トラブルシューティングのツールと方法論

この章の内容は、次のとおりです。

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

管理者はあらゆる外部ホストに対して統計情報、テクニカル サポートの収集、エラーおよびイベントをエクスポートし、ファブリック（APICおよびスイッチ）からコア ファイルとデバッグ データを処理するエクスポート ポリシーをAPICで設定することができます。 エクスポートはXML、JSON、Web ソケット、SCP、HTTP などのさまざまな形式にできます。 エクスポートはサブスクライブでき、定期的またはオンデマンドでストリーミングできます。

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。

アウトオブバンド DNS 接続

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

ファイル エクスポート用のリモート ロケーションの作成

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

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

オンデマンド テクニカルサポート ファイルの送信

ステップ 1 メニュー バーで、[Admin] をクリックします。
ステップ 2 サブメニュー バーで、[Import/Export] をクリックします。
ステップ 3 [Navigation] ペインで、[Export Policies] を展開します。
ステップ 4 [On-demand TechSupport] を右クリックし、[Create On-demand TechSupport] を選択します。
ステップ 5 [Create On-demand TechSupport] ダイアログボックスで、次の操作を実行します。
a) [Name] フィールドに、テクニカルサポート ファイルのエクスポート ポリシーの名前を入力します。

b) [Export Destination] ドロップダウン リストから、テクニカルサポート ファイルを受信する送信先ホストのプロファイルを選択します。
必要な送信先のプロファイルが表示されない場合は、[Create Remote Path of a File] を選択してここで定義します。
c) [Data Container] ドロップダウン リストから、uni/fabric/tscont を選択します。
d) 必要なソースデバイス（リーフまたはスパイン）が表示されない場合は、[Source Nodes] テーブルで、+ アイコンをクリックし、デバイスを選択して、[Update] をクリックします。
e) [Source Nodes] テーブルで送信元名をダブルクリックし、ドロップダウン リストの右にある青のアイコンをクリックして、ソース デバイスの [System Information] ウィンドウを開きます。
ソース デバイスの情報を確認するには、タブを使用します。
f) [State] フィールドで、[triggered] オプション ボタンをクリックして、ファイルを送信できるようにします。
g) [Submit] をクリックして、テクニカルサポート ファイルを送信します。

（注） オンデマンドのテクニカルサポート ファイルは別の APIC に保存し、ストレージと CPU 条件のバランスを取ることができます。 場所を確認するには、[Navigation] ペインでオンデマンドのテクニカルサポート ポリシーをクリックし、[Work] ペインで [OPERATIONAL] タブをクリックします。 コントローラが [EXPORT LOCATION] フィールドに表示されます。

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 カウンタはファブリックのドロップやミスルートを検出し、迅速なデバッグとアプリケーション接続問題の分離を可能にします。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。 送信元リーフと送信先リーフ以外のリーフにノンゼロのカウンタがあると、管理者はそのリーフをドリル ダウンできます。

従来の設定では、baremetal 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量をモニタリングするのはほぼ不可能です。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 baremetal 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 ツー リーフ（TEP ツー TEP）のアトミック カウンタは、次のことを提供できます。

- ドロップ、承認および超過パケットのカウント
- 最後の 30 秒などの短期データ収集、5 分、15 分、またはそれ以上などの長期データ収集
- スパインごとのトラフィックの詳細
- 継続的なモニタリング

テナントのアトミック カウンタは次の機能を提供できます。

- ドロップ、承認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。
  - エンドポイント ツー エンドポイント
  - オプションのドリル ダウン付きの EPG ツー EPG
  - EPG ツー エンドポイント
  - EPG ツー *（任意）
  - エンドポイント ツー外部 IP アドレス

アトミック カウンタに関する注意事項および制約事項

- IP アドレスが認識されないピュア レイヤ 2 設定（IP アドレスは 0.0.0.0）では、EP から EPG および EPG から EP のアトミック カウンタ ポリシーはサポートされていません。 この場合、EP から EP および EPG から EPG のポリシーはサポートされています。 外部ポリシーは VRF ベースで、認識された IP アドレスが必要であり、サポートされています。
- アトミック カウンタの送信元または送信先が EP である場合、EP は静的ではなく動的でなければいけません。 動的 EP （fv:CEp）と異なり、静的 EP （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。
- 両方の EPG が同じリーフに対してローカルな EPG から EPG のポリシーでは、送信カウンタのみ更新されます。
- リーフのスイッチがすべてのスパイン スイッチに対して完全メッシュにないトランジット トポロジでは、リーフからリーフ（TEPからTEP）のカウンタは予期どおりに動作しません。
- 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。
- アトミック カウンタ関連の制限については、『*Cisco ACI Verified Scalability Limits*』 を参照してください。

アトミック カウンタの設定

ステップ 1 メニュー バーで、[Tenants] をクリックします。

ステップ 2 サブメニュー バーで、必要なテナントをクリックします。

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

ステップ 4 [Troubleshoot Policies] の下で [Atomic Counter Policy] を拡張し、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。
必要な識別情報は送信元のタイプ（エンドポイント、エンドポイント 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) トラフィックの送信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、および送信元と送信先の 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、アプリケーション セントリック インフラストラクチャ 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。 各デバイスで SNMP サービスを有効または無効にするように選択できます。 また、各デバイスで SNMP v1 および v2 要求の処理方法を設定できます。

