Cisco APIC Troubleshooting Guide

最終更新：2016 年 06 月 30 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

新機能および変更された機能に関する情報

次の表は、この最新リリースまでのガイドでの主な変更点の概要を示したものです。ただし、このリリースまでのこのガイドの変更点や新機能の中には一部、この表に記載されていないものもあります。

Cisco APIC のリリース バージョン	機能	説明
Release 1.2(2)	アップリンク障害検出のためのポート トラッキング ポリシー	アップリンク障害検出は、ファブリック アクセス グローバル ポート トラッキング ポリシーで有効にできます。ポート トラッキング ポリシーが、リーフ スイッチとスパイン スイッチとの間のリンクの状態を監視します。有効なポート トラッキング ポリシーがトリガーされると、リーフ スイッチは、EPGが展開されているスイッチのすべてのアクセス インターフェイスを停止します。リーフ スイッチのモデルに応じて、各リーフ スイッチは、各スパイン スイッチへの 6、8、または 12 個のアップリンク接続を持つことができます。ポート トラッキング ポリシーは、ポリシーをトリガーするアップリンク接続の数と、指定のアップリンク数を超過した後にリーフ スイッチ アクセス ポートを復旧するまでの遅延タイマーを指定します。

Cisco APIC のリリース バージョン	機能	説明
Release 1.2(2)	設定ゾーン	設定ゾーンは、ACI ファブリックを、さまざまなタイミングで実行される設定変更により更新できる多様なゾーンに分割します。これにより、トラフィックを中断したりファブリックをダウンさせたりする可能性もある、障害ファブリック全体の設定を展開してしまうリスクが制限されます。管理者はクリティカルではないゾーンに設定を展開し、それが適切であることを確認した時点でクリティカルゾーンに展開できます。注：無効にされた設定ゾーンに属するノードは、アップグレードまたはダウングレードしないでください。

はじめに

この前書きは、次の項で構成されています。

対象読者

このガイドは、データ システム、ネットワーク、ストレージ システムのトラブルシューティングに関して経歴があるシステムおよびネットワーク エンジニアを対象としています。

表記法

コマンドの説明には、次のような表記法が使用されます。

表記法	説明
bold	太字の文字は、表示どおりにユーザが入力するコマンドおよびキーワードです。
italic	イタリック体の文字は、ユーザが値を入力する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角カッコで囲んで示しています。
[x | y]	いずれか 1 つを選択できる省略可能なキーワードや引数は、角カッコで囲み、縦棒で区切って示しています。

表記法	説明
{x | y}	必ずいずれか1つを選択しなければならない必須キーワードや引数は、波カッコで囲み、縦棒で区切って示しています。
[x {y | z}]	角カッコまたは波カッコが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。角カッコ内の波カッコと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
`variable`	ユーザが値を入力する変数であることを表します。イタリック体が使用できない場合に使用されます。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。

例では、次の表記法を使用しています。

表記法	説明
`screen フォント`	スイッチが表示する端末セッションおよび情報は、screen フォントで示しています。
`太字の screen フォント`	ユーザが入力しなければならない情報は、太字の screen フォントで示しています。
イタリック体の *screen* フォント	ユーザが値を指定する引数は、イタリック体の screen フォントで示しています。
< >	パスワードのように出力されない文字は、山カッコ（<>）で囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

このマニュアルでは、次の表記法を使用しています。

（注） 「注釈」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

警告 IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger.You are in a situation that could cause bodily injury.Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

関連資料

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）のマニュアル

ACL のマニュアルは、次の URL で入手できます。http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html

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）シミュレータのマニュアル

Cisco ACI Simulator のマニュアルは、次の URL から入手できます。http://www.cisco.com/c/en/us/support/cloud-systems-management/application-centric-infrastructure-simulator/tsd-products-support-series-home.html。

Cisco Nexus 9000 シリーズ スイッチのマニュアル

Cisco Nexus 9000 シリーズ スイッチのマニュアルは、次の URL で入手できます。http://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/tsd-products-support-series-home.html

Cisco Application Virtual Switch のマニュアル

Cisco Application Virtual Switch（AVS）のマニュアルは、次の URL で入手できます。http://www.cisco.com/c/en/us/support/switches/application-virtual-switch/tsd-products-support-series-home.html

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）と OpenStack の統合に関するマニュアル

Cisco ACI と OpenStack の統合に関するマニュアルは、次の URL から入手できます。http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html

マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、apic-docfeedback@cisco.com までご連絡ください。ご協力をよろしくお願いいたします。

第 1 章

トラブルシューティングのツールと方法論

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。

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。

ファイルのエクスポートに関するガイドラインと制約事項

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

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

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

ファイル エクスポート用のリモート ロケーションの作成

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

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

g) [Submit] をクリックします。`

オンデマンド テクニカルサポート ファイルの送信

ステップ 1 メニュー バーで、[Admin] をクリックします。

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

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

ステップ 4 [On-demand TechSupport] を右クリックし、[Create On-demand TechSupport] を選択します。

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

a) [Name] フィールドに、テクニカルサポート ファイルのエクスポート ポリシーの名前を入力します。

b) ファイルをリモート宛先ではなくコントローラにエクスポートする場合は、[Export to Controller] を選択します。

c) [Export Destination] ドロップダウン リストから、テクニカルサポート ファイルを受信する宛先ホストのプロファイルを選択します。
目的の宛先のプロファイルが表示されない場合は、[Create Remote Location] を選択してここで定義します。

d) [Data Container] ドロップダウン リストから、[uni/fabric/tscont] を選択します。

e) 目的の送信元デバイス（リーフまたはスパイン）が [Source Nodes] テーブルに表示されない場合は、[+] アイコンをクリックし、デバイスを選択して、[Update] をクリックします。

f) [Source Nodes] テーブルで送信元名をダブルクリックし、ドロップダウン リストの右にある青のアイコンをクリックして、ソース デバイスの [System Information] ウィンドウを開きます。
ソース デバイスの情報を確認するには、タブを使用します。

g) [State] フィールドで、[triggered] オプション ボタンをクリックして、ファイルを送信できるようにします。

h) [Submit] をクリックして、テクニカルサポート ファイルを送信します。

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

i) ポリシー名を右クリックし、[Collect Tech Support] を選択します。

j) [Yes] を選択して、テクニカル サポート情報の収集を開始します。

Syslog の使用

Syslog について

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

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

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

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

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

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

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

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

Syslog の宛先および宛先グループの作成

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

ステップ 1 メニュー バーで、[Admin] をクリックします。

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

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

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

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

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

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

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

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

e) [Next] をクリックします。

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

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

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

b) （任意） [Name] フィールドに、宛先ホストの名前を入力します。

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

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

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

f) [OK] をクリックします。

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

ステップ 8 [Finish] をクリックします。

Syslog 送信元の作成

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

はじめる前に

syslog モニタリング宛先グループを作成します。

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

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

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

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

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

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

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

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

ステップ 7 [+] をクリックして syslog 送信元を作成します。

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

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

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

アトミック カウンタの使用

アトミック カウンタについて

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

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

リーフ間（TEP 間）のアトミック カウンタは次を提供できます。

- 送信パケット、受信パケット、ドロップ パケット、および超過パケットのカウント
  - 送信パケット：送信数は、送信元 TEP（トンネル エンドポイント）から宛先 TEP に送信されたパケット数を表します。
  - 受信パケット：受信数は、宛先TEPが送信元TEPから受信したパケット数を表します。
  - ドロップパケット：ドロップ数は、伝送中にドロップされたパケット数を表します。この数値は、送信パケット量と受信パケット量の差です。
  - 超過パケット：超過数は、伝送中に受信された超過パケット数を表します。この数値は、転送の不一致または間違った場所へのルーティングミスによって予期せず受信されたパケット量です。

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

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

テナントのアトミック カウンタは次を提供できます:

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

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

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

アトミック カウンタに関する注意事項および制約事項

- アトミック カウンタの使用は、エンドポイントが異なるテナントまたは同じテナント内の異なるコンテキスト（VRF）にある場合はサポートされません。
- IP アドレスが学習されない純粋なレイヤ 2 設定（IP アドレスは 0.0.0.0）では、エンドポイント/EPG 間および EPG/エンドポイント間のアトミック カウンタ ポリシーはサポートされませ

ん。この場合、エンドポイント間および EPG 間のポリシーはサポートされます。外部ポリシーは学習された IP アドレスが必要な Virtual Routing and Forwarding（VRF）ベースであり、サポートされます。

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

アトミック カウンタの構成

ステップ 1 メニュー バーで、[Tenants] をクリックします。

ステップ 2 サブメニュー バーで、必要なテナントをクリックします。

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

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

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

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

a) [Name] フィールドにポリシーの名前を入力します。

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

c) トラフィックの宛先の識別情報を選択するか、入力します。

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

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

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

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

SNMP の使用

SNMP の概要

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

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

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

ACI での SNMP アクセスのサポート

ACI での SNMP のサポートは次のとおりです。

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

（注） ACI は最大 10 個のトラップ レシーバをサポートします。

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

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

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

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

SNMP の設定

GUI による SNMP ポリシーの設定

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

はじめる前に

SNMP 通信を有効にするには、以下の設定が必要です。

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

ステップ 1 メニュー バーで、[Fabric] をクリックします。

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

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

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

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

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

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

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

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

ステップ 8 [OK] をクリックします。

ステップ 9 [Submit] をクリックします。`

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

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

a) [Name] フィールドに、ポッド ポリシー グループの名前を入力します。
b) [SNMP Policy] ドロップダウン リストから、設定した SNMP ポリシーを選択して、[Submit] をクリックします。

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

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

ステップ 14 [Submit] をクリックします。`

ステップ 15 [OK] をクリックします。

GUI による SNMP トラップ通知先の設定

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

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

ステップ 1 メニュー バーで、[Admin] をクリックします。

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

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

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

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

a) [Name] フィールドに、SNMP 通知先の名前を入力し、[Next] をクリックします。
b) [Create Destinations] テーブルで + アイコンをクリックし、[Create SNMP Trap Destination] ダイアログボックスを開きます。
c) [Host Name/IP] フィールドに、送信先ホストの IP アドレスまたは完全修飾ドメイン名を入力します。
（注） Cisco APIC Release 1.2(2) 以降のリリースは、IPv6 SNMP トラップ宛先をサポートします。
d) 通知先のポート番号と SNMP バージョンを選択します。
e) SNMP v1 または v2c 通知先の場合、[Security Name] として設定したコミュニティ名の 1 つを入力し、[v3 Security Level] として noauth を選択します。
f) SNMP v3 通知先の場合、[Security Name] として設定したユーザ名の 1 つを入力し、必要な [v3 Security Level] を選択します。
g) [Management EPG] ドロップダウン リストから管理 EPG を選択します。
h) [OK] をクリックします。
i) [Finish] をクリックします。

GUI による SNMP トラップ ソースの設定

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

ステップ 1 メニュー バーで、[Fabric] をクリックします。

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

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

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

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

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

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

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

a) [Name] フィールドに、SNMP ポリシーの名前を入力します。

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

c) [Submit] をクリックします。`

SNMP を使用したシステムのモニタリング

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

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

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

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

SPAN の使用

SPAN の概要

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

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

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

マルチノード SPAN

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

SPAN の注意事項と制約事項

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

SPAN セッションの設定

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

ステップ 1 メニュー バーで、[Tenants] をクリックします。

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

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

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

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

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

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

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

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

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

次の作業

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

トレースルートの使用

トレースルートの概要

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

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

tracerouteは、エンドポイント間やリーフ間（トンネル エンドポイント、またはTEP間）など、さまざまなモードをサポートしています。トレースルートはファブリック全体のすべてのパスを検出し、外部エンドポイントの出口を検出します。パスが妨げられているかどうかを発見するのに役立ちます。

tracerouteの注意事項および制約事項

- tracerouteの送信元または宛先がエンドポイントである場合、そのエンドポイントはスタティックではなくダイナミックである必要があります。ダイナミック エンドポイント（fv:CEp）とは異なり、スタティック エンドポイント（fv:StCEp）にはtracerouteに必要な子オブジェクト（fv:RsCEpToPathEp）がありません。
- traceroute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。
- traceroute関連の制限については、『*Verified Scalability Guide for Cisco ACI*』というマニュアルを参照してください。

エンドポイント 間での traceroute の実行

ステップ 1 メニュー バーで、[Tenants] をクリックします。

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

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

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

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

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

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

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

f) （任意） [IP Protocol] ドロップダウン リストから、traceroute パケット用のプロトコルを選択します。デフォルトでは、プロトコルは未定義（0）ですが、traceroute パケットがフィルタまたはファイアウォールを通過できるようにするためにプロトコルの指定が必要な場合があります。

g) （任意） [Source Port] および [Destination Port] の各ドロップダウン リストから、traceroute パケット用の送信元および宛先のプロトコル番号を選択します。

h) [Admin State] ドロップダウン リストから、[Start] を選択します。

i) [Submit] をクリックして、トレースルートを起動します。

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

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

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

（注） 複数のパスが、送信元ノードから宛先ノードへの移動に使用されている場合があります。

（注） 見やすくするには、[Name] 列などの複数の列の幅を広げます。

第 2 章

エンドポイント接続のトラブルシューティング

エンドポイント接続のトラブルシューティング

ステップ 1 各エンドポイントの動作ステータスを調べます。
動作ステータスにはエンドポイントのエラーや設定ミスが示されます。参照先

エンドポイントのステータスの確認，（20 ページ）。

ステップ 2 トンネル インターフェイスのステータスを調べます。
動作ステータスにはトンネルのエラーや設定ミスが示されます。トンネルインターフェイスのステータスの確認，（21 ページ）を参照してください。

ステップ 3 エンドポイント グループ（EPG）間でトレースルートを実行します。
トレースルートでは、スパイン ノードなどの中間ノード、およびエンドポイント間の問題が明らかになります。エンドポイント 間での traceroute の実行，（18 ページ）を参照してください。

ステップ 4 エンドポイントのアトミック カウンタを設定します。
アトミック カウンタは、発信元エンドポイントがパケットを送信しているか、また送信先エンドポイントがパケットを受信しているか、そして受信されたパケット数が送信されたパケット数に等しいかどうかを確認します。アトミック カウンタの構成，（10 ページ）を参照してください。

ステップ 5 各 EPG でコントラクトを調べます。
各 EPG でのコントラクトを調べ、EPG 間でのトラフィックの流れが許可されているかを確認します。テストとして一時的にコントラクトを開き、無制限のトラフィックを許可することができます。

ステップ 6 発信元パケットをモニタリング ノードに転送するようにスパン ポリシーを設定します。
モニタリング ノードのパケット アナライザが、誤ったアドレスやプロトコルなどのパケットの問題を示します。SPAN セッションの設定, （16 ページ）を参照してください。

ステータスの確認

エンドポイントのステータスの確認

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、[Application Profiles] を拡張して、エンドポイントが含まれるアプリケーション プロファイルを拡張します。
ステップ 4 [Application EPGs] を展開し、確認する EPG をクリックします。
ステップ 5 [Work] ペインで、[Endpoint] テーブルのエンドポイントのリストから送信元エンドポイントをダブルクリックし、[Client End Point] ダイアログボックスを開きます。
ステップ 6 [Client End Point] ダイアログボックスで、エンドポイントのプロパティを確認し、[Operational] タブをクリックします。
ステップ 7 [Operational] タブで、健全性、ステータスおよび障害情報を表示します。
[Status] テーブルで、変更、イベント、またはエラーなどのエントリがある項目をクリックします。
ステップ 8 [Client End Point] ダイアログボックスを閉じます。
ステップ 9 [Endpoint] テーブルでエンドポイントの [Interface] エントリを表示し、ノードとトンネル ID をメモに記録します。
ステップ 10 送信先エンドポイントでこの手順を繰り返します。

トンネル インターフェイスのステータスの確認

この手順では、トンネル インターフェイスの動作ステータスを調べる方法を示します。

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、[Inventory] をクリックします。

ステップ 3 [Navigation] ペインでポッドを拡張し、発信元エンドポイント インターフェイスのノード ID を拡張します。

ステップ 4 ノードの下で [Interfaces] を拡張し、[Tunnel Interfaces] を拡張して、発信元エンドポイント インターフェイス のトンネル ID をクリックします。

ステップ 5 [Work] ペインで、トンネル インターフェイスのプロパティを確認し、[Operational] タブをクリックします。

ステップ 6 [Operational] タブで、健全性、ステータスおよび障害情報を表示します。
[Status] テーブルで、変更、イベント、またはエラーなどのエントリがある項目をクリックします。

ステップ 7 送信先エンドポイント インターフェイスでこの手順を繰り返します。

SFP モジュールの接続

SFP モジュールを新規カードに接続する場合は、カードと通信するためにモジュールのリンク速度ポリシーを作成する必要があります。リンク速度ポリシーを作成するには、次の手順に従います。

ステップ 1 リンク速度を指定するインターフェイス ポリシーを作成します。

例：

```
<fabricHIfPol name="SpeedPol" speed="1G"/>
```

ステップ 2 インターフェイス ポリシー グループ内のリンク速度ポリシーを参照します。

例：

```
<infraAccPortGrp name="myGroup">
   <infraRsHIfPol tnFabricHIfPolName="SpeedPol"/>
</infraAccPortGrp>
```

第 3 章

IP ベース EPG のトラブルシューティング

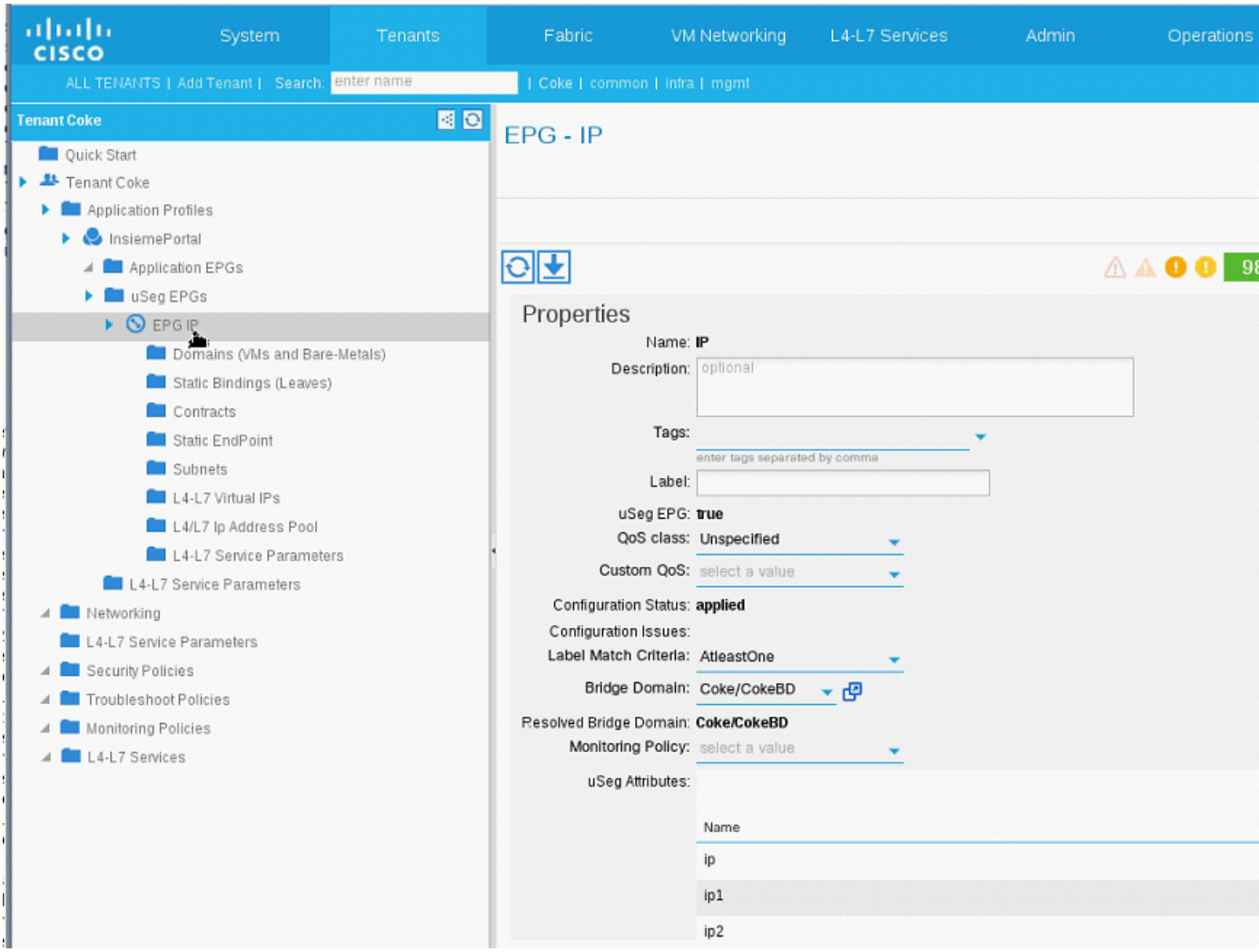
IP ベース EPG のトラブルシューティング

アプリケーション EPG と IP ベース EPG という、作成可能な 2 種類のエンドポイント グループ（EPG）があります。IP ベース EPG は、マイクロセグメント EPG であるという点で、通常のアプリケーション EPG とは異なっています。この手順は、IP ベース EPG を正しく設定したことを確認する方法を説明します。

ステップ 1 作成した IP ベース EPG が、GUI の [uSeg EPGs] フォルダの下に（次のスクリーン キャプチャに示すように）一覧表示されていることを確認します。
REST API を使用して作成された「IP」という uSeg EPG の下には、1 つの IP ベース EPG が表示されます。

ステップ 2 各 EPG IP（IP ベース EPG）について、EPG - IP の [Properties] 画面（ウィンドウ ペインの右側）にある情報が正しいことを確認します。

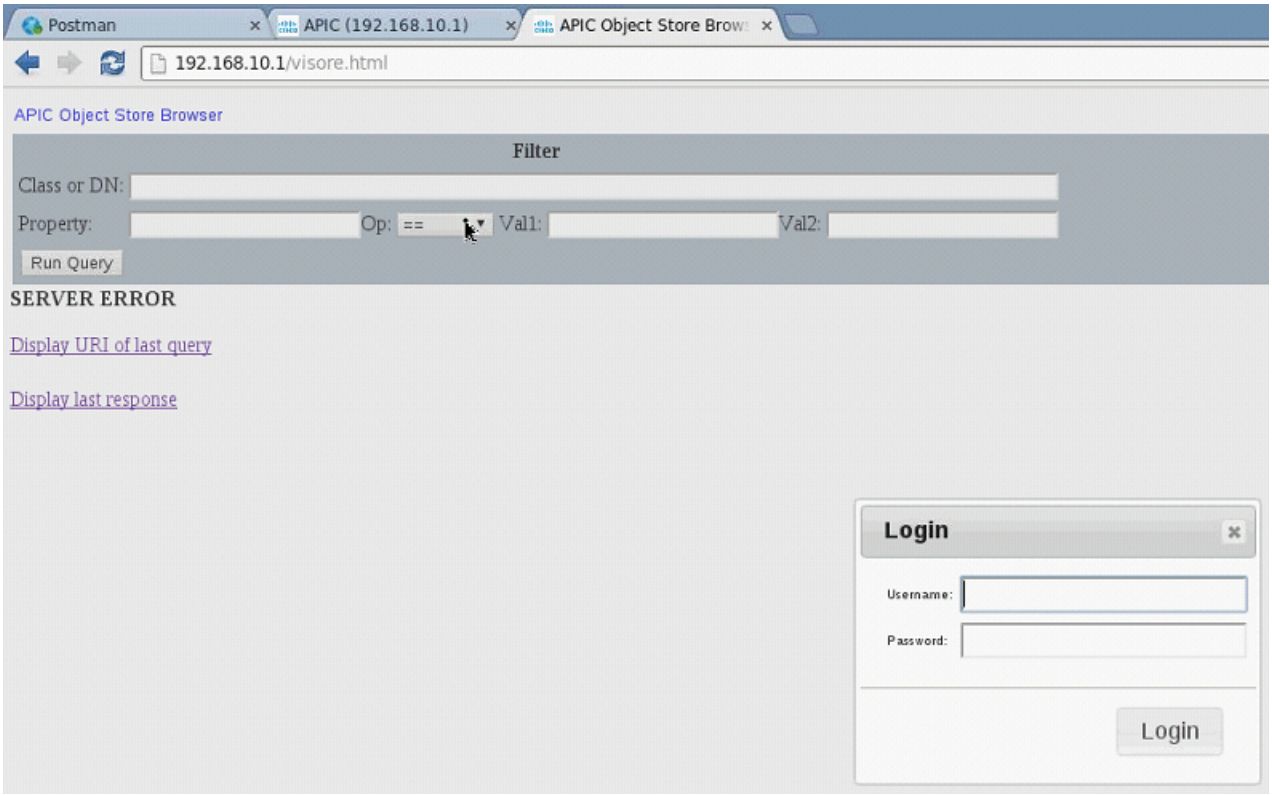
IP ベース EPG のトラブルシューティング



画面下部に表示されている IP ベース EPG と IP アドレスのリストを確認します。

ステップ 3 Web ブラウザから、APIC の IP アドレスと、続いて「/visore.html」を、次のように入力します。Visore は、EPG などの、システム内のすべてのオブジェクトを表示できるツールです。Visore を使用して、IP ベース EPG が正しく設定されていることを確認します。

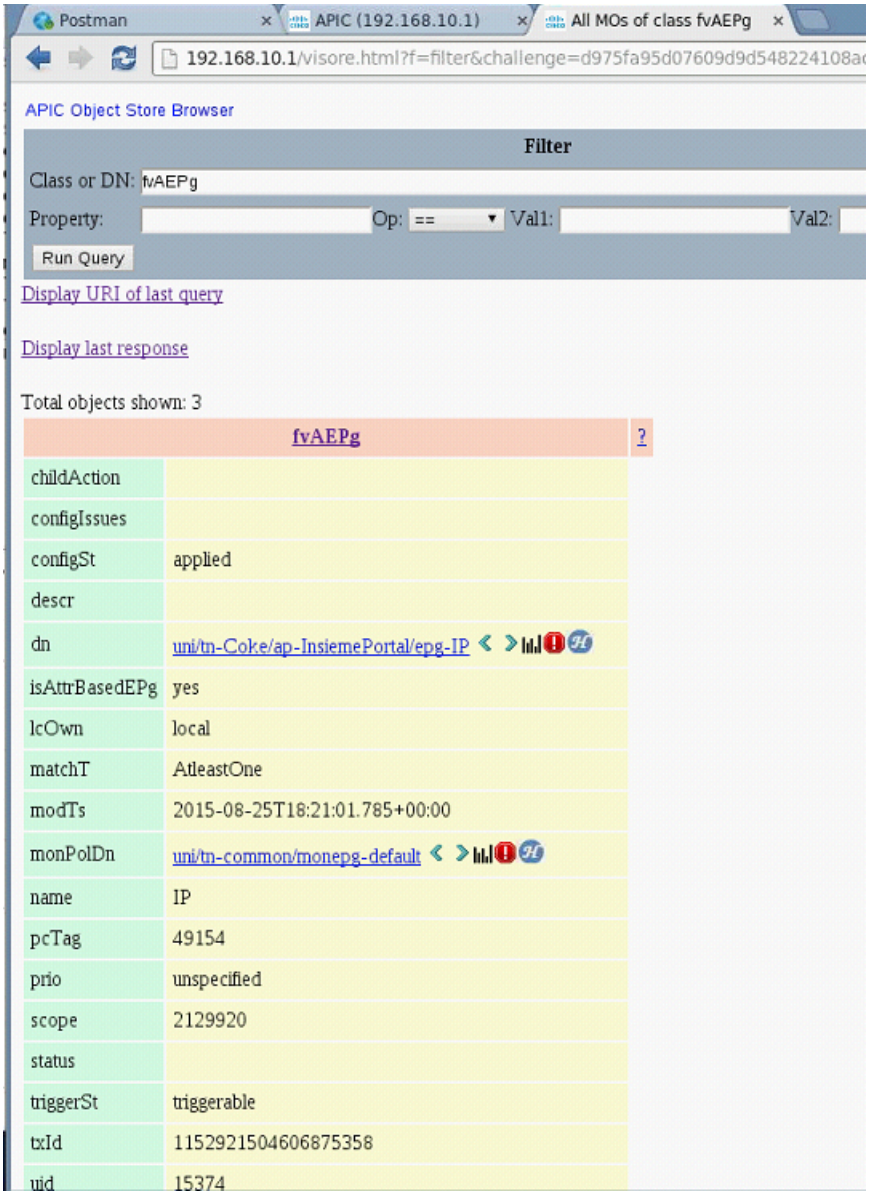
IP ベース EPG のトラブルシューティング



ステップ 4 ユーザ名とパスワードを入力して、[Login] をクリックし、Visore にログインします。

ステップ 5 次のように、[Class or DN] の横にあるフィールドにクラスの名前を入力して（たとえば「fvAEPg」）、GUI で確認した IP ベース EPG のクエリを実行します。

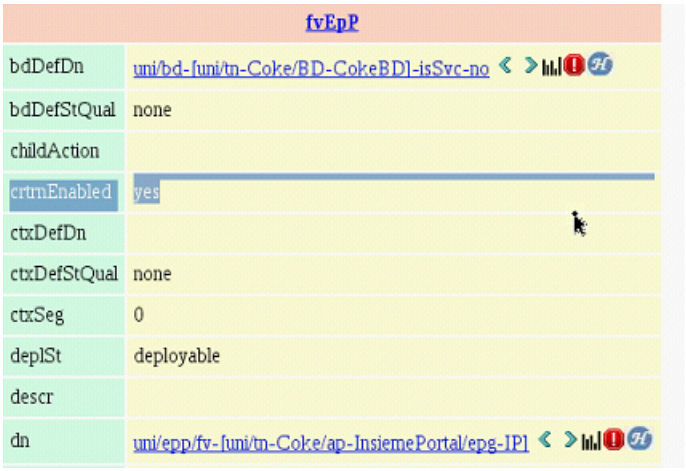
IP ベース EPG のトラブルシューティング



（注） これは、APIC の観点からのビューです。上記では [Total objects shown] が 3 と表示されていますが、これはスイッチにダウンロードされた EPG が 3 つあるということです。GUI で前には「IP」とリストされていた IP ベース EPG が、現在では「dn」の横に表示されていることを確認できます。さらに、「isAttrBasedEPg」の横に [yes] が表示されているということは、それが IP ベース EPG として適正に設定されていることを意味します。アプリケーション EPG と IP ベース EPG の両方を含むすべてのオブジェクトが、Visore を使用して正しく設定されていることを確認できます。

ステップ 6 これはスイッチの観点から見たビューです。スイッチ上で、fvEpP クラスのクエリを実行して、EPG や「crtrnEnabled」属性を確認できます。これは IP ベース EPG に対しては [yes] に設定されます。

IP ベース EPG のトラブルシューティング



ステップ 7 適正な構成であることを確認するために、この EPG の下で、EPG の子が IP アドレスとともに表示されていることを調べます。設定されている各 IP アドレスには、次のように、トラフィックを分類するためにスイッチが使用する（「l3IpCktEp」という）1 つのオブジェクトがあります。

