管理

この章の内容は、次のとおりです。

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。

インバンドおよびアウトオブバンド管理アクセス

管理テナントでは、ファブリック管理機能へのアクセスを設定するための便利な方法が提供されます。APIC を介してファブリック管理機能にアクセスできると同時に、インバンドおよびアウトオブバンドのネットワーク ポリシー経由で直接アクセスすることもできます。

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、KB 記事、「*Configuring Static Management Access in Cisco APIC*」を参照してください。
- このタスク例のビデオを視聴するには、ビデオを掲載している Web ページ を参照してください。

手順の概要

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。
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。
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。
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。
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。
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。
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。
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。
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。
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。
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。
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。
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。

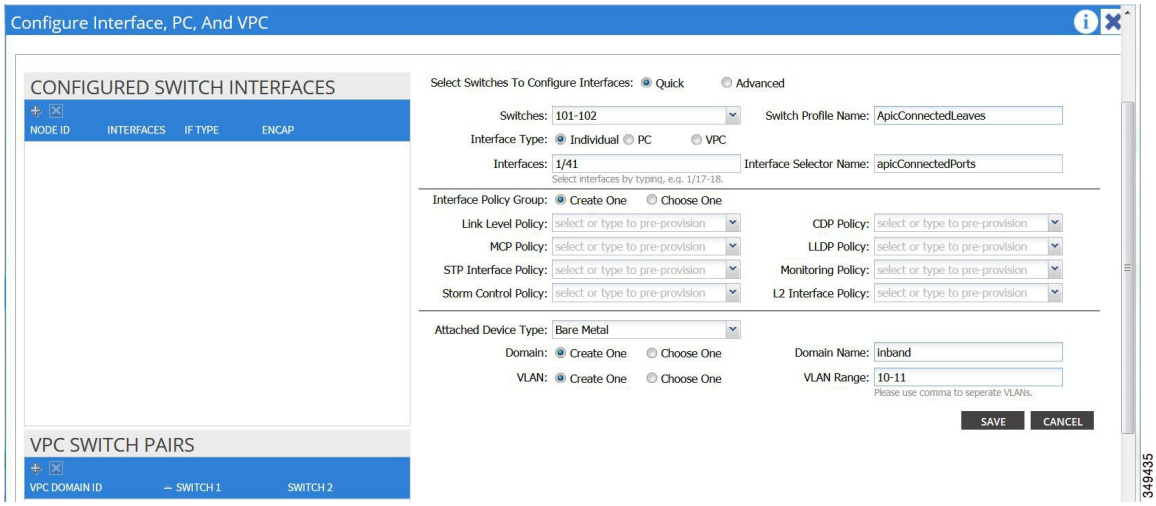
手順の詳細

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ように、次の画像のようなダイアログボックスが表示されます。



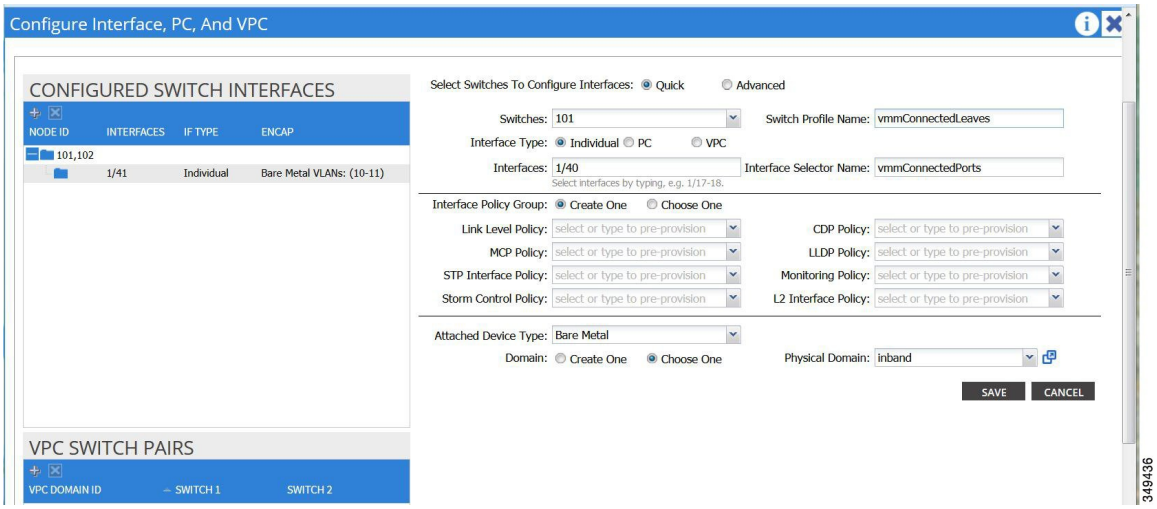
e) [Interface Type] 領域で、[Individual] オプション ボタンが選択されていることを確認します。
f) [Interfaces] フィールドで、APIC が接続されているポートを入力します。
g) [Interface Selector Name] フィールドに、ポート プロファイルの名前（apicConnectedPorts）を入力します。
h) [Interface Policy Group] フィールドで、[Create One] オプション ボタンをクリックします。
i) [Attached Device Type] フィールドで、適切なデバイス タイプを選択してドメイン（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ように、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。

