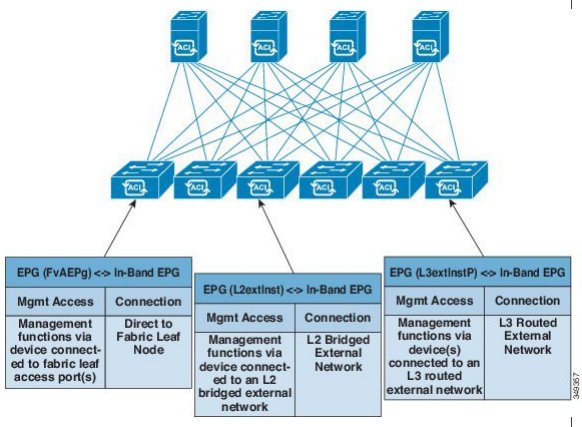
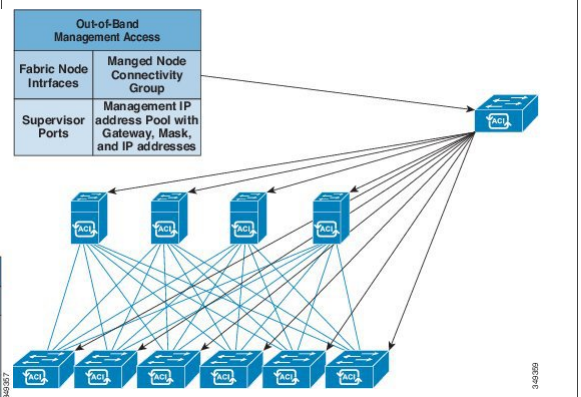
管理

この章の内容は、次のとおりです。

管理のワークフロー

ACI 管理アクセスのワークフロー

このワークフローでは、ACI ファブリック内のスイッチへの管理接続を設定するために必要な手順の概要を示します。

インバンド管理アクセス	アウトオブバンド管理アクセス
	

1. 前提条件

- インフラセキュリティ ドメインに読み取り/書き込みアクセス権限があることを確認します。
- 必要なインターフェイスを持つターゲット リーフ スイッチが使用できることを確認します。

2. ACI リーフ スイッチのアクセス ポートの設定

次の管理アクセス シナリオのいずれかを選択します。

- **インバンド**管理の場合は、『』のインバンド設定に推奨されるトピックに従います。
- **アウトオブバンド**管理の場合は、『』のアウトオブバンド設定に推奨されるトピックに従います。

推奨されるトピック

詳細については、『』の次のトピックを参照してください。

- 拡張 GUI を使用したインバンド管理アクセスの設定, （6 ページ）
- NX-OS スタイルの CLI を使用したインバンド管理アクセスの設定, （10 ページ）
- REST API を使用したインバンド管理アクセスの設定, （11 ページ）
- 拡張 GUI を使用したアウトオブバンド管理アクセスの設定, （15 ページ）
- NX-OS スタイルの CLI を使用したアウトオブバンド管理アクセスの設定, （16 ページ）
- REST API を使用したアウトオブバンド管理アクセスの設定, （17 ページ）

管理アクセスの追加

APIC コントローラには、管理ネットワークに到達するルートが 2 つあります。1 つはインバンド管理インターフェイスを使用し、もう 1 つはアウトオブバンド管理インターフェイスを使用します。

- インバンド管理アクセス：APIC および ACI ファブリックへのインバンド管理接続を設定できます。APIC がリーフ スイッチと通信するときに APIC によって使用される VLAN を最初に設定し、次に VMM サーバがリーフ スイッチとの通信に使用する VLAN を設定します。
- アウトオブバンド管理アクセス：APIC および ACI ファブリックへのアウトオブバンド管理接続を設定できます。アウトオブバンドエンドポイント グループ（EPG）に関連付けられるアウトオブバンド契約を設定し、外部ネットワーク プロファイルにその契約を接続します。

（注） APIC アウトオブバンド管理接続のリンクは、1 Gbps である必要があります。

APIC コントローラは、インバンド管理インターフェイスが設定されている場合は、アウトオブバンド管理インターフェイスを通してインバンド管理インターフェイスを常に選択します。アウトオブバンド管理インターフェイスは、インバンド管理インターフェイスが設定されていない場合、または宛先アドレスが APIC のアウトオブバンド管理サブネットと同じサブネットにある場合にのみ使用されます。この動作は、変更または再設定できません。

APIC 管理インターフェイスは IPv6 アドレスをサポートしないため、このインターフェイスを介して外部 IPv6 サーバに接続することはできません。

インバンドまたはアウトオブバンドの管理テナントで外部管理インスタンス プロファイルを設定しても、ファブリック全体の通信ポリシーで設定されているプロトコルには影響しません。外部管理インスタンスプロファイルで指定されているサブネットおよびコントラクトは、HTTP/HTTPS または SSH/Telnet には影響しません。

GUI での管理アクセスの追加

APIC コントローラには、管理ネットワークに到達するルートが 2 つあります。1 つはインバンド管理インターフェイスを使用し、もう 1 つはアウトオブバンド管理インターフェイスを使用します。

インバンド管理ネットワークは、ACI ファブリックを使用して APIC がリーフ スイッチや外部と通信することを可能にし、ファブリック自体を使用して外部管理デバイスが APIC またはリーフ スイッチおよびスパイン スイッチと通信することを可能にします。

アウトオブバンド管理ネットワークの設定は、コントローラ、リーフ スイッチ、およびスパイン スイッチの管理ポートの設定を定義します。

APIC コントローラは、インバンド管理インターフェイスが設定されている場合は、アウトオブバンド管理インターフェイスを通してインバンド管理インターフェイスを常に選択します。アウト

オブバンド管理インターフェイスは、インバンド管理インターフェイスが設定されていない場合、または宛先アドレスが APIC のアウトオブバンド管理サブネットと同じサブネットにある場合にのみ使用されます。この動作は、変更または再設定できません。APIC 管理インターフェイスは IPv6 アドレスをサポートしないため、このインターフェイスを介して外部 IPv6 サーバに接続することはできません。

APIC アウトオブバンド管理接続のリンクは、1 Gbps である必要があります。

IPv4/IPv6 アドレスおよびインバンド ポリシー

インバンド管理アドレスは、ポリシーによってのみ（Postman REST API、NX-OS スタイル CLI、または GUI）APIC コントローラにプロビジョニングできます。また、インバンド管理アドレスは、各ノードに静的に設定する必要があります。

アウトオブバンド ポリシーの IPv4/IPv6 アドレス

アウトオブバンド管理アドレスは、ブートストラップ時に、またはポリシーを使用して（Postman REST API、NX-OS スタイル CLI、GUI）APIC コントローラにプロビジョニングできます。また、アウトオブバンド管理アドレスは、各ノードに静的にまたはクラスタ全体にアドレスの範囲（IPv4/IPv6）を指定することによって設定する必要があります。IP アドレスは、範囲からクラスタ内のノードにランダムに割り当てられます。

既存の IP tables 機能をミラーリングする IPv6 の変更

すべての IPv6 は、ネットワーク アドレス変換（NAT）を除いて、既存の IP tables 機能をミラーリングします。

既存の IP tables

1. 以前は、IPv6 テーブルのすべてのルールが一度に 1 つずつ実行され、すべてのルールの追加または削除に対してシステム コールが行われていました。
2. 新しいポリシーが追加されるたびに、ルールが既存の IP tables ファイルに追加され、ファイルへの追加変更は行われませんでした。
3. 新しい送信元ポートがアウトオブバンドポリシーで設定されると、同じポート番号で送信元と宛先のルールを追加しました。

IP tables への変更

1. IP tables が作成されると、はじめにハッシュ マップに書き込まれ、次に中間ファイル IP tables-new に書き込まれてこれが復元されます。保存すると、新しい IP tables ファイルが /etc/sysconfig/ フォルダに作成されます。これら両方のファイルは同じ場所にあります。すべてのルールにシステム コールを行う代わりに、ファイルを復元および保存している時にのみシステム コールを行う必要があります。

2 ルールを追加する代わりに新しいポリシーがファイルに追加されると、hashmapsにデフォルトポリシーをロードし、新しいポリシーを確認し、hashmaps に追加することによって、IP テーブルがゼロから作成されます。その後、中間ファイル（/etc/sysconfig/iptables-new）に書き込まれて保存されます。

3 アウトオブバンド ポリシーのルールの送信元ポートだけを設定することはできません。宛先ポートまたは送信元ポートいずれかを宛先ポートとともにルールに追加できます。

4 新しいポリシーが追加されると、新しいルールが IP tables ファイルに追加されます。このルールは、IP tables デフォルト ルールのアクセス フローを変更します。

```
-A INPUT -s <OOB Address Ipv4/Ipv6> -j apic-default
```

5 新しいルールが追加された場合、これは IP tables-new ファイルに存在して IP tables ファイルには存在せず、IP tables-new ファイルにエラーがあることを意味します。復元が正常な場合に限り、ファイルが保存され、新しいルールを IP tables ファイルで確認できます。

（注）
- IPv4 のみ有効な場合、IPv6 ポリシーを設定しないでください。
- IPv6 のみ有効な場合、IPv4 ポリシーを設定しないでください。
- IPv4 と IPv6 の両方が有効な場合にポリシーが追加されると、両方のバージョンに設定されます。したがって、IPv4 サブネットを追加すると IP tables に追加され、同様に IPv6 サブネットは IPv6 tables に追加されます。

基本 GUI を使用したインバンド管理アクセスの設定

（注） インバンド管理アクセスでは、IPv4アドレスとIPv6アドレスがサポートされます。スタティック設定を使用した IPv6 設定がサポートされます（インバンドとアウトバンドの両方）。IPv4 および IPv6 のインバンドおよびアウトオブバンドのデュアル設定は、スタティック設定を使用する場合にのみサポートされます。詳細については、「*Configuring Static Management Access in Cisco APIC*」の KB 記事を参照してください。

手順

ステップ 1 APIC GUI の [Basic Mode] にログインし、メニュー バーで、[System] > [In Band & Out Of Band] の順にクリックします。

ステップ 2 [Navigation] ペインで、[InBand Management Configuration] を選択します。

ステップ 3 （任意） [Encap] フィールドで、必要に応じてインバンド管理に使用するデフォルト VLAN を変更するために新しい値を入力します。

ステップ 4 [Nodes] を展開し、次のアクションを実行します。

a) [Nodes] フィールドで、適切なノードを選択してインバンド アドレスを関連付けます。
b) [IP Address] フィールドに目的の IPv4 または IPv6 アドレスを入力します。
c) [Gateway] フィールドに目的の IPv4 または IPv6 ゲートウェイ アドレスを入力します。[Submit] をクリックします。

（注） デフォルト ゲートウェイの IP アドレスは、インバンド管理用の VRF の ACI ファブリックの拡散型ゲートウェイになります。

ステップ 5 [L2 Connectivity] タブをクリックし、[Ports] を展開して、次のアクションを実行します。

a) [Path] フィールドで、ドロップダウン リストから、管理用サーバまたは外部に接続されているポートを選択します。
b) [Encap] フィールドで、このポートで使用する VLAN を指定します。

ステップ 6 [Gateway IP Address for External Connectivity] を展開し、[IP address] フィールドに外部接続用の目的のゲートウェイ IPv4 および IPv6 アドレスが一覧表示されます。

ステップ 7 [ACL] を展開し、インバンド管理ネットワークに接続する目的のポートを追加します。[Submit] をクリックします。

インバンド管理アクセスが確立されました。

拡張 GUI を使用したインバンド管理アクセスの設定

（注） インバンド管理アクセスでは、IPv4 アドレスと IPv6 アドレスがサポートされます。スタティック設定を使用した IPv6 設定がサポートされます（インバンドとアウトバンドの両方）。IPv4 および IPv6 のインバンドおよびアウトオブバンドのデュアル設定は、スタティック設定を使用する場合にのみサポートされます。詳細については、「*Configuring Static Management Access in Cisco APIC*」の KB 記事を参照してください。

手順

ステップ 1 メニュー バーで、[FABRIC] > [Access Policies] を選択します。[Navigation] ペインで、[Interface Policies] を展開します。

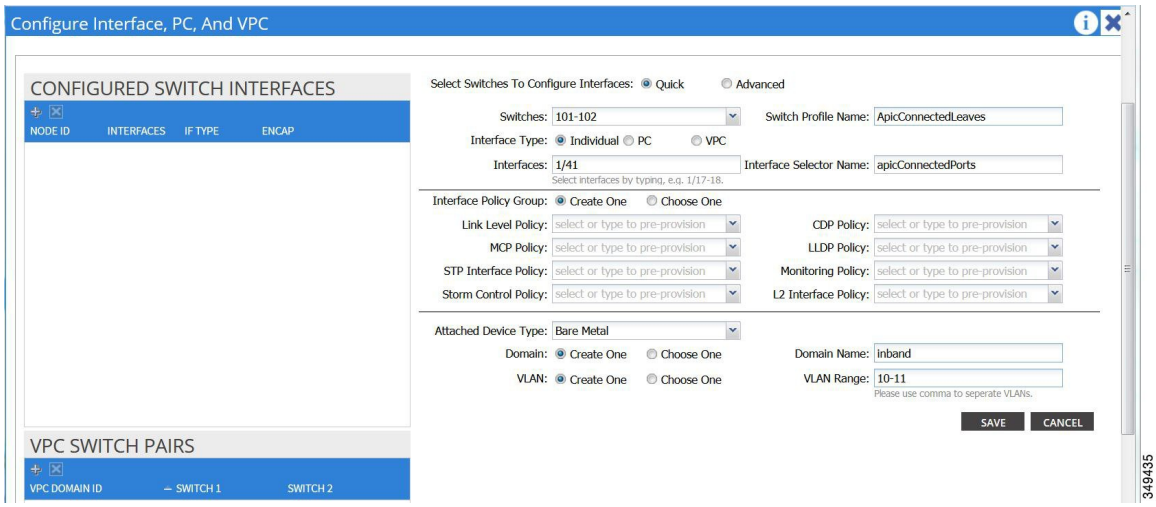
ステップ 2 [Navigation] ペインで、[Switch Policies] を右クリックし、[Configure Interface, PC and VPC] を選択します。

ステップ 3 [Configure Interface, PC, and VPC] ダイアログボックスで、APIC に接続されているスイッチ ポートを設定し、次の操作を実行します。

a) スイッチ図の横にある大きい [+] アイコンをクリックして、新しいプロファイルを作成して VLAN を APIC 用に設定します。
b) [Switches] フィールドのドロップダウン リストから、APIC が接続されているスイッチのチェックボックスをオンにします（leaf1 および leaf2）。

c) [Switch Profile Name] フィールドに、プロファイルの名前（apicConnectedLeaves）を入力します。

d) [+] アイコンをクリックして、ポートを設定します。
ユーザがコンテンツを入力できる、次の画像のようなダイアログボックスが表示されます。



e) [Interface Type] 領域で、[Individual] オプション ボタンが選択されていることを確認します。

f) [Interfaces] フィールドで、APIC が接続されているポートを入力します。

g) [Interface Selector Name] フィールドに、ポート プロファイルの名前（apicConnectedPorts）を入力します。

h) [Interface Policy Group] フィールドで、[Create One] オプション ボタンをクリックします。

i) [Attached Device Type] フィールドで、適切なデバイス タイプを選択してドメイン（ベア メタル）を設定します。

j) [Domain] フィールドで、[Create One] オプション ボタンをクリックします。

k) [Domain Name] フィールドに、ドメイン名を入力します（inband）。

l) [VLAN] フィールドで、[Create One] オプション ボタンを選択します。

m) [VLAN Range] フィールドに、VLAN 範囲を入力します。[Save] をクリックし、[Save] をもう一度クリックします。[Submit] をクリックします。

ステップ 4 [Navigation] ペインで、[Switch Policies] を右クリックし、[Configure Interface, PC and VPC] を選択します。