IP ベース EPG のトラブルシューティング

fvRtIpEppAtt	
childAction	
dn	uni/epp/fv-[uni/tn-Coke/ap-InsiemePortal/epg-IP]/rtl3IpEppAtt-[sys/ctx-[vxlan-2129920]/bd-[vxlan-15990735]/ipcktep-[1.2.3.6/32]]
lcOwn	local
modTs	2015-08-25T18:21:15.233+00:00
status	
tCl	l3IpCktEp
tDn	sys/ctx-[vxlan-2129920]/bd-[vxlan-15990735]/ipcktep-[1.2.3.6/32]

fvRtIpEppAtt	
childAction	
dn	uni/epp/fv-[uni/tn-Coke/ap-InsiemePortal/epg-IP]/rtl3IpEppAtt-[sys/ctx-[vxlan-2129920]/bd-[vxlan-15990735]/ipcktep-[1.2.3.4/32]]
lcOwn	local
modTs	2015-08-25T18:21:15.233+00:00
status	
tCl	l3IpCktEp
tDn	sys/ctx-[vxlan-2129920]/bd-[vxlan-15990735]/ipcktep-[1.2.3.4/32]

fvRtIpEppAtt	
childAction	
dn	uni/epp/fv-[uni/tn-Coke/ap-InsiemePortal/epg-IP]/rtl3IpEppAtt-[sys/ctx-[vxlan-2129920]/bd-[vxlan-15990735]/ipcktep-[1.2.3.5/32]]
lcOwn	local
modTs	2015-08-25T18:21:15.233+00:00
status	
tCl	l3IpCktEp
tDn	sys/ctx-[vxlan-2129920]/bd-[vxlan-15990735]/ipcktep-[1.2.3.5/32]

設定が完了すると、パケットの着信時に、スイッチはパケットを分類するためにこれらのオブジェクトが使用されます。

ステップ 8 すべてのエンドポイントの pcTag と、設定した IP アドレスが一致していることを確認します。どの EPG にも、pcTag があります。設定した IP アドレスに一致するすべてのエンドポイントは、この pcTag に分類されます。どのエンドポイントにも、クラスのクエリを実行できる IP アドレスがあります。トラブルシューティングを行う場合には、これらのエンドポイント（サーバ）が、この IP ベース EPG に適正に分類されているかどうかを確認することができます（pcTag は IP ベース EPG に一致している必要があります）。

IP-EPGスイッチのトラブルシューティングコマンドの使用

トラブルシューティングのためにIP-EPG（「IpCkt」とも呼ばれる）にアクセスするには、次の手順に従います。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	リーフにログインします。	
ステップ 2	/mit/sys ディレクトリに移動します。	
ステップ 3	/mit/sys ディレクトリで、ctx（vrf コンテキスト ディレクトリ）を見つけます。	
ステップ 4	VRF cts ディレクトリで、IpCkt が設定されている特定の BD ディレクトリに移動します。	そこには IpCkt があります。 （注） このマニュアルでは、「IpCkt」と「IP-EPG」は置き換え可能な語として使用しています。
ステップ 5	そのディレクトリに移動すると、「cat summary」から、IpCkt に関する情報を取得できます。	
ステップ 6	このサマリの「operSt」が「未サポート（unsupported）」ではないことを確認します。	
ステップ 7	IpCkt が設定されている BD に対応する VLAN ID を検索します。	（注） VLAN ID は、いずれかの **show vlan internal bd-info** コマンドまたは **show system internal epm vlan all** コマンドを使用して検索できます。
ステップ 8	BD の VLAN ID を見つけたら、「show system internal epm <vlan-id> detail」を発行します。	ここでは、特定の sclass を持つすべての設定済み IpCkts を表示できる必要があります（これは、/mit/sys ディレクトリ内の該当する表示内容と一致している必要があります）。
ステップ 9	vsh での手順を vsh_lc に繰り返します。	
ステップ 10	BD で IpCtk に一致する IP があるトラフィックを送信し、「show system internal epm endp ip <a.b.c.d>」を実行すると、取得した IP に、「sclass」と特定の sclass 値の IP フラグがあることを確認できます。	
ステップ 11	vsh での手順を vsh_lc に繰り返します。	

スイッチのトラブルシューティング コマンドのリストは、次のとおりです。

```
Cd /mits/sys/ctx-vxlan…/bd-vxlan…
     - cat summary
Vsh -c “show system internal epm vlan all” or
Vsh -c “show vlan internal bd-info”
Vsh -c “show system internal epm vlan <vlan-id> detail”
Vsh -c “show system internal epm endp ip <a.b.c.d>"
Vsh_lc -c “show system internal epm vlan all” or
Vsh_lc -c “show vlan internal bd-info”
Vsh_lc -c “show system internal epm vlan <vlan-id> detail”
vsh_lc -c “show system internal epm endp ip <a.b.c.d>”
vsh_lc -c “show system internal epm epg”
```

第 4 章

ヘルス スコアを使用したトラブルシューティング

ヘルススコア

APIC は、ポリシー モデルを使用してデータをヘルス スコアに組み入れます。ヘルス スコアはインフラストラクチャ、アプリケーション、またはサービスなどさまざまな領域で集約できます。

ヘルス スコア、エラー、ヘルス スコアの計算については、『*Cisco APIC Fundamentals Guide*』を参照してください。

ヘルス スコアのタイプ

APIC は次のヘルス スコアのタイプをサポートします。

- システム：ネットワーク全体の健全性を要約します。
- リーフ：ネットワークのリーフ スイッチの健全性を要約します。リーフ健全性には、ファントレイ、電源、および CPU を含むスイッチのハードウェア健全性が含まれます。
- テナント：テナントとテナントのアプリケーションの健全性を要約します。

ネットワーク健全性のモニタリング

ヘルス スコアでは、ネットワーク階層をドリル ダウンして特定の管理対象オブジェクト（MO）のエラーを分離し、パフォーマンス上の問題を分離することができます。アプリケーションの（テ

ナントごとの）ヘルス、またはリーフ スイッチの（ポッドごとの）ヘルスを確認することで、ネットワーク ヘルスを確認できます。

ヘルス スコアによるフィルタリング

次のツールを使用して、ヘルス スコアをフィルタリングできます。

- ヘルス スクロール バー：ヘルス スクロール バーを使って、どのオブジェクトを表示するかを指定できます。スコアを下げれば、ヘルス スコアの低いオブジェクトだけ見ることができます。
- 低いヘルス スコアの表示：低いヘルス スコアを表示するには、ギア アイコンをクリックし、[Show only degraded health score] を選択します。

テナントの健全性の表示

アプリケーション ヘルスを表示するには、メニュー バーで [Tenants] > [tenant-name] をクリックし、次に [Navigation] ペインでテナント名をクリックします。GUI がアプリケーションや EPG を含むテナントの健全性の要約を表示します。テナントの設定をドリルダウンするには、ヘルス スコアをダブルクリックします。

健全性の要約の場合は、[Work] ペインの [Health] タブをクリックします。ネットワークのこの表示がヘルス スコアとネットワーク上の MO 間の関係を示すので、パフォーマンスの問題を分離し、解決することができます。たとえば、テナントのコンテクストの管理オブジェクトの共通シーケンスは、**テナント > アプリケーション プロファイル > アプリケーション EPG > EPP > ファブリックの場所 > EPG からパス アタッチメント > ネットワーク パス エンドポイント > 集約インターフェイス > 集約されたインターフェイス > 集約されたメンバー インターフェイス**となります。

ファブリックの健全性の表示

ファブリックの健全性を表示するには、メニュー バーの [Fabric] をクリックします。[Navigation] ペインで、ポッドを選択します。GUIは、ノードを含むポッドの健全性の要約を表示します。ファブリック設定の一部をドリル ダウンするには、ヘルス スコアをダブルクリックします。

健全性の要約の場合は、[Work] ペインの [Health] タブをクリックします。ネットワークのこの表示がヘルス スコアとネットワーク上の MO 間の関係を示すので、パフォーマンスの問題を分離し、解決することができます。たとえば、ファブリックのコンテキストにおける管理対象オブジェクトの共通シーケンスは、**ポッド > リーフ > シャーシ > ファン トレイ スロット > 回線モジュールのスロット > 回線モジュール > ファブリック ポート > レイヤ 1 物理インターフェイス設定 > 物理インターフェイス実行時間状態**です。

（注） 物理ネットワークの問題などのファブリックの問題は、MOが直接関連する場合は、テナントのパフォーマンスに影響を及ぼすことがあります。

Visore での MO 健全性の表示

Visore で MO の健全性を表示するには、H アイコンをクリックします。

次の MO を使って、健全性情報を表示します。

- health:Inst
- health:NodeInst
- observer:Node
- observer:Pod

Visore に関する詳細情報については、『*Cisco Application Centric Infrastructure Fundamentals*』の資料を参照してください。

ログを使用するヘルス スコアのデバッグ

次のログ ファイルを使用して、APIC のヘルス スコアをデバッグできます。

- svc_ifc_eventmgr.log
- svc_ifc_observer.log

ログを使用してヘルス スコアをデバッグする場合、次の項目を確認してください。

- syslog （エラーまたはイベント）の送信元を確認します。
- syslog ポリシーが APIC で設定されているかどうかを確認します。
- syslog ポリシー タイプおよび重大度が正しく設定されているかどうかを確認します。
- コンソール、ファイル、RemoteDest、または Prof の syslog 宛先を指定できます。RemoteDest の場合は、syslog サーバが実行しておりアクセス可能であることを確認します。

エラーの表示

次のように、エラーの要約を表示できます。

- システム エラー：[System] > [Faults] を選択します。
- テナント エラー：[Tenants] > [tenant-name] をクリックし、左ペインでテナント名をクリックして、右ペインで [Faults] タブを選択します。

- ファブリック エラー：[Fabric] をクリックし、左ペインでポッドをクリックし、右ペインで [Faults] タブをクリックします。

第 5 章

クラスタのトラブルシューティング

クラスタ管理の注意事項

APIC クラスタは複数の APIC コントローラで構成され、ACI ファブリックに対する統合されたリアルタイム モニタリング、診断および構成管理機能がオペレータに提供されます。最適なシステム パフォーマンスが得られるように、APIC クラスタを変更する場合は次のガイドラインに従ってください。

（注） クラスタへの変更を開始する前に、必ずその状態を確認してください。クラスタに対して計画した変更を実行するときは、クラスタ内のすべてのコントローラが正常である必要があります。クラスタ内の 1 つ以上の APIC コントローラのヘルス ステータスが「十分に正常」でない場合は、先に進む前にその状況を修復してください。また、APIC に追加されたコントローラが、APIC クラスタ内の他のコントローラと同じバージョンのファームウェアを実行していることを確認します。APIC クラスタの健全性の問題の解決についての詳細は、『*Cisco APIC Troubleshooting Guide*』を参照してください。

クラスタを管理する場合、次の一般的ガイドラインに従ってください。

- 現在クラスタにない APIC からのクラスタ情報は無視します。正確なクラスタ情報ではありません。
- クラスタ スロットには、APIC シャーシ ID が含まれます。スロットを設定すると、割り当てられたシャーシ ID の APIC を解放するまでそのスロットは使用できません。

- APIC ファームウェア アップグレードが進行中の場合は、それが完了し、クラスタが完全に適合するまでクラスタへの他の変更はしないでください。
- 電源の再投入を行う場合は、その前に必ず APIC クラスタ コントローラを解放し、次いでクラスタに再度追加します。このガイドラインに従わない場合、クラスタ上にある APIC クラスタ データベース シャードが破壊される可能性があります。このガイドラインでは、コントローラの全消去の実行と、クラスタ内の他の APIC コントローラから APIC クラスタ データベースの有効なコピーを復元するためのクラスタ同期の実行が求められています。

APIC クラスタ サイズの拡大

APIC クラスタ サイズを拡大するには、次のガイドラインに従ってください。

- クラスタの拡大がファブリックのワークロードの要求に影響しないときに、クラスタの拡大を予定します。
- クラスタ内の 1 つ以上の APIC コントローラのヘルス ステータスが「十分に正常」でない場合は、先に進む前にその状況を修復してください。
- ハードウェア インストレーション ガイドの手順に従って、新しい APIC コントローラを準備します。PING テストでインバンド接続を確認します。
- クラスタの目標サイズを既存のクラスタ サイズ コントローラ数に新規コントローラ数を加えた数になるように増やします。たとえば、既存のクラスタ サイズ コントローラの数が 3 で、3 台のコントローラを追加する場合は、新しいクラスタの目標サイズを 6 に設定します。クラスタは、クラスタにすべての新規コントローラが含まれるまで一度にコントローラ 1 台ずつ順にサイズを増やします。

（注） 既存の APIC コントローラが利用できなくなった場合、クラスタの拡大は停止します。クラスタの拡大を進める前に、この問題を解決します。

- 各アプライアンスの追加時に APIC が同期化しなければならないデータ量によって、拡大処理を完了するために必要な時間はアプライアンスごとに 10 分を超える可能性があります。クラスタが正常に拡大すると、APIC の運用サイズと目標サイズが同じになります。

（注） APIC がクラスタの拡大を完了するまでは、クラスタに追加の変更をしないようにします。

クラスタでの APIC コントローラの交換

APIC コントローラを交換するには、次の注意事項に従ってください。

- クラスタ内の 1 つ以上の APIC コントローラのヘルス ステータスが「十分に正常」でない場合は、先に進む前にその状況を修復してください。
- クラスタの同期がファブリックのワークロードの要求に影響しないときに、APICコントローラの交換を予定します。
- 交換する APIC コントローラの ID 番号を記録します。
- APIC 1 または 2 にログインし、APIC3 のシャットダウンを起動します。
- APIC3 を解放します。
- ハードウェア インストレーション ガイドの手順に従って、APIC コントローラの交換を準備します。PING テストでインバンド接続を確認します。

（注） 交換する前にAPICコントローラを解放しないと、クラスタによる交換コントローラの吸収が妨げられます。さらに、解放されたAPICコントローラを稼働状態に戻す前に、全消去を実行して工場出荷時の状態にリセットします。

- APICクラスタに交換コントローラを追加する場合、以前APICコントローラで使用したコントローラID番号を交換するAPICコントローラに割り当てます。APICが交換するコントローラとクラスタの同期へと進みます。

（注） 既存のAPICコントローラが使用できなくなると、クラスタの同期が停止します。クラスタの同期を進める前に、この問題を解決します。

- データ量によって APIC はコントローラの交換時に同期する必要があり、交換が完了するまでに交換コントローラごとに 10 分以上かかることがあります。交換コントローラとクラスタが正常に同期されると、APIC の動作サイズと目標サイズは未変更のままです。

（注） APIC がクラスタの同期を完了するまで、クラスタに追加の変更を加えないでください。

- クラスタの同期がファブリックのワークロードの要求に影響しないときに、APICコントローラの交換を予定します。
- UUIDとファブリックのドメイン名は、リブートしてもAPICコントローラに保持されます。ただし、初期状態にリブートするとこの情報は削除されます。APIC コントローラを 1 つのファブリックから別のファブリックへ移動する場合、そのコントローラを異なるACIファブリックに追加する前に初期状態にリブートする必要があります。

クラスタ サイズの縮小

APIC クラスタのサイズを縮小し、クラスタから除去される APIC コントローラ アプライアンスを解放するには、以下のガイドラインに従ってください。

警告 縮小されたクラスタに含まれる APIC コントローラ アプライアンスの電源を切って解放するプロセスに順次従わないと、予期しない結果を招く可能性があります。ファブリックへの接続を維持するには、認識されない APIC コントローラ アプライアンスを使わないでください。

（注） クラスタ サイズを縮小すると、残りの APIC コントローラ アプライアンスの負荷が増大します。

- クラスタの同期がファブリックのワークロードの要求に影響しないときに、APIC コントローラ サイズの縮小を予定します。
- クラスタの目標サイズを新たな低い値に減らします。たとえば、既存のクラスタ サイズが 6 で、3 台のコントローラを削除する場合は、クラスタの目標サイズを 3 に減らします。
- 既存のクラスタの最も大きな番号が付いた コントローラ アプライアンス ID から始め、新しいより小さい目標番号に到達するまで、1 つずつ交換する APIC コントローラ アプライアンスを解放して、電源を切り、接続解除します。

  各コントローラ アプライアンスの解放と削除が終わると、APIC がクラスタを同期します。
- 既存の APIC アプライアンスが使用できなくなると、クラスタの同期は停止します。クラスタの同期を進める前に、この問題を解決します。
- データ量によって APIC はアプライアンスの交換時に同期する必要があり、各コントローラ アプライアンスの解放が完了するまでにアプライアンスごとに 10 分以上かかることがあります。

警告 クラスタに追加の変更を行う前に、必要な解放手順全体を完了し、APIC がクラスタの同期を完了できるようにしてください。

クラスタ内の Cisco APIC の交換

（注） クラスタの管理の詳細については、「クラスタ管理の注意事項」を参照してください。

（注） クラスタの拡大または縮小については、『『*Cisco APIC Getting Started Guide*』』を参照してください。

（注） APIC を交換すると、パスワードは必ずクラスタから同期されます。APIC 1 を交換するときには、パスワードの入力を求められますが、そのパスワードはクラスタ内の既存のパスワードを優先して無視されます。APIC 2 または 3 を交換するときには、パスワードの入力は求められません。

ステップ 1 交換する APIC を特定します。

ステップ 2 **controller** *controller-id* **decommission** コマンドを使用して、APIC を解放します。

（注） APIC を解放すると、APIC ID とシャーシ ID のマッピングが削除されます。通常、新しい APIC には、異なる APIC ID があるので、クラスタに新しい APIC を追加するにはこのマップを削除する必要があります。

ステップ 3 同じ APIC を再稼動する場合には、次の手順に従ってください。

a) **acidiag reboot** コマンドを使用して、APIC を再起動します。
b) APIC がエラーなしでブートされることを確認します。
c) **controller** *controller-id* **commission** コマンドを使用して、APIC を稼働します。
d) クラスタの残りの部分に新しい APIC 情報が伝播するまでに数分かかります。

ステップ 4 新しい APIC を稼動する場合は、次の手順に従ってください。

a) ファブリックから APIC を切断します。
b) ファブリックに交換 APIC を接続します。
c) **controller** *controller-id* **commission** コマンドを使用して、APIC を稼働します。
d) 新しい APIC を起動します。
e) クラスタの残りの部分に新しい APIC 情報が伝播するまでに数分かかります。

クラスタのトラブルシューティングのシナリオ

次の表は、Cisco APIC に共通するクラスタのトラブルシューティングのシナリオを示します。

問題	ソリューション
APIC ノードはクラスタ内でエラーが発生します。たとえば、5 つの APIC のクラスタのノード 2 がエラーを起こすとします。	2 つの解決策があります。 • 目標サイズはそのままにし、APIC を交換します。APIC の交換の手順については、「クラスタ内の Cisco APIC の交換」を参照してください。 • クラスタ サイズを 4 に縮小するには、コントローラ 5 を解放し、APIC 2 として再稼動します。APIC の解放および再稼働の手順については、「クラスタ内の Cisco APIC の交換」を参照してください。目標サイズは 4 のままにし、再設定した APIC が実行されると動作サイズは 4 になります。 （注） 交換する APIC をクラスタに追加し、目標サイズと運用サイズを拡張できます。新しい APIC を追加する手順については、『*Getting Started Guide for the Cisco APIC*』を参照してください。
新しい APIC はファブリックに接続し、リーフ スイッチへの接続は失われます。	インフラストラクチャ VLAN の不一致があるかを確認するには、次のコマンドを使用します。 • cat /mit/sys/lldp/inst/if-\[eth1--1\]/ctrlradj/summary：リーフ スイッチ上で設定された VLAN を表示します。 • cat /mit/sys/lldp/inst/if-\[eth1--1\]/ctrlradj/summary：接続された APIC によってアドバタイズされるインフラストラクチャ VLAN を表示します。 これらのコマンドの出力が異なる VLAN を表示する場合、新しい APIC は正しいインフラストラクチャ VLAN で設定されていません。この問題を解決するには、次の手順に従います。 • レスキューユーザを使用して APIC にログインします。 （注） APIC はファブリックの一部ではないため、管理者のクレデンシャルは機能しません。 • 設定を消去し、**acidiag touch setup** コマンドを使って APIC を再起動します。 • APIC を再設定します。ファブリック名、TEP アドレス、およびクラスタの APIC にマッチするインフラストラクチャ VLAN を確認します。 • リーフ ノードをリロードします。

問題	ソリューション
起動後に 2 つの APIC が通信できません。	この問題は次の一連のイベントの後に発生することがあります。 • APIC1 と APIC2 が相互に検出する。 • APIC1 がリブートし、新しいシャーシ ID（APIC1a）でアクティブになる。 • 2 つの APIC が通信しなくなる。 このシナリオでは、APIC1a が APIC2 を検出しますが、APIC2 はオフラインと見なされる APIC1 があるクラスタ内に存在するので使用できません。その結果、APIC1a は APIC2 からのメッセージを受け入れません。 この問題を解決するには、APIC2 上の APIC1 を解放し、再度 APIC1 を稼働させます。
解放された APIC はクラスタに参加します。	この問題は次の一連のイベントの後に発生することがあります。 • クラスタのメンバが使用不可になるか、またはクラスタが分割されます。 • APIC が解放されます。 • クラスタの復旧後には、解放された APIC は自動的に稼働します。 問題を解決するには、クラスタの復旧後に APIC を解放します。
再起動後のシャーシ ID の不一致。	この問題は、APIC がクラスタで登録されたシャーシ ID と異なるシャーシ ID で起動したときに起こります。その結果、この APIC からのメッセージが廃棄されます。 この問題を解決するには、リブートの前に APIC が解放されていることを確認してください。
APIC はクラスタ サイズの変更時にエラーを表示します。	さまざまな条件が、AdminstrativeClusterSize に合わせたクラスタによる OperationalClusterSize の拡張の妨げになる可能性があります。詳しくは、エラーを検査し、「クラスタのエラー」を確認してください。
APIC がクラスタに参加できない。	この問題は、クラスタを拡大するときに 2 つの APIC が同じクラスタ ID で設定されると起こります。その結果、2 つのうち 1 つの APIC がクラスタに参加できず、拡張競合シャーシ ID 不一致のエラーが表示されます。 この問題を解決するには、新しいクラスタ ID でクラスタの外側に APIC を設定します。

問題	ソリューション
APICがクラスタで到達不能。	この問題を診断するには、次の設定を確認してください。 • ファブリック検出が完了していることを確認します。 • ファブリックから欠落しているスイッチを特定します。 • スイッチが APIC からの IP アドレスを要求し、受信したかどうかを確認します。 • スイッチがソフトウェアイメージをロードしたことを確認します。 • スイッチがアクティブになっている時間を確認します。 • すべてのプロセスがスイッチ上で動作していることを確認します。詳細については、acidiag コマンドを参照してください。 • 欠落しているスイッチに正しい日付と時刻が設定されていることを確認します。 • スイッチが他の APIC と通信できることを確認します。
クラスタが拡大しない。	この問題は、次の状況で発生します。 • OperationalClusterSize が APIC の数より少ない。 • 展開のコンテンダがない（たとえば、admin サイズは 5 ですがクラスタ ID が 4 の APIC がありません） • クラスタと新しい APIC の間に接続がない • 新しい APIC によってハートビート メッセージが拒否される • システム ヘルスが正常でない • 使用できないアプライアンスが再配置に関するデータ サブセットを伝送している • 再配置に関するデータ サブセットがあるアプライアンスでサービスがダウンしている • 再ロケーションに関連するデータ サブセットの不健全

問題	ソリューション
APIC がダウンしている。	次の点をチェックします。 • 接続の問題：ping を使用して接続を確認します。 • インターフェイス タイプの不一致：すべての APIC がインバンド通信になっていることを確認します。 • ファブリック接続：ファブリック接続が正常であること、およびファブリック検出が完了していることを確認します。 • 拒否されたハートビート：fltInfraIICIMsgSrcOutsider エラーを確認します。一般的なエラーには、動作クラスタ サイズ、シャーシ ID の不一致、動作クラスタ サイズの外の送信元 ID、承認されていない送信元、およびファブリック ドメインの不一致が含まれます。

クラスタのエラー

APIC は、クラスタの問題の診断に役立つさまざまなエラーをサポートします。ここでは、2 つの主要なクラスタのエラーの種類について説明します。

エラーの破棄

APIC は現在のクラスタのピアまたはクラスタ拡大候補以外からのクラスタ メッセージを破棄します。APIC はメッセージを破棄すると、発信元の APIC のシリアル番号、クラスタ ID 、およびタイムスタンプを含むエラーを生成します。次の表で、破棄されるメッセージのエラーを要約します。

Fault	意味
expansion-contender-chassis-id-mismatch	送信側 APIC のシャーシ ID が拡大のためにクラスタが認識するシャーシ ID と一致しません。
expansion-contender-fabric-domain-mismatch	送信側 APIC のファブリック ID が拡大のためにクラスタが認識するファブリック ID と一致しません。
expansion-contender-id-is-not-next-to-oper-cluster-size	送信側 APIC に拡大に不適切なクラスタ ID があります。値は、現在の OperationalClusterSize よりも 1 大きい必要があります。
expansion-contender-message-is-not-heartbeat	送信側 APIC が継続的ハートビート メッセージを送信しません。
fabric-domain-mismatch	送信側 APIC のファブリック ID がクラスタのファブリック ID と一致しません。

Fault	意味
operational-cluster-size-distance-cannot-be-bridged	送信側 APIC に、受信側 APIC のものとは 1 以上違う OperationalClusterSize があります。受信側 APIC は要求を拒否します。
source-chassis-id-mismatch	送信側 APIC のシャーシ ID がクラスタに登録されたシャーシ ID と一致しません。
source-cluster-id-illegal	送信側 APIC に許可されていないクラスタ ID 値があります。
source-has-mismatched-target-chassis-id	送信側 APIC の目標シャーシ ID が受信側 APIC のシャーシ ID に一致しません。
source-id-is-outside-operational-cluster-size	送信側 APIC に、クラスタの OperationalClusterSize 外のクラスタ ID があります。
source-is-not-commissioned	送信側 APIC には、クラスタで現在解放されているクラスタ ID があります。

クラスタ変更時エラー

次のエラーは、APIC のクラスタ サイズの変更時のエラーがある場合に適用されます。

Fault	意味
cluster-is-stuck-at-size-2	このエラーは、OperationalClusterSize が拡張期間にわたり 2 のままになると発行されます。問題を解決するには、クラスタの目標サイズをリストアします。
most-right-appliance-remains-commissioned	クラスタ内の最後の APIC が稼働中であり、それがクラスタの縮小を妨げています。
no-expansion-contender	クラスタがより大きいクラスタ ID を持つ APIC を検出できず、クラスタの拡張を行えません。
service-down-on-appliance-carrying-replica-related-to-relocation	移動するデータのサブセットは、障害が起きているサービス上にコピーがあります。APIC に複数のこのような障害があることを示します。
unavailable-appliance-carrying-replica-related-to-relocation	移動するデータのサブセットは、使用できない APIC 上にコピーがあります。このエラーを解決するには、使用できない APIC を復元します。
unhealthy-replica-related-to-relocation	移動するデータのサブセットは、正常でない APIC 上にコピーがあります。このエラーを解決するには、障害の根本原因を特定します。

APIC の使用不可

次のクラスタのエラーは、APIC が使用できない場合に適用できます。

Fault	意味
fltInfraReplicaReplicaState	クラスタがデータのサブセットを起動できません。
fltInfraReplicaDatabaseState	データ ストア サービスの破損を示します。
fltInfraServiceHealth	データのサブセットが完全には機能していないことを示します。
fltInfraWiNodeHealth	APIC が完全には機能していないことを示します。

第 6 章

統計情報を使用したトラブルシューティング

GUI での統計情報の表示

アプリケーションプロファイル、物理インターフェイス、ブリッジドメイン、ファブリックノードなど、APIC GUI を使用して、多数のオブジェクトの統計情報を表示できます。GUI で統計情報を表示するには、[Navigation] ペインでオブジェクトを選択し、[STATS] タブをクリックします。

たとえば、インターフェイスの統計情報を表示するには、次の手順を実行します。

ステップ 1 メニュー バーで、[FABRIC] > [INVENTORY] を選択します。
ステップ 2 [Navigation] ペインで、ポッドを選択します。
ステップ 3 ポッドを展開し、スイッチを展開します。
ステップ 4 [Navigation] ペインで、[Interfaces] を拡張し、eth1/1 を選択します。
ステップ 5 [Work] ペインで、[STATS] タブを選択します。

APIC がインターフェイスの統計情報を表示します。

次の作業

[Work] ウィンドウの次のアイコンを使って、APIC での統計情報の表示方法を管理できます。

- Refresh：統計情報を手動で更新します。
- Show Table View：表とチャートの表示を切り替えます。
- Start or Stop Stats：統計情報の自動更新を有効または無効にします。
- Select Stats：表示するカウンタとサンプルのインターバルを指定します。
- Download Object as XML：XML 形式でオブジェクトをダウンロードします。
- Measurement Type（ギア アイコン）：統計情報の測定タイプを指定します。オプションとして累積値、定期値、平均値、傾向値があります。

スイッチの統計情報コマンド

次のコマンドを使って、ACI リーフ スイッチの統計情報を表示できます。

コマンド	目的
レガシー Cisco Nexus の **show**/**clear** コマンド	詳細については、『*Cisco Nexus 9000 Series NX-OS Configuration Guide*』を参照してください。

コマンド	目的
show platform internal counters port [*port_num* | **detail** | **nz** | {**internal** [**nz** | *int_port_num*]}]	スパイン ポートの統計情報を表示します。 • *port_num*：スロットのない前面ポート番号。 • [detail]：SNMP、クラス、および転送統計情報を返します。 • [nz]：非ゼロの値のみを表示します。 • **internal**：内部ポート統計情報を表示します。 • *int_port_num*：内部論理ポート番号。たとえば、BCM-0/97 の場合は、97 を入力します。 （注） リンクのリセットが行われると、スイッチのカウンタはゼロに戻されます。カウンタ リセットの条件には、次のものがあります。 • 偶発的なリンクのリセット • 手動で有効にしたポートがある（ポートを無効にしていた）
show platform internal counters vlan[*hw_vlan_id*]	VLAN 統計情報を表示します。
show platform internal counters tep[*tunnel_id*]	TEP 統計情報を表示します。
show platform internal counters flow[*rule_id* | {**dump** [*asic inst*] | [**slice direction** | **index***hw_index*]}]	フロー統計情報を表示します。
clear platform internal counters port[*port_num* | {**internal** [*int_port_num*]}]	ポート統計情報を消去します。
clear platform internal counters vlan[*hw_vlan_id*]	VLAN カウンタを消去します。
debug platform internal stats logging level*log_level*	デバッグのログ レベルを設定します。
debug platform internal stats logging {**err**|**trace**|**flow**}	デバッグのロギング タイプを設定します。

