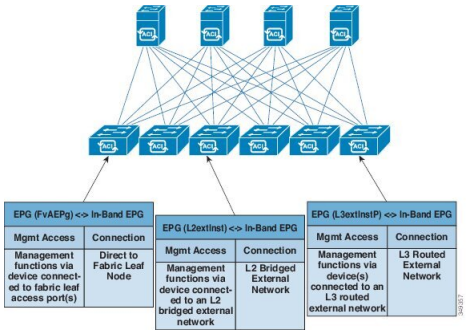
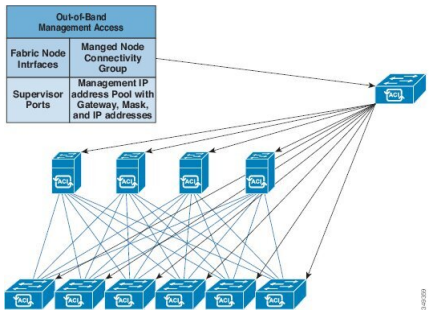
管理

この章は、次の内容で構成されています。

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、『*APIC Basic Configuration Guide*』のインバンド設定向け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、『*APIC Basic Configuration Guide*』のアウトオブバンド設定向け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、『*APIC Basic Configuration Guide*』の以下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
- 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
- REST API を使用したインバンド管理アクセスの設定
- 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
- 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
- REST API を使用したアウトオブバンド管理アクセスの設定

管理アクセスの追加

イン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。5.3(1) リリース以降、Telnet はサポートされていません。

GUI での管理アクセスの追加

Cisco Application Policy Infrastructure Controller（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では、Cisco APIC が Cisco Application Centric Infrastructure（ACI）ファブリックを使用してリーフ スイッチや外部と通信でき、外部管理デバイスがファブリック自体を使用して Cisco APIC またはリーフ スイッチおよびスパイン スイッチと通信できます。

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。

Cisco 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 Cisco 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。

Cisco ACI には、管理テナントおよびインバンド VRF インスタンスのブリッジ ドメインのサブネット設定に基づいて、インバンド管理用のルートをプログラムする機能があります。これらのルートは、ブリッジ ドメインからサブネット設定が削除されると削除されます。

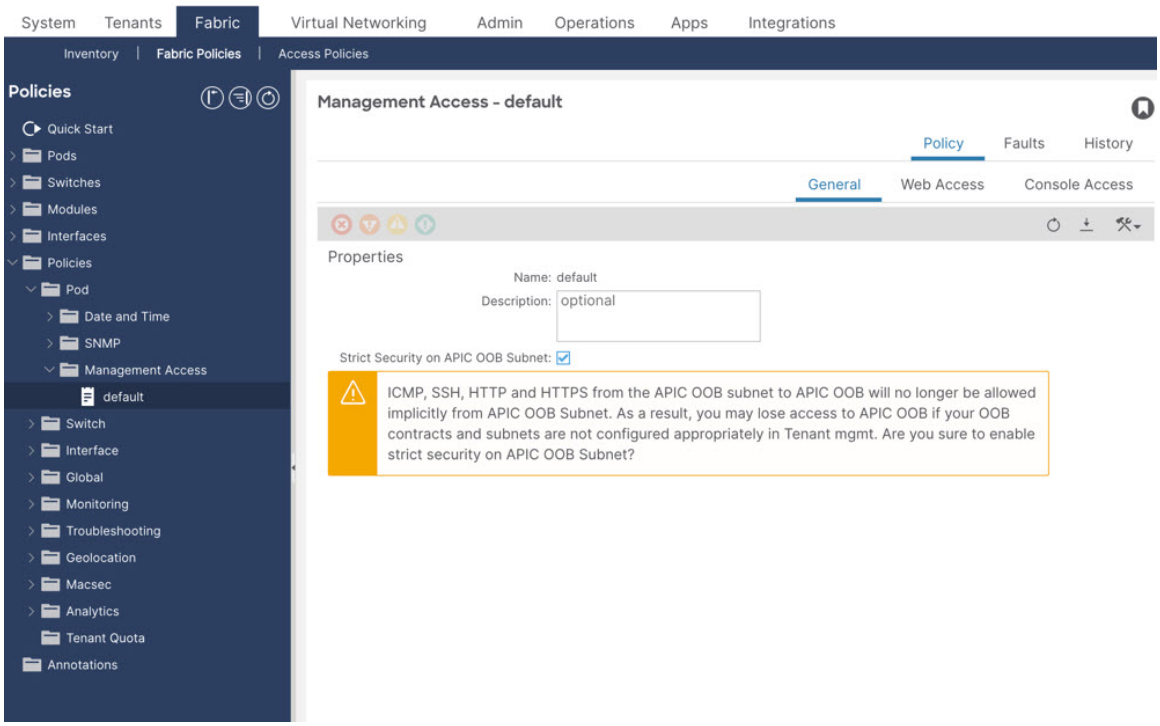
Cisco APIC アウトオブバンド管理接続のリンクは、1 Gbps である必要があります。

OOB 管理 IP を使用した APIC へのアクセスは、コントラクトと許可されたサブネットを構成することで制限できます。ただし、APIC OOB サブネットに属する IP アドレスは、コントラクトとサブネットの構成に関係なく、ICMP、SSH、HTTP、HTTPS、および TCP 4200 を使用した APIC OOB へのアクセスが常に許可されます。このセーフガードは、構成ミスによる APIC アクセスの偶発的な損失を防ぐために導入されています。Cisco APIC リリース 6.1(1) 以降では、APIC GUI の **[ファブリック（Fabric）]** > **[ファブリック ポリシー（Fabric Policies）]** > **[ポリシー（Policies）]** > **[ポッド（Pod）]** > **[管理アクセス（Management Access）]** にあるデフォルトの管理 アクセスを構成する際に **[APIC OOB サブネットでの厳格なセキュリティ（Strict Security on APIC OOB Subnet）]** オプションを有効にすることで、このセーフガードを削除できます。

厳密モードを有効にするとすぐに、[管理アクセス（Management Access）] 画面に警告が表示されます（以下を参照）。厳格モードの有効化に関する同様の警告は、**[外部管理ネットワーク プロファイル（ External Management Network Profile）]** 画面にも表示されます（**[テナント**

（**Tenants**）] > [管理（**mgmt**）] > [ネットワーク インスタンス プロファイル（**External Management Network Instance Profiles**）] の下にあります）。

図 *1:* 厳密セキュリティ モードを有効にした後に表示される警告



IP アドレスによる APIC へのアクセスを許可しないコントラクトとサブネット（外部管理ネットワーク インスタンス プロファイル内）を使用して **[APIC OOB サブネットで厳格なセキュリティ（Strict Security on APIC OOB Subnet）]** を有効にすると、OOB IP アドレスを介した APIC へのアクセスが失われます。APIC OOB サブネットと同じネットワークから APIC にアクセスすることもできません。このような場合は、コンソールにログインし、`acidiag enableoobrecovery` コマンドを使用して、**[APIC OOB サブネットの厳格なセキュリティ（Strict Security on APIC OOB Subnet）]** を無効にします。

（注） ARP 情報をキャッシュする重複する IP アドレスとファイアウォールは、管理ネットワークではサポートされません。これらの条件が存在すると、アップグレード後に Cisco APIC 管理アクセスが完全に失われる可能性があります。

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。

管理アクセスの注意事項および制約事項

- vzAnyは共有サービスのコンシューマとしてサポートされますが、共有サービスのプロバイダとしてはサポートされません。 vzAny 共有サービス コンシューマと vzAny プロバイダはサポートされていません。
- アウトオブバンド管理アクセスを設定する場合、アウトオブバンドコントラクトのロギングオプション（ACL コントラクトおよび許可/拒否ログの有効化と表示）はサポートされません。
- インバンド管理 VRF をリーフ ノードにプッシュするには、リーフ ノードのインバンド管理アドレスを設定する必要があります。
- ゲートウェイ サブネットに [この IP アドレスをプライマリにする（Make this IP address primary）] が選択されていない限り、インバンド管理 VRF のブリッジ ドメイン サブネット IP アドレスをセカンダリ IP アドレスとして割り当てることができます。
- 次のポートはアウトオブバンド コントラクトで拒否できません。
  - プロトコル icmp、レート制限、設定不可
  - tcp dpt：22、レート制限、構成不可
  - tcp dpt：80、デフォルトではリスニング プロセスなし
  - tcp dpt：443、デフォルトの UI/API
  - tcp dpt：4200、Web 経由の SSH アクセス、デフォルトではリッスン プロセスなし

  外部ネットワーク インスタンス プロファイルでサブネットを定義すると、上記のポートリストは、構成された OOB サブネットの送信元に制限されます。

  IPv4 または IPv6 サブネットが外部ネットワーク インスタンス プロファイルで定義されていない場合、対応するアドレス ファミリに対して OOB 契約は有効になりません。

  IPv4 と IPv6 の両方の OOB コントラクトを有効にするには、外部ネットワーク インスタンス プロファイルの下で、少なくとも 1 つの IPv4 サブネットと 1 つの IPv6 サブネットを構成する必要があります。

  リーフ スイッチおよびスパイン スイッチの SNMP の場合、**[ファブリック ポリシー（Fabric Policies）] > [ポッド（Pod）] > [SNMP]** で構成されている**[クライアント エントリ（Client**

Entries）] サブネットは、OOB コントラクトの前に一致します。**[クライアント エントリ（Client Entries）]**の下にサブネットが構成されていない場合は、どの送信元でも SNMP が許可されます。たとえば、UDP **dpt:161** です。

デフォルトでは、リーフ スイッチとスパイン スイッチの管理インターフェイスには IP アドレスが割り当てられていません。ただし、IP アドレスが割り当てられると、帯域外契約で拒否できないポートがいくつかあります。これらは、ACI の組み込み機能に必要です。たとえば、NTP、DHCP、ICMP などです。

外部ネットワーク インスタンス プロファイルで定義されているサブネットは、APIC にのみ適用されます。リーフ スイッチとスパイン スイッチでは、任意の送信元（0.0.0.0/0）が許可されます。

- スパイン スイッチは、インバンド管理 IP アドレスの ARP を解決しません。このため、インバンド管理ネットワーク内のデバイスはスパイン スイッチと通信できません。スパイン スイッチへのアクセスは、レイヤ 3 ネットワーク経由でのみ可能です。
-

ウィザードによるインバンドおよびアウトオブバンド管理アクセスの設定

APIC、リリース 3.1(x) では、管理アクセスの設定を簡略化するためのウィザードが追加されました。このドキュメントに含まれる、管理アクセスを設定する他の方法も引き続き使用できます。

手順

ステップ 1 **In-Band Management Access** を設定するには、次の手順を実行します:

a) メニュー バーで、**Tenants** > **mgmt** をクリックします。
b) **Quick Start** を展開します。
c) **In-Band Management Access** > **Configure In-Band Management Access** > **Start** をクリックします。
d) **Nodes** を管理ネットワークに、**IP addresses** をノードに、通信フィルタを **Connected Devices** に、そして通信フィルタを **Remote Attached Devices** に追加する手順に従います。

ステップ 2 **Out-of-Band Management Access** を設定するには、次の手順を実行します:

a) メニュー バーで、**Tenants** > **mgmt** をクリックします。
b) **Quick Start** を展開します。
c) **Out-of-Band Management Access** > **Configure Out-of-Band Management Access** > **Start** をクリックします。

d) **Nodes** をアウトオブバンド管理ネットワークに、**IP addresses** をノードに、許可されたサブネットを**External Hosts** に追加する手順に従います。そうすると、通信フィルタが **Access** のための通信を決定します。

Cisco APIC 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、**[ファブリック（FABRIC）]** > **[アクセス ポリシー（Access Policies）]** の順に選択します。

ステップ 2 **[Navigation]**ペインで、**[インターフェイス]** 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、Cisco Application Policy Infrastructure Controller (APIC) に接続されるスイッチ 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、新しいプロファイルを作成して VLAN を Cisco 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、Cisco APIC を接続す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。

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) **[インターフェイス（Interfaces）]** フィールドで、Cisco APIC が接続され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。[送信（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。
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、**[テナント（TENANTS）]** > **[管理（mgmt）]** をクリックします。**[ナビゲーション（Navigation）]** ペインで、**[テナント管理（Tenant mgmt）]** > **[ネットワーキング（Networking）]** > **[ブリッジ ドメイン（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 **[ナビゲーション（Navigation）]** ペインで、**[テナント管理（Tenant mgmt）]** > **[ノード管理 EPG（Node Management EPGs）]** を展開します。[Node Management EPGs] を右クリックし、[Create In-Band Management EPG] を選択します。Cisco 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。

ステップ 10 **[ナビゲーション（Navigation）]** ペインで、**[ノード管理アドレス（Node Management Addresses）]** を右クリックし、**[ノード管理アドレスの作成（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 Cisco 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。Cisco 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 **[ナビゲーション（Navigation）]**ペインの**[ノード管理アドレス（Node Management Addresses）]**の下で、Cisco APIC のポリシー名（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）
[システム（System）]>**[システム設定（System Settings）]**>**[APIC接続設定（APIC Connectivity Preferences）]** をクリックして、アウトオブバンド管理アクセスを Cisco APIC サーバのデフォルトの管理接続モードに設定できます。次に、[Connectivity Preferences] ページで [inband] をクリックします。

Cisco APIC 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。

リーフ スイッチとスパイン スイッチ、および Cisco APIC のアウトオブバンド管理アクセス アドレスを設定する必要があります。

始める前に

Cisco Application Policy Infrastructure Controller（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、**[テナント（Tenants）]**>**[管理（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) **アウトオブ バンド ゲートウェイ** フィールドで、外部アウトオブバンド管理ネットワークの IP アドレスとネットワーク マスクを入力します。

f) **[アウトオブバンド IP アドレス]** フィールドに、スイッチに割り当てられる希望の IPv4 または Ipv6 アドレスの範囲を入力します。[Submit] 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。

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、**[コントラクト（Contracts）]** > **[アウトオブバンド コントラクト（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) **[フィルタ]** を展開し、**[名前]** 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 **[ナビゲーション（Navigation）]** ペインで、**[ノード管理 EPG（Node Management EPG）]** > **[アウトオブバンド EPG - デフォルト（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 **[ナビゲーション（Navigation）]** ペインで、**[外部ネットワーク インスタンス プロファイル（External Network Instance Profile）]** を右クリックし、**[外部管理エンティティ インスタンスの作成（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 EPG 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）
[システム（System）]>**[システム設定（System Settings）]**>**[APIC接続設定（APIC Connectivity Preferences）]** をクリックして、アウトオブバンド管理アクセスを Cisco APIC サーバのデフォルトの管理接続モードに設定できます。次に、[Connectivity Preferences] ページで [ooband] をクリックします。

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。コアおよびテクニカル サポート データはサポートされていません。
- エクスポートされるファイルの宛先 IP アドレスは、IPv6 アドレスであってはなりません。
- 5 つを超えるノードからのテクニカル サポートを同時にトリガーしないでください。特に Cisco Application Policy Infrastructure Controller（APIC）にエクスポートする場合、または帯域幅とコンピューティング リソースが不十分な外部サーバにエクスポートする場合は、トリガーを実行しないでください。
- ファブリック内のすべてのノードからテクニカル サポートを定期的に収集するには、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）。
- Cisco APIC の同じノードに対して複数のテクニカル サポート ポリシーをスケジュールしないでください。同じノードで複数のテクニカル サポート ポリシーのインスタンスを同

時に実行すると、Cisco APIC が大量に消費されたり、 CPU サイクルやその他のリソースが切り替えられたりする可能性があります。

- メンテナンス モードになっているノードについては、オンデマンド テクニカル サポート ポリシーではなく、通常のテクニカル サポート ポリシーを使用することをお勧めします。
- メンテナンス モードのノードに対する進行中のテクニカル サポートのステータスは、Cisco APIC GUI の **[管理（Admin）]** > **[テクニカル サポート（Tech Support）]** > ***[policy_name]*** > **[操作（Operational）]** > **[ステータス（Status）]** セクションでは使用できません。テクニカル サポート ポリシーの **[コントローラへのエクスポート（Export to Controller）]** または **[エクスポート先（Export Destination）]** に基づいて、コントローラ（`/data/techsupport`）または宛先サーバを確認し、テクニカル サポートがキャプチャされていることを確認できます。
- Cisco APIC からのテクニカル サポートの収集は、リーフ スイッチ上のコアがビジー状態の場合にはタイムアウトすることがあります。BGP などのルーティング プロセスや HAL などのプラットフォーム プロセスが CPU を占有すると、コアがビジーになる可能性があります。テクニカル サポートの収集がタイムアウトした場合は、CPU 使用率を調べて、CPU 占有が発生しているかどうかを確認します。そのような場合には、リーフ スイッチのテクニカル サポートを直接収集すれば、タイムアウトの問題を回避できます。

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) [送信（Submit）] をクリックします。

GUI を使用したオンデマンド テクニカル サポート 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 **[オンデマンド テクニカル サポート（On-demand Tech Support）]** を右クリックし、**[オンデマンド テクニカル サポートの作成（Create On-demand Tech Support）]** を選択します。