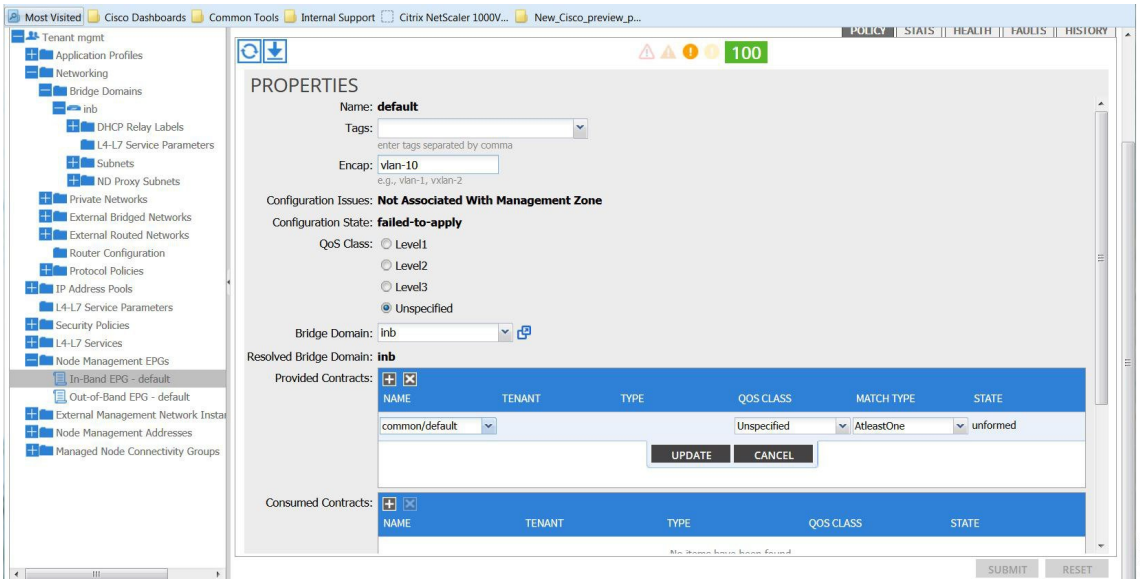
c) [Bridge Domain] ドロップダウン フィールドから、ブリッジ ドメインを選択します。[Submit] をクリックします。

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。

CLI を使用したインバンド管理アクセスの設定

手順の概要

1. 管理トラフィック用の VLAN ネームスペースを作成します。
2. 管理トラフィック用の物理ドメインを作成します。
3. インバンド トラフィック用のリーフ セレクタを作成します。
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。
5. 管理アドレス プールを作成します。
6. ノード管理グループを作成します。

手順の詳細

ステップ 1 管理トラフィック用の VLAN ネームスペースを作成します。

例：

```
admin@apic1:~> cd /aci/fabric/access-policies/pools/vlan/
admin@apic1:vlan> mocreate inband static-allocation
admin@apic1:vlan> moconfig commit
Committing mo 'fabric/access-policies/pools/vlan/inband-static-allocation'

All mos committed successfully.
```

```
admin@apic1:vlan> cd inband-static-allocation/encap-blocks
admin@apic1:encap-blocks> mocreate vlan10 vlan11
admin@apic1:encap-blocks> cd vlan10-vlan11
admin@apic1:vlan10-vlan11> moset name encap
admin@apic1:vlan10-vlan11> moconfig commit
Committing mo 'fabric/access-policies/pools/vlan/inband-static-allocation/encap-blocks/vlan10-vlan11'

All mos committed successfully.
admin@apic1:vlan10-vlan11>
```

ステップ 2 管理トラフィック用の物理ドメインを作成します。

例：

```
admin@apic1:~> cd /aci/fabric/access-policies/physical-and-external-domains/physical-domains/
admin@apic1:physical-domains> mocreate inband
admin@apic1:physical-domains> moconfig commit
Committing mo 'fabric/access-policies/physical-and-external-domains/physical-domains/inband'

All mos committed successfully.
admin@apic1:physical-domains> cd inband
admin@apic1:inband> moset vlan-pools fabric/access-policies/pools/vlan/inband-static-allocation
admin@apic1:inband> moconfig commit
Committing mo 'fabric/access-policies/physical-and-external-domains/physical-domains/inband'

All mos committed successfully.
admin@apic1:inband>
```