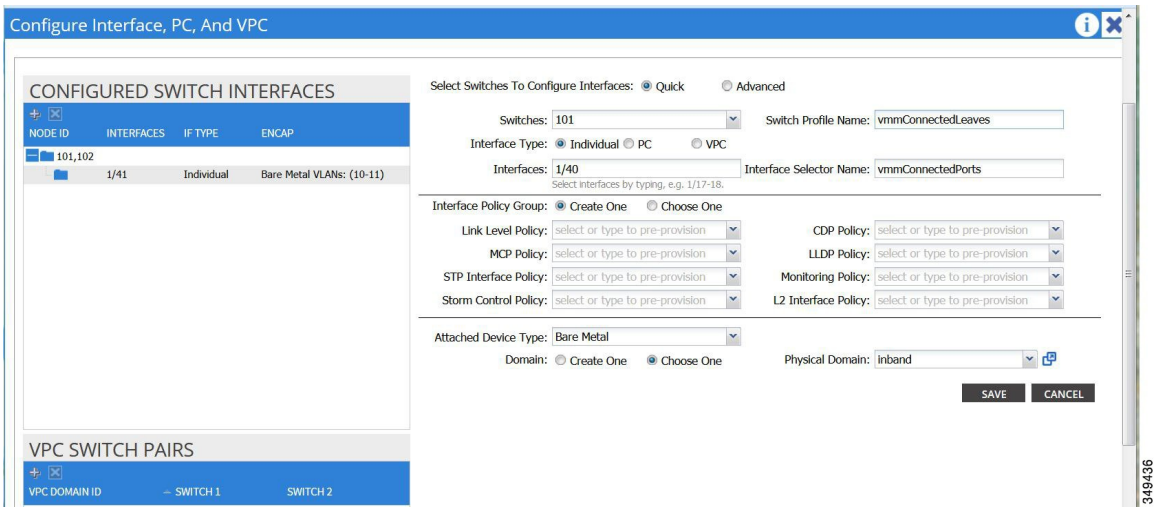
ステップ 5 [Configure Interface, PC, and VPC] ダイアログ ボックスで、次のアクションを実行します。

a) スイッチ図の横にある大きい [+] アイコンをクリックして、新しいプロファイルを作成して VLAN をサーバ用に設定します。

b) [Switches] フィールドのドロップダウン リストから、サーバが接続されているスイッチのチェックボックスをオンにします（leaf1）。

c) [Switch Profile Name] フィールドに、プロファイルの名前（vmmConnectedLeaves）を入力します。

d) [+] アイコンをクリックして、ポートを設定します。
ユーザがコンテンツを入力できる、次の画像のようなダイアログボックスが表示されます。



e) [Interface Type] 領域で、[Individual] オプション ボタンが選択されていることを確認します。
f) [Interfaces] フィールドで、サーバが接続されているポートを入力します（1/40）。
g) [Interface Selector Name] フィールドに、ポート プロファイルの名前を入力します。
h) [Interface Policy Group] フィールドで、[Create One] オプション ボタンをクリックします。
i) [Attached Device Type] フィールドで、適切なデバイス タイプを選択してドメイン（ベア メタル）を設定します。
j) [Domain] フィールドのドロップダウン リストから、[Choose One] オプション ボタンをクリックします。
k) [Physical Domain] ドロップダウン リストから、前に作成したドメインを選択します。
l) [Domain Name] フィールドに、ドメイン名を入力します。
m) [Save] をクリックし、[Save] をもう一度クリックします。

ステップ 6 [Configure Interface, PC, and VPC] ダイアログボックスで、[Submit] をクリックします。

ステップ 7 メニュー バーで、[TENANTS] > [mgmt] をクリックします。[Navigation] ペインで、[Tenant mgmt] > [Networking] > [Bridge Domains] を展開し、インバンド接続のブリッジ ドメインを設定します。

ステップ 8 インバンドブリッジ ドメイン（inb）を展開します。[Subnets] を右クリックします。[Create Subnets] をクリックし、次の操作を実行してインバンド ゲートウェイを設定します。

a) [Create Subnet] ダイアログボックスで、[Gateway IP] フィールドに、インバンド管理ゲートウェイ IP アドレスとマスクを入力します。
b) [Submit] をクリックします。

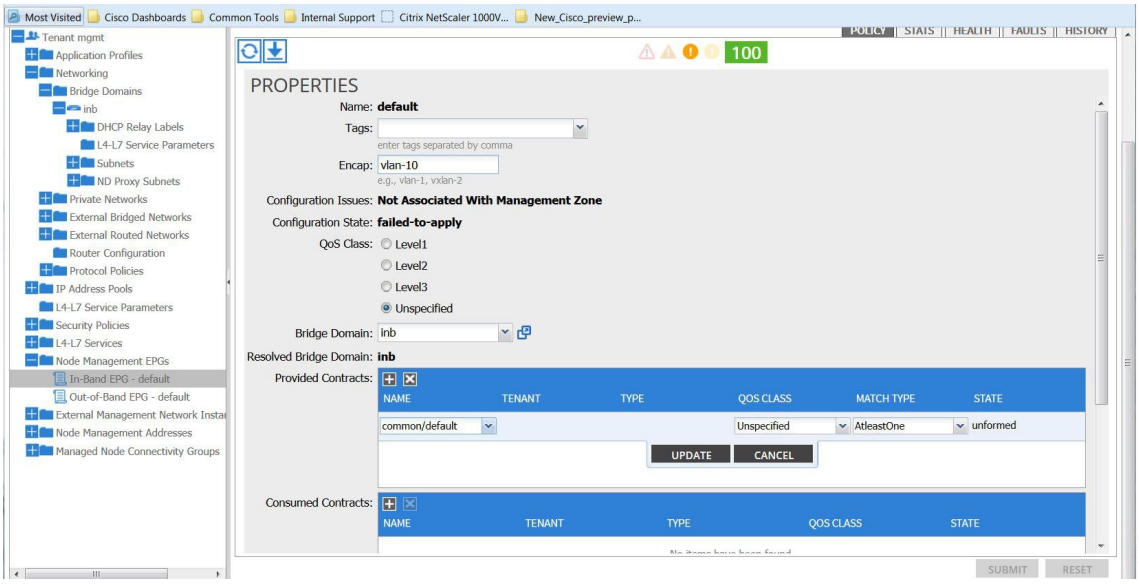
ステップ 9 [Navigation] ペインで、[Tenant mgmt] > [Node Management EPGs] の順に展開します。[Node Management EPGs] を右クリックし、[Create In-Band Management EPG] を選択します。APIC と通信するために使用するインバンド EPG の VLAN を設定するには、次の操作を実行します。

a) [Name] フィールドに、インバンド管理 EPG 名を入力します。
b) [Encap] フィールドで、VLAN（vlan-10）を入力します。
c) [Bridge Domain] ドロップダウン フィールドから、ブリッジ ドメインを選択します。[Submit] をクリックします。
d) [Navigation] ペインで、新しく作成したインバンド EPG を選択します。

e) [Provided Contracts] を展開します。[Name] フィールドで、ドロップダウン リストから、デフォルトのコントラクトを選択し、VMM サーバが存在する EPG で消費されるデフォルトのコントラクトを EPG が提供できるようにします。

f) [Update] をクリックし、[Submit] をクリックします。

次の画像のようなダイアログボックスが表示されます。



ステップ 10 [Navigation] ペインで、[Node Management Addresses] を右クリックし、[Create Node Management Addresses] をクリックし、次の操作を実行してファブリック内の APIC コントローラに割り当てる IP アドレスを設定します。

a) [Create Node Management Addresses] ダイアログボックスで、[Policy Name] フィールドに、ポリシー名（apicInb）を入力します。

b) [Nodes] フィールドの [Select] 列で、このファブリックの一部となるノードのチェックボックスをオンにします（apic1、apic2、apic3）。

c) [Config] フィールドで、[In-Band Addresses] チェックボックスをオンにします。

d) [Node Range] フィールドに、範囲を入力します。

e) [In-Band IP Addresses] 領域の [In-Band Management EPG] フィールドで、ドロップダウン リストから [default] を選択します。これで、デフォルトのインバンド管理 EPG が関連付けられます。

f) [In-Band IP Addresses] フィールドと [Gateway] フィールドに、必要に応じて IPv4 アドレスまたは IPv6 アドレスを入力します。

g) [Submit] をクリックします。これで、APIC の IP アドレスが設定されました。

ステップ 11 [Navigation] ペインで、[Node Management Addresses] を右クリックします。[Create Node Management Addresses] をクリックし、次の操作を実行して、ファブリック内のリーフ スイッチおよびスパイン スイッチの IP アドレスを設定します。

a) [Create Node Management Addresses] ダイアログボックスで、[Policy Name] フィールドに、ポリシー名（switchInb）を入力します。

b) [Nodes] フィールドの [Select] 列で、このファブリックの一部となるノードの横のチェックボックスをオンにします（leaf1、leaf2、spine1、spine2）。

c) [Config] フィールドで、[In-Band Addresses] チェックボックスをクリックします。
d) [Node Range] フィールドに、範囲を入力します。
e) [In-Band IP Addresses] 領域の [In-Band Management EPG] フィールドで、ドロップダウン リストから [default] を選択します。デフォルトのインバンド管理 EPG が関連付けられました。
f) [In-Band IP Addresses] フィールドと [Gateway] フィールドに、必要に応じて IPv4 アドレスまたは IPv6 アドレスを入力します。
g) [Submit] をクリックします。[Confirm] ダイアログボックスで、[Yes] をクリックします。リーフおよびスパイン スイッチの IP アドレスが設定されました。

ステップ 12 [Navigation] ペインの [Node Management Addresses] 下で、APIC ポリシー名（apicInb）をクリックして設定を確認します。[Work] ペインに、さまざまなノードに割り当てられた IP アドレスが表示されます。

ステップ 13 [Navigation] ペインの [Node Management Addresses] 下で、スイッチ ポリシー名（switchInb）をクリックします。[Work] ペインに、スイッチに割り当てられている IP アドレスと使用しているゲートウェイ アドレスが表示されます。

（注） アウトオブバンド管理アクセスを APIC サーバのデフォルト管理接続モードにするには、[Fabric] > [Fabric Policies] > [Global Policies] > [Connectivity Preferences] をクリックします。次に、[Connectivity Preferences] ページで [inband] をクリックします。

NX-OS スタイルの CLI を使用したインバンド管理アクセスの設定

手順

ステップ 1 APIC インバンド管理用の VLAN を次の例に示すように割り当てます。

例：

```
apic1(config)#
apic1(config)# vlan-domain inband-mgmt
apic1(config-vlan) vlan 10
apic1(config-vlan) exit
```

ステップ 2 インバンド管理ポートへの外部接続を次の例に示すように提供します。

例：

（注） このステップでは、コントローラはリーフ スイッチ上のポートに接続されます。そのポート上に VLAN ドメイン メンバーを追加する必要があります。この例では、リーフ 101 の ポート イーサネット 1/2 がコントローラ 1 に接続されます。VLAN ドメイン メンバーの「インバンド管理」を設定します。これは、接続の一部です。そのほかの部分として、管理ステーションはインターフェイス イーサネット 1/3 のリーフ 102 に接続されます。コントローラはリーフ スイッチ（この場合はリーフ 102）の 1 つのポートに接続された 1 つのマシンです。このマシンは外部（イーサネット 1/3）からコントローラに接続しようします。

```
apic1(config)#
apic1(config)# leaf 101
apic1(config-leaf) internet ethernet 1/2
apic1(config-leaf-if)# vlan-domain member inband-mgmt
apic1(config-leaf-if)# exit
apic1(config)# leaf 102
apic1(config-leaf) internet ethernet 1/3
apic1(config-leaf-if)# vlan-domain member inband-mgmt
apic1(config-leaf-if)# switchport trunk allowed vlan
apic1(config-leaf-if)# exit
```

（注） インバンド管理アクセスを APIC サーバのデフォルト管理接続モードにするには、次の CLI コマンド シーケンスを使用します。

```
apic1# configure
apic1(config)# mgmt_connectivity pref inband
```

REST API を使用したインバンド管理アクセスの設定

インバンド管理アクセスでは、IPv4 アドレスと IPv6 アドレスがサポートされます。スタティック設定を使用した IPv6 設定がサポートされます（インバンドとアウトバンドの両方）。IPv4 および IPv6 のインバンドおよびアウトオブバンドのデュアル設定は、スタティック設定を使用する場合にのみサポートされます。詳細については、「*Configuring Static Management Access in Cisco APIC*」の KB 記事を参照してください。

手順

ステップ 1 VLAN ネームスペースを作成します。

例：

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

<?xml version="1.0" encoding="UTF-8"?>
<!-- api/policymgr/mo/uni.xml -->
<polUni>
  <infraInfra>
    <!-- Static VLAN range -->
    <fvnsVlanInstP name="inband" allocMode="static">
      <fvnsEncapBlk name="encap" from="vlan-10" to="vlan-11"/>
    </fvnsVlanInstP>
  </infraInfra>
</polUni>
```

ステップ 2 物理ドメインを作成します。

例：

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

<?xml version="1.0" encoding="UTF-8"?>
<!-- api/policymgr/mo/uni.xml -->
<polUni>
  <physDomP name="inband">
    <infraRsVlanNs tDn="uni/infra/vlanns-inband-static"/>
  </physDomP>
</polUni>
```

ステップ 3 インバンド管理用のセレクタを作成します。

例：

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

<?xml version="1.0" encoding="UTF-8"?>
<!-- api/policymgr/mo/.xml -->
<polUni>
  <infraInfra>
    <infraNodeP name="vmmNodes">
      <infraLeafS name="leafS" type="range">
        <infraNodeBlk name="single0" from_="101" to_="101"/>
      </infraLeafS>
      <infraRsAccPortP tDn="uni/infra/accportprof-vmmPorts"/>
    </infraNodeP>

    <!-- Assumption is that VMM host is reachable via eth1/40. -->
    <infraAccPortP name="vmmPorts">
      <infraHPortS name="portS" type="range">
        <infraPortBlk name="block1"
                      fromCard="1" toCard="1"
                      fromPort="40" toPort="40"/>
        <infraRsAccBaseGrp tDn="uni/infra/funcprof/accportgrp-inband" />
      </infraHPortS>
    </infraAccPortP>


    <infraNodeP name="apicConnectedNodes">
      <infraLeafS name="leafS" type="range">
        <infraNodeBlk name="single0" from_="101" to_="102"/>
      </infraLeafS>
      <infraRsAccPortP tDn="uni/infra/accportprof-apicConnectedPorts"/>
    </infraNodeP>

    <!-- Assumption is that APIC is connected to eth1/1. -->
    <infraAccPortP name="apicConnectedPorts">
      <infraHPortS name="portS" type="range">
        <infraPortBlk name="block1"
                      fromCard="1" toCard="1"
                      fromPort="1" toPort="3"/>
        <infraRsAccBaseGrp tDn="uni/infra/funcprof/accportgrp-inband" />
      </infraHPortS>
    </infraAccPortP>

    <infraFuncP>
      <infraAccPortGrp name="inband">
        <infraRsAttEntP tDn="uni/infra/attentp-inband"/>
      </infraAccPortGrp>
    </infraFuncP>

    <infraAttEntityP name="inband">
      <infraRsDomP tDn="uni/phys-inband"/>
    </infraAttEntityP>
```

```
  </infraInfra>
</polUni>
```

ステップ 4 インバンド ブリッジ ドメインとエンドポイント グループ（EPG）を設定します。

例：

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

<?xml version="1.0" encoding="UTF-8"?>
<!-- api/policymgr/mo/.xml -->
<polUni>
  <fvTenant name="mgmt">
    <!-- Configure the in-band management gateway address on the
         in-band BD. -->
    <fvBD name="inb">
      <fvSubnet ip="10.13.1.254/24"/>
    </fvBD>

    <mgmtMgmtP name="default">
      <!-- Configure the encap on which APICs will communicate on the
           in-band network. -->
      <mgmtInB name="default" encap="vlan-10">
        <fvRsProv tnVzBrCPName="default"/>
      </mgmtInB>
    </mgmtMgmtP>
  </fvTenant>
</polUni>
```