[オンデマンド テクニカル サポートの作成（Create On-demand Tech Support）] ダイアログ ボックスが表示されます。

ステップ 5 **[オンデマンド テクニカル サポートの作成（Create On-demand Tech Support）]** 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、**[オンデマンド テクニカル サポートの作成（Create On-demand Tech Support）]** ダイアログ ボックスのヘルプアイコンをクリックします。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 **[送信（Submit）]** をクリックし、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、**[ナビゲーション（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、**[作業（Work）]** ペインで **[操作（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。

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。定期的に設定のバックアップとエクスポートを行うか、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れば、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) 以降では、AES-256 暗号化を有効にすることにより APIC 設定ファイルのセキュア プロパティを暗号化できます。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 には、AES パスフレーズのハッシュが表示されます。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、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、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。

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、Cisco Application Policy Infrastructure Controller（APIC）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。次の手順を使用して、データのバックアップをトリガーします。

（注） スケジューラ ポリシーで設定されている **[最大同時ノード数（Maximum Concurrent Nodes）]** の値によって、スケジューラ ポリシーで指定された時間に動作する設定エクスポート ポリシーの数が決まります。

たとえば、スケジューラ ポリシーで **[最大同時ノード数（Maximum Concurrent Nodes）]** が **1** に設定され、同じスケジューラ ポリシーを使用する 2 つのエクスポート ポリシーが設定されている場合、1 つのエクスポートポリシーは成功し、もう 1 つは失敗します。ただし、**[最大同時ノード数（Maximum Concurrent Nodes）]** を **2** に設定すると、両方の設定が成功します。

ユーザが読み取り専用権限でログインしている場合でも、[オンデマンド テクニカル サポート（On-Demand Tech Support）] ポリシーまたは [設定のエクスポート（Configuration Export）] ポリシーを右クリックして **[トリガー（Trigger）]** を選択すると、テクニカル サポート データをエクスポートできます。

手順

ステップ 1 メニュー バーで、**[管理（Admin）]** > **[インポート/エクスポート（Import/Export）]** の順に選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ポリシーのインポート（Import Policies）]** を右クリックして、**[設定のインポート ポリシーの作成（Create Configuration Import 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。

フィールドの説明については、ヘルプ（[?]）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 **[設定インポート ポリシーの作成（Create Configuration Import Policy）]** ダイアログのフィールドに値を入力したら、**[送信（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。これは **[設定（Configuration）]** タブで確認できます。バックアップ ファイルが右側の **[設定（Configuration）]** ペインに表示されます。

（注）
Cisco Network Assurance Engine（NAE）を展開して必要な設定を行った場合も、一定間隔でデータを収集するための Cisco APIC のエクスポート ポリシーが Cisco APIC に作成されますCisco NAE エクスポート ポリシーは、アシュアランス コントロール設定に基づく名前で識別できます。Cisco APIC で Cisco NAE エクスポート ポリシーを削除すると、Cisco NAE エクスポート ポリシーが Cisco APIC に再表示されます。Cisco NAE エクスポート ポリシーを削除しないことをお勧めします。

ステップ 5 **[ナビゲーション（Navigation）]** ペインで、**[ポリシーのエクスポート（Export Policies）]** > **[設定（Configuration）]** > ***[policy_name]*** の順に選択します。

ステップ 6 **[作業（Work）]** ペインで、**[操作（Operational）]** > **[ジョブ ステータス（Job Status）]** タブをクリックします。

この画面では、ジョブのエクスポートに関する情報を含むテーブルを表示できます。ジョブのエクスポートをトリガーしなかった場合、テーブルは空になります。**[状態（State）]** カラムは、ジョブのエクスポート ステータスを示します。設定可能な値は次のとおりです。

- `success`：ジョブが成功しました。
- `failed`：ジョブが失敗しました。
- `success-with-warnings`：ジョブは成功しましたが、いくつかの問題がありました。

[詳細（Details）] カラムは、整合性検証が成功したか失敗したかを示します。

バックアップを作成した場合、Cisco APIC は作成されたバックアップファイルの **[操作（Operational）]** ビューに表示されるファイルを作成します。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。

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。

（注）
ファブリックのクリーンリロードを実行し、以前に保存した設定をインポートすると、タイムゾーンはデフォルトでUTC に変更されます。このような状況では、APIC クラスタの設定のインポート後に、タイムゾーンをローカル タイムゾーンにリセットします。

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。

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
  - 失敗（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）
- ユーザー名
- 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` に設定されている場合、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. **[インポート/エクスポート（IMPORT / EXPORT）]** を選択します。
3. **[ポリシーのエクスポート（Export Policies）]** の下で、**[設定（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. **[形式（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. **[今すぐ開始（Start Now）]** の横で、**[いいえ（No）]** または **[はい（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. **[暗号化（Encryption）]** フィールドでは、設定ファイルの暗号化を有効または無効にするオプションがあります。
11. 設定が完了したら、[Start Now] をクリックします。
12. **[送信（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。

有効になっている場合、繰り返しスナップショットは **[管理（Admin）]** > **[インポート/エクスポート（Import/Export）]** > **[ポリシーのエクスポート（Export Policies）]** > **[設定（Configuration）]** > **[defaultAuto]** に保存できます

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、最初にインポート ポリシーを作成します。**[管理（Admin）]** > **[インポート/エクスポート（Import / Export）]**に移動し、**[ポリシーのインポート（Import Policies）]** をクリックします。右クリックし、**[設定のインポート ポリシーの作成]** を選択して、インポート ポリシーの属性を設定します。

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。

繰り返しスナップショットを作成することもできます。

（注） 有効になっている場合、繰り返しスナップショットは**Admin** > **Import/Export** > **Export Policies** > **Configuration** > **defaultAuto** で保存されます。

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 ポリシーを使用すると、2 つのスナップショットの間で行われた変更を元に戻して、以前に保存したスナップショットに対する設定変更を効果的にロールバックすることができます。ポリシーがトリガーされると、次のようにオブジェクトが処理されます。

- 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 アーカイブは直接的にはサポートされていません。ただし、スナップショット マネージャ ポリシー（configSnapshotMgrP）を使用して、リモートで保存されたエクスポートをスナップショットにすることができます。詳細については、スナップショット マネージャ ポリシー （30 ページ）を参照してください。
- configRollbackP ポリシーでは、リモート パス設定は不要です。リモート パスが指定されている場合は無視されます。

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 フィールドには、最初のスナップショット（S1）と次のスナップショット 2（S2）を設定する必要があります。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、スナップショット間の違いが算出されて適用されます。

MO は次のように処理されます。

- S1 には存在するが S2 には存在しない MO：これらの MO は S2 の前に削除されました。ロールバックではこれらの MO が再作成されます。
- S2 には存在するが S1 には存在しない MO：これらの MO は S1 の後に作成されました。ロールバックでは、次の場合にこれらの MO が削除されます。
  - S2 の取得後に MO が変更されていない。
  - S2 の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が異なる MO：S2 の取得後にプロパティが別の値に変更されている場合、プロパティはそのまま残ります。変更されていない場合は、ロールバックによってこれらのプロパティは S1 の値に戻ります。

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

ロールバックは予測が困難なため、ロールバックによる実際の変更が行われないプレビューモード（preview を true に設定）も利用できます。このモードでは算出と diff ファイルの生成のみが行われ、ロールバックを実際に実行した場合の状況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、https://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シビラティ（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シビラティ（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は、『*Cisco APIC Faults, Events, and System Messages Management Guide*』で説明しています。システム ログ メッセージのリストについては『*Cisco ACI System Messages Reference Guide*』を参照してください。

（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 [Format] フィールドで、Syslog メッセージの形式を選択します。

デフォルトは [aci]、または RFC 3164 準拠のメッセージ形式ですが、NX-OS スタイル形式に設定することもできます。

c) 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。

d) 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 リストからシビラティ（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。

e) 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 リストからシビラティ（重大度）の最小値を選択します。

f) [Next] をクリックします。

g) [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
指定した DNS サーバがインバンド接続を介して到達可能に設定されている場合、リモート syslog 宛先のホスト名解決に失敗するリスクがあります。この問題を回避するには、IP アドレスを使用して syslog サーバを設定します。ホスト名を使用する場合は、アウトオブバンド インターフェイス経由で DNS サーバに到達できることを確認します。

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） 最小シビラティ（重大度）、**[シビラティ（重大度）（Severity）]**、**[ポート（Port）]** 番号、および syslog **[ファシリティ（Facility）]**を選択します。

[ファシリティ（Facility）]は、メッセージを生成したプロセスを示すためにオプションで使用できる番号で、受信側でのメッセージの処理方法を決定するために使用できます。

e) 5.2（3）以降のリリースでは、**[トランスポート（Transport）]** フィールドで、メッセージに使用するトランスポート プロトコルを選択します。

- リリース 5.2(4) より前のリリースでは、メッセージに使用するトランスポート プロトコルとして **tcp** または **udp** を選択します。
- 5.2(4) リリース以降では、メッセージに使用するトランスポートプロトコルのオプションとして、**ssl** も選択できるようになりました。この機能を使用すると、（クライアントとして機能している）ACI スイッチが、ロギングにセキュアな接続をサポートする（サーバーとして機能している）リモート Syslog サーバーに対してセキュアな暗号化されたアウトバウンド接続を確立できるようになります。認証と暗号化により、この機能では、セキュリティ保護されていないネットワーク上でもセキュアな通信を実現できます。

  メッセージに使用するトランスポート プロトコルとして **ssl** を選択した場合は、必要な SSL 証明書もアップロードする必要があることに注意してください。**[認証局の作成（Create Certificate Authority）]** ウィンドウに移動して、必要な SSL 証明書をアップロードできます。

  [管理（Admin）] > **[AAA]** > **[セキュリティ（Security）]** > **[公開キー管理（Public Key Management）]** > **[認証局（Certificate Authorities）]**を選択し、その後**[アクション（Actions）]** > **[認証局の作成（Create Certificate Authority）]**を選択します。

トランスポート プロトコルのデフォルト オプションは **udp** です。

f) [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。

g) [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 **[完了（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。

始める前に

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 メッセージのシビラティ（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）

5.2(3) リリース以降、エンドポイント セキュリティ グループ (ESG) は、これらのモードで EPG の代替として使用できます。

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。
- Cisco APIC リリース 3.1(2m) 以降では、ファブリックのライフタイム内のパスで統計情報が生成されなかった場合、そのパスに対するアトミック カウンタは生成されません。また、**[トラフィック マップ（Traffic Map）]**（**[可視化（Visualization）]** タブにあるもので、**[操作（Operations）]** > **[可視化（Visualization）]** を Cisco APIC GUIで選択する）には、すべてのパスではなく、アクティブなパス、つまりファブリックの寿命のいずれかの時点で、トラフィックがあったパスだけが表示されます。
- 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 の送信元と接続先で動作しますが、IPv4 アドレスと IPv6 アドレスを混在させて送信元 IP アドレスと接続先 IP アドレスを構成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に存在する MAC アドレスおよび IP アドレスからのトラフィックと、両者へのトラフィックだけがカウントされます。fvCEp の管理対象オブジェクトで IP アドレス フィールドが空の場合、その MAC アドレスとの間で送受信される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。Cisco 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 管理対象オブジェクト自体にある 1 つの IP アドレスのみがカウントされます。特定の IP アドレスとの送受信に関連したアトミック 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 管理対象オブジェクトを使用します。
- 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。
- エンドポイントが同じ EPG に属している場合、IPv6 ヘッダーを持つレイヤ 2 ブリッジド トラフィックの、それらのエンドポイント間でのアトミック カウンタ統計は報告されません。
- EPG または ESG から L3Out EPG に流れるトラフィックに対してアトミック カウンタが機能するには、すべてのプレフィックスとマッチさせるため、0/0 ではなく 0/1 および 128/1 を使用して L3Out EPG を設定します。
- Cisco APIC のトラフィック マップ モードが「trail」に設定されていて、Cisco APIC が F1545 障害を生成した場合、この障害をクリアできる唯一の方法は、トラフィック マップ モードを「path」に設定することです。トラフィック マップ モードを変更するには、**[操作（Operations）]** > **[可視化（Visualization）]** に移動し、**[設定（Settings）]** をクリックし、[モード（Mode）] の**パス**を選択して、**[送信（Submit）]** をクリックします。これにより、入力と出力の両方でポートごとのトンネル統計が得られます。

  トレール モードでは、トンネル論理インターフェイスの最大スケール インデックスに到達する可能性が高くなります。このモードは、より多くのソフトウェアおよびハードウェア リソースを消費します。論理インターフェイスは、ハードウェア内のトンネルに関連付けられている ID です。

  トレイル モードを指定したトンネル エンドポイント（TEP）間に単一のトンネルがある場合は、より多くのハードウェア リソースも消費されます。たとえば、6 つのファブリック ポートと 1 つのトンネルがある場合、ハードウェアは、トンネルの数にファブリック ポートの数を掛けた数に等しいエントリ数を消費します。

  ソフトウェアの場合、割り当てられた論理インターフェイスの数が 2048 を超えると、ハードウェアにエントリを作成できません。その結果、統計情報を取得できません。アトミック カウンタの場合、この問題は減少または超過として表示されることがあります。

  パス モードには、TEP のエントリだけがあります。vPC の場合、2 つのエントリがインストールされます。したがって、上限に達する可能性は低くなります。

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** ウィンドウで、テナントを展開し、**Policies** を展開し、それから **Troubleshoot** を展開します。

ステップ 4 **Troubleshoot** 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 について

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、Cisco ACI ファブリックを管理しモニタリングする各 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。

5.1(1) リリース以降、SNMPv3 は Secure Hash Algorithm-2（SHA-2）認証タイプをサポートします。

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。

Cisco ACI での SNMP アクセスのサポート

（注） Cisco Application Centric Infrastructure（ACI）でサポートされる MIB の完全なリストについては、 https://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。

Cisco ACI での SNMP 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 Cisco Application Policy Infrastructure Controller（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 Cisco 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 Cisco APIC によってサポートされます。

（注） Cisco 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 Cisco APIC によってサポートされます。
- Cisco APIC IPv6 アドレスを使用した SNMP はサポートされていません。

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

リリース	説明
6.1(2)	APIC の起動中に SNMP デーモンが起動しません。これは、ユーザーが SNMP ポリシーをポッド プロファイル ポリシーにアタッチし、adminSt を「有効」に構成すると開始されます。同様に、ユーザーが adminSt を「無効」に構成するか、ポッド プロファイル ポリシーから SNMP ポリシーを削除すると停止します。この動作は、SNMP トラップデーモンにも適用されます。したがって、SNMP トラップ集約機能は、SNMP ポリシー管理状態に依存します。SNMP トラップ集約を機能させるには、すべての APIC をトラップ転送先として追加します。
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)	Cisco 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。

SNMP トラップ集約機能

SNMP トラップ集約機能を使用すると、ファブリック ノードからの SNMP トラップを Cisco Application Policy Infrastructure Controller（APIC）によって集約でき、ファブリック ノードから受信した SNMP トラップを APIC によって外部宛先に転送できます。

トラップが個々のファブリック ノードからではなく APIC から送信されることが予想される場合は、この機能を使用します。この機能を有効にすると、APIC は SNMP プロキシとして機能します。

考えられる障害を処理するために、クラスタ内のすべての APIC を SNMP トラップ アグリゲータとして設定することを強く推奨します。SNMP ポリシーでは、複数のトラップの宛先を設定できます。トラップの集約と転送を設定するには、次の手順を実行します。

1. スイッチからトラップを受信するように各 APIC コントローラを設定します。次の設定を使用した GUI による SNMP トラップ通知先の設定 （47 ページ） の手順に従います。
   - **[ホスト名/IP（Host Name / IP）]** フィールドで、APIC の IPv4 または IPv6 アドレスを指定します。
   - **[管理 EPG（Management EPG）]** リストから、アウトオブバンドまたはインバンド管理 EPG を選択します。

   クラスタ内の各 APIC をトラップの宛先として設定するには、この手順を繰り返します。
2. 集約トラップを外部サーバに転送するように APIC を設定します。次の設定を使用した GUI による SNMP ポリシーの設定 （45 ページ） の手順に従います。
   - **[トラップ転送サーバ（Trap Forward Servers）]** テーブルで、外部サーバの **IP アドレス**を追加します。

トラップの集約と転送では、転送されるトラップの送信元 IP アドレスは、実際の送信元ノードではなく、アグリゲータのアドレス（この場合は APIC）になります。実際の送信元を特定するには、OID で検索する必要があります。次の例では、アドレス 10.202.0.1 が APIC IP アドレスで、アドレス 10.202.0.201 が元の送信元リーフ スイッチの IP アドレスです。

```
08:53:10.372378 IP
(tos 0x0, ttl 60, id 59067, offset 0, flags [DF], proto UDP (17), length 300)
    10.202.0.1.45419 > 192.168.254.200.162: [udp sum ok]
    { SNMPv2c C="SNMP-ACI" { V2Trap(252) R=609795065
    .1.3.6.1.2.1.1.3.0=25847714 .1.3.6.1.6.3.1.1.4.1.0=.1.3.6.1.4.1.9.9.276.0.1
    .1.3.6.1.2.1.2.2.1.1.436207616=436207616 .1.3.6.1.2.1.2.2.1.7.436207616=2
    .1.3.6.1.2.1.2.2.1.8.436207616=2 .1.3.6.1.2.1.31.1.1.1.1.436207616="eth1/1"
    .1.3.6.1.2.1.2.2.1.3.436207616=6 .1.3.6.1.2.1.2.2.1.2.436207616="eth1/1"
    .1.3.6.1.2.1.31.1.1.1.18.436207616=""
    .1.3.6.1.4.1.9.10.22.1.4.1.1.6="10.202.0.201" } }
```

