



# ファイバチャネル NPV

この章は、次の内容で構成されています。

- [ファイバチャネル接続の概要](#) (1 ページ)
- [NPV トラフィック管理](#) (4 ページ)
- [SAN A/B の分離](#) (7 ページ)
- [SAN ポート チャネル](#) (7 ページ)
- [ファイバチャネル N ポート仮想化のガイドラインと制限事項](#) (8 ページ)
- [ファイバチャネル N ポート仮想化でサポートされるハードウェア](#) (10 ページ)
- [ファイバチャネル N ポート仮想化の相互運用性](#) (10 ページ)
- [ファイバチャネル NPV GUI の設定](#) (11 ページ)
- [ファイバチャネル NPV NX-OS スタイル CLI の設定](#) (19 ページ)
- [ファイバチャネル NPV REST API の設定](#) (23 ページ)

## ファイバチャネル接続の概要

Cisco ACI では、N ポート仮想化 (NPV) モードを使用したリーフスイッチでのファイバチャネル (FC) 接続がサポートされています。NPV により、スイッチにおいて、ローカル接続されたホストポート (N ポート) からの FC トラフィックをノードプロキシ (NP ポート) アップリンクに集約して、コアスイッチに送ることができます。

スイッチは、NPV を有効にした後は NPV モードになります。NPV モードはスイッチ全体に適用されます。NPV モードのスイッチに接続するエンドデバイスはそれぞれ、この機能を使用するために N ポートとしてログインする必要があります (ループ接続デバイスはサポートされていません)。(NPV モードの) エッジスイッチから NPV コアスイッチへのすべてのリンクは、(E ポートではなく) NP ポートとして確立されます。このポートは、通常のスイッチ間リンクに使用されます。



- (注) FC NPV アプリケーションにおける ACI リーフ スイッチの役割は、ローカル接続された SAN ホストとローカル接続されたコアスイッチ間の FC トラフィックのパスを提供することです。リーフ スイッチでは SAN ホスト間のローカル スイッチングは行われず、FC トラフィックはスパイン スイッチに転送されません。

### FC NPV の利点

FC NPV では次の機能を提供します。

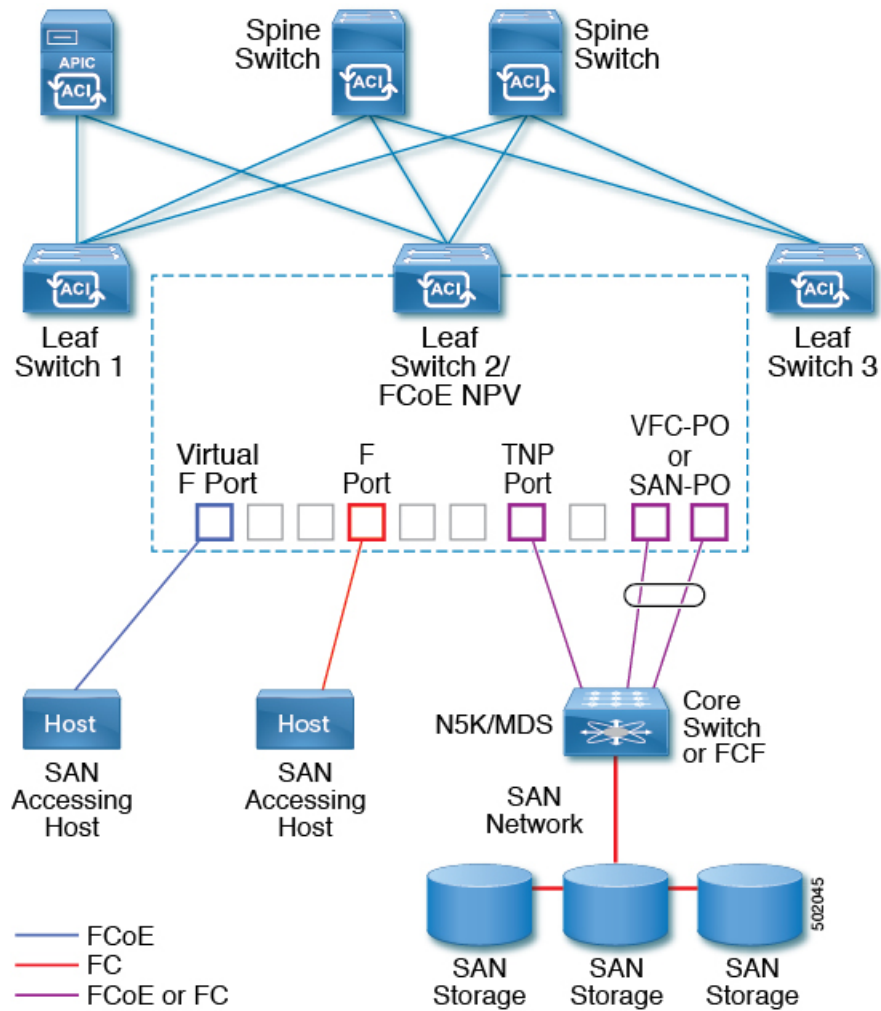
- ファブリックでドメイン ID を追加しなくても、ファブリックに接続するホスト数が増加します。NPV のコアスイッチのドメイン ID は、複数の NPV スイッチ間で共有されます。
- FC ホストと FCoE ホストは、ネイティブの FC インターフェイスを使用して SAN ファブリックに接続します。
- トラフィックの自動マッピングによるロード バランシング。NPV に接続しているサーバを新しく追加した場合に、トラフィックが現在のトラフィック負荷に基づいて、外部のアップリンク間で自動的に分散されます。
- トラフィックの静的マッピング。NPV に接続しているサーバを、外部のアップリンクに静的にマッピングすることができます。

### FC NPV モード

ACI の Feature-set `fcoe-npv` は、最初に FCoE/FC 設定がプッシュされるときに、デフォルトで自動的に有効になります。

### FC トポロジ

ACI ファブリック経由の FC トラフィックをサポートするさまざまな設定のトポロジを、次の図に示します。



- ACI リーフスイッチ上のサーバー/ストレージホストインターフェイスは、ネイティブの FC ポートか仮想 FC (FCoE) ポートのどちらかとして機能するように設定できます。
- FC コアスイッチへのアップリンクインターフェイスは、次のいずれかのポートタイプとして設定できます。
  - ネイティブ FC NP ポート
  - SAN-PO NP ポート
- FCF スイッチへのアップリンク インターフェイスは、次のいずれかのポートタイプとして設定できます。
  - 仮想 (vFC) NP ポート
  - vFC-PO NP ポート

- N ポート ID 仮想化 (NPV) がサポートされており、デフォルトで有効になっています。そのため、単一のリンクを経由して N ポートに複数の N ポート ID またはファイバチャネル ID (FCID) を割り当てるのが可能です。
- コアスイッチへの NP ポートでは、トランキングを有効にすることができます。トランキングにより、ポートで複数の VSAN をサポートできます。トランクモードが有効になった NP ポートのことを、TNP ポートと呼びます。
- 複数の FC NP ポートを結合してコアスイッチへの SAN ポートチャネル (SAN-PO) とすることができます。トランキングは SAN ポートチャネルでサポートされます。
- FCF ポートでは 4/16/32 Gbps および自動速度設定がサポートされますが、ホストインターフェイスでは 8Gbps はサポートされません。デフォルトの速度は「auto」です。
- FC NP ポートでは、4/8/16/32 Gbps および自動速度設定がサポートされます。デフォルトの速度は「auto」です。
- Flogi に続く複数の FDISC (ネスト NPV) は、FC/FCoE ホストと FC/FCoE NP リンクによってサポートされます。
- FEX の背後にある FCoE ホストは、FCoE NP/アップリンクを介してサポートされます。
- APIC 4.1(1) リリース以降、FEX の背後にある FCoE ホストは、ファイバチャネル NP/アップリンクを介してサポートされます。
- 1 つの FEX の背後にあるすべての FCoE ホストは、複数の vFC および vFC-PO アップリンク間、または単一のファイバチャネル/SAN ポートチャネルアップリンクを通じてロードバランシングできます。
- SAN ブートは、FEX で FCoE アップリンク経由でサポートされます。
- APIC 4.1(1) リリース以降、SAN ブートは FC/SAN-PO アップリンクでもサポートされます。
- SAN ブートは、FEX を介して接続された FCoE ホストの vPC を介してサポートされます。