ステップ 5 アドレス プールを作成します。

例：

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

<?xml version="1.0" encoding="UTF-8"?>
<!-- api/policymgr/mo/.xml -->
<polUni>
  <fvTenant name="mgmt">
    <!-- Adresses for APIC in-band management network -->
    <fvnsAddrInst name="apicInb" addr="10.13.1.254/24">
      <fvnsUcastAddrBlk from="10.13.1.1" to="10.13.1.10"/>
    </fvnsAddrInst>

    <!-- Adresses for switch in-band management network -->
    <fvnsAddrInst name="switchInb" addr="10.13.1.254/24">
      <fvnsUcastAddrBlk from="10.13.1.101" to="10.13.1.120"/>
    </fvnsAddrInst>
  </fvTenant>
</polUni>
```

（注） IPv6 のダイナミック アドレス プールはサポートされていません。

ステップ 6 管理グループを作成します。

例：

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

<?xml version="1.0" encoding="UTF-8"?>
<!-- api/policymgr/mo/.xml -->
<polUni>
  <infraInfra>
    <!-- Management node group for APICs -->
    <mgmtNodeGrp name="apic">
      <infraNodeBlk name="all" from_="1" to_="3"/>
      <mgmtRsGrp tDn="uni/infra/funcprof/grp-apic"/>
    </mgmtNodeGrp>
```

```
    <!-- Management node group for switches-->
    <mgmtNodeGrp name="switch">
      <infraNodeBlk name="all" from_="101" to_="104"/>
      <mgmtRsGrp tDn="uni/infra/funcprof/grp-switch"/>
    </mgmtNodeGrp>

    <!-- Functional profile -->
    <infraFuncP>
      <!-- Management group for APICs -->
      <mgmtGrp name="apic">
        <!-- In-band management zone -->
        <mgmtInBZone name="default">
          <mgmtRsInbEpg tDn="uni/tn-mgmt/mgmtp-default/inb-default"/>
          <mgmtRsAddrInst tDn="uni/tn-mgmt/addrinst-apicInb"/>
        </mgmtInBZone>
      </mgmtGrp>

      <!-- Management group for switches -->
      <mgmtGrp name="switch">
        <!-- In-band management zone -->
        <mgmtInBZone name="default">
          <mgmtRsInbEpg tDn="uni/tn-mgmt/mgmtp-default/inb-default"/>
          <mgmtRsAddrInst tDn="uni/tn-mgmt/addrinst-switchInb"/>
        </mgmtInBZone>
      </mgmtGrp>
    </infraFuncP>
  </infraInfra>
</polUni>
```

（注） IPv6 のダイナミック アドレス プールはサポートされていません。

基本 GUI を使用したアウトオブバンド管理アクセスの設定

（注） アウトオブバンド管理アクセスでは、IPv4 アドレスと IPv6 アドレスがサポートされます。

手順

ステップ 1 APIC GUI の [Basic Mode] にログインし、メニューバーで、[System] > [In Band & Out Of Band] の順に選択します。

ステップ 2 [Navigation] ペインで、[Out-of-Band EPG - default] をクリックします。

ステップ 3 [Work] ペインで、[Properties] の下の [Nodes] を展開し、適切なノードを IPv4 または IPv6 アドレスおよびデフォルト ゲートウェイと関連付けます。[Update] をクリックします。

ステップ 4 [Access Restrictions] を展開し、ACI ファブリック ノードのアウトオブバンド管理アドレスと通信する目的の外部サブネットのリストを追加します。

ステップ 5 外部サブネットの [ACL] を展開し、ACI ファブリック ノードの管理を許可する L4 ポートの適切な情報を入力します。
アウトオブバンド管理アクセスが設定されました。

拡張 GUI を使用したアウトオブバンド管理アクセスの設定

（注） アウトオブバンド管理アクセスでは、IPv4 アドレスと IPv6 アドレスがサポートされます。

はじめる前に

APIC アウトオブバンド管理接続のリンクは、1 Gbps である必要があります。

手順

ステップ 1 メニュー バーで、[TENANTS] > [mgmt] を選択します。[Navigation] ペインで、[Tenant mgmt] を展開します。

ステップ 2 [Node Management Addresses] を右クリックし、[Create Node Management Addresses] をクリックします。

ステップ 3 [Create Node Management Addresses] ダイアログボックスで、次の操作を実行します。

a) [Policy Name] フィールドに、ポリシー名（switchOob）を入力します。

b) [Nodes] フィールドで、適切なリーフおよびスパイン スイッチ（leaf1、leaf2、spine1）の横にあるチェックボックスをオンにします。

c) [Config] フィールドで、[Out of-Band Addresses] のチェックボックスをオンにします。

（注） [Out-of-Band IP addresses] 領域が表示されます。

d) [Out-of-Band Management EPG] フィールドで、ドロップダウン リストから EPG を選択します（デフォルト）。

e) [Out-of-Band IP Addresses] フィールドおよび [Out-of-Band Gateway] フィールドに、スイッチに割り当てられる希望する IPv4 アドレスまたは IPv6 アドレスを入力します。[OK] をクリックします。

ノード管理 IP アドレスが設定されます。APIC だけではなくリーフ スイッチおよびスパイン スイッチにもアウトオブバンド管理アクセスのアドレスを設定する必要があります。

ステップ 4 [Navigation] ペインで、[Node Management Addresses] を展開し、作成したポリシーをクリックします。

[Work] ペインに、スイッチに対するアウトオブバンド管理アドレスが表示されます。

ステップ 5 [Navigation] ペインで、[Security Policies] > [Out-of-Band Contracts] を展開します。

ステップ 6 [Out-of-Band Contracts] を右クリックし、[Create Out-of-Band Contract] をクリックします。

ステップ 7 [Create Out-of-Band Contract] ダイアログボックスで、次のタスクを実行します。

a) [Name] フィールドに、コントラクトの名前（oob-default）を入力します。

b) [Subjects] を展開します。[Create Contract Subject] ダイアログボックスで、[Name] フィールドに、サブジェクト名（oob-default）を入力します。

c) [Filters]を展開し、[Name]フィールドで、ドロップダウンリストから、フィルタの名前（default）を選択します。[Update] をクリックし、[OK] をクリックします。

d) [Create Out-of-Band Contract] ダイアログボックスで、[Submit] をクリックします。

アウトオブバンド EPG に適用できるアウトオブバンド コントラクトが作成されます。

ステップ 8 [Navigation] ペインで、[Node Management EPGs] > [Out-of-Band EPG - default] を展開します。

ステップ 9 [Work] ペインで、[Provided Out-of-Band Contracts] を展開します。

ステップ 10 [OOB Contract] カラムで、ドロップダウン リストから、作成したアウトオブバンド コントラクト（oob-default）を選択します。[Update] をクリックし、[Submit] をクリックします。
コントラクトがノード管理 EPG に関連付けられます。

ステップ 11 [Navigation] ペインで、[External Network Instance Profile] を右クリックし、[Create External Management Entity Instance] をクリックします。

ステップ 12 [Create External Management Entity Instance] ダイアログボックスで、次の操作を実行します。

a) [Name] フィールドに、名前（oob-mgmt-ext）を入力します。

b) [Consumed Out-of-Band Contracts] フィールドを展開します。[Out-of-Band Contract] ドロップダウン リストから、作成したコントラクト（oob-default）を選択します。[Update] をクリックします。
アウトオブバンド管理によって提供された同じコントラクトを選択します。

c) [Subnets] フィールドに、サブネット アドレスを入力します。[Submit] をクリックします。
ここで選択したサブネットアドレスだけがスイッチの管理に使用されます。含まれていないサブネット アドレスはスイッチの管理に使用できません。

ノード管理 EPG は、外部ネットワーク インスタンス プロファイルに接続されます。アウトオブバンド管理接続が設定されます。

（注） アウトオブバンド管理アクセスを APIC サーバのデフォルト管理接続モードにするには、[Fabric] > [Fabric Policies] > [Global Policies] > [Connectivity Preferences] をクリックします。次に、[Connectivity Preferences] ページで [ooband] をクリックします。

NX-OS スタイルの CLI を使用したアウトオブバンド管理アクセスの設定

はじめる前に

APIC アウトオブバンド管理接続のリンクは、1 Gbps である必要があります。

手順

外部管理サブネットに対するアウトオブバンド管理インターフェイスのアクセス制御を次のように提供します。

例：

```
apic1(config-tenant)# external-l3 epg default oob-mgmt
apic1(config-tenant-l3ext-epg)#match ip 10.0.0.0/8
apic1(config-tenant-l3ext-epg)# exit
apic1(config)# exit
```

（注） アウトオブバンド管理アクセスを APIC サーバのデフォルト管理接続モードにするには、次の CLI コマンド シーケンスを使用します。

```
apic1 # configure
apic1(config)# mgmt_connectivity pref ooband
```

REST API を使用したアウトオブバンド管理アクセスの設定

アウトオブバンド管理アクセスでは、IPv4 アドレスと IPv6 アドレスがサポートされます。

はじめる前に

APIC アウトオブバンド管理接続のリンクは、1 Gbps である必要があります。

手順

ステップ 1 アウトオブバンド コントラクトを作成します。

例：

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

<polUni>
    <fvTenant name="mgmt">
        <!-- Contract -->
        <vzOOBBrCP name="oob-default">
            <vzSubj name="oob-default">
                <vzRsSubjFiltAtt tnVzFilterName="default" />
            </vzSubj>
        </vzOOBBrCP>
    </fvTenant>
</polUni>
```

ステップ 2 アウトオブバンド コントラクトをアウトオブバンド EPG に関連付けます。

例：

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

<polUni>
    <fvTenant name="mgmt">
        <mgmtMgmtP name="default">
            <mgmtOoB name="default">
                <mgmtRsOoBProv tnVzOOBBrCPName="oob-default" />
            </mgmtOoB>
        </mgmtMgmtP>
    </fvTenant>
</polUni>
```

ステップ 3 アウトオブバンド コントラクトを外部管理 EPG に関連付けます。

例：

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

<polUni>
    <fvTenant name="mgmt">
        <mgmtExtMgmtEntity name="default">
            <mgmtInstP name="oob-mgmt-ext">
                <mgmtRsOoBCons tnVzOOBBrCPName="oob-default" />
```

```
                <!-- SUBNET from where switches are managed -->
                <mgmtSubnet ip="10.0.0.0/8" />
            </mgmtInstP>
        </mgmtExtMgmtEntity>
    </fvTenant>
</polUni>
```

ステップ 4 管理アドレス プールを作成します。

例：

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

<polUni>
    <fvTenant name="mgmt">
        <fvnsAddrInst name="switchOoboobaddr" addr="172.23.48.1/21">
            <fvnsUcastAddrBlk from="172.23.49.240" to="172.23.49.244"/>
        </fvnsAddrInst>
    </fvTenant>
</polUni>
```

ステップ 5 ノード管理グループを作成します。

例：

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

<polUni>
    <infraInfra>
        <infraFuncP>
            <mgmtGrp name="switchOob">
                <mgmtOoBZone name="default">
                    <mgmtRsAddrInst tDn="uni/tn-mgmt/addrinst-switchOoboobaddr" />
                    <mgmtRsOobEpg tDn="uni/tn-mgmt/mgmtp-default/oob-default" />
                </mgmtOoBZone>
            </mgmtGrp>
        </infraFuncP>
        <mgmtNodeGrp name="switchOob">
            <mgmtRsGrp tDn="uni/infra/funcprof/grp-switchOob" />
            <infraNodeBlk name="default" from_="101" to_="103" />
        </mgmtNodeGrp>
    </infraInfra>
</polUni>
```

（注） デフォルトの接続モードとしてアウトオブバンド管理接続を使用するように APIC サーバを設定できます。

```
POST https://apic-ip-address/api/node/mo/.xml
<polUni>
<fabricInst>
    <mgmtConnectivityPrefs interfacePref="ooband"/>
</fabricInst>
</polUni>
```

テクニカルサポート、統計情報、およびコアファイルのエクスポート

ファイルのエクスポートについて

管理者は、APIC 内で、コア ファイルとデバッグ データを処理するために、統計情報、テクニカル サポートの収集、障害およびイベントをファブリック（APIC およびスイッチ）から外部ホストにエクスポートするようエクスポート ポリシーを設定できます。エクスポートはXML、JSON、Web ソケット、Secure Copy Protocol（SCP）、HTTP などのさまざまな形式にできます。ストリーミング、定期的、またはオンデマンドの各形式でエクスポートを登録できます。

管理者は、転送プロトコル、圧縮アルゴリズム、転送の頻度などポリシーの詳細を設定できます。ポリシーは、AAA を使用して認証されたユーザによって設定できます。実際の転送のセキュリティ メカニズムは、ユーザ名とパスワードに基づいています。内部的に、ポリシー要素はデータのトリガーを処理します。

ファイルのエクスポートに関するガイドラインと制約事項

- HTTPエクスポートとストリーミングAPI形式は、統計情報の場合にのみサポートされます。コア情報と **テクニカル サポート** データはサポートされません。
- エクスポートされるファイルの宛先 IP は、IPv6 アドレスであってはなりません。

（注） 特に、APIC、または帯域幅と計算用リソースが不足している外部サーバにエクスポートする場合は、5 つを超えるノードから同時に**テクニカル サポート**をトリガーしないでください。

ファブリック内のすべてのノードから定期的に**テクニカル サポート**を収集するには、複数のポリシーを作成する必要があります。各ポリシーは、ノードのサブセットをカバーする必要があり、時間をずらしてトリガーされるようにスケジュールします（少なくとも 30 分離す）。

ファイル エクスポート用のリモート ロケーションの作成

この手順では、エクスポートされたファイルを受け取るリモート ホストのホスト情報とファイル転送セッティングを設定します。

手順

ステップ 1 メニュー バーで、[Admin] をクリックします。
ステップ 2 サブメニュー バーで、[Import/Export] をクリックします。
ステップ 3 [Navigation] ペインで、[Export Policies] を展開します。
ステップ 4 [Remote Locations] を右クリックし、[Create Remote Path of a File] を選択します。
ステップ 5 [Create Remote Path of a File] ダイアログボックスで、次の操作を実行します。
a) [Name] フィールドに、リモート ロケーションの名前を入力します。
b) [Host Name/IP] フィールドに、送信先ホストの IP アドレスまたは完全修飾ドメイン名を入力します。
c) [Protocol] フィールドで、必要なファイル転送プロトコルのオプション ボタンをクリックします。
d) [Remote Path] フィールドで、リモート ホストでファイルが保存されるパスを入力します。
e) リモート ホストにログインするためのユーザ名とパスワードを入力し、パスワードを確認します。
f) [Management EPG] ドロップダウン リストから管理 EPG を選択します。
g) [Submit] をクリックします。

GUI を使用したオンデマンドの techsupport ファイルの送信

手順

ステップ 1 メニュー バーで、[Admin] をクリックします。
ステップ 2 サブメニュー バーで、[Import/Export] をクリックします。
ステップ 3 [Navigation] ペインで、[Export Policies] を展開します。
ステップ 4 [On-demand TechSupport] を右クリックし、[Create On-demand TechSupport] を選択します。
[Create On-demand TechSupport] ダイアログボックスが表示されます。
ステップ 5 [Create On-demand TechSupport] ダイアログボックスのフィールドに適切な値を入力します。
（注） フィールドの説明については、[Create On-demand TechSupport] ダイアログボックスの情報アイコン（i）をクリックします。ヘルプ ファイルが開いてプロパティの説明ページが表示されます。
ステップ 6 [Submit] をクリックして、テクニカルサポート ファイルを送信します。
（注） オンデマンドのテクニカルサポート ファイルは別の APIC に保存し、ストレージと CPU 条件のバランスを取ることができます。場所を確認するには、[Navigation] ペインでオンデマンドのテクニカルサポート ポリシーをクリックし、[Work] ペインで [OPERATIONAL] タブをクリックします。コントローラが [EXPORT LOCATION] フィールドに表示されます。

ステップ 7 ポリシー名を右クリックし、[Collect Tech Support] を選択します。

ステップ 8 [Yes] を選択して、テクニカル サポート情報の収集を開始します。

NX-OS スタイルの CLI を使用したオンデマンドの techsupport ファイルの送信

（注） APIC にエクスポートする場合や、帯域幅と計算のリソースが不足している外部サーバにエクスポートする場合は特に、同時に 5 つを超えるノードから techsupport ファイルの回収をトリガーしないでください。

APIC の過剰なストレージの使用を避けるには、ローカルに保存された techsupport ファイルをすぐに削除してください。

はじめる前に

techsupport ファイルをエクスポートするリモート パスを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**triggertechsupport** {**all** | **controllersswitch***node-id*} [**remotename***remote-path-name*] 例： `apic1# trigger techsupport switch 101,103 remotename remote5`	コントローラ、スイッチ、またはすべてからリモートパスへの techsupport ファイルのエクスポートをトリガーします。スイッチの場合、範囲またはカンマ区切りのリストを指定できます。リモートホストを指定しない場合、ファイルはコントローラ自体に収集されます。
ステップ 2	**triggertechsupporthost***host-id* 例： `apic1# trigger techsupport host`	指定されたホストからリモートパスへの techsupport ファイルのエクスポートをトリガーします。リモート ホストを指定しない場合、ファイルはコントローラ自体に収集されます。
ステップ 3	**triggertechsupportlocal** 例： `apic1# trigger techsupport local`	リモート ホストへのローカル techsupport ファイルのエクスポートをトリガーします。リモートホストを指定しない場合、ファイルはコントローラ自体に収集されます。

	コマンドまたはアクション	目的
ステップ 4	**showtechsupport** {**all** | **controllersswitch***node-id*} **status** 例： `apic1# show techsupport switch 101 status`	techsupport ファイルがトリガーされると、このコマンドによって techsupport レポートのステータスが表示されます。

例

次に、apic1 コントローラのローカルに保存されるようにスイッチ 101 の techsupport ファイルをトリガーする例を示します。