SNMP トラップ集約機能は、SNMPV2 トラップ集約および転送をサポートする Cisco APIC リリース 3.1(1) で導入されました。Cisco APIC リリース 4.2(6) および 5.1(1)以降では、SNMPv3 トラップの集約および転送がサポートされています。

（注） APIC がデコミッションされた場合、ユーザは廃止された APIC をクリーン再起動する必要があります。SNMP トラップ集約機能はデコミッションされた APIC でアクティブであるため、デコミッションされた APIC がクリーン再起動されない場合、ユーザはトラップ宛先で重複トラップを受信する可能性があります。

SNMP の設定

GUI による SNMP ポリシーの設定

この手順では、Cisco ACI モード スイッチの SNMP ポリシーを構成し、有効にします。

始める前に

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 Cisco APIC アウトオブバンド IP アドレスを構成します。Cisco APIC セットアップ中にアウトオブバンドアドレスを構成した場合は、「mgmt」テナントのアドレスを再度設定しないでください。

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) （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。

d) **[コミュニティ ポリシー（Community Policies）]** テーブルで **[+]** アイコンをクリックし、**[名前（Name）]** を入力して、**[更新（Update）]** をクリックします。

コミュニティポリシー名の最大長は32文字です。名前には、アンダースコア（_）、ハイフン（-）、またはピリオド（。）の文字、数字、および特殊文字のみを使用できます。名前に @ 記号を含めることはできません。

e) **[Trap Forward Servers]** テーブルで、**[+]**アイコンをクリックし、外部サーバの**[IP Address]** を入力し、**[Update]**をクリックします。

ステップ 7 必須: 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 **[送信（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 [送信（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) **[ホスト名/IP（Host Name/IP）]** フィールドに、IPv4 または IPv6 アドレスまたは宛先ホストの完全修飾ドメイン名を入力します。

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 v1 または v2c セキュリティ名の最大長は 32 文字です。名前には、アンダースコア（_）、ハイフン（-）、またはピリオド（。）の文字、数字、および特殊文字のみを使用できます。SNMP v2c の場合、@ 記号も使用できます。

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。

SNMP v3 セキュリティ名の最大長は 32 文字です。名前は大文字または小文字で始まる必要があり、文字、数字、およびアンダースコア（_）、ハイフン（-）、ピリオド（。）、または@記号の特殊文字のみを使用できます。

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) **[完了（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) [送信（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。

テナントまたはスイッチで SPAN を設定できます。スイッチ上で設定する場合、SPAN をファブリック ポリシーまたはアクセス ポリシーとして設定できます。

APIC は、SPAN（ERSPAN）のカプセル化されたリモート拡張をサポートします。

リリース 4.1(1i) 以降、次の機能がサポートされるようになりました。

- 送信元とポートチャネルが同じスイッチ上でローカルである限り、宛先として静的ポートチャネルを使用した、ローカル SPAN に対するサポート。

（注） APIC リリース 4.1(1i) 以降を実行していて、宛先として静的ポート チャネルを設定した後、4.1(1i) より前のリリースにダウングレードすると、これが原因で SPAN セッションが管理者無効状態になります。この機能は、リリース 4.1.(1i) より前には利用できませんでした。機能への影響はありません。

- レイヤ 3 インターフェイス フィルタリングを使用して送信元 SPAN を設定するときに、レイヤ 3 インターフェイスの IP プレフィックスを含める必要がなくなりました。
- 1 つ以上のフィルタ エントリのグループであるフィルタ グループ設定のサポート。フィルタ グループを使用すれば、受信したパケットを SPAN を使用して分析する必要があるかどうかを判断するために使用される一致基準が指定できます。
- ASIC の入力での転送が原因でドロップされたパケットをキャプチャし、事前設定された SPAN 宛先に送信する SPAN-on-drop 機能。SPAN-on-drop 設定には、アクセス ポートを SPAN 送信元として使用するアクセス ドロップ、ファブリック ポートを SPAN 送信元として使用するファブリック ドロップ、およびノード上のすべてのポートを SPAN 送信元として使用するグローバル ドロップの 3 種類があります。SPAN-on-drop は、通常の SPAN を使用し (CLI、GUI、および REST API 経由) とトラブルシューティング SPAN を使用して (CLI および REST API のみを経由) 設定されます。この機能の設定の詳細については、*GUI* を使用した *SPAN* の設定、*NX-OS* スタイル *CLI* を使用した *SPAN* の設定、および *REST API* を使用した *SPAN* の設定を参照してください。

マルチノード SPAN

APIC の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 グループのすべてのメンバーと彼らが接続する場所を追跡するために、適切な範囲にポリシーのスパンを広げることが可能です。メンバーが移動すると、APIC は新しいリーフにポリシーを自動的にプッシュします。たとえば、エンドポイントが新しいリーフ スイッチに VMotion により移動すると、スパンの設定は自動的に調整されます。

ACI ファブリックは、カプセル化リモート SPAN（ERSPAN）形式の次の 2 つの拡張をサポートします。

- アクセスまたはテナント SPAN：VLAN をフィルタとして使用するかどうかにかかわらず、リーフ スイッチのフロント パネル ポートに対して実行されます。リーフ スイッチの Broadcom Trident 2 ASIC は、ERSPAN タイプ 1 形式とはわずかに異なるバージョンをサポートします。上記で参照したドキュメントで定義されている ERSPAN タイプ 1 フォーマットとは、GRE ヘッダーが 4 バイトのみであり、シーケンス フィールドがないという点で異なっています。GREヘッダーは常に次のようにエンコードされます–0x000088be。0x88be は ERSPAN タイプ 2 を示していますが、フィールドの残りの 2 バイトにより、これは 4 バイトの GRE ヘッダーを持つ ERSPAN タイプ 1 パケットとして識別されます。
- ファブリック SPAN：リーフ スイッチの Northstar ASIC により、またはスパイン スイッチの Alpine ASIC により実行されます。これらの ASIC は ERSPAN タイプ 2 および 3 フォー

マットをサポートしていますが、ACI ファブリックは現在、ファブリック SPAN の ERSPAN タイプ 2 のみをサポートしています。これについては、上記のベースライン ドキュメントに記載されています。

ERSPAN ヘッダーの説明については、次の URL にある IETF インターネット ドラフトを参照してください。https://tools.ietf.org/html/draft-foschiano-erspan-00

SPAN の注意事項と制約事項

（注） 多くのガイドラインと制約事項は、スイッチが第 1 世代スイッチか第 2 世代スイッチかによって異なります。スイッチの生成は次のように定義されます。

- 第 1 世代スイッチは、スイッチ名の末尾に「EX」、「FX」、「FX2」などのサフィックスがないことで識別されます（N9K-9312TX など）。
- 第 2 世代スイッチは、スイッチ名の末尾に「EX」、「FX」、「FX2」などのサフィックスが付いています。

- サポートされる SPAN のタイプはさまざまです。
  - 第 1 世代のスイッチの場合、テナントおよびアクセス SPAN は、カプセル化された SPAN（ERSPAN）タイプ I を使用します（Cisco Application Policy Infrastructure Controller（APIC）GUI のバージョン 1 オプション）。
  - 第 2 世代スイッチの場合、テナントおよびアクセス SPAN は、カプセル化された SPAN（ERSPAN）タイプ II（Cisco APIC GUI のバージョン 2 オプション）を使用します。
  - ファブリック SPAN は ERSPAN タイプ II を使用します。
- リリース 5.2(3) 以降、ERSPAN は IPv6 接続先をサポートしています。
- 6.0(3) リリースは、次の SPAN 制限がある Cisco N9K-C9808 スイッチをサポートします。
  - 出力（トランジット（Tx））SPAN はサポートされていません。
  - ドロップ時の SPAN はサポートされていません。
  - 複数のセッションで同じ SPAN 送信元を使用することはできません。
  - SPAN は、最大 343 バイトの MTU をサポートします。
- uSeg EPG または ESG は、SPAN 送信元 EPG として使用できません。これは、SPAN 送信元フィルタが VLAN ID に基づいているためです。したがって、エンドポイントが uSeg EPG または ESG に分類されている場合でも、その VLAN が SPAN 送信元 EPG の VLAN である場合、エンドポイントからのトラフィックはミラーリングされます。
- ERSPAN セッションを構成するときに、SPAN ソースに GOLF VRF インスタンス内のスパイン スイッチからの宛先とインターフェイスが含まれている場合、L3Out プレフィックス

が間違った BGP ネクストホップで GOLF ルータに送信され、GOLF からその L3Out への接続が切断されます。

- 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。
- FEX インターフェイスのローカル SPAN では、FEX インターフェイスは SPAN 送信元としてのみ使用でき、SPAN 宛先としては使用できません。
  - 第 1 世代スイッチでは、レイヤ 3 スイッチド トラフィックに対して Tx SPAN は機能しません。
  - 第 2 世代のスイッチでは、トラフィックがレイヤ 2 またはレイヤ 3 のどちらでスイッチングされているかにかかわらず、Tx SPAN は機能しません。

Rx SPAN に制限はありません。

FEX ファブリック ポートチャネル（NIF）の SPAN の場合、メンバー インターフェイスは第 1 世代リーフ スイッチの SPAN 送信元インターフェイスとしてサポートされます。

（注） 第 2 世代スイッチで FEX ファブリック ポートチャネル（NIF）メンバー インターフェイスを SPAN 送信元インターフェイスとして設定することもできますが、これは Cisco APIC リリース 4.1 より前のリリースではサポートされていません。

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。

- ERSPAN 宛先 IP アドレスは、エンドポイントとしてファブリックで学習する必要があります。

  APIC リリース 6.1(2) 以降、ERSPAN 宛先 IP アドレスは、L3Out（ERSPAN over L3Out）から学習され、到達可能なアドレスにすることもできます。
- SPAN は IPv6 トラフィックをサポートします。
- ポート チャネルまたは vPC の個別ポート メンバーは送信元として設定されます。ポート チャネル、vPC、または vPC コンポーネントを SPAN セッションの送信元として使用します。
- 宛先 EPG が削除されるか使用できない場合、ERSPAN 送信元グループで障害は発生しません。
- SPAN フィルタは、第 2 世代のリーフ スイッチでのみサポートされます。

  アクセス SPAN 送信元は、特定の時点で次のいずれかのフィルタのみをサポートします。
  - EPG
  - 外部ルーティング（L3Out）

- L3Out フィルタを使用してアクセス SPAN 送信元を展開する場合は、L3Out が一致するインターフェイスにも展開されていることを確認します。
  - L3Out がポートに展開されている場合、SPAN 送信元は同じポートに展開する必要があります。
  - L3Out が PC に展開されている場合、SPAN 送信元は同じ PC に展開する必要があります。
  - L3Out が vPC に展開されている場合、SPAN 送信元は同じ vPC に展開する必要があります。
- L3Out ルーテッド インターフェイスおよびルーテッド サブインターフェイスはポートまたは PC に導入できますが、L3Out SVI はポート、PC、または vPC に導入できます。L3Out フィルタを使用する SPAN 送信元は、それに応じて展開する必要があります。
- L3Out フィルタは、ファブリック SPAN またはテナント SPAN セッションではサポートされません。
- EPG ブリッジ ドメインの [L3 設定（L3 Configuration）] タブで正しい L3Out を選択する必要があります。そうしないと、基本的な L3Out のパケット フローが機能しません。
- カプセル化値は、ルーテッドサブインターフェイスおよびSVIには必須ですが、ルーテッドインターフェイスには適用されません。L3Outサブインターフェイスまたは SVI カプセル化値は、EPG カプセル化値とは異なる必要があります。

  SPAN セッション内で EPG フィルタが有効になっている場合、中継、つまり tx 方向のインターフェイスから送信される ARP パケットはスパンされません。
- 次の場合、SPAN フィルタはサポートされません。
  - ファブリック ポート
  - ファブリックおよびテナント SPAN セッション
  - スパイン スイッチ
- 公式にサポートされているよりも多くの L4 ポート範囲を追加しようとしても、L4 ポート範囲フィルタ エントリは追加されません。
- SPAN 送信元グループ レベルまたは個々の SPAN 送信元レベルで、サポートされているフィルタ エントリより多くのエントリを関連付けようとすると、SPAN セッションは起動しません。
- 公式にサポートされているよりも多くのフィルタ エントリを追加または削除すると、削除されたフィルタ エントリは TCAM に残ります。
- アクティブな SPAN セッションの最大数や、SPAN フィルタ制限など、SPAN 関連の制限については、『*Verified Scalability Guide for Cisco ACI*』ドキュメントを参照してください。
- SPAN-on-drop 機能では、次の注意事項と制限事項が適用されます。
  - SPAN-on-drop 機能は、第 2 世代リーフ スイッチでサポートされます。

- SPAN-on-drop 機能は、LUX ブロック内の転送ドロップがあるパケットのみをキャプチャします。これは、入力での転送ドロップ パケットをキャプチャします。SPAN-on-drop 機能は、BMX（バッファ）ドロップおよび RWX（出力）ドロップをキャプチャできません。
- トラブルシューティング CLI を使用して SPAN-on-drop と Cisco APICを有効にして宛先として SPAN セッションを作成する場合、100 MBの データがキャプチャされるとセッションは無効になります。
- モジュラ シャーシでは、SPAN-on-drop 機能はライン カードでドロップされたパケットに対してのみ機能します。ファブリック カードでドロップされたパケットはスパンされません。
- SPAN-on-drop ACL と他の SPAN ACL はマージされません。SPAN-on-drop セッションが ACL ベースの SPAN とともにインターフェイスで設定されている場合、そのインターフェイスでドロップされたパケットは SPAN-on-drop セッションにのみ送信されます。
- SPAN on drop と SPAN ACL を同じセッションで設定することはできません。
- アクセスまたはファブリック ポート ドロップ セッションとグローバル ドロップ セッションが設定されている場合、アクセスまたはファブリック ポート ドロップ セッションがグローバル ドロップ セッションよりも優先されます。
- TCAM でサポートされるフィルタ エントリの数=（M * S1 * 1 + N * S2 * 2）+（S3 * 2）。これは、rx SPAN または tx SPAN に個別に適用されます。現在この式に従うと、tx または rx SPAN でサポートされる最大フィルタ エントリは各方向で 480 です（また、フィルタ グループ アソシエーション（S3 = 0 を意味する）なしで、16 個のポート範囲を含む他の送信元が設定されていない場合））。フィルタ エントリの数が最大許容数を超えると、障害が発生します。フィルタエントリでレイヤ4ポート範囲を指定できることに注意してください。ただし、16個のレイヤ4ポートが単一のフィルタ エントリとしてハードウェアにプログラムされます。

（注）
- M = IPv4 フィルタの数
- S1 = IPv4 フィルタを使用した送信元の数
- N = IPv6 フィルタの数
- S2 = IPv6 フィルタを使用した送信元の数
- S3 =フィルタ グループが関連付けられていない送信元の数

- PC または vPC の LACP ポリシーで MAC ピニングを設定すると、PC メンバー ポートは LACP 個別ポートモードになり、PC は動作しません。したがって、このような PC での SPAN 送信元設定は失敗し、「No operating src / dst」障害が生成されます。MAC ピニング モードが設定されている場合、SPAN は個々のポートでのみ設定できます。

- Cisco Application Centric Infrastructure（ACI）リーフ スイッチで受信されたパケットは、スパンインターフェイスが入力インターフェイスと出力インターフェイスの両方で設定されている場合でも、一度だけスパンされます。
- ルーテッド外部 SPAN 送信元フィルタを使用すると、Tx 方向のユニキャストのみが表示されます。Rx 方向では、ユニキャスト、ブロードキャスト、およびマルチキャストを確認できます。
- L3Out フィルタは、送信マルチキャスト SPAN ではサポートされません。L3Out は、入力 ACL フィルタでは sclass / dclass の組み合わせとして表されるため、ユニキャスト トラフィックのみを照合できます。送信マルチキャスト トラフィックは、ポートおよびポート チャネルでのみスパンできます。
- ポート チャネル インターフェイスを SPAN 宛先として使用できるのは、-EX 以降のスイッチだけです。
- SPAN フィルタ（5 タプル フィルタ）が適用されている場合、同じ送信元インターフェイスで複数の SPAN セッションを設定することはできません。

  リーフ スイッチのローカル SPAN 宛先ポートは、着信トラフィックを予期しません。レイヤ 2 インターフェイス ポリシーを設定し、**VLAN 範囲**プロパティを**グローバル範囲**ではなく**ポート ローカル範囲**に設定することで、スイッチが着信 SPAN 宛先ポート トラフィックをドロップするようにできます。このポリシーを SPAN 宛先ポートに適用します。レイヤ2インターフェイスポリシーを設定するには、GUI で次の場所に移動します。**[ファブリック（Fabric）]**>**[アクセス ポリシー（Access Policies）]**>**[ポリシー（Policies）]**>**[インターフェイス（Interface）]** > **[L2 インターフェイス（L2 Interface）]**