## NPV トラフィック管理

通常は、すべてのトラフィックにおいて、すべての使用可能なアップリンクの使用を許可することをお勧めします。NPV トラフィック管理は、自動トラフィック エンジニアリングがネットワーク要件を満たさない場合にだけ使用してください。

### 自動アップリンク選択

NPV は、外部 NP アップリンク インターフェイスの自動選択をサポートしています。サーバ (ホスト) インターフェイスがアップになると、サーバ インターフェイスと同じ VSAN 内で利用可能な外部インターフェイスから、負荷が最も少ない外部インターフェイスが選択されます。

新しい外部インターフェイスが動作可能になっても、新たに利用可能になったアップリンクを含めるために既存の負荷は自動的に再分散されません。外部インターフェイスが新しいアップリンクを選択できるようになってから、サーバインターフェイスが動作します。

## トラフィック マップ

FCNPVは、トラフィックマップをサポートしています。トラフィックマップにより、サーバ（ホスト）インターフェイスがコアスイッチに接続するために使用可能な外部（NPアップリンク）インターフェイスを指定できます。



**Note** FCNPVトラフィックマップがサーバインターフェイスに設定されると、サーバインターフェイスはそのトラフィックマップ内の外部インターフェイスからのみ選択する必要があります。指定された外部インターフェイスがいずれも動作していない場合、サーバは非動作状態のままになります。

FC NPV トラフィック マップ機能を使用すると、次のようなメリットが得られます。

- 特定のサーバインターフェイス（またはサーバインターフェイスの範囲）に外部インターフェイスの事前設定された設定を割り当てることによって、トラフィックエンジニアリングが容易になります。
- インターフェイスの再初期化またはスイッチの再起動後に、サーバインターフェイスは同じトラフィックパスを提供することで、常に同じ外部インターフェイス（または指定された外部インターフェイスのセットのいずれか）に接続するので、永続的なFCID機能の適切な動作が確保されます。

## 複数の NP リンクにまたがるサーバログインの破壊的自動ロードバランシング

FCNPVは、サーバログインの中断的ロードバランシングをサポートしています。中断的ロードバランシングが有効の場合、新しいNPアップリンクが動作すると、FCNPVによって、サーバインターフェイスがすべての利用可能なNPアップリンクにわたって再分配されます。サーバインターフェイスを一方のNPアップリンクからの他方のNPアップリンクに移動するために、FCNPVはサーバインターフェイスを強制的に再初期化して、サーバがコアスイッチへのログインを新たに実行するようにします。

別のアップリンクに移されたサーバインターフェイスだけが再初期化されます。移されたサーバインターフェイスごとにシステムメッセージが生成されます。



**Note** サーバインターフェイスを再配布すると、接続されたエンドデバイスへのトラフィックが中断されます。既存のポートチャネルにメンバーを追加しても、中断的自動ロードバランシングはトリガーされません。

サーバトラフィックの中断を避けるために、新しいNPアップリンクを追加してから、この機能をイネーブルし、サーバインターフェイスが再配布されてからこの機能を再度ディセーブルにしてください。

ディスラプティブロードバランシングがイネーブルでない場合、サーバインターフェイスの一部またはすべてを手動で再初期化して、新しいNPアップリンクインターフェイスにサーバトラフィックを分散することができます。

## FC NPV トラフィック管理のガイドライン

FC NPV トラフィック管理を導入するには、次の注意事項に従ってください。

- NPV トラフィック管理は、自動トラフィック エンジニアリングがネットワーク要件を満たさない場合にだけ使用してください。
- すべてのサーバインターフェイスにトラフィック マップを設定する必要はありません。FC NPV はデフォルトで自動トラフィック管理を使用します。
- NPアップリンクインターフェイスのセットを使用するように設定されたサーバインターフェイスは、利用可能なNPアップリンクインターフェイスがなくても、他の利用可能なNPアップリンクインターフェイスを使用できません。
- ディスラプティブロードバランシングがイネーブルになると、サーバインターフェイスは1つのNPアップリンクから別のNPアップリンクに移動される場合があります。NPアップリンクインターフェイス間を移動する場合、FCNPVではコアスイッチに再度ログインする必要があり、トラフィックの中断が生じます。
- サーバのセットを特定のコアスイッチにリンクするには、サーバインターフェイスをNPアップリンクインターフェイスのセット（すべてこのコアスイッチに接続されている）に関連付けてください。
- コアスイッチに永続的なFC IDを設定し、トラフィックマップ機能を使用してサーバインターフェイスのトラフィックをNPアップリンクに送ります（すべてのアップリンクが関連付けられたコアスイッチに接続しています）。
- トラフィックマップの固定を初めて設定する際は、最初のトラフィックマップを設定する前に、サーバのホストポートをシャットダウンする必要があります。
- トラフィックのマッピングを複数のアップリンクに設定していて、ホストへのログインに使用されるトラフィックマップを削除する場合は、先にホストをシャットダウンする必要があります。
- FEXの背後にあるFCoEホストのトラフィックマップを設定する場合、1つのホストを複数のFCoE NP/アップリンク（VFCまたはVFC-PO）または単一のファイバチャネル/SANポートチャネルNP/アップリンクにマッピングできます。