```
apic1# trigger techsupport switch 101

Triggering techsupport for Switch 101 using policy supNode101, setting filters to default
value

Triggered on demand tech support successfully for Switch 101, will be available at:
/data/techsupport on
the controller. Use 'show techsupport' with your options to check techsupport status.
```

REST API を使用したオンデマンドの techsupport ファイルの送信

手順

ステップ 1 REST API を使用して次の例のような XML を POST 送信し、テクニカル サポート ファイルのリモート宛先を設定します。

例：

```
<fileRemotePath userName="" remotePort="22" remotePath="" protocol="sftp" name="ToSupport"
 host="192.168.200.2"
dn="uni/fabric/path-ToSupport" descr="">

<fileRsARemoteHostToEpg tDn="uni/tn-mgmt/mgmtp-default/oob-default"/>

</fileRemotePath>
```

ステップ 2 REST API を使用して次のような XML を POST 送信し、オンデマンドのテクニカル サポート ファイルを生成します。

例：

```
<dbgexpTechSupOnD upgradeLogs="no" startTime="unspecified" name="Tech_Support_9-20-16"
exportToController="no"
endTime="unspecified" dn="uni/fabric/tsod-Tech_Support_9-20-16" descr="" compression="gzip"

category="forwarding" adminSt="untriggered">

<dbgexpRsExportDest tDn="uni/fabric/path-ToSupport"/>
```

```
<dbgexpRsTsSrc tDn="topology/pod-1/node-102/sys"/>
<dbgexpRsTsSrc tDn="topology/pod-1/node-103/sys"/>
<dbgexpRsTsSrc tDn="topology/pod-1/node-101/sys"/>
<dbgexpRsData tDn="uni/fabric/tscont"/>
</dbgexpTechSupOnD>
```

概要

このトピックでは、次の情報を提供します。

- Cisco APIC の設定のインポートとエクスポートを使用して、設定の状態を最新の既知の良好な状態に回復する方法
- Cisco APIC の設定ファイルのセキュア プロパティを暗号化する方法

ユーザ設定のスケジュールバックアップとオンデマンドバックアップの両方を行うことができます。設定の状態を回復すると（「ロールバック」とも呼ばれます）、以前良好であった既知の状態に戻ることができます。そのためのオプションは、アトミック置換と呼ばれます。設定インポートポリシー（configImportP）は、アトミック＋置換（importMode=atomic、importType=replace）をサポートします。これらの値に設定すると、インポートされる設定が既存の設定を上書きし、インポートされるファイルに存在しない既存の設定があれば削除されます。 定期的な設定のバックアップとエクスポートを行うか、または既知の良好な設定のエクスポートを明示的にトリガーする限り、後で以下の CLI、REST API、および GUI 用の手順を使用してこの設定を復元することができます。

Cisco APIC を使用した設定状態の回復に関する詳細な概念情報については、『*Cisco Application Centric Infrastructure Fundamentals Guide*』を参照してください。

次の項では、設定ファイルのセキュア プロパティの暗号化に関する概念情報を提供します。

設定ファイルの暗号化

リリース 1.1(2) 以降、AES-256 暗号化を有効にすることにより APIC 設定ファイルを暗号化できます。AES 暗号化はグローバル設定オプションです。すべてのセキュア プロパティは AES 構成設定に従っています。テナント設定などの ACI ファブリック設定のサブセットを AES 暗号化を使用してエクスポートするが、ファブリック設定の残りの部分は暗号化しないということはできません。セキュア プロパティのリストについては、『Cisco Application Centric Infrastructure Fundamentals』の「Appendix K: Secure Properties」を参照してください。

APIC は、16 ～ 32 文字のパスフレーズを使用して AES-256 キーを生成します。APIC GUI では、AES パスフレーズのハッシュを表示します。このハッシュを使用して、2 つの ACI ファブリックで同じパスフレーズが使用されているかどうかを確認できます。このハッシュをクライアント コンピュータにコピーして、別の ACI ファブリックのパスフレーズ ハッシュと比較できます。これ

により、それらのハッシュが同じパスフレーズを使用して生成されたかどうかを確認できます。ハッシュを使用して、元のパスフレーズまたは AES-256 キーを再構築することはできません。

暗号化された設定ファイルを使用する際は、次のガイドラインに従ってください。

- AES 暗号化設定オプションを使用しているファブリックに古い ACI 設定をインポートするための後方互換性がサポートされています。

（注） 逆の互換性はサポートされていません。AES 暗号化が有効になっている ACI ファブリックからエクスポートされた設定を古いバージョンの APIC ソフトウェアにインポートすることはできません。

- ファブリック バックアップ設定のエクスポートを実行するときは、必ず AES 暗号化を有効にします。これにより、ファブリックを復元するときに、設定のすべてのセキュア プロパティが正常にインポートされるようになります。

（注） AES 暗号化を有効にせずにファブリック バックアップ設定がエクスポートされると、どのセキュア プロパティもエクスポートに含まれません。そのような暗号化されていないバックアップにはセキュア プロパティは何も含まれていないため、そのようなファイルをインポートしてシステムを復元すると、ファブリックの管理者およびすべてのユーザがシステムからロックアウトされてしまう可能性があります。

- 暗号化キーを生成する AES パスフレーズは、ACI 管理者やその他のユーザが復元したり読み取ったりすることはできません。AES パスフレーズは保存されません。APIC は、AES パスフレーズを使用して AES キーを生成した後でそのパスフレーズを廃棄します。AES キーはエクスポートされません。AES キーは、エクスポートされず、REST API を使用して取得できないため、復元できません。
- 同じ AES-256 パスフレーズは、常に同じ AES-256 キーを生成します。設定のエクスポートファイルは、同じ AES パスフレーズを使用する他の ACI ファブリックにインポートできます。
- トラブルシューティングを目的として、セキュアプロパティの暗号化データが含まれていない設定ファイルをエクスポートします。設定のエクスポートを実行する前に一時的に暗号化をオフにすると、エクスポートされた設定からすべてのセキュアプロパティ値が削除されます。すべてのセキュアプロパティが削除されたそのような設定ファイルをインポートするには、インポート マージ モードを使用します。インポート置換モードは使用しません。インポート マージ モードを使用すると、ACI ファブリック内の既存セキュア プロパティが保持されます。
- デフォルトでは、APIC は復号できないフィールドが含まれているファイルの設定のインポートを拒否します。この設定をオフにするときは注意してください。このデフォルト設定がオフになっているときに設定のインポートが適切に実行されないと、ファブリックの AES 暗号

化設定に一致しない設定ファイルのインポート時にACIファブリックのすべてのパスワードが削除される可能性があります。

（注） このガイドラインに従わないと、ファブリック管理者を含むすべてのユーザがシステムからロックアウトされる可能性があります。

GUI を使用したリモート ロケーションの設定

この手順では、APIC GUIを使用してリモートロケーションを作成する方法について説明します。

手順

ステップ 1 メニュー バーで、[ADMIN] > [Import/Export] の順に選択します。

ステップ 2 ナビゲーション ペインで、[Remote Locations] を右クリックして [Create Remote Location] を選択します。
[Create Remote Location] ダイアログが表示されます。

ステップ 3 [Create Remote Location] ダイアログのフィールドに適切な値を入力します。
（注） フィールドの説明については、[i] アイコンをクリックするとヘルプ ファイルが表示されます。

ステップ 4 [Create Remote Location] ダイアログのフィールドに値を入力したら、[Submit] をクリックします。
これで、データをバックアップするためのリモート ロケーションが作成されました。

NX-OS スタイルの CLI を使用したリモート ロケーションの設定

ACI ファブリックでは、techsupport またはコンフィギュレーション ファイルをエクスポートする 1 つ以上のリモート宛先を設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `apic1# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**[no]remotepath***remote-path-name* 例： `apic1(config)# remote path myFiles`	リモート パスのコンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**user***username* 例： `apic1(config-remote)# user admin5`	リモート サーバにログインするユーザ名を設定します。パスワードを入力するように求められます。
ステップ 4	**path** {**ftp** | **scp** | **sftp**} *host*[*:port*] [**remote-directory**] 例： `apic1(config-remote)# path sftp filehost.example.com:21 remote-directory /reports/apic`	リモート サーバへのパスとプロトコルを設定します。パスワードを入力するように求められます。

例

次に、ファイルをエクスポートするためにリモート パスを設定する例を示します。

```
apic1# configure
apic1(config)# remote path myFiles
apic1(config-remote)# user admin5
You must reset the password when modifying the path:
Password:
Retype password:
apic1(config-remote)# path sftp filehost.example.com:21 remote-directory /reports/apic
You must reset the password when modifying the path:
Password:
Retype password:
```

REST API を使用したリモート ロケーションの設定

この手順では、REST API を使用してリモート ロケーションを作成する方法について説明します。

```
<fileRemotePath name="local" host="‟host or ip" protocol="‟ftp|scp|sftp" remotePath="‟path to
 folder" userName="‟uname" userPasswd="‟pwd" />
```

GUI を使用したエクスポート ポリシーの設定

この手順では、APIC GUI を使用してエクスポート ポリシーを設定する方法について説明します。データのバックアップをトリガーするには、次の手順に従います。

手順

ステップ 1 メニュー バーで、[Admin] > [Import/Export] の順に選択します。

ステップ 2 ナビゲーション ペインで、[Export Policies] を右クリックして [Create Configuration Export Policy] を選択します。

[Create Configuration Export Policy] ダイアログが表示されます。

ステップ 3 [Create Configuration Export Policy] ダイアログのフィールドに適切な値を入力します。

（注） フィールドの説明については、[i] アイコンをクリックするとヘルプ ファイルが表示されます。

ステップ 4 [Create Configuration Export Policy] ダイアログのフィールドに値を入力したら、[Submit] をクリックします。

これで、バックアップが作成されました。[Configuration] タブでこれを確認できます（右側の [Configuration] ペインにバックアップ ファイルが表示されます）。[Operational] タブで状況（実行中、成功、または失敗）を確認できます。まだトリガーしていない場合は、空になっています。バックアップを作成するとファイルが作成され、作成したバックアップ ファイルの [Operational] ビューに表示されます。そのデータをインポートする場合は、インポート ポリシーを作成する必要があります。

NX-OS スタイルの CLI を使用したエクスポート ポリシーの設定

はじめる前に

スケジュールに従ってスナップショットをエクスポートする場合、エクスポート ポリシーを設定する前にスケジューラを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `apic1# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**[no]snapshotexport***policy-name* 例： `apic1(config)# snapshot export myExportPolicy`	スナップショットをエクスポートするポリシーを作成します。
ステップ 3	**format** {**xml** | **json**} 例： `apic1(config-export)# format json`	エクスポートされたコンフィギュレーション ファイルのデータ形式を指定します。
ステップ 4	**[no]schedule***schedule-name* 例： `apic1(config-export)# schedule EveryEightHours`	（任意） スナップショットをエクスポートする既存のスケジューラを指定します。

	コマンドまたはアクション	目的
ステップ 5	**[no]target** [**infra** | **fabric** | *tenant-name*] 例： `apic1(config-export)# target tenantExampleCorp`	（任意） エクスポートのターゲットを割り当てます。ファブリック、インフラ、特定のテナント、またはなしにすることができます。ターゲットを指定しない場合、すべての設定情報がエクスポートされます。デフォルトではターゲットはありません。
ステップ 6	**[no]remotepath***remote-path-name* 例： `apic1(config-export)# remote path myBackupServer`	（任意） ファイルが送信される設定済みのリモート パスの名前を指定します。リモート パスを指定しない場合、ファイルはコントローラ内のフォルダにローカルにエクスポートされます。デフォルトではリモート パスはありません。
ステップ 7	**end** 例： `apic1(config-export)# end`	EXEC モードに戻ります。
ステップ 8	**triggersnapshotexport***policy-name* 例： `apic1# trigger snapshot export myExportPolicy`	スナップショット エクスポート タスクを実行します。エクスポート ポリシーにスケジューラを設定する場合、すぐにエクスポートする場合を除きこの手順は不要です。

例

次に、特定のテナント設定についてJSON形式のスナップショット ファイルの定期的なエクスポートを設定する例を示します。

```
apic1# configure
apic1(config)# snapshot export myExportPolicy
apic1(config-export)# format json
apic1(config-export)# target tenantExampleCorp
apic1(config-export)# schedule EveryEightHours
```

REST API を使用したエクスポート ポリシーの設定

REST API を使用してエクスポート ポリシーを設定するには、次の手順に従います。

```
POST
https://<ip-of-apic>/api/mo/uni/fabric.xml
<fabricInst dn="uni/fabric">
<configExportP name="export" format="xml" adminSt="triggered">
<configRsExportDestination tnFileRemotePathName="backup" />
</configExportP>
```

```
<fileRemotePath name="backup" host="10.10.10.1" protocol="scp"
remotePath="/home/user" userName="user" userPasswd="pass" />
</fabricInst>
```

GUI を使用したインポート ポリシーの設定

この手順では、APIC GUI を使用してインポート ポリシーを設定する方法について説明します。バックアップ データをインポートするには、次の手順に従います。

手順

ステップ 1 メニュー バーで、[ADMIN] > [Import/Export] の順に選択します。

ステップ 2 ナビゲーション ペインで、[Import Policies] を右クリックして [Create Configuration Import Policy] を選択します。
[Create Configuration Import Policy] ダイアログが表示されます。

ステップ 3 [Create Configuration Import Policy] ダイアログのフィールドに適切な値を入力します。
（注） フィールドの説明については、[i] アイコンをクリックするとヘルプ ファイルが表示されます。[Replace]、[Merge]、[Best Effort]、[Atomic] などのインポート タイプやモードの詳細については、『*Cisco Application Centric Infrastructure Fundamentals Guide*』を参照してください。

ステップ 4 [Create Configuration Import Policy] ダイアログのフィールドに値を入力したら、[Submit] をクリックします。

NX-OS スタイルの CLI を使用したインポート ポリシーの設定

NX-OS スタイルの CLI を使用してインポート ポリシーを設定するには、次のように入力します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `apic1# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**[no]snapshotimport***policy-name* 例： `apic1(config)# snapshot import myImportPolicy`	スナップショットをインポートするポリシーを作成します。

	コマンドまたはアクション	目的
ステップ 3	**file***filename* 例： `apic1(config-import)# file ce2_DailyAutoBackup-2015-11-21T01-00-17.tar.gz`	インポートするファイルの名前を指定します。
ステップ 4	**action** {**merge** | **replace**} 例： `apic1(config-import)# action replace`	インポートされた構成設定を現在の設定とマージするかどうか、またはインポートされた設定で現在の設定を完全に置き換えるかどうかを指定します。
ステップ 5	**[no]mode** {**atomic** | **best-effort**} 例： `apic1(config-import)# mode atomic`	インポートされた設定を適用するときに設定エラーをインポート プロセスでどのように処理するかを指定します。ベストエフォート型のインポート モードではアーカイブ内の個々の設定エラーをスキップし、アトミック モードでは設定エラーがあるとインポートをキャンセルします。
ステップ 6	**[no]remotepath***remote-path-name* 例： `apic1(config-import)# remote path myBackupServer`	（任意） ファイルをインポートする設定済みリモートパスの名名を指定します。リモート パスを指定しない場合、ファイルはコントローラ内のフォルダからローカルにインポートされます。デフォルトではリモート パスはありません。
ステップ 7	**end** 例： `apic1(config-import)# end`	EXEC モードに戻ります。
ステップ 8	**triggersnapshotimport***policy-name* 例： `apic1# trigger snapshot import myImportPolicy`	スナップショット インポート タスクを実行します。

例

次に、スナップショット ファイルのインポートの設定および実行を行って現在の設定を置き換える例を示します。