  特定のパケットに SPAN を設定すると、SPAN はそのパケットに対して 1 回だけサポートされます。最初の SSN の Rx の SPAN によってトラフィックが選択された場合、2 番目の SSN の Tx の SPAN によってトラフィックが再度選択されることはありません。したがって、SPAN セッションの入力ポートと出力ポートが単一のスイッチ上にある場合、SPAN セッションのキャプチャは一方向のみです。SPAN セッションは双方向トラフィックを表示できません。
- フィルタ グループに設定された SPAN ACL フィルタは、アクセス インターフェイスから出力されるブロードキャスト、不明ユニキャスト、およびマルチキャスト（BUM）トラフィックをフィルタリングしません。出力方向の SPAN ACL は、ユニキャスト IPv4 または IPv6 トラフィックに対してのみ機能します。

  SPAN 宛先をローカル ポートとして設定する場合、EPG はそのインターフェイスに展開できません。

  リーフ スイッチでは、VRF フィルタを持つ SPAN 送信元は、VRF インスタンスの下のすべての通常のブリッジ ドメインとすべてのレイヤ 3 SVI にマッチします。

  スパイン スイッチでは、VRF を持つ SPAN 送信元は、設定された VRF VNID トラフィックのみにマッチします。また、ブリッジ ドメイン フィルタは、ブリッジ ドメイン VNID トラフィックのみにマッチします。

- 独自の SPAN 拡張フィルタ エントリを作成する場合、拡張フィルタ エントリの管理対象オブジェクトを識別するために、**__UI__AUTO__CONFIG__DEFAULT__EXTENDED__MO** をオブジェクト名として使用することはできません。
- 同じ速度の SPAN 接続先インターフェイスを使用します。SPAN セッションによってモニターされるトラフィックは、接続先ポートがオーバーサブスクライブされていないが、他の SPAN 接続先ポートの 1 つがオーバーサブスクライブされている場合でも、SPAN バッファのドロップが原因でトラフィック損失が発生する可能性があります。SPAN トラフィック レートは、接続先インターフェイスの速度が異なる場合、およびそれらの 1 つがオーバーサブスクライブされている場合、最も遅い SPAN 接続先インターフェイス速度に制限されます。
- 構成されているどの送信元インターフェイスよりも高い SPAN 接続先インターフェイス速度を使用し、マイクロバーストに十分な余裕がある速度を選択します。クラウドスケール ASIC は、SPAN クラスのマイクロバースト モニタリング オプションを提供しません。
- SPAN 宛先グループ機能では、次の注意事項と制限事項が適用されます。
  - [ERSPAN over L3Out]：宛先が Infra L3Out の背後にある場合、サポートされません。
  - [ERSPAN over L3Out]：スパン送信元がスパイン ノードのファブリック ポートである場合、サポートされません。
  - インフラ SR-MPLS L3out を介した ERSPAN はサポートされていません。
  - 宛先がリモート リーフ アップリンク ファブリック ポートのユーザー テナント L3out を介して到達可能な場合、リモート リーフの L3out を介した ERSPAN はサポートされません。

GUI を使用した SPAN の設定

Cisco APIC GUI を使用したテナント SPAN セッションの設定

SPAN は、スイッチまたはテナントで設定できます。このセクションでは、Cisco APIC GUI を使用して、複製された送信元パケットをリモート トラフィック アナライザに転送するようにテナントの SPAN ポリシーを設定する方法について説明します。設定手順では、1 つ以上の GUI ダイアログ ボックスのフィールドに値を入力する必要があります。フィールドを理解し、有効な値を決定するには、ダイアログ ボックスの右上隅にあるヘルプアイコン（**?**）をクリックしてヘルプ ファイルを表示します。

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 **[ナビゲーション（Navigation）]** ペインでテナントを展開し、**[ポリシー（Policies）]** > **[トラブルシューティング（Troubleshooting）]** > を展開して、**[SPAN]** を展開します。

[SPAN] に表示される 2 つのノード：**[SPAN 宛先グループ（SPAN Destination Groups）]** と **[SPAN 送信元グループ（SPAN Source Groups）]**。

ステップ 4 **[ナビゲーション（Navigation）]**の下で **[SPAN 送信元グループ（SPAN Source Groups）]** を右クリックし、**[SPAN 送信元グループの作成（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 5 **[SPAN送信元グループの作成（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ます。

ステップ 6 **[送信元の作成（Create Sources）]** テーブルを展開し、**[SPAN 送信元の作成]** ダイアログ ボックスを開きます。

ステップ 7 **[SPAN 送信元の作成（Create SPAN Source）]** 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。

ステップ 8 SPAN送信元の作成が完了したら、**[OK]** をクリックします。

[SPAN 送信元グループの作成（Create VRF）] ダイアログ ボックスに戻ります。

ステップ 9 **[リモート場所の作成（Create Remote Location）]**ダイアログのフィールドに値を入力したら、**[送信（Submit）]** をクリックします。

次のタスク

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。

APIC GUI を使用した SPAN フィルタ グループの設定

手順

ステップ 1 メニュー バーで **[ファブリック（Fabric）]** をクリックし、サブメニュー バーで **[アクセス ポリシー（ Access Policies）]**をクリックします。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ポリシー（Policies）]** > **[トラブルシューティング（Troubleshooting）]** を展開し、**[SPAN]** を展開します

ステップ 3 **[SPAN]** の下で **[SPAN フィルタ グループ（SPAN Filter Groups）]** を右クリックし、**[SPAN フィルタ グループの作成（Create SPAN Filter Group）]** を選択します。
[フィルタ グループの作成（Create Filter Group）] ダイアログボックスが表示されます。

ステップ 4 SPAN フィルタ グループの名前を入力します。**[フィルタ エントリ（Filter Entries）]** テーブルで、**[+]** をクリックし、次のフィールドに値を入力します。

- **[送信元 IP プレフィックス（Source IP Prefix）]**：*IP* アドレス/マスクの形式で送信元 IP アドレスを入力します。IPv4 アドレスおよび IPv6 アドレスのどちらもサポートされていま

す。**0.0.0.0** の値は、このフィールドで**任意の** IPv4 アドレス エントリを指定するために、**::** の値は、**任意の** IPv6 アドレスエントリを指定するために使用します。

- **[最初の送信元ポート（First Source Port）]** 最初の送信元レイヤー 4 ポートを入力します。このフィールドは、**[最後の送信元ポート（Last Source Port）]** フィールドとともに、送信元ポートをフィルタリングするためのポート範囲を指定します。値**0** は、このフィールドで**任意の**エントリを指定するために使用します。
- **[最後の送信元ポート（Last Source Port）]** 最後の送信元レイヤー 4 ポートを入力します。このフィールドは、**[最初の送信元ポート（First Source Port）]** フィールドとともに、送信元ポートをフィルタリングするためのポート範囲を指定します。値**0** は、このフィールドで**任意の**エントリを指定するために使用します。
- **[宛先 IP プレフィックス（Destination IP Prefix）]** : *IP* アドレス/マスクの形式で宛先 IP アドレスを入力します。IPv4 アドレスおよび IPv6 アドレスのどちらもサポートされています。**0.0.0.0** の値は、このフィールドで**任意の** IPv4 アドレス エントリを指定するために、**::** の値は、**任意の** IPv6 アドレスエントリを指定するために使用します。
- **[最初の宛先ポート（First Destination Port）]** : 最初の宛先レイヤー 4 ポートを入力します。このフィールドは、**[最後の宛先ポート（Last Destination Port）]** フィールドとともに、宛先ポートをフィルタリングするためのポート範囲を指定します。値**0** は、このフィールドで**任意の**エントリを指定するために使用します。
- **[最後の宛先ポート（Last Destination Port）]** : 最後の宛先レイヤー 4 ポートを入力します。このフィールドは、**[最初の宛先ポート（First Destination Port）]** フィールドとともに、宛先ポートをフィルタリングするためのポート範囲を指定します。値**0** は、このフィールドで**任意の**エントリを指定するために使用します。
- **[IP プロトコル（IP Protocol）]** : IP プロトコルを入力します。値 **0** は、このフィールドで**任意の**エントリを指定するために使用します。
- **[拡張フィルタ エントリ（Extended Filter Entries）]** テーブルで、**[+]** をクリックし、次のフィールドに値を入力します。
  - **[名前（Name）]:** 拡張フィルタ エントリの名前を入力します。
  - **[最初の DSCP（DSCP From）]** : DSCP 値を入力します。このフィールドは、**[最後の DSCP（DSCP To）]** フィールドとともに、DSCP 値をフィルタリングする範囲を指定します。
  - **[最後ののDSCP（DSCP To）]** : DSCP 値を入力します。このフィールドは、**[最初の DSCP（DSCP From）]** フィールドとともに、DSCP 値をフィルタリングする範囲を指定します。
  - **[最初の Dot1P（Dot1P From）]** : Dot1P 値を入力します。このフィールドは、**[最後の Dot1P（Dot1P To）]** フィールドとともに、Dot1P 値をフィルタリングする範囲を指定します。

- **[最後の Dot1P（Dot1P To）]**：Dot1P 値を入力します。このフィールドは、**[最初の Dot1P（Dot1P From）]** フィールドとともに、Dot1P 値をフィルタリングする範囲を指定します。

  送信元ポートと宛先ポートの範囲、または DSCP と Dot1P の範囲の値を指定できます。送信元ポートと宛先ポートの範囲、および DSCP と Dot1P の範囲の両方を指定すると、障害が表示されます。

  DSCP または Dot1P は、出力方向ではサポートされていません。方向として **[両方（Both）]** を選択した場合、DSCP または Dot1P のいずれかが入力方向のみでサポートされ、出力方向ではサポートされません。

- **[TCP フラグ（TCP Flags）]** ドロップダウンリストで、**TCPフラグ**を選択します。

  TCP フラグを設定できるのは、フィルタ グループのドロップダウン リストで **[未指定（Unspecified）]** または **[TCP]** を **[IP プロトコル（IP Protocol）]** として選択した場合だけです。

- **[パケット タイプ（Packet Type）]**：パケット タイプを選択します。**[ルート/スイッチ（Routed/Switched）]**、**[ルート（Routed）]**、または **[スイッチのみ（Switched Only）]** のいずれかを選択します。

ステップ 5 このフォームの各フィールドに適切な値を入力したら、**[更新（Update）]** をクリックし、**[送信（Submit）]** をクリックします。

APIC GUI を使用したアクセス SPAN ポリシーの設定

この手順では、Cisco APIC GUI を使用してアクセス SPAN ポリシーを設定します。設定手順では、1 つ以上の GUI ダイアログ ボックスのフィールドに値を入力する必要があります。

手順

ステップ 1 メニューバーで、**[ファブリック（Fabric）]** > **[アクセス ポリシー（Access Policies）]** をクリックします。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ポリシー（Policies）]** > **[トラブルシューティング（Troubleshooting）]** > **[SPAN]** を展開します。

[SPAN] の下には、**[SPAN 送信元グループ（SPAN Source Groups）]**, **[SPAN フィルタ グループ（SPAN Filter Groups）]**、および **[SPAN 宛先グループ（SPAN Destination Groups）]** の 3 つのノードが表示されます。

ステップ 3 **[SPAN 送信元グループ（SPAN Source Groups）]** を右クリックし、**[SPAN 送信元グループの作成（Create SPAN Source Groups）]** 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 4 **[SPAN 送信元グループの作成（Create SPAN Source Group）]** 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。

ステップ 5 **[送信元の作成（Create Sources）]** テーブルを展開し、**[SPAN 送信元の作成（Create SPAN Source）]** ダイアログ ボックスを開いて、必須のフィールドに適切な値を入力します。

ステップ 6 [Create SPAN Source] ダイアログ ボックスで、[Add Source Access Paths] を展開して、ソース パスを指定します。

[送信元をパスに関連付ける（Associate Source to Path）] ダイアログ ボックスが表示されます。

ステップ 7 **[送信元をパスに関連付ける（Associate Source to Path）]** 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。

ステップ 8 送信元とパスの関連付けが完了したら、**[OK]** をクリックします。

[SPAN 送信元の作成（Create SPAN Source）] ダイアログ ボックスに戻ります。

ステップ 9 SPAN 送信元の作成が完了したら、**[OK]** をクリックします。

[SPAN 送信元グループの作成（Create VRF）] ダイアログ ボックスに戻ります。

ステップ 10 SPAN 送信元グループの設定が完了したら、**[送信（Submit）]** をクリックします。

次のタスク

SPAN 宛先のトラフィック アナライザを使用して、SPAN 送信元からのデータ 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。

Cisco APIC GUI を使用したファブリック SPAN ポリシーの設定

このセクションでは、Cisco APIC GUI を使用してファブリック SPAN ポリシーを作成する方法について説明します。設定手順では、1 つ以上の GUI ダイアログ ボックスのフィールドに値を入力する必要があります。

手順

ステップ 1 メニュー バーで、**[ファブリック（Fabric）]** > **[ファブリック ポリシー（Fabric Policies）]** をクリックします。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ポリシー（Policies）]** > **[トラブルシューティング（Troubleshooting）]** > **[SPAN]** を展開します。

[SPAN] の下には、**[SPAN 送信元グループ（SPAN Source Groups）]**, **[SPAN フィルタ グループ（SPAN Filter Groups）]**、および **[SPAN 宛先グループ（SPAN Destination Groups）]** の 3 つのノードが表示されます。

ステップ 3 **[SPAN 送信元グループ（SPAN Source Groups）]** を右クリックし、**[SPAN 送信元グループの作成（Create SPAN Source Groups）]** 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 4 **[SPAN 送信元グループの作成（Create SPAN Source Group）]** 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。

ステップ 5 **[送信元の作成（Create Sources）]** テーブルを展開し、**[SPAN 送信元の作成]** ダイアログ ボックスを開きます。

ステップ 6 **[SPAN 送信元の作成（Create SPAN Source）]** 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。

ステップ 7 完了したら、[OK] をクリックします。

[SPAN 送信元グループの作成（Create VRF）] ダイアログ ボックスに戻ります。

ステップ 8 **[リモート場所の作成（Create Remote Location）]** ダイアログのフィールドに値を入力したら、**[送信（Submit）]** をクリックします。

次のタスク

SPAN 宛先のトラフィック アナライザを使用して、SPAN 送信元からのデータ 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。

APIC GUI を使用した外部アクセス用のレイヤ 3 EPG SPAN セッションの設定

この手順は、Cisco APIC GUI を使用して外部アクセス用のレイヤ 3 EPG SPAN ポリシーを設定する方法を示しています。設定手順では、1 つ以上の GUI ダイアログ ボックスのフィールドに値を入力する必要があります。

手順

ステップ 1 メニュー バーで、**[ファブリック（Fabric）]** > **[アクセス ポリシー（Access Policies）]** をクリックします。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ポリシー（Policies）]** > **[トラブルシューティング（Troubleshooting）]** > **[SPAN]** を展開します。

[SPAN] の下には、**[SPAN 送信元グループ（SPAN Source Groups）]**, **[SPAN フィルタ グループ（SPAN Filter Groups）]**、および **[SPAN 宛先グループ（SPAN Destination Groups）]** の 3 つのノードが表示されます。

ステップ 3 **[SPAN 送信元グループ（SPAN Source Groups）]** を右クリックし、**[SPAN 送信元グループの作成（Create SPAN Source Groups）]** 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 4 **[SPAN 送信元グループの作成（Create SPAN Source Group）]** 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。

ステップ 5 **[フィルタ グループ（Filter Group）]** フィールドで、フィルタ グループを選択または作成します。

詳細については、APIC GUI を使用した SPAN フィルタ グループの設定 （57 ページ）を参照してください。

ステップ 6 **[送信元の作成（Create Sources）]** テーブルを展開し、**[SPAN 送信元の作成（Create SPAN Source）]** ダイアログ ボックスを開きいて、以下の操作を実行します。

a) 送信元ポリシーの**[名前（Name）]** を入力します。

b) トラフィック フローの **[方向（Direction）]** オプションを選択します。

c) (オプション) **[ドロップ パケットのスパニング（Span Drop Packets）]** チェックボックスをクリックしてチェックマークを付けます。オンにすると、SPAN-on-drop 機能が有効になります。

d) 外部アクセスの場合は、**[外部にルーティング（Routed Outside）]**（**[タイプ（Type）]** フィールド）をクリックします。

（注）
外部アクセスで **[外部にルーティング（Routed Outside）]** を選択した場合、**[名前（Name）]**、**[アドレス（Address）]**、および **[Encap]** フィールドが表示されて、**[L3 Outside]** を設定できるようになります。

e) **[送信元アクセス パスの追加（Add Source Access Paths）]** を展開して、送信元パスを指定します。

[送信元をパスに関連付ける（Associate Source to Path）] ダイアログ ボックスが表示されます。

f) **[送信元をパスに関連付ける（Associate Source to Path）]** 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。

g) 送信元とパスの関連付けが完了したら、**[OK]** をクリックします。

[SPAN 送信元の作成（Create SPAN Source）] ダイアログ ボックスに戻ります。

h) SPAN 送信元の作成が完了したら、**[OK]** をクリックします。

[SPAN 送信元グループの作成（Create VRF）] ダイアログ ボックスに戻ります。

ステップ 7 SPAN 送信元グループの設定が完了したら、**[送信（Submit）]** をクリックします。

次のタスク

SPAN 宛先のトラフィック アナライザを使用して、SPAN 送信元からのデータ 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。