GUI を使用する統計情報しきい値の管理

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

ステップ 2 [Navigation] ペインで + をクリックし、[Monitoring Policies] を展開します。

ステップ 3 [Navigation] ペインで、モニタリング ポリシー名（デフォルトなど）を拡張します。

ステップ 4 [Stats Collection Policies] をクリックします。

ステップ 5 [Stats Collection Policies] ウィンドウで、しきい値を設定するモニタリング オブジェクトおよび統計タイプを選択します。

ステップ 6 [Work] ペインで、[CONFIG THRESHOLDS] の下の + をアイコンをクリックします。

ステップ 7 [THRESHOLDS FOR COLLECTION] ウィンドウで + をクリックし、しきい値を追加します。

ステップ 8 [Choose a Property] ウィンドウで、統計タイプを選択します。

ステップ 9 [EDIT STATS THRESHOLD] ウィンドウで、次のしきい値を指定します。

- Normal Value：カウンタの有効値。
- Threshold Direction：しきい値が最大値または最小値かどうかを示します。
- Rising Thresholds（Critical、Major、Minor、Warning）：値がしきい値を上回った場合にトリガーされます。
- Falling Thresholds（Critical、Major、Minor、Warning）：値がしきい値を下回った場合にトリガーされます。

ステップ 10 上限および下限しきい値の設定値とリセット値を指定できます。設定値はエラーがトリガーされるタイミングを指定します。リセット値はエラーが消去されるタイミングを指定します。

ステップ 11 しきい値を保存するには、[SUBMIT] をクリックします。

ステップ 12 [THRESHOLDS FOR COLLECTION] ウィンドウで、[CLOSE] をクリックします。

統計情報に関するトラブルシューティングのシナリオ

次の表で、Cisco APIC に共通する統計情報に関するトラブルシューティングのシナリオを要約します。

問題	ソリューション
APICは、設定済みのモニタリングポリシーを課すことはありません。	モニタリング ポリシーが適用されていても、APIC が統計情報の収集やトリガーしきい値に対する操作など、対応するアクションを実行しないと問題が発生します。問題を解決するには、次の手順に従ってください。 • monPolDn が正しいモニタリング ポリシーを指していることを確認します。 • セレクタが正しく設定され、エラーがないことを確認します。 • テナントのオブジェクトの場合は、モニタリング ポリシーとの関係を確認します。
設定した一部の統計情報が見つからない。	問題を解決するには、次の手順に従ってください。 • モニタリング ポリシーおよび収集ポリシー内でデフォルトによって無効になっている統計情報を確認します。 • 収集ポリシーを確認し、統計情報がデフォルトで無効になっているか、または特定のインターバルで無効になっているかを識別します。 • 統計ポリシーを確認し、統計情報がデフォルトで無効になっているか、または特定のインターバルで無効になっているかを識別します。 （注） ファブリック ヘルスの統計情報を除き、5 分間の統計情報がスイッチに保存され、スイッチがリブートされると失われます。
統計情報や履歴を設定した期間保持できない	問題を解決するには、次の手順に従ってください。 • 収集設定を確認してください。モニタリング ポリシーの最上位レベルで設定されていると、特定のオブジェクトまたは統計タイプでは、統計情報が無効になる場合があります。 • モニタリング オブジェクトに割り当てられた収集ポリシーを確認します。ポリシーが存在するのを確認し、管理状態および履歴保持の値を確認します。 • 統計タイプが正しく設定されていることを確認します。

問題	ソリューション
設定されたインターバルにわたって保持されない統計情報がある。	設定が履歴記録サイズの最大値を超えていないかどうか確認します。制限事項は次のとおりです。 • 5 分間の細かさでのスイッチ統計情報は 12 サンプル（5 分間の細かさの統計情報の 1 時間分）に限られています。 • 1000 サンプルの厳しい制限があります。たとえば、1 時間の細かさの統計情報は 41 日間まで保持できます。
エクスポートポリシーは設定されるが、APIC が統計情報をエクスポートしない。	問題を解決するには、次の手順に従ってください。 • 送信先ポリシーの状態オブジェクトを確認します。 • 統計をエクスポートする予定のノードでエクスポート ステータスのオブジェクトをチェックし、エクスポート ステータスと詳細のプロパティを確認してください。集約された EPG 統計は APIC ノードから 15 分ごとにエクスポートされます。その他の統計は、送信元ノードから 5 分ごとにエクスポートされます。たとえば、EPG が 2 つのリーフ スイッチに展開され、EPG 集約パートにエクスポートするように設定されていると、それらパートはノードから 5 分ごとにエクスポートされます。 • 設定が、統計情報エクスポート ポリシーの最大数を超過しているかどうかを確認します。統計情報エクスポート ポリシーの最大数は、テナント数とほぼ同じです。 （注） 各テナントは、複数の統計情報エクスポートポリシーを持つことができ、複数のテナントで同じエクスポートポリシーを共有できますが、ポリシーの総数はテナントの概数までに制限されます。
5 分間統計が変動する	APIC は 10 秒ごとに 5 分間の細かさの統計情報を収集しますが、この値は一部のインターフェイスの収集インターバルと完全には一致しません。その結果、統計情報が少し長い、または短い期間を表す場合があります。
一部の履歴統計情報が見つからない。	詳しくは、「統計情報の消去」を参照してください。

統計情報の消去

APIC とスイッチは次のように統計情報を消去します。

- スイッチ：スイッチは次のように統計情報を消去します。

- スイッチの 5 分間の統計情報は、5 分間カウンタ値が報告されないと消去されます。この状況は、ポリシーによってオブジェクトが削除されるか、または統計情報が無効化されるときに起こる場合があります。
- より細分化された統計情報は、1 時間以上統計情報がないと消去されます。これは次の場合に起きることがあります。
  - 統計情報がポリシーによって無効化されている。
  - スイッチが 1 時間以上 APIC から切断されている。
- スイッチは5分後に削除されたオブジェクトの統計情報を消去します。オブジェクトがこの時間内に再作成されると、統計カウントは未変更のままになります。
- 無効化されたオブジェクト統計情報は 5 分後に削除されます。
- システム状態が変化し、統計情報レポートが 5 分間無効化されると、このスイッチによって統計情報が消去されます。

• APIC：APIC はインターフェイス、EPG、温度センサー、およびヘルス統計情報を含むオブジェクトを、1 時間後に消去します。

第 7 章

ポート トラッキングを使用したトラブルシューティング

アップリンク障害検出のためのポートトラッキングポリシー

アップリンク障害検出は、ファブリック アクセス グローバル ポート トラッキング ポリシーで有効にできます。ポート トラッキング ポリシーが、リーフ スイッチとスパイン スイッチとの間のリンクの状態を監視します。有効なポート トラッキング ポリシーがトリガーされると、リーフ スイッチは、EPG が展開されているスイッチのすべてのアクセス インターフェイスを停止します。

（注） 拡張 GUI では、ポート トラッキングは、[Fabric] -> [Access Policies] -> [Port Tracking] にあります。基本 GUI では、ポート トラッキングは、[System] -> [Port Tracking] にあります。

リーフ スイッチのモデルに応じて、各リーフ スイッチは、各スパイン スイッチへの 6、8、または 12 個のアップリンク接続を持つことができます。ポート トラッキング ポリシーは、ポリシーをトリガーするアップリンク接続の数と、指定のアップリンク数を超過した後にリーフ スイッチ アクセス ポートを復旧するまでの遅延タイマーを指定します。

ポート トラッキング ポリシーの動作例を以下に示します。

- 各リーフ スイッチには、スパイン スイッチへの 6 個のアクティブなアップリンク接続があります。

- ポート トラッキング ポリシーは、ポリシーをトリガーする各リーフ スイッチへのアクティブなアップリンク接続のしきい値を 2 に指定します。
- ポート トラッキング ポリシーは、リーフ スイッチからスパイン スイッチへのアクティブなアップリンク接続の数が 2 にドロップするとトリガーされます。
- 各リーフ スイッチはそのアップリンク接続をモニタし、ポリシーで指定されているしきい値に従ってポート トラッキング ポリシーをトリガーします。
- アップリンク接続が復旧すると、リーフ スイッチは遅延タイマーが満了するまで、アクセス ポートの再開を待機します。これによりファブリックは、リーフ スイッチ アクセス ポートでトラフィックを再開する前に、再統合する時間を取ることができます。大規模なファブリックでは、遅延タイマーに長めの時間を設定することが必要になる場合があります。

（注） このポリシーの設定には注意が必要です。ポート トラッキングをトリガーするアクティブ スパイン リンク数に対するポート トラッキングの設定が高すぎると、すべてのリーフ スイッチ アクセス ポートがダウンします。

GUI を使用したポート トラッキング

この手順では、GUI を使用したポート トラッキング機能の使用方法について説明します。

ステップ 1 [Fabric] メニューから、[Access Policies] を選択します。

ステップ 2 [Access Policies] の左側のナビゲーション ウィンドウで、[Global Polices] を選択します。

ステップ 3 [Global Policies] タブの下で、[Port Tracking] タブを選択します。

ステップ 4 ポート トラッキング機能をオンにするには、[Properties] の下の [Port tracking state] の横で [on] を選択します。

ステップ 5 ポート トラッキング機能をオフにするには、[Properties] の下の [Port tracking state] の横で [off] を選択します。

ステップ 6 [Delay restore timer] を設定します。これはファブリック ポート トラッキングの開始後に、ダウンリンクを回復して起動するまでの秒数を指定するために使う設定パラメータです。

ステップ 7 下回ったらこの設定をトリガーする、残りのリンクの最大数（0～12のいずれかの設定値）を入力します（デフォルトは 0 です）。

ステップ 8 [Submit] をクリックして、目的のポート トラッキング設定をファブリックのすべてのスイッチにプッシュします。

NX-OS CLI を使用したポート トラッキング

この手順では、NX-OS CLI を使用したポート トラッキング機能の使用方法について説明します。

ステップ 1 ポート トラッキング機能を次のようにオンにします。

例：

```
apic1# show porttrack
Configuration
Admin State                  : on
Bringup Delay(s)             : 120
Bringdown # Fabric Links up  : 0
```

ステップ 2 ポート トラッキング機能を次のようにオフにします。

例：

```
apic1# show porttrack
Configuration
Admin State                  : off
Bringup Delay(s)             : 120
Bringdown # Fabric Links up  : 0
```

REST API を使用したポート トラッキング

はじめる前に

この手順では、REST API を使用したポート トラッキング機能の使用方法について説明します。

ステップ 1 REST API を使用して、次のようにポート トラッキング機能をオンにします（**admin state**：**on**）。

```
<polUni>
<infraInfra dn="uni/infra">
<infraPortTrackPol name="default" delay="5" minlinks="4" adminSt="on">

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

ステップ 2 REST API を使用して、次のようにポート トラッキング機能をオフにします（**admin state**：**off**）。

```
<polUni>
<infraInfra dn="uni/infra">
<infraPortTrackPol name="default" delay="5" minlinks="4" adminSt="off">

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

第 8 章

設定ゾーンのトラブルシューティング

設定ゾーン

設定ゾーンは、ACI ファブリックを、さまざまなタイミングで実行される設定変更により更新できる多様なゾーンに分割します。これにより、トラフィックを中断したりファブリックをダウンさせたりする可能性もある、障害ファブリック全体の設定を展開してしまうリスクが制限されます。管理者はクリティカルではないゾーンに設定を展開し、それが適切であることを確認した時点でクリティカル ゾーンに展開できます。

次のポリシーは、設定組織ゾーンのアクションを指定します。

- `infrazone:ZoneP` は、システム アップグレード時に自動的に作成されます。削除したり変更したりすることはできません。
- `infrazone:Zone` には、1 つ以上のノード グループ（`NodeGrp`）が含まれます。1 つのノードが属することができるのは、1 つのゾーン（`infrazone:Zone`）のみです。`NodeGrp` には、名前と展開モードの 2 つの属性があります。展開モードのプロパティは、次のように指定できます。
  - `enabled`：保留中の更新は即座に送信されます。
  - `disabled`：新規の更新は延期されます。

（注） 無効にされた（disabled）設定ゾーンのノードは、アップグレード、ダウングレード、稼働、または解放しないでください。

- `triggered`：保留中の更新は即座に送信され、展開モードは`triggered`に変更する前の値に自動的にリセットされます。

特定の一群のノードに対するポリシーを作成、修正、または削除すると、更新はポリシーを展開する各ノードに送信されます。ポリシー クラスと `infrazone` 設定に基づいて、以下のことが起きます。

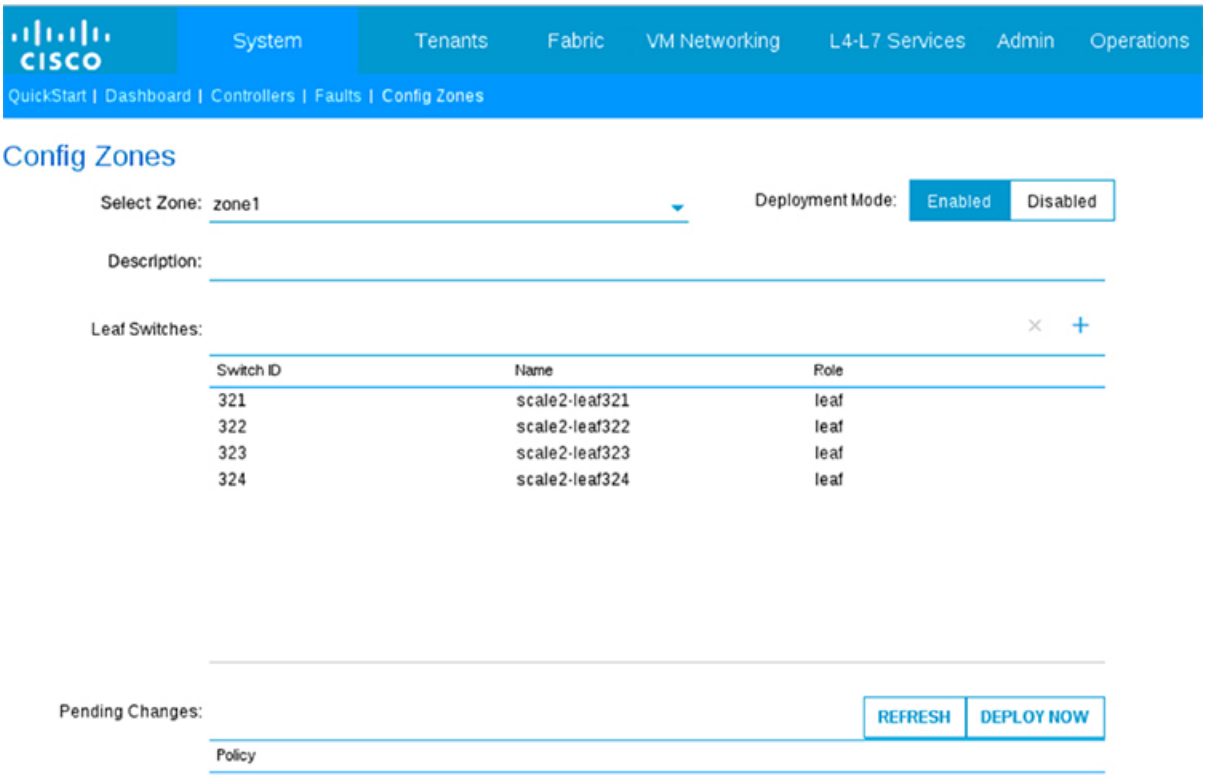
- `infrazone`設定に従わないポリシーの場合、APICは更新をすべてのファブリック ノードに即座に送信します。
- `infrazone` 設定に従うポリシーの場合、更新は `infrazone` 設定に応じて次のように続行します。
  - ノードが`infrazone:Zone`に属している場合、ゾーンの展開モードが有効に設定されていれば、更新は即座に送信されます。設定されていなければ、更新は延期されます。
  - ノードが`infrazone:Zone`に属していない場合、更新は即座に実行されます。これはACIファブリックのデフォルトの動作です。

GUI を使用した設定ゾーンの作成

はじめる前に

この手順では、GUI を使用して設定ゾーンを作成する方法について説明します。

次の画面は、設定ゾーンの作成、その展開モードの設定、ゾーンへのノードの追加を実行できるGUIの場所を示しています。このビューで、すべての延期された更新情報を確認できます。



NX-OS スタイルの CLI を使用した設定ゾーンの作成

この手順では、NX-OS CLI を使用して設定ゾーンを作成する方法について説明します。

NX-OS CLI を使用して設定ゾーンを作成するには、次の手順に従います。

例：

```
apic1# configure
apic1(config)# zones
apic1(config-zones)# zone testZone
apic1(config-zone)# description testZone-Description
apic1(config-zone)# deployment-mode enabled
apic1(config-zone)# switch 101-102 , 103
apic1(config-zone)# exit
apic1(config-zones)# exit
apic1(config)# exit
```

REST API を使用した設定ゾーンの作成

はじめる前に

この手順では、REST API を使用して設定ゾーンを作成する方法について説明します。

REST API を使用して設定ゾーンを作成するには、次の手順に従います。

例：

```
<infraInfra>
        <infrazoneZoneP name="default">
    <infrazoneZone name=”Group1" deplMode="disabled">
    <infrazoneNodeGrp name=”nodeGroup">
     <infraNodeBlk name=”nodeblk1" from_=101 to_=101/>
     <infraNodeBlk name=”nodeblk2” from_=103 to_=103/>
    </infrazoneNodeGrp>
   </infrazoneZone>
   <infrazoneZone name=”Group2" deplMode="enabled">
    <infrazoneNodeGrp name=”nodeGroup2">
     <infraNodeBlk name=”nodeblk" from_=102 to_=102/>  </infrazoneNodeGrp>
    </infrazoneZone>
   </infrazoneZoneP>
</infraInfra>
```

設定ゾーンのサポート対象ポリシー

次のポリシーが、設定ゾーン用にサポートされています。

```
analytics:CfgSrv
bgp:InstPol
callhome:Group
callhome:InvP
callhome:QueryGroup
cdp:IfPol
cdp:InstPol
comm:Pol
comp:DomP
coop:Pol
datetime:Pol
dbgexp:CoreP
dbgexp:TechSupP
dhcp:NodeGrp
dhcp:PodGrp
edr:ErrDisRecoverPol
ep:ControlP
ep:LoopProtectP
eqptdiagp:TsOdFabP
eqptdiagp:TsOdLeafP
fabric:AutoGEp
fabric:ExplicitGEp
fabric:FuncP
fabric:HIfPol
fabric:L1IfPol
fabric:L2IfPol
fabric:L2InstPol
fabric:L2PortSecurityPol
```

```
fabric:LeCardP
fabric:LeCardPGrp
fabric:LeCardS
fabric:LeNodePGrp
fabric:LePortP
fabric:LePortPGrp
fabric:LFPortS
fabric:NodeControl
fabric:OLeafS
fabric:OSpineS
fabric:PodPGrp
fabric:PortBlk
fabric:ProtGEp
fabric:ProtPol
fabric:SFPortS
fabric:SpCardP
fabric:SpCardPGrp
fabric:SpCardS
fabric:SpNodePGrp
fabric:SpPortP
fabric:SpPortPGrp
fc:DomP
fc:FabricPol
fc:IfPol
fc:InstPol
file:RemotePath
fvns:McastAddrInstP
fvns:VlanInstP
fvns:VsanInstP
fvns:VxlanInstP
infra:AccBaseGrp
infra:AccBndlGrp
infra:AccBndlPolGrp
infra:AccBndlSubgrp
infra:AccCardP
infra:AccCardPGrp
infra:AccNodePGrp
infra:AccPortGrp
infra:AccPortP
infra:AttEntityP
infra:CardS
infra:ConnFexBlk
infra:ConnFexS
infra:ConnNodeS
infra:DomP
infra:FexBlk
infra:FexBndlGrp
infra:FexGrp
infra:FexP
infra:FuncP
infra:HConnPortS
infra:HPathS
infra:HPortS
infra:LeafS
infra:NodeBlk
infra:NodeGrp
infra:NodeP
infra:OLeafS
infra:OSpineS
infra:PodBlk
infra:PodGrp
infra:PodP
infra:PodS
infra:PolGrp
infra:PortBlk
infra:PortP
infra:PortS
infra:PortTrackPol
infra:Profile
infra:SHPathS
infra:SHPortS
infra:SpAccGrp
infra:SpAccPortGrp
```

```
infra:SpAccPortP
infra:SpineP
infra:SpineS
isis:DomPol
l2ext:DomP
l2:IfPol
l2:InstPol
l2:PortSecurityPol
l3ext:DomP
lacp:IfPol
lacp:LagPol
lldp:IfPol
lldp:InstPol
mcp:IfPol
mcp:InstPol
mgmt:NodeGrp
mgmt:PodGrp
mon:FabricPol
mon:InfraPol
phys:DomP
psu:InstPol
qos:DppPol
snmp:Pol
span:Dest
span:DestGrp
span:SpanProv
span:SrcGrp
span:SrcTargetShadow
span:SrcTargetShadowBD
span:SrcTargetShadowCtx
span:TaskParam
span:VDest
span:VDestGrp
span:VSpanProv
span:VSrcGrp
stormctrl:IfPol
stp:IfPol
stp:InstPol
stp:MstDomPol
stp:MstRegionPol
trig:SchedP
vmm:DomP
vpc:InstPol
vpc:KAPol
```

第 9 章

ACL の許可および拒否ログを使用したトラブルシューティング

GUI を使用した ACL 契約許可ロギングの有効化

次の手順は、GUI を使用して契約許可ロギングを有効にする方法を示しています。

ステップ 1 メニュー バーで、[Tenants] > [<tenant name>] の順に選択します。

ステップ 2 [Navigation] ペインで、[Security Policies] を展開します。

ステップ 3 [Contracts] を右クリックし、[Create Contract] を選択します。

ステップ 4 [Create Contract] 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、契約の名前を入力します。

b) [Scope] フィールドで、そのスコープ（[VRF]、[Tenant]、または [Global]）を選択します

c) オプション。契約に適用するターゲット DSCP または QoS クラスを設定します。

d) [Subjects] を展開します。

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

ステップ 6 件名と説明（オプション）を入力します。

ステップ 7 オプション。ターゲット DSCP のドロップダウン リストから、件名に適用する DSCP を選択します。

ステップ 8 契約を両方向でなくコンシューマからプロバイダの方向にのみ適用するのでない限り、[Apply Both Directions] はオンにしたままにしておきます。

ステップ 9 [Apply Both Directions] をオフにした場合は、[Reverse Filter Ports] をオンのままにして、レイヤ 4 の送信元と宛先のポートを交換します。これによりルールはプロバイダからコンシューマに適用されます。

ステップ 10 [Filter Chain] を展開します。

ステップ 11 [Name] ドロップダウン リストで、オプションを選択します。たとえば [arp]、[default]、[est]、または [icmp] をクリックします。

ステップ 12 [Directives] ドロップダウン リストで、[log] をクリックします。

ステップ 13 [Update] をクリックします。

ステップ 14 [OK] をクリックします。

ステップ 15 [Submit] をクリックします。
ロギングがこの契約に対して有効になります。

NX-OS CLI を使用した ACL 契約許可ロギングの有効化

次の例は、NX-OS CLI を使用して契約許可ロギングを有効にする方法を示しています。

ステップ 1 契約許可ルールにより送信できたパケットまたはフローのロギングを有効にするには、次のコマンドを使用します。

```
configure
tenant <tenantName>
contract <contractName> type <permit>
subject <subject Name>
access-group <access-list> <in/out/both> log
```

例：
次に例を示します。

```
apic1# configure
apic1(config)# tenant BDMode1
apic1(config-tenant)# contract Logicmp type permit
apic1(config-tenant-contract)# subject icmp
apic1(config-tenant-contract-subj)# access-group arp both log
```

ステップ 2 許可ロギングを無効にするには、no 形式の access-group コマンドを使用します。たとえば、`no access-group arp both log` コマンドを使用します。

REST API を使用した ACL 契約許可ロギングの有効化

次の例は、REST API を使用して契約許可ロギングを有効にする方法を示しています。

契約許可ロギングを有効にするには、次の例のようなデータを POST します。

```
POST https://192.0.20.123/api/node/mo/uni/tn-sgladwin_t1/brc-ICMP_Contract.json
{
"vzBrCP":{
   "attributes":{
      "dn" : "uni/tn-sgladwin_t1/brc-ICMP_Contract",
      "name" : "ICMP_Contract",
      "rn" : "brc-ICMP_Contract","
      "status" : "created"},
   "children":[{
      "vzSubj":{
         "attributes":{
            "dn" : "uni/tn-sgladwin_t1/brc-ICMP_Contract/subj-Permit_Contract_ICMP",
            "name" : "Permit_Contract_ICMP","rn":"subj-Permit_Contract_ICMP",
            "status":"created"},
   "children":[{
      "vzRsSubjFiltAtt":{
            "attributes":{
            "status":"created,modified",
            "tnVzFilterName":"icmp",
            "directives":"log"},
   "children":[]}}]}}]}}
response: {"totalCount":"0","imdata":[]}
```

GUI を使用した禁止契約拒否ロギングの有効化

次の手順は、GUI を使用して禁止契約拒否ロギングを有効にする方法を示しています。

ステップ 1 メニュー バーで、[Tenants] > [<tenant name>] の順に選択します。

ステップ 2 [Navigation] ペインで、[Security Policies] を展開します。

ステップ 3 [Taboo Contracts] を右クリックし、[Create Taboo Contract] を選択します。

ステップ 4 [Create Taboo Contract] ダイアログ ボックスで、次の操作を実行して禁止契約を指定します。

a) [Name] フィールドに、契約の名前を入力します。

b) オプション。[Description] フィールドに、禁止契約の説明を入力します。

c) [Subjects] を展開します。

ステップ 5 b. [Create Taboo Contract Subject] ダイアログ ボックスで、次の操作を実行します。

a) [Specify Identity of Subject] 領域に、名前と説明（オプション）を入力します。

b) [Filters] を展開します。

c) [Name] ドロップダウン リストから、<tenant_name>/arp、<tenant_name>/default、<tenant_name>/est、<tenant_name>/icmp のいずれかの値、または [Create Filter] を選択します。

（注） [Specify Filter Identity] 領域で [Create Filter] を選択した場合、次の操作を実行して、ACL 拒否ルールの基準を指定します。

1. 名前とオプションの説明を入力します。
2. [Entries] を展開し、ルールの名前を入力し、ルールの ACL 拒否条件を選択します。
3. [Update] をクリックします。
4. [Submit] をクリックします。`

ステップ 6 [Directives] ドロップダウン リストで、[log] をクリックします。

ステップ 7 [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。
ロギングがこの禁止契約に対して有効になります。

NX-OS CLI を使用した禁止契約拒否ロギングの有効化

次の例は、NX-OS CLI を使用して禁止契約拒否ロギングを有効にする方法を示しています。

ステップ 1 禁止契約拒否ルールのためにドロップされたパケットまたはフローのロギングを有効にするには、次のコマンドを使用します。

```
configure
tenant <tenantName>
contract <contractName> type <deny>
subject <subject Name>
access-group <access-list> <both> log
```

例：
次に例を示します。

```
apic1# configure
apic1(config)# tenant BDMode1
apic1(config-tenant)# contract dropFTP type deny
```

```
apic1(config-tenant-contract)# subject dropftp
apic1(config-tenant-contract-subj)# access-group https both log
```

ステップ 2 拒否ロギングを無効にするには、no 形式の access-group コマンドを使用します。たとえば、`no access-group https both log` コマンドを使用します。

REST API を使用した禁止契約拒否ロギングの有効化

次の例は、REST API を使用して禁止契約拒否ロギングを有効にする方法を示しています。

ACL 拒否ロギングを有効にするには、次の例のようなデータを POST します。

```
POST https://192.0.20.123/api/node/mo/uni/tn-sgladwin_t1/taboo-TCP_Taboo_Contract.json
{
"vzTaboo":{
   "attributes":{
      "dn":"uni/tn-sgladwin_t1/taboo-TCP_Taboo_Contract",
      "name":"TCP_Taboo_Contract",
      "rn":"taboo-TCP_Taboo_Contract",
      "status":"created"},
   "children":[{
      "vzTSubj":{
         "attributes":{
            "dn":"uni/tn-sgladwin_t1/taboo-TCP_Taboo_Contract/tsubj-TCP_Filter_Subject",
            "name":"TCP_Filter_Subject",
            "rn":"tsubj-TCP_Filter_Subject",
            "status":"created"},
         "children":[{
            "vzRsDenyRule":{
               "attributes":{
                  "tnVzFilterName":"TCP_Filter",
                  "directives":"log",
                  "status":"created"},
         "children":[]}}]}}]}}
response: {"totalCount":"0","imdata":[]}
```

GUI を使用した ACL 許可および拒否ログの表示

次の手順は、GUI を使用して、トラフィック フローの ACL 許可および拒否ログを（有効になっていれば）表示する方法を示しています。

ステップ 1 メニュー バーで、[Tenants] > [<tenant name>] の順に選択します。

ステップ 2 [Navigation] ペインで、[Tenant <tenant name>] をクリックします。

ステップ 3 [Tenant <tenant name>] 作業ペインで、[Operational] タブをクリックします。

ステップ 4 [Operational] タブの下で、[Flows] タブをクリックします。
[Flows] タブの下で、いずれかのタブをクリックして、レイヤ 2 許可ログ（[L2 Permit]）、レイヤ 3 許可ログ（[L3 Permit]）、レイヤ 2 拒否ログ（[L2 Drop]）、またはレイヤ 3 拒否ログ（[L3 Drop]）のログ データを表示します。各タブで、トラフィックがフローしていれば、ACL ロギング データを表示できます。データ ポイントは、ログ タイプと ACL ルールに応じて異なります。たとえば、[L3 Permit] ログには次のデータ ポイントが含まれます。

- Timestamp
- VRF
- 送信元 IP アドレス
- 宛先 IP アドレス
- プロトコル
- 送信元ポート
- 宛先ポート
- 送信元 MAC アドレス
- 宛先 MAC アドレス
- ノード（データ送信元のスイッチ）
- 送信元インターフェイス
- VLAN
- VRF カプセル化

（注） また、[Flows] タブの横の [Packets] タブを使用して、シグニチャ、送信元、および宛先が同じであるパケットのグループ（最大 10 個）の ACL ログにアクセスできます。送信されたりドロップされたりするパケットのタイプを確認できます。

REST API を使用した ACL 許可および拒否ログ

次の例は、REST API を使用して、トラフィック フローの許可および拒否ログ データを表示する方法を示しています。

はじめる前に

ACL 契約許可および拒否ログのデータを表示する前に、許可または拒否ロギングを有効にする必要があります。

REST API を使用して次のクエリを送信します。

```
GET
https://192.0.20.123/api/node/mo/uni/tn-sgladwin_t1.json?rsp-subtree-include=stats&rsp-subtree-class=fvOverallHealthHist15min
{
"totalCount":"1",
"imdata":[{
"fvTenant":{
   "attributes":{
       "childAction":"",
       "descr":"",
       "dn":"uni/tn-sgladwin_t1",
       "lcOwn":"local",
       "modTs":"2016-06-22T15:46:30.745+00:00",
       "monPolDn":"uni/tn-common/monepg-default",
       "name":"sgladwin_t1",
       "ownerKey":"",
       "ownerTag":"",
       "status":"",
       "uid":"15374"
}}}]}
```

NX-OS CLI を使用した ACL 許可および拒否ログの表示

次の手順は、NX-OS CLI **show acllog** コマンドを使用して ACL ログの詳細を表示する方法を示しています。

コマンドの完全な構文は、次のとおりです。**show acllog {permit | drop} l3 {pkt | flow} tenant <tenant name> vrf <vrf name> srcip <source ip> dstip <destination ip> srcport <source port> dstport <destination port> protocol <protocol> srcintf <source interface> start-time <startTime> end-time <endTime>**