```
apic1# show snapshot files
File    : ce2_DailyAutoBackup-2015-11-21T01-00-17.tar.gz
Created : 2015-11-21T01:00:21.167+00:00
Root    :
Size    : 22926

apic1# configure
apic1(config)# snapshot import myImportPolicy
apic1(config-import)# file ce2_DailyAutoBackup-2015-11-21T01-00-17.tar.gz
apic1(config-import)# action replace
apic1(config-import)# mode atomic
apic1(config-import)# end
apic1# trigger snapshot import myImportPolicy
```

REST API を使用したインポート ポリシーの設定

REST API を使用してインポート ポリシーを設定するには、次の手順に従います。

```
POST
https://<ip-of-apic>/api/mo/uni/fabric.xml
<fabricInst dn="uni/fabric">
<configImportP name="imp" fileName="aa.tar.gz" adminSt="triggered" importType="replace"
importMode="best-effort">
<configRsImportSource tnFileRemotePathName="backup" />
</configImportP>
<fileRemotePath name="backup" host="10.10.10.1" protocol="scp"
remotePath="/home/user" userName="user" userPasswd="pass" />
</fabricInst>
```

GUI を使用した設定ファイルの暗号化

AES-256 暗号化はグローバル設定オプションです。有効にすると、すべてのセキュア プロパティは AES の構成設定に準拠します。特定の targetDn を持つ設定エクスポートを使用して、ACI ファブリック設定の一部をエクスポートできます。ただし、REST API を使用して、セキュア プロパティと AES 暗号化を含むテナント設定などの ACI ファブリック部分のみをエクスポートすることはできません。REST API 要求時にはセキュア プロパティは含まれません。

この項では、AES-256 暗号化を有効にする方法について説明します。

手順

ステップ 1 メニュー バーで、[ADMIN] > [AAA] を選択します。

ステップ 2 ナビゲーション ペインで、[AES Encryption Passphrase and Keys for Config Export (and Import)] をクリックします。

右側のペインに、[Global AES Encryption Settings for all Configurations Import and Export] ウィンドウが表示されます。

ステップ 3 パスフレーズを作成します（16 ～ 32 文字の長さ）。使用される文字のタイプに制限はありません。

ステップ 4 [Submit] をクリックします。

（注） パスフレーズを作成して送信すると、バックエンドでキーが生成され、パスフレーズを復元することはできません。したがって、パスフレーズは、キーを自動的に生成した後で削除されるため、誰にも表示されません。バックアップは、パスフレーズを知っている場合にのみ動作します（他のユーザは誰も開くことはできません）。

[Key Configured] フィールドには [yes] と表示されます。[Encrpyted Passphrase] フィールドには暗号化されたハッシュ（実際のパスフレーズではなく、そのハッシュでしかありません）が表示されます。

ステップ 5 パスフレーズを設定および確認したら、[Enable Encryption] の横にあるチェックボックスをオンにして AES 暗号化機能を有効にします（オンにします）。

これで、エクスポートおよびインポート ポリシーの [Global AES Encryption Settings] フィールドはデフォルトで有効になります。

（注）
- インポートおよびエクスポート ポリシーで [Fail Import if secure fields cannot be decrypted] 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（デフォルトではオンになっています）。設定をインポートするときにこのチェックボックスをオフにしないことを強くお勧めします。このチェックボックスをオフにすると、システムがすべてのフィールドをインポートしようとしても、暗号化できないフィールドはブランクまたは欠落となります。その結果、管理者のパスワードがブランクまたは欠落となると、システムからロックアウトされる可能性があります（システムからロックアウトされた場合は、『*Cisco APIC Troubleshooting Guide*』を参照してください）。このチェックボックスをオフにすると、警告メッセージが表示されます。このボックスをオンにすると、ロックアウトを予防するためのセキュリティ チェックが行われ、その設定はインポートされません。
- [Enable Encryption] チェックボックスが選択されていない（オフ）場合は、暗号化が無効になり、エクスポートされるすべての設定（エクスポート）でセキュア フィールド（パスワードや証明書など）が欠落します。このチェックボックスを選択する（オン）と、暗号化が有効になり、すべてのエクスポートでセキュア フィールドが表示されます。
- 暗号化を有効にした後は、新しいインポートまたはエクスポート ポリシーの作成時にパスフレーズを設定することはできません。前に設定したパスフレーズは、このボックス内のすべての設定およびすべてのテナントにわたってグローバルになっています。このタブから設定をエクスポートすると（パスフレーズが設定され、暗号化は有効）、完全なバックアップ ファイルが得られます。暗号化が有効になっていない場合、セキュア プロパティが削除されたバックアップ ファイルが得られます。これらのバックアップ ファイルは、TAC サポート エンジニア向けにエクスポートする場合に役立ちます（たとえば、すべてのセキュア フィールドが欠落しているため）。これは、設定内のすべてのセキュア プロパティに該当します。また、暗号化キーをクリアするクリア オプションもあります。

次の表で、設定インポートの動作と関連する結果のリストに注意してください。

設定インポートの動作シナリオ	結果
以前のリリースからの古い設定	古いリリースの設定のインポートは完全にサポートされ、古い設定に保存されているすべてのセキュア フィールドが正常にインポートされます。
AES 暗号化が設定されていないときの設定インポート	セキュア フィールドがない設定のインポートである場合は、前に説明した動作で正常に行われます。インポートされる設定にセキュア フィールドがある場合は、拒否されます。
AES パスフレーズが一致しないときの設定インポー	セキュア フィールドがない設定

設定インポートの動作シナリオ	結果
ト	のインポートである場合は、前に説明した動作で正常に行われます。インポートされる設定にセキュア フィールドがある場合は、拒否されます。
AES パスフレーズが一致するときの設定インポート	正常にインポートされます。
コピー/ペーストされたフィールドで AES パスフレーズが一致しないときの設定インポート	この特殊なケースは、別のパスフレーズを使用してエクスポートされた他の設定からセキュア フィールドをコピー/ペーストした場合に発生します。最初のパスでインポートされるバックアップ ファイルを解析しているときに、正しく復号できないプロパティがあった場合、インポートはどのシャードもインポートせずに失敗します。したがって、あるシャードですべてのプロパティを復号することができない場合、すべてのシャードが拒否されます。

NX-OS スタイルの CLI を使用したコンフィギュレーション ファイルの暗号化

NX-OS スタイルの CLI を使用してコンフィギュレーション ファイルを暗号化するには、次の手順を実行します。

```
apic1# configure
apic1(config)# crypto aes
 <CR>
apic1(config)# crypto aes
apic1(config-aes)#
 clear-encryption-key  Clears AES encryption key
encryption            Enable AES Encryption
no                    Negate a command or set its defaults
passphrase            Configure passphrase for AES encryption

bash                  bash shell for unix commands
end                   Exit to the exec mode
exit                  Exit from current mode
fabric                show fabric related information
show                  Show running system information
where                 show the current mode
```

```
apic1(config-aes)# encryption
 <CR>
apic1(config-aes)# encryption
apic1(config-aes)#
 clear-encryption-key  Clears AES encryption key
encryption            Enable AES Encryption
no                    Negate a command or set its defaults
passphrase            Configure passphrase for AES encryption

bash                  bash shell for unix commands
end                   Exit to the exec mode
exit                  Exit from current mode
fabric                show fabric related information
show                  Show running system information
where                 show the current mode
apic1(config-aes)# passphrase
 WORD  Passphrase for AES encryption (Range of chars: 16-32) in quotes
apic1(config-aes)# passphrase "abcdefghijklmnopqrstuvwxyz"
apic1(config-aes)#
```

REST API を使用した設定ファイルの暗号化

手順

REST API を使用して設定ファイルを暗号化するには、次の例のような XML を POST 送信します。

例：

```
https://apic-ip-address/api/mo/uni/fabric.xml
<pkiExportEncryptionKey passphrase="abcdefghijklmnopqrstuvwxyz"
strongEncryptionEnabled="true"/>
```

コントローラコンフィギュレーションのバックアップ、復元、およびロールバック

ここでは、コントローラ コンフィギュレーションのバックアップ（スナップショットの作成）、復元、およびロールバックのための一連の機能について説明します。

設定ファイルのバックアップ、復元、およびロールバックのワークフロー

この項では、設定ファイルのバックアップ、復元、およびロールバックのワークフローについて説明します。本書で説明されている機能はすべて同じワークフロー パターンに従います。対応するポリシーを設定すると、ジョブをトリガーするために **admintSt** を **triggered** に設定する必要があります。

ジョブがトリガーされると、**configJobCont** タイプのコンテナ オブジェクトで **configJob** タイプのオブジェクト（実行を表す）が作成されます（Naming プロパティの値はポリシー DN に設定され

ます）。コンテナの **lastJobName** フィールドを使用して、そのポリシーに対してトリガーされた最後のジョブを確認することができます。

（注） 同時に最大 5 つの **configJob** オブジェクトが単一ジョブ コンテナに保持され、それぞれの新規ジョブがトリガーされます。そのために、最も古いジョブは削除されます。

configJob オブジェクトには、次の情報が含まれています。

- 実行時間
- 処理または生成されるファイルの名前
- 以下のステータス：
  - Pending
  - Running
  - Failed
  - Fail-no-data
  - Success
  - Success-with-warnings
- 詳細の文字列（障害メッセージと警告）
- 進捗率 = 100 * lastStepIndex/totalStepCount
- 最後に行われた内容を示す lastStepDescr フィールド

fileRemotePath オブジェクトについて

fileRemotePath オブジェクトは、以下のリモート ロケーションパスのパラメータを保持しています。

- ホスト名または IP
- ポート
- プロトコル：FTP、SCP など
- リモート ディレクトリ（ファイル パスではない）
- ユーザ名
- パスワード

（注） パスワードは、変更するたびに再送信する必要があります。

設定例

以下に設定サンプルを示します。

fabricInst（uni/fabric）の下に、次のように入力します。

```
<fileRemotePath name="path-name" host="host name or ip" protocol="scp"
remotePath="path/to/some/folder" userName="user-name" userpasswd="password" />
```

コントローラへの設定のエクスポート

設定のエクスポートでは、クラスタ内の32個のシャードすべてからユーザ設定可能な管理対象オブジェクト（MO）のツリーを抽出して別々のファイルに書き込み、tar gzipに圧縮します。次に、tar gzip を、事前設定されているリモート ロケーション（**fileRemotePath** オブジェクトを指す **configRsRemotePath** を使用して設定）にアップロードするか、またはコントローラ上の**スナップショット**として保存します。

（注） 詳細については、「スナップショット」の項を参照してください。

configExportP ポリシーは次のように設定されます。

- **name**：ポリシー名
- **format**：エクスポートされたアーカイブ内にデータを保存する形式（xml または json）
- **targetDn**：エクスポートする特定のオブジェクトのドメイン名（DN）（空はすべてを意味します）
- **snapshot**：true の場合、ファイルはコントローラ上に保存され、リモート ロケーションの設定は不要です。
- **includeSecureFields**：デフォルトで true に設定され、暗号化されたフィールド（パスワードなど）をエクスポートのアーカイブに含めるかどうかを示します。

（注） このスナップショットに関する情報を保持する **configSnapshot** オブジェクトが作成されます（「スナップショット」の項を参照）。

エクスポートのスケジューリング

エクスポート ポリシーは、事前設定されたスケジュールに基づいて自動的にエクスポートをトリガーするスケジューラーにリンクできます。これは、ポリシーから **trigSchedP** オブジェクトへの **configRsExportScheduler** 関係によって行われます（後の「設定例」の項を参照）。

（注） スケジューラーはオプションです。ポリシーは、adminStを**triggered**に設定することにより、いつでもトリガーできます。

トラブルシューティング

生成されたアーカイブをリモート ロケーションにアップロードできないことを示すエラー メッセージが表示された場合は、接続の問題に関する項を参照してください。

NX-OS スタイルの CLI を使用した設定例

以下に、NX-OS スタイルの CLI を使用した設定例を示します。

```
apic1(config)# snapshot
 download  Configuration snapshot download setup mode
export    Configuration export setup mode
import    Configuration import setup mode
rollback  Configuration rollback setup mode
upload    Configuration snapshot upload setup mode
apic1(config)# snapshot export policy-name
apic1(config-export)#
 format    Snapshot format: xml or json
no        Negate a command or set its defaults
remote    Set the remote path configuration will get exported to
schedule  Schedule snapshot export
target    Snapshot target

bash      bash shell for unix commands
end       Exit to the exec mode
exit      Exit from current mode
fabric    show fabric related information
show      Show running system information
where     show the current mode
apic1(config-export)# format xml
apic1(config-export)# no remote path             [If no remote path is specified, the file
 is exported locally to a folder in the controller]
apic1(config-export)# target                     [Assigns the target of the export, which
can be fabric, infra, a specific tenant, or none. If no target is specified, all configuration
 information is exported.]
WORD  infra, fabric or tenant-x
apic1(config-export)#
apic1# trigger snapshot export policy-name       [Executes the snapshot export task]
apic1# ls /data2                                 [If no remote path is specified, the
configuration export file is saved locally to the controller under the folder data2]
ce_Dailybackup.tgz
```

GUI を使用した設定例

以下に、GUI を使用した設定例を示します。

1. メニュー バーで、[ADMIN] タブをクリックします。
2. [IMPORT/EXPORT] を選択します。
3. [Export Policies] の下で、[Configuration] を選択します。
4. [Configuration] の下で、ロールバック先の設定をクリックします。たとえば、デフォルトである [defaultOneTime] をクリックできます。
5. [Format] の横で、JSON 形式または XML 形式のいずれかに対するボタンを選択します。
6. [Start Now] の横で、[No] または [Yes] のボタンを選択し、今すぐトリガーするかスケジュールに基づいてトリガーするかを示します（最も簡単な方法は、ただちにトリガーすることを選択することです）。
7. [Target DN] フィールドに、エクスポートするテナント設定の名前を入力します。
8. 設定をコントローラ自体に保存する場合は、[Snapshot] オプションをオンにします。リモート ロケーションを設定する場合は、このオプションをオフにします。

9 [Scheduler] フィールドでは、オプションで、設定をエクスポートする時間と方法を指示するスケジューラを作成できます。

10 [Encryption] フィールドでは、オプションで、設定ファイルの暗号化を有効または無効にすることができます。

11 設定が完了したら、[Start Now] をクリックします。

12 [SUBMIT] をクリックして、設定のエクスポートをトリガーします。

REST API を使用した設定例

以下に、REST API を使用した設定例を示します。