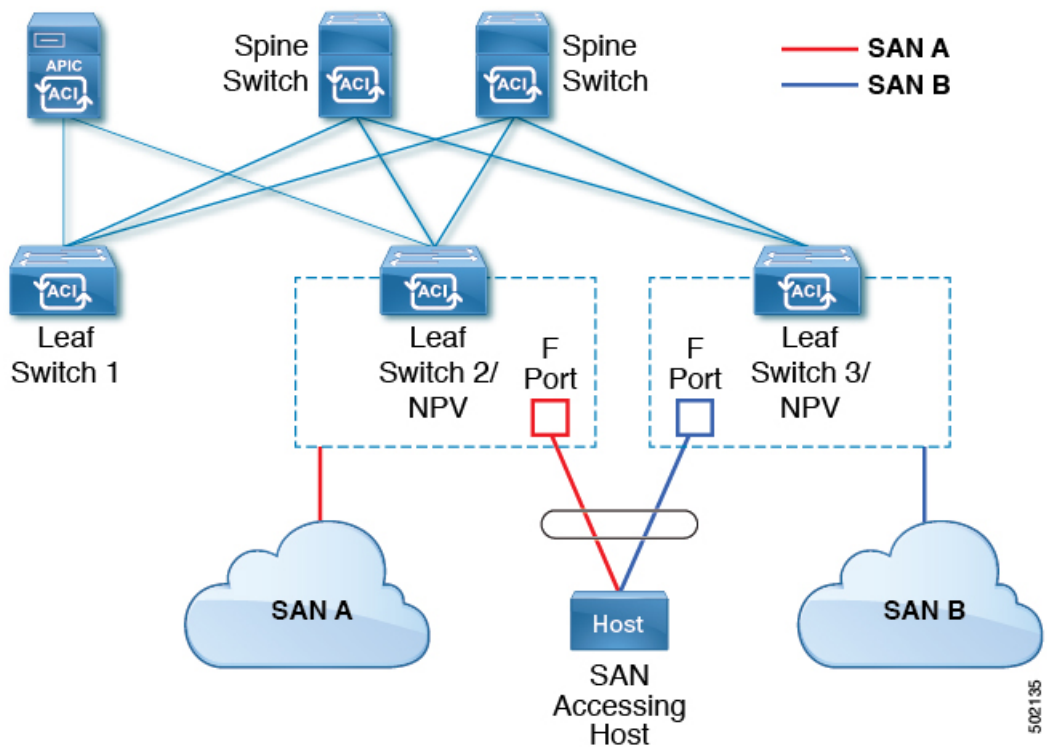


**Note** サーバが外部インターフェイスに静的にマッピングされている場合は、外部インターフェイスが何らかの理由でダウンする事態に備えて、サーバトラフィックが再分配されません。

## SAN A/B の分離

SAN A と SAN B の分離により、いずれかのファブリック コンポーネントが障害を起こしても SAN 接続が使用できることが保証されます。SAN A と SAN B の分離は、ファブリック全体で導入されている VSAN を分割することで、物理的または論理的に実現できます。

図 1: SAN A/B の分離



## SAN ポート チャンネル

### SAN ポート チャンネルについて

- SAN ポート チャンネルは、同じファイバチャネル ノードに接続された一組の FC インターフェイスを結合して 1 つのリンクとして動作させる論理インターフェイスです。
- SAN ポート チャンネルにより、帯域の利用率と可用性がサポートされます。

- Cisco ACI スイッチの SAN ポート チャンネルは、FC コア スイッチに接続するため、そして VSAN のアップリンク間で最適な帯域幅利用と透過型のフェールオーバーを実現するために使用されます。

### SAN ポート チャンネルのガイドラインと制限事項

- Cisco ACI スイッチのアクティブ ポート チャンネルの最大数 (SAN ポート チャンネルと VFC アップリンク/NP ポート チャンネルの合計) は 7 です。追加で設定されたポート チャンネルはすべて、既存のいずれかのアクティブ ポート チャンネルをシャットダウンまたは削除するまで、**errdisabled** 状態のままです。既存のアクティブ ポート チャンネルをシャットダウンまたは削除してから、**errdisabled** のポート チャンネルを shut/no shut してアップします。
- SAN ポート チャンネルに結合できる FC インターフェイスの最大数は 16 個に制限されます。
- SAN ポート チャンネルの Cisco ACI スイッチでのデフォルトのチャンネル モードは**アクティブ**です。これは変更できません。
- SAN ポート チャンネルがコア スイッチとして Cisco FC コア スイッチに接続されている場合は、アクティブなチャンネル モードだけがサポートされます。Cisco FC コア スイッチでアクティブなチャンネルモードを設定する必要があります。

### SAN ポート チャンネル モードについて

SAN ポート チャンネルは、デフォルトではチャンネル モードがアクティブの状態を設定されています。アクティブの場合、ピア ポートのチャンネルグループ モードに関係なく、メンバー ポートはピア ポートとのポートチャンネルプロトコルのネゴシエーションを開始します。チャンネルグループで設定されているピア ポートがポートチャンネルプロトコルをサポートしていない場合、またはネゴシエーション不可能を示すステータスを返す場合、ポートチャンネルは無効になります。アクティブのポートチャンネルモードでは、片側でポートチャンネルメンバーのポートの有効化および無効化を明示的に行わなくても、自動回復が可能です。

## ファイバチャンネル N ポート仮想化のガイドラインと制限事項

ファイバチャンネル N ポート仮想化 (NPV) を設定する場合、次の注意事項および制限事項に注意してください。

- ファイバチャンネル NP ポートはトランク モードをサポートしますが、ファイバチャンネル F ポートはサポートしません。
- トランク ファイバチャンネルポートでは、最も高い VSAN により内部ログインが行われません。
- コア スイッチで次の機能を有効にする必要があります。



```
feature npiv
feature fport-channel-trunk
```

- 8G のアップリンク速度を使用する場合は、コア スイッチで IDLE フィル パターンを設定する必要があります。



(注) Cisco MDS スイッチでの IDLE フィル パターンの設定例を次に示します。

```
Switch(config)# int fc2/3
Switch(config)# switchport fill-pattern IDLE speed 8000
Switch(config)# show run int fc2/3
```

```
interface fc2/3
switchport speed 8000
switchport mode NP
switchport fill-pattern IDLE speed 8000
no shutdown
```

- Cisco APIC 4.1(1) リリース以降では、ファイバチャネル NPV のサポートは Cisco N9K-C93180YC-FX スイッチに限定されます。
- ファイバチャネル設定にはポート 1 ~ 48 を使用できます。ポート 49 ~ 54 をファイバチャネルポートにすることはできません。
- ポートをイーサネットからファイバチャネルに、またはその逆に変換する場合は、スイッチをリロードする必要があります。Currently, you can convert only one contiguous range of ports to Fibre Channel ports, and this range must be a multiple of 4, ending with a port number that is a multiple of 4.現時点で変換できるのは、ファイバチャネルポートの連続した範囲のポートだけです。そしてこの範囲は4の倍数である必要があります、最後のポート番号は4の倍数になっている必要があります。たとえば、1 ~ 4、1 ~ 8、21 ~ 24 などです。
- Brocade ポート ブレードファイバチャネル 16 ~ 32 へのファイバチャネルアップリンク (NP) 接続は、Cisco N9K-93180YC-FX リーフスイッチポートが 8G の速度で設定されている場合はサポートされません。
- 選択したポートの速度が SFP によってサポートされている必要があります。たとえば、32G の SFP は 8/16/32G をサポートするため、4G のポート速度には 8G または 16G の SFP が必要です。16G の SFP のサポートは 4/8/16G であるため、32G のポート速度には 32G の SFP が必要です。
- 速度の自動ネゴシエーションがサポートされています。デフォルトの速度は「auto」です。
- 40G およびブレークアウトポートではファイバチャネルを使用できません。
- FEX を FC ポートに直接接続することはできません。
- FEX HIF ポートを FC に変換することはできません。

## ファイバチャネル N ポート仮想化でサポートされるハードウェア

ファイバチャネル N ポート仮想化 (FC NPV) は、次のスイッチでサポートされます。

- N9K-C93108TC-FX
- N9K-C93180YC-FX

次のファイバチャネル Small Form-Factor Pluggable (SFP) トランシーバはサポートされていません。

- DS-SFP-FC8G-SW : 2/4/8G (2G の FC NPV ポート速度はサポート外)
- DS-SFP-FC16G-SW : 4/8/16G (FC NPV ポート速度が 32G の場合は非互換)
- DS-SFP-FC32G-SW : 8/16/32G (FC NPV ポート速度が 4G の場合は非互換)

サポートされている NPIV コア スイッチは、Cisco Nexus 5000 シリーズ、Nexus 6000 シリーズ、Nexus 7000 シリーズ (FCoE)、および Cisco MDS 9000 シリーズ マルチレイヤ スイッチです。

## ファイバチャネル N ポート仮想化の相互運用性

次の表に、Cisco Application Policy Infrastructure Controller (APIC) のファイバチャネル N ポート仮想化 (FC NPV) 機能の相互運用性がテストされたサードパーティ製品を示します。

表 1: FC NPV でサポートされるサードパーティ製品

サードパーティ スイッチ ベンダー	Brocade
サードパーティ ハードウェア モデル	DS-6620B
サードパーティ ソフトウェア リリース	8.2.1a
Cisco NX-OS リリース	14.1(1) 以降
Cisco Nexus 9000 モデル	N9K-C93180YC-FX
相互運用性モード	NA (NPV)
Cisco SFP モジュール	DS-SFP-FC32G-SW
サードパーティ SFP モジュール	Brocade-32G