ステップ 1 次の例では、**show acllog permit l3 pkt tenant <tenant name> vrf <vrf name> [detail]** コマンドを使用して、送信された一般的な VRF ACL レイヤ 3 許可パケットに関する詳細情報を表示する方法を示しています。

```
apic1# show acllog permit l3 pkt tenant common vrf default detail
acllog permit l3 packets detail:
srcIp      : 10.2.0.19
dstIp      : 10.2.0.16
protocol   : udp
srcPort    : 13124
dstPort    : 4386
srcIntf    : port-channel5
vrfEncap   : VXLAN: 2097153
pktLen     : 112
srcMacAddr : 00:00:15:00:00:28
dstMacAddr : 00:00:12:00:00:25
timeStamp  : 2015-03-17T21:31:14.383+00:00
```

ステップ 2 次の例では、**show acllog** コマンドを使用して、一般的な VRF レイヤ 3 UDP パケット（送信元 IP アドレス 10.2.0.19、宛先 IP アドレス 10.2.0.16、送信元ポート 13124、宛先ポート 4386、送信元インターフェイス ポートチャネル 15、開始時刻 2015-03-17T21:00:00、および終了時刻 2015-03-18T00:00:00）に関する情報を表示する方法を示しています。

```
apic1# show acllog permit l3 pkt tenant common vrf copy srcip 10.2.0.19 dstip 10.2.0.16 srcport
13124 dstport 4386
protocol 17 srcintf port-channel5 start-time 2015-03-17T21:00:00 end-time  2015-03-18T00:00:00
acllog Permit L3 Packets
     srcIp       dstIp         protocol  srcport   dstport   Node      srcIntf         vrfEncap
      pktLen   timeStamp
 ------------    -----------   -----     --------  -------   ------   ---------       -------------
   --------  --------------
   10.2.0.19     10.2.0.16      udp      13124      4386      101      port-channel5   VXLAN:
2097153   112      2015-03-17T21:


                        31:14.383+00:00
```

ステップ 3 次の例では、 **show acllog permit l2 pkt tenant <tenant name> vrf <vrf name> [detail]** コマンドを使用して、送信されたデフォルトの VRF レイヤ 2 パケットに関する詳細情報を表示する方法を示しています。

```
apic1# show acllog permit l2 pkt tenant common vrf default detail

acllog permit l2 packets detail:
srcIntf    : port-channel5
pktLen     : 1
srcMacAddr : 00:00:66:00:00:66
```

```
dstMacAddr : 00:00:89:00:00:00
timeStamp  : 2015-03-17T21:31:14.383+00:00
```

ステップ 4 次の例では、**show acllog permit l2 pkt tenant <tenant name> vrf <vrf name> srcintf <s interface>** コマンドを使用して、インターフェイス ポートチャネル 15 から送信されたデフォルトの VRF レイヤ 2 パケットに関する情報を表示する方法を示しています。

```
apic1# show acllog permit l2 pkt tenant common vrf default srcintf port-channel5
acllog permit L2 Packets
      Node          srcIntf       pktLen     timeStamp
 --------------  --------------  --------  --------------
                 port-channel5      1      2015-03-17T21:
                                           31:14.383+00:00
```

ステップ 5 次の例では、**show acllog drop l3 pkt tenant <tenant name> vrf <vrf name> [detail]** コマンドを使用して、ACL 拒否ルールによりドロップされたパケットに関する詳細情報を表示する方法を示しています。

```
apic1# show acllog drop l3 pkt tenant common vrf copy detail
acllog drop l3 packets detail:
srcIp      : 10.2.0.19
dstIp      : 10.2.0.16
protocol   : udp
srcPort    : 13124
dstPort    : 4386
srcIntf    : port-channel5
vrfEncap   : VXLAN: 2097153
pktLen     : 112
srcMacAddr : 00:00:15:00:00:28
dstMacAddr : 00:00:12:00:00:25
timeStamp  : 2015-03-17T21:31:14.383+00:00
```

ステップ 6 次の例は、**show acllog drop l3 flow tenant <tenant name> vrf <vrf name> srcip <source ip> dstip <dst ip> srcport <src port> dstport <dst port> protocol <protocol> srcintf <src intf>** コマンドの使用方法を示しています。このコマンドにより、UDP パケット（ドロップされたもの、および送信元 IP アドレス 10.2.0.19、宛先 IP アドレス 10.2.0.16、送信元ポート 13124、宛先ポート 4386、およびソース インターフェイス ポートチャネル 15 を持つもの）についての情報が表示されます。

```
apic1# show acllog drop l3 pkt tenant common vrf copy srcip 10.2.0.19 dstip 10.2.0.16 srcPort 13124
 dstPort 4386 protocol 17 srcintf port-channel5
acllog drop L3 Packets
     srcIp           dstIp       protocol  srcPort   dstPort        Node          srcIntf
 vrfEncap      pktLen     timeStamp
 --------------  --------------  --------  --------  --------  --------------  --------------
--------------  --------  --------------
   10.2.0.19       10.2.0.16       udp      13124      4386                    port-channel5
VXLAN: 2097153    112     2015-03-17T21: 31:14.383+00:00
```

ステップ 7 次の例は、**show acllog drop l2 pkt tenant <tenant name> vrf <vrf name> [detail]** コマンドの使用方法を示しています。このコマンドは、ACL 拒否ルールのためにドロップされたパケットに関する詳細情報を表示します。

```
apic1# show acllog drop l2 pkt tenant common vrf copy detail
```

```
acllog drop l2 packets detail:
srcIntf    : port-channel87
pktLen     : 1122
srcMacAddr : 00:00:11:00:00:11
dstMacAddr : 11:00:32:00:00:33
timeStamp  : 2015-03-17T21:31:14.383+00:00
```

ステップ 8 次の例は、**show acllog drop l2 pkt tenant <tenant name> vrf <vrf name> srcintf <srcintf name>** コマンドの使用方法を示しています。このコマンドは、特定のインターフェイスから発信された、ドロップされたパケットに関する情報を表示します。

```
apic1# show acllog drop l2 pkt tenant common vrf copy srcintf port-channel87
acllog drop L2 Packets
      Node          srcIntf       pktLen     timeStamp
 --------------  --------------  --------  --------------
                 port-channel87    1122    2015-03-17T21:
                                           31:14.383+00:00
```

第 10 章

マルチポッドのトラブルシューティング

GUI を使用したマルチポッドのトラブルシューティング

TBD（Vipul Jain と Vijay Krishnan がこの機能の手順を送ることになっている SME です）

NX-OSCLIを使用したマルチポッドのトラブルシューティング

TBD：Vipul および Vijay から情報を待っています。

REST API を使用したマルチポッドのトラブルシューティング

TBD

第 11 章

デジタルオプティカルモニタリングを使用したトラブルシューティング

GUI を使用したデジタル オプティカル モニタリングの有効化

物理インターフェイスに関するデジタル オプティカル モニタリング（DOM）統計情報を表示するには、その前にスイッチポリシーを使用し、グループポリシーに関連付けて、リーフまたはスパイン インターフェイスの DOM を有効にします。

GUI を使用して DOM を有効にするには、次の手順に従います。

ステップ 1 メニュー バーで、[Fabric] > [Fabric Policies] の順に選択します。

ステップ 2 [Navigation] ペインで、[Switch Policies] > [Policies] > [Fabric Node Controls] の順に展開します。

ステップ 3 [Fabric Node Controls] を展開すると、既存のポリシーのリストが表示されます。

ステップ 4 [Work] ペインで、[ACTIONS] ドロップダウン メニューをクリックし、[Create Fabric Node Control] を選択します。
[Create Fabric Node Control] ダイアログ ボックスが表示されます。

ステップ 5 [Create Fabric Node Control] 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) オプション。[Description] フィールドに、ポリシーの説明を入力します。
c) [Enable DOM] の横にあるボックスをオンにします。

ステップ 6 [SUBMIT] をクリックして、ポリシーを作成します。
これでこのポリシーを、続くいくつかの手順に従って、ポリシー グループおよびプロファイルに関連付けることができます。

ステップ 7 [Navigation] ペインで、[Switch Policies] > [Policy Groups] の順に展開します。

ステップ 8 [Work] ペインで、[ACTIONS] ドロップダウン メニューをクリックし、[Create Leaf Switch Policy Group]（スパインの場合は [Create Spine Switch Policy Group]）を選択します。
[Create Leaf Switch Policy Group] または [Create Spine Switch Policy Group] ダイアログ ボックスが表示されます。

ステップ 9 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 グループの名前を入力します。
b) [Node Control Policy] ドロップダウン メニューから、既存のポリシー（作成したばかりのポリシーなど）を選択するか、または [Create Fabric Node Control] を選択します。
c) [Submit] をクリックします。

ステップ 10 作成したポリシー グループをスイッチに次のように接続します。

a) [Navigation] ペインで、[Switch Policies] > [Profiles] を展開します。
b) [Work] ペインで、[ACTIONS] ドロップダウン メニューをクリックし、[Create Leaf Switch Profile] または [Create Spine Switch Profile] を選択します。
c) ダイアログ ボックスで、[Name] フィールドにプロファイルの名前を入力します。
d) プロファイルに関連付けるスイッチの名前を、[Switch Associations] で追加します。
e) [Blocks] プルダウン メニューから、該当するスイッチの横のチェックボックスをオンにします。
f) [Policy Group] プルダウン メニューから、前に作成したポリシー グループを選択します。
g) [UPDATE] をクリックし、[SUBMIT] をクリックします。

REST API を使用したデジタル オプティカル モニタリングの有効化

物理インターフェイスに関するデジタル オプティカル モニタリング（DOM）統計情報を表示するには、インターフェイスの DOM を有効にします。

REST API を使用して DOM を有効にするには、次の手順に従います。

ステップ 1 次の例のように、ファブリック ノード制御ポリシー（fabricNodeControlPolicy）を作成します。

```
<fabricNodeControl dn="uni/fabric/nodecontrol-testdom" name="testdom" control="1"
rn="nodecontrol-testdom" status="created" />
```

ステップ 2 次のように、ファブリック ノード制御ポリシーをポリシー グループに関連付けます。

```
<?xml version="1.0" encoding="UTF-8" ?>
 <fabricLeNodePGrp dn="uni/fabric/funcprof/lenodepgrp-nodegrp2" name="nodegrp2"
rn="lenodepgrp-nodegrp2" status="created,modified" >

    <fabricRsMonInstFabricPol tnMonFabricPolName="default" status="created,modified" />
    <fabricRsNodeCtrl tnFabricNodeControlName="testdom" status="created,modified" />

</fabricLeNodePGrp>
```

ステップ 3 ポリシー グループをスイッチ（次の例ではスイッチは 103）に、次のように関連付けます。

```
<?xml version="1.0" encoding="UTF-8" ?>
 <fabricLeafP>
  <attributes>
   <dn>uni/fabric/leprof-leafSwitchProfile</dn>
   <name>leafSwitchProfile</name>
   <rn>leprof-leafSwitchProfile</rn>
   <status>created,modified</status>
  </attributes>
  <children>
   <fabricLeafS>
    <attributes>
     <dn>uni/fabric/leprof-leafSwitchProfile/leaves-test-typ-range</dn>
     <type>range</type>
     <name>test</name>
     <rn>leaves-test-typ-range</rn>
     <status>created,modified</status>
    </attributes>
    <children>
     <fabricNodeBlk>
      <attributes>
       <dn>uni/fabric/leprof-leafSwitchProfile/leaves-test-typ-range/nodeblk-09533c1d228097da</dn>

       <from_>103</from_>
       <to_>103</to_>
       <name>09533c1d228097da</name>
       <rn>nodeblk-09533c1d228097da</rn>
       <status>created,modified</status>
      </attributes>
     </fabricNodeBlk>
    </children>
    <children>
     <fabricRsLeNodePGrp>
      <attributes>
       <tDn>uni/fabric/funcprof/lenodepgrp-nodegrp2</tDn>
       <status>created</status>
      </attributes>
     </fabricRsLeNodePGrp>
    </children>
   </fabricLeafS>
```

```
 </children>
</fabricLeafP>
```

GUI を使うデジタル オプティカル モニタリングを使用したトラブルシューティング

GUI を使用して DOM 統計情報を表示するには、次の手順に従います。

はじめる前に

インターフェイスの DOM 統計情報を表示するには、インターフェイスのデジタル オプティカル モニタリング（DOM）統計情報を事前に有効にしておく必要があります。

ステップ 1 メニュー バーで、[Fabric]、[Inventory] の順に選択します。
ステップ 2 [Navigation] ペインで、調査する物理インターフェイスがあるポッドとリーフ ノードを展開します。
ステップ 3 [Interfaces] を展開します。
ステップ 4 [Physical Interfaces] を展開します。
ステップ 5 調査する物理インターフェイスを展開します。
ステップ 6 [DOM Stats] を選択します。
DOM 統計情報がインターフェイスに表示されます。

REST API を使うデジタル オプティカル モニタリングを使用したトラブルシューティング

DOM 統計情報を XML の REST API クエリを使用して表示するには、次の手順に従います。

はじめる前に

インターフェイスの DOM 統計情報を表示するには、インターフェイスのデジタル オプティカル モニタリング（DOM）を事前に有効にしておく必要があります。

次の例は、REST API クエリを使用して、物理インターフェイスについての DOM 統計情報（node-104 の eth1/25）を表示する方法を示しています。

```
GET
https://192.0.20.123/api/node/mo/topology/pod-1/node-104/sys/phys-[eth1/25]/phys/domstats.xml?query-target=
children&target-subtree-class=ethpmDOMRxPwrStats&subscription=yes
```

次の応答が返されます。

```
response : {
   "totalCount":"1",
      "subscriptionId":"72057611234705430",
          "imdata":[
{"ethpmDOMRxPwrStats":{
   "attributes":{
      "alert":"none",
      "childAction":"",
      "dn":"topology/pod-1/node-104/sys/phys[eth1/25]/phys/domstats/rxpower",
      "hiAlarm":"0.158490",
      "hiWarn":"0.079430",
      "loAlarm":"0.001050",
      "loWarn":"0.002630",
      "modTs":"never",
      "status":"",
       "value":"0.139170"}}}]}
```

第 12 章

Cisco APIC パスワードの復元およびフォールバック ログイン ドメインの使用

APICパスワードの回復

APIC のパスワードを復元するには、次の手順に従います。

ステップ 1 「aci-admin-passwd-reset.txt」という空のファイルを作成し、保存します。

ステップ 2 このファイルを USB ドライブに追加します。

ステップ 3 USB ドライブを Cisco APIC の背面にある USB ポートの 1 つに接続します。

ステップ 4 Cisco Integrated Management Controller（CIMC）を使用するかまたはデバイスの電源を再投入して、APIC を再起動します。

ステップ 5 [Press any key to enter the menu] というプロンプトが APIC により表示された場合は、キーを押して起動プロセスを中断します。

ステップ 6 APIC は、サポートされる Linux バージョンを表示します。システムにインストールされたバージョンを強調表示し、**e** を押して起動コマンドを編集します。

ステップ 7 カーネルを強調表示し、**e** を押してコマンドをブート シーケンスで編集します。

ステップ 8 次に示すように、コマンドの最後に空のファイルの名前を追加します。

例：

```
[ Minimal BASH-like line editing is supported.  For the first word, TAB
  lists possible command completions. Anywhere else TAB lists the possible
```

```
  completions of a device/filename. ESC at any time cancels. ENTER
  at any time accepts your changes.]

< rhgb quiet selinux=0 audit=1  aci-admin-passwd-reset
```

ステップ 9 **Enter** キーを押して、ファイルを保存します。

ステップ 10 **b** を押して APIC を起動します。

（注） パスワードリセット操作をキャンセルし、デフォルトのブートパラメータに戻るには、**Esc** キーと **Enter** キーを押します。

ステップ 11 APIC が起動し、新しい管理者パスワードの入力を求めます。

NX-OS スタイルの CLI を使用した Cisco APIC 設定を消去するレスキューユーザ アカウントの使用

レスキューユーザは、APIC へのアクセスを（クラスタ内にない場合でも）提供する緊急ログインです。このログインを使用して、設定の消去を含め、トラブルシューティング コマンドを実行できます。

（注） APIC が正常なクラスタの一部である場合、レスキューユーザ アカウントは admin パスワードで保護されます。

ステップ 1 Cisco Integrated Management Controller（CIMC）コンソールを使用して APIC にアクセスします。

ステップ 2 レスキューユーザとしてログインします。

（注） admin パスワードを使用して APIC ファブリックにログオンしている場合、レスキューユーザ パスワードはその admin パスワードと同じです。そうでない場合、レスキューユーザ パスワードはありません。

ステップ 3 **acidiag touch** コマンドを使用して設定をクリアします。

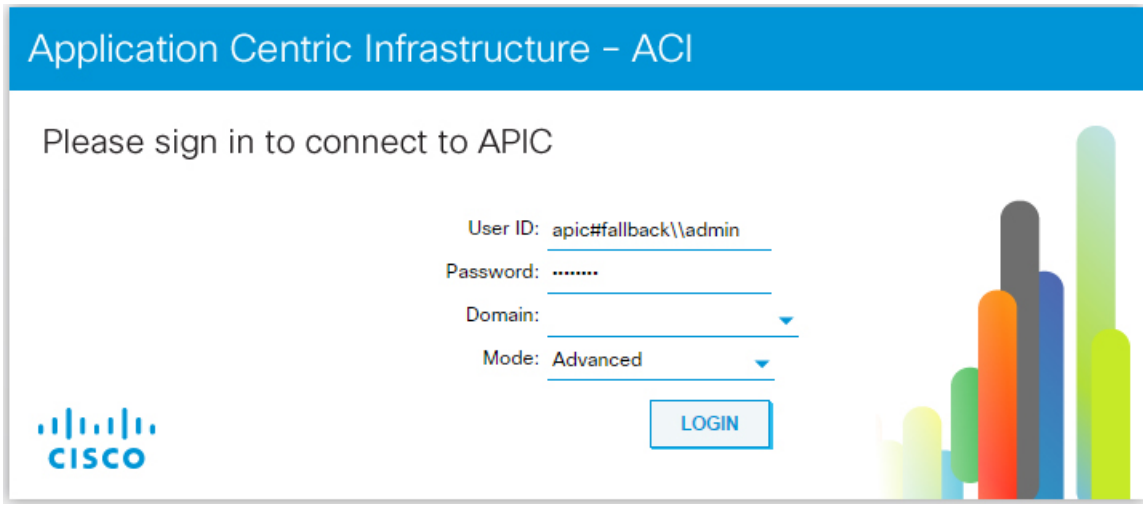
例：

```
apic1# acidiag touch setup
```

フォールバック ログイン ドメインを使用したローカル データベースへのログイン

ロックアウト時にローカルユーザデータベースを使用してログインできる、「フォールバック」という非表示のログイン ドメインがあります。認証方式に使用するユーザ名の形式は、`apic#fallback\\<username>` です。

フォールバック ログイン ドメインを使用して、ローカルデータベースにGUIでログインします。



または次に示すように、NX-OS CLIを使用して、フォールバック ログイン ドメインにログインします。

```
apic1(config)# aaa authentication login domain fallback
apic1(config-domain)# ?
group Set provider group for login domain
realm Specify server realm
```

または次に示すように、REST API を使用して、フォールバック ログイン ドメインにログインできます。

- URL：https://ifav41-ifc1/api/aaaLogin.xml
- データ：

```
<aaaUser name="apic#fallback\\admin"
pwd="passwordhere"/>
```

第 13 章

リーフ接続のトラブルシューティング

切断されたリーフの復旧

リーフにプッシュされた設定により、リーフのすべてのファブリック インターフェイス（リーフをスパインに接続するインターフェイス）が無効になっている場合、リーフへの接続は完全に失われます。このリーフは、ファブリックで非アクティブになります。リーフに設定をプッシュしようとしても、接続が失われているため実行されません。この項では、そのようなシナリオでの接続解除リーフを復元する方法について説明します。ファブリック インターフェイスの少なくとも 1 つは、次の手順で有効にされている必要があり、残りのインターフェイスは、GUI、REST API、CLI を使用して有効にできます。最初のインターフェイスを有効にするには、REST API を使用してポリシーを POST し、POST したポリシーを削除してファブリック ポートを無効にします。以下のように、リーフにポリシーを POST して、無効のポートを有効にすることができます。

（注） 次の例では、1/49 はスパインに接続しているリーフ ポートの 1 つであると想定しています。

ステップ 1 APIC からブラックリスト ポリシーをクリアします（REST API を使用）。

例：

```
$APIC_Address/api/policymgr/mo/.xml
<polUni>
    <fabricInst>
        <fabricOOServicePol>
                        <fabricRsOosPath tDn="topology/pod-1/paths-$LEAF_Id/pathep-[eth1/49]"
lc="blacklist" status ="deleted" />
        </fabricOOServicePol>
    </fabricInst>
</polUni>
```

ステップ 2 **l1EthIfSetInServiceLTask** を使用して必要なインターフェイスを起動するために、ローカル タスクをノード自体に POST します。

例：

```
$LEAF_Address/api/node/mo/topology/pod-1/node-$LEAF_Id/sys/action.xml
<actionLSubj oDn="sys/phys-[eth1/49]">
<l1EthIfSetInServiceLTask adminSt='start'/>
</actionLSubj>
```

第 14 章

ファブリックの再構築

ファブリックの再構築

この手順により、ファブリックを再構築（再初期化）できます。これは次のいずれかの理由で実行が必要になる場合があります。

- TEP IP を変更する
- インフラ VLAN を変更する
- ファブリック名を変更する
- TAC トラブルシューティング タスクを実行する

⚠

注意 この手順は非常に破壊的です。既存のファブリックを削除して新しいファブリックを再作成することになります。

はじめる前に

この手順を開始する前に、次の点を確認します。

- 設定のスケジュールされた定期バックアップ
- リーフとスパインへのコンソール アクセス
- 設定済みで到達可能な CIMC（KVM コンソール アクセスに必要）

- Java の問題がない

ステップ 1 現在の設定を維持したい場合は、次の手順で設定のエクスポートを実行できます。http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/kb/b_KB_Using_Import_Export_to_Recover_Config_States.html

ステップ 2 KVM コンソールに接続して **>acidiag touch clean** と入力し、APIC を削除します（複数の APIC の削除は任意の順序で実行できます）。APIC を削除すると、APIC の設定は消去され、起動スクリプト内の設定で起動します。すべての APIC に対してこの手順を実行します。

（注） **acidiag touch** コマンドは、起動スクリプトで APIC を起動しないため、この手順では役に立ちません。

ステップ 3 ノードを削除し、この削除がすべてのリーフ/スパインで行われるようにします。ノードがファブリック検出モードで起動することと、以前に設定されたファブリックの一部ではないことを確認します。リーフ/スパインで、コンソール ポートに接続し、次のコマンドでノードを削除します。

a) **>acidiag touch clean**
b) **>acidiag touch setup**
c) **>acidiag reboot**

（注） 前のすべてのファブリック設定が削除されたことを確認するのは非常に重要です。前のいずれかのファブリック設定が 1 つのノードに存在しているだけでも、ファブリックは再構築できません。

ここでノードを、ファブリック検出用に再起動する必要があります。すべてのノードで、次の手順を実行します。

ステップ 4 すべての APIC に対して起動スクリプトを実行します。この時点で、上記の値、TEP、TEP Vlan、ファブリック名のいずれかまたはすべてを変更できます。これらがすべての APIC で一貫していることを確認します。詳細については、http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/getting-started/b_APIC_Getting_Started_Guide/b_APIC_Getting_Started_Guide_chapter_01.html#concept_F46E2193E3134CD090B65B16038D11A9 を参照してください。

ステップ 5 apic1 にログインし、次のサイトに示されている手順を使用して設定インポートを実行します。http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/kb/b_KB_Using_Import_Export_to_Recover_Config_States.html

ステップ 6 ノード上のファブリックを再構築するためにファブリックが前のファブリック登録ポリシーを使用しているため、数分待機します（ファブリックのサイズ次第では、このステップは時間がかかる可能性があります）。

第 15 章

ウィザードのトラブルシューティング

トラブルシューティング ウィザードについて

トラブルシューティング ウィザードにより、ネットワークの動作を理解して視覚化でき、問題が発生した場合にネットワークの懸念事項を軽減できます。

このウィザードにより、ユーザ（管理者ユーザ）は、2 つのエンドポイントを選択して指定可能な、特定の期間に発生する問題をトラブルシューティングできます。たとえば、断続的なパケッ

ト損失があるものの理由がわからない2つのエンドポイントがあるとします。トラブルシューティング GUI により、問題を評価し、このエラー動作を引き起こしていると推定される各マシンにログオンしなくても、問題を効果的に解決できます。

後からセッションを再実行する場合もあるため、セッションには一意の名前を指定してください。また、事前設定されたテストの使用も選択できます。デバッグは、エンドポイント間、内部から外部エンドポイントの方向、外部から内部エンドポイントの方向で実行できます。

さらに、デバッグを実行する期間を定義できます。トラブルシューティング GUI では、検索するエンドポイントの送信元および宛先エンドポイントを入力することができます。MAC、IPv4、またはIPv6アドレスを使用してこれを行い、それからテナント別に選択できます。また、TACに送信できるトラブルシューティング レポートを生成することもできます。

次の項では、トラブルシューティング ウィザードのトポロジについて説明します。これは調査中の 2 つのエンドポイントに関連する要素のみを示す、ファブリックの簡易表示です。

（注） トラブルシューティング ウィザード CLI コマンドのリストについては、『*Cisco APIC Command-Line Interface User Guide*（*Cisco APIC* コマンド行インターフェイス ユーザ ガイド）』を参照してください。

関連トピック

トラブルシューティング ウィザードの使用を開始する，（93 ページ）
トラブルシューティング ウィザードのトポロジ，（99 ページ）

トラブルシューティング ウィザードの使用を開始する

トラブルシューティング ウィザードの使用を開始する前に、管理者ユーザとしてログオンする必要があります。送信元と宛先のエンドポイント（Ep）を指定し、トラブルシューティング セッションの期間を選択します。この期間は、イベント、エラー レコード、展開レコード、監査ログ、および統計情報を取得するために使用されます（説明や期間は、[Start] をクリックする前の、ウィザードの最初のページでしか編集できません）。

（注） [GENERATE REPORT] ボタンまたは [START] ボタンを一度クリックしたら、送信元と宛先のエンドポイントは変更できません。送信元と宛先の情報を入力した後に変更するには、新しいセッションを開始する必要があります。

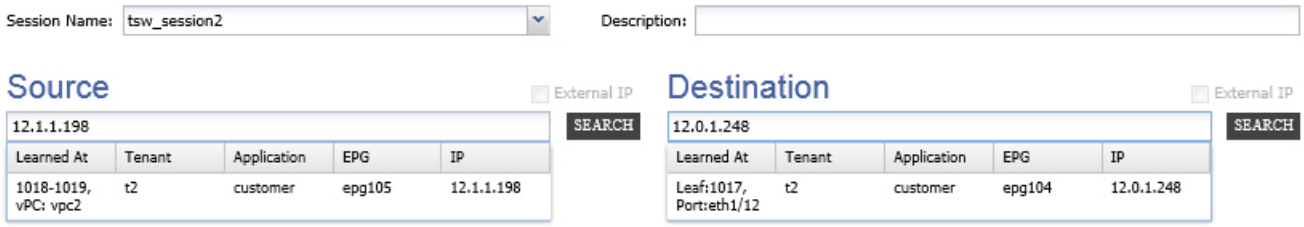
（注） トラブルシューティング ウィザードの画面をナビゲートするときには、いつでもスクリーンショットを撮り、画面の右上にある印刷アイコン（ ）をクリックしてプリンタに送信する（または PDF として保存する）ことができます。また、画面表示を変更できるズームインとズームアウトのアイコン（ ）もあります。

トラブルシューティング セッション情報を設定するには、次の手順を実行します。

ステップ 1 次のように、画面の上部から [OPERATIONS] を選択し、それから [VISIBILITY & TROUBLESHOOTING] を選択します。

[Visibility & Troubleshooting] 画面が表示されます。

ステップ 2 既存のトラブルシューティング セッションを（ドロップダウン メニューを使用して）使用するか、または新しいトラブルシューティングセッションを作成するかを選択できます。新しい住所を作成するには、[Session Name] フィールドに名前を入力します（以下では例として「tsw_session2」を使用しています）。



ステップ 3 追加情報を提供するために、[Description] フィールドに説明を入力します。（この手順は任意です）。

ステップ 4 [Source] プルダウン メニューから、MAC、IPv4、または IPv6 アドレスを入力するか、あるいは既存のものを選択します。

ステップ 5 [SEARCH] をクリックします。
ボックスが次のように表示され、選択に役立つ詳細情報を示す 1 つ以上の行が示されます。各行は、入力した IP アドレス（[IP] 列）が、特定のエンドポイント グループ（[EPG] 列）にあること、特定のアプリケーション（[Application] 列）に属すること、特定のテナント（[Tenant] 列）にあることを示します。リーフ番号、FEX 番号、およびポートの詳細が、[Learned At] 列に示されます。

ステップ 6 [Destination] プルダウン メニューから、MAC、IPv4、または IPv6 アドレスを入力するか、あるいは既存のものを選択します。

ステップ 7 [SEARCH] をクリックします。

ボックスが表示され、選択に役立つ詳細情報を示す 1 つ以上の行が示されます（前述の [Source] エンドポイント検索の説明と同じです）。

ステップ 8 外部インターネット プロトコルにエンドポイントを使用する場合は、[External IP] チェックボックスをオンにします。

（注） エンドポイントと外部 IP に関する詳細については、『*Cisco Application Centric Infrastructure Fundamentals*』の資料を参照してください。

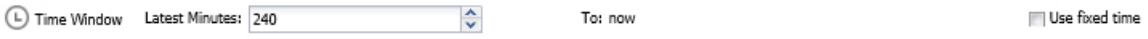
（注） 理想的には、同じテナントから送信元と宛先のエンドポイントを選択する必要があります。そのようにしないと、このマニュアルで後述するように、一部のトラブルシューティング機能が影響を受ける可能性があります。これらのエンドポイントを選択すると、[Faults] トラブルシューティング画面に示されている 2 つのエンドポイントを接続するトポロジついて把握できます。

ステップ 9 [From]（セッション開始時刻）と [To]（セッション終了時刻）プルダウン メニューで時刻を選んで、期間を選択します。

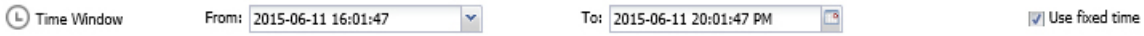
以下に示す [Time Window] は、過去の特定の期間内に発生した問題のデバッグに使用されます。また、イベント、すべてのレコード、展開レコード、監査ログ、および統計情報の取得にも使用されます。すべてのレコード用に 1 つと、個々のリーフ（またはノード）用に 1 つの、2 セットの期間があります。