```
<configExportP name="policy-name" format="xml" targetDn="/some/dn or empty which means
everything"
snapshot="false" adminSt="triggered">
<configRsRemotePath tnFileRemotePathName="some remote path name" />
<configRsExportScheduler tnTrigSchedPName="some scheduler name" />
</configExportP>
```

（注） リモートロケーションを指定するときに、スナップショットをTrueに設定すると、バックアップはリモート パスを無視し、ファイルをコントローラに保存します。

コントローラへの設定のインポート

設定のインポートでは、指定されている以前にエクスポートされたアーカイブのダウンロード、抽出、解析、分析、および適用を、一度に1つのシャードずつ行います（infra、fabric、tn-common、その他すべて、の順）。fileRemotePath 設定は、エクスポートの場合と同様に実行されます（configRsRemotePath を使用）。スナップショットのインポートもサポートされます。

configImportP ポリシーは次のように設定されます。

- **name**：ポリシー名
- **fileName**：インポートするアーカイブ ファイルの名前（パス ファイルではない）
- **importMode**
  - ベスト エフォート モード：各 MO は個々に適用され、エラーがあっても無効な MO がスキップされるだけです。

    （注） オブジェクトがコントローラに存在しない場合、そのオブジェクトの子は設定されません。ベスト エフォート モードでは、オブジェクトの子を設定しようとします。

  - アトミック モード：設定はシャード全体で適用されます。1つのエラーがあると、シャード全体が元の状態にロールバックされます。
- **importType**

- replace：現在のシステム設定は、インポートされる内容またはアーカイブで置換されます（アトミック モードのみをサポート）
- merge：何も削除されず、アーカイブの内容が既存のシステム設定上に適用されます。

- **snapshot**：true の場合、ファイルはコントローラから取得され、リモート ロケーションの設定は不要です。
- **failOnDecryptErrors**：（デフォルトで true）現在システムに設定されているキーとは異なるキーでアーカイブが暗号化されている場合、ファイルはインポートされません。

トラブルシューティング

以下のシナリオでは、トラブルシューティングが必要な可能性があります。

- 生成されたアーカイブをリモート ロケーションからダウンロードできなかった場合は、接続の問題に関する項を参照してください。
- インポートは正常に終了したが警告が表示された場合は、詳細を確認してください。
- ファイルを解析できなかった場合は、以下のシナリオを参照してください。
  - ファイルが有効な XML または JSON ファイルでない場合は、エクスポートされたアーカイブから取得したファイルが手動で変更されたかどうかを確認してください。
  - オブジェクト プロパティに未知のプロパティまたはプロパティ値がある場合は、以下の原因が考えられます。
    - プロパティが削除されたか、または未知のプロパティ値が手動で入力された
    - モデル タイプの範囲が変更された（後方互換性がないモデル変更）
    - 名前付けプロパティ リストが変更された
- MO を設定できなかった場合は、以下に注意してください。
  - ベスト エフォート モードでは、エラーをログに記録し、その MO をスキップします
  - アトミック モードでは、エラーをログに記録し、シャードをスキップします

NX-OS スタイルの CLI を使用した設定例

以下に、NX-OS スタイルの CLI を使用した設定例を示します。

```
apic1# configure
apic1(config)# snapshot
 download  Configuration snapshot download setup mode
export    Configuration export setup mode
import    Configuration import setup mode
rollback  Configuration rollback setup mode
upload    Configuration snapshot upload setup mode
apic1(config)# snapshot import
 WORD       Import configuration name
default
rest-user
```

```
apic1(config)# snapshot import policy-name
apic1(config-import)#
 action  Snapshot import action merge|replace
file    Snapshot file name
mode    Snapshot import mode atomic|best-effort
no      Negate a command or set its defaults
remote  Set the remote path configuration will get imported from

bash    bash shell for unix commands
end     Exit to the exec mode
exit    Exit from current mode
fabric  show fabric related information
show    Show running system information
where   show the current mode
apic1(config-import)# file < from "show snapshot files" >
apic1(config-import)# no remote path
apic1(config-import)#
apic1# trigger snapshot import policy-name       [Executes the snapshot import task]
```

GUI を使用した設定例

以下に、GUI を使用した設定例を示します。

1. メニュー バーで、[ADMIN] タブをクリックします。
2. [IMPORT/EXPORT] を選択します。
3. [Import Policies] の下で、[Configuration] を選択します。
4. [Configuration] の下で、[Create Configuration Import Policy] を選択します。[CREATE CONFIGURATION IMPORT POLICY] ウィンドウが表示されます。
5. [Name] フィールドでは、ファイル名は、バックアップされたファイル名と一致する必要があり、かなり固有の形式です。ファイル名は、バックアップを行った担当者が知っています。
6. 次の 2 つのオプションは、設定の状態の回復に関連しています（「ロールバック」とも呼ばれる）。これらのオプションは、[Input Type] と [Input Mode] です。設定の状態を回復する場合、以前良好であった既知の状態にロールバックします。そのためのオプションは [Atomic Replace] です。
7. 設定をコントローラ自体に保存する場合は、[Snapshot] オプションをオンにします。リモート ロケーションを設定する場合は、このオプションをオフにします。
8. [Import Source] フィールドで、作成済みのリモート ロケーションと同じ値を指定します。
9. [Encryption] フィールドでは、オプションで、設定ファイルの暗号化を

   有効または無効にすることができます。
10. [SUBMIT] をクリックして、設定のインポートをトリガーします。

REST API を使用した設定例

以下に、REST API を使用した設定例を示します。

```
<configImportP name="policy-name" fileName="someexportfile.tgz" importMode="atomic"
importType="replace" snapshot="false" adminSt="triggered">
<configRsRemotePath tnFileRemotePathName="some remote path name" />
</configImportP>
```

スナップショット

スナップショットは設定のバックアップのアーカイブであり、コントローラで管理されているフォルダに保存（および複製）されます。スナップショットを作成するには、**snapshot** プロパティを true に設定してエクスポートを実行します。この場合、リモート パスの設定は不要です。スナップショットをユーザに公開するために、**configSnapshot** タイプのオブジェクトが作成されます。

configSnapshot オブジェクトは以下を提供します。

- ファイル名
- ファイル サイズ
- 作成日
- 何のスナップショットであるかを示すルート DN（ファブリック、インフラ、特定のテナントなど）
- スナップショットを削除する機能（retire フィールドを true に設定）

スナップショットをインポートするには、インポート ポリシーの snapshot プロパティを true に設定し、スナップショット ファイルの名前を指定します（configSnapshot から）。

スナップショット マネージャ ポリシー

configSnapshotManagerP ポリシーを使用すると、リモートで保存したエクスポート アーカイブのスナップショットを作成することができます。ポリシーにリモート パスを付加し、ファイル名（configImportP と同じ）を指定し、モードをダウンロードに設定し、トリガーすることができます。マネージャは、ファイルをダウンロードし、そのファイルを分析してアーカイブが有効であることを確認し、そのファイルをコントローラに保存し、対応する configSnapshot オブジェクトを作成します。スナップショット マネージャを使用すると、リモート ロケーションにスナップショット アーカイブをアップロードすることもできます。この場合、モードをアップロードに設定する必要があります。

トラブルシューティング

トラブルシューティングについては、接続の問題に関する項を参照してください。

NX-OS CLI を使用した、コントローラからリモート パスへのスナップショットのアップロード

```
apic1(config)# snapshot upload policy-name
apic1(config-upload)#
 file    Snapshot file name
no      Negate a command or set its defaults
remote  Set the remote path configuration will get uploaded to

bash    bash shell for unix commands
end     Exit to the exec mode
exit    Exit from current mode
fabric  show fabric related information
show    Show running system information
where   show the current mode
apic1(config-upload)# file <file name from "show snapshot files">
```

```
apic1(config-upload)# remote path remote-path-name
apic1# trigger snapshot upload policy-name       [Executes the snapshot upload task]
```

NX-OS CLI を使用した、コントローラからリモート パスへのスナップショットのダウンロード

```
apic1(config)# snapshot download policy-name
apic1(config-download)#
 file    Snapshot file name
no      Negate a command or set its defaults
remote  Set the remote path configuration will get downloaded from

bash    bash shell for unix commands
end     Exit to the exec mode
exit    Exit from current mode
fabric  show fabric related information
show    Show running system information
where   show the current mode
apic1(config-download)# file < file from remote path>
apic1(config-download)# remote path remote-path-name
apic1# trigger snapshot download policy-name       [Executes the snapshot download task]
```

GUI を使用したスナップショットのアップロードとダウンロード

スナップショットファイルをリモートロケーションにアップロードするには、次の手順に従います。

1. [Config Rollbacks] ペインにリストされているスナップショットを右クリックし、[Upload to Remote Location option] を選択します。[Upload snapshot to remote location] ボックスが表示されます。
2. [Submit] をクリックします。

リモートロケーションからスナップショットファイルをダウンロードするには、次の手順に従います。

1. 画面の右上にあるインポート アイコンをクリックします。[Import remotely stored export archive to snapshot] ボックスが表示されます。
2. [File Name] フィールドにファイル名を入力します。
3. [Import Source] プルダウンからリモート ロケーションを選択するか、または [Or create a new one] の横にあるボックスをオンにして新しいリモート ロケーションを作成します。
4. [Submit] をクリックします。

REST API を使用したスナップショットのアップロードとダウンロード

```
<configSnapshotManagerP name="policy-name" fileName="someexportfile.tgz"
mode="upload|download" adminSt="triggered">
<configRsRemotePath tnFileRemotePathName="some remote path name" />
</configSnapshotManagerP>
```

ロールバック

configRollbackP ポリシーは、2 つのスナップショット間で行われた変更を元に戻すために使用されます。オブジェクトは、次のように処理されます。

- 削除された MO を再作成します

- 作成された MO を削除します
- 変更された MO を元に戻します

（注） ロールバック機能はスナップショットに対してのみ動作します。リモートアーカイブはサポートされません。リモート アーカイブを使用するには、スナップショット マネージャを使用してそこからロールバック用のスナップショットを作成することができます。ポリシーでは、リモート パス設定は不要です。指定されていても、無視されます。

ロールバックのワークフロー

ポリシーの snapshotOneDN フィールドと snapshotTwoDn フィールドを設定する必要があり、最初のスナップショット（S1）がスナップショット 2（S2）より前である必要があります。トリガーされると、スナップショットが抽出および分析され、それらの間の違いが計算され、適用されます。

MO の場所：

- S1 に存在するが、S2 には存在しない：これらの MO は削除され、ロールバックにより再作成されます
- S1 には存在しないが、S2 には存在する：これらの MO は S1 後に作成されており、以下に該当する場合はロールバックにより削除されます。
  - これらの MO は S2 取得後に変更されていない
  - S2 取得後に作成または変更された MO の子孫がない
- S1 と S2 の両方に存在するが、プロパティ値は異なる：S2 取得後にプロパティが別の値に変更されていない限り、これらの MO プロパティは S1 に戻されます。この場合、現状どおりになります。

  ロールバック機能では、これらの計算の結果として生成された設定が含まれている diff ファイルも生成されます。この設定の適用は、ロールバック プロセスの最後のステップです。このファイルの内容は、readiff と呼ばれる特殊な REST API を使用して取得できます。apichost/mqapi2/snapshots.readiff.xml?jobdn=SNAPSHOT_JOB_DN

  ロールバック（予測は困難）にはプレビュー モード（preview を true に設定）もあり、ロールバックにより実際の変更が行われないようにします。diffファイルを計算して生成し、ロールバックを実際に実行したときに何が発生するかを正確にプレビューできます。

Diff ツール

2 つのスナップショット間の diff 機能を提供する別の特殊な REST API を使用できます。apichost/mqapi2/snapshots.diff.xml?s1dn=SNAPSHOT_ONE_DN&s2dn=SNAPSHOT_TWO_DN

NX-OS スタイルの CLI を使用した設定例

この例では、NX-OS スタイルの CLI を使用してロールバックを設定および実行する方法を示します。

```
apic1# show snapshot files
File    : ce2_DailyAutoBackup-2015-11-21T01-00-17.tar.gz
Created : 2015-11-21T01:00:21.167+00:00
Root    :
Size    : 22926

File    : ce2_DailyAutoBackup-2015-11-21T09-00-21.tar.gz
Created : 2015-11-21T09:00:24.025+00:00
Root    :
Size    : 23588

apic1# configure
apic1(config)# snapshot rollback myRollbackPolicy
apic1(config-rollback)# first-file ce2_DailyAutoBackup-2015-11-21T01-00-17.tar.gz
apic1(config-rollback)# second-file ce2_DailyAutoBackup-2015-11-21T09-00-21.tar.gz
apic1(config-rollback)# preview
apic1(config-rollback)# end
apic1# trigger snapshot rollback myRollbackPolicy
```

GUI を使用した設定例

この例では、GUI を使用してロールバックを設定および実行する方法を示します。

1. メニュー バーで、[Admin] タブをクリックします。
2. [Admin] タブにある [Config Rollbacks] をクリックします。
3. [Config Rollbacks] リスト（左側のペイン）で最初の設定ファイルを選択します。
4. [Configuration for selected snapshot] ペイン（右側のペイン）で 2 番目の設定ファイルを選択します。
5. [Compare with previous snapshot] ドロップダウン メニュー（右側のペインの下部）をクリックし、リストから 2 番目の設定ファイルを選択します。その後、2 つのスナップショット間の違いを比較できるように diff ファイルが生成されます。

（注） ファイルが生成された後、これらの変更を元に戻すことができます。

REST API を使用した設定例

この例では、REST API を使用してロールバックを設定および実行する方法を示します。

