
        VIF        vNIC            Link State  Oper State Prot State    Prot Role   Admin
 Pin  Oper Pin   Transport
        ---------- --------------- ----------- ---------- ------------- -----------
---------- ---------- ---------
               692 eth0             Error       Error      Active        Primary     0/0
        0/0        Ether
    Fabric ID: B
        Path ID: 1
        VIF        vNIC            Link State  Oper State Prot State    Prot Role   Admin
 Pin  Oper Pin   Transport
        ---------- --------------- ----------- ---------- ------------- -----------
---------- ---------- ---------
               693 eth0             Up          Active     Passive       Backup      0/0
```

```
        1/15       Ether
UCS-A#
```

ファブリック インターコネクトの退避ステータスの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope 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 detail**	指定されたファブリック インターコネクトに関する詳細を表示します。

例

次に、ファブリック インターコネクトの詳細なステータスを表示する例を示します。

（注） Admin Evacuation と Oper Evacuation はファブリック インターコネクトの退避ステータスを示します。

```
 UCS-A /fabric-interconnect # show detail

Fabric Interconnect:
    ID: B
    Product Name: Cisco UCS 6248UP
    PID: UCS-FI-6248UP
    VID: V01
    Vendor: Cisco Systems, Inc.
    Serial (SN): SSI171400HG
    HW Revision: 0
    Total Memory (MB): 16165
    OOB IP Addr: 10.193.32.172
    OOB Gateway: 10.193.32.1
    OOB Netmask: 255.255.255.0
    OOB IPv6 Address: ::
    OOB IPv6 Gateway: ::
    Prefix: 64
    Operability: Operable
    Thermal Status: Ok
    Admin Evacuation: On
    Oper Evacuation: On
    Current Task 1:
    Current Task 2:
    Current Task 3:
```

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 サーバーでのセキュア 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 サーバー上に 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 M4 および M5 サーバーおよび C480 M5 サーバーの安全なファームウェア アップデートのために、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。

- クラスタ構成の場合は、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ことが示されているかを確認します。
- スタンドアロン構成の場合、ファブリック インターコネクトの [全体のステータス（Overall Status）] が [操作可能（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ーについて、すべてのサーバーが検出され、検出が失敗しないことを確認します。サーバー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ー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ー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 には、ファームウェア バージョンの変更が毎回必要です。サーバを同じファームウェア バージョンにアップグレードするためにインストール 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前に、Cisco UCS ドメイン のすべてのエンドポイントが十分に機能し、すべてのプロセスが完了している必要があります。機能状態でないエンドポイントはアップグレードまたはダウングレードすることはできません。

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

Cisco UCS 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。
- クラスタ構成の場合は、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ことが示されているかを確認します。

- スタンドアロン構成の場合、ファブリック インターコネクトの[全体のステータス（Overall Status）] が [操作可能（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 （37 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、http://www.cisco.com/en/US/partner/products/ps11736/products_installation_and_configuration_guides_list.htmlCisco 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-Series Rack-Mount Server Integration Guide』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 に認識されるように、各ネットワーク ストレージ デバイスで該当する IQN イニシエータ名を変更します。

Cisco UCS ファブリック インターコネクトのファイバ チャネル ポートが Cisco 以外の製品に接続されている場合は、これらのファイバ チャネル ポートが個別のファイバ チャネル リンクとして動作し、ポート チャネルに集約されていないことを確認します。

（注） ファイバチャネルポートのチャネルは、シスコ以外のテクノロジーとの互換性がありません。

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope system**	システム モードを開始します。
ステップ 2	UCS-A /system # **create backup** *URL* **all-configuration enabled**	**commit-buffer** コマンドを入力するとすぐに実行される、有効化された All Configuration バックアップ操作を作成します。 **all-configuration** オプションでは、サーバ関連、ファブリック関連、システム関連の設定をバックアップします次のいずれかの構文を使用してバックアップするファイルの URL を指定します。 • **ftp:**// *username***@***hostname* / *path* • **scp:**// *username@hostname* / *path* • **sftp:**// *username@hostname* / *path* • **tftp:**// *hostname* **:** *port-num* / *path*

	コマンドまたはアクション	目的
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。

例

次の例では、SCP を使用して host35 という名前のホストに All Configuration バックアップ ファイルを作成し、トランザクションをコミットしています。