（注） 期間の設定には 2 つのオプションがあり、[Use fixed time] チェックボックスを使用して切り替えることができます。

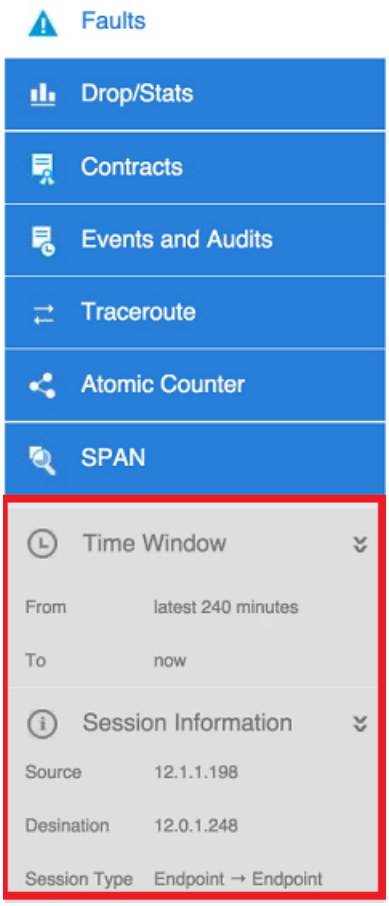
- 任意の「直近の分数」に基づいて（デフォルトは 240 分ですが、変更可能です）、次のように繰り返しの期間を指定できます。



- または、次のように [Use fixed time] チェックボックスをオンにして、[From] および [To] フィールドにセッションの固定期間を指定することもできます。



（注） デフォルトの期間は、セッションを作成した時刻に先立つ、デフォルトの「直近 240 分」に基づいたものになります（つまり、セッションには直近 240 分のデータが含まれることを意味します）。次に示すように、期間情報の設定または変更は、左側のナビゲーション ウィンドウの下部から行うこともできます。



ステップ 10 画面の右下にある [START] をクリックして、トラブルシューティング セッションを開始します。
トラブルシューティング セッションのトポロジ図が読み込まれて表示されます。

（注） トラブルシューティング ウィザード CLI コマンドのリストについては、『*Cisco APIC Command-Line Interface User Guide*（*Cisco APIC* コマンド行インターフェイス ユーザ ガイド）』を参照してください。

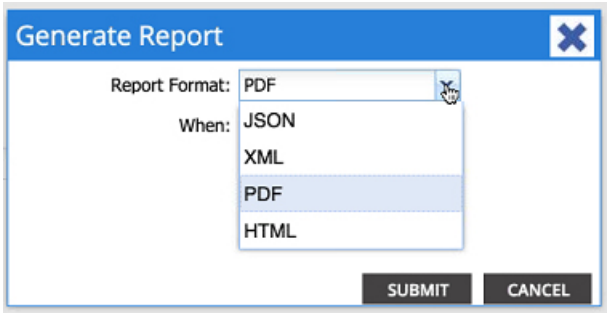
トラブルシューティング レポートの生成

トラブルシューティング レポートは、JSON、XML、PDF、および HTML などのいくつかの形式で生成できます。形式を選択した後は、レポートをダウンロード（またはレポートのダウンロードをスケジュール）して、それをオフライン分析に使用したり、TAC に送信してサポート ケースを作成したりできます。

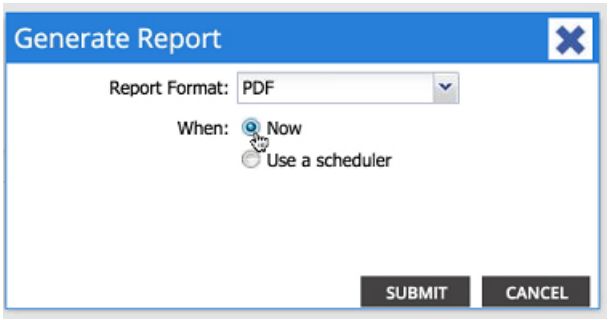
トラブルシューティング レポートを生成するには、次の手順に従います。

ステップ 1 画面の右下隅から、[GENERATE REPORT] を選択します。
次の手順に示されている、出力形式を選択できるボックスが表示されます。

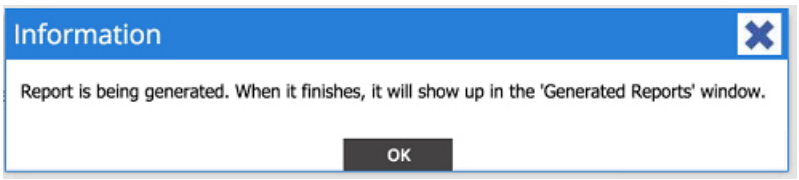
ステップ 2 [Generate Report] ドロップダウン ボックスから、出力形式（**XML**、**HTML**、**JSON**、または **PDF**）を次のように選択します。



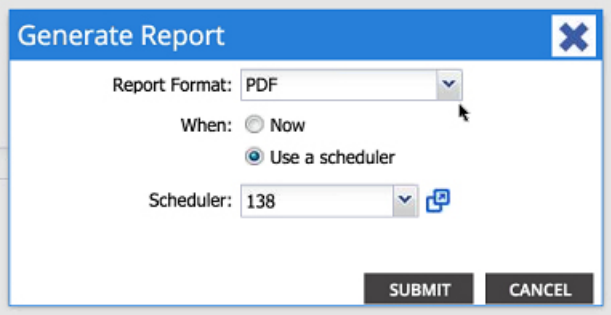
ステップ 3 レポートのダウンロードが即座に実行されるようにスケジュールするには、[Now] ボタンを次のようにオンにして、[SUBMIT] をクリックします。



[Information] ボックス（以下に示す）が表示され、生成されたレポートの取得場所が示されます。

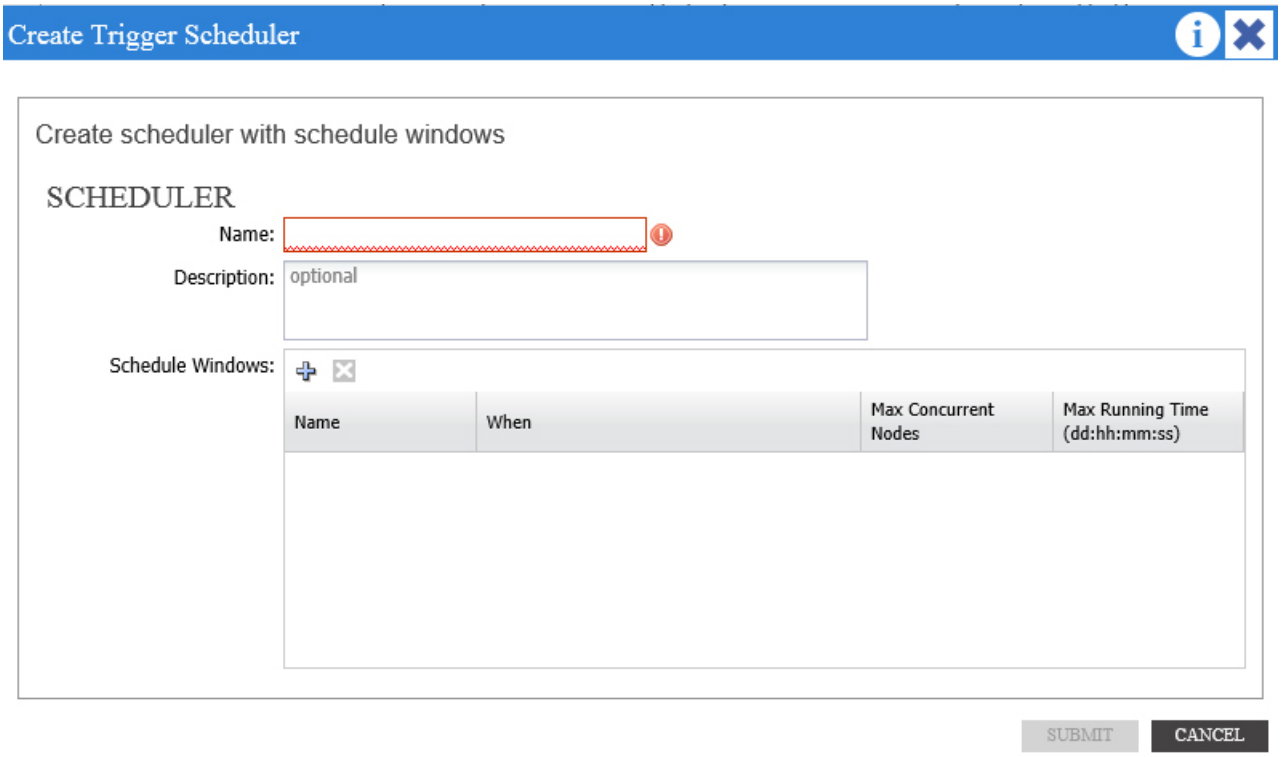


ステップ 4 レポートの生成が後で実行されるようにスケジュールするには、次のように [Use a scheduler] をクリックして、スケジュールを選択します。



[Scheduler] プルダウン メニューから、既存のスケジュールを選択するか、以下のように [Create Scheduler] を選択して新規スケジュールを作成します。

[CREATE TRIGGER SCHEDULE] ウィンドウが、以下のように表示されます。

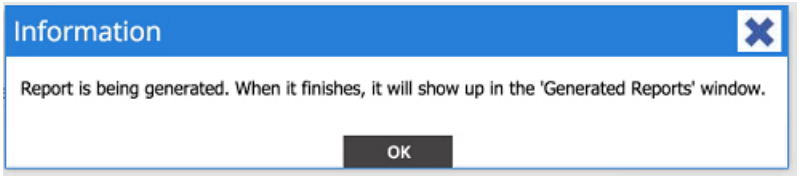


ステップ 5 [Name]、[Description]（オプション）、および [Schedule Windows] の情報を入力します。

（注） [SCHEDULER] の使用方法の詳細については、オンライン ヘルプを参照してください。

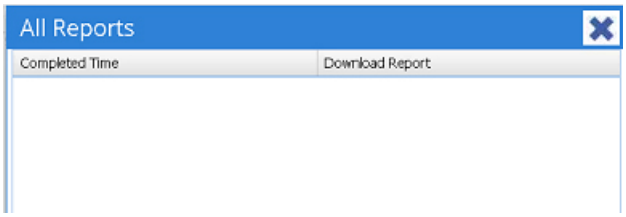
ステップ 6 [Submit] をクリックします。

ファブリックのサイズや存在するエラーまたはイベントの数に応じて、レポートの生成にはいくらかの時間がかかります（数分から最大で数十分）。レポートの生成中には、次のようにステータス メッセージが表示されます。



トラブルシューティング レポートを取得および表示するには、[SHOW GENERATED REPORTS] を選択します。
サーバのクレデンシャル（**ユーザ名**と**パスワード**）を、[Authentication Required] ウィンドウに入力します。トラブルシューティング レポートは、システムにローカルにダウンロードされます。

以下のように [ALL REPORTS] ウィンドウが表示され、直前にトリガーしたレポートも含め、生成したすべてのレポートが一覧表示されます。そこから、リンクをクリックして、選択した出力ファイル形式に応じてレポートをダウンロードするかまたはすぐに表示することができます（たとえば、ファイルが PDF であれば、ブラウザですぐに開くことができます）。



トラブルシューティング ウィザードのトポロジ

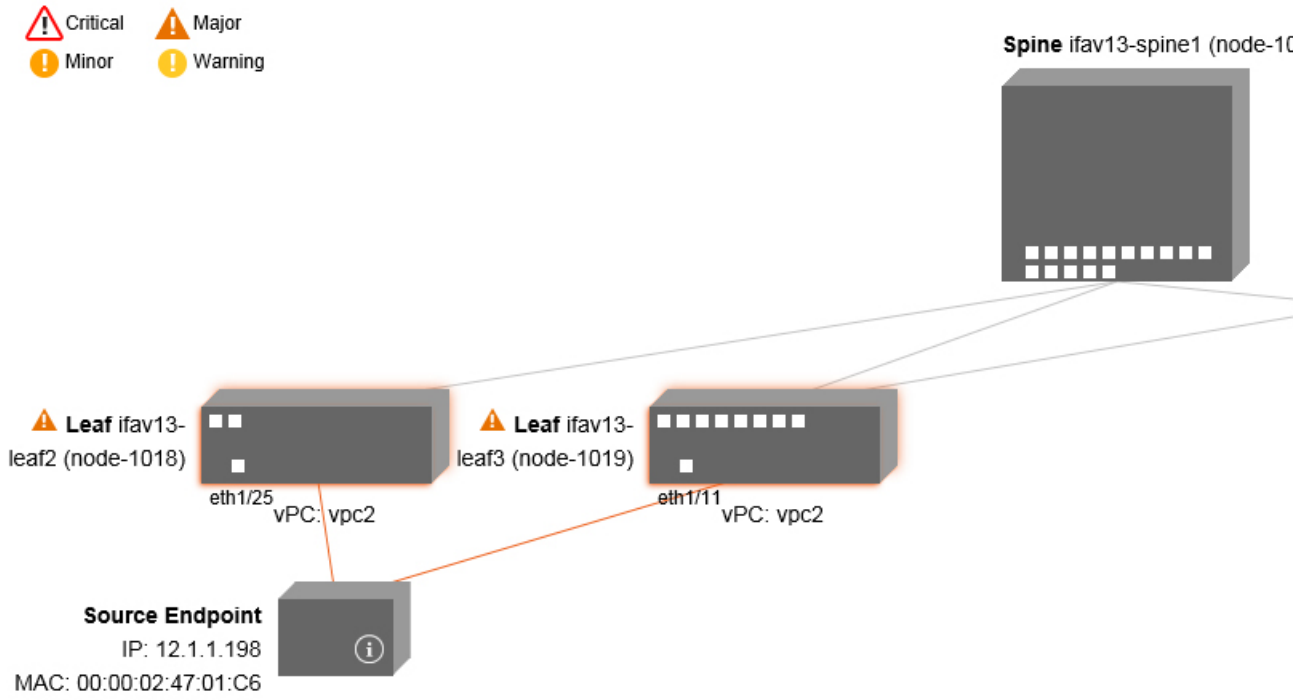
この項では、トラブルシューティング ウィザードのトポロジについて説明します。トポロジは、送信元と宛先エンド ポイント（Ep）のファブリックへの接続方法、送信元から宛先へのネットワーク パス、および中間スイッチについて示します。

次のウィザード トポロジ図に示すように、送信元エンドポイントはトポロジの左側に表示され、宛先エンドポイントは右側に表示されます。

（注） このウィザードのトポロジは、送信元エンドポイントから宛先エンドポイントへのトラフィックに関連するデバイスの、リーフ、スパイン、および FEX のみを示します。ただし、他にも多くのリーフ（何十、何百ものリーフや他の多くのスパイン）が存在する可能性があります。

このトポロジは、リンク、ポート、デバイスも示します。アイコンにカーソルを合わせると、EPが属しているテナント、属しているアプリケーション、および使用しているトラフィックのカプセル化（VLAN など）を表示できます。

次に示すように、画面の左側には色の凡例があり、トポロジ図の各色に関連付けられている重大度レベルが説明されています（たとえば、重大とマイナーなど）。



トポロジ内のボックスやポートなどのアイテムにカーソルを合わせると、詳細情報が表示されます。ポートまたはリンクに色が付いている場合は、トラブルシューティングを行うべき問題があることを示しています。たとえば、色が赤またはオレンジであれば、ポートまたはリンクにエラーがあることを示しています。色が白である場合には、エラーは発生していません。リンクに円で囲まれた番号が付いている場合、その数は、同じ 2 ノード間で、円の色で示されている重大度のエラーにより影響を受けるパラレル リンクの数を示しています。ポートにカーソルを合わせると、どのポートが送信元 Ep に接続されているかを確認できます。

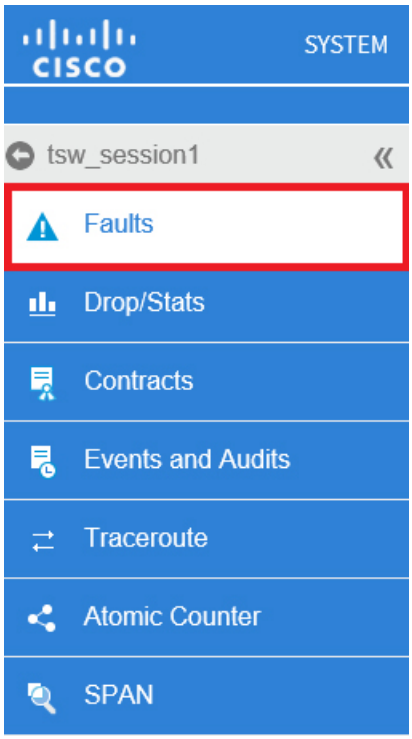
リーフを右クリックすると、スイッチのコンソールにアクセスできます。そのデバイスにログインできるポップアップ ウィンドウが表示されます。

（注）

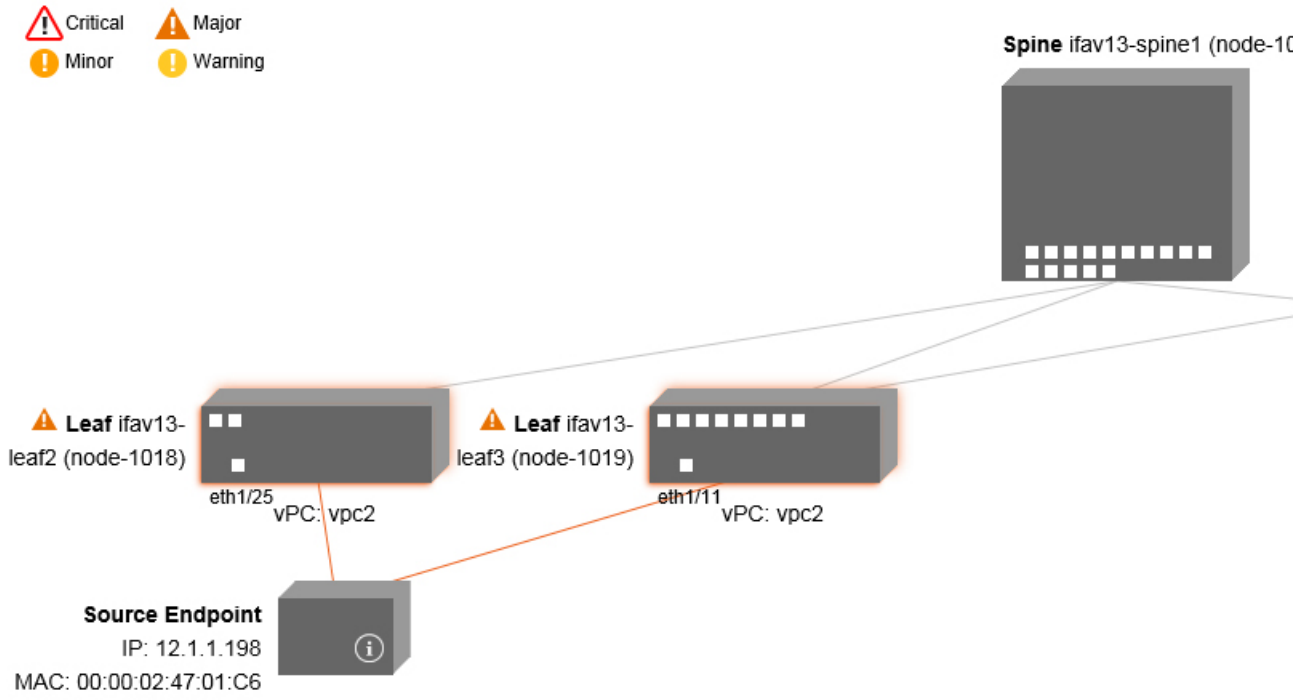
- L4 から L7 のサービスがあれば（ファイアウォールとロード バランサ）、それらもトポロジに表示されます。
- ロード バランサがあるトポロジでは、宛先は VIP（仮想 IP）であると予期されます。
- エンドポイントが ESX サーバの背後にあると、ESX はトポロジに示されます。

[Faults] トラブルシューティング画面の使用

[Faults] トラブルシューティング画面の使用を開始するには、次のように左側ナビゲーション ウィンドウの [Faults] をクリックします。

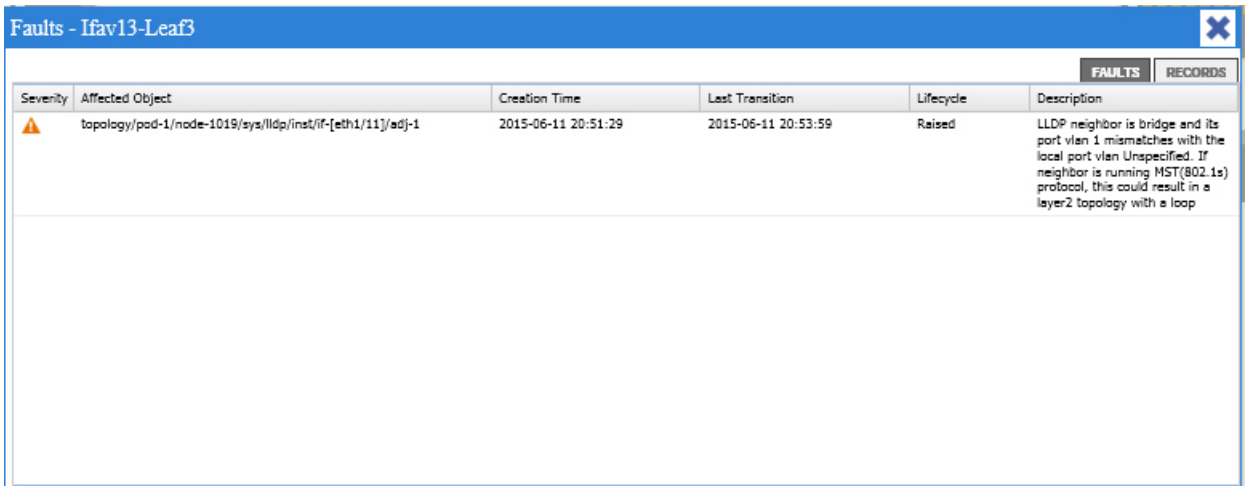


[Faults] 画面には、前に選択した 2 つのエンドポイントを接続するトポロジと、検出されたエラーが表示されます。指定された通信のエラーのみが表示されます。どの場所でもエラーがあれば、重大度を伝えるために特定の色で強調表示されます。各色に関連付けられている重大度レベルを理解するには、画面の上部にある色の凡例（以下に示す）を参照してください。このトポロジは、トラブルシューティングセッションに関連するリーフ、スパイン、およびFEXを示します。リーフ、スパイン、およびFEXなどの項目の上にカーソルを合わせる（またはエラーをクリックしてオンにする）と、分析の詳細情報が表示されます。



（注） ホワイトのボックスは、その特定の分野でトラブルシューティングを行うべき問題がないことを示します。

エラーをクリックすると、2 つのタブ（[FAULTS] と [RECORDS]）があるボックスが表示されます。そのタブには、[Severity]、[Affected Object]、[Creation Time]、[Last Transaction]、[Lifecycle]、および [Description] を含む、分析のための詳細情報が示されています。

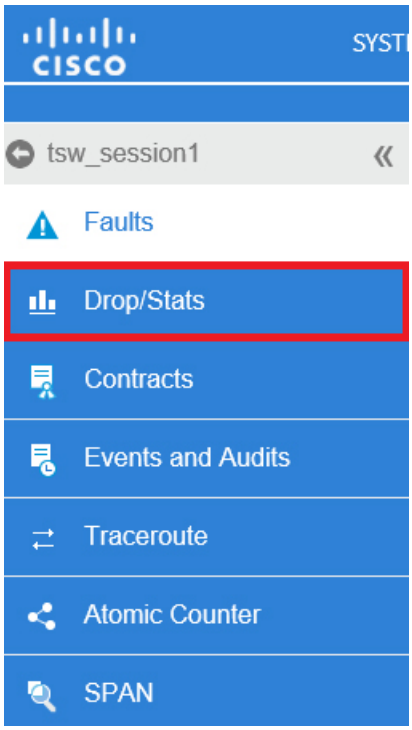


関連トピック

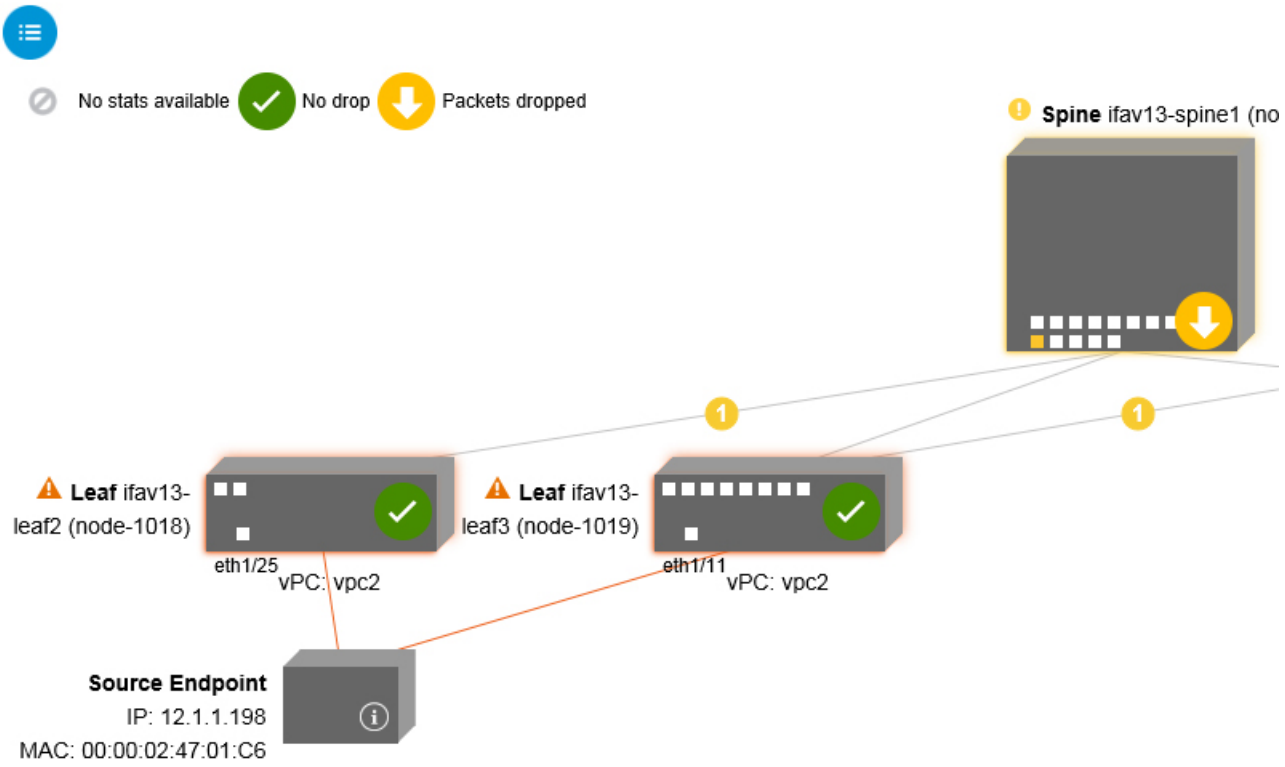
[Drop/Statistics] トラブルシューティング画面の使用, （103 ページ）

[Drop/Statistics] トラブルシューティング画面の使用

[Drop/Stats] トラブルシューティング画面の使用を開始するには、次のように左側ナビゲーションウィンドウの [Drop/Stats] をクリックします。



[Drop/Stats] 画面には、トポロジと、ドロップからのすべての統計情報が表示され、ドロップの存在箇所（存在しない箇所）を明確に把握できます。ドロップ イメージをクリックすると、分析の詳細を表示できます。



ドロップ イメージをクリックすると、[Drop/Stats] 画面の上部に 3 つのタブが表示され、表示される統計情報は特定のリーフまたはスイッチに合わせてローカライズされます。

次の 3 つの統計情報タブがあります。

- **ドロップ統計情報（DROP STATS）**

  このタブには、ドロップ カウンタの統計情報が表示されます。ここにはさまざまなレベルでドロップされたパケットが表示されます。

  （注） デフォルトではゼロ値のカウンタは非表示ですが、すべての値を表示するように選択することもできます。

- **契約のドロップ（CONTRACT DROPS）**

  このタブには、発生した契約のドロップのリストが表示されます。これは個々のパケット ログ（ACL ログ）であり、**送信元インターフェイス、送信元 IP アドレス、送信元ポート、宛先 IP アドレス、宛先ポート**、および**プロトコル**などの各パケットについての情報が表示されます。