Cisco APIC GUI を使用したテナント SPAN ポリシーの宛先グループの構成

このセクションでは、Cisco APIC GUI を使用して、テナント SPAN ポリシーの宛先グループを作成する方法について説明します。設定手順では、1 つ以上の GUI ダイアログ ボックスのフィールドに値を入力する必要があります。

SPAN宛先グループと送信元を作成すれば、SPAN宛先のトラフィック アナライザを使用して、SPAN 送信元からのデータ 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。

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 **[ナビゲーション（Navigation）]** ペインでテナントを展開し、**[ポリシー（Policies）]** > **[トラブルシューティング（Troubleshooting）]** > を展開して、**[SPAN]** を展開します。

[SPAN] に表示される 2 つのノード：**[SPAN 宛先グループ（SPAN Destination Groups）]** と **[SPAN 送信元グループ（SPAN Source Groups）]**。

ステップ 4 **[SPAN 宛先グループ（SPAN Destination Groups）]** を右クリックして、**[SPAN 宛先グループの作成（Create SPAN Destination Groups）]** を選択します。**[Create SPAN Destination Group]** ダイアログが表示されます。

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) オプション。**[説明（Description）]** フィールドに、グループの説明を入力します。

c) **[宛先タイプ（Destination Type）]**で、**[アプリケーション EPG（Application EPG ）]** または **[L3Out EPG（L3Out EPG）]**を選択します。

SPAN パケットの **[宛先タイプ（Destination Type）]** として **[アプリケーション EPG（Application EPG）]** を指定する場合は、テナント、アプリケーション プロファイル、および宛先 EPG も含める必要があります。

SPAN パケットの **[宛先タイプ（Destination Type）]** として **[L3Out EPG]** を 指定する場合は、テナント、L3Out 名、および外部 EPG ネットワークも含める必要があります。

d) 複製されたパケットを受信するリモート サーバの **[宛先 IP（Destination IP）]** を指定します。

e) **[送信元 IP/プレフィックス（Source IP/Prefix）]**：送信元パケットの IP サブネットのベース IP アドレスです。

f) SPAN パケットの **[フロー ID（Flow ID）]** を指定します。指定できる範囲は 1 ～ 1023 です。デフォルトは 1 です。

g) **[TTL]** またはホップ制限を指定します。範囲は1ー255 ホップです。ゼロに設定する場合、TTL は指定されません。デフォルトは 64 ホップです。

h) **[MTU]** 値を指定します。範囲は 64 ～ 9216 です。デフォルトは、 1518 です。

i) SPAN 宛先の **[DSCP]** レベルを指定します。

ステップ 5 完了したら、[送信（Submit）] をクリックします。

宛先グループが作成されます。

Cisco APIC GUI を使用したアクセス SPAN ポリシーの宛先グループの設定

このセクションでは、Cisco APIC GUI を使用して、アクセス SPAN ポリシーの宛先グループを作成する方法について説明します。設定手順では、1 つ以上の GUI ダイアログ ボックスのフィールドに値を入力する必要があります。

SPAN宛先グループと送信元を作成すれば、SPAN宛先のトラフィック アナライザを使用して、SPAN送信元からのデータ 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。

手順

ステップ 1 メニューバーで、**[ファブリック（Fabric）]** > **[アクセス ポリシー（Access Policies）]** をクリックします。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ポリシー（Policies）]** > **[トラブルシューティング（Troubleshooting）]** > **[SPAN]** を展開します。

[SPAN] の下には、**[SPAN 送信元グループ（SPAN Source Groups）]**, **[SPAN フィルタ グループ（SPAN Filter Groups）]**、および **[SPAN 宛先グループ（SPAN Destination Groups）]** の 3 つのノードが表示されます。

ステップ 3 **[SPAN 宛先グループ（SPAN Destination Groups）]** を右クリックして、**[SPAN 宛先グループの作成（Create SPAN Destination Groups）]** を選択します。**[Create SPAN Destination Group]** ダイアログが表示されます。

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) オプション。**[説明（Description）]** フィールドに、グループの説明を入力します。

c) **[宛先タイプ（Destination Type）]**で、**[アプリケーション EPG（Application EPG ）]** または **[L3Out EPG（L3Out EPG）]**を選択します。

SPAN パケットの **[宛先タイプ（Destination Type）]** として **[アプリケーション EPG（Application EPG）]** を指定する場合は、テナント、アプリケーション プロファイル、および宛先 EPG も含める必要があります。

SPAN パケットの **[宛先タイプ（Destination Type）]** として **[L3Out EPG]** を 指定する場合は、テナント、L3Out プロファイル、および外部ネットワークも含める必要があります。

d) 複製されたパケットを受信するリモート サーバの **[宛先 IP（Destination IP）]** を指定します。

e) **[送信元 IP/プレフィックス（Source IP/Prefix）]** : 送信元パケットの IP サブネットのベース IP アドレスです。

f) SPAN パケットの **[フロー ID（Flow ID）]** を指定します。指定できる範囲は 1 ～ 1023 です。デフォルトは 1 です。

g) **[TTL]** またはホップ制限を指定します。範囲は1ー255 ホップです。ゼロに設定する場合、TTL は指定されません。デフォルトは 64 ホップです。

h) **[MTU]** 値を指定します。範囲は 64 ～ 9216 です。デフォルトは、 1518 です。

i) SPAN 宛先の **[DSCP]** レベルを指定します。

ステップ 4 完了したら、[送信（Submit）] をクリックします。

宛先グループが作成されます。

Cisco APIC GUI を使用したファブリック SPAN ポリシーの宛先グループの設定

このセクションでは、Cisco APIC GUI を使用して、ファブリック SPAN ポリシーの宛先グループを作成する方法について説明します。設定手順では、1 つ以上の GUI ダイアログ ボックスのフィールドに値を入力する必要があります。

SPAN宛先グループと送信元を作成すれば、SPAN宛先のトラフィック アナライザを使用して、SPAN 送信元からのデータ 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。

（注） スパン送信元をスパイン ポートとして構成し、L3Outを接続先として選択すると、対応するスパイン ノードで障害が発生し、無効な構成について通知されます。

手順

ステップ 1 メニュー バーで、**[ファブリック（Fabric）]** > **[ファブリック ポリシー（Fabric Policies）]** をクリックします。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ポリシー（Policies）]** > **[トラブルシューティング（Troubleshooting）]** > **[SPAN]** を展開します。

[SPAN] の下には、**[SPAN 送信元グループ（SPAN Source Groups）]**, **[SPAN フィルタ グループ（SPAN Filter Groups）]**、および **[SPAN 宛先グループ（SPAN Destination Groups）]** の 3 つのノードが表示されます。

ステップ 3 **[SPAN 宛先グループ（SPAN Destination Groups）]** を右クリックして、**[SPAN 宛先グループの作成（Create SPAN Destination Groups）]** を選択します。**[Create SPAN Destination Group]** ダイアログが表示されます。

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) オプション。**[説明（Description）]** フィールドに、グループの説明を入力します。
c) **[宛先タイプ（Destination Type）]**で、**[アプリケーション EPG（Application EPG ）]** または **[L3Out EPG（L3Out EPG）]**を選択します。

SPAN パケットの **[宛先タイプ（Destination Type）]** として **[アプリケーション EPG（Application EPG）]** を指定する場合は、テナント、アプリケーション プロファイル、および宛先 EPG も含める必要があります。

SPAN パケットの **[宛先タイプ（Destination Type）]** として **[L3Out EPG]** を 指定する場合は、テナント、L3Out プロファイル、および外部ネットワークも含める必要があります。

d) 複製されたパケットを受信するリモート サーバの **[宛先 IP（Destination IP）]** を指定します。
e) **[送信元 IP/プレフィックス（Source IP/Prefix）]**：送信元パケットの IP サブネットのベース IP アドレスです。
f) SPAN パケットの **[フロー ID（Flow ID）]** を指定します。指定できる範囲は 1 ～ 1023 です。デフォルトは 1 です。
g) **[TTL]** またはホップ制限を指定します。範囲は 1 ー 255 ホップです。ゼロに設定する場合、TTL は指定されません。デフォルトは 64 ホップです。
h) **[MTU]** 値を指定します。範囲は 64 ～ 9216 です。デフォルトは、 1518 です。
i) SPAN 宛先の **[DSCP]** レベルを指定します。

ステップ 4 完了したら、[送信（Submit）] をクリックします。

宛先グループが作成されます。

次のタスク

まだ作成していない場合は、ファブリック SPAN ポリシーの送信元を設定します。

NX-OS スタイルの CLI を使用した SPAN の構成

NX-OS スタイルの CLI を使用したアクセス モードでのローカル SPAN の設定

これは、アクセス リーフ ノードにローカルな従来の SPAN 設定です。1 つ以上のアクセス ポートまたはポート チャネルから発信されたトラフィックをモニタリングし、同じリーフ ノードにローカルな宛先ポートに送信できます。

手順

ステップ 1 **configure terminal**

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。

例：

```
apic1# configure terminal
```

ステップ 2 [**no**] **monitor access session** *session-name*

アクセス モニタリング セッション設定を作成します。

例：

```
apic1(config)# monitor access session mySession
```

ステップ 3 [**no**] **description** *text*

このアクセス モニタリング セッションの説明を追加します。テキストにスペースが含まれている場合は、単一引用符で囲む必要があります。

例：

```
apic1(config-monitor-access)# description "This is my SPAN session"
```

ステップ 4 [**no**] **destination interface ethernet** *slot/port* **leaf** *node-id*

宛先インターフェイスを指定します。宛先インターフェイスを FEX ポートにすることはできません。

例：

```
apic1(config-monitor-access)# destination interface ethernet 1/2 leaf 101
```

ステップ 5 [**no**] **source interface ethernet** {[*fex/*]*slot/port* | *port-range*} **leaf** *node-id*

送信元インターフェイス ポートまたはポート範囲を指定します。

例：

```
apic1(config-monitor-access)# source interface ethernet 1/2 leaf 101
```

ステップ 6 **drop enable**

ASIC でドロップされたすべてのパケットをキャプチャし、事前設定された SPAN 宛先に送信する、SPAN オン ドロップ機能をイネーブルにします。

例：

```
apic1(config-monitor-access-source)# drop enable
```

ステップ 7 [**no**] **direction** {**rx** | **tx** | **both**}

モニタリングするトラフィックの方向を指定します。方向は、送信元ポートごとに独立して設定できます。

例：

```
apic1(config-monitor-access-source)# direction tx
```

ステップ 8 [**no**] **filter tenant** *tenant-name* **application** *application-name* **epg** *epg-name*

モニタリングするトラフィックのフィルタ処理を行います。フィルタは、送信元ポート範囲ごとに独立して設定できます。

例：

```
apic1(config-monitor-access-source)# filter tenant t1 application app1 epg epg1
```

ステップ 9 **exit**

アクセス モニタリング セッション設定モードに戻ります。

例：

```
apic1(config-monitor-access-source)# exit
```

ステップ 10 [**no**] **destination interface port-channel** *port-channel-name-list* **leaf** *node-id*

宛先インターフェイスを指定します。宛先インターフェイスを FEX ポートにすることはできません。

（注）
リリース 4.1(1) 以降、コマンド例に示すように、宛先インターフェイスとしてスタティック ポート チャネルを使用できるようになりました。

例：

```
apic1(config-monitor-access)# destination interface port-channel pc1 leaf 101
```

ステップ 11 [**no**] **source interface port-channel** *port-channel-name-list* **leaf** *node-id* [**fex** *fex-id*]

送信元インターフェイス ポート チャネルを指定します。

（トラフィックの方向とフィルタ設定を入力します。ここには表示されていません）。

例：

```
apic1(config-monitor-access)# source interface port-channel pc5 leaf 101
```

ステップ 12 [**no**] **filter tenant** *tenant-name* **l3out** *L3Out-name* **vlan** *interface-VLAN*

モニタリングするトラフィックのフィルタ処理を行います。フィルタは、送信元ポート範囲ごとに独立して設定できます。

（注）
リリース 4.1(1) 以降、例に示すように、L3Out インターフェイス フィルタリングを設定するときに IP プレフィックスを指定する必要がなくなりました。

例：

```
apic1(config-monitor-access-source)# filter tenant t1 l3out l3out1 vlan 2820
```

ステップ 13 [**no**] **shutdown**

モニタリング セッションをディセーブル（またはイネーブル）にします。

例：

```
apic1(config-monitor-access)# no shut
```

例

この例は、ローカル アクセス モニタリング セッションを設定する方法を示しています。

```
apic1# configure terminal
apic1(config)# monitor access session mySession
apic1(config-monitor-access)# description "This is my SPAN session"
apic1(config-monitor-access)# destination interface ethernet 1/2 leaf 101
apic1(config-monitor-access)# source interface ethernet 1/1 leaf 101
apic1(config-monitor-access)# drop enable
apic1(config-monitor-access-source)# direction tx
apic1(config-monitor-access-source)# filter tenant t1 application app1 epg epg1
```

```
apic1(config-monitor-access-source)# exit
apic1(config-monitor-access)# no shut
apic1(config-monitor-access)# show run
# Command: show running-config monitor access session mySession
# Time: Fri Nov 6 23:55:35 2015
  monitor access session mySession
    description "This is my SPAN session"
    destination interface eth 1/2 leaf 101
    source interface eth 1/1 leaf 101
      direction tx
      filter tenant t1 application app1 epg epg
      exit
    exit
```

NX-OS スタイルの CLI を使用した SPAN フィルタ グループの設定

次の手順では、SPAN フィルタ グループとフィルタ エントリを設定する方法について説明します。

手順

ステップ 1 configure

グローバル設定モードを開始します。

例：

```
apic1# configure
```

ステップ 2 [no] monitor access filter-group *filtergroup-name*

アクセス モニタリング フィルタ グループ設定を作成します。

例：

```
apic1(config)# monitor access filter-group filtergroup1
```

ステップ 3 [no] filter srcaddress *source-address* dstaddress *destination-address* srcport-from *source-from-port* srcport-to *source-to-port* dstport-from *destination-from-port* dstport-to *destination-to-port* ipproto *IP-protocol*

フィルタ グループのフィルタ エントリを設定します。ここで、

- *source-address* は、*IP* アドレス/マスク 形式の送信元 IP アドレスです。IPv4 アドレスおよび IPv6 アドレスのどちらもサポートされています。**0.0.0.0** の値は、このフィールドで **任意の** IPv4 アドレス エントリを指定するために、**::** の値は、**任意の** IPv6 アドレスエントリを指定するために使用します。
- *destination-address* は、*IP* アドレス/マスク形式の宛先 IP アドレスです。IPv4 アドレスおよび IPv6 アドレスのどちらもサポートされています。**0.0.0.0** の値は、このフィールドで **任意の** IPv4 アドレス エントリを指定するために、**::** の値は、**任意の** IPv6 アドレスエントリを指定するために使用します。

- *source-from-port* は、最初の送信元レイヤ 4 ポートです。このフィールドは、**srcport-to** フィールドとともに、送信元ポートをフィルタリングするためのポート範囲を指定します。値 **0** は、このフィールドで**任意の**エントリを指定するために使用します。
- *source-to-port* は、最後の送信元レイヤ 4 ポートです。このフィールドは、**srcport-from** フィールドとともに、送信元ポートをフィルタリングするためのポート範囲を指定します。値 **0** は、このフィールドで**任意の**エントリを指定するために使用します。
- *destination-from-port* は、最初の宛先レイヤ 4 ポートです。このフィールドは、**dstport-to** フィールドとともに、宛先ポートをフィルタリングするためのポート範囲を指定します。値 **0** は、このフィールドで**任意の**エントリを指定するために使用します。
- *destination-to-port* は、最後の宛先レイヤ 4 ポートです。このフィールドは、**dstport-from** フィールドとともに、宛先ポートをフィルタリングするためのポート範囲を指定します。値 **0** は、このフィールドで**任意の**エントリを指定するために使用します。
- *IP-protocol* は IP プロトコルです。値 **0** は、このフィールドで**任意の**エントリを指定するために使用します。

例：

```
apic1(config-monitor-fltgrp)# filter srcaddress 1.1.1.0/24 dstaddress 0.0.0.0 srcport-from
 0 srcport-to 0 dstport-from 0 dstport-to 0 ipproto 20
```

ステップ 4 **exit**

アクセス モニター フィルタ グループ設定モードに戻ります。

例：

```
apic1(config-monitor-fltgrp)# exit
```

ステップ 5 **exit**

グローバル コンフィギュレーション モードを終了します。

例：

```
apic1(config)# exit
```

例

この例は、SPAN フィルタ グループとフィルタ エントリを設定する方法を示しています。

```
apic1# configure
apic1(config)# monitor access filter-group filtergroup1
apic1(config-monitor-fltgrp)# filter srcaddress 1.1.1.0/24 dstaddress 0.0.0.0 srcport-from
 0 srcport-to 0 dstport-from 0 dstport-to 0 ipproto 20
apic1(config-monitor-fltgrp)# exit
apic1(config)# exit
```

NX-OS スタイルの CLI を使用した SPAN フィルタ グループの関連付け

次の手順では、フィルタ グループを SPAN 送信元グループに関連付ける方法について説明します。

手順

ステップ 1 **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。

例：

```
apic1# configure
```

ステップ 2 [**no**] **monitor access session** *session-name*

アクセス モニタリング セッション設定を作成します。

例：

```
apic1(config)# monitor access session session1
```

ステップ 3 **filter-group** *filtergroup-name*

フィルタ グループを関連付けます。

例：

```
apic1(config-monitor-access)# filter-group filtergroup1
```

ステップ 4 **no filter-group**

必要に応じて、フィルタ グループの関連付けを解除します。

例：

```
apic1(config-monitor-access)# no filter-group
```

ステップ 5 [**no**] **source interface ethernet** {[*fex/*]*slot/port* | *port-range*} **leaf** *node-id*