```
UCS-A# scope system
UCS-A /system* # create backup scp://user@host35/backups/all-config.bak all-configuration
 enabled
Password:
UCS-A /system* # commit-buffer
UCS-A /system #
```

Full State バックアップ ポリシーの構成

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

	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 backup-policy default**	All Configuration エクスポート ポリシー モードを開始します。
ステップ 3	UCS-A /org/backup-policy # **set hostname** {*hostname* | *ip-addr* | *ip6-addr*}	バックアップポリシーが格納されている場所のホスト名、IPv4 または IPv6 アドレスを指定します。これには、サーバー、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。

	コマンドまたはアクション	目的
		（注） IPv4 や IPv6 アドレスではなくホスト名を使用する場合、DNS サーバを設定する必要があります。Cisco UCS ドメインが Cisco UCS Central に登録されていないか、または DNS 管理が [ローカル（local）] に設定されている場合は、Cisco UCS Manager で DNS サーバを設定します。Cisco UCS ドメインが Cisco UCS Central に登録されていて、DNS 管理が [グローバル（global）] に設定されている場合は、Cisco UCS Central で DNS サーバを設定します。
ステップ 4	UCS-A /org/backup-policy # **set protocol** {**ftp** | **scp** | **sftp** | **tftp**}	リモート サーバーとの通信時に使用するプロトコルを指定します。
ステップ 5	UCS-A /org/backup-policy # **set user** *username*	システムがリモート サーバーへのログインに使用する必要のあるユーザー名を指定します。この手順は、TFTP プロトコルを使用する場合には適用されません。
ステップ 6	UCS-A /org/backup-policy # **set password**	**Enter** キーを押すと、パスワードを入力するように促されます。 リモート サーバーのユーザー名のパスワードを指定します。この手順は、TFTP プロトコルを使用する場合には適用されません。
ステップ 7	UCS-A /org/backup-policy # **set remote-file** *filename*	バックアップ ファイルのフルパスを指定します。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。
ステップ 8	UCS-A /org/backup-policy # **set adminstate** {**disable** | **enable**}	ポリシーの管理状態を指定します。次のいずれかになります。

	コマンドまたはアクション	目的
		• **[enabled]**：Cisco UCS Manager は、**[Schedule]** フィールドで指定されたスケジュールを使用してバックアップ ファイルをエクスポートします。 • **[disabled]**：Cisco UCS Manager はファイルをエクスポートしません。
ステップ 9	UCS-A /org/backup-policy # **set schedule** {**daily** | **weekly** | **bi-weekly**}	Cisco UCS Manager がバックアップ ファイルをエクスポートする頻度を指定します。
ステップ 10	UCS-A /org/backup-policy # **set descr** *description*	バックアップポリシーの説明を指定します。 256 文字以下で入力します。次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
ステップ 11	UCS-A /org/backup-policy # **commit-buffer**	トランザクションをコミットします。

例

次の例では、週単位のバックアップのための full state バックアップ ポリシーを設定し、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 org /
UCS-A /org # scope backup-policy default
UCS-A /org/backup-policy # set hostname host35
UCS-A /org/backup-policy* # set protocol scp
UCS-A /org/backup-policy* # set user UserName32
UCS-A /org/backup-policy* # set password
Password:
UCS-A /org/backup-policy* # set remote-file /backups/full-state1.bak
UCS-A /org/backup-policy* # set adminstate enable
UCS-A /org/backup-policy* # set schedule weekly
UCS-A /org/backup-policy* # set descr "This is a full state weekly backup."
UCS-A /org/backup-policy* # commit-buffer
UCS-A /org/backup-policy #
```

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

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニターリング モードを開始します。
ステップ 2	UCS-A /monitoring # **scope callhome**	モニターリング Call Home モードを開始します。
ステップ 3	UCS-A /monitoring/callhome # **disable**	Call Home をイネーブルにします。
ステップ 4	UCS-A /monitoring/callhome # **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、Smart Call Home を無効にし、トランザクションをコミットする例を示します。

```
UCS-A# scope monitoring
UCS-A /monitoring # scope callhome
UCS-A /monitoring/callhome # disable
UCS-A /monitoring/callhome* # commit-buffer
UCS-A /monitoring/callhome #
```