  （注） すべてのパケットがここに表示されるわけではありません。

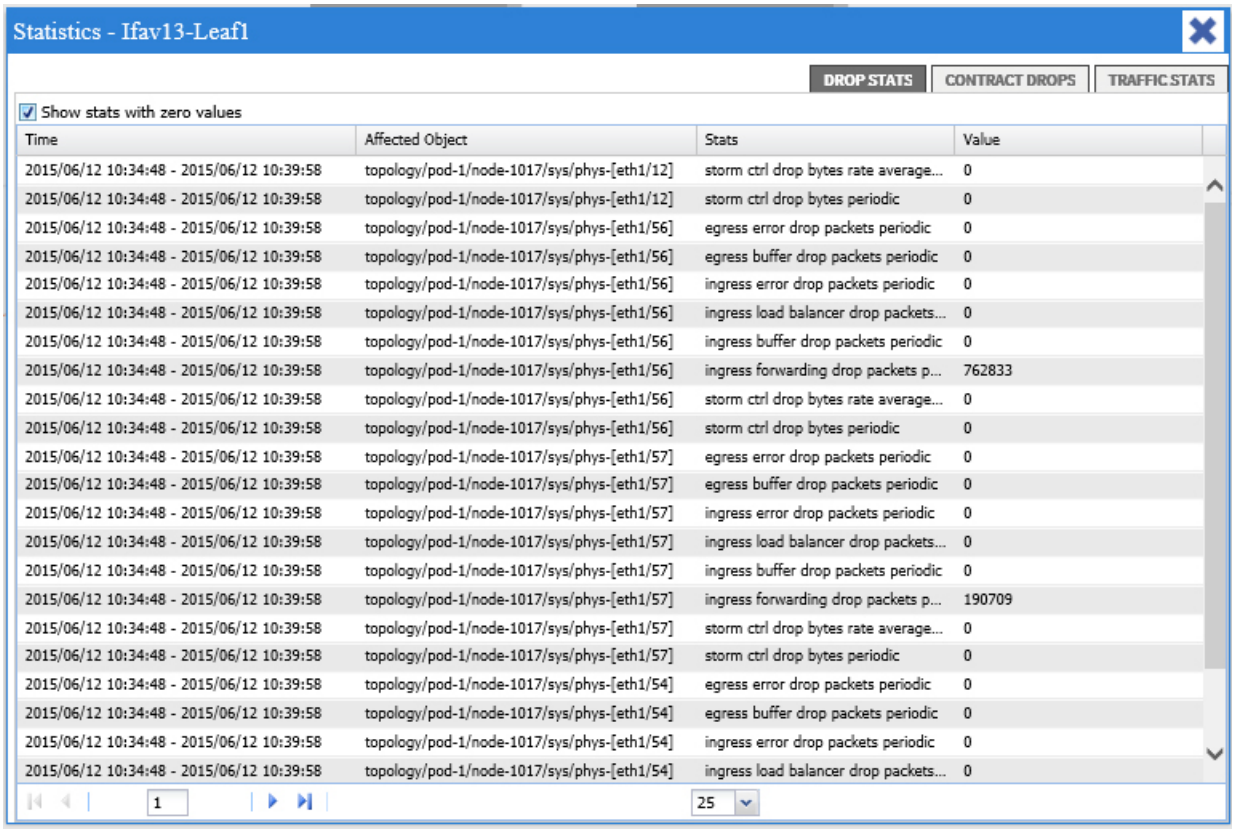
- **トラフィック統計情報（TRAFFIC STATS）**

このタブは、進行中のトラフィックを示す統計情報を表示します。これは転送済みのパケット数です。

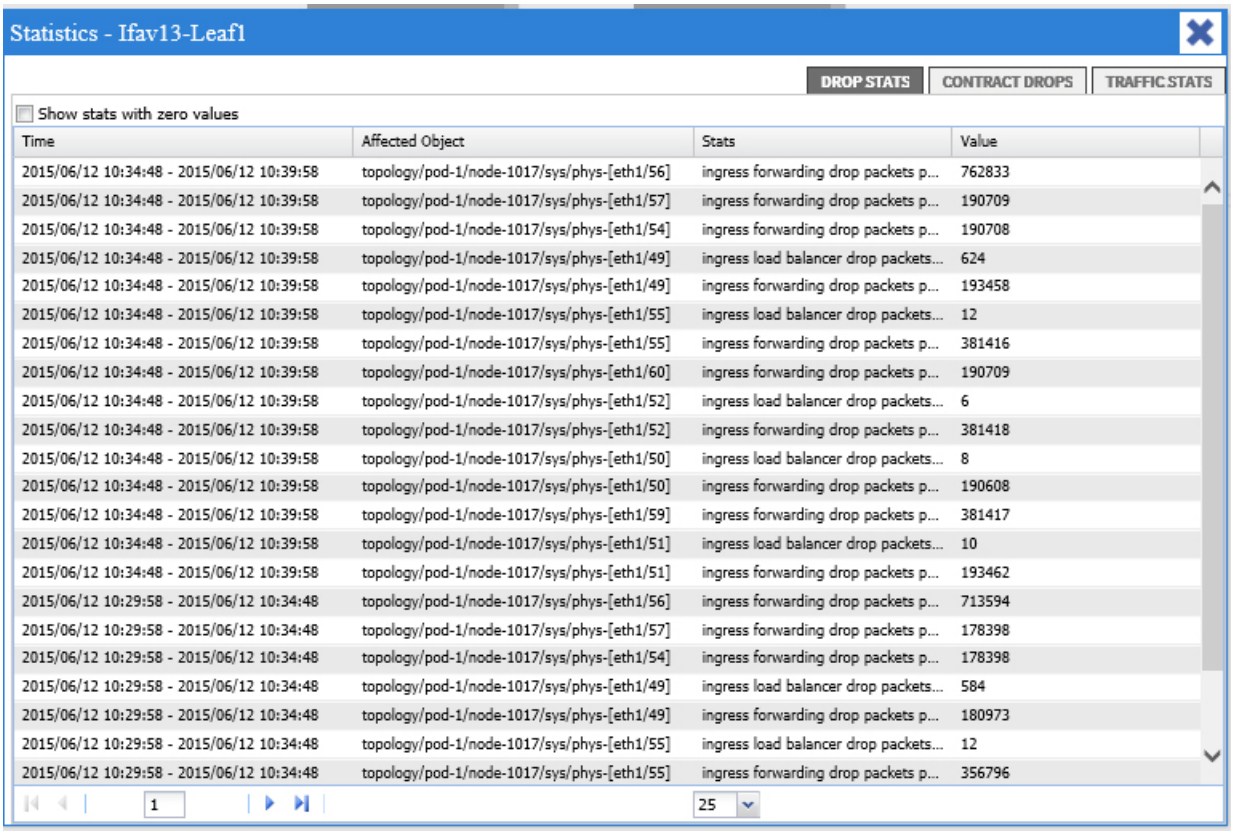
（注） デフォルトではゼロ値のカウンタは非表示ですが、すべての値を表示するように選択することもできます。

また、画面の左上隅にある [All] アイコン（ ）をクリックして、すべてのマネージドオブジェクトの全統計情報をすばやく表示できます。

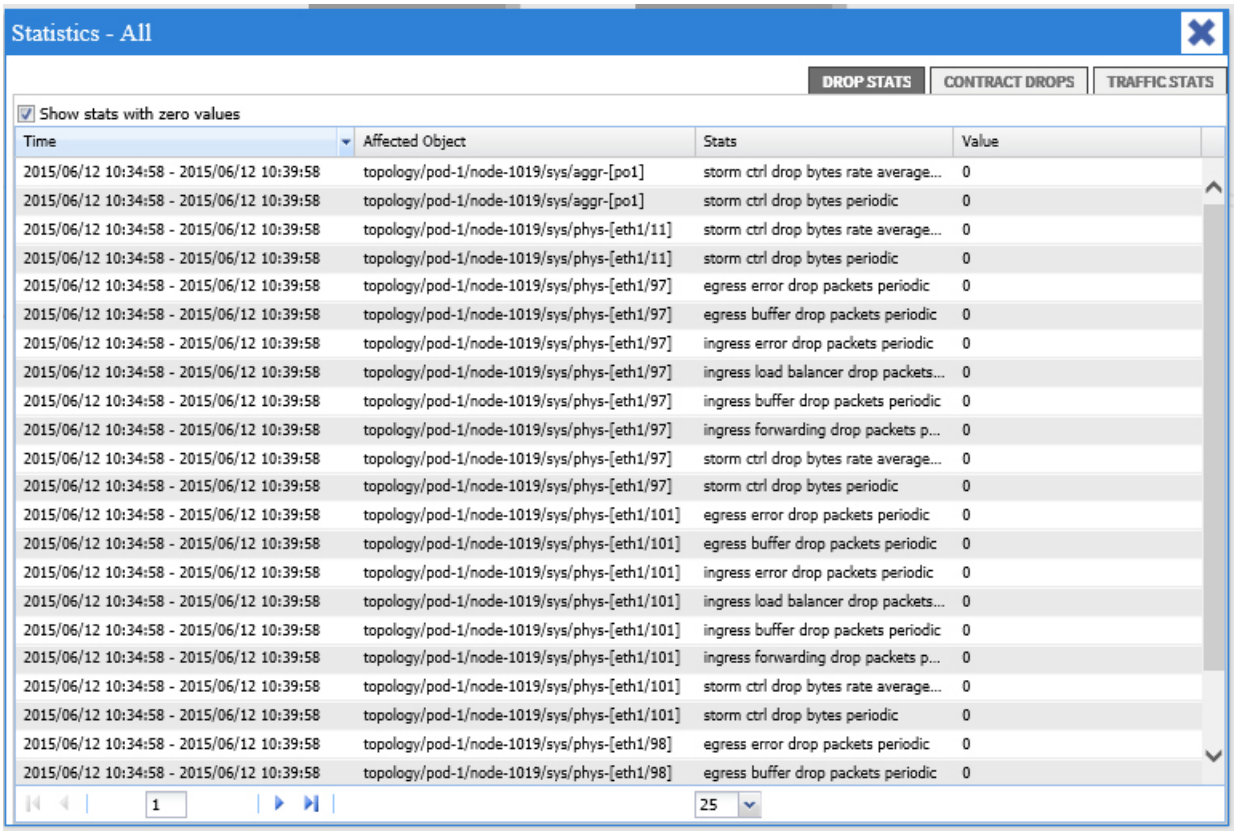
また、ゼロまたはゼロ以外のドロップを選択することもできます。[Show stats with zero values] ボックス（画面の左上隅にある）をオンにすると、既存のすべてのドロップを表示できます。[Time]、[Affected Object]、[Stats]、および [Value] の各フィールドには、次のようにゼロ以外のすべての値のデータが取り込まれます。



[Show stats with zero values] ボックスをオフにすると、次のようにゼロ以外のドロップがある結果が表示されます。



（注） [All] アイコンをクリックすると、同じ論理が適用されます。3 つのタブすべて（[DROP STATS]、[CONTRACT DROPS]、および [TRAFFIC STATS] も使用可能であり、同じタイプの情報が表示されます。以下に示すのは、[Show stats with zero values] がオンになっている [Statistics - All] 画面です。

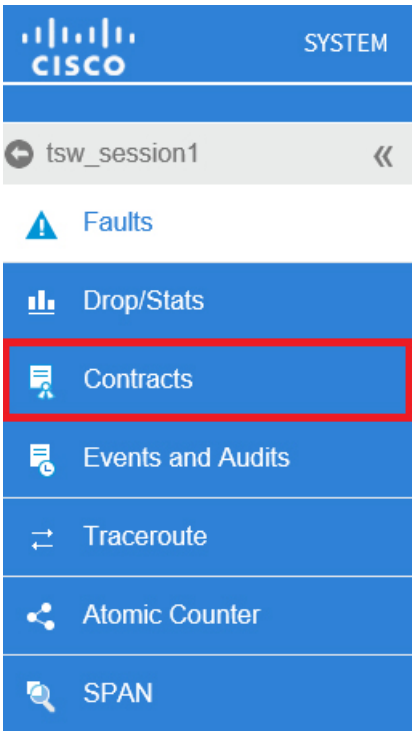


関連トピック

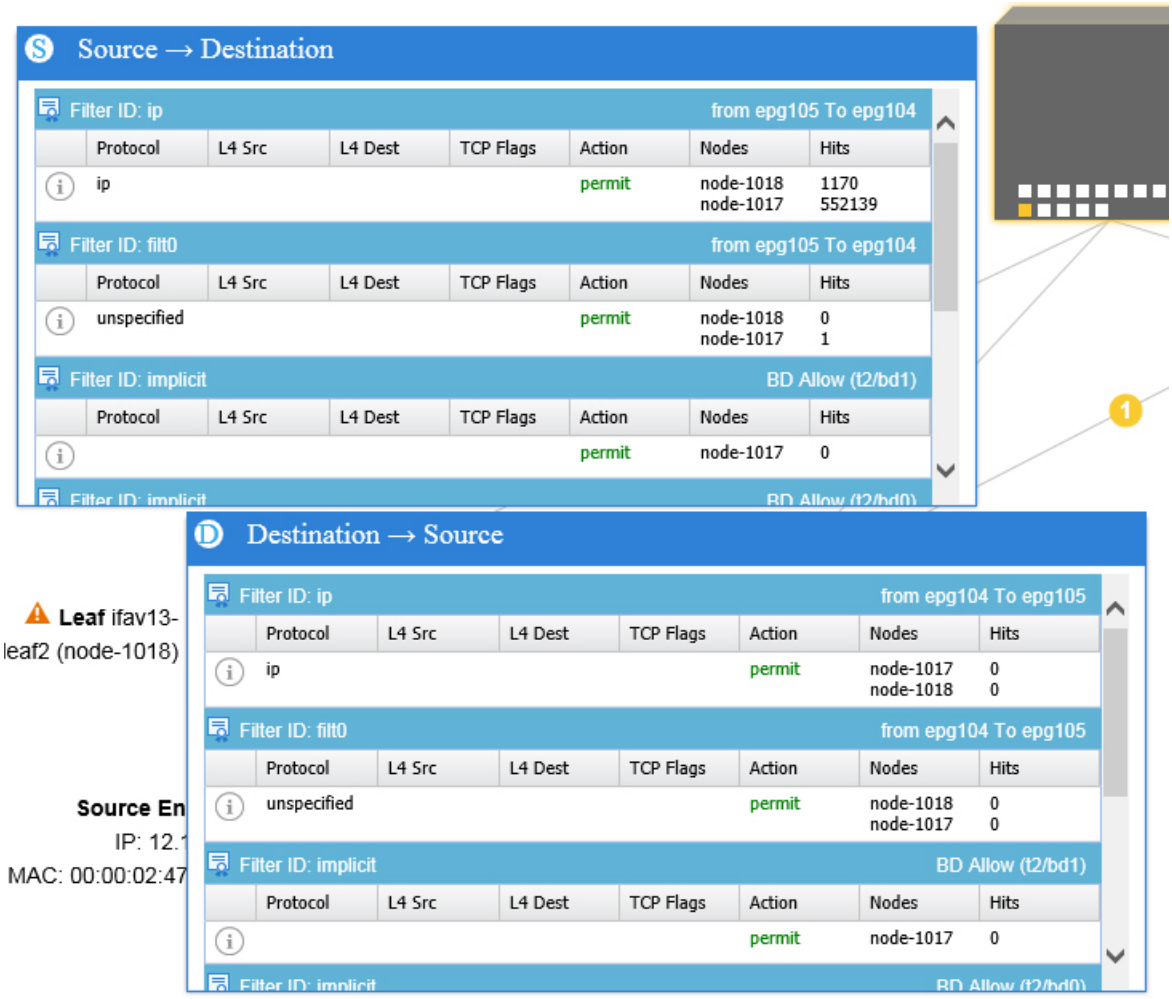
[Contracts] トラブルシューティング画面の使用, （107 ページ）

[Contracts] トラブルシューティング画面の使用

[Contracts] トラブルシューティング画面の使用を開始するには、次のように左側ナビゲーションウィンドウの [Contracts] をクリックします。

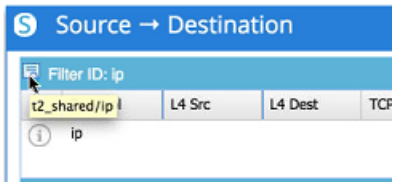


[Contracts] トラブルシューティング画面には、次のように送信元から宛先と宛先から送信元の双方に適用される契約が表示されます。



上に示す青の表見出し行はそれぞれ、フィルタを示します。特定のリーフまたはスイッチ用の複数のフィルタ エントリ（[Protocol]、[L4 Src]、[L4 Dest]、[TCP Flags]、[Action]、[Node]、および [Hits]）を示す複数の行が、各フィルタの下にあります。

証明書アイコンの上にカーソルを合わせると、次のように契約名と契約フィルタ名が表示されます。



青の各表見出し行（つまりフィルタ）の右側に表示されるテキストは、たとえば以下のような、契約のタイプを示します。

- EPG 間

- BD 許可
- Any-to-Any
- コンテキスト拒否

これらの契約は、送信元から宛先と、宛先から送信元に分類されます。

（注） 各フィルタで示されるヒット数は累積されます（つまり、その契約ヒット、契約フィルタ、またはルールの合計ヒット数は、各リーフに示されます）。統計情報は、1 分ごとに自動的に更新されます。

情報（  ）アイコンにカーソルを合わせると、ポリシー情報を入手できます。また、どの EPG が参照されているのかを確認することもできます。

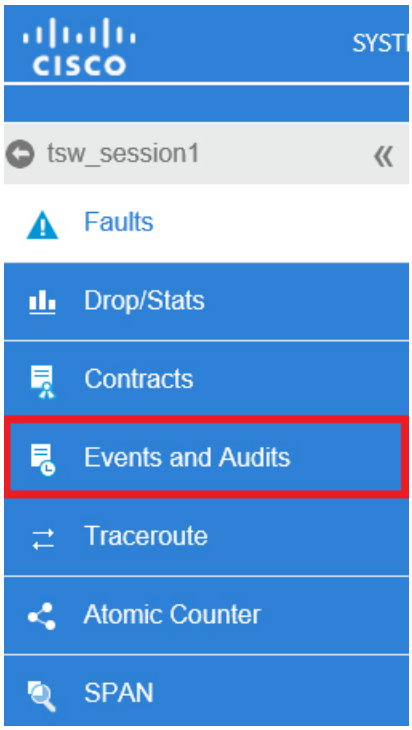
（注） エンドポイント間に契約がない場合には、[There is no contract data] ポップアップで示されます。

関連トピック

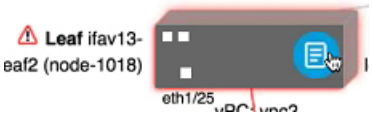
[Events] トラブルシューティング画面の使用, （110 ページ）

[Events] トラブルシューティング画面の使用

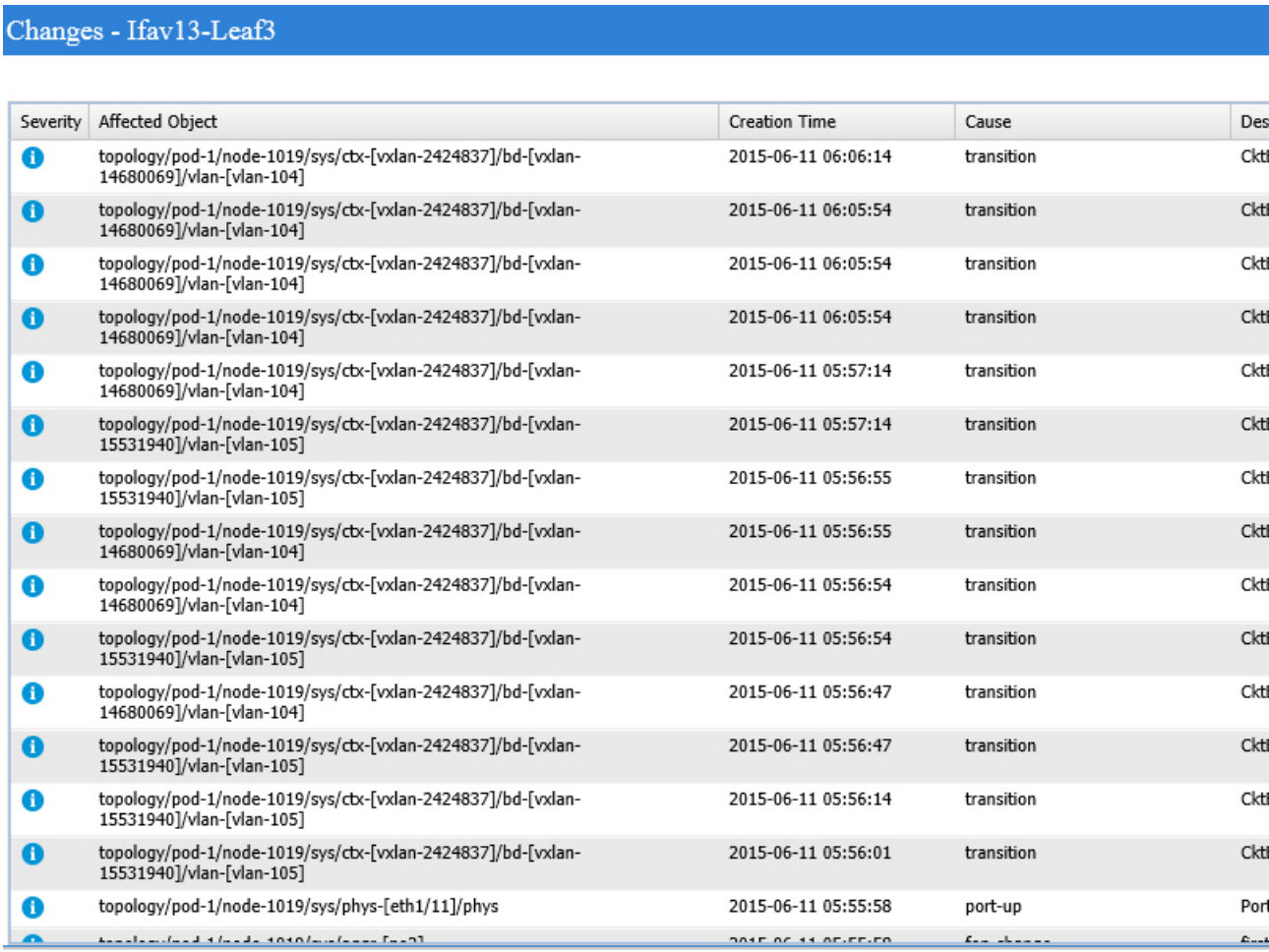
[Events and Audits] トラブルシューティング画面の使用を開始するには、次のように左側ナビゲーション ウィンドウの [Events and Audits] をクリックします。



次のように、個々のリーフまたはスパインをクリックすると、個々のイベントの詳細情報を表示できます。



この個別イベント情報の例を次に示します。

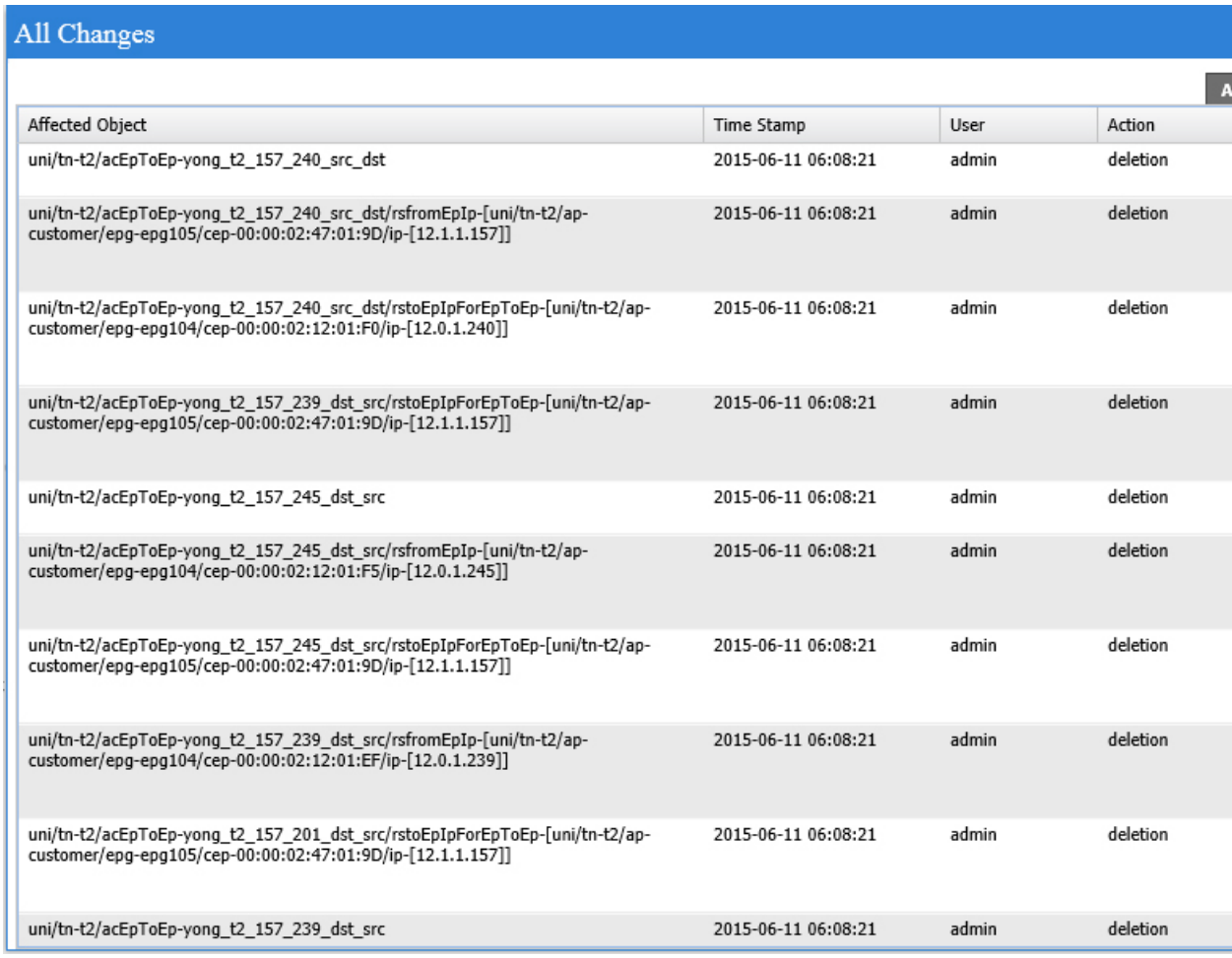

Changes - Ifav13-Leaf3

Severity	Affected Object	Creation Time	Cause	Des
	topology/pod-1/node-1019/sys/ctx-[vxlan-2424837]/bd-[vxlan-14680069]/vlan-[vlan-104]	2015-06-11 06:06:14	transition	Ckt
	topology/pod-1/node-1019/sys/ctx-[vxlan-2424837]/bd-[vxlan-14680069]/vlan-[vlan-104]	2015-06-11 06:05:54	transition	Ckt
	topology/pod-1/node-1019/sys/ctx-[vxlan-2424837]/bd-[vxlan-14680069]/vlan-[vlan-104]	2015-06-11 06:05:54	transition	Ckt
	topology/pod-1/node-1019/sys/ctx-[vxlan-2424837]/bd-[vxlan-14680069]/vlan-[vlan-104]	2015-06-11 06:05:54	transition	Ckt
	topology/pod-1/node-1019/sys/ctx-[vxlan-2424837]/bd-[vxlan-14680069]/vlan-[vlan-104]	2015-06-11 05:57:14	transition	Ckt
	topology/pod-1/node-1019/sys/ctx-[vxlan-2424837]/bd-[vxlan-15531940]/vlan-[vlan-105]	2015-06-11 05:57:14	transition	Ckt
	topology/pod-1/node-1019/sys/ctx-[vxlan-2424837]/bd-[vxlan-15531940]/vlan-[vlan-105]	2015-06-11 05:56:55	transition	Ckt
	topology/pod-1/node-1019/sys/ctx-[vxlan-2424837]/bd-[vxlan-14680069]/vlan-[vlan-104]	2015-06-11 05:56:55	transition	Ckt
	topology/pod-1/node-1019/sys/ctx-[vxlan-2424837]/bd-[vxlan-14680069]/vlan-[vlan-104]	2015-06-11 05:56:54	transition	Ckt
	topology/pod-1/node-1019/sys/ctx-[vxlan-2424837]/bd-[vxlan-15531940]/vlan-[vlan-105]	2015-06-11 05:56:54	transition	Ckt
	topology/pod-1/node-1019/sys/ctx-[vxlan-2424837]/bd-[vxlan-14680069]/vlan-[vlan-104]	2015-06-11 05:56:47	transition	Ckt
	topology/pod-1/node-1019/sys/ctx-[vxlan-2424837]/bd-[vxlan-15531940]/vlan-[vlan-105]	2015-06-11 05:56:47	transition	Ckt
	topology/pod-1/node-1019/sys/ctx-[vxlan-2424837]/bd-[vxlan-15531940]/vlan-[vlan-105]	2015-06-11 05:56:14	transition	Ckt
	topology/pod-1/node-1019/sys/ctx-[vxlan-2424837]/bd-[vxlan-15531940]/vlan-[vlan-105]	2015-06-11 05:56:01	transition	Ckt
	topology/pod-1/node-1019/sys/phys-[eth1/11]/phys	2015-06-11 05:55:58	port-up	Port

この画面で使用できる 2 つのタブは、[EVENTS] と [DEPLOYMENT RECORDS] です。

- [EVENTS] は、システム（物理インターフェイスや VLAN など）で発生したすべての変更のイベント レコードを示します。特定の各リーフについてリストされる個々のイベントがあります。これらのイベントは、[Severity]、[Affected Object]、[Creation Time]、[Cause]、および [Description] に基づいて分類できます。
- [DEPLOYMENT RECORDS] は、物理インターフェイス、VLAN、VXLAN、および L3 CTX に対するポリシーの展開を示します。これらのレコードは、epg により VLAN がリーフに配置されていた時間を示します。

[All Changes] 画面の [All] アイコン（ ）をクリックすると、指定した期間内（またはトラブルシューティング セッション時）に行われた変更を示すすべてのイベントを表示できます。



[All Changes] 画面には、次の 3 つのタブがあります。

- **AUDITS**

  監査はリーフと関連付けられていないため、[All Changes] 画面でしか使用できません。

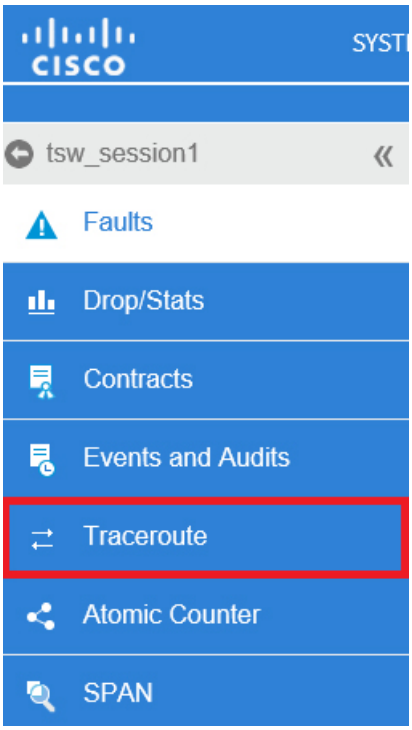
- EVENTS（前述）
- DEPLOYMENT RECORDS（前述）

関連トピック

[Traceroute] トラブルシューティング画面の使用, （113 ページ）

[Traceroute] トラブルシューティング画面の使用

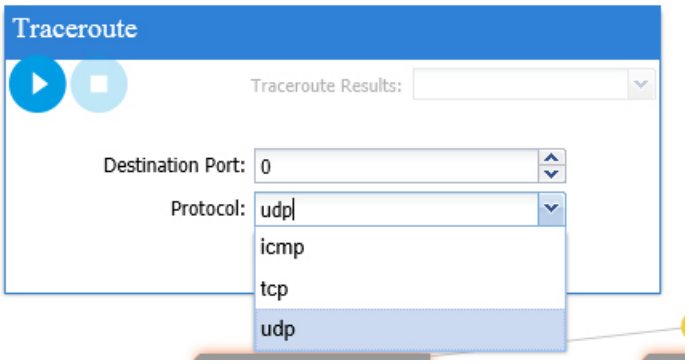
[Traceroute] トラブルシューティング画面の使用を開始するには、次のように左側ナビゲーションウィンドウの [Traceroute] をクリックします。



トラブルシューティングのために traceroute 作成して実行するには、次の手順に従います。

1 [TRACEROUTE] ボックスで、[Destination Port] プルダウン メニューから宛先ポートを選択します。

2 次のように、[Protocol] プルダウン メニューからプロトコルを選択します。



サポートされるオプションは、次のとおりです。

- **icmp**
  このプロトコルは、送信元リーフから宛先エンドポイントへの方向のみに traceroute を実行するという点で、単方向です。
- **tcp**

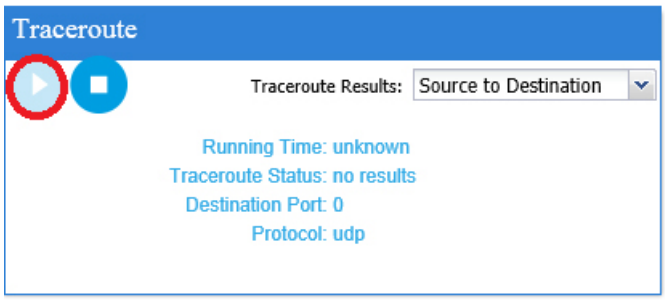
このプロトコルは、**udp** プロトコルについての前述の説明に従えば、双方向でもあります。

- **udp**
  このプロトコルは、traceroute を送信元リーフから宛先エンドポイントに実行し、次に宛先リーフから送信元エンドポイントに実行するという点で、双方向です。

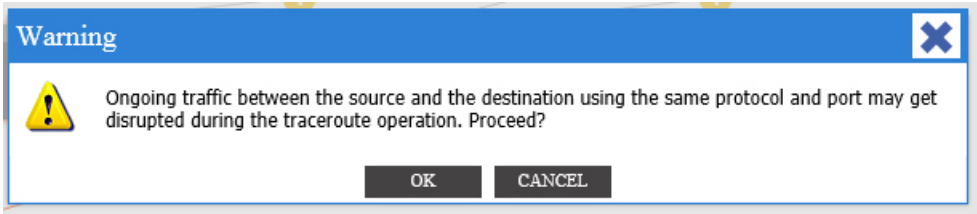
（注） IPv4 でサポートされているプロトコルは、UDP、TCP、および ICMP のみです。IPv6 では、サポートされるのは UDP のみです。