送信元インターフェイス ポートまたはポート範囲を指定します。

例：

```
apic1(config-monitor-access)# source interface ethernet 1/9 leaf 101
```

ステップ 6 **filter-group** *filtergroup-name*

フィルタ グループを SPAN 送信元に関連付けます。

例：

```
apic1(config-monitor-access-source)# filter-group filtergroup2
```

ステップ 7 **exit**

アクセス モニター フィルタ グループ設定モードに戻ります。

例：

```
apic1(config-monitor-access-source)# exit
```

ステップ 8 **no filter-group**

必要に応じて、SPAN 送信元からフィルタ グループの関連付けを解除します。

例：

```
apic1(config-monitor-access-source)# no filter-group
```

ステップ 9 **exit**

アクセス モニター フィルタ グループ設定モードに戻ります。

例：

```
apic1(config-monitor-access)# exit
```

ステップ 10 **exit**

グローバル コンフィギュレーション モードを終了します。

例：

```
apic1(config)# exit
```

例

この例は、フィルタ グループを関連付ける方法を示しています。

```
apic1# configure
apic1(config)# monitor access session session1
apic1(config-monitor-access)# filter-group filtergroup1
apic1(config-monitor-access)# source interface ethernet 1/9 leaf 101
apic1(config-monitor-access-source)# filter-group filtergroup2
apic1(config-monitor-access-source)# exit
apic1(config-monitor-access-source)# no filter-group
apic1(config-monitor-access)# exit
apic1(config)# exit
```

NX-OS スタイルの CLI を使用したアクセス モードでの ERSPAN の設定

ACI ファブリックでは、アクセス モードの ERSPAN 設定を使用して、1 つ以上のリーフ ノードのアクセス ポート、ポート チャネル、および vPC から発信されたトラフィックを監視できます。

ERSPAN セッションの場合、宛先は常にエンドポイント グループ (EPG) で、これらはファブリック内のどこにでも展開できます。監視対象のトラフィックは、どこであれ、EPGが移動した場所である宛先に転送されます。

手順

ステップ 1 **configure terminal**

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。

例：

```
apic1# configure terminal
```

ステップ 2 [**no**] **monitor access session** *session-name*

アクセス モニタリング セッション設定を作成します。

例：

```
apic1(config)# monitor access session mySession
```

ステップ 3 [**no**] **description** *text*

このモニタリング セッションの説明を追加します。テキストにスペースが含まれている場合は、単一引用符で囲む必要があります。

例：

```
apic1(config-monitor-access)# description "This is my access ERSPAN session"
```

ステップ 4 [**no**] **destination tenant** *tenant-name* **application** *application-name* **epg** *epg-name* **destination-ip** *dest-ip-address* **source-ip-prefix** *src-ip-address*

宛先インターフェイスをテナントとして指定し、宛先コンフィギュレーションモードを開始します。

例：

```
apic1(config-monitor-access)# destination tenant t1 application app1 epg epg1
destination-ip 192.0.20.123 source-ip-prefix 10.0.20.1
```

ステップ 5 [**no**] **erspan-id** *flow-id*

ERSPAN セッションの ERSPAN ID を設定します。ERSPAN の範囲は 1 ～ 1023 です。

例：

```
apic1(config-monitor-access-dest)# erspan-id 100
```

ステップ 6 [**no**] **ip dscp** *dscp-code*

ERSPAN トラフィックのパケットの DiffServ コード ポイント（DSCP）値を設定します。指定できる範囲は 0 ～ 64 です。

例：

```
apic1(config-monitor-access-dest)# ip dscp 42
```

ステップ 7 [**no**] **ip ttl** *ttl-value*

ERSPAN トラフィックの IP 存続可能時間（TTL）値を設定します。範囲は 1 ～ 255 です。

例：

```
apic1(config-monitor-access-dest)# ip ttl 16
```

ステップ 8 [**no**] **mtu** *mtu-value*

ERSPAN セッションの最大伝送単位（MTU）サイズを設定します。指定できる範囲は 64 ～ 9216 バイトです。

例：

```
apic1(config-monitor-access-dest)# mtu 9216
```

ステップ 9 **exit**

モニター アクセス設定モードに戻ります。

例：

```
apic1(config-monitor-access-dest)#
```

ステップ 10 [**no**] **source interface ethernet** {[*fex/*]*slot/port* | *port-range*} **leaf** *node-id*

送信元インターフェイス ポートまたはポート範囲を指定します。

例：

```
apic1(config-monitor-access)# source interface eth 1/2 leaf 101
```

ステップ 11 [**no**] **source interface port-channel** *port-channel-name-list* **leaf** *node-id* [**fex** *fex-id*]

送信元インターフェイスのポートチャネルを指定します。

例：

```
apic1(config-monitor-access)# source interface port-channel pc1 leaf 101
```

ステップ 12 [**no**] **source interface vpc** *vpc-name-list* **leaf** *node-id1 node-id2* [**fex** *fex-id1 fex-id2*]

送信元インターフェイス vPC を指定します。

例：

```
apic1(config-monitor-access)# source interface vpc pc1 leaf 101 102
```

ステップ 13 **drop enable**

ASIC でドロップされたすべてのパケットをキャプチャし、事前設定された SPAN 宛先に送信する、SPAN オン ドロップ機能をイネーブルにします。

例：

```
apic1(config-monitor-access-source)# drop enable
```

ステップ 14 [**no**] **direction** {**rx** | **tx** | **both**}

モニタリングするトラフィックの方向を指定します。方向は、送信元ポートごとに独立して設定できます。

例：

```
apic1(config-monitor-access-source)# direction tx
```

ステップ 15 [**no**] **filter tenant** *tenant-name* **application** *application-name* **epg** *epg-name*

モニタリングするトラフィックのフィルタ処理を行います。フィルタは、送信元ポート範囲ごとに独立して設定できます。

例：

```
apic1(config-monitor-access-source)# filter tenant t1 application app1 epg epg1
```

ステップ 16 **exit**

アクセス モニタリング セッション設定モードに戻ります。

例：

```
apic1(config-monitor-access-source)# exit
```

ステップ 17 **[no] shutdown**

モニタリング セッションをディセーブル（またはイネーブル）にします。

例：

```
apic1(config-monitor-access)# no shut
```

例

この例は、ERSPAN アクセス モニタリング セッションを設定する方法を示しています。

```
apic1# configure terminal
apic1(config)# monitor access session mySession
apic1(config-monitor-access)# description "This is my access ERSPAN session"
apic1(config-monitor-access)# destination tenant t1 application app1 epg epg1
destination-ip 192.0.20.123 source-ip-prefix 10.0.20.1
apic1(config-monitor-access-dest)# erspan-id 100
apic1(config-monitor-access-dest)# ip dscp 42
apic1(config-monitor-access-dest)# ip ttl 16
apic1(config-monitor-access-dest)# mtu 9216
apic1(config-monitor-access-dest)# exit
apic1(config-monitor-access)# source interface eth 1/1 leaf 101
apic1(config-monitor-access-source)# direction tx
apic1(config-monitor-access-source)#drop enable
apic1(config-monitor-access-source)# filter tenant t1 application app1 epg epg1
apic1(config-monitor-access-source)# exit
apic1(config-monitor-access)# no shut
apic1(config-monitor-access)# show run
# Command: show running-config monitor access session mySession
# Time: Fri Nov 6 23:55:35 2015
  monitor access session mySession
    description "This is my ERSPAN session"
    source interface eth 1/1 leaf 101
      direction tx
      filter tenant t1 application app1 epg epg1
      exit
    destination tenant t1 application app1 epg epg1 destination-ip 192.0.20.123
source-ip-prefix 10.0.20.1
      ip dscp 42
      ip ttl 16
      erspan-id 9216
```

```
    mtu 9216
    exit
  exit
```

この例は、モニタリング送信元としてポート チャネルを設定する方法を示しています。

```
apic1(config-monitor-access)# source interface port-channel pc3 leaf 105
```

この例は、モニタリング送信元として vPC の 1 つのレッグを設定する方法を示しています。

```
apic1(config-monitor-access)# source interface port-channel vpc3 leaf 105
```

次の例は、FEX 101 からのポートの範囲をモニタリング送信元として設定する方法を示しています。

```
apic1(config-monitor-access)# source interface eth 101/1/1-2 leaf 105
```

NX-OS スタイルの CLI を使用したファブリック モードでの ERSPAN の設定

ACI ファブリックでは、ファブリック モードの ERSPAN 設定を使用して、リーフ ノードまたはスパイン ノードの 1 つ以上のファブリック ポートから発信されたトラフィックをモニタリングできます。ローカル SPAN はファブリック モードではサポートされていません。

ERSPAN セッションの場合、宛先は常にエンドポイント グループ (EPG) で、これらはファブリック内のどこにでも展開できます。監視対象のトラフィックは、どこであれ、EPGが移動した場所である宛先に転送されます。ファブリック モードでは、ファブリック ポートのみが送信元として許可されますが、リーフ スイッチとスパイン スイッチの両方が許可されます。

手順

ステップ 1 **configure terminal**

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。

例：

```
apic1# configure terminal
```

ステップ 2 [**no**] **monitor fabric session** *session-name*

ファブリック モニタリング セッション設定を作成します。

例：

```
apic1(config)# monitor fabric session mySession
```

ステップ 3 [**no**] **description** *text*

このモニタリング セッションの説明を追加します。テキストにスペースが含まれている場合は、単一引用符で囲む必要があります。

例：

```
apic1(config-monitor-fabric)# description "This is my fabric ERSPAN session"
```

ステップ 4 [**no**] **destination tenant** *tenant-name* **application** *application-name* **epg** *epg-name* **destination-ip** *dest-ip-address* **source-ip-prefix** *src-ip-address*

宛先インターフェイスをテナントとして指定し、宛先コンフィギュレーションモードを開始します。

例：

```
apic1(config-monitor-fabric)# destination tenant t1 application app1 epg epg1
destination-ip 192.0.20.123 source-ip-prefix 10.0.20.1
```

ステップ 5 [**no**] **erspan-id** *flow-id*

ERSPAN セッションの ERSPAN ID を設定します。ERSPAN の範囲は 1 ～ 1023 です。

例：

```
apic1(config-monitor-fabric-dest)# erspan-id 100
```

ステップ 6 [**no**] **ip dscp** *dscp-code*

ERSPAN トラフィックのパケットの DiffServ コード ポイント（DSCP）値を設定します。指定できる範囲は 0 ～ 64 です。

例：

```
apic1(config-monitor-fabric-dest)# ip dscp 42
```

ステップ 7 [**no**] **ip ttl** *ttl-value*

ERSPAN トラフィックの IP 存続可能時間（TTL）値を設定します。範囲は 1 ～ 255 です。

例：

```
apic1(config-monitor-fabric-dest)# ip ttl 16
```

ステップ 8 [**no**] **mtu** *mtu-value*

ERSPAN セッションの最大伝送単位（MTU）サイズを設定します。指定できる範囲は 64 ～ 9216 バイトです。

例：

```
apic1(config-monitor-fabric-dest)# mtu 9216
```

ステップ 9 **exit**

モニター アクセス設定モードに戻ります。

例：

```
apic1(config-monitor-fabric-dest)#
```

ステップ 10 [**no**] **source interface ethernet** {*slot/port* | *port-range*} **switch** *node-id*

送信元インターフェイス ポートまたはポート範囲を指定します。

例：

```
apic1(config-monitor-fabric)# source interface eth 1/2 switch 101
```

ステップ 11 **drop enable**

ASIC でドロップされたすべてのパケットをキャプチャし、事前設定された SPAN 宛先に送信する、SPAN オン ドロップ機能をイネーブルにします。

例：

```
apic1(config-monitor-fabric-source)# drop enable
```

ステップ 12 [**no**] **direction** {**rx** | **tx** | **both**}

モニタリングするトラフィックの方向を指定します。方向は、送信元ポートごとに独立して設定できます。

例：

```
apic1(config-monitor-fabric-source)# direction tx
```

ステップ 13 [**no**] **filter tenant** *tenant-name* **bd** *bd-name*

ブリッジ ドメインでトラフィックをフィルタリングします。

例：

```
apic1(config-monitor-fabric-source)# filter tenant t1 bd bd1
```

ステップ 14 [**no**] **filter tenant** *tenant-name* **vrf** *vrf-name*

VRF でトラフィックをフィルタリングします。

例：

```
apic1(config-monitor-fabric-source)# filter tenant t1 vrf vrf1
```

ステップ 15 **exit**

アクセス モニタリング セッション設定モードに戻ります。

例：

```
apic1(config-monitor-fabric-source)# exit
```

ステップ 16 [**no**] **shutdown**

モニタリング セッションをディセーブル（またはイネーブル）にします。

例：

```
apic1(config-monitor-fabric)# no shut
```

例

この例は、ERSPAN ファブリック モニタリング セッションを設定する方法を示しています。

```
apic1# configure terminal
apic1(config)# monitor fabric session mySession
apic1(config-monitor-fabric)# description "This is my fabric ERSPAN session"
apic1(config-monitor-fabric)# destination tenant t1 application app1 epg epg1
destination-ip 192.0.20.123 source-ip-prefix 10.0.20.1
apic1(config-monitor-fabric-dest)# erspan-id 100
apic1(config-monitor-fabric-dest)# ip dscp 42
apic1(config-monitor-fabric-dest)# ip ttl 16
apic1(config-monitor-fabric-dest)# mtu 9216
apic1(config-monitor-fabric-dest)# exit
apic1(config-monitor-fabric)# source interface eth 1/1 switch 101
apic1(config-monitor-fabric-source)# drop enable
apic1(config-monitor-fabric-source)# direction tx
apic1(config-monitor-fabric-source)# filter tenant t1 bd bd1
apic1(config-monitor-fabric-source)# filter tenant t1 vrf vrf1
apic1(config-monitor-fabric-source)# exit
apic1(config-monitor-fabric)# no shut
```

NX-OS スタイルの CLI を使用したテナント モードでの ERSPAN の設定

ACI ファブリックでは、テナント モードの ERSPAN 設定を使用して、テナント内のエンドポイント グループから発信されたトラフィックをモニタリングできます。

テナント モードでは、送信元 EPG から発信されたトラフィックは、同じテナント内の宛先 EPG に送信されます。送信元または宛先の EPG がファブリック内で移動しても、トラフィックのモニタリングには影響しません。

手順

ステップ 1 **configure terminal**

グローバル設定モードを開始します。

例：

```
apic1# configure terminal
```

ステップ 2 [**no**] **monitor tenant** *tenant-name* **session** *session-name*

テナント モニタリング セッション設定を作成します。

例：

```
apic1(config)# monitor tenant session mySession
```

ステップ 3 [**no**] **description** *text*

このアクセス モニタリング セッションの説明を追加します。テキストにスペースが含まれている場合は、単一引用符で囲む必要があります。

例：

```
apic1(config-monitor-tenant)# description "This is my tenant ERSPAN session"
```

ステップ 4 [**no**] **destination tenant** *tenant-name* **application** *application-name* **epg** *epg-name* **destination-ip** *dest-ip-address* **source-ip-prefix** *src-ip-address*

宛先インターフェイスをテナントとして指定し、宛先コンフィギュレーション モードを開始します。

例：

```
apic1(config-monitor-tenant)# destination tenant t1 application app1 epg epg1
destination-ip 192.0.20.123 source-ip-prefix 10.0.20.1
```

ステップ 5 [**no**] **erspan-id** *flow-id*

ERSPAN セッションの ERSPAN ID を設定します。ERSPAN の範囲は 1 ～ 1023 です。

例：

```
apic1(config-monitor-tenant-dest)# erspan-id 100
```

ステップ 6 [**no**] **ip dscp** *dscp-code*

ERSPAN トラフィックのパケットの DiffServ コード ポイント（DSCP）値を設定します。指定できる範囲は 0 ～ 64 です。

例：

```
apic1(config-monitor-tenant-dest)# ip dscp 42
```

ステップ 7 [**no**] **ip ttl** *ttl-value*

ERSPAN トラフィックの IP 存続可能時間（TTL）値を設定します。範囲は 1 ～ 255 です。

例：

```
apic1(config-monitor-tenant-dest)# ip ttl 16
```

ステップ 8 [**no**] **mtu** *mtu-value*

ERSPAN セッションの最大伝送単位（MTU）サイズを設定します。指定できる範囲は 64 ～ 9216 バイトです。

例：

```
apic1(config-monitor-tenant-dest)# mtu 9216
```

ステップ 9 **exit**

モニター アクセス設定モードに戻ります。

例：

```
apic1(config-monitor-tenant-dest)#
```

ステップ 10 [**no**] **source application** *application-name* **epg** *epg-name*

送信元インターフェイス ポートまたはポート範囲を指定します。

例：

```
apic1(config-monitor-tenant)# source application app2 epg epg5
```

ステップ 11 [**no**] **direction** {**rx** | **tx** | **both**}

モニタリングするトラフィックの方向を指定します。方向は、送信元ポートごとに独立して設定できます。

例：

```
apic1(config-monitor-tenant-source)# direction tx
```

ステップ 12 **exit**

アクセス モニタリング セッション設定モードに戻ります。

例：

```
apic1(config-monitor-tenant-source)# exit
```

ステップ 13 [**no**] **shutdown**

モニタリング セッションをディセーブル（またはイネーブル）にします。

例：

```
apic1(config-monitor-tenant)# no shut
```

例

この例は、ERSPAN テナント モニタリング セッションを設定する方法を示しています。

```
apic1# configure terminal
apic1(config)# monitor access session mySession
apic1(config-monitor-tenant)# description "This is my tenant ERSPAN session"
apic1(config-monitor-tenant)# destination tenant t1 application app1 epg epg1
destination-ip 192.0.20.123 source-ip-prefix 10.0.20.1
apic1(config-monitor-tenant-dest)# erspan-id 100
apic1(config-monitor-tenant-dest)# ip dscp 42
apic1(config-monitor-tenant-dest)# ip ttl 16
apic1(config-monitor-tenant-dest)# mtu 9216
apic1(config-monitor-tenant-dest)# exit
apic1(config-monitor-tenant)# source application app2 epg epg5
apic1(config-monitor-tenant-source)# direction tx
apic1(config-monitor-tenant-source)# exit
apic1(config-monitor-tenant)# no shut
```