ステップ 3 インバンド トラフィック用のリーフ セレクタを作成します。

例：

```
admin@apic1:~> cd /aci/fabric/access-policies/switch-policies/profiles
admin@apic1:profiles> mocreate vmmNodes
admin@apic1:profiles> moconfig commit
Committing mo 'fabric/access-policies/switch-policies/profiles/vmmNodes'

All mos committed successfully.
admin@apic1:profiles> cd vmmNodes
admin@apic1:vmmNodes> mocreate leaf-selector leafS range
admin@apic1:vmmNodes> moconfig commit
Committing mo 'fabric/access-policies/switch-policies/profiles/vmmNodes/leaf-selector-leafS-range'

All mos committed successfully.
admin@apic1:vmmNodes>
admin@apic1:vmmNodes> cd leaf-selector-leafS-range
admin@apic1:leaf-selector-leafS-range> mocreate single0
admin@apic1:leaf-selector-leafS-range> cd single0
admin@apic1:single0> moset to 101
admin@apic1:single0> moset from 101
admin@apic1:single0> moconfig commit
Committing mo 'fabric/access-policies/switch-policies/profiles/vmmNodes/leaf-selector-leafS-range/single0'

All mos committed successfully.
admin@apic1:single0>
admin@apic1:single0> cd ../../associated-interface-selector-profiles
admin@apic1:associated-interface-selector-profiles> mocreate
fabric/access-policies/interface-policies/profiles/interfaces/vmmPorts
admin@apic1:associated-interface-selector-profiles> moconfig commit
Committing mo 'fabric/access-policies/switch-policies/profiles/vmmNodes/associated-interface-selector-profiles/[fabric/access-policies
/interface-policies/profiles/interfaces/vmmPorts]'

All mos committed successfully.
admin@apic1:associated-interface-selector-profiles>
admin@apic1:associated-interface-selector-profiles> cd /aci/fabric/access-policies/interface-policies/profiles/interfaces
admin@apic1:interfaces> mocreate vmmPorts
admin@apic1:interfaces> moconfig commit
Committing mo 'fabric/access-policies/interface-policies/profiles/interfaces/vmmPorts'

All mos committed successfully.
admin@apic1:interfaces> cd vmmPorts
admin@apic1:vmmPorts> mocreate portS range
admin@apic1:vmmPorts> moconfig commit
Committing mo 'fabric/access-policies/interface-policies/profiles/interfaces/vmmPorts/portS-range'

All mos committed successfully.
admin@apic1:vmmPorts>
admin@apic1:vmmPorts> cd portS-range
admin@apic1:portS-range> mocreate block1
admin@apic1:portS-range> cd block1
```

```
admin@apic1:block1> moset from-module 1
admin@apic1:block1> moset to-module 1
admin@apic1:block1> moset from-port 40
admin@apic1:block1> moset to-port 40
admin@apic1:block1> moconfig commit
Committing mo 'fabric/access-policies/interface-policies/profiles/interfaces/vmmPorts/portS-range/block1'

All mos committed successfully.
admin@apic1:block1>
admin@apic1:block1> cd ../
admin@apic1:portS-range> moset policy-group
fabric/access-policies/interface-policies/policy-groups/interface/inband
admin@apic1:portS-range> moconfig commit
Committing mo 'fabric/access-policies/interface-policies/profiles/interfaces/vmmPorts/portS-range'

All mos committed successfully.
admin@apic1:portS-range>
admin@apic1:portS-range> cd /aci/fabric/access-policies/switch-policies/profiles
admin@apic1:profiles> mocreate apicConnectedNodes
admin@apic1:profiles> moconfig commit
Committing mo 'fabric/access-policies/switch-policies/profiles/apicConnectedNodes'

All mos committed successfully.
admin@apic1:profiles> cd apicConnectedNodes
admin@apic1:apicConnectedNodes> mocreate leaf-selector leafS range
admin@apic1:apicConnectedNodes> moconfig commit
Committing mo 'fabric/access-policies/switch-policies/profiles/apicConnectedNodes/leaf-selector-leafS-range'

All mos committed successfully.
admin@apic1:apicConnectedNodes>
admin@apic1:apicConnectedNodes> cd leaf-selector-leafS-range
admin@apic1:leaf-selector-leafS-range> mocreate single0
admin@apic1:leaf-selector-leafS-range> cd single0
admin@apic1:single0> moset to 102
admin@apic1:single0> moset from 101
admin@apic1:single0> moconfig commit
Committing mo 'fabric/access-policies/switch-policies/profiles/apicConnectedNodes/leaf-selector-leafS-range/single0'

All mos committed successfully.
admin@apic1:single0>
admin@apic1:single0> cd ../../associated-interface-selector-profiles
admin@apic1:associated-interface-selector-profiles> mocreate
fabric/access-policies/interface-policies/profiles/interfaces
/apicConnectedPorts
admin@apic1:associated-interface-selector-profiles> moconfig commit
Committing mo 'fabric/access-policies/switch-policies/profiles/apicConnectedNodes/associated-interface-selector-profiles/[fabric/access-policies
/interface-policies/profiles/interfaces/apicConnectedPorts]'

All mos committed successfully.
admin@apic1:associated-interface-selector-profiles>
admin@apic1:associated-interface-selector-profiles> cd /aci/fabric/access-policies/interface-policies/profiles/interfaces
admin@apic1:interfaces> mocreate apicConnectedPorts
admin@apic1:interfaces> moconfig commit
Committing mo 'fabric/access-policies/interface-policies/profiles/interfaces/apicConnectedPorts'

All mos committed successfully.
admin@apic1:interfaces> cd apicConnectedPorts
admin@apic1:apicConnectedPorts> mocreate portS range
admin@apic1:apicConnectedPorts> moconfig commit
Committing mo 'fabric/access-policies/interface-policies/profiles/interfaces/apicConnectedPorts/portS-range'

All mos committed successfully.
admin@apic1:apicConnectedPorts>
admin@apic1:apicConnectedPorts> cd portS-range
admin@apic1:portS-range> mocreate block1
admin@apic1:portS-range> cd block1
admin@apic1:block1> moset from-module 1
admin@apic1:block1> moset to-module 1
admin@apic1:block1> moset from-port 1
admin@apic1:block1> moset to-port 3
admin@apic1:block1> moconfig commit
Committing mo 'fabric/access-policies/interface-policies/profiles/interfaces/apicConnectedPorts/portS-range/block1'

All mos committed successfully.
admin@apic1:block1> cd ../
admin@apic1:portS-range> moset policy-group
fabric/access-policies/interface-policies/policy-groups/interface/inband
admin@apic1:portS-range> moconfig commit
Committing mo 'fabric/access-policies/interface-policies/profiles/interfaces/apicConnectedPorts/portS-range'

All mos committed successfully.
admin@apic1:portS-range>
admin@apic1:portS-range> cd /aci/fabric/access-policies/interface-policies/policy-groups/interface
admin@apic1:interface> mocreate inband
admin@apic1:interface> moconfig commit
Committing mo 'fabric/access-policies/interface-policies/policy-groups/interface/inband'

All mos committed successfully.
admin@apic1:interface> cd inband
```

```
admin@apic1:inband> moset attached-entity-profile
fabric/access-policies/global-policies/attachable-entity-profile/inband
admin@apic1:inband> moconfig commit
Committing mo 'fabric/access-policies/interface-policies/policy-groups/interface/inband'

All mos committed successfully.
admin@apic1:inband>
admin@apic1:inband> cd /aci/fabric/access-policies/global-policies/attachable-entity-profile
admin@apic1:attachable-entity-profile> mocreate inband
admin@apic1:attachable-entity-profile> moconfig commit
Committing mo 'fabric/access-policies/global-policies/attachable-entity-profile/inband'

All mos committed successfully.
admin@apic1:attachable-entity-profile> cd inband/domains-associated-to-interfaces
admin@apic1:domains-associated-to-interfaces> mocreate
fabric/access-policies/physical-and-external-domains/physical-domains/inband
admin@apic1:domains-associated-to-interfaces> moconfig commit
Committing mo 'fabric/access-policies/global-policies/attachable-entity-profile/inband/domains-associated-to-interfaces/[fabric/access-policies
/physical-and-external-domains/physical-domains/inband]'

All mos committed successfully.
admin@apic1:domains-associated-to-interfaces>
```