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。

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リブートする前に、未解決の障害の基準設定を作成します。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、「基準設定有効期限間隔」と呼ばれます。障害のベースライン有効期限の変更 （26ページ）、Cisco UCS Manager の基準設定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します。

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニターリング モードを開始します。
ステップ 2	UCS-A /monitoring # **scope fault policy**	モニターリング障害ポリシー モードを開始します。
ステップ 3	UCS-A /monitoring/fault-policy # **show**	障害ポリシーの詳細を表示します。

	コマンドまたはアクション	目的
ステップ 4	UCS-A /monitoring/fault-policy # **set baseline-expiration-interval** {*days hours minutes seconds*}	ベースライン有効期限を変更します。 デフォルトのベースライン有効期限は 24 時間です。 （注） ベースライン有効期限が切れると、すべての障害は新しい障害として表示されます。
ステップ 5	UCS-A /monitoring/fault-policy* # **commit**	トランザクションをコミットします。
ステップ 6	UCS-A /monitoring/fault-policy # **show**	障害ポリシーの詳細を表示します。

例

次に、障害のベースライン有効期限を変更する例を示します。

```
UCS-A# scope monitoring
UCS-A /monitoring # scope fault policy
UCS-A /monitoring/fault-policy # show

Fault Policy:
    Clear Action Clear Interval Retention Interval (dd:hh:mm:ss) Flap Interval (sec)
  Baseline Expiration Interval (dd:hh:mm:ss)
    ------------ -------------- -------------------------------- -----------------------
 -----------------------------------------
    Retain       00:00:20:00    00:01:00:00                      10
  10:00:00:12

UCS-A /monitoring/fault-policy # set baseline-expiration-interval 0 2 24 0
UCS-A /monitoring/fault-policy* # commit
UCS-A /monitoring/fault-policy # show

Fault Policy:
    Clear Action Clear Interval Retention Interval (dd:hh:mm:ss) Flap Interval (sec)
  Baseline Expiration Interval (dd:hh:mm:ss)
    ------------ -------------- -------------------------------- -----------------------
 -----------------------------------------
    Retain       10:00:00:00    01:01:01:01                      10
  00:02:24:00
UCS-A /monitoring/fault-policy #
```

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope monitoring**	モニターリング モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /monitoring # **show new-faults**	ベースライン化後、およびアップグレード中のファブリック インターコネクトのリブートにより生成された障害を示します。
ステップ 3	UCS-A /monitoring # **show baseline-faults**	アップグレード中のファブリック インターコネクトのリブート前にベースライン化された障害を示します。

例

次に、アップグレードプロセスのさまざまな段階で生成された障害を表示する方法の例を示します。

プライマリ ファブリック インターコネクトのリブート前の障害

```
UCS-A# show fault
Severity  Code     Last Transition Time     ID       Description
--------- -------- ----------------------- -------- -----------
Major     F0283    2015-06-17T21:08:09.301     57360 fc VIF 687 on server 1 / 6 of switch
 A  down, reason: NPV upstream port not available
Warning   F0156    2015-06-17T21:07:44.114     53557 Server, vendor(Cisco Systems Inc),
 model(N20-B6620-1), serial(QCI133400WR) in slot 1/3 presence: mismatch
Major     F0283    2015-06-16T21:02:33.014     72467 fc VIF 688 on server 1 / 6 of switch
 B  down, reason: NPV upstream port not available
Major     F0207    2015-06-15T22:40:11.636     57312 Adapter  host interface 1/6/1/1
link state: down
Major     F0479    2015-06-15T22:40:11.635     57311 Virtual interface 687 link state
is down
Major     F0207    2015-06-15T22:40:11.633     57310 Adapter  host interface 1/6/1/2
link state: down
Major     F0479    2015-06-15T22:40:11.632     57309 Virtual interface 688 link state
is down
```