# ファイバチャネル NPV GUI の設定

## GUI を使用したネイティブ ファイバチャネル ポート プロファイルの設定

この手順では、ファイバチャネルのホスト（サーバなど）に接続するための一連のネイティブファイバチャネル（FC）Fポートの設定を行います。

設定を簡単に行うため、この手順では **[Configure Interface, PC, and vPC]** ウィザードを使用します。

### 手順

**ステップ 1** APIC メニューバーで、**[Fabric] > [Access Policies] > [Quickstart]** に移動し、**[Configure an interface, PC, and vPC]** をクリックします。

**ステップ 2** **[Configured Switch Interfaces]** ツールバーで、**[+]** をクリックしてスイッチプロファイルを作成します。次のアクションを実行します。

このスイッチプロファイルでは、サーバホストポートを設定します。別のスイッチプロファイルでは、アップリンクポートを設定します。

a) **[Switches]** ドロップダウンリストで、**NPV リーフ スイッチ** を選択します。

この操作によって、自動的にリーフ スイッチ プロファイルが作成されます。**[Switch Profile Name]** テキスト ボックスで、リーフ スイッチ プロファイルの名前を受け入れるか変更できます。

- b) さらにインターフェイス設定を開くには、ポートで大きな緑色の **[+]** をクリックします。
- c) **[Interface Type]** で、**[FC]** を選択して、ファイバチャネル ホスト インターフェイス ポート（F ポート）を指定します。
- d) **[Interfaces]** で、FC ポートのポート範囲を入力します。

FC ポートに変換できるポートの連続範囲は1つだけです。この範囲は4の倍数にする必要があります、4の倍数のポート番号で終わる必要があります（たとえば、1～4、1～8、21～24は有効な範囲です）。

この操作によってインターフェイスセクタポリシーが作成されます。**[Interface Selector Name]** テキスト ボックスで、ポリシーの名前を受け入れるか変更できます。

**(注)** イーサネットからFCへのポートの変換には、スイッチのリロードが必要です。インターフェイスポリシーを適用すると、スイッチをリロードするよう求める通知アラームがGUIに表示されます。スイッチのリロード中はスイッチへの通信が中断され、スイッチにアクセスしようとするタイムアウトになります。

- e) [Policy Group Name] ドロップダウンリストで、[Create FC Interface Policy Group] を選択します。
- f) [Create FC Interface Policy Group] ダイアログボックスで、[Name] フィールドに名前を入力します。
- g) [Fibre Channel Interface Policy] ドロップダウンリストで、[Create Fibre Channel Interface Policy] を選択します。
- h) [Create Fibre Channel Interface Policy] ダイアログボックスで、[Name] フィールドに名前を入力し、次の設定を行います。

フィールド	設定
ポート モード	ホスト インターフェイスの場合、[F] を選択します。
Trunk Mode	ホスト インターフェイスの場合、[trunk-off] を選択します。
速度	[auto] (デフォルト) を選択します。
[自動最大速度 (Auto Max Speed)]	Auto Max Speed設定は、速度が <b>auto</b> の場合にのみ適用されます。  [Auto Max Speed]は、速度が自動モードのときに最大速度を制限します。
Receive Buffer Credit	[64] を選択します。

- i) [Submit] をクリックして、ファイバチャネル インターフェイス ポリシーを保存し、[Create FC Interface PolicyGroup] ダイアログボックスに戻ります。
- j) [Attached Entity Profile] ドロップダウンリストで、[Create Attachable Access Entity Profile] を選択します。  
  
アタッチ可能なエンティティ プロファイルのオプションでは、リーフ アクセス ポート ポリシーを展開するインターフェイスを指定します。
- k) [Name] フィールドに、アタッチ可能なエンティティのポリシーの名前を入力します。
- l) [Domains (VMM, Physical, or External) To Be Associated To Interfaces] ツールバーで、[+] をクリックしてドメイン プロファイルを追加します。
- m) [Domain Profile] ドロップダウンリストで、[Create Fibre Channel Domain] を選択します。
- n) [Name] フィールドに、ファイバチャネル ドメインの名前を入力します。
- o) [VSAN Pool] ドロップダウンリストで、[Create VSAN Pool] を選択します。
- p) [Name] フィールドに、VSAN プールの名前を入力します。
- q) [Encap Blocks] ツールバーで、[+] をクリックして VSAN 範囲を追加します。
- r) [Create VSAN Ranges] ダイアログボックスで、[From] および [To] の VSAN 番号を入力します。
- s) [Allocation Mode] で、[Static Allocation] を選択し、[OK] をクリックします。
- t) [Create VSAN Ranges] ダイアログボックスで、[Submit] をクリックします。

- u) [Create Fibre Channel Domain] ダイアログボックスで、[Submit] をクリックします。
  - (注) ファイバチャネルドメインでは、FCoE ではなくネイティブ FC ポートを使用する場合、VLAN プールや VSAN 属性を設定する必要はありません。
- v) [Create Attachable Access Entity Profile] ダイアログボックスで、[Update] をクリックしてファイバチャネルドメインプロファイルを選択し、[Submit] をクリックします。
- w) [Create FC Policy Group] ダイアログボックスで、[Submit] をクリックします。
- x) [Configure Interface, PC, and vPC] ダイアログボックスで、[Save] をクリックして、サーバーホストポートのこのスイッチプロファイルを保存します。
  - (注) イーサネットから FC へのポートの変換には、スイッチのリロードが必要です。インターフェイスポリシーを適用すると、スイッチをリロードするよう求める通知アラームが GUI に表示されます。スイッチのリロード中はスイッチへの通信が中断され、スイッチにアクセスしようとするするとタイムアウトになります。
  - (注) たとえば、アップリンクをダウンリンクとして再設定し、スイッチをリロードするなど、スイッチのポートプロファイルを変更すると、スイッチが Cisco APIC から設定を取得するまで、スイッチとの通信が中断されます。

[Fabric] > [Access Policies] > [Switches] > [Leaf Switches] > [Profiles] > [<名前>] で、[Leaf Profiles] 作業ペインの [Associated Interface Selector Profiles] リストにファイバチャネルポートプロファイルが表示されます。

#### 次のタスク

- ファイバチャネルアップリンク接続プロファイルを設定します。
- テナント内のサーバポートとアップリンクポートを展開し、ファイバチャネルのコアスイッチに接続します。

## GUI を使用したネイティブ FC ポートチャネル プロファイルの設定

この手順では、ファイバチャネルのコアスイッチへのアップリンク接続に使用するネイティブファイバチャネルポートチャネル (FC PC) プロファイルを設定します。



- (注) この手順は、[Configure Interface, PC, and vPC] ウィザードを使用して実行することもできます。

#### 始める前に

アタッチ可能なエンティティプロファイルを含む、アップリンク接続を設定します。

## 手順

**ステップ 1** [Fabric] > [Access Policies] > [Interfaces] > [Leaf Interfaces] > [Profiles] の順に展開します。

**ステップ 2** [Profiles] を右クリックし、[Create Leaf Interface Profile] をクリックします。

**ステップ 3** [Create Leaf Interface Profile] ダイアログボックスで、次の手順を実行します。

- a) [Name] フィールドに、リーフ インターフェイス プロファイルの名前を入力します。
- b) [Interface Selectors] ツールバーで、[+] をクリックして [Create Access Port Selector] ダイアログボックスを表示します。
- c) [Name] フィールドに、ポート セレクタの名前を入力します。
- d) [Interface IDs] フィールドで、FC PC ポートのポート範囲を入力します。