3 traceroute を作成したら、次のように [Play]（または [Start]）ボタンをクリックして traceroute を開始します。

（注） [Play] ボタンを押すと、システムにポリシーが作成されます。



（注） **警告**メッセージは、次のように表示されます。

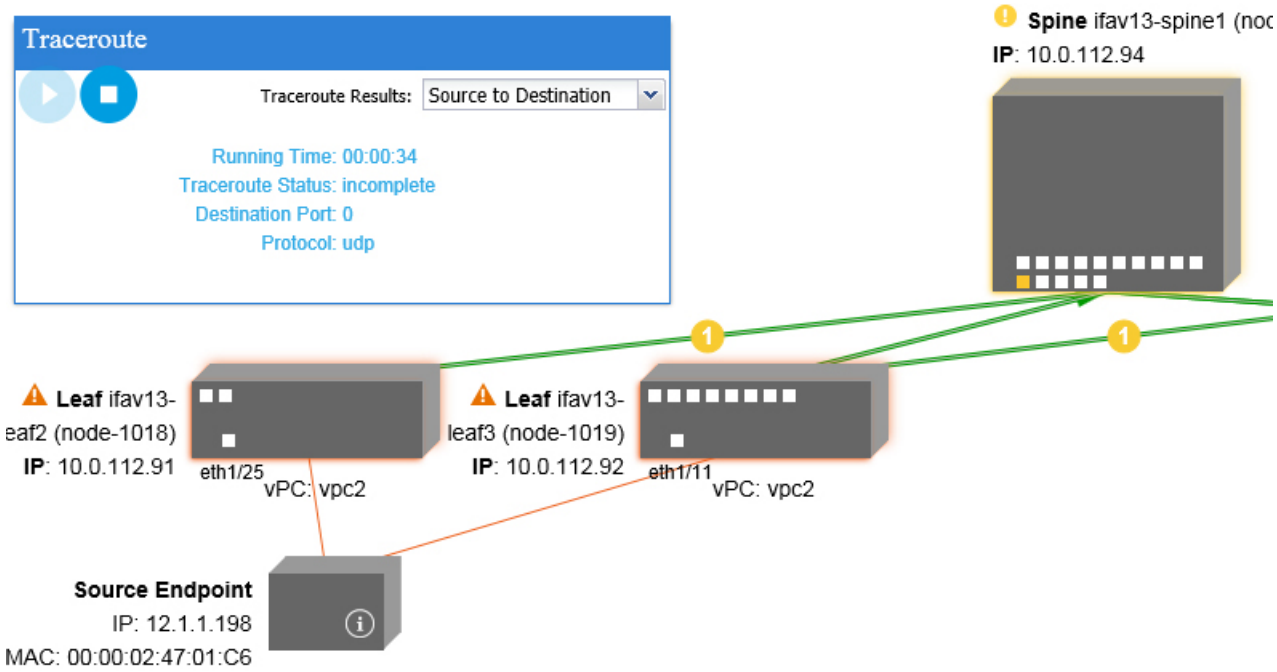


4 [OK] をクリックして続行すると、traceroute が実行を開始します。

5 traceroute を終了するには、[Stop] ボタンをクリックします。

（注） [Stop] ボタンを押すと、ポリシーはシステムから削除されます。

traceroute が完了すると、起動した場所と結果を確認できます。[Traceroute Results] の横にプルダウンメニューがあり、traceroute が起動された場所（送信元から宛先または宛先から送信元）が以下のように表示されます。



さらに、結果は [Traceroute] ボックス（上記参照）に表示されます。これには**実行時間、traceroute のステータス、宛先ポート、**および**プロトコル**についての情報が含まれます。

結果は、緑または赤（あるいはその両方）の矢印で示されます。緑色の矢印は、traceroute プローブに応答した、パス内の各ノードを表すために使用しています。赤い矢印の起点は、traceroute プローブに応答した最終ノードであり、パスの終端を表します。traceroute を起動する方向は選択しません。そのようにしなくても、traceroute はセッションに対して常に起動します。セッションに応じて、以下のようになります。

- EP から外部 IP または外部 IP から EP の場合、traceroute は常に EP から外部 IP の方向に起動します。
- EP 間であり、プロトコルが ICMP の場合、traceroute は常に送信元から宛先の方向に起動します。
- EP 間であり、プロトコルが UDP/TCP の場合、traceroute は常に双方向です。

（注） [Traceroute Results] ドロップダウンメニューは、上記のシナリオ #3 の各方向の結果を明らかにする/可視化するために使用できます。シナリオ #1 と #2 では、これは常にグレー表示です。

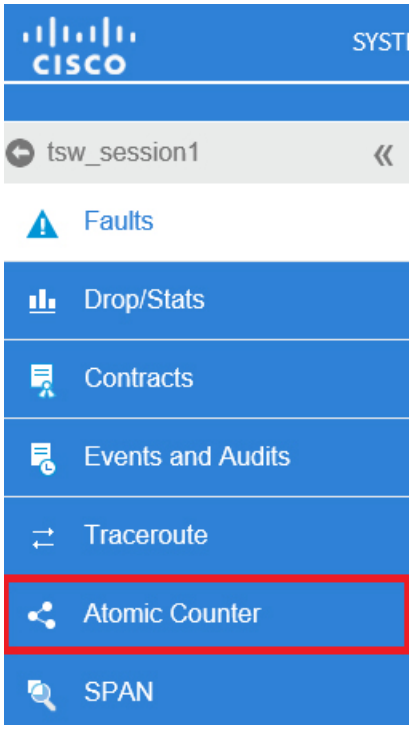
（注） [Traceroute Status] が未完了を示している場合は、データの一部が返されるのを引き続き待機することになります。[Traceroute Status] が [complete] を示している場合は、実際に完了しています。

関連トピック

[Atomic Counter] トラブルシューティング画面の使用, （117 ページ）

[Atomic Counter] トラブルシューティング画面の使用

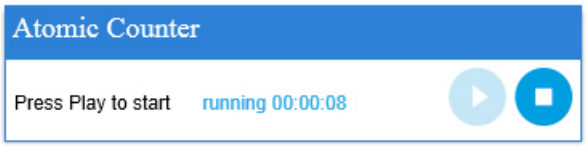
[Atomic Counter] トラブルシューティング画面の使用を開始するには、次のように左側ナビゲーション ウィンドウの [Atomic Counter] をクリックします。



[Atomic Counter] 画面は、発信元と宛先の情報を取得し、それに基づくカウンタ ポリシーを作成するために使用されます。2 つのエンドポイント間のアトミック カウンタ ポリシーを作成し、送信元から宛先および宛先から送信元を行き来するトラフィックをモニタできます。どの程度のトラフィックが行き来したかを判別できます。さらに、送信元と宛先のリーフ間で異常（ドロップまたは超過パケット）が報告されているかどうかを特に判別します。

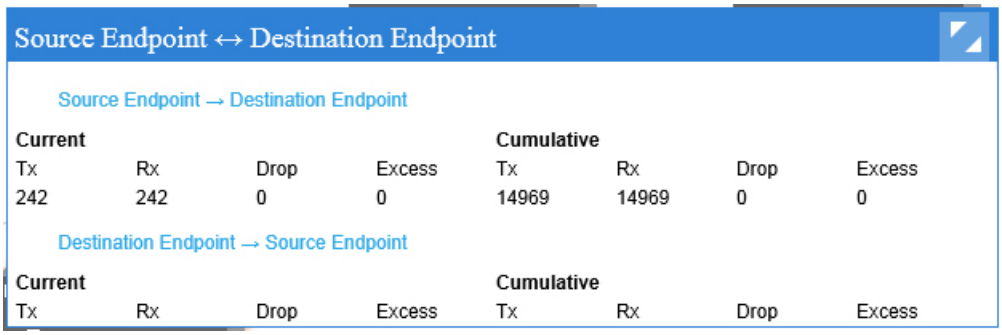
以下に示すとおり、画面上部には [Play]（または [Start]）および [Stop] ボタンがあり、任意の時点でアトミック カウンタ ポリシーを開始または停止したり、送信済みのパケット数をカウントしたりできます。

（注） [Play] ボタンを押すと、システム上にポリシーが作成され、パケット カウンタが開始されます。[Stop] ボタンを押すと、ポリシーはシステムから削除されます。

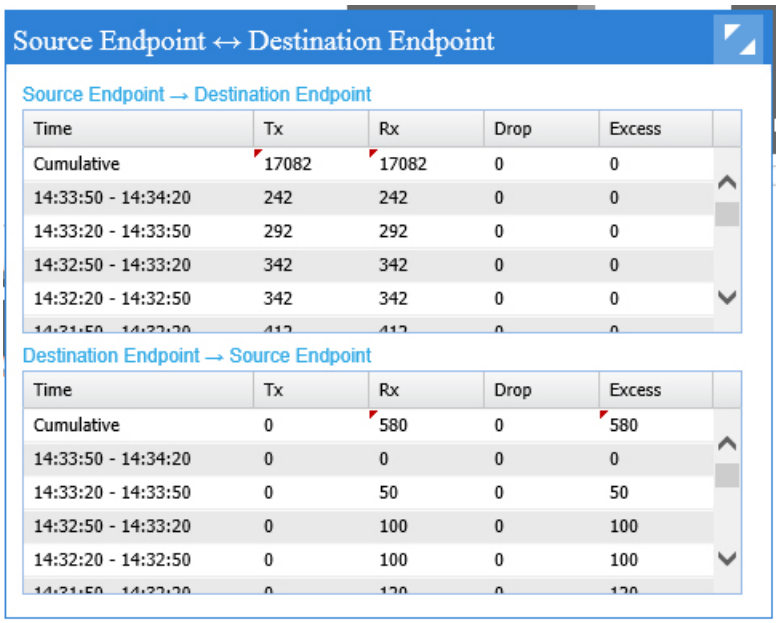


結果は 2 つの異なる形式で表示されます。ポリシーは、いずれかの簡略形式（概要を含む）、または（[Expand] ボタンをクリックして）拡張形式で表示できます。簡易および拡張のどちらの形式も、両方向を表示します。拡張形式は、累積カウントと直近30秒間隔ごとのカウントを表示するのに対し、簡易形式は、累積カウントと直近の 1 間隔のカウントのみを表示します。

簡易形式は、次のように表示されます。



拡張形式は、次のように表示されます。

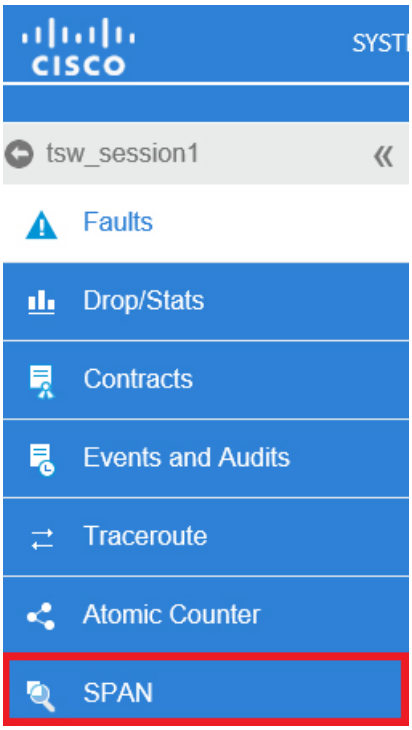


関連トピック

[SPAN] トラブルシューティング画面の使用, （119 ページ）

[SPAN] トラブルシューティング画面の使用

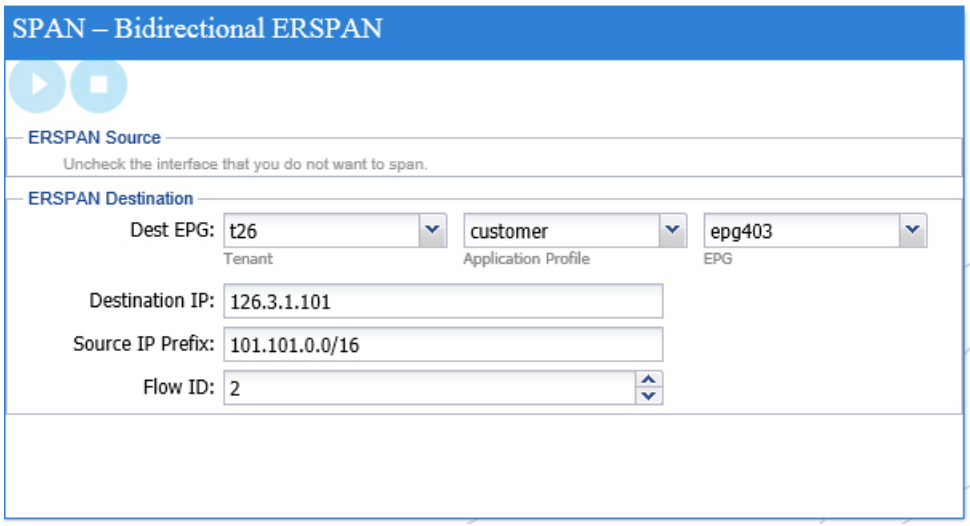
[SPAN] トラブルシューティング画面の使用を開始するには、次のように左側ナビゲーション ウィンドウの [SPAN] をクリックします。



この画面を使用して、双方向トラフィックに SPAN（またはミラー）を実行したり、アナライザにリダイレクトしたりできます。SPAN セッションでは、コピーを作成して、アナライザに送信します。

このコピーは、特定のホスト（アナライザの IP アドレス）に送られます。それから Wireshark などのソフトウェア ツールを使用すると、パケットを表示できます。セッション情報には、発信元と宛先の情報、セッション タイプ、およびタイムスタンプの範囲があります。

[SPAN - Bidirectional ERSPAN] ボックスが、以下のように表示されます。



（注） [Play] ボタンを押すと、システムにポリシーが作成されます。[Stop] ボタンを押すと、ポリシーはシステムから削除されます。

（注） トラブルシューティング ウィザード CLI コマンドのリストについては、『*Cisco APIC Command-Line Interface User Guide*（*Cisco APIC* コマンド行インターフェイス ユーザ ガイド）』を参照してください。

L4 - L7 サービス検証シナリオ

トラブルシューティング ウィザードは、2 つのエンドポイントを提供し、それらのエンドポイント間の対応するトポロジを表示することができます。L4 ～ L7 のサービスがトポロジ内の 2 つのエンドポイント間に存在している場合、それらも表示できます。

この項では、このリリースで検証された L4 ～ L7 のシナリオについて説明します。L4 ～ L7 のサービス内では、トポロジの数が非常に大きくなっています。これはつまり、それぞれのファイアウォール、ロード バランサ、および組み合わせが、さまざまな設定を持つ可能性があることを意味します。ファイアウォールがトポロジ内の 2 つのエンドポイント間に存在している場合、トラブルシューティング ウィザードは、ファイアウォールのデータと、ファイアウォールからリーフへの接続を取得します。ロード バランサが 2 つのエンドポイント間に存在している場合、サーバまでではなく、ロード バランサまでの情報を取得して表示できます。

次の表は、トラブルシューティング ウィザードで検証済みの、L4 ～ L7 のサービス シナリオを示しています。

シナリオ	1	2	3	4	5	6
ノード数	1	1	2	1	1	2
デバイス	Goto FW（vrf 分割）	GoTo SLB	GoTo、GoTo FW、SLB	FW-GoThrough	SLB-GoTo	FW、SLB（GoThrough、GoTo）
アーム数	2	2	2	2	2	2
コンシューマ	EPG	EPG	EPG	L3Out	L3Out	L3Out
Provider	EPG	EPG	EPG	EPG	EPG	EPG
デバイスの種類	VM	VM	VM	physical	physical	physical
コントラクト範囲	テナント	コンテキスト	コンテキスト	コンテキスト	コンテキスト	global

シナリオ	1	2	3	4	5	6
Connector Mode	L2	L2	L2、L2	L2、L3	L3	L3 / L2、L3
サービスの付加	BSW	BSW	DL/PC	通常のポート	vPC	通常のポート
クライアントの付加	FEX	FEX	FEX	通常のポート	通常のポート	通常のポート
サーバの付加	vPC	vPC	vPC	通常のポート	通常のポート	通常のポート

エンドポイント間接続用 API のリスト

次に示すのは、EP 間（エンドポイント間）接続に使用できるトラブルシューティング ウィザード API のリストです。

interactive API

エンドポイント（ep）間のインタラクティブ トラブルシューティング セッションを作成するには、**interactive** API を使用します。モジュール名は **troubleshoot.eptoeputils.topo** で、関数は **getTopo** です。interactive API の必須引数（**req_args**）は **- session** です。

次の表に、オプションの引数（**opt_args**）とそれぞれの説明を示します。

構文の説明

オプションの引数（opt_args）	説明
- srcep	送信元エンドポイント名
- dstep	宛先エンドポイント名
- srcip	送信元エンドポイント IP アドレス
- dstip	宛先エンドポイント IP アドレス
- srcmac	送信元エンドポイント MAC
- dstmac	宛先エンドポイント MAC
- srcextip	L3 外部送信元 IP アドレス
- dstextip	L3 外部宛先 IP アドレス
- starttime	トラブルシューティング セッションの開始時刻
- endtime	トラブルシューティング セッションの終了時刻
- latestmin	開始時刻から始まるトラブルシューティング セッションの期間（分単位）
- description	セッションについての説明
- scheduler	レポート生成用のスケジューラ名
- srcepid	Obsolete
- dstepid	Obsolete
- include	Obsolete
- format	生成されるレポートの形式
- ui	内部的に使用（無視）

- sessionurl	レポートの場所
-action	traceroute/atomiccounter の start/stop/status など
- mode	内部的に使用
- _dc	内部的に使用
- ctx	内部的に使用

createsession API

エンドポイント間トラブルシューティング セッションを作成するには、**createsession** API を使用します。モジュール名は **troubleshoot.eptoeputils.session** で、関数は **createSession** です。

createsession API の必須引数（**req_args**）は **- session** (session name) です。

次の表に、オプションの引数（**opt_args**）とそれぞれの説明を示します。

構文の説明

オプションの引数（opt_args）	説明
- srcep	送信元エンドポイント名
- dstep	宛先エンドポイント名
- srcip	送信元エンドポイント IP アドレス
- dstip	宛先エンドポイント IP アドレス
- srcmac	送信元エンドポイント MAC
- dstmac	宛先エンドポイント MAC
- srcextip	L3 外部送信元 IP アドレス
- dstextip	L3 外部宛先 IP アドレス
- starttime	トラブルシューティング セッションの開始時刻
- endtime	トラブルシューティング セッションの終了時刻
- latestmin	開始時刻から始まるトラブルシューティング セッションの期間（分単位）
- description	セッションについての説明

- format	生成されるレポートの形式
- ui	内部的に使用（無視）
-action	traceroute/atomiccounter の start/stop/status など
- scheduler	
- srctenant	ソース エンドポイントのテナントの名前
- srcapp	ソース エンドポイントのアプリケーションの名前
- srcepg	ソース エンドポイントのエンドポイント グループの名前
- dsttenant	宛先エンドポイントのテナントの名前
- dstapp	宛先エンドポイントのアプリケーションの名前
- dstepg	宛先エンドポイントのエンドポイント グループの名前
- mode	内部的に使用

modifysession API

エンドポイント（ep）間のトラブルシューティング セッションを変更するには、**modifysession** API を使用します。モジュール名は **troubleshoot.eptoeputils.topo** で、関数は **modifySession** です。

modifysession API の必須引数（**req_args**）は **- session** (session name) および **- mode** です。

次の表に、オプションの引数（**opt_args**）とそれぞれの説明を示します。

構文の説明

オプションの引数（opt_args）	説明
- starttime	トラブルシューティング セッションの開始時刻
- endtime	トラブルシューティング セッションの終了時刻
- latestmin	開始時刻から始まるトラブルシューティング セッションの期間（分単位）
- description	セッションについての説明

atomiccounter API

エンドポイント（ep）間のアトミック カウンタ セッションを作成するには、**atomiccounter** API を使用します。モジュール名は **troubleshoot.eptoeputils.atomiccounter** で、関数は **manageAtomicCounterPols** です。

atomiccounter API の必須引数（**req_args**）には、次のものが含まれます。

- - session
- - action
- - mode

（注） atomiccounter API のオプションの引数（**opt_args**）はありません。

traceroute API

API を使用してエンドポイント（ep）間トレースルート セッションを作成するには、**traceroute** API を使用します。モジュール名は **troubleshoot.eptoeputils.traceroute** で、関数は **manageTracerouteP ols** です。

traceroute API の必須引数（**req_args**）には、次のものが含まれます。

- - session (session name)
- - action (start/stop/status)
- - mode

構文の説明

オプションの引数（opt_args）	説明
- protocol	プロトコル名
- dstport	宛先ポート名

span API

エンドポイント（ep）間のスパン トラブルシューティング セッションを作成するには、**span** API を使用します。モジュール名は **troubleshoot.eptoeputils.span** で、関数は **monitor** です。

span API の必須引数（**req_args**）には、次のものが含まれます。

- - session (session name)

• - action (start/stop/status)

次の表に、オプションの引数（**opt_args**）とそれぞれの説明を示します。

構文の説明

オプションの引数（opt_args）	説明
- srcep	送信元エンドポイント名
- dstep	宛先エンドポイント名
- srcip	送信元エンドポイント IP アドレス
- dstip	宛先エンドポイント IP アドレス
- srcmac	送信元エンドポイント MAC
- dstmac	宛先エンドポイント MAC
- srcextip	L3 外部送信元 IP アドレス
- dstextip	L3 外部宛先 IP アドレス
- starttime	トラブルシューティング セッションの開始時刻
- endtime	トラブルシューティング セッションの終了時刻
- latestmin	開始時刻から始まるトラブルシューティングセッションの期間（分単位）
- description	セッションについての説明
- scheduler	レポート生成用のスケジューラ名
- srcepid	Obsolete
- dstepid	Obsolete
- include	Obsolete
- format	生成されるレポートの形式
- ui	内部的に使用（無視）
- sessionurl	レポートの場所
-action	traceroute/atomiccounter の start/stop/status など
- srctenant	ソース エンドポイントのテナントの名前

- srcapp	ソース エンドポイントのアプリケーションの名前
- srcepg	ソース エンドポイントのエンドポイント グループの名前
- dsttenant	宛先エンドポイントのテナントの名前
- dstapp	宛先エンドポイントのアプリケーションの名前
- dstepg	宛先エンドポイントのエンドポイント グループの名前
- mode	内部的に使用
- _dc	内部的に使用
- ctx	内部的に使用

generatereport API

API を使用してトラブルシューティング レポートを生成するには、**generatereport** API を使用します。モジュール名は **troubleshoot.eptoeputils.report** で、関数は **generateReport** です。

generatereport API の必須引数（**req_args**）は **- session** (session name) および **- mode** です。

次の表に、オプションの引数（**opt_args**）とそれぞれの説明を示します。

構文の説明

オプションの引数（opt_args）	説明
- include	Obsolete
- format	生成されるレポートの形式

schedulereport API

API を使用してトラブルシューティング レポートの生成をスケジュールするには、**schedulereport** API を使用します。モジュール名は **troubleshoot.eptoeputils.report** で、関数は **scheduleReport** です。schedulereport API の必須引数（**req_args**）は **- session** です。

schedulereport API の必須引数（**req_args**）には、次のものが含まれます。

- - session (session name)

- - scheduler (scheduler name)
- - mode

次の表に、オプションの引数（**opt_args**）とそれぞれの説明を示します。

構文の説明

オプションの引数（opt_args）	説明
- starttime	トラブルシューティング セッションの開始時刻
- endtime	トラブルシューティング セッションの終了時刻
- latestmin	開始時刻から始まるトラブルシューティング セッションの期間（分単位）
- include	Obsolete
- format	生成されるレポートの形式
- action	traceroute/atomiccounter の start/stop/status など

getreportstatus API

API を使用して生成済みレポートのステータスを取得するには、**getreportstatus** API を使用します。モジュール名は **troubleshoot.eptoeputils.report** で、関数は **getStatus** です。

getreportstatus API の必須引数（**req_args**）には、次のものが含まれます。

- - session (session name)
- - sessionurl (session URL)
- - mode

（注） getreportstatus API のオプションの引数（**opt_args**）はありません。

getreportslist API

API を使用して生成済みレポートのリストを取得するには、**getreportslist** API を使用します。モジュール名は **troubleshoot.eptoeputils.report** で、関数は **getReportsList** です。

getreportslist API の必須引数（**req_args**）は **- session** (session name) および **- mode** です。

（注） getreportslist API のオプションの引数（**opt_args**）はありません。

getsessionslist API

API を使用してトラブルシューティング セッションのリストを取得するには、**getsessionslist** API を使用します。モジュール名は **troubleshoot.eptoeputils.session** で、関数は **getSessions** です。

getsessionlist API の必須引数（**req_args**）は **- mode** です。

（注） getsessionlist API のオプションの引数（**opt_args**）はありません。

getsessiondetail API

API を使用してトラブルシューティング セッションについての特定の詳細を取得するには、**getsessiondetail** API を使用します。モジュール名は **troubleshoot.eptoeputils.session** で、関数は **getSessionDetail** です。

getsessiondetail API の必須引数（**req_args**）は **- session** (session name) および **- mode** です。

（注） getsessiondetail API のオプションの引数（**opt_args**）はありません。

deletesession API

API を使用して特定のトラブルシューティング セッションを削除するには、**deletesession** API を使用します。モジュール名は **troubleshoot.eptoeputils.session** で、関数は **deleteSession** です。

deletesession API の必須引数（**req_args**）は **- session** (session name) です。

次の表に、オプションの引数（**opt_args**）とそれぞれの説明を示します。

構文の説明

オプションの引数（opt_args）	説明
- srcep	送信元エンドポイント名
- dstep	宛先エンドポイント名
- srcip	送信元エンドポイント IP アドレス
- dstip	宛先エンドポイント IP アドレス

- srcmac	送信元エンドポイント MAC
- dstmac	宛先エンドポイント MAC
- srcextip	L3 外部送信元 IP アドレス
- dstextip	L3 外部宛先 IP アドレス
- starttime	トラブルシューティング セッションの開始時刻
- endtime	トラブルシューティング セッションの終了時刻
- latestmin	開始時刻から始まるトラブルシューティング セッションの期間（分単位）
- description	セッションについての説明
- scheduler	レポート生成用のスケジューラ名
- srcepid	Obsolete
- dstepid	Obsolete
- include	Obsolete
- format	生成されるレポートの形式
- ui	内部的に使用（無視）
- sessionurl	レポートの場所
- action	traceroute/atomiccounter の start/stop/status など
- mode	内部的に使用
- _dc	内部的に使用
- ctx	内部的に使用

clearreports API

API を使用して生成済みレポートのリストをクリアするには、**clearreports** API を使用します。モジュール名は **troubleshoot.eptoeputils.report** で、関数は **clearReports** です。

clearreports API の必須引数（**req_args**）は **- session** (session name) および **- mode** です。

（注） clearreports API のオプションの引数（**opt_args**）はありません。

contracts API

API を使用して契約情報を取得するには、**contracts** API を使用します。モジュール名は **troubleshoot.eptoeputils.contracts** で、関数は **getContracts** です。

contracts API の必須引数（**req_args**）は **- session** (session name) および **- mode** です。

contracts API のオプションの引数（**opt_args**）はありません。

エンドポイントからレイヤ 3 への外部接続用 API のリスト

次に示すのは、EP 間（エンドポイント間）接続に使用できるトラブルシューティング ウィザード API のリストです。

interactive API

エンドポイント（ep）とレイヤ 3（L3）との間の外部インタラクティブ トラブルシューティング セッションを作成するには、**interactive** API を使用します。モジュール名は **troubleshoot.epextutils.epext_topo** で、関数は **getTopo** です。interactive API の必須引数（**req_args**）は、**- session**、**- include**、および **- mode** です。

次の表は、オプションの引数（**opt_args**）を示しています。

構文の説明

オプションの引数（opt_args）	説明
- refresh	

createsession API

API を使用してエンドポイント（Ep）とレイヤ 3（L3）との間の外部トラブルシューティング セッションを作成するには、**createsession** API を使用します。モジュール名は **troubleshoot.epextutils.epextsession** で、関数は **createSession** です。createsession API の必須引数（**req_args**）は **- session** (session name) です。

次の表に、オプションの引数（**opt_args**）とそれぞれの説明を示します。

構文の説明

オプションの引数（opt_args）	説明
- srcep	送信元エンドポイント名
- dstep	宛先エンドポイント名
- srcip	送信元エンドポイント IP アドレス
- dstip	宛先エンドポイント IP アドレス
- srcmac	送信元エンドポイント MAC
- dstmac	宛先エンドポイント MAC
- srcextip	L3 外部送信元 IP アドレス
- dstextip	L3 外部宛先 IP アドレス
- starttime	トラブルシューティング セッションの開始時刻

- endtime	トラブルシューティング セッションの終了時刻
- latestmin	開始時刻から始まるトラブルシューティング セッションの期間（分単位）
- description	セッションについての説明
- scheduler	レポート生成用のスケジューラ名
- srcepid	Obsolete
- dstepid	Obsolete
- include	Obsolete
- format	生成されるレポートの形式
- ui	内部的に使用（無視）
- sessionurl	レポートの場所
-action	traceroute/atomiccounter の start/stop/status など
- mode	内部的に使用
- _dc	内部的に使用
- ctx	内部的に使用

modifysession API

エンドポイント（Ep）とレイヤ 3（L3）との間の外部トラブルシューティング セッションを変更するには、**modifysession** API を使用します。モジュール名は **troubleshoot.epextutils.epextsession** で、関数は **modifySession** です。modifysession API の必須引数（**req_args**）は **- session** (session name) です。

次の表に、オプションの引数（**opt_args**）とそれぞれの説明を示します。

構文の説明

オプションの引数（opt_args）	説明
- srcep	送信元エンドポイント名
- dstep	宛先エンドポイント名
- srcip	送信元エンドポイント IP アドレス

- dstip	宛先エンドポイント IP アドレス
- srcmac	送信元エンドポイント MAC
- dstmac	宛先エンドポイント MAC
- srcextip	L3 外部送信元 IP アドレス
- dstextip	L3 外部宛先 IP アドレス
- starttime	トラブルシューティング セッションの開始時刻
- endtime	トラブルシューティング セッションの終了時刻
- latestmin	開始時刻から始まるトラブルシューティング セッションの期間（分単位）
- description	セッションについての説明
- scheduler	レポート生成用のスケジューラ名
- srcepid	Obsolete
- dstepid	Obsolete
- include	Obsolete
- format	生成されるレポートの形式
- ui	内部的に使用（無視）
- sessionurl	レポートの場所
-action	traceroute/atomiccounter の start/stop/status など
- mode	内部的に使用
- _dc	内部的に使用
- ctx	内部的に使用

atomiccounter API

エンドポイント（ep）間のアトミック カウンタ セッションを作成するには、**atomiccounter** API を使用します。モジュール名は **troubleshoot.epextutils.epext_ac** で、関数は **manageAtomicCounterPols** です。

atomiccounter API の必須引数（**req_args**）には、次のものが含まれます。

- - session (session name)
- - action (start/stop/status)