プライマリ ファブリック インターコネクトのリブート後の障害

```
UCS-A# show fault
Severity  Code     Last Transition Time     ID       Description
--------- -------- ----------------------- -------- -----------
Major     F0209    2015-06-17T21:40:49.301     57760 Adapter uplink interface on server
 1 / 6 of switch A  down, Please verify the connectivity to Fabric Interconnect.
Major     F0207    2015-06-17T21:40:11.636     57712 Adapter  host interface 1/6/1/1
link state: down
Major     F0479    2015-06-17T21:40:11.635     57711 Virtual interface 685 link state
is down
Major     F0283    2015-06-17T21:08:09.301     57360 fc VIF 687 on server 1 / 6 of switch
 A  down, reason: NPV upstream port not available
Warning   F0156    2015-06-17T21:07:44.114     53557 Server, vendor(Cisco Systems Inc),
 model(N20-B6620-1), serial(QCI133400WR) in slot 1/3 presence: mismatch
Major     F0283    2015-06-16T21:02:33.014     72467 fc VIF 688 on server 1 / 6 of switch
 B  down, reason: NPV upstream port not available
Major     F0207    2015-06-15T22:40:11.636     57312 Adapter  host interface 1/6/1/1
link state: down
Major     F0479    2015-06-15T22:40:11.635     57311 Virtual interface 687 link state
is down
```

```
Major     F0207    2015-06-15T22:40:11.633     57310 Adapter  host interface 1/6/1/2
link state: down
Major     F0479    2015-06-15T22:40:11.632     57309 Virtual interface 688 link state
is down
```

プライマリ ファブリック インターコネクトのリブートにより生成された障害を表示する方法

```
UCS-A /monitoring # show new-faults
Severity  Code     Last Transition Time     ID       Description
--------- -------- ----------------------- -------- -----------
Major     F0209    2015-06-17T21:40:49.301     57760 Adapter uplink interface on server
 1 / 6 of switch A  down, Please verify the connectivity to Fabric Interconnect.
Major     F0207    2015-06-17T21:40:11.636     57712 Adapter  host interface 1/6/1/1
link state: down
Major     F0479    2015-06-17T21:40:11.635     57711 Virtual interface 685 link state
is down
```

プライマリ ファブリック インターコネクトのリブート前の障害を表示する方法

```
UCS-A# show baseline-faults
Severity  Code     Last Transition Time     ID       Description
--------- -------- ----------------------- -------- -----------
Major     F0283    2015-06-17T21:08:09.301     57360 fc VIF 687 on server 1 / 6 of switch
 A  down, reason: NPV upstream port not available
Warning   F0156    2015-06-17T21:07:44.114     53557 Server, vendor(Cisco Systems Inc),
 model(N20-B6620-1), serial(QCI133400WR) in slot 1/3 presence: mismatch
Major     F0283    2015-06-16T21:02:33.014     72467 fc VIF 688 on server 1 / 6 of switch
 B  down, reason: NPV upstream port not available
Major     F0207    2015-06-15T22:40:11.636     57312 Adapter  host interface 1/6/1/1
link state: down
Major     F0479    2015-06-15T22:40:11.635     57311 Virtual interface 687 link state
is down
Major     F0207    2015-06-15T22:40:11.633     57310 Adapter  host interface 1/6/1/2
link state: down
Major     F0479    2015-06-15T22:40:11.632     57309 Virtual interface 688 link state
is down
```

ファブリック インターコネクトの動作の確認

Cisco UCS ドメイン をハイ アベイラビリティ クラスタ設定で実行する場合は、両方のファブリック インターコネクトの動作を確認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 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**	ファブリック インターコネクトの情報を表示します。

	コマンドまたはアクション	目的
		ファブリック インターコネクトの動作が Operable 状態であることを確認します。動作可能な状態でない場合は、**show tech-support** コマンドを実行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。**show tech-support** コマンドの詳細については、『*Cisco UCS Manager B-Series Troubleshooting Guide*』を参照してください。

例

次の例では、両方のファブリック インターコネクトの動作が Operable 状態として表示されています。

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect # show
Fabric Interconnect:
    ID OOB IP Addr     OOB Gateway     OOB Netmask     Operability
    -- --------------- --------------- --------------- -----------
    A  192.168.100.10  192.168.100.20  255.255.255.0   Operable