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：

```
admin@apic1:~> cd /aci/tenants/mgmt/networking/bridge-domains/inb/subnets
admin@apic1:subnets> mocreate 10.13.1.254/24
admin@apic1:subnets> moconfig commit
Committing mo 'tenants/mgmt/networking/bridge-domains/inb/subnets/10.13.1.254:24'

All mos committed successfully.
admin@apic1:subnets>
admin@apic1:subnets> cd /aci/tenants/mgmt/node-management-epgs/default/in-band/default
admin@apic1:default> moset encap vlan-10
admin@apic1:default> moconfig commit
Committing mo 'tenants/mgmt/node-management-epgs/default/in-band/default'

All mos committed successfully.
admin@apic1:default>
admin@apic1:default> cd provided-contracts
admin@apic1:provided-contracts> mocreate default
admin@apic1:provided-contracts> moconfig commit
Committing mo 'tenants/mgmt/node-management-epgs/default/in-band/default/provided-contracts/default'

All mos committed successfully.
admin@apic1:provided-contracts>
```

ステップ 5 管理アドレス プールを作成します。

例：

```
admin@apic1:provided-contracts> cd /aci/tenants/mgmt/node-management-addresses/address-pools
admin@apic1:address-pools> mocreate switchInb
admin@apic1:address-pools> cd switchInb
admin@apic1:switchInb> moset gateway-address 10.13.1.254/24
admin@apic1:switchInb> moconfig commit
Committing mo 'tenants/mgmt/node-management-addresses/address-pools/switchInb'

All mos committed successfully.
admin@apic1:switchInb> cd address-blocks
admin@apic1:address-blocks> mocreate 10.13.1.101 10.13.1.120
admin@apic1:address-blocks> moconfig commit
Committing mo 'tenants/mgmt/node-management-addresses/address-pools/switchInb/address-blocks/10.13.1.101-10.13.1.120'

All mos committed successfully.
admin@apic1:address-blocks>
admin@apic1:address-blocks>
admin@apic1:address-blocks> cd /aci/tenants/mgmt/node-management-addresses/address-pools
admin@apic1:address-pools> mocreate apicInb
admin@apic1:address-pools> cd apicInb
admin@apic1:apicInb> moset gateway-address 10.13.1.254/24
admin@apic1:apicInb> moconfig commit
Committing mo 'tenants/mgmt/node-management-addresses/address-pools/apicInb'

All mos committed successfully.
admin@apic1:apicInb> cd address-blocks
```

```
admin@apic1:address-blocks> mocreate 10.13.1.1 10.13.1.10
admin@apic1:address-blocks> moconfig commit
Committing mo 'tenants/mgmt/node-management-addresses/address-pools/apicInb/address-blocks/10.13.1.1-10.13.1.10'

All mos committed successfully.
admin@apic1:address-blocks>
```

ステップ 6 ノード管理グループを作成します。

例：

```
admin@apic1:~> cd aci/tenants/mgmt/node-management-addresses/
admin@apic1:node-management-addresses> mocreate node-management-address apic
admin@apic1:node-management-addresses> moconfig commit
Committing mo 'tenants/mgmt/node-management-addresses/node-management-address-apic'

All mos committed successfully.
admin@apic1:node-management-addresses> cd node-management-address-apic/node-blocks/
admin@apic1:node-blocks> mocreate all
admin@apic1:node-blocks> cd all
admin@apic1:all> moset from 1
admin@apic1:all> moset to 3
admin@apic1:all> moconfig commit
Committing mo 'tenants/mgmt/node-management-addresses/node-management-address-apic/node-blocks/all'

All mos committed successfully.
admin@apic1:all>
admin@apic1:all> cd ../../
admin@apic1:node-management-address-apic> moset managed-node-connectivity-group
tenants/mgmt/node-management-addresses/connectivity-groups/apic
admin@apic1:node-management-address-apic> moconfig commit
Committing mo 'tenants/mgmt/node-management-addresses/node-management-address-apic'

All mos committed successfully.
admin@apic1:node-management-address-apic>
admin@apic1:node-management-address-apic>
admin@apic1:node-management-address-apic> cd ../
admin@apic1:node-management-addresses> mocreate node-management-address switch
admin@apic1:node-management-addresses> moconfig commit
Committing mo 'tenants/mgmt/node-management-addresses/node-management-addresses/switch'

All mos committed successfully.
admin@apic1:node-management-addresses>
admin@apic1:node-management-addresses> cd node-management-address-switch/node-blocks/
admin@apic1:node-blocks> mocreate all
admin@apic1:node-blocks> cd all
admin@apic1:all> moset from 101
admin@apic1:all> moset to 104
admin@apic1:all> moconfig commit
Committing mo 'tenants/mgmt/node-management-addresses/node-management-address-switch/node-blocks/all'

All mos committed successfully.
admin@apic1:all>
admin@apic1:all> cd ../../
admin@apic1:node-management-address-switch> moset managed-node-connectivity-group
tenants/mgmt/node-management-addresses
/connectivity-groups/switch
admin@apic1:node-management-address-switch> moconfig commit
Committing mo 'tenants/mgmt/node-management-addresses/node-management-address-switch'

All mos committed successfully.
admin@apic1:node-management-address-switch>
admin@apic1:node-management-address-switch>
admin@apic1:node-management-address-switch> cd /aci/tenants/mgmt/node-management-addresses/connectivity-groups/
admin@apic1:connectivity-groups> mocreate aci
admin@apic1:connectivity-groups> moconfig commit
Committing mo '/aci/tenants/mgmt/node-management-addresses/connectivity-groups/aci'

All mos committed successfully.
admin@apic1:connectivity-groups>
admin@apic1:connectivity-groups> cd aci/
admin@apic1:aci> mocreate inb-managed-nodes-zone in-band-zone default
admin@apic1:aci> moconfig commit
Committing mo '/aci/tenants/test/node-management-addresses/connectivity-groups/aci/inb-managed-nodes-zone/default'

All mos committed successfully.
admin@apic1:aci>
admin@apic1:aci> cd inb-managed-nodes-zone/
admin@apic1:inb-managed-nodes-zone> moset in-band-ip-address-pool
tenants/mgmt/node-management-addresses/address-pools/apicInb
admin@apic1:inb-managed-nodes-zone> moset in-band-management-epg
```

```
tenants/mgmt/node-management-epgs/default/in-band/default
admin@apic1:inb-managed-nodes-zone> moconfig commit
Committing mo '/tenants/test/node-management-addresses/connectivity-groups/aci/inb-managed-nodes-zone/in-band-ip-address-pool'
Committing mo '/tenants/test/node-management-addresses/connectivity-groups/aci/inb-managed-nodes-zone/in-band-management-epg'

All mos committed successfully.
admin@apic1:inb-managed-nodes-zone>
admin@apic1:inb-managed-nodes-zone> cd ../../
admin@apic1:connectivity-groups> mocreate switch
admin@apic1:connectivity-groups> moconfig commit
Committing mo '/tenants/test/node-management-addresses/connectivity-groups/switch'

All mos committed successfully.

admin@apic1:connectivity-groups>
admin@apic1:connectivity-groups> cd switch/
admin@apic1:switch> mocreate inb-managed-nodes-zone in-band-zone default
admin@apic1:switch> moconfig commit
Committing mo '/tenants/test/node-management-addresses/connectivity-groups/switch/inb-managed-nodes-zone/default

All mos committed successfully.

admin@apic1:switch> cd inb-managed-nodes-zone/
admin@apic1:inb-managed-nodes-zone> moset in-band-ip-address-pool
tenants/mgmt/node-management-addresses/address-pools/switchInb
admin@apic1:inb-managed-nodes-zone> moset in-band-management-epg
tenants/mgmt/node-management-epgs/default/in-band/default
admin@apic1:inb-managed-nodes-zone> moconfig commit
Committing mo '/tenants/mgmt/node-management-addresses/address-pools/switchInb/in-band-ip-address-pool'
Committing mo '/tenants/mgmt/node-management-epgs/default/in-band/default/in-band-management-epg'

All mos committed successfully.

admin@apic1:inb-managed-nodes-zone>
```

