トラブルシューティング

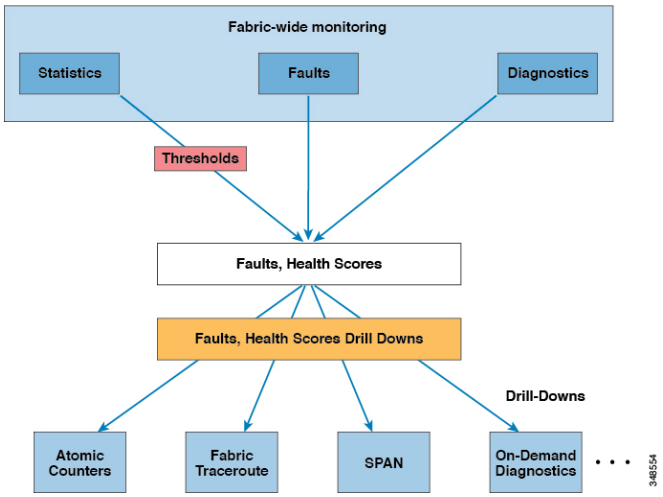
この章は、次の内容で構成されています。

- トラブルシューティング （1 ページ）
- ACL 契約の許可および拒否ログについて （2 ページ）
- ARP、ICMP Ping および Traceroute （3 ページ）
- アトミック カウンタ （4 ページ）
- デジタル オプティカル モニタリング（DOM）について （5 ページ）
- ヘルススコア （6 ページ）
- SPAN の概要 （12 ページ）
- SNMP について （13 ページ）
- Syslog について （13 ページ）
- トラブルシューティング ウィザードについて （14 ページ）
- Cisco Nexus 9000 スイッチの安全な消去について （15 ページ）

トラブルシューティング

ACI ファブリックでは、次の図に示すように広範なトラブルシューティングとモニタリングのツールが提供されます。

図 *1:* トラブルシューティング



ACL 契約の許可および拒否ログについて

契約ルールのトラフィック フローをログ記録および監視するには、契約の許可ルールのため送信されることが許可されたパケットまたはフローのログを有効化および表示するか、契約の許可ルールのためドロップされたフローのログを有効化および表示できます。

- 禁止契約拒否ルール
- 契約の件名でアクションを拒否する
- 契約または件名の例外
- ACI ファブリックの ACL コントラクト許可は、EX または FX で終わる名前の Nexus 9000 シリーズ スイッチ、およびそれ以降のすべてのモデルでのみサポートされます。たとえば、N9K-C93180LC-EX や N9K-C9336C-FX のように指定してください。
- ACI ファブリックでのログの拒否は、すべてのプラットフォームでサポートされています。
- 管理契約のフィルタでログ directive を使用することはサポートされていません。ログ directive を設定すると、ゾーン分割ルールの展開エラーが発生します。

標準および禁止契約と件名についての詳細は、『*CiscoApplication Centric Infrastructure Fundamentals*』および『*Cisco APIC Basic Configuration Guide*』を参照してください。

ACL 許可および拒否ログ出力に含まれる EPG データ

Cisco APIC、リリース 3.2(1) まで、ACL 許可および拒否ログでは、記録されている契約に関連付けられた EPG を識別していませんでした。リリース 3.2(1) では、送信元 EPG と 送信先 EPG が ACI 許可および拒否ログの出力に追加されます。ACL 許可および拒否ログには、次の制限を持つ関連 EPG を含めます。

- ネットワーク内の EPG の配置によっては、ログの EPG データを使用できない場合があります。
- 設定の変更が発生するとき、ログデータが期限切れになっている可能性があります。安定した状態では、ログ データは正確です。

ログが次にフォーカスされているとき、許可および拒否ログの EPG データは最も正確になります。

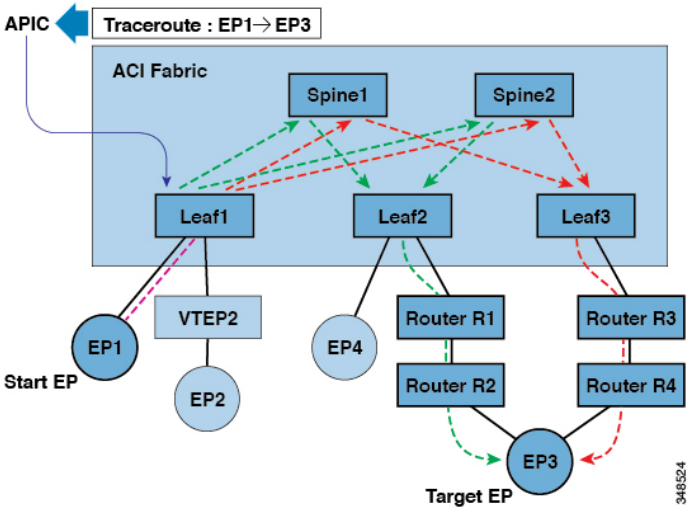
- 入力 TOR で入力ポリシーがインストールされており、出力 TOR で出力ポリシーがインストールされている場合の EPG から EPG へのフロー。
- 境界リーフ TOR で 1 個のポリシーが適用され、非 BL TOR で他のポリシーが適用されている場合の EPG から L3Out へのフロー。

ログ出力の EPG は、共有サービス（共有 L3Outs を含む）で使用される uSeg Epg または Epg ではサポートされていません。

ARP、ICMP Ping および Traceroute

デフォルトゲートウェイ IP アドレスの ARP は入力リーフスイッチでトラップされます。入力リーフスイッチは ARP リクエストを接続先にユニキャストし、接続先は ARP 応答を送信します。

図 *2 : APIC* エンドポイント/エンドポイント トレースルート



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

トレースルート モードには、エンドポイント/エンドポイント、リーフ/リーフ（TEP/TEP）があります。トレースルートはファブリック全体のすべてのパスを検出し、外部エンドポイントの出口を検出します。パスが妨げられているかどうかを発見するのに役立ちます。

トレースルートはIPv6の送信元と宛先アドレスで動作しますが、IPv4アドレスとIPv6アドレスを混在させて送信元IPアドレスと宛先アドレスを構成することはできません。送信元（RsTrEpIpSrc）と接続先（RsTrEpIpDst）の関係は、fvIpタイプの送信元と接続先をサポートします。同じエンドポイントから複数のIPアドレスが学習されることがあります。管理者は、目的の送信元アドレスと宛先アドレスを選択します。

アトミック カウンタ

Cisco APIC リリース 6.1(2) 以降、アトミック カウンタはサポートされなくなりました。

アトミックカウンタは、ファブリック内のドロップと誤ルーティングを検出します。結果の統計により、アプリケーションの接続の問題