次の表に、オプションの引数（**opt_args**）とそれぞれの説明を示します。

構文の説明

オプションの引数（**opt_args**）	説明
- srcep	送信元エンドポイント名
- dstep	宛先エンドポイント名
- srcip	送信元エンドポイント IP アドレス
- dstip	宛先エンドポイント IP アドレス
- srcmac	送信元エンドポイント MAC
- dstmac	宛先エンドポイント MAC
- srcextip	L3 外部送信元 IP アドレス
- dstextip	L3 外部宛先 IP アドレス
- starttime	トラブルシューティング セッションの開始時刻
- endtime	トラブルシューティング セッションの終了時刻
- latestmin	開始時刻から始まるトラブルシューティング セッションの期間（分単位）
- ui	内部的に使用（無視）
- mode	内部的に使用
- _dc	内部的に使用
- ctx	内部的に使用

traceroute API

API を使用してエンドポイント（ep）とレイヤ 3 との間のトレースルート トラブルシューティング セッションを作成するには、**traceroute** API を使用します。モジュール名は **troubleshoot.epextutils.epext_traceroute** で、関数は **manageTraceroutePols** です。

traceroute API の必須引数（**req_args**）には、次のものが含まれます。

- - session (session name)
- - action (start/stop/status)

構文の説明

オプションの引数（**opt_args**）	説明
- protocol	プロトコル名
- dstport	宛先ポート名
- srcep	送信元エンドポイント
- dstep	宛先エンドポイント
- srcip	送信元 IP アドレス
- dstip	宛先 IP アドレス
- srcextip	送信元外部 IP アドレス
- dstIp	宛先外部 IP アドレス
- ui	内部的に使用（無視）
- mode	内部的に使用
- _dc	内部的に使用
- ctx	内部的に使用

span API

エンドポイント（Ep）とレイヤ 3（L3）との間の外部スパン トラブルシューティング セッションを作成するには、**span** API を使用します。モジュール名は **troubleshoot.epextutils.epext_span** で、関数は **monitor** です。

span API の必須引数（**req_args**）には、次のものが含まれます。

- - session (session name)
- - action (start/stop/status)
- - mode

構文の説明

次の表に、オプションの引数（**opt_args**）とそれぞれの説明を示します。

オプションの引数（**opt_args**）	説明

- portslist	ポートのリスト
- dstapic	宛先 APIC
- srcipprefix	ソース エンドポイントの IP アドレス プレフィクス
- flowid	フロー ID
- dstepg	宛先エンドポイント グループ
- dstip	宛先エンドポイント IP アドレス
- analyser	???
- desttype	宛先タイプ
- spansrcports	SPAN 送信元ポート

generatereport API

API を使用してトラブルシューティング レポートを生成するには、**generatereport** API を使用します。モジュール名は **troubleshoot.eptoeputils.report** で、関数は **generateReport** です。

generatereport API の必須引数（**req_args**）は **- session** (session name) です。

次の表に、オプションの引数（**opt_args**）とそれぞれの説明を示します。

構文の説明

オプションの引数（opt_args）	説明
- srcep	送信元エンドポイント名
- dstep	宛先エンドポイント名
- srcip	送信元エンドポイント IP アドレス
- dstip	宛先エンドポイント IP アドレス
- srcmac	送信元エンドポイント MAC
- dstmac	宛先エンドポイント MAC
- srcextip	L3 外部送信元 IP アドレス
- dstextip	L3 外部宛先 IP アドレス

- starttime	トラブルシューティング セッションの開始時刻
- endtime	トラブルシューティング セッションの終了時刻
- latestmin	開始時刻から始まるトラブルシューティング セッションの期間（分単位）
- description	セッションについての説明
- scheduler	レポート生成用のスケジューラ名
- srcepid	Obsolete
- dstepid	Obsolete
- include	Obsolete
- format	生成されるレポートの形式
- ui	内部的に使用（無視）
- sessionurl	レポートの場所
-action	traceroute/atomiccounter の start/stop/status など
- mode	内部的に使用
- _dc	内部的に使用
- ctx	内部的に使用

schedulereport API

API を使用してトラブルシューティング レポートの生成をスケジュールするには、**schedulereport** API を使用します。モジュール名は **troubleshoot.eptoeputils.report** で、関数は **scheduleReport** です。schedulereport API の必須引数（**req_args**）は **- session** です。

schedulereport API の必須引数（**req_args**）には、次のものが含まれます。

- - session (session name)
- - scheduler (scheduler name)

次の表に、オプションの引数（**opt_args**）とそれぞれの説明を示します。

構文の説明

オプションの引数（**opt_args**）	説明

- srcep	送信元エンドポイント
- dstep	宛先エンドポイント
- srcip	送信元エンドポイント IP アドレス
- dstip	宛先エンドポイント IP アドレス
- srcmac	送信元エンドポイント MAC
- dstmac	宛先エンドポイント MAC
- srcextip	L3 外部送信元 IP アドレス
- dstextip	L3 外部宛先 IP アドレス
- starttime	トラブルシューティング セッションの開始時刻
- endtime	トラブルシューティング セッションの終了時刻
- latestmin	開始時刻から始まるトラブルシューティング セッションの期間（分単位）
- description	セッションについての説明
- srcepid	Obsolete
- dstepid	Obsolete
- include	Obsolete
- format	生成されるレポートの形式
- ui	内部的に使用（無視）
- sessionurl	レポートの場所
-action	traceroute/atomiccounter の start/stop/status など
- mode	内部的に使用
- _dc	内部的に使用
- ctx	内部的に使用

getreportstatus API

API を使用して生成済みレポートのステータスを取得するには、**getreportstatus** API を使用します。モジュール名は **troubleshoot.eptoeputils.report** で、関数は **getStatus** です。

getreportstatus API の必須引数（**req_args**）には、次のものが含まれます。

- - session (session name)
- - sessionurl (session URL)
- - mode

（注） getreportstatus API のオプションの引数（**opt_args**）はありません。

getreportslist API

API を使用して生成済みレポートのリストを取得するには、**getreportslist** API を使用します。モジュール名は **troubleshoot.eptoeputils.report** で、関数は **getReportsList** です。

getreportslist API の必須引数（**req_args**）は **- session** (session name) および **- mode** です。

（注） getreportslist API のオプションの引数（**opt_args**）はありません。

getsessionslist API

API を使用してトラブルシューティング セッションのリストを取得するには、**getsessionslist** API を使用します。モジュール名は **troubleshoot.epextutils.epextsession** で、関数は **getSessions** です。

（注） この API には必須引数はありません。

次の表に、オプションの引数（**opt_args**）とそれぞれの説明を示します。

構文の説明

オプションの引数（opt_args）	説明
- session	セッション名
- srcep	送信元エンドポイント名
- dstep	宛先エンドポイント名

- srcip	送信元エンドポイント IP アドレス
- dstip	宛先エンドポイント IP アドレス
- srcmac	送信元エンドポイント MAC
- dstmac	宛先エンドポイント MAC
- srcextip	L3 外部送信元 IP アドレス
- dstextip	L3 外部宛先 IP アドレス
- starttime	トラブルシューティング セッションの開始時刻
- endtime	トラブルシューティング セッションの終了時刻
- latestmin	開始時刻から始まるトラブルシューティング セッションの期間（分単位）
- description	セッションについての説明
- scheduler	レポート生成用のスケジューラ名
- srcepid	Obsolete
- dstepid	Obsolete
- include	Obsolete
- format	生成されるレポートの形式
- ui	内部的に使用（無視）
- sessionurl	レポートの場所
- action	traceroute/atomiccounter の start/stop/status など
- mode	内部的に使用
- _dc	内部的に使用
- ctx	内部的に使用

getsessiondetail API

API を使用してトラブルシューティング セッションについての特定の詳細を取得するには、**getsessiondetail** API を使用します。モジュール名は **troubleshoot.epextutils.session** で、関数は **getSessionDetail** です。getsessiondetail API の必須引数（**req_args**）は **- session** (session name) です。

次の表に、オプションの引数（**opt_args**）とそれぞれの説明を示します。

構文の説明

オプションの引数（opt_args）	説明
- srcep	送信元エンドポイント名
- dstep	宛先エンドポイント名
- srcip	送信元エンドポイント IP アドレス
- dstip	宛先エンドポイント IP アドレス
- srcmac	送信元エンドポイント MAC
- dstmac	宛先エンドポイント MAC
- srcextip	L3 外部送信元 IP アドレス
- dstextip	L3 外部宛先 IP アドレス
- starttime	トラブルシューティング セッションの開始時刻
- endtime	トラブルシューティング セッションの終了時刻
- latestmin	開始時刻から始まるトラブルシューティング セッションの期間（分単位）
- description	セッションについての説明
- scheduler	レポート生成用のスケジューラ名
- srcepid	Obsolete
- dstepid	Obsolete
- include	Obsolete
- format	生成されるレポートの形式
- ui	内部的に使用（無視）

- sessionurl	レポートの場所
- action	traceroute/atomiccounter の start/stop/status など
- mode	内部的に使用
- _dc	内部的に使用
- ctx	内部的に使用

deletesession API

API を使用して特定のトラブルシューティングセッションを削除するには、**deletesession** API を使用します。モジュール名は **troubleshoot.epextutils.epextsession** で、関数は **deleteSession** です。

deletesession API の必須引数（**req_args**）は **- session** (session name) および **- mode** です。

（注） deletesession API のオプションの引数（**opt_args**）はありません。

clearreports API

API を使用して生成済みレポートのリストをクリアするには、**clearreports** API を使用します。モジュール名は **troubleshoot.eptoeputils.report** で、関数は **clearReports** です。

clearreports API の必須引数（**req_args**）は **- session** (session name) および **- mode** です。

（注） clearreports API のオプションの引数（**opt_args**）はありません。

contracts API

API を使用して契約情報を取得するには、**contracts** API を使用します。モジュール名は **troubleshoot.epextutils.epext_contracts** で、関数は **getContracts** です。contracts API の必須引数（**req_args**）は **- session** (session name) です。

次の表に、オプションの引数（**opt_args**）とそれぞれの説明を示します。

構文の説明

オプションの引数（opt_args）	説明
- srcep	送信元エンドポイント名

- dstep	宛先エンドポイント名
- srcip	送信元エンドポイント IP アドレス
- dstip	宛先エンドポイント IP アドレス
- srcmac	送信元エンドポイント MAC
- dstmac	宛先エンドポイント MAC
- srcextip	L3 外部送信元 IP アドレス
- dstextip	L3 外部宛先 IP アドレス
- starttime	トラブルシューティング セッションの開始時刻
- endtime	トラブルシューティング セッションの終了時刻
- latestmin	開始時刻から始まるトラブルシューティング セッションの期間（分単位）
- epext	エンドポイントから外部
- mode	内部的に使用
- _dc	内部的に使用
- ctx	内部的に使用
- ui	内部的に使用（無視）

ratelimit API

この項では、**ratelimit** API についての情報を記載しています。モジュール名は **troubleshoot.eptoeputils.ratelimit** で、関数は **control** です。ratelimit API の必須引数（**req_args**）は、**- action** (start/stop/status) です。

次の表に、オプションの引数（**opt_args**）とそれぞれの説明を示します。

構文の説明

オプションの引数（opt_args）	説明
- srcep	送信元エンドポイント名
- dstep	宛先エンドポイント名

- srcip	送信元エンドポイント IP アドレス
- dstip	宛先エンドポイント IP アドレス
- srcmac	送信元エンドポイント MAC
- dstmac	宛先エンドポイント MAC
- srcextip	L3 外部送信元 IP アドレス
- dstextip	L3 外部宛先 IP アドレス
- starttime	トラブルシューティング セッションの開始時刻
- endtime	トラブルシューティング セッションの終了時刻
- latestmin	開始時刻から始まるトラブルシューティング セッションの期間（分単位）
- epext	エンドポイントから外部
- mode	内部的に使用
- _dc	内部的に使用
- ctx	内部的に使用

13ext API

この項では、**13ext** API についての情報を記載しています。モジュール名は **troubleshoot.epextutils.l3ext** で、関数は **execute** です。13ext API の必須引数（**req_args**）は、**- action** (start/stop/status) です。

次の表に、オプションの引数（**opt_args**）とそれぞれの説明を示します。

構文の説明

オプションの引数（opt_args）	説明
- srcep	送信元エンドポイント名
- dstep	宛先エンドポイント名
- srcip	送信元エンドポイント IP アドレス
- dstip	宛先エンドポイント IP アドレス

- srcmac	送信元エンドポイント MAC
- dstmac	宛先エンドポイント MAC
- srcextip	L3 外部送信元 IP アドレス
- dstextip	L3 外部宛先 IP アドレス
- starttime	トラブルシューティング セッションの開始時刻
- endtime	トラブルシューティング セッションの終了時刻
- latestmin	開始時刻から始まるトラブルシューティング セッションの期間（分単位）
- epext	エンドポイントから外部
- mode	内部的に使用

第 16 章

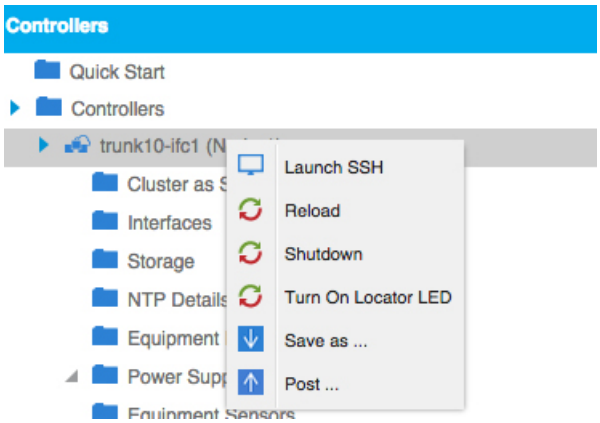
APIC のトラブルシューティングの操作

APIC システムのシャット ダウン

この手順では、APIC システムをシャットダウンする方法について説明します。

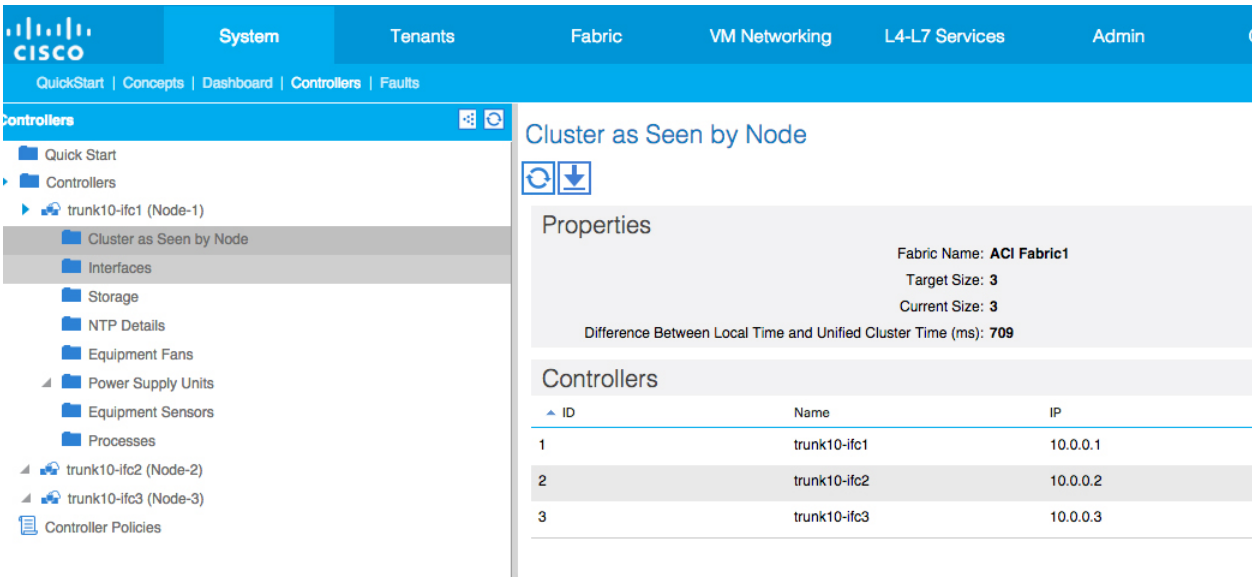
（注） システムをシャットダウンしてから、移動させ（ファブリック全体の再配置）、電源を入れると、それに応じてタイム ゾーンまたは NTP サーバ（あるいはその両方）が更新されます。

1 APIC は一度に 1 つずつ、右クリックして、プルダウン メニューから [Shutdown] を選択してシャットダウンします。



2 新しい場所で APIC を起動します。

3 クラスタが完全に統合されていることを次のように確認します。



4 次の APIC に進みます。

はじめる前に

クラスタ ヘルスが十分に正常であることを確認します。

GUI を使用した APIC コントローラのシャットダウン

このマニュアルでは、APIC コントローラをシャットダウンする方法について説明します。

（注） この手順は、APIC コントローラのみ（APIC システム全体ではない）をシャットダウンする方法を説明します。この手順を実行すると、コントローラはすぐにシャットダウンされます。コントローラの再起動は実マシンから行うしか方法がないため、シャットダウンの実行には注意が必要です。。マシンにアクセスする必要がある場合には、この章の「GUI を使用したロケータ LED のオンへの切り替え」の項を参照してください。

単一の APIC コントローラをシャットダウンするには、次の手順に従います。

（注） 可能であれば、APIC は一度に 1 つずつ移動させます。オンラインのクラスタに少なくとも 2 つの APIC がある限り、読み取り/書き込みアクセス権があります。複数の APIC を一度に再配置する必要がある場合、残りのオンラインのコントローラは 1 つまたはなしという結果になり、ファブリックはシャットダウン時に読み取り専用モードになります。この間、エンドポイントの移動（仮想マシンの移動）を含め、ポリシー変更はできません。APIC を次の手順でシャットダウンしたら、コントローラを再配置し、新しいラックで再度電源を入れます。次に、クラスタ ヘルスが十分に正常な状態に戻ったことを確認します。

1 メニュー バーで、[System] をクリックします。

2 サブメニュー バーで、[Controllers] をクリックします。

3 [Controllers] で、リロードする APIC ノード（たとえば、**apic1 (Node-1)**）をクリックします。

4 画面上部の右ウィンドウ ペインで、[General] タブをクリックします。

5 画面上部の右ウィンドウ ペインのタブから、[ACTIONS] プルダウン メニューをクリックします。

6 プルダウン メニューから [Shutdown] を選択すると、APIC コントローラは即座にリロードされます。

（注） この [Shutdown] オプションを使用する別の方法として、APIC ノード（**apic1 (Node-1)** など）を右クリックし、プルダウン リストから [Shutdown] を選択します。

7 コントローラを再配置して、電源を入れます。

8 クラスタ ヘルスが十分に正常な状態に戻ったことを確認します。

GUI を使用した APIC リロード オプションの使用

このマニュアルでは、GUI を使用して APIC コントローラ（APIC システム全体ではない）をリロードする方法を説明します。

APIC コントローラをリロードするには、次の手順を実行します。

1 メニュー バーで、[System] をクリックします。

2 サブメニュー バーで、[Controllers] をクリックします。

3 [Controllers] で、リロードする APIC ノード（たとえば、**apic1 (Node-1)**）をクリックします。

4 画面上部の右ウィンドウ ペインで、[General] タブをクリックします。

5 画面上部の右ウィンドウ ペインのタブから、[ACTIONS] プルダウン メニューをクリックします。

6 プルダウン メニューから [Reload] を選択すると、APIC コントローラは即座にリロードされます。

（注） この [Reload] オプションを使用する別の方法として、APIC ノード（**apic1 (Node-1)** など）を右クリックし、プルダウン リストから [Reload] を選択します。

GUI を使用した LED ロケータの制御

このマニュアルでは、GUI を使用して APIC コントローラの LED ロケータをオンにする方法を説明します。

GUI を使用して APIC コントローラの LED ロケータをオン（またはオフ）にするには、次の手順に従います。

1 メニュー バーで、[System] をクリックします。

2 サブメニュー バーで、[Controllers] をクリックします。

3 [Controllers] で、リロードする APIC ノード（たとえば、**apic1 (Node-1)**）をクリックします。

4 画面上部の右ウィンドウ ペインで、[General] タブをクリックします。

5 画面上部の右ウィンドウ ペインのタブから、[ACTIONS] プルダウン メニューをクリックします。

6 プルダウン メニューから、[Turn On LED Locator]（または [Turn Off LED Locator]）を選択します。

（注） このオプションを使用する別の方法として、APIC ノード（**apic1 (Node-1)** など）を右クリックし、プルダウン メニューから [Turn On LED Locator]（または [Turn Off LED Locator]）を選択します。

第 17 章

SSL 暗号方式のトラブルシューティング

SSL 暗号化について

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 ）の Representational State Transfer（REST）API は、HTTPS/SSL/TLS サポートがますます厳しくなっている状況下で、そのソリューションが新しいバージョンに導入されるようになったときから進化を遂げてきました。このマニュアルの目的は、Cisco ACI REST API での HTTPS、SSL、および TLS サポートの進化について説明し、クライアントが REST API をセキュアな方法で使用するために必要な事柄の手引きを読者に提供することです。

HTTPS は、Secure Sockets Layer（SSL）または Transport Layer Security（TLS）のいずれかを使用して、HTTP セッション用のセキュア接続を確立するプロトコルです。SSL または TLS は、クライアントと HTTP サーバとの間のトラフィックを暗号化するために使用されます。さらに、HTTPS をサポートするサーバには、サーバの信頼性を確認するために、通常はクライアントが使用できる証明書があります。これはサーバ側でクライアントを認証するのとは逆です。この場合、サーバは「わたしは server_xyz で、ここにその証明書があります」と伝えていることになります。クライアントはその証明書を使用して、サーバが「server_xyz」であることを確認できます。

SSL/TLS には他の重要な側面があり、これには各プロトコルで使用できるサポート対象の暗号化の暗号方式と、SSL または TLS プロトコルの継承セキュリティが関係しています。SSL は、SSLv1、SSLv2、SSLv3 という 3 つのバージョンを経てきましたが、そのどれもが今ではセキュアではないと見なされています。TLS は、TLSv1、TLSv1.1、TLSv1.2 と 3 つのバージョンを経てきましたが、TLSv1.1 と TLSv1.2 のみがセキュアと見なされています。クライアントは使用可能な最高バージョンの TLS を使用し、サーバは TLSv1.1 と TLSv1.2 のみをサポートするのが理想的です。ただし、ほとんどのサーバは、旧式クライアントに対応するために TLSv1 のサポートを維持する必要があります。

ほぼすべての最新ブラウザは、TLSv1.1 と TLSv1.2 の両方をサポートします。ただし、HTTPS を使用するクライアントはブラウザではない場合もあります。クライアントが Web サーバと通信する Java アプリケーションまたは Python スクリプトであるという場合があり、その場合には

HTTPS/TLS をネゴシエートする必要があります。このような状況では、サポート対象とサポート箇所についての確認ははるかに重要になります。

サポートされる SSL 暗号化の確認

はじめる前に

この項では、CLI を使用して、サポートされている SSL 暗号方式を判別する方法について説明します。

ステップ 1 次のように、openssl 環境でサポートされている暗号方式を取得します。

例：

```
openssl ciphers 'ALL:eNULL'
```

ステップ 2 次のように、SED などのツールを使用して、暗号方式を分離します。

例：

```
openssl ciphers 'ALL:eNULL' |  sed -e 's/:/\n/g'
```

ステップ 3 次のように、暗号方式をループ処理して、APIC をポーリングし、どの暗号方式がサポートされているかを確認します。

例：

```
openssl s_client -cipher ?<some cipher to test>? -connect <apic ipaddress>:<ssl port, usually 443>
```

次の暗号の例を参照してください。

例：

```
openssl s_client -cipher ?ECDHE-ECDSA-AES128-GCM-SHA256? -connect 10.1.1.14:443
```

（注） 応答に CONNECTED が含まれていれば、その暗号方式はサポートされています。

付 録 A

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 このコマンドのセットは文書化を目的として公開しており、ACIの日常業務での使用は推奨しません。これらは内部コマンドとしての使用を意図しており、正しく使用しないとネットワークに重大な問題を引き起こす可能性があります。どの操作を実行する場合でも、実行する前にファブリックに対するすべての影響を理解しておくようにしてください。

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 targeted：目的のクラスタのサイズ • active=：APIC が到達可能であるかどうかを示す • health=：全体的な APIC のヘルスの要約サービスと、低下したヘルス スコアが表示されます。 • chassisID=：特定の APIC の既知のシャーシ ID （注） ピアのシャーシ ID は、現在クラスタ内にない APIC には正しくない可能性があります。
bootcurr	次回の起動時に、APIC システムは Linux パーティションで現在の APIC イメージを起動します。このオプションは、通常時の使用を予期していません。
bootother	次回の起動時に、APIC システムは Linux パーティションで前の APIC イメージを起動します。このオプションは、通常時の使用を予期していません。
bond0test	リーフへの APIC 接続の破壊的テストです。これはシスコ社内でのテスト目的のみに使用され、それ以外の使用では、ファブリックへの APIC 接続に問題を引き起こす可能性があります。
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	指定の APIC インターフェイスを停止して再起動します。

オプション	機能
preservelogs	APIC は現在のログをアーカイブします。これは通常の再起動時に自動的に実行されます。このオプションは、ハード リブート前に使用できます。
run	選択可能な 2 つのオプションは、iptables-list と lldptool です。iptables-list は、管理テナント契約により制御される Linux iptables を表示するために使用されます。lldptool は、APIC により送受信される lldp 情報を表示するために使用されます。
rvread	データ層の状態を要約します。出力は、各サービス用のデータ層の状態についての要約を示します。シャード ビューは昇順で複製を表示します。
rvread *service*	すべてのレプリカのすべてのシャード上にある、サービス用のデータ層の状態が表示されます。 （注） 以下に例を示します。例, （161 ページ）
rvread*service shard*	すべてのレプリカの特定のシャード上にある、サービス用のデータ層の状態が表示されます。 （注） 以下に例を示します。例, （161 ページ）
rvread *service shard replica*	特定のシャードとレプリカ上にある、サービス用のデータ層の状態が表示されます。 （注） 以下に例を示します。例, （161 ページ）
validateimage	ファームウェア リポジトリにイメージをロードする前に、イメージを検証することができます。この機能は、リポジトリに追加されるイメージの通常プロセスの一部として実行されることに注意してください。
validateenginxconf	APIC 上の生成済み nginx 設定ファイルを検証して、nginx がその設定ファイルを使用して開始できることを確認します。これは nginx Web サーバが APIC 上で稼働していない場合の、デバッグでの使用を意図しています。

表 *2* : サーバ *ID*

サービス	ID
cliD	1
コントローラ	2
eventmgr	3
extXMLApi	4
policyelem	5
policymgr	6
reader	7
ae	8
topomgr	9
observer	10
dbgr	11
observerelem	12
dbgrelem	13
vmmmgr	14
nxosmock	15
bootmgr	16
appliancedirector	17
adrelay	18
ospaagent	19
vleafelem	20
dhcpd	21
scripthandler	22
idmgr	23

サービス	ID
ospaelem	24
osh	25
opflexagent	26
opflexelem	27
confelem	28
vtap	29

表 *3* : データ状態

状態	ID
COMATOSE	0
NEWLY_BORN	1
UNKNOWN	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。
インストーラ	APIC に新しいイメージをインストールし、-c でクリーン インストールを実行します。
mgmt	APIC のすべてのサービスを指定します。
reboot	APICを再起動します。
restart	APIC のサービスを再起動します。
start	APIC のサービスを起動します。
stop	APIC のサービスを停止します。
touch [clean | setup]	APIC の設定をリセットします。 • **clean** オプションは、APICのネットワーク設定（ファブリック名、IP アドレス、ログインなど）を保持すると同時に、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 ネットワーク設定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。

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	ルート パスワードの生成に使用するトークンを生成します。これは必要に応じて TAC の操作中に、指示どおりに使用します。
version	APIC ISO ソフトウェアのバージョンを表示します。

例

次の例は、**acidiag** コマンドの使用方法を示しています。

```
admin@apic1:~> acidiag version
1.0.0.414

admin@apic1:~> acidiag verifyapic
openssl_check: certificate details
subject= CN=Insieme,O=Insieme Networks,L=SanJose,ST=CA,C=US
issuer= O=Default Company Ltd,L=Default City,C=XX
notBefore=Jul 19 20:40:32 2013 GMT
notAfter=Jul 19 20:40:32 2014 GMT
openssl_check: passed
ssh_check: passed
all_checks: passed

admin@apic1:~> acidiag avread
Local appliance ID=1 ADDRESS=10.0.0.1 TEP ADDRESS=10.0.0.0/16
CHASSIS_ID=10220833-ea00-3bb3-93b2-ef1e7e645889
Cluster of 3 lm(t):1(2014-07-12T19:54:04.877+00:00) appliances
  (out of targeted 3 lm(t):3(2014-07-12T19:55:03.442+00:00))
   with FABRIC_DOMAIN name=mininet set to version=1.0(0.414)
lm(t):3(2014-07-12T19:55:13.564+00:00)
    appliance id=1 last mutated at 2014-07-12T19:46:06.831+00:00 address=10.0.0.1 tep
address=10.0.0.0/16
       oob address=192.168.10.1/24 version=1.0(0.414) lm(t):1(2014-07-12T19:54:05.146+00:00)

       chassisId=10220833-ea00-3bb3-93b2-ef1e7e645889 lm(t):1(2014-07-12T19:54:05.146+00:00)

        commissioned=1 registered=1 active=yes(zeroTime)
        health=(applnc:255 lm(t):1(2014-07-12T20:01:22.934+00:00) svc's)
    appliance id=2 last mutated at 2014-07-12T19:51:10.649+00:00 address=10.0.0.2 tep
address=10.0.0.0/16
       oob address=192.168.10.2/24 version=1.0(0.414) lm(t):2(2014-07-12T19:54:05.064+00:00)

       chassisId=5d74122c-2ab9-3ccb-b06d-f620d5e20ccd lm(t):2(2014-07-12T19:54:05.064+00:00)

        commissioned=1 registered=1 active=yes(2014-07-12T19:51:10.651+00:00)
        health=(applnc:255 lm(t):2(2014-07-12T20:01:22.442+00:00) svc's)
    appliance id=3 last mutated at 2014-07-12T19:54:05.028+00:00 address=10.0.0.3 tep
address=10.0.0.0/16
       oob address=192.168.10.3/24 version=1.0(0.414) lm(t):3(2014-07-12T19:54:05.361+00:00)

       chassisId=71355d49-6fe7-3a78-a361-72d6c1e3360c lm(t):3(2014-07-12T19:54:05.361+00:00)

        commissioned=1 registered=1 active=yes(2014-07-12T19:54:05.029+00:00)
        health=(applnc:255 lm(t):3(2014-07-12T20:01:22.892+00:00) svc's)
clusterTime=<diff=0 common=2014-07-14T16:52:20.343+00:00 local=2014-07-14T16:52:20.343+00:00
 pF=<displForm=0
```

```
    offsSt=0 offsVlu=0 lm(t):3(2014-07-12T19:55:03.750+00:00)>>
------------------------------------------------

admin@apic1:~> 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)>>

admin@apic1:~> 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)>>
```

索 引