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、KB 記事、「*Configuring Static Management Access in Cisco APIC*」を参照してください。

手順の概要

1. VLAN ネームスペースを作成します。
2. 物理ドメインを作成します。
3. インバンド管理用のセレクタを作成します。
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。
5. アドレス プールを作成します。
6. 管理グループを作成します。

手順の詳細

ステップ 1　VLAN ネームスペースを作成します。

例：

```
POST
https://APIC-IP/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/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/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/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/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/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。

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。
- このタスク例のビデオを視聴するには、ビデオを掲載している Web ページ を参照してください。

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。

手順の概要

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。
2. [Node Management Addresses] を右クリックし、[Create Node Management Addresses] をクリックします。
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。
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。
5. [Navigation] ペインで、[Security Policies] > [Out-of-Band Contracts] を展開します。
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。
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。
8. [Navigation] ペインで、[Node Management EPGs] > [Out-of-Band EPG - default] を展開します。
9. [Work] ペインで、[Provided Out-of-Band Contracts] を展開します。
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契約（oob-default）を選択します。[Update] をクリックし、[Submit] をクリックします。
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。
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。

手順の詳細

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、契約の名前（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契約が作成されます。

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契約（oob-default）を選択します。[Update] をクリックし、[Submit] をクリックします。
契約がノード管理 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、作成した契約（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契約を選択します。

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。

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。

手順の概要

1. アウトオブバンド契約を作成します。
2. アウトオブバンド契約をアウトオブバンド EPG に関連付けます。
3. アウトオブバンド契約を外部管理 EPG に関連付けます。
4. 管理アドレス プールを作成します。
5. ノード管理グループを作成します。

手順の詳細

ステップ 1 アウトオブバンド契約を作成します。

例：

```
admin@apic1:~> cd /aci/tenants/mgmt/security-policies
admin@apic1:security-policies> cd out-of-band-contracts
admin@apic1:out-of-band-contracts> moconfig commit
Committing mo 'tenants/mgmt/security-policies/out-of-band-contracts/oob-default'

All mos committed successfully.
admin@apic1:out-of-band-contracts> cd oob-default
admin@apic1:oob-default> cd subjects
admin@apic1:subjects> mocreate oob-default
admin@apic1:subjects> moconfig commit
Committing mo 'tenants/mgmt/security-policies/out-of-band-contracts/oob-default/subjects/oob-default'

All mos committed successfully.
admin@apic1:subjects> cd oob-default
admin@apic1:oob-default> cd filters
admin@apic1:filters> mocreate default
admin@apic1:filters> moconfig commit
Committing mo
'tenants/mgmt/security-policies/out-of-band-contracts/oob-default/subjects/oob-default/filters/default'

All mos committed successfully.
```

ステップ 2 アウトオブバンド契約をアウトオブバンド EPG に関連付けます。

例：

```
admin@apic1:~> cd /aci/tenants/mgmt/node-management-epgs/default
admin@apic1:default> cd out-of-band
```

```
admin@apic1:out-of-band> cd default
admin@apic1:default> cd provided-out-of-band-contracts
admin@apic1:provided-out-of-band-contracts> mocreate oob-default
admin@apic1:provided-out-of-band-contracts> moconfig commit
Committing mo
'tenants/mgmt/node-management-epgs/default/out-of-band/default/provided-out-of-band-contracts/oob-default'