NX-OS スタイルの CLI を使用したグローバル SPAN-On-Drop セッションの設定

このセクションでは、ノード上のすべてのポートを SPAN 送信元とするグローバル ドロップを作成する方法を示します。

手順

ステップ 1 **configure terminal**

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。

例：

```
apic1# configure terminal
```

ステップ 2 [**no**] **monitor fabric session** *session-name*

ファブリック モニタリング セッション設定を作成します。

例：

```
apic1(config)# monitor fabric session Spine301-GD-SOD
```

ステップ 3 [**no**] **description** *text*

このモニタリング セッションの説明を追加します。テキストにスペースが含まれている場合は、単一引用符で囲む必要があります。

例：

```
apic1(config-monitor-fabric)# description "This is my fabric ERSPAN session"
```

ステップ 4 **source global-drop switch**

ASIC でドロップされたすべてのパケットをキャプチャし、事前設定された SPAN 宛先に送信する、SPAN オン ドロップ機能をイネーブルにします。

例：

```
apic1(config-monitor-fabric)# source global-drop switch
```

ステップ 5 [**no**] **destination tenant** *tenant-name***application** *application-name* **epg** *epg-name* **destination-ip** *dest-ip-address* **source-ip-prefix** *src-ip-address*

宛先インターフェイスをテナントとして指定し、宛先コンフィギュレーション モードを開始します。

例：

```
apic1(config-monitor-fabric-dest)# destination tenant ERSPAN application A1 epg E1
destination-ip 165.10.10.155 source-ip-prefix 22.22.22.22
```

例

次に、SPAN-on-Drop セッションを設定する例を示します。

```
apic1# configure terminal
apic1(config)# monitor fabric session Spine301-GD-SOD
apic1(config-monitor-fabric)# source global-drop switch
apic1(config-monitor-fabric)# destination tenant ERSPAN application A1 epg E1
destination-ip 179.10.10.179 source-ip-prefix 31.31.31.31
```

REST API を使用した SPAN の構成

REST API を使用した ERSPAN 宛先のファブリック宛先グループの設定

このセクションでは、REST API を使用して、ERSPAN 宛先のファブリック宛先グループを設定することにより、REST API の使用方法を示します。使用可能なプロパティのリストについては、『*APIC* 管理情報モデル資料』を参照してください。

手順

ERSPAN 宛先のファブリック宛先グループを設定します。

```
POST https://<APIC_IP>/api/node/mo/uni/infra.xml
<spanDestGrp annotation="" descr="" name="Dest2" nameAlias="" ownerKey="" ownerTag="">
    <spanDest annotation="" descr="" name="Dest2" nameAlias="" ownerKey="" ownerTag="">
    <spanRsDestEpg annotation="" dscp="unspecified" finalIp="0.0.0.0" flowId="1"
ip="179.10.10.179"
     mtu="1518"srcIpPrefix="20.20.20.2" tDn="uni/tn-ERSPAN/ap-A1/epg-E1" ttl="64"
ver="ver2"
     verEnforced="no"/>
    </spanDest>
</spanDestGrp>
```

REST API を使用したグローバル ドロップ送信元グループの設定

このセクションでは、REST API を使用してグローバル ドロップ送信元グループを構成することにより、REST API の使用方法を示します。使用可能なプロパティのリストについては、『*APIC* 管理情報モデル資料』を参照してください。

手順

グローバル ドロップ送信元グループを構成します。

```
POST https://<APIC_IP>/api/node/mo/uni/infra.xml
<spanSrcGrp adminSt="enabled" annotation="" descr="" name="Spine-402-GD-SOD" nameAlias="">

   <spanSrc annotation="" descr="" dir="both" name="402" nameAlias=""  spanOnDrop="yes">

    <spanRsSrcToNode annotation="" tDn="topology/pod-1/node-402"/>
    </spanSrc><spanSpanLbl annotation="" descr="" name="402-dst-179" nameAlias=""
tag="yellow-green"/>
</spanSrcGrp>
```

REST API を使用した SPAN 宛先としてのリーフ ポートの設定

このセクションでは、REST API を使用してリーフ ポートを SPAN 宛先として設定することにより、REST API の使用方法を示します。使用可能なプロパティのリストについては、『*APIC* 管理情報モデル資料』を参照してください。

手順

リーフ ポートを SPAN 宛先として設定します。

```
POST https://<APIC_IP>/api/node/mo/uni/infra.xml
<spanDestGrp annotation="" descr="" name="Dest4" nameAlias="" ownerKey="" ownerTag="">
    <spanDest annotation="" descr="" name="Dest4" nameAlias="" ownerKey="" ownerTag="">
    <spanRsDestPathEp annotation="" mtu="1518"
tDn="topology/pod-1/paths-301/pathep-[eth1/18]"/>
    </spanDest>
</spanDestGrp>
```

REST API を使用した SPAN アクセス送信元グループの設定

このセクションでは、REST API を使用して SPAN アクセス ソース グループを設定することにより、REST API の使用方法を示します。使用可能なプロパティのリストについては、『*APIC* 管理情報モデル資料』を参照してください。

手順

SPAN アクセス送信元グループを設定します。

```
POST https://<APIC_IP>/api/node/mo/uni/infra.xml
<spanSrcGrp adminSt="enabled" annotation="" descr=""  name="Test-Src2" nameAlias=""
ownerKey=""
 ownerTag="">
    <spanSrc annotation="" descr="" dir="both" name="Src1" nameAlias="" ownerKey=""
ownerTag=""
     spanOnDrop="yes">
    <spanRsSrcToPathEp annotation="" tDn="topology/pod-1/paths-301/pathep-[eth1/1]"/>
    </spanSrc>
   <spanSpanLbl annotation="" descr="" name="Dest1" nameAlias="" ownerKey="" ownerTag=""

     tag="yellow-green"/>
</spanSrcGrp>
```

REST API を使用した SPAN ファブリック送信元グループの設定

このセクションでは、REST API を使用して SPAN ファブリック送信元グループを設定することにより、REST API の使用方法を示します。使用可能なプロパティのリストについては、『*APIC* 管理情報モデル資料』を参照してください。

手順

SPAN ファブリック送信元グループを設定します。

```
POST https://<APIC_IP>/api/node/mo/uni/infra.xml
<spanSrcGrp adminSt="enabled" annotation="" descr="" name="Test-Src2" nameAlias=""
ownerKey=""
 ownerTag="">
    <spanSrc annotation="" descr="" dir="both" name="Src1" nameAlias="" ownerKey=""
     ownerTag="" spanOnDrop="yes">
    <spanRsSrcToPathEp annotation="" tDn="topology/pod-1/paths-301/pathep-[eth1/51]"/>
    </spanSrc>
   <spanSpanLbl annotation="" descr="" name="Dest2" nameAlias="" ownerKey="" ownerTag=""

     tag="yellow-green"/>
</spanSrcGrp>
```

REST API を使用した ERSPAN 宛先のアクセス宛先グループの設定

このセクションでは、REST API を使用して、ERSPAN 宛先のアクセス宛先グループを設定することにより、REST API の使用方法を示します。使用可能なプロパティのリストについては、『*APIC* 管理情報モデル資料』を参照してください。

手順

ERSPAN 宛先のアクセス宛先グループを設定します。

```
POST https://<APIC_IP>/api/node/mo/uni/infra.xml
<spanDestGrp annotation="" descr="" name="Dest4" nameAlias="" ownerKey=""
  ownerTag="">
    <spanDest annotation="" descr="" name="Dest4" nameAlias="" ownerKey=""
     ownerTag="">
    <spanRsDestPathEp annotation="" mtu="1518" tDn="topology/pod-1/paths-301/pathep-
     [eth1/18]"/>
    </spanDest>
</spanDestGrp>
```

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。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。

トレースルートでは、次のようなさまざまなモードがサポートされています。

- エンドポイント間、リーフ間（トンネル エンドポイント、または TEP 間）
- エンドポイントから外部 IP
- 外部 IP からエンドポイント
- 外部 IP 間

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*』ドキュメントを参照してください。
- エンドポイントを新しいMACアドレス（トレースルート ポリシーを設定する際に指定した MAC アドレスと異なる）の ToR スイッチに移動すると、トレースルート ポリシーでそのエンドポイントに「missing-target」と表示されます。この場合は、新しい MAC アドレスを指定して新しいトレースルート ポリシーを設定する必要があります。
- ポリシーベースのリダイレクト機能を含むフローに対してトレースルートを実行する場合、パケットがサービスデバイスからリーフ スイッチに送信されるときに、リーフ スイッチが存続時間（TTL）期限切れメッセージを送信元に伝えるために使用する IP アドレス

は、必ずしもサービス デバイスのブリッジ ドメインのスイッチ仮想インターフェイス（SVI）の IP アドレスにはなりません。この動作は表面的なものであり、トラフィックが予期された経路をたどっていないことを示すものではありません。

エンドポイント 間での traceroute 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 **[ナビゲーション]** ペインでテナントを展開し、**[ポリシー]** > **[トラブルシューティング]** を展開します。

ステップ 4 [Troubleshoot] で次のトレースルート ポリシーのいずれかを右クリックします。

- [Endpoint-to-Endpoint Traceroute Policies] を右クリックして [Create Endpoint-to-Endpoint Traceroute Policy] を選択する
- [Endpoint-to-External-IP Traceroute Policies] を右クリックして [Create Endpoint-to-External-IP Traceroute Policy] を選択する
- [External-IP-to-Endpoint Traceroute Policies] を右クリックして [Create External-IP-to-Endpoint Traceroute Policy] を選択する
- [External-IP-to-External-IP Traceroute Policies] を右クリックして [Create External-IP-to-External-IP Traceroute Policy] を選択する

ステップ 5 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、ダイアログボックスの右上隅にあるヘルプ アイコン（[?]）をクリックしてください。

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 Endpoints] タブ、[Results] タブの順にクリックします。

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。

acidiag コマンド

Cisco APIC でのトラブルシューティング操作では、**acidiag** コマンドを使用します。

⚠

注意 このコマンドは、ACIの日常的な操作を目的としたものではありません。コマンドのすべての形式は、非常に混乱を招く可能性があり、適切に使用しないとネットワークに重大な問題が発生する場合があります。実行する前に、ファブリックへの完全な影響を理解してください。

クラスタ コマンド

```
acidiag

acidiag avread

acidiag fnvread

acidiag fnvreadex
```

構文の説明

オプション	機能
avread	クラスタ内のAPICを表示します。avreadの出力は次のとおりです。 • Cluster of：動作するクラスタのサイズ • out of target：必要なクラスタ サイズ • active=：APICが到達可能かどうかを示します • health=：全体的なAPICの正常性の概要。正常性スコアが低下しているサービスを表示します。 • chassisID=：所定の APIC に対する既知のシャーシ ID。 （注） 現在クラスタにない APIC については、ピア シャーシ ID が正しくない可能性があります。

オプション	機能
bootcurr	次回の起動時に、APIC システムは Linux パーティション内の現在の APIC イメージを起動します。このオプションは、通常は使用されません。
bootother	次回の起動時に、APIC システムは Linux パーティションの以前の APIC イメージを起動します。このオプションは、通常は使用されません。
bond0test	リーフへの APIC 接続の中断テスト。これは、シスコの内部テスト目的でのみ使用されます。それ以外では、ファブリックへの APIC 接続で問題が発生する可能性があります。
fnvread	ファブリックに登録されているスイッチ ノードのアドレスと状態を表示します。
fnvreadex	ファブリックに登録されているスイッチのノードの追加情報を表示します。
linkflap	指定された APIC インターフェイスを停止およびバックアップします。
preservelogs	APIC は現在のログをアーカイブします。通常の再起動中に、これは自動的に発生します。このオプションは、ハード リブートの前に使用できます。
run	使用可能な 2 つのオプションは、iptables-list と lldptool です。iptables-list は、管理テナント コントラクトによって制御される Linux iptables を表示するために使用されます。 lldptool は、APIC によって送受信される lldp 情報を表示するために使用されます。
rvread	データ レイヤの状態を要約します。出力には、各サービスのデータ レイヤの状態の概要が表示されます。シャード ビューには、レプリカが昇順で表示されます。
acidiag rvread *service*	すべてのレプリカのすべてのシャードでのサービスのデータ レイヤの状態を表示します。 （注） 例については、例 （94 ページ） を参照してください。

オプション	機能
acidiag rvread *service shard*	すべてのレプリカの特定のシャードでのサービスのデータ レイヤの状態を表示します。 （注） 例については、例 （94 ページ）を参照してください。
acidiag rvread *service shard replica*	特定のシャードとレプリカでのサービスのデータ レイヤの状態を表示します。 （注） 例については、例 （94 ページ） を参照してください。
validateimage	イメージをファームウェア リポジトリにロードする前に、イメージを検証できます。この関数は、リポジトリに追加されるイメージのプロセスの通常の一部として実行されることに注意してください。
validateenginxconf	APIC で生成された nginx 構成ファイルを検証して、nginx がその構成ファイルで起動できることを確認します。これは、nginx Web サーバーが APIC で実行されていない場合のデバッグでの使用を目的としています。

サービス ID

次の表にリストされているサービス ID は、**man acidiag** コマンドを入力するときにも表示されます。

表 *2:* サービス *ID*

サービス	ID
cliD	1
コントローラ	2
eventmgr	3
extXMLApi	4
ポリシー要素	5
policymgr	6
リーダー	7

サービス	ID
AE	8
topomgr	9
observer	10
dbgr	11
observerelem	12
dbgrelem	13
vmmmgr	14
nxosmock	15
bootmgr	16
appliancedirector	17
adrelay	18 日
ospaagent	19
vleafelem	20
dhcpd	21
scripthandler	22
idmgr	23
ospaelem	24
osh	25
opflexagent	26
opflexelem	27
confelem	28
vtap	29
snmpd	30
opflexp	31
分析	32
policydist	33
plghandler	34
domainmgr	35

サービス	ID
licensemgr	36
なし	37
platformmgr	38
edmgr	39

表 *3:* データの状態

州	ID
コマトーセ	0
NEWLY_BORN	1
不明ファイル	2
DATA_LAYER_DIVERGED	11
DATA_LAYER_DEGRADED_LEADERSHIP	12
DATA_LAYER_ENTIRELY_DIVERGED	111
DATA_LAYER_PARTIALLY_DIVERGED	112
DATA_LAYER_ENTIRELY_DEGRADED_LEADERSHIP	121
DATA_LAYER_PARTIALLY_DEGRADED_LEADERSHIP	122
FULLY_FIT	255

システムのキーワード

```
acidiag [start|stop|restart] [mgmt|xinetd]

acidiag installer  -u imageurl -c

acidiag reboot

acidiag  touch [clean|setup]

acidiag verifyapic
```

構文の説明

オプション	機能
-c	クリーン インストールを指定します
-u	APIC イメージの URL を指定します。
imageurl	APIC イメージを指定します。

オプション	機能
installer	APIC に新しいイメージをインストールします。-cでクリーンインストールを実行します。
mgmt	上のすべてのサービスを指定します。APIC
reboot	APICを再起動します。
restart	APIC でサービスを再起動します。
start	APIC でサービスを開始します。
stop	APIC でサービスを停止します。
touch [clean | setup]	APIC の構成をリセットします。 • **clean** オプションは、APIC ネットワーク構成（ファブリック名、IP アドレス、ログインなど）を保持しますが、すべてのポリシー データを削除します。 • **setup** オプションは、ポリシー データと APIC ネットワーク構成の両方を削除します。
verifyapic	APIC ソフトウェアのバージョンを表示します。
xinetd	sshおよびtelnetデーモンを制御するxinetd（拡張インターネット デーモン）サービスを指定します。5.3(1) リリース以降、telnet はサポートされていません。

診断キーワード

```
acidiag crashsuspecttracker

acidiag dbgtoken

acidiag version
```

構文の説明

オプション	機能
crashsuspecttracker	クラッシュを示すサービスまたはデータのサブセットの状態を追跡します。
dbgtoken	root パスワードの生成に使用するトークンを生成します。これは、必要な場合には、TAC と連携しながら、その指示どおりに使用してください。