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

SNMP の設定

GUI による SNMP の設定

この手順では、APIC で SNMP エージェントを設定し、有効にします。

ステップ 1 メニュー バーで、[Fabric] をクリックします。

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

ステップ 3 [Navigation] ペインで、[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。

ステップ 6 [Create SNMP 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、SNMP ポリシーの名前を入力します。

b) [Admin State] フィールドで、オプション ボタンをクリックして、[Enabled] を選択します。

c) [Community Policies] テーブルで + アイコンをクリックし、名前を入力して、[Update] をクリックします。

d) （任意） [SNMP v3 Users] テーブルで + アイコンをクリックし、名前を入力して、ユーザの認証データを入力し、[Update] をクリックします。
この手順は SNMPv3 アクセスが必要な場合のみ実行します。

ステップ 7 （任意） [Create SNMP Policy] ダイアログボックスで、次のオプションの操作を実行し、許可された SNMP 管理ステーションを設定します。

a) [Client Group Policies] テーブルで + アイコンをクリックし、[Create SNMP Client Group Profile] ダイアログボックスを開きます。

b) [Name] フィールドに、SNMP クライアント グループのプロファイル名を入力します。

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

d) [Client Entries] テーブルで + アイコンをクリックします。

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

ステップ 8 [OK] をクリックします。

ステップ 9 [Submit] をクリックします。

ステップ 10 [Pod Policies] の下で [Policy Groups] を拡張して、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。

ステップ 11 [Create POD Policy Group] ダイアログボックスで、

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] で、[default] をクリックします。

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

ステップ 14 [Submit] をクリックします。

ステップ 15 [OK] をクリックします。

GUI による SNMP トラップ通知先の設定

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

ステップ 1 メニュー バーで、[Admin] をクリックします。

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

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

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

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

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

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

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

d) 通知先のポート番号と SNMP バージョンを選択します。

e) SNMP v1 または v2c 通知先の場合、[Security Name] として設定したコミュニティ名の 1 つを入力し、[v3 Security Level] として noauth を選択します。

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

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

h) [OK] をクリックします。

i) [Finish] をクリックします。

GUI による SNMP トラップ ソースの設定

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

ステップ 1 メニュー バーで、[Fabric] をクリックします。

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

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

ステップ 4 必要なモニタリング ポリシーを拡張し、[Callhome/SNMP/Syslog] を選択します。
[Common Policy] を選択する場合は、[Common Policy] を右クリックして、[Create SNMP Source] を選択し、そのダイアログボックスで次の手順に従ってください。

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

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

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

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

a) [Name] フィールドに、SNMP ポリシーの名前を入力します。
b) [Include] フィールドで、必要な通知タイプ（イベント、監査ログ、エラー）のチェックボックスをオンにします。
c) [Min Severity] ドロップダウン リストから、通知をトリガーする [Info] 重大度レベルを選択します。
d) [Dest Group] ドロップダウン リストから、通知を送信する既存の通知先を選択するか、または [Create SNMP Trap Destination Group] を選択して新しい通知先を作成します。
SNMP トラップの通知先グループを作成する手順は、別項で説明します。
e) [Submit] をクリックします。

SPAN の使用

SPAN の概要

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

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

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

マルチノード SPAN

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

SPAN の注意事項と制約事項

- SPAN はトラブルシューティングのために使用します。 SPAN トラフィックはスイッチ リソースのユーザ トラフィックと競合します。 負荷を最小限にするには、分析対象の特定のトラフィックだけをコピーするように SPAN を設定します。
- SPAN 送信元として l3extLIfP のレイヤ 3 サブインターフェイスを指定することはできません。外部ソースからのトラフィックをモニタリングするためにはポート全体を使用します。
- アクティブな SPAN セッションの最大数など、SPAN 関連の制限については、『*Cisco ACI Verified Scalability Limits*』 を参照してください。

SPAN セッションの設定

この手順では、複製されたソース 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 SPAN ポリシーを設定する方法を示します。

ステップ 1 メニュー バーで、[Tenants] をクリックします。

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

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

ステップ 4 [SPAN] の下で [SPAN Destination Groups] を右クリックし、[Create SPAN Destination Group] を選択します。

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

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

ステップ 6 [SPAN] の下で [SPAN Source Groups] を右クリックし、[Create SPAN Source Group] を選択します。

ステップ 7 [Create SPAN Source Group] ダイアログボックスで、次の操作を実行します。

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

i) [Submit] をクリックして、SPAN 送信元グループを保存します。

次の作業

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

トレースルートの使用

トレースルートの概要

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

テナントのエンドポイントから開始された 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のゲートウェイを示します。

トレースルートはエンドポイントからエンドポイント、およびリーフからリーフ（トンネル エンドポイント、またはTEP から TEP）を含むさまざまなモードをサポートします。 トレースルートはファブリック全体のすべてのパスを検出し、外部エンドポイントの出口を検出します。パスが妨げられているかどうかを発見するのに役立ちます。

トレースルートの注意事項および制約事項

- トレースルートの送信元または送信先が EP の場合、EP は静的ではなく動的でなければいけません。 動的 EP（fv:CEp）とは異なり、静的 EP （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。
- トレースルート関連の制限については、『*Cisco ACI Verified Scalability Limits*』 を参照してください。

EPG 間のトレースルートの実行

この手順では、2 つのエンドポイント間のパスをテストし、表示するトレースルートの設定と実行の方法を示します。

ステップ 1 メニュー バーで、[Tenants] をクリックします。

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

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

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

ステップ 5 [Create Endpoint-to-Endpoint Traceroute Policy] ダイアログボックスで、次の操作を実行します。

a) [Name] フィールドにトレースルート ポリシーの名前を入力します。

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

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

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

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

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

g) [Submit] をクリックして、トレースルートを起動します。

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

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

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

（注） 複数のパスが発信元ノードから送信先まで横断している場合があります。

見やすくするには、[名前] カラムなど、1 つまたは複数のカラムの幅を広げます。