ポート チャネルには最大 16 個のポートを持たせることができます。

FC ポートに変換できるポートの連続範囲は1つだけです。この範囲は4の倍数にする必要があり、4の倍数のポート番号で終わる必要があります（たとえば、1～4、1～8、21～24は有効な範囲です）。

(注) イーサネットからFCへのポートの変換には、スイッチのリロードが必要です。インターフェイスポリシーを適用すると、スイッチを手動でリロードするよう求める通知アラームがGUIに表示されます。スイッチのリロード中はスイッチへの通信が中断され、スイッチにアクセスしようとするときタイムアウトになります。

- e) [Interface Policy Group] ドロップダウンリストで、[Create FC PC Interface Policy Group] を選択します。
- f) [Name] フィールドに、FCPC インターフェイス ポリシー グループの名前を入力します。
- g) [Fibre Channel Interface Policy] ドロップダウンリストで、[Create Fibre Channel Interface Policy] を選択します。
- h) [Name] フィールドに、FC PC インターフェイス ポリシーの名前を入力します。
- i) [Create Interface FC Policy] ダイアログボックスで、[Name] フィールドに名前を入力し、次の設定を行います。

フィールド	設定
ポート モード	アップリンク インターフェイスの場合、[NP] を選択します。
Trunk Mode	アップリンク インターフェイスの場合、[trunk-on] を選択します。

- j) [Submit] をクリックして、FC PC インターフェイス ポリシーを保存し、[Create FC PC Interface Policy Group] ダイアログボックスに戻ります。
- k) **Port Channel Policy** ドロップで、**Create Port Channel Policy** を選択します。
- l) [Name] フィールドに、ポート チャネル ポリシーの名前を入力します。

このメニューにある他の設定は無視できます。

- m) [Submit] をクリックして、ポート チャネル ポリシーを保存し、[Create FC PC Interface Policy Group] ダイアログボックスに戻ります。
- n) [Attached Entity Profile] ドロップダウンリストで、既存のアタッチ可能なエンティティプロフィールを選択します。
- o) [Submit] をクリックして [Create Access Port Selector] ダイアログボックスに戻ります。
- p) [OK] をクリックして [Create Leaf Interface Profile] ダイアログボックスに戻ります。
- q) [OK] をクリックして [Leaf Interfaces - Profiles] 作業ペインに戻ります。

**ステップ 4** [Fabric] > [Access Policies] > [Switches] > [Leaf Switches] > [Profiles] の順に展開します。

**ステップ 5** 作成したリーフ スイッチ プロファイル を右クリックし、[Create Interface Profile] をクリックします。

**ステップ 6** [Create Interface Profile] ダイアログボックスで、次の手順を実行します。

- a) [Interface Select Profile] ドロップダウンリストで、ポート チャネル用に作成したリーフ インターフェイス プロファイルを選択します。
- b) [Submit] をクリックして [Leaf Interfaces - Profiles] 作業ペインに戻ります。

(注) イーサネットから FC へのポートの変換には、スイッチのリロードが必要です。インターフェイスポリシーを適用すると、スイッチをリロードするよう求める通知アラームが GUI に表示されます。スイッチのリロード中はスイッチへの通信が中断され、スイッチにアクセスしようとするときタイムアウトになります。

[Fabric] > [Access Policies] > [Switches] > [Leaf Switches] > [Profiles] > [<名前>] で、作業ペインの [Associated Interface Selector Profiles] リストに FC ポート チャネル プロファイルが表示されます。

---

### 次のタスク

テナント内のサーバポートとアップリンクポートを展開し、ファイバチャネルのコアスイッチに接続します。

## ファイバチャネル ポートの展開

この手順では、ファイバチャネルサーバホストポートとアップリンクポートをアクティブにします。

### 始める前に

- ファイバチャネル (FC) サーバホストポート プロファイル (F ポート) を設定します。
- FC アップリンク ポート プロファイル (NP または TNP ポート) を設定します。
- 関連付けられている 2 つのインターフェイス セレクタ プロファイル (1 つはホストポート用、1 つはアップリンクポート用) を含むリーフスイッチプロファイルを設定します。

## 手順

- ステップ 1** [Tenants] > [<テナント名>] > [Application Profiles] の順に展開します。  
テナントが存在しない場合は、テナントを作成する必要があります。
- ステップ 2** [Application Profiles] を右クリックし、[Create Application Profile] をクリックして、次の操作を実行します。
- [Name] フィールドに、アプリケーション プロファイルの名前を入力します。
  - [Submit] をクリックします。
- ステップ 3** [Tenants] > [<テナント名>] > [Application Profiles] > [<名前>] > [Application EPGs] の順に展開します。
- ステップ 4** [Application EPGs] を右クリックし、[Create Application EPG] をクリックして、次の操作を実行します。
- ステップ 5** [Create Application EPG] ダイアログボックスで、次の操作を実行します。
- [Name] フィールドに、アプリケーション EPG の名前を入力します。
  - 次を設定します。
- | フィールド                         | 設定                   |
|-------------------------------|----------------------|
| <b>Intra EPG Isolation</b>    | [Unenforced] を選択します。 |
| <b>Preferred Group Member</b> | [Exclude] を選択します。    |
| <b>カプセル化のフラッディング</b>          | [Disabled] を選択します。   |
- [Bridge Domain] ドロップダウンリストで、[Create Bridge Domain] を選択します。
  - [Name] フィールドに、ブリッジ ドメインの名前を入力します。
  - [Type] で、[fc] を選択してファイバチャンネルブリッジドメインを指定します。
  - [VRF] ドロップダウンリストで、[Create VRF] を選択します。
  - [Name] フィールドに、VRF の名前を入力します。
  - [Submit] をクリックして [Create Bridge Domain] ダイアログボックスに戻ります。
  - [Next]、[Next]、[Finish] の順にクリックして [Create Application EPG] ダイアログボックスに戻ります。
  - [Finish] をクリックします。
- ステップ 6** [Tenants] > [<テナント名>] > [Application Profiles] > [<名前>] > [Application EPGs] > [<名前>] > [Domains (VMs and Bare-Metals)] の順に展開します。
- ステップ 7** [Domains (VMs and Bare-Metals)] を右クリックし、[Add Fibre Channel Domain Association] をクリックして、次の操作を実行します。
- [Fibre Channel Domain Profile] ドロップダウンリストで、ホストポートの設定時に作成したファイバチャンネルドメインを選択します。
  - [Submit] をクリックします。



**ステップ 8** [Tenants] > [<テナント名>] > [Application Profiles] > [<名前>] > [Application EPGs] > [<名前>] > [Fibre Channel (Paths)] の順に展開し、次の操作を実行します。

このステップでは、サーバ ホスト ポートを展開します。

- a) [Fibre Channel (Paths)] を右クリックし、[Deploy Fibre Channel] をクリックします。
- b) [Path Type] コントロールで、[Port] をクリックします。
- c) [Node] ドロップダウンリストで、リーフ スイッチを選択します。
- d) [Path] ドロップダウンリストで、サーバ ホスト ポートとして設定されているリーフ スイッチ ポートを選択します。
- e) [VSAN] フィールドに、ポートの VSAN を入力します。
- f) [VSAN Mode] コントロールで、[Native] をクリックします。
- g) [Type] が fcoe であることを確認します。
- h) (オプション) トラフィック マップを必要とする場合は、[Pinning Label] ドロップダウンリストを使用します。

(注) 複数のアップリンク ポートが使用可能で、ホスト ポートにおいて常にその FLOGI を特定のアップリンクに送るようにする場合は、固定プロファイル (トラフィック マップ) を作成してホスト ポートをアップリンク ポートに関連付けることができます。そのようにしない場合は、使用可能なアップリンク ポート間でホストがロードバランスされます。