All mos committed successfully.
```

ステップ 3 アウトオブバンド契約を外部管理 EPG に関連付けます。

例：

```
admin@apic1:~> cd /aci/tenants/mgmt
admin@apic1:mgmt> cd external-network-instance-profiles
admin@apic1:external-network-instance-profiles> cd external-entities-default
admin@apic1:external-entities-default> cd external-management-entity-instances
admin@apic1:external-management-entity-instances> mocreate default
Committing mo
'tenants/mgmt/external-network-instance-profiles/external-entities-default/external-management-entity-instances/default'

All mos committed successfully.
admin@apic1:external-management-entity-instances> cd default
admin@apic1:default> cd consumed-out-of-band-contracts
admin@apic1:consumed-out-of-band-contracts> mocreate oob-default
admin@apic1:consumed-out-of-band-contracts> moconfig commit
Committing mo
'tenants/mgmt/external-network-instance-profiles/external-entities-default/external-management-entity-instances/default
/consumed-out-of-band-contracts/oob-default'

All mos committed successfully.
admin@apic1:consumed-out-of-band-contracts> cd ..
admin@apic1:default> cd subnets
admin@apic1:subnets> mocreate 10.0.0.0/8
admin@apic1:subnets> moconfig commit
Committing mo
'tenants/mgmt/external-network-instance-profiles/external-entities-default/external-management-entity-instances
/default/subnets/10.0.0.0:8'

All mos committed successfully.
```

ステップ 4 管理アドレス プールを作成します。

例：

```
admin@apic1:~> cd /aci/tenants/mgmt
admin@apic1:mgmt> cd node-management-addresses
admin@apic1:node-management-addresses> cd address-pools
admin@apic1:address-pools> mocreate switchOoboobaddr
admin@apic1:address-pools> cd switchOoboobaddr
admin@apic1:switchOoboobaddr> moset gateway-address 172.23.48.1/21
admin@apic1:switchOoboobaddr> moconfig commit
Committing mo 'tenants/mgmt/node-management-addresses/address-pools/switchOoboobaddr'

All mos committed successfully.
admin@apic1:switchOoboobaddr> cd address-blocks
admin@apic1:address-blocks> mocreate 172.23.49.240 172.23.49.244
admin@apic1:address-blocks> moconfig commit
Committing mo
'tenants/mgmt/node-management-addresses/address-pools/switchOoboobaddr/address-blocks/172.23.49.240-172.23.49.244'

All mos committed successfully.
```

ステップ 5 ノード管理グループを作成します。

例：

```
admin@apic1:~> cd /aci/tenants/mgmt
admin@apic1:mgmt> cd node-management-addresses
```

```
admin@apic1:node-management-addresses> cd node-groups
admin@apic1:node-groups> mocreate switchOob
admin@apic1:node-groups> cd switchOob
admin@apic1:switchOob> moset type range
admin@apic1:switchOob> moconfig commit
Committing mo 'tenants/mgmt/node-management-addresses/node-groups/switchOob'

All mos committed successfully.
admin@apic1:switchOob> mocreate connectivity-group uni/infra/funcprof/grp-switchOob
admin@apic1:switchOob> moconfig commit
Committing mo
'tenants/mgmt/node-management-addresses/node-groups/switchOob/connectivity-group-[uni/infra/funcprof/grp-switchOob]'

All mos committed successfully.
admin@apic1:switchOob> cd node-blocks
admin@apic1:node-blocks> mocreate default
admin@apic1:node-blocks> cd default
admin@apic1:default> moset from 101
admin@apic1:default> moset to 103
admin@apic1:default> moconfig commit
Committing mo 'tenants/mgmt/node-management-addresses/node-groups/switchOob/node-blocks/default'

All mos committed successfully.
```

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。

手順の概要

1. アウトオブバンド契約を作成します。
2. アウトオブバンド契約をアウトオブバンド EPG に関連付けます。
3. アウトオブバンド契約を外部管理 EPG に関連付けます。
4. 管理アドレス プールを作成します。
5. ノード管理グループを作成します。

手順の詳細

ステップ 1 アウトオブバンド契約を作成します。

例：

```
POST
https://APIC-IP/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 アウトオブバンド契約をアウトオブバンド EPG に関連付けます。

例：

```
POST
https://APIC-IP/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 アウトオブバンド契約を外部管理 EPG に関連付けます。

例：