```
<configRollbackP name="policy-name" snapshotOneDn="dn/of/snapshot/one"
snapshotOneDn="dn/of/snapshot/two" preview="false" adminSt="triggered" />
```

Syslog の使用

Syslog について

稼働中、シスコ アプリケーション セントリック インフラストラクチャ（ACI）システムでの障害またはイベントは、コンソール、ローカル ファイル、および別のシステム上のロギング サーバへのシステム ログ（syslog）の送信をトリガーできます。システム ログ メッセージには、通常、障害またはイベントに関する情報のサブセットが含まれます。システム ログ メッセージには、監査ログとセッション ログのエントリを含めることもできます。

（注） APIC およびファブリック ノードが生成できる syslog メッセージのリストについては、http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/syslog/guide/aci_syslog/ACI_SysMsg.html を参照してください。

多くのシステム ログ メッセージは、ユーザが実行している処理、あるいはユーザが設定または管理しているオブジェクトに固有のものです。これらのメッセージには次のようなものがあります。

- 情報メッセージ。実行している処理のヘルプおよびヒントを提供します。
- 警告メッセージ。ユーザが設定または管理しているオブジェクト（ユーザ アカウントやサービス プロファイルなど）に関連するシステム エラーの情報を提供します。

システム ログ メッセージを受信してモニタするためには、syslog 宛先（コンソール、ローカル ファイル、または syslog サーバを実行している 1 つ以上のリモート ホスト）を指定する必要があります。また、コンソールに表示されるか、ファイルまたはホストによってキャプチャされるメッセージの重大度の最小値を指定できます。syslog メッセージを受信するローカル ファイルは `/var/log/external/messages` です。

Syslog 送信元は、オブジェクト モニタリング ポリシーを適用できる任意のオブジェクトにすることができます。送信されるメッセージの重大度の最小値、syslog メッセージに含める項目、および syslog の宛先を指定できます。

Syslog の表示形式を NX-OS スタイル形式に変更できます。

これらのシステム メッセージを生成する障害またはイベントの詳細については、『*Cisco APIC Faults, Events, and System Messages Management Guide*』で説明されており、システム ログ メッセージは『*Cisco ACI System Messages Reference Guide*』にリストされています。

（注） システム ログ メッセージは、必ずしもシステムに問題があることを示しているとは限りません。単に情報を通知するだけのメッセージもありますし、通信回線、内部ハードウェア、またはシステム ソフトウェアに関する問題点の診断に役立つメッセージもあります。

Syslog の宛先および宛先グループの作成

この手順では、ロギングおよび評価用の syslog データの宛先を設定します。syslog データは、コンソール、ローカル ファイル、または宛先グループ内の 1 つまたは複数の syslog サーバにエクスポートできます。

手順

ステップ 1 メニュー バーで、[Admin] をクリックします。

ステップ 2 サブメニュー バーで、[External Data Collectors] をクリックします。

ステップ 3 [Navigation] ペインで、[Monitoring Destinations] を展開します。

ステップ 4 [Syslog] を右クリックし、[Create Syslog Monitoring Destination Group] を選択します。

ステップ 5 [Create Syslog Monitoring Destination Group] ダイアログボックスで、次の操作を実行します。

a) グループおよびプロファイルの [Name] フィールドに、モニタリングの宛先グループおよびプロファイルの名前を入力します。

b) グループおよびプロファイルの [Admin State] ドロップダウン リストで、[enabled] を選択します。

c) ローカル ファイルへの syslog メッセージの送信を有効にするには、[Local File Destination] の [Admin State] ドロップダウン リストから [enabled] を選択し、[Local File Destination] の [Severity] ドロップダウン リストから重大度の最小値を選択します。
syslog メッセージを受信するローカル ファイルは `/var/log/external/messages` です。

d) コンソールへの syslog メッセージの送信を有効にするには、[Console Destination] の [Admin State] ドロップダウン リストから [enabled] を選択し、[Console Destination] の [Severity] ドロップダウン リストから重大度の最小値を選択します。

e) [Next] をクリックします。

f) [Create Remote Destinations] 領域で、[+] をクリックしてリモート宛先を追加します。

注意 使用する DNS サーバがインバンド接続を介して到達できるように設定されていると、リモート syslog 宛先のホスト名解決が失敗する可能性があります。この問題を回避するには、IP アドレスを使用して syslog サーバを設定するか、ホスト名を使用する場合は、DNS サーバがアウトオブバンド インターフェイスを介して到達可能であることを確認してください。

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

a) [Host] フィールドに、送信先ホストの IP アドレスまたは完全修飾ドメイン名を入力します。

b) （任意） [Name] フィールドに、宛先ホストの名前を入力します。

c) [Admin State] フィールドで、[enabled] オプション ボタンをクリックします。

d) （任意） 重大度の最小値 [Severity]、[Port] 番号、および syslog の [Forwarding Facility] を選択します。

e) [Management EPG] ドロップダウン リストから管理エンドポイント グループを選択します。

f) [OK] をクリックします。

ステップ 7 （任意） リモート宛先グループにリモート宛先を追加するには、もう一度 [+] をクリックし、[Create Syslog Remote Destination] ダイアログボックスの手順を繰り返します。

ステップ 8 [Finish] をクリックします。

Syslog 送信元の作成

Syslog 送信元は、オブジェクト モニタリング ポリシーを適用できる任意のオブジェクトにすることができます。

はじめる前に

syslog モニタリング宛先グループを作成します。

手順

ステップ 1 メニュー バーおよびナビゲーション フレームから、関心領域の [Monitoring Policies] メニューに移動します。
テナント、ファブリック、およびアクセスのモニタリング ポリシーを設定できます。

ステップ 2 [Monitoring Policies] を展開し、モニタリング ポリシーを選択して展開します。
[Fabric] > [Fabric Policies] > [Monitoring Policies] > [Common Policy] の下に、基本モニタリング ポリシーがあります。このポリシーは、すべての障害とイベントに適用され、ファブリック内のすべてのノードとコントローラに自動的に導入されます。または、スコープが限定された既存のポリシーを指定することもできます。

ステップ 3 モニタリング ポリシーの下で、[Callhome/SNMP/Syslog] をクリックします。

ステップ 4 [Work] ペインで、[Source Type] ドロップダウン リストから [Syslog] を選択します。

ステップ 5 [Monitoring Object] リストから、モニタ対象の管理対象オブジェクトを選択します。
目的のオブジェクトがリストに表示されない場合は、次の手順に従います。

a) [Monitoring Object] ドロップダウン リストの右側にある [Edit] アイコンをクリックします。
b) [Select Monitoring Package] ドロップダウン リストから、オブジェクト クラス パッケージを選択します。
c) モニタ対象の各オブジェクトのチェックボックスをオンにします。
d) [Submit] をクリックします。

ステップ 6 テナント モニタリング ポリシーでは、[All] ではなく特定のオブジェクトを選択すると、[Scope] 選択が表示されます。
[Scope] フィールドで、オプション ボタンを選択して、このオブジェクトに関して送信するシステム ログ メッセージを指定します。

- [all]：このオブジェクトに関連するすべてのイベントと障害を送信します。

- [specific event]：このオブジェクトに関連する指定されたイベントのみを送信します。[Event] ドロップダウン リストからイベント ポリシーを選択します。
- [specific fault]：このオブジェクトに関連する指定された障害のみを送信します。[Fault] ドロップダウン リストから障害ポリシーを選択します。

ステップ 7 [+] をクリックして syslog 送信元を作成します。

ステップ 8 [Create Syslog Source] ダイアログボックスで、次の操作を実行します。

a) [Name] フィールドに、syslog 送信元の名前を入力します。
b) [Min Severity] ドロップダウン リストから、送信するシステム ログ メッセージの重大度の最小値を選択します。
c) [Include] フィールドで、送信するメッセージ タイプのチェックボックスをオンにします。
d) [Dest Group] ドロップダウン リストから、システム ログ メッセージの送信先の syslog 宛先グループを選択します。
e) [Submit] をクリックします。

ステップ 9 （任意） syslog 送信元を追加するには、もう一度 [+] をクリックし、[Create Syslog Source] ダイアログボックスの手順を繰り返します。

REST API を使用した NX-OS CLI 形式での Syslog 表示の有効化

デフォルトで Syslog 形式は RFC 5424 に準拠しています。次の例のように、Syslog のデフォルト表示を NX-OS タイプ形式に変更できます。

```
apic1# moquery -c "syslogRemoteDest"
Total Objects shown: 1

# syslog.RemoteDest
host                : 172.23.49.77
adminState          : enabled
childAction         :
descr               :
dn                  : uni/fabric/slgroup-syslog-mpod/rdst-172.23.49.77
epgDn               :
format              : nxos
forwardingFacility  : local7
ip                  :
lcOwn               : local
modTs               : 2016-05-17T16:51:57.231-07:00
monPolDn            : uni/fabric/monfab-default
name                : syslog-dest
operState           : unknown
port                : 514
rn                  : rdst-172.23.49.77
severity            : information
status              :
uid                 : 15374
vrfId               : 0
vrfName             :
```

NX-OS タイプ形式で Syslog を表示できるようにするには、REST API を使用して次の手順を実行します。

手順

ステップ 1 次の例に示すように、NX-OS タイプ形式での Syslog の表示を有効にします。

```
POST https://192.168.20.123/api/node/mo/uni/fabric.xml
<syslogGroup name="DestGrp77" format="nxos">
<syslogRemoteDest name="slRmtDest77" host="172.31.138.20" severity="debugging"/>
</syslogGroup>
```

syslogGroup は Syslog モニタリングの宛先グループ、sysLogRemoteDest は事前に設定した Syslog サーバの名前、host は事前に設定した Syslog サーバの IP アドレスです。

ステップ 2 次の例に示すように、Syslog 形式をデフォルトの RFC 5424 形式に戻します。