UCS-A /fabric-interconnect # exit
UCS-A# scope fabric-interconnect b
UCS-A /fabric-interconnect # show
Fabric Interconnect:
    ID OOB IP Addr     OOB Gateway     OOB Netmask     Operability
    -- --------------- --------------- --------------- -----------
    B  192.168.100.11  192.168.100.20  255.255.255.0   Operable
```

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **show cluster state**	ハイ アベイラビリティ クラスタの両方のファブリック インターコネクトの動作状態およびリーダーシップ ロールを表示します。 両方のファブリック インターコネクト（A および B）が Up 状態であること、および HA が Ready 状態であることを確

	コマンドまたはアクション	目的
		認します。ファブリック インターコネクトが Up 状態でない場合、または HA が Ready 状態でない場合、 **show tech-support** コマンドを実行し、シスコ テクニカル サポートにお問い合わせください。ファームウェア アップグレードに進まないでください。 **show tech-support** コマンドの詳細については、『*Cisco UCS Troubleshooting Guide*』を参照してください。 また、どのファブリック インターコネクトがプライマリ ロールで、どのファブリック インターコネクトが従属ロールであるかにも注目してください。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この情報が必要です。

例

次の例の表示では、両方のファブリック インターコネクトが Up 状態、HA が Ready 状態、ファブリックインターコネクトAがプライマリ ロール、ファブリックインターコネクト B が従属ロールです。

```
UCS-A# show cluster state
Cluster Id: 0x4432f72a371511de-0xb97c000de1b1ada4

A: UP, PRIMARY
B: UP, SUBORDINATE

HA READY
```

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

始める前に

このメンテナンス ポリシーを遅延展開のために設定する場合は、スケジュールを作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、[org-name] に **/** を入力します。
ステップ 2	UCS-A /org # **scope maint-policy default**	デフォルト メンテナンス ポリシーのメンテナンス ポリシー モードを開始します。
ステップ 3	UCS-A /org/maint-policy # **set reboot-policy** {**immediate** | **timer-automatic** | **user-ack**}	サービス プロファイルがサーバーに関連付けられている場合、関連付けを完了するにはサーバーをリブートする必要があります。reboot-policy コマンドを指定すると、このメンテナンス ポリシーを含むすべてのサービス プロファイルについて発生するタイミングを決定できます。有効な値は次のとおりです。 • **immediate**：サービス プロファイルが変更されると、すぐにサーバーがリブートします。 • **timer-automatic** ：**set scheduler** コマンドを使用して、メンテナンス操作が適用されるタイミングを指定するスケジュールを選択できます。スケジュールした時間に Cisco UCS によってサーバーがリブートされ、サービスプロファイルの変更が完了します。 • **user-ack** ：ユーザーは、変更が適用される前に **apply pending-changes** コマンドを使用して変更を明示的に確認する必要があります。

	コマンドまたはアクション	目的
		デフォルト メンテナンス ポリシーのリブート ポリシーを **user-ack** に設定することを推奨します。
ステップ 4	（任意） UCS-A /org/maint-policy # **set scheduler** *scheduler-name*	reboot-policy プロパティが timer-automatic に設定された場合、メンテナンス操作がサーバーに適用されるタイミングを指定するスケジュールを選択する必要があります。スケジュールした時間に Cisco UCS によってサーバーがリブートされ、サービスプロファイルの変更が完了します。
ステップ 5	UCS-A /org/maint-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

次に、デフォルト メンテナンス ポリシーのリブート ポリシーを変更し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # scope maint-policy default
UCS-A /org/maint-policy* # set reboot-policy user-ack
UCS-A /org/maint-policy* # commit-buffer
UCS-A /org/maint-policy #
```

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 モニタリング モードを開始します。

UCS-A# **scope monitoring**

ステップ 2 管理インターフェイス モニタリング ポリシーをイネーブルにするか、ディセーブルにします。

UCS-A /monitoring # **set mgmt-if-mon-policy admin-state** {**enabled** | **disabled**}

ステップ 3 UCS-A /monitoring # **commit-buffer**

トランザクションをシステムの設定にコミットします。

ステップ 4 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 5 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 6 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。

例

次に、管理インターフェイス モニタリング ポリシーを無効にし、トランザクションをコミットする例を示します。

```
UCS-A# scope monitoring
UCS-A /monitoring # set mgmt-if-mon-policy admin-state enabled
UCS-A /monitoring* # commit-buffer
UCS-A /monitoring #
```