- i) [Submit] をクリックします。
- j) ファイバチャネルポート ホストごとに**ステップ a** から繰り返します。

**ステップ 9** [Tenants] > [<テナント名>] > [Application Profiles] > [<名前>] > [Application EPGs] > [<名前>] > [Fibre Channel (Paths)] の順に展開し、次の操作を実行します。

このステップでは、アップリンク ポート チャネルを展開します。

- a) [Fibre Channel (Paths)] を右クリックし、[Deploy Fibre Channel] をクリックします。
- b) [Path Type] コントロールで、[Direct Port Channel] をクリックします。
- c) [Port Type] ドロップダウンリストで、アップリンク ポートチャネルを選択します。
- d) [VSAN] フィールドに、ポートのデフォルトの VSAN を入力します。
- e) [VSAN Mode] コントロールで、ポートの VSAN の場合は [Native] をクリックし、トランクの VSAN の場合は [Regular] をクリックします。
- f) [Type] が fcoe であることを確認します。
- g) [Submit] をクリックします。
- h) ファイバチャネルアップリンク ポートまたはポート チャネルごとに**ステップ a** から繰り返します。

## ファイバチャネルポートのトラフィック マップの設定

複数のアップリンク ポートが使用可能なアプリケーションでは、デフォルトで、サーバトラフィックが使用可能なアップリンク ポート間でロードバランスされます。場合によっては、1

つ以上の特定のアップリンク ポートまたはポート チャンネルにログイン要求 (FLOGI) を送信するようサーバを設定する必要があります。このような場合、固定プロファイル (トラフィック マップ) を作成して、それらのアップリンク ポートまたはポート チャンネルにサーバポートを関連付けることができます。

この手順では、1 つ以上のサーバポートと 1 つ以上のアップリンク ポートまたはポート チャンネルがすでに設定済みであると仮定します。サーバポートがすでに設定済みであるため、最初に、アップリンクにマッピングするすべてのサーバポートをシャットダウン (無効化) する必要があります。トラフィック マップを設定した後で、再度ポートを有効にします。

### 始める前に

この手順では、次の項目がすでに設定済みであることを前提としています。

- サーバポート (F ポート) およびアップリンク ポートまたはポート チャンネル (NP ポート)
- テナント (アプリケーション プロファイルおよびアプリケーション EPG を含む)



(注) 固定プロファイル (トラフィック マップ) を作成する前に、アップリンクにマッピングするサーバポートをシャットダウンする必要があります。

### 手順

- ステップ 1** [Fabric] > [Inventory] > [Pod <n>] > [Leaf <n>] > [Interfaces] > [FC Interfaces] 作業ウィンドウを選択し、アップリンクにマッピングするサーバインターフェイス ポートを選択して無効にします。
- ステップ 2** [Tenants] > [<テナント名>] > [Application Profiles] > [<アプリケーション プロファイル名>] > [Application EPGs] > [<EPG 名>] > [Fibre Channel (Paths)] の順に展開し、次の操作を実行します。
- a) [Fibre Channel (Paths)] を右クリックし、[Deploy Fibre Channel] をクリックします。
  - b) [Path Type] コントロールで、[Port] をクリックします。
  - c) [Node] ドロップダウンリストで、リーフ スイッチを選択します。
  - d) [Path] ドロップダウンリストで、特定のアップリンク ポートにマッピングするサーバポートを選択します。
  - e) [VSAN] フィールドに、ポートのデフォルトの VSAN を入力します。
  - f) [VSAN Mode] コントロールで、[Native] をクリックします。
  - g) [Type] が fcoe であることを確認します。
  - h) [Pinning Label] ドロップダウンリストで、[Create Pinning Profile] を選択します。
  - i) [Name] フィールドに、トラフィック マップの名前を入力します。
  - j) [Path Type] コントロールで、[Port] をクリックして単一の NP アップリンク ポートに接続するか、[Direct Port Channel] をクリックして FC ポート チャンネルに接続します。

パスの種類で [Port] を選択した場合は、表示される [Node] ドロップダウンリストでリーフスイッチを選択する必要もあります。

パスの種類で [Direct Port Channel] を選択した場合は、インターフェイスポリシーグループで定義した FC PC を選択する必要もあります。

- k) [Path] ドロップダウンリストで、サーバポートをマッピングするアップリンクポートまたはポートチャネルを選択します。
- l) [Submit] をクリックして [Deploy Fibre Channel] ダイアログボックスに戻ります。
- m) [Submit] をクリックします。

**ステップ 3** [Fabric] > [Inventory] > [Pod <n>] > [Leaf <n>] > [Interfaces] > [FC Interfaces] 作業ウィンドウを選択し、アップリンクにマッピングするサーバインターフェイスポートを選択して再び有効にします。

## ファイバチャネル NPV NX-OS スタイル CLI の設定

### CLI を使用したファイバチャネル インターフェイスの設定

NPV 対応リーフスイッチでは、ユニバーサルポートをファイバチャネル (FC) ポートに変換することができます。FC ポートは F ポートまたは NP ポートのどちらかにすることができ、NP ポートではポートチャネルを形成できます。

#### 手順

**ステップ 1** ポートの範囲をイーサネットからファイバチャネルに変換します。

例：

```
apicl(config)# leaf 101
apicl(config-leaf)# slot 1
apicl(config-leaf-slot)# port 1 12 type fc
```

この例では、リーフ 101 のポート 1/1-12 をファイバチャネルポートに変換します。[no] 形式の **port type fc** コマンドで、ポートをファイバチャネルから再びイーサネットに変換します。

(注) ポートの変換はリーフスイッチのリブート後にのみ行われます。

現在のところ、FC ポートに変換できるポートの連続範囲は 1 つだけです。この範囲は 4 の倍数にする必要があり、4 の倍数のポート番号で終わる必要があります (例：1 ~ 4、1 ~ 8、21 ~ 24)。

**ステップ 2** すべてのファイバチャネル インターフェイスを設定します。

例：

```

apic1(config)# leaf 101
apic1(config-leaf)# interface fc 1/1
apic1(config-leaf-fc-if)# switchport mode [f | np]
apic1(config-leaf-fc-if)# switchport rxbbcredit <16-64>
apic1(config-leaf-fc-if)# switchport speed [16G | 32G | 4G | 8G | auto | unknown]
apic1(config-leaf-fc-if)# switchport trunk-mode [ auto | trunk-off | trunk-on | un-init]
apic1(config-leaf-fc-if)# switchport [trunk allowed] vsan <1-4093> tenant <name> \
                                application <name> epg <name>

```

(注) FC ホスト インターフェイス (F ポート) は、8Gbps の速度設定をサポートしていません。

FC インターフェイスは、アクセス モードまたはトランク モードで設定できます。FC ポートをアクセス モードに設定するには、次のコマンド形式を使用します。

例：

```
apic1(config-leaf-fc-if)# switchport vsan 2 tenant t1 application a1 epg e1
```

FC ポートをトランク モードに設定するには、次のコマンド形式を使用します。

例：

```
apic1(config-leaf-fc-if)# switchport trunk allowed vsan 4 tenant t1 application a1 epg e1
```

FC ポート チャネルを設定するには、FC ポート インターフェイス テンプレートを設定し、FC ポートチャネルのメンバーになる FC インターフェイスに適用します。