オプション	機能
version	APIC ISO ソフトウェアのバージョンを表示します。

例

次に、**acidiag** コマンドの使用例を示します。

```
apic1# acidiag version 2.2.1o


apic1# acidiag verifyapic
openssl_check: certificate details
subject= CN=ABC12345678,serialNumber=PID:APIC-SERVER-L1 SN:ABC12345678
issuer= CN=Cisco Manufacturing CA,O=Cisco Systems
notBefore=Sep 28 17:17:42 2016 GMT
notAfter=Sep 28 17:27:42 2026 GMT
openssl_check: passed
ssh_check: passed
all_checks: passed


apic1# acidiag avread
Local appliance ID=1 ADDRESS=10.0.0.1 TEP ADDRESS=10.0.0.0/16 ROUTABLE IP ADDRESS=0.0.0.0
 CHASSIS_ID=1009f750-adab-11e9-a044-8dbd212cd556
Cluster of 7 lm(t):1(2019-08-08T01:02:17.961-07:00) appliances (out of targeted 7
lm(t):7(2019-08-08T03:50:57.240-07:00)) with FABRIC_DOMAIN name=ACI Fabric1 set to
version=apic-4.2(0.235j) lm(t):1(2019-08-17T01:09:16.413-07:00); discoveryMode=PERMISSIVE
 lm(t):0(1969-12-31T17:00:00.007-07:00); drrMode=OFF
lm(t):0(1969-12-31T17:00:00.007-07:00); kafkaMode=OFF
lm(t):0(1969-12-31T17:00:00.007-07:00)
        appliance id=1  address=10.0.0.1 lm(t):1(2019-08-08T01:02:08.544-07:00) tep
address=10.0.0.0/16 lm(t):1(2019-08-08T01:02:08.544-07:00) routable address=0.0.0.0
lm(t):1(zeroTime) oob address=172.23.96.10/21 lm(t):1(2019-08-08T01:02:18.218-07:00)
version=4.2(0.235j) lm(t):1(2019-08-15T15:22:00.158-07:00)
chassisId=1009f750-adab-11e9-a044-8dbd212cd556 lm(t):1(2019-08-15T15:22:00.158-07:00)
capabilities=0X3EEFFFFFFFFF--0X2020--0X7F lm(t):1(2019-08-17T01:13:46.997-07:00)
rK=(stable,present,0X206173722D687373) lm(t):1(2019-08-08T01:02:18.228-07:00)
aK=(stable,present,0X206173722D687373) lm(t):1(2019-08-08T01:02:18.228-07:00)
oobrK=(stable,present,0X206173722D687373) lm(t):1(2019-08-08T01:02:18.228-07:00)
oobaK=(stable,present,0X206173722D687373) lm(t):1(2019-08-08T01:02:18.228-07:00)
cntrlSbst=(APPROVED, FCH1748V0SZ) lm(t):1(2019-08-15T15:22:00.158-07:00) (targetMbSn=
lm(t):0(zeroTime), failoverStatus=0 lm(t):0(zeroTime)) podId=1
lm(t):1(2019-08-08T01:02:08.544-07:00) commissioned=YES lm(t):1(zeroTime) registered=YES
 lm(t):1(2019-08-08T01:02:08.544-07:00) standby=NO lm(t):1(2019-08-08T01:02:08.544-07:00)
 DRR=NO lm(t):0(zeroTime) apicX=NO lm(t):1(2019-08-08T01:02:08.544-07:00) virtual=NO
lm(t):1(2019-08-08T01:02:08.544-07:00) active=YES(2019-08-08T01:02:08.544-07:00)
health=(applnc:255 lm(t):1(2019-08-17T01:39:26.296-07:00) svc's)
        appliance id=2  address=10.0.0.2 lm(t):7(2019-08-08T03:50:55.470-07:00) tep
address=10.0.0.0/16 lm(t):2(2019-07-23T17:51:38.997-07:00) routable address=0.0.0.0
lm(t):0(zeroTime) oob address=172.23.96.11/21 lm(t):1(2019-08-18T23:14:28.720-07:00)
version=4.2(0.235j) lm(t):2(2019-08-15T15:22:00.300-07:00)
chassisId=694e6a98-adac-11e9-ad79-d1f60e3ee822 lm(t):2(2019-08-15T15:22:00.300-07:00)
capabilities=0X3EEFFFFFFFFF--0X2020--0X2 lm(t):2(2019-08-14T07:55:10.074-07:00)
rK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.829-07:00)
aK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.829-07:00)
oobrK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.829-07:00)
oobaK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.829-07:00)
cntrlSbst=(APPROVED, FCH1748V0MS) lm(t):2(2019-08-15T15:22:00.300-07:00) (targetMbSn=
lm(t):0(zeroTime), failoverStatus=0 lm(t):0(zeroTime)) podId=1
lm(t):2(2019-08-08T01:42:03.670-07:00) commissioned=YES
```

```
lm(t):1(2019-08-08T01:02:17.961-07:00) registered=YES
lm(t):7(2019-07-24T15:24:25.693-07:00) standby=NO lm(t):2(2019-08-08T01:42:03.670-07:00)
 DRR=NO lm(t):1(2019-08-08T01:02:17.961-07:00) apicX=NO
lm(t):2(2019-08-08T01:42:03.670-07:00) virtual=NO lm(t):0(zeroTime)
active=YES(2019-08-13T17:02:32.983-07:00) health=(applnc:255
lm(t):2(2019-08-17T01:32:51.454-07:00) svc's)
        appliance id=3  address=10.0.0.3 lm(t):7(2019-08-08T03:50:55.470-07:00) tep
address=10.0.0.0/16 lm(t):3(2019-07-23T19:05:56.405-07:00) routable address=0.0.0.0
lm(t):0(zeroTime) oob address=172.23.96.12/21 lm(t):1(2019-08-18T23:14:28.721-07:00)
version=4.2(0.235j) lm(t):3(2019-08-15T15:21:59.893-07:00)
chassisId=1f98b916-adb7-11e9-a6f8-abe00a04e8e6 lm(t):3(2019-08-15T15:21:59.893-07:00)
capabilities=0X3EEFFFFFFFFF--0X2020--0X4 lm(t):3(2019-08-14T07:55:22.256-07:00)
rK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.824-07:00)
aK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.824-07:00)
oobrK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.824-07:00)
oobaK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.824-07:00)
cntrlSbst=(APPROVED, FCH1930V1X6) lm(t):3(2019-08-15T15:21:59.893-07:00) (targetMbSn=
lm(t):0(zeroTime), failoverStatus=0 lm(t):0(zeroTime)) podId=1
lm(t):3(2019-08-08T02:15:20.560-07:00) commissioned=YES
lm(t):2(2019-08-08T01:42:15.337-07:00) registered=YES
lm(t):7(2019-07-24T15:24:25.693-07:00) standby=NO lm(t):3(2019-08-08T02:15:20.560-07:00)
 DRR=NO lm(t):2(2019-08-08T01:42:15.337-07:00) apicX=NO
lm(t):3(2019-08-08T02:15:20.560-07:00) virtual=NO lm(t):0(zeroTime)
active=YES(2019-08-13T17:02:33.182-07:00) health=(applnc:255
lm(t):3(2019-08-15T16:08:46.119-07:00) svc's)
        appliance id=4  address=10.0.0.4 lm(t):7(2019-08-08T03:50:55.470-07:00) tep
address=10.0.0.0/16 lm(t):4(2019-07-23T17:46:15.545-07:00) routable address=0.0.0.0
lm(t):0(zeroTime) oob address=172.23.97.231/21 lm(t):1(2019-08-18T23:14:28.717-07:00)
version=4.2(0.235j) lm(t):4(2019-08-15T15:22:00.669-07:00)
chassisId=3a7f38aa-adac-11e9-8869-a9e520cdc042 lm(t):4(2019-08-15T15:22:00.669-07:00)
capabilities=0X3EEFFFFFFFFF--0X2020--0X8 lm(t):4(2019-08-14T07:54:59.490-07:00)
rK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.825-07:00)
aK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.825-07:00)
oobrK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.825-07:00)
oobaK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.825-07:00)
cntrlSbst=(APPROVED, FCH1902V1WW) lm(t):4(2019-08-15T15:22:00.669-07:00) (targetMbSn=
lm(t):0(zeroTime), failoverStatus=0 lm(t):0(zeroTime)) podId=1
lm(t):4(2019-08-08T02:40:09.610-07:00) commissioned=YES
lm(t):3(2019-08-08T02:15:32.613-07:00) registered=YES
lm(t):7(2019-07-24T15:24:25.693-07:00) standby=NO lm(t):4(2019-08-08T02:40:09.610-07:00)
 DRR=NO lm(t):3(2019-08-08T02:15:32.613-07:00) apicX=NO
lm(t):4(2019-08-08T02:40:09.610-07:00) virtual=NO lm(t):0(zeroTime)
active=YES(2019-08-15T15:21:59.914-07:00) health=(applnc:255
lm(t):4(2019-08-17T01:39:26.477-07:00) svc's)
        appliance id=5  address=10.0.0.5 lm(t):7(2019-08-08T03:50:55.470-07:00) tep
address=10.0.0.0/16 lm(t):5(2019-07-23T19:05:11.089-07:00) routable address=0.0.0.0
lm(t):0(zeroTime) oob address=172.23.97.232/21 lm(t):1(2019-08-18T23:14:28.723-07:00)
version=4.2(0.235j) lm(t):5(2019-08-15T15:22:00.248-07:00)
chassisId=35428666-adb7-11e9-a315-1d7671b518b3 lm(t):5(2019-08-15T15:22:00.248-07:00)
capabilities=0X3EEFFFFFFFFF--0X2020--0X10 lm(t):5(2019-08-14T07:55:19.573-07:00)
rK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.854-07:00)
aK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.854-07:00)
oobrK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.854-07:00)
oobaK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.854-07:00)
cntrlSbst=(APPROVED, FCH1902V1EG) lm(t):5(2019-08-15T15:22:00.248-07:00) (targetMbSn=
lm(t):0(zeroTime), failoverStatus=0 lm(t):0(zeroTime)) podId=1
lm(t):5(2019-08-08T03:03:50.338-07:00) commissioned=YES
lm(t):4(2019-08-08T02:40:15.939-07:00) registered=YES
lm(t):7(2019-07-24T15:24:25.693-07:00) standby=NO lm(t):5(2019-08-08T03:03:50.338-07:00)
 DRR=NO lm(t):4(2019-08-08T02:40:15.939-07:00) apicX=NO
lm(t):5(2019-08-08T03:03:50.338-07:00) virtual=NO lm(t):0(zeroTime)
active=YES(2019-08-15T15:21:59.756-07:00) health=(applnc:255
lm(t):5(2019-08-17T01:32:43.730-07:00) svc's)
        appliance id=6  address=10.0.0.6 lm(t):7(2019-08-08T03:50:55.470-07:00) tep
```

```
address=10.0.0.0/16 lm(t):6(2019-07-23T19:39:41.972-07:00) routable address=0.0.0.0
lm(t):0(zeroTime) oob address=172.31.170.230/21 lm(t):1(2019-08-18T23:14:28.727-07:00)
version=4.2(0.235j) lm(t):6(2019-08-15T15:22:00.562-07:00)
chassisId=066c943a-adbc-11e9-bbed-257398025731 lm(t):6(2019-08-15T15:22:00.562-07:00)
capabilities=0X3EEFFFFFFFFF--0X2020--0X20 lm(t):6(2019-08-14T07:55:20.053-07:00)
rK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.820-07:00)
aK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.821-07:00)
oobrK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.821-07:00)
oobaK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.821-07:00)
cntrlSbst=(APPROVED, WZP22350JFT) lm(t):6(2019-08-15T15:22:00.562-07:00) (targetMbSn=
lm(t):0(zeroTime), failoverStatus=0 lm(t):0(zeroTime)) podId=9
lm(t):6(2019-08-08T03:28:11.246-07:00) commissioned=YES
lm(t):5(2019-08-08T03:03:57.387-07:00) registered=YES
lm(t):7(2019-07-24T15:24:25.693-07:00) standby=NO lm(t):6(2019-08-08T03:28:11.246-07:00)
 DRR=NO lm(t):5(2019-08-08T03:03:57.387-07:00) apicX=NO
lm(t):6(2019-08-08T03:28:11.246-07:00) virtual=NO lm(t):0(zeroTime)
active=YES(2019-08-13T17:30:37.663-07:00) health=(applnc:255
lm(t):6(2019-08-15T15:57:05.128-07:00) svc's)
        appliance id=7  address=10.0.0.7 lm(t):7(2019-08-08T03:50:48.149-07:00) tep
address=10.0.0.0/16 lm(t):7(2019-07-24T15:24:19.988-07:00) routable address=0.0.0.0
lm(t):0(zeroTime) oob address=172.31.172.157/21 lm(t):1(2019-08-18T23:14:28.722-07:00)
version=4.2(0.235j) lm(t):7(2019-08-15T15:22:00.539-07:00)
chassisId=859be4ae-ae61-11e9-9840-7d9d67698989 lm(t):7(2019-08-15T15:22:00.539-07:00)
capabilities=0X3EEFFFFFFFFF--0X2020--0X40 lm(t):7(2019-08-14T07:55:23.872-07:00)
rK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.824-07:00)
aK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.824-07:00)
oobrK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.824-07:00)
oobaK=(stable,present,0X206173722D687373) lm(t):1(2019-08-15T15:22:00.824-07:00)
cntrlSbst=(APPROVED, FCH2051V116) lm(t):7(2019-08-15T15:22:00.539-07:00) (targetMbSn=
lm(t):0(zeroTime), failoverStatus=0 lm(t):0(zeroTime)) podId=10
lm(t):7(2019-08-08T03:50:48.149-07:00) commissioned=YES
lm(t):6(2019-08-08T03:28:16.727-07:00) registered=YES
lm(t):6(2019-07-24T15:27:25.518-07:00) standby=NO lm(t):7(2019-08-08T03:50:48.149-07:00)
 DRR=NO lm(t):6(2019-08-08T03:28:16.727-07:00) apicX=NO
lm(t):7(2019-08-08T03:50:48.149-07:00) virtual=NO lm(t):0(zeroTime)
active=YES(2019-08-13T17:30:45.488-07:00) health=(applnc:255
lm(t):7(2019-08-17T01:39:26.549-07:00) svc's)
------------------------------------------------
clusterTime=<diff=2817 common=2019-08-19T15:33:55.929-07:00
local=2019-08-19T15:33:53.112-07:00 pF=<displForm=0 offsSt=0 offsVlu=-25200
lm(t):7(2019-08-08T03:50:55.925-07:00)>>
------------------------------------------------


apic1# acidiag rvread 6 3 1
(6,3,1)  st:6 lm(t):3(2014-10-16T08:48:20.238+00:00) le: reSt:LEADER voGr:0 cuTerm:0x19
 lCoTe:0x18
   lCoIn:0x1800000000001b2a veFiSt:0x31 veFiEn:0x31 lm(t):3(2014-10-16T08:48:20.120+00:00)

    lastUpdt 2014-10-16T09:07:00.214+00:00
------------------------------------------------
clusterTime=<diff=65247252 common=2014-10-16T09:07:01.837+00:00
local=2014-10-15T14:59:34.585+00:00
    pF=<displForm=0 offsSt=0 offsVlu=0 lm(t):3(2014-10-16T04:50:08.714+00:00)>>


apic1# acidiag rvread 6 3
(6,3,1)  st:6 lm(t):3(2014-10-16T08:48:20.238+00:00) le: reSt:LEADER voGr:0 cuTerm:0x19
 lCoTe:0x18
   lCoIn:0x1800000000001b2a veFiSt:0x31 veFiEn:0x31 lm(t):3(2014-10-16T08:48:20.120+00:00)

    lastUpdt 2014-10-16T09:08:30.240+00:00
(6,3,2)  st:6 lm(t):1(2014-10-16T08:47:25.323+00:00) le: reSt:FOLLOWER voGr:0 cuTerm:0x19
 lCoTe:0x18
   lCoIn:0x1800000000001b2a veFiSt:0x49 veFiEn:0x49 lm(t):1(2014-10-16T08:48:20.384+00:00)
```

```
 lp: clSt:2
    lm(t):1(2014-10-16T08:47:03.286+00:00) dbSt:2 lm(t):1(2014-10-16T08:47:02.143+00:00)
 stMmt:1
     lm(t):0(zeroTime) dbCrTs:2014-10-16T08:47:02.143+00:00 lastUpdt
2014-10-16T08:48:20.384+00:00
(6,3,3)  st:6 lm(t):2(2014-10-16T08:47:13.576+00:00) le: reSt:FOLLOWER voGr:0 cuTerm:0x19
 lCoTe:0x18
    lCoIn:0x1800000000001b2a veFiSt:0x43 veFiEn:0x43 lm(t):2(2014-10-16T08:48:20.376+00:00)

     lastUpdt 2014-10-16T09:08:30.240+00:00
-------------------------------------------
clusterTime=<diff=65247251 common=2014-10-16T09:08:30.445+00:00
local=2014-10-15T15:01:03.194+00:00
    pF=<displForm=0 offsSt=0 offsVlu=0 lm(t):3(2014-10-16T04:50:08.714+00:00)>>
```

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