I/O モジュールのステータスの確認

Cisco UCS がハイ アベイラビリティ クラスタ設定で実行されている場合、すべてのシャーシで両方の I/O モジュールのステータスを確認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 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 # **show**	指定したシャーシの指定した I/O モジュールのステータスを表示します。 I/O モジュールの全体的なステータスが Operable 状態であることを確認します。

	コマンドまたはアクション	目的
		全体的なステータスが Operable 状態ではない場合、 **show tech-support** コマンドを実行し、シスコ テクニカル サポートにお問い合わせください。ファームウェア アップグレードに進まないでください。 **show tech-support** コマンドの詳細については、『*Cisco UCS Troubleshooting Guide*』を参照してください。

例

次の例では、シャーシ 1 の両方の I/O モジュールの全体的なステータスが Operable 状態として表示されています。

```
UCS-A# scope chassis 1
UCS-A /chassis # scope iom 1
UCS-A /chassis/iom # show
IOM:
    ID         Side  Fabric ID Overall Status
    ---------- ----- --------- --------------
             1 Left  A         Operable

UCS-A /chassis/iom # exit
UCS-A /chassis # scope iom 2
UCS-A /chassis/iom # show
IOM:
    ID         Side  Fabric ID Overall Status
    ---------- ----- --------- --------------
             2 Right B         Operable
```

サーバのステータスの確認

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *chassis-id / server-id*	指定したシャーシの指定したサーバについて、シャーシのサーバ モードを入力します。
ステップ 2	UCS-A /chassis/server # **show status detail**	サーバのステータスの詳細を表示します。 サーバの全体的なステータスが Ok、Unavailable、または障害を示さない値か確認します。全体的なステータスが障害を示す状態（Discovery Failed など）の

	コマンドまたはアクション	目的
		場合、そのサーバのエンド ポイントはアップグレードできません。

例

次の例では、シャーシ 1 のサーバ 7 の全体的なステータスが Ok 状態として表示されています。

```
UCS-A# scope server 1/7
UCS-A /chassis/server # show status detail
Server 1/7:
    Slot Status: Equipped
    Conn Path: A,B
    Conn Status: A,B
    Managing Instance: B
    Availability: Unavailable
    Admin State: In Service
    Overall Status: Ok
    Oper Qualifier: N/A
    Discovery: Complete
    Current Task:
```

シャーシのサーバのアダプタのステータスの確認

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *chassis-id / server-id*	指定したシャーシ内の指定したサーバでシャーシ サーバ モードを開始します
ステップ 2	UCS-A /chassis/server # **show adapter status**	アダプタのステータスを表示します。 アダプタの全体的なステータスがOperable状態であることを確認します。アダプタの全体的なステータスがOperable以外の状態にある場合は、アップグレードできません。ただし、Cisco UCS ドメイン 内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。

例

次の例では、シャーシ 1 のサーバ 7 のアダプタの全体的なステータスが Operable 状態として表示されています。

```
UCS-A# scope server 1/7
UCS-A /chassis/server # show adapter status
```

```
Server 1/1:
    Overall Status
    --------------
    Operable
```

UCS Manager の正常性およびアップグレード前チェック ツール

UCS Manager の正常性およびアップグレード前チェック ツールは、アップグレード前にクラスタが正常であることを確認するために設計された、自動正常性およびアップグレード前チェック機能を提供します。この健全性チェックを実行するだけでなく、正常でないと判明したすべてのクラスタに対して修正措置を講じることが必要です。続行する前に、UCS Manager 正常性チェックによって報告されたすべての問題を修正してください。

データ パスの準備が整っていることの確認

（注） 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。

VIF パスとカウントは、Cisco UCS Manager GUI 内ではなく、CLI からのみモニターしてください。

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 [ナビゲーション]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。 この数がアップグレードの前に稼働していたイーサネット インターフェイスの数と一致することを確認します。
ステップ 3	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。	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。

オプション	説明
show platform fwm info hw-stm | grep '1.' | wc –l	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。
show hardware internal libsdk mtc l2 mac-table-ce valid-only | egrep "^ *[0-9]" | wc -l	UCS 6324（UCS Mini）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。
show hardware mac address-table 1 | wc -l	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。

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
```

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。