```
POST
https://APIC-IP/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/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/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>
```

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。

（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。

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。

オンデマンド テクニカルサポート ファイルの送信

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。
ステップ 5 [Create On-demand TechSupport] 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、テクニカルサポート ファイルのエクスポート ポリシーの名前を入力します。

b) ファイルをリモート宛先ではなくコントローラにエクスポートする場合は、[Export to Controller] を選択します。
c) [Export Destination] ドロップダウン リストから、テクニカルサポート ファイルを受信する宛先ホストのプロファイルを選択します。
目的の宛先のプロファイルが表示されない場合は、[Create Remote Location] を選択してここで定義します。
d) [Data Container] ドロップダウン リストから、[uni/fabric/tscont] を選択します。
e) 目的の送信元デバイス（リーフまたはスパイン）が [Source Nodes] テーブルに表示されない場合は、[+] アイコンをクリックし、デバイスを選択して、[Update] をクリックします。
f) [Source Nodes] テーブルで送信元名をダブルクリックし、ドロップダウン リストの右にある青のアイコンをクリックして、ソース デバイスの [System Information] ウィンドウを開きます。
ソース デバイスの情報を確認するには、タブを使用します。
g) [State] フィールドで、[triggered] オプション ボタンをクリックして、ファイルを送信できるようにします。
h) [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。
i) ポリシー名を右クリックし、[Collect Tech Support] を選択します。
j) [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。

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 ロケーションの作成

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。

ステップ 1 メニュー バーで、[ADMIN] タブをクリックします。

ステップ 2 [IMPORT/EXPORT] を選択します。

ステップ 3 [Import/Export] の下で、[Remote Locations] をクリックします。

[CREATE REMOTE LOCATION] ウィンドウが表示されます。

ステップ 4 [Description] フィールドに、説明を入力します（この手順は任意です）。

ステップ 5 [Host Name (or IP Address)] フィールドに、IP アドレスまたはホスト名を入力します。

ステップ 6 [scp]、[ftp]、または [sftp] のボタンを選択して、プロトコルを指定します。

ステップ 7 [Remote Path] フィールドで、パスを指定します。

ステップ 8 [Username] フィールドに、ユーザ名を入力します。

ステップ 9 [Password] フィールドにパスワードを入力し、[Confirm Password] フィールドで確認します。

ステップ 10 [Management EPG] フィールドでは、インバンド オプションまたはアウトオブバンド オプションを指定することも、空白のままにしておくこともできます。

ステップ 11 [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。

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。

ステップ 1 メニュー バーで、[Admin] タブをクリックします。

ステップ 2 [IMPORT/EXPORT] を選択します。

ステップ 3 [Export Policies] の下で、[Configuration] を選択します。

ステップ 4 [Create Configuration Export Policy] を選択します。
[CREATE CONFIGURATION EXPORT POLICY] ウィンドウが表示されます。

ステップ 5 [Name] フィールドにエクスポート ポリシーの名前を入力します。

ステップ 6 [Description] フィールドに、説明を入力します（この手順は任意です）。

ステップ 7 [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。

ステップ 8 [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）。

ステップ 9 設定全体のバックアップではなく部分バックアップを行う場合は、[Target DN] フィールドに名前を入力します。たとえば、1 つの特定テナントのみをバックアップする場合は、そのテナントの識別名（DN）を入力します。空白のままにすると、すべてがバックアップされます（デフォルト）。

ステップ 10 [Scheduler] フィールドで、事前プロビジョニングを選択または入力します。

ステップ 11 [Export Destination] フィールドで、データのバックアップ先のリモート ロケーションを指定します。

ステップ 12 [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] タブがあり、そこで、実行中、成功、または失敗のどれであるかを確認できます。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

アップを作成した場合、ファイルが作成され、作成したバックアップ ファイルの操作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。

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。

ステップ 1 メニュー バーで、[ADMIN] タブをクリックします。

ステップ 2 [IMPORT/EXPORT] を選択します。

ステップ 3 [Import Policies] の下で、[Configuration] を選択します。

ステップ 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。

ステップ 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。

ステップ 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。
[Replace]、[Merge]、[Best Effort]、[Atomic] などの入力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 7 [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。

ステップ 8 設定が完了したら、[Start Now] をクリックします。

ステップ 9 [Submit] をクリックします。

CLI を使用したエクスポート ポリシーの設定

CLI を使用してエクスポート ポリシーを設定するには、次のように入力します。

```
cd /aci/admin/import-export/export-policies/configuration
admin@trunk13-ifc1:configuration> mocreate myExport
admin@trunk13-ifc1:configuration> cd myExport
admin@trunk13-ifc1:myExport> moset export-destination myServer
admin@trunk13-ifc1:myExport> moconfig commit
Committing mo 'admin/import-export/export-policies/configuration/myExport'

All mos committed successfully.
```

CLI を使用したインポート ポリシーの設定

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。

```
cd /aci/admin/import-export/import-policies
admin@trunk13-ifc1:import-policies> mocreate myImport
admin@trunk13-ifc1:import-policies> cd myImport
admin@trunk13-ifc1:myImport> moset file-name ce_export-2014-07-03T21-59-14.tar.gz
admin@trunk13-ifc1:myImport> moconfig commit
Committing mo 'admin/import-export/import-policies/myImport'

All mos committed successfully
```

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>
```

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

APIC GUI を使用して設定ファイルを暗号化するには、次の手順に従います。

ステップ 1 メニュー バーで、[ADMIN] タブを選択します。

ステップ 2 [ADMIN] タブの下で [AAA] タブを選択します。

ステップ 3 左側のナビゲーション ペインで、[AES Encryption Passphrase and Keys for Config Export (and Import)] を選択します。

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 4 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 5 [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 6 パスフレーズを設定して確認したら、[Enable Encryption] の横にあるチェックボックスをクリックして、AES 暗号化機能をオンまたはオフにします。

（注） このチェックボックスにマークが付いておらず（オフ）暗号化が無効になっている場合、エクスポートされるすべての設定（エクスポート）に、セキュア フィールド（パスワードや証明書など）は含まれていません。このボックスにマークを付けると（オン）、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。

ステップ 7 [ADMIN] タブの下で [IMPORT/EXPORT] を選択します。

ステップ 8 左側のナビゲーション ペインで [Import Policies] を選択します。

ステップ 9 [Import Policies] の下で [Configuration] を選択します。

前に [Enable Encryption] をオンにした場合、左側のナビゲーション ペインの [Configuration] の下に設定インポート ポリシー（またはポリシーのリスト）が表示され、そのプロパティを設定できます。

ステップ 10 [Fail Import if secure fields cannot be decrypted] の横にあるチェックボックスがオンになっている（デフォルトの選択）ことを確認します。

（注） このチェックボックスは、デフォルトで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。このボックスをオフにすると、システムはすべてのフィールドのインポートを試みますが、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しているために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（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）。このボックスをオフにすると、警告メッセージのポップアップ画面が表示されます。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。

ステップ 11 左側のナビゲーション ペインの [Export Policies] タブの下の [Configuration] タブで、設定ファイルをエクスポートするためのプロパティを設定することもできます。

前に説明した設定インポート ポリシーのプロパティの設定と同じ手順に従います。

（注） このセクションではパスフレーズを設定できません。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。

ステップ 12 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	この特定のケースは、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のセキュア フィールドを、ユーザがコピー/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。