ポート チャネルには最大 16 個のメンバーを持たせることができます。

例：

```

apic1(config)# template fc-port-channel my-fc-pc
apic1(config-fc-po-ch-if)# lacp max-links 4
apic1(config-fc-po-ch-if)# lacp min-links 1
apic1(config-fc-po-ch-if)# vsan-domain member dom1
apic1(config-fc-po-ch-if)# exit
apic1(config)# leaf 101
apic1(config-leaf)# interface fc 1/1-2
apic1(config-leaf-fc-if)# fc-channel-group my-fc-pc
apic1(config-leaf-fc-if)# exit
apic1(config-leaf)# interface fc-port-channel my-fc-pc
apic1(config-leaf-fc-pc)# switchport mode [f | np]
apic1(config-leaf-fc-pc)# switchport rxbbcredit <16-64>
apic1(config-leaf-fc-pc)# switchport speed [16G | 32G | 4G | 8G | auto | unknown]
apic1(config-leaf-fc-pc)# switchport trunkmode [ auto | trunk-off | trunk-on | un-init]

```

## CLI を使用したファイバチャネル NPV ポリシーの設定

### 始める前に

NPV アプリケーションで使用するリーフスイッチポートをファイバチャネル (FC) ポートに変換した。

### 手順

**ステップ 1** ファイバチャネル F ポート ポリシー グループのテンプレートを作成します。

例 :

```
apicl(config)# template fc-policy-group my-fc-policy-group-f-ports
apicl(config-fc-pol-grp-if)# vsan-domain member dom1
apicl(config-fc-pol-grp-if)# switchport mode f
apicl(config-fc-pol-grp-if)# switchport trunk-mode trunk-off
```

速度など、他のスイッチポート設定を行うことができます。

**ステップ 2** ファイバチャネル NP ポート ポリシー グループのテンプレートを作成します。

例 :

```
apicl(config)# template fc-policy-group my-fc-policy-group-np-ports
apicl(config-fc-pol-grp-if)# vsan-domain member dom1
apicl(config-fc-pol-grp-if)# switchport mode np
apicl(config-fc-pol-grp-if)# switchport trunk-mode trunk-on
```

速度など、他のスイッチポート設定を行うことができます。

**ステップ 3** ファブリック全体のファイバチャネル ポリシーを作成します。

例 :

```
apicl(config)# template fc-fabric-policy my-fabric-fc-policy
apicl(config-fc-fabric-policy)# fctimer e-d-tov 1000
apicl(config-fc-fabric-policy)# fctimer r-a-tov 5000
apicl(config-fc-fabric-policy)# fcoe fcmmap 0E:FC:01
```

**ステップ 4** ファイバチャネル ポート チャネル ポリシーを作成します。

例 :

```
apicl(config)# template fc-port-channel my-fc-pc
apicl(config-fc-po-ch-if)# lACP max-links 4
apicl(config-fc-po-ch-if)# lACP min-links 1
apicl(config-fc-po-ch-if)# vsan-domain member dom1
```

**ステップ 5** リーフ全体のファイバチャネル ポリシー グループを作成します。

例：

```
apic1(config)# template fc-leaf-policy my-fc-leaf-policy
apic1(config-fc-leaf-policy)# npv auto-load-balance disruptive
apic1(config-fc-leaf-policy)# fcoe fka-adv-period 10
```

(注) ここに示すポリシー コマンドは単なる例であり、必須の設定ではありません。

**ステップ 6** リーフ ポリシー グループを作成します。

```
apic1(config)# template leaf-policy-group lpg1
apic1(config-leaf-policy-group)# inherit fc-fabric-policy my-fabric-fc-policy
apic1(config-leaf-policy-group)# inherit fc-leaf-policy my-fc-leaf-policy
```

FC 関連のポリシーを継承することによって、リーフ ポリシー グループが作成されます。

**ステップ 7** リーフ プロファイルを作成し、リーフポリシーグループをリーフグループに適用します。

例：

```
apic1(config)# leaf-profile my-leaf-profile
apic1(config-leaf-profile)# leaf-group my-leaf-group
apic1(config-leaf-group)# leaf 101
apic1(config-leaf-group)# leaf-policy-group lpg1
```

この例では、リーフ ポリシー グループ lpg1 にグループ化された、ファブリック全体の FC ポリシーとリーフ全体の FC ポリシーを、リーフ 101 に適用します。

**ステップ 8** リーフ インターフェイス プロファイルを作成し、fc ポリシーグループを一組の FC インターフェイスに適用します。

例：

```
apic1(config)# leaf-interface-profile my-leaf-interface-profile
apic1(config-leaf-if-profile)# leaf-interface-group my-leaf-interface-group
apic1(config-leaf-if-group)# fc-policy-group my-fc-policy-group-f-ports
apic1(config-leaf-if-group)# interface fc 1/1-10
```

## CLI を使用した NPV トラフィック マップの設定

この手順では、FC/FCoE サーバ（ホスト） インターフェイスから NP モードに設定された FC/FCoE 外部（アップリンク） インターフェイスに送信されるトラフィックをマッピングします。

始める前に

すべてのサーバ インターフェイスが F ポートである必要があり、すべてのアップリンク インターフェイスが NP ポートである必要があります。

## 手順

例 :

```

apicl(config)# leaf 101
apicl(config-leaf)# npv traffic-map server-interface \
  { vfc <slot/port> | vfc-po <po-name> | fc <slot/port> } \
  label <name> tenant <tn> app <ap> epg <ep>
apicl(config-leaf)# npv traffic-map external-interface \
  { vfc <slot/port> | vfc-po <po-name> | fc <slot/port> } \
  tenant <tn> label <name>

```

例 :

```

apicl(config)# leaf 101
apicl(config-leaf)# npv traffic-map server-interface vfc 1/1 label serv1 tenant t1 app
ap1 epg epg1
apicl(config-leaf)# npv traffic-map external-interface vfc-po my-fc-pc tenant t1 label
ext1

```

## ファイバチャネル NPV REST API の設定

### REST API を使用した FC 接続の設定

FC が有効なインターフェイスと Epg REST API を使用して、FC プロトコルを使用してこれらのインターフェイスへのアクセスを設定することができます。

## 手順

- ステップ 1** VSAN プールを作成するには、次の例などと XML post を送信します。この例では、VSAN プール myVsanPool1 を作成し、vsan-50 から vsan-60 までを含むように VSAN の範囲を指定します。

例 :

```

https://apic-ip-address/api/mo/uni/infra/vsanns-[myVsanPool1]-static.xml

<fvnsVsanInstP allocMode="static" name="myVsanPool1">
  <fvnsVsanEncapBlk from="vsan-50" name="encap" to="vsan-60"/>
</fvnsVsanInstP>

```

- ステップ 2** ファイバチャネル ドメインを作成するには、次の例のように XML で post を送信します。この例では、ファイバチャネル ドメイン (VSAN ドメイン) myFcDomain1 を作成し、VSAN プール myVsanPool1 に関連付けます。

例 :

```
https://apic-ip-address/api/mo/uni/fc-myFcDomain1.xml

<fcDomP name="myFcDomain1">
  <fcRsVsanNs tDn="uni/infra/vsanns-[myVsanPool1]-static"/>
</fcDomP>
```

**ステップ 3** FC ポートのアタッチ エンティティ ポリシー (AEP) を作成するには、次の例のように XML で POST を送信します。この例では、AEP myFcAEP1 を作成し、ファイバチャネルドメイン myFcDomain1 に関連付けます。

例：

```
https://apic-ip-address/api/mo/uni.xml

<polUni>
<infraInfra>
  <infraAttEntityP name="myFcAEP1">
    <infraRsDomP tDn="uni/fc-myFcDomain1"/>
  </infraAttEntityP>
</infraInfra>
</polUni>
```