```
POST https://192.168.20.123/api/node/mo/uni/fabric.xml
<syslogGroup name="DestGrp77" format="aci">
<syslogRemoteDest name="slRmtDest77" host="172.31.138.20" severity="debugging"/>
</syslogGroup>
```

アトミック カウンタの使用

アトミック カウンタについて

アトミック カウンタは、フロー間のトラフィックに関する統計情報を収集できます。アトミック カウンタを使用すると、ファブリック内のドロップとルーティングミスを検出し、アプリケーション接続に関する問題の迅速なデバッグと分離が可能になります。たとえば、管理者はすべてのリーフ スイッチでアトミック カウンタを有効にして、エンドポイント 1 からエンドポイント 2 のパケットをトレースすることができます。送信元と宛先のリーフ スイッチ以外のリーフ スイッチにゼロ以外のカウンタがある場合、管理者はそれらのリーフにドリル ダウンできます。

従来の設定では、ベア メタル NIC から特定の IP アドレス（エンドポイント）または任意の IP アドレスへのトラフィックの量をモニタすることはほぼ不可能です。アトミック カウンタでは、データ パスに干渉することなく、管理者がベア メタル エンドポイントから受信されたパケットの数を数えることができます。さらに、アトミック カウンタはエンドポイントまたはアプリケーション グループで送受信されるプロトコルごとのトラフィックをモニタリングできます。

リーフ間（TEP 間）のアトミック カウンタは次を提供できます。

- 送信パケット、受信パケット、ドロップ パケット、および超過パケットのカウント
  - 送信パケット：送信数は、送信元 TEP（トンネル エンドポイント）から宛先 TEP に送信されたパケット数を表します。
  - 受信パケット：受信数は、宛先 TEP が送信元 TEP から受信したパケット数を表します。

- ドロップパケット：ドロップ数は、伝送中にドロップされたパケット数を表します。この数値は、送信パケット量と受信パケット量の差です。
- 超過パケット：超過数は、伝送中に受信された超過パケット数を表します。この数値は、転送の不一致または間違った場所へのルーティングミスによって予期せず受信されたパケット量です。

- 最後の 30 秒などの短期間のデータ収集、5 分、15 分、またはそれ以上の長期間のデータ収集
- スパイン トラフィックごとの詳細（TEP、リーフ、または VPC の数が 64 未満の場合に使用可能）
- 継続的なモニタリング

（注） リーフ間（TEP間）アトミック カウンタは累積であり、クリアできません。 ただし、30 秒のアトミック カウンタは 30 秒間隔でリセットされるため、断続的な問題や、再発する問題の分離に使用できます。アトミック カウンタには、アクティブなファブリック ネットワーク タイム プロトコル（NTP）ポリシーが必要です。

テナントのアトミック カウンタは次を提供できます。

- 送信、受信、ドロップ、および超過パケットを含む、ファブリック全体のトラフィックのアプリケーション固有カウンタ
- モードは次を含みます。
  - EPtoEP（エンドポイント間）
  - EPGtoEPG（エンドポイント グループ間）

    （注） EPGtoEPG の場合、オプションには ipv4 のみ、ipv6 のみ、ipv4、ipv6 が含まれます。ipv6 オプションがある場合は必ず TCAM エントリを 2 回使用します。これは、スケール数が、純粋な ipv4 ポリシーの場合に予期される数より小さい可能性があることを意味します。

  - EPGtoEP（エンドポイント グループ/エンドポイント間）
  - EPtoAny（エンドポイント ツー エニー）
  - AnytoEP（エニー ツー エンドポイント）
  - EPGtoIP（エンドポイント グループ/IP 間、外部 IP アドレスの場合にのみ使用）
  - EPtoExternalIP（エンドポイント/外部 IP アドレス間）

アトミック カウンタに関する注意事項および制約事項

- アトミック カウンタの使用は、エンドポイントが異なるテナントまたは同じテナント内の異なるコンテキスト（VRF）にある場合はサポートされません。
- IP アドレスが学習されない純粋なレイヤ 2 設定（IP アドレスは 0.0.0.0）では、エンドポイント/EPG 間および EPG/エンドポイント間のアトミック カウンタ ポリシーはサポートされません。この場合、エンドポイント間および EPG 間のポリシーはサポートされます。外部ポリシーは学習された IP アドレスが必要な Virtual Routing and Forwarding（VRF）ベースであり、サポートされます。
- アトミック カウンタの送信元または宛先がエンドポイントである場合、そのエンドポイントはスタティックではなくダイナミックである必要があります。ダイナミック エンドポイント（fv:CEp）とは異なり、スタティック エンドポイント（fv:StCEp）にはアトミック カウンタに必要な子オブジェクト（fv:RsCEpToPathEp）がありません。
- 中継トポロジでは、リーフ スイッチはすべてのスパイン スイッチを使用したフル メッシュにはなく、リーフ間（TEP 間）のカウンタは予期どおりに動作しません。
- リーフ間（TEP 間）アトミック カウンタの場合、トンネル数がハードウェア制限を上回ると、システムはモードをトレール モードからパス モードに変更し、ユーザにはスパインごとのトラフィックは表示されなくなります。
- アトミック カウンタはスパイン プロキシ トラフィックはカウントしません。
- ファブリックに入る前、またはリーフ ポートに転送される前にドロップされたパケット、アトミック カウンタによって無視されます。
- ハイパーバイザで切り替えられるパケット（同じポート グループとホスト）はカウントされません。
- アトミック カウンタには、アクティブなファブリック ネットワーク タイム プロトコル（NTP）ポリシーが必要です。
- アトミック カウンタは IPv6 の送信元と宛先で動作しますが、IPv4 アドレスと IPv6 アドレスを混在させて送信元 IP アドレスと宛先 IP アドレスを設定することはできません。
- 送信元または宛先として fvCEp を使用して設定されたアトミック カウンタ ポリシーでは、fvCEp 管理対象オブジェクト（MO）に存在する MAC アドレスおよび IP アドレスからの、または両者へのトラフィックのみがカウントされます。 fvCEp MO の IP アドレス フィールドが空である場合、その MAC アドレスへの/からのすべてのトラフィックが IP アドレスに関係なくカウントされます。APIC が fvCEp について複数の IP アドレスを学習している場合、前述のように、fvCEp MO 自体にある 1 つの IP アドレスのみがカウントされます。特定の IP アドレスへの/からのアトミック カウンタ ポリシーを設定するには、送信元または宛先として fvIp MO を使用します。
- fvCEp の背後に fvIp が存在する場合は、fvCEp ベースのポリシーではなく fvIP ベースのポリシーを追加する必要があります。

アトミック カウンタの構成

手順

ステップ 1 メニュー バーで、[Tenants] をクリックします。

ステップ 2 サブメニュー バーで、必要なテナントをクリックします。

ステップ 3 [Navigation] ペインでテナントを拡張し、[Troubleshoot Policies] を拡張します。

ステップ 4 [Troubleshoot Policies] の下で [Atomic Counter Policy] を展開し、トラフィック トポロジを選択します。
エンドポイントの組み合わせ、エンドポイント グループ、外部インターフェイスおよびIPアドレス間のトラフィックを測定できます。

ステップ 5 必要なトポロジを右クリックして、[Add*topology*Policy] を選択し、[Add Policy] ダイアログボックスを開きます。

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

a) [Name] フィールドにポリシーの名前を入力します。

b) トラフィックの送信元の識別情報を選択するか、入力します。
必要な識別情報のソース（エンドポイント、エンドポイントのグループ、外部インターフェイス、または IP アドレス）によって異なります。

c) トラフィックの宛先の識別情報を選択するか、入力します。

d) （任意） （任意）[Filters] テーブルで + アイコンをクリックし、カウントするトラフィックのフィルタリングを指定します。
表示される [Create Atomic Counter Filter] ダイアログボックスで、IP プロトコル番号（たとえば TCP=6）によるフィルタリング、および送信元と宛先の IP ポート番号によるフィルタリングを指定できます。

e) [Submit] をクリックし、アトミック カウンタ ポリシーを保存します。

ステップ 7 [Navigation] ペインで、選択したトポロジの下の新しいアトミック カウンタ ポリシーを選択します。
ポリシー設定が [Work] ペインに表示されます。

ステップ 8 [Work] ペインで [Operational] タブをクリックし、[Traffic] サブタブをクリックして、アトミック カウンタの統計情報を表示します。

SNMP の使用

SNMP の概要

Cisco Application Centric Infrastructure （ACI）は、管理情報ベース（MIB）と通知（トラップ）を含む広範な SNMPv1、v2、および v3 のサポートを提供します。SNMP 標準では、ACI ファブリックを管理しモニタするさまざまな MIB をサポートするサードパーティ製アプリケーションを使用できます。

SNMPv3 はさらに広範なセキュリティ機能を提供します。各 SNMPv3 デバイスで SNMP サービスを有効または無効にするように選択できます。また、各デバイスで SNMP v1 および v2 要求の処理方法を設定できます。

SNMP の使用方法の詳細については、『*Cisco ACI MIB Quick Reference*』を参照してください。

ACI での SNMP アクセスのサポート

ACI での SNMP のサポートは次のとおりです。

- SNMP 読み取りクエリー（Get、Next、Bulk、Walk）は、リーフおよびスパイン スイッチと APIC によってサポートされます。
- SNMP 書き込みコマンド（Set）は、リーフおよびスパイン スイッチまたは APIC によってサポートされません。
- SNMP トラップ（v1、v2c、および v3）は、リーフおよびスパイン スイッチと APIC によってサポートされます。

（注） ACI は最大 10 個のトラップ レシーバをサポートします。

- SNMPv3 は、リーフおよびスパイン スイッチと APIC によってサポートされます。

表 *1*：*Cisco APIC* リリースでの *SNMP* サポートの変更

リリース	説明
1.2(2)	SNMP トラップの宛先として IPv6 サポートを追加。
1.2(1)	APIC コントローラの SNMP サポートを追加。以前のリリースでは、リーフおよびスパイン スイッチについてのみ SNMP がサポートされています。

ACI でサポートされる MIB の完全なリストについては、http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/mib/list/mib-support.html を参照してください。

SNMP の設定

GUI による SNMP ポリシーの設定

この手順では、ACI スイッチの SNMP ポリシーを設定し、有効にします。

はじめる前に

SNMP 通信を有効にするには、以下の設定が必要です。

- アウトオブバンド コントラクトを設定して SNMP トラフィックを許可します。SNMP トラフィックは、通常、SNMP 要求に UDP ポート 161 を使用します。
- 'mgmt' テナントで APIC アウトオブバンド IP アドレスを設定します。アウトオブバンド アドレスは APIC セットアップ時に設定されますが、アウトオブバンド コントラクトを有効にするには 'mgmt' テナントでアドレスを明示的に設定する必要があります。

手順

ステップ 1 メニュー バーで、[Fabric] をクリックします。

ステップ 2 サブメニュー バーで、[Fabric Policies] をクリックします。

ステップ 3 [Navigation] ペインで、[Pod Policies] を展開します。

ステップ 4 [Pod Policies] の下で [Policies] を展開します。

ステップ 5 [SNMP] を右クリックし、[Create SNMP Policy] を選択します。
新しい SNMP ポリシーを作成する代わりに、次の手順で示されるものと同じ方法で [default] ポリシー フィールドを編集できます。

ステップ 6 SNMP ポリシーのダイアログボックスで、次の操作を実行します。

a) [Name] フィールドに、SNMP ポリシーの名前を入力します。
b) [Admin State] フィールドで、[Enabled] を選択します。
c) [Community Policies] テーブルで [+] アイコンをクリックし、[Name]（@ 記号を除く）を入力して [Update] をクリックします。
d) （任意） [SNMP v3 Users] テーブルで + アイコンをクリックし、名前を入力して、ユーザの認証データを入力し、[Update] をクリックします。
この手順は SNMPv3 アクセスが必要な場合のみ実行します。

ステップ 7 許可された SNMP 管理ステーションを設定するには、SNMP ポリシーのダイアログボックスで、次の操作を実行します。

a) [Client Group Policies] テーブルで + アイコンをクリックし、[Create SNMP Client Group Profile] ダイアログボックスを開きます。
b) [Name] フィールドに、SNMP クライアント グループのプロファイル名を入力します。
c) [Associated Management EPG] ドロップダウン リストから管理 EPG を選択します。
d) [Client Entries] テーブルで + アイコンをクリックします。

e) [Name] フィールドにクライアントの名前を入力し、[Address] のフィールドにクライアントの IP アドレスを入力して、[Update] をクリックします。

（注） SNMP 管理ステーションが SNMPv3 を使用して APIC と接続する場合、APIC は SNMP クライアント グループのプロファイルに指定されたクライアント IP アドレスを強制しません。SNMPv3 の場合、管理ステーションが [Client Entries] リストに含まれている必要がありますが、SNMPv3 クレデンシャルのみでアクセス可能なため、IP アドレスが一致している必要はありません。

ステップ 8 [OK] をクリックします。

ステップ 9 [Submit] をクリックします。

ステップ 10 [Pod Policies] の下で [Policy Groups] を展開して、ポリシー グループを選択するか、または [Policy Groups] を右クリックし、[Create POD Policy Group] を選択します。
新しいポッドポリシーグループを作成することも、既存のグループを使用することもできます。ポッド ポリシー グループには、SNMP ポリシーに加えて他のポッド ポリシーを含めることができます。

ステップ 11 ポッド ポリシー グループのダイアログボックスで、次の操作を実行します。

a) [Name] フィールドに、ポッド ポリシー グループの名前を入力します。

b) [SNMP Policy] ドロップダウン リストから、設定した SNMP ポリシーを選択して、[Submit] をクリックします。

ステップ 12 [Pod Policies] の下で [Profiles] を展開し、[default] をクリックします。

ステップ 13 [Work] ペインで、[Fabric Policy Group] ドロップダウン リストから、作成したポッド ポリシー グループを選択します。

ステップ 14 [Submit] をクリックします。

ステップ 15 [OK] をクリックします。

GUI による SNMP トラップ通知先の設定

この手順では、SNMP トラップ通知を受信する SNMP マネージャのホスト情報を設定します。

（注） ACI は最大 10 個のトラップ レシーバをサポートします。10 個より多く設定すると、一部では通知が受信されません。

手順

ステップ 1 メニュー バーで、[Admin] をクリックします。

ステップ 2 サブメニュー バーで、[External Data Collectors] をクリックします。

ステップ 3 [Navigation] ペインで、[Monitoring Destinations] を展開します。

ステップ 4 [SNMP] を右クリックし、[Create SNMP Monitoring Destination Group] を選択します。

ステップ 5 [Create SNMP Monitoring Destination Group] ダイアログボックスで、次の操作を実行します。

a) [Name] フィールドに、SNMP 通知先の名前を入力し、[Next] をクリックします。

b) [Create Destinations] テーブルで + アイコンをクリックし、[Create SNMP Trap Destination] ダイアログボックスを開きます。

c) [Host Name/IP] フィールドに、送信先ホストの IP アドレスまたは完全修飾ドメイン名を入力します。

（注） Cisco APIC Release 1.2(2) 以降のリリースは、IPv6 SNMP トラップ宛先をサポートします。

d) 通知先のポート番号と SNMP バージョンを選択します。

e) SNMP v1 または v2c 通知先の場合、[Security Name] として設定したコミュニティ名の 1 つを入力し、[v3 Security Level] として [noauth] を選択します。
SNMP コミュニティ名に @ 記号を含めることはできません。

f) SNMP v3 通知先の場合、[Security Name] として設定したユーザ名の 1 つを入力し、必要な [v3 Security Level] を選択します。

g) [Management EPG] ドロップダウン リストから管理 EPG を選択します。

h) [OK] をクリックします。

i) [Finish] をクリックします。

GUI による SNMP トラップ ソースの設定

この手順では、ファブリック内のソース オブジェクトを選択して有効にし、SNMP トラップ通知を生成します。

手順

ステップ 1 メニュー バーで、[Fabric] をクリックします。

ステップ 2 サブメニュー バーで、[Fabric Policies] をクリックします。

ステップ 3 [Navigation] ペインで、[Monitoring Policies] を展開します。
共通ポリシー、デフォルト ポリシーで SNMP ソースを作成することも、または新しいモニタリング ポリシーを作成することもできます。

ステップ 4 必要なモニタリング ポリシーを展開し、[Callhome/SNMP/Syslog] を選択します。

[Common Policy] を選択する場合は、[Common Policy] を右クリックして、[Create SNMP Source] を選択し、そのダイアログボックスで次の手順に従ってください。

ステップ 5 [Work] ペインで、[Monitoring Object] ドロップダウン リストから [ALL] を選択します。

ステップ 6 [Source Type] ドロップダウン リストから、[SNMP] を選択します。

ステップ 7 テーブルで + アイコンをクリックし、[Create SNMP Source] ダイアログボックスを開きます。

ステップ 8 [Create SNMP Source] ダイアログボックスで、次の操作を実行します。

a) [Name] フィールドに、SNMP ポリシーの名前を入力します。

b) [Dest Group] ドロップダウン リストから、通知を送信する既存の宛先を選択するか、または [Create SNMP Monitoring Destination Group] を選択して、新しい宛先を作成します。
SNMP の通知先グループを作成する手順は、別項で説明します。

c) [Submit] をクリックします。

SNMP を使用したシステムのモニタリング

個々のホスト（APIC またはその他のホスト）をリモートでモニタし、特定のノードの状態を確認できます。

SNMP を使用してシステムの CPU とメモリの使用状況をチェックし、CPU のスパイクが発生しているかどうかを確認できます。SNMP（ネットワーク管理システム）は、SNMP クライアントを使用して APIC の情報にアクセスし、情報を取得します。

リモートでシステムにアクセスして、情報がネットワーク管理システムのコンテキストに属するものかどうかを確認し、CPU またはメモリの使用量が多すぎないか、またはシステムやパフォーマンスの問題が発生しているかどうかを調べることができます。問題の原因がわかると、システムの正常性をチェックし、メモリまたは CPU の使用量が多すぎないかどうかを確認できます。

詳細については、『*Cisco ACI MIB Quick Reference Manual*』を参照してください。

SPAN の使用

SPAN の概要

スイッチド ポート アナライザ（SPAN）ユーティリティを使って、詳細なトラブルシューティングの実行または特定のアプリケーション ホストからトラフィックのサンプルを取得し、プロアクティブなモニタリングと分析を行うことができます。

SPAN は 1 つ以上のポート、VLAN、またはエンドポイント グループ（EPG）からのトラフィックをコピーし、ネットワーク アナライザによる分析のためにコピーしたトラフィックを 1 つ以上の送信先に送信します。このプロセスはどの接続デバイスも中断せず、ハードウェア内で実施されるので不要な CPU 負荷を防ぎます。

SPANセッションはソースが受信したトラフィック（入力トラフィック）、ソースから送信したトラフィック（出力トラフィック）、またはその両方をモニタリングするように設定できます。デフォルトでは、SPAN はすべてのトラフィックをモニタリングしますが、選択したトラフィックだけをモニタリングするようにフィルタを設定できます。

マルチノード SPAN

APIC トラフィックのモニタリング ポリシーは、各アプリケーション グループのメンバーとそれが接続する場所を追跡するために、適切な場所でポリシーを SPAN することが可能です。いずれかのメンバーが移動した場合、APIC は新しいリーフ スイッチに自動的にポリシーをプッシュします。たとえば、エンドポイントが新しいリーフ スイッチに VMotion すると、SPAN 設定が自動的に調整されます。

SPAN の注意事項と制約事項

- SPANはトラブルシューティングのために使用します。SPAN トラフィックはスイッチ リソースのユーザ トラフィックと競合します。負荷を最小限にするには、分析対象の特定のトラフィックだけをコピーするように SPAN を設定します。
- SPAN 送信元として l3extLIfP のレイヤ 3 サブインターフェイスを指定することはできません。外部ソースからのトラフィックをモニタリングするためにはポート全体を使用します。
- テナントおよびアクセス SPAN は カプセル化リモート拡張 SPAN（ERSPAN）タイプ I を使用し、ファブリック SPAN は ERSPAN タイプ II を使用します。ERSPAN ヘッダーについては、IETF の Internet Draft（https://tools.ietf.org/html/draft-foschiano-erspan-00）を参照してください。
- ファブリックでは ERSPAN の宛先 IP をエンドポイントとして学習する必要があります。
- SPAN は IPv6 トラフィックをサポートしますが、ERSPAN の宛先 IP を IPv6 アドレスにすることはできません。
- アクティブな SPAN セッションの最大数など、SPAN 関連の制限については、『『*Verified Scalability Guide for Cisco ACI*』』という資料 を参照してください。

SPAN セッションの設定

この手順では、リモート トラフィック アナライザにレプリケートされたソース パケットを転送するようにポリシーを設定する方法を示します。

手順

ステップ 1 メニュー バーで、[Tenants] をクリックします。

ステップ 2 サブメニュー バーで、送信元エンドポイントを含むテナントをクリックします。

ステップ 3 [Navigation] ペインでテナントを拡張し、[Troubleshooting Policies] を拡張して、[SPAN] を拡張します。

ステップ 4 [SPAN] の下で [SPAN Destination Groups] を右クリックし、[Create SPAN Destination Group] を選択します。
[Create SPAN Destination Group] ダイアログが表示されます。

ステップ 5 [Create SPAN Destination Group] ダイアログボックスの必須フィールドに適切な値を入力し、[OK]、[Submit] の順にクリックします。
（注） フィールドの説明については、ダイアログボックスの右上隅にある情報アイコン（i）をクリックするとヘルプ ファイルが表示されます。

ステップ 6 [SPAN] の下で [SPAN Source Groups] を右クリックし、[Create SPAN Source Group] を選択します。
[Create SPAN Source Group] ダイアログが表示されます。

ステップ 7 [Create SPAN Source Group] ダイアログボックスの必須フィールドに適切な値を入力し、[OK]、[Submit] の順にクリックします。
（注） フィールドの説明については、ダイアログボックスの右上隅にある情報アイコン（i）をクリックするとヘルプ ファイルが表示されます。

次の作業

SPAN 送信先のトラフィック アナライザを使用して、SPAN 送信元 EPGからのデータ パケットを観察し、パケット形式、アドレス、プロトコルおよびその他の情報を確認できます。

トレースルートの使用

トレースルートの概要

traceroute ツールは、パケットが送信先に移動するときに実際に通るルートを検出するために使用されます。traceroute では、ホップごとに使用されるパスが識別され、双方向で各ホップにタイムスタンプが付けられます。traceroute を使用すると、発信元のデバイスと送信先に最も近いデバイスの間のパスに沿ってポート接続をテストできます。送信先に到達できない場合は、パス検出によってパスが障害ポイントまで追跡されます。

テナントのエンドポイントから開始されたトレースルートは、入力リーフのスイッチに表示される中間ホップとしてデフォルト ゲートウェイを示します。

トレースルートは、エンドポイント間やリーフ間（トンネル エンドポイント、または TEP 間）など、さまざまなモードをサポートしています。トレースルートはファブリック全体のすべてのパ

スを検出し、外部エンドポイントの出口を検出します。パスが妨げられているかどうかを発見するのに役立ちます。

トレースルートの注意事項および制約事項

- トレースルートの送信元または宛先がエンドポイントである場合、そのエンドポイントはスタティックではなくダイナミックである必要があります。ダイナミック エンドポイント（fv:CEp）とは異なり、スタティック エンドポイント（fv:StCEp）にはトレースルートに必要な子オブジェクト（fv:RsCEpToPathEp）がありません。
- トレースルートは IPv6 の送信元と宛先で動作しますが、IPv4 アドレスと IPv6 アドレスを混在させて送信元 IP アドレスと宛先 IP アドレスを設定することはできません。
- トレースルート関連の制限については、『*Verified Scalability Guide for Cisco ACI*』というマニュアルを参照してください。

エンドポイント間でのトレースルートの実行

手順

ステップ 1 メニュー バーで、[Tenants] をクリックします。

ステップ 2 サブメニュー バーで、送信元エンドポイントを含むテナントをクリックします。

ステップ 3 [Navigation] ペインでテナントを拡張し、[Troubleshoot Policies] を拡張します。

ステップ 4 [Troubleshoot Policies] の下で、[Endpoint-to-Endpoint Traceroute Policies] を右クリックし、[Create Endpoint-to-Endpoint Traceroute Policy] を選択します。

ステップ 5 [Create Endpoint-to-Endpoint Traceroute Policy] ダイアログボックスのフィールドに適切な値を入力し、[Submit] をクリックします。

（注） フィールドの説明については、[Create Endpoint-to-Endpoint Traceroute Policy] ダイアログボックスの右上隅にある情報アイコン（i）をクリックします。

ステップ 6 **[Navigation]** ペインまたは [Traceroute Policies] テーブルで、traceroute ポリシーをクリックします。トレースルート ポリシーが [Work] ペインに表示されます。

ステップ 7 [Work] ペインで [Operational] タブをクリックし、[Source End Points] タブをクリックして、[Results] タブをクリックします。

ステップ 8 [Traceroute Results] テーブルで、追跡に使用された単数または複数のパスを確認します。

（注）
- 複数のパスが、送信元ノードから宛先ノードへの移動に使用されている場合があります。
- [Name] 列など、1 つまたは複数の列の幅を広げると確認しやすくなります。