CLI を使用した設定ファイルの暗号化

CLI を使用して設定ファイルの暗号化を設定するには、次のようにします。
エディタでオブジェクトを開き、passphrase と strongEncryption:yes を設定します。

```
admin@ifav74-ifc1:exportcryptkey> vi /mit/uni/exportcryptkey/mo

# AES Encryption Passphrase and Keys for Config Export (and Import)


# Configurable Properties:
clearEncryptionKey             : no
descr                          : Object was created during upgrade
name                           :
ownerKey                       :
ownerTag                       :
passphrase                     : abcdefghijklmnopqrstuvwxyz
passphraseKeyDerivationVersion : v1
strongEncryptionEnabled        : yes

Save file and

admin@ifav74-ifc1:exportcryptkey> moconfig commit
Committing mo 'uni/exportcryptkey'

All mos committed successfully.
admin@ifav74-ifc1:exportcryptkey>
```

REST API を使用した設定ファイルの暗号化

REST API を使用して設定ファイルを暗号化するには、次のように入力します。

```
POST
https://<ip-of-apic>/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。

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。

トリガーされると、タイプ **configJob**（その実行を表す）のオブジェクトがタイプ **configJobCont**（名前付けプロパティ値をポリシー DN に設定）のコンテナ オブジェクトに作成されます。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

Remote Path

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]
```

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。

```
ifav101-apic1# configure
ifav101-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
ifav101-apic1(config)# snapshot import
 WORD       Import configuration name
default
rest-user
ifav101-apic1(config)# snapshot import policy-name
ifav101-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
ifav101-apic1(config-import)# file < from "show snapshot files" >
ifav101-apic1(config-import)# no remote path
ifav101-apic1(config-import)#
ifav101-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。[Replace]、[Merge]、[Best Effort]、[Atomic] などの入力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。
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。

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。

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。

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。

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。

アウトオブバンド DNS 接続

（注） テクニカル サポートや Cisco Call Home ホームなどのアプリケーションでは、ホスト名を正しく解決するためにリーフ スイッチでインバンドとアウトオブバンドの DNS 接続が必要です。

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
- 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。
- 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

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。

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、名前を入力して、[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。

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。

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 Trap Destination Group] [Create SNMP Monitoring Destination Group] を選択します。

ステップ 5 [Create SNMP Trap Destination Group] [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。
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。

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) [Include] フィールドで、必要な通知タイプ（イベント、監査ログ、エラー）のチェックボックスをオンにします。
c) [Min Severity] ドロップダウン リストから、通知をトリガーする [Info] 重大度レベルを選択します。
d) [Dest Group] ドロップダウン リストから、通知を送信する既存の通知先を選択するか、または [Create SNMP Trap Destination Group] [Create SNMP Monitoring Destination Group]を選択して新しい通知先を作成します。
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。
e) [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。
- 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。

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。

ステップ 5 [Create SPAN 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、SPAN 宛先グループの名前を入力します。
b) [Create Destinations] テーブルで + アイコンをクリックし、[Create SPAN Destination] ダイアログボックスを開きます。
c) [Name] フィールドに、SPAN 宛先の名前を入力します。
d) [Destination EPG] ドロップダウン リストで、宛先テナント、アプリケーション プロファイル、または複製されたパケットの転送先の EPG を選択または入力します。
e) [Destination IP] フィールドで、複製されたパケットを受信するリモート サーバの IP アドレスを入力します。
f) [Source IP Prefix] フィールドに、ソース パケットの IP サブネットの基本 IP アドレスを入力します。
g) （任意） [Flow ID] フィールドで、SPAN パケットのフロー ID 値を増分または減分します。
h) （任意） [TTL] フィールドで、SPAN トラフィックでのパケットの IP 存続可能時間（TTL）値を増分または減分します。
i) （任意） [MTU] フィールドで、パケットの MTU トランケーション サイズを増分または減分します。
j) （任意） [DSCP] フィールドで、SPAN トラフィックでのパケットの IP DSCP 値を増分または減分します。
k) [OK] をクリックして、SPAN 送信先を保存します。
l) [Submit] をクリックして、SPAN 送信先グループを保存します。

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。

ステップ 7 [Create SPAN Source 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、SPAN 送信元グループの名前を入力します。
b) [Destination Group] ドロップダウン リストから、以前設定した SPAN 送信先グループを選択します。

c) [Create Sources] テーブルで + アイコンをクリックし、[Create ERSPAN Source] ダイアログボックスを開きます。
d) [Name] フィールドに、送信元の名前を入力します。
e) [Direction] フィールドで、送信元に着信するパケット、送信元から発信するパケット、または着信と発信の両方のパケットを複製および転送するかどうかに基づいて、オプション ボタンを選択します。
f) [Source EPG] ドロップダウン リストから、そのパケットが SPAN 送信先に複製および転送される EPG（テナント / アプリケーション プロファイル / EPG によって特定）を選択します。
g) [OK] をクリックして、SPAN 送信元を保存します。
h) [Submit] をクリックして、SPAN 送信元グループを保存します。

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

トレースルート 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。トレースルートでは、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。トレースルートを使用すると、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 traceroute 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。

traceroute 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。

traceroute の注意事項および制約事項

- traceroute 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 traceroute に必要な子オブジェクト（fv:RsCEpToPathEp）がありません。

- traceroute 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 traceroute の実行

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で、次の操作を実行します。

a) [Name] フィールドに traceroute ポリシーの名前を入力します。

b) [Source End Points] テーブルで + アイコンをクリックし、トレースルートの発信元を編集します。

c) [Source MAC] ドロップダウン リストから送信元エンドポイントの MAC アドレスを選択または入力し、[Update] をクリックします。

d) [Destination End Points] テーブルで + アイコンをクリックし、トレースルートの発信先を編集します。

e) [Destination MAC] ドロップダウン リストから、宛先エンドポイントの MAC アドレスを選択または入力し、[Update] をクリックします。

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

g) [Submit] をクリックして、トレースルートを起動します。

ステップ 6 [Navigation] ペインまたは [Traceroute Policies] テーブルで、トレースルート 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。

（注） 見やすくするには、[Name] 列などの複数の列の幅を広げます。