**ステップ 4** サーバホストポートの FC インターフェイスポリシーとポリシーグループを作成するには、XML で POST を送信します。この例は次の要求を実行します。

- サーバホストポートの FC インターフェイスポリシー myFcHostIfPolicy1 を作成します。これらは、トランキングのない F ポートです。
- FC ホスト インターフェイスポリシー myFcHostIfPolicy1 を含む FC インターフェイスポリシーグループ myFcHostPortGroup1 を作成します。
- ポリシーグループを FC インターフェイスポリシーに関連付けて、これらのポートを FC ポートに変換します。
- ホストポートプロファイル myFcHostPortProfile を作成します。
- ポートを 5～8 の範囲で指定するポートセレクタ myFcHostSelector を作成します。
- リーフノード 104 を指定するノードセレクタ myFcNode1 を作成します。
- リーフノード 104 を指定するノードセレクタ myLeafSelector を作成します。
- ホストポートをリーフノードに関連付けます。

例：

```
https://apic-ip-address/api/mo/uni.xml

<polUni>
  <infraInfra>
    <fcIfPol name="myFcHostIfPolicy1" portMode="f" trunkMode="trunk-off" speed="auto"/>

    <infraFuncP>
      <infraFcAccPortGrp name="myFcHostPortGroup1">
        <infraRsFcL2IfPol tnFcIfPolName="myFcHostIfPolicy1" />
      </infraFcAccPortGrp>
    </infraFuncP>
    <infraAccPortP name="myFcHostPortProfile">
```



```

        <infraHPortS name="myFcHostSelector" type="range">
            <infraPortBlk name="myHostPorts" fromCard="1" toCard="1" fromPort="1"
toPort="8" />
            <infraRsAccBaseGrp tDn="uni/infra/funcprof/fcaccportgrp-myFcHostPortGroup1"
/>
        </infraHPortS>
    </infraAccPortP>
    <infraNodeP name="myFcNode1">
        <infraLeafS name="myLeafSelector" type="range">
            <infraNodeBlk name="myLeaf104" from_"="104" to_"="104" />
        </infraLeafS>
        <infraRsAccPortP tDn="uni/infra/accportprof-myHostPorts" />
    </infraNodeP>
</infraInfra>
</polUni>

```

(注) この設定を適用する場合は、ポートを FC ポートとしてアップするためにスイッチのリロードが必要になります。

現在のみ FC ポートに変換できるポートの 1 つの連続した範囲と、この範囲にする必要がありますが 4 の倍数で終わるポート番号 4 の倍数ことです。たとえば、1 ~ 4、1 ~ 8、21 ~ 24 などです。

**ステップ 5** アップリンク ポート チャネルの FC アップリンク ポート インターフェイス ポリシーとポリシーグループを作成するには、XML で POST を送信します。この例は次の要求を実行します。

- アップリンク ポートの FC インターフェイス ポリシー `myFcUplinkIfPolicy2` を作成します。これらは、ランキングが有効になっている NP ポートです。
- FC アップリンク インターフェイス ポリシー `myFcUplinkIfPolicy2` を含む FC インターフェイスバンドル ポリシーグループ `myFcUplinkBundleGroup2` を作成します。
- ポリシーグループを FC インターフェイス ポリシーに関連付けて、これらのポートを FC ポートに変換します。
- アップリンク ポート プロファイル `myFcUplinkPortProfile` を作成します。
- ポートを 1/9 ~ 12 の範囲で指定するポートセレクタ `myFcUplinkSelector` を作成します。
- ホスト ポートをリーフ ノード 104 に関連付けます。

例：

`https://apic-ip-address/api/mo/uni.xml`

```

<polUni>
    <infraInfra>
        <fcIfPol name="myFcUplinkIfPolicy2" portMode="np" trunkMode="trunk-on"
speed="auto"/>
        <infraFuncP>
            <infraFcAccBndlGrp name="myFcUplinkBundleGroup2">
                <infraRsFcL2IfPol tnFcIfPolName="myFcUplinkIfPolicy2" />
            </infraFcAccBndlGrp>
        </infraFuncP>
        <infraAccPortP name="myFcUplinkPortProfile">
            <infraHPortS name="myFcUplinkSelector" type="range">
                <infraPortBlk name="myUplinkPorts" fromCard="1" toCard="1" fromPort="9"
toPort="12" />
            </infraHPortS>
        </infraAccPortP>
    </infraInfra>
</polUni>

```

```

        <infraRsAccBaseGrp
tDn="uni/infra/funcprof/fcaccportgrp-myFcUplinkBundleGroup2" />
        </infraHPortS>
    </infraAccPortP>
    <infraNodeP name="myFcNode1">
        <infraLeafS name="myLeafSelector" type="range">
            <infraNodeBlk name="myLeaf104" from_"104" to_"104" />
        </infraLeafS>
        <infraRsAccPortP tDn="uni/infra/accportprof-myUplinkPorts" />
    </infraNodeP>
</infraInfra>
</polUni>

```

(注) この設定を適用する場合は、ポートを FC ポートとしてアップするためにスイッチのリロードが必要になります。

現在のみ FC ポートに変換できるポートの 1 つの連続した範囲と、この範囲にする必要がありますが 4 の倍数で終わるポート番号 4 の倍数ことです。たとえば、1～4、1～8、21～24 などです。

**ステップ 6** テナント、アプリケーションプロファイル、EPG を作成し、FCブリッジドメインを EPG に関連付けるするには、次の例などと XML post を送信します。例では、FC およびアプリケーション EPG `epg1` をサポートするように設定されたターゲットテナントの下に、ブリッジドメイン `myFcBD1` を作成します。これにより、ファイバチャネルドメイン `myFcDomain1` とファイバチャネルパスが、リーフスイッチ 104 のインターフェイス 1/7 に関連付けられます。各インターフェイスは、VSAN に関連付けられます。

例：

<https://apic-ip-address/api/mo/uni/tn-tenant1.xml>

```

<fvTenant name="tenant1">
  <fvCtx name="myFcVRF"/>
  <fvBD name="myFcBD1" type="fc">
    <fvRsCtx tnFvCtxName="myFcVRF"/>
  </fvBD>
  <fvAp name="appl">
    <fvAEPg name="epg1">
      <fvRsBd tnFvBDName="myFcBD1"/>
      <fvRsDomAtt tDn="uni/fc-myFcDomain1"/>
      <fvRsFcPathAtt tDn="topology/pod-1/paths-104/pathep-[fc1/1]" vsan="vsan-50"
vsanMode="native"/>
      <fvRsFcPathAtt tDn="topology/pod-1/paths-104/pathep-[fc1/2]" vsan="vsan-50"
vsanMode="native"/>
    </fvAEPg>
  </fvAp>
</fvTenant>

```

**ステップ 7** サーバポートをアップリンクポートに固定するトラフィックマップを作成するには、次の例のように XML で POST を送信します。この例では、サーバポート `vFC 1/47` をアップリンクポート `FC 1/7` に固定するトラフィックマップを作成します。

例：

<https://apic-ip-address/api/mo/uni/tn-tenant1.xml>

```

<fvTenant name="tenant1">
  <fvAp name="appl">

```

```
<fvAEPg name="epg1">
  <fvRsFcPathAtt tDn="topology/pod-1/paths-104/pathep-[eth1/47]" vsan="vsan-50"
vsanMode="native">
    <fcPinningLbl name="label1"/>
  </fvRsFcPathAtt>
</fvAEPg>
</fvAp>
</fvTenant>
```

[https://apic-ip-address/api/mo/uni/tn-vfc\\_t1.xml](https://apic-ip-address/api/mo/uni/tn-vfc_t1.xml)

```
<fvTenant name="tenant1">
  <fcPinningP name="label1">
    <fcRsPinToPath tDn="topology/pod-1/paths-104/pathep-[fc1/7]"/>
  </fcPinningP>
</fvTenant>
```

(注) トラフィック マップの固定を初めて設定する場合は、最初のトラフィック マップを設定する前にサーバ ホスト ポートをシャットダウンする必要があります。



## 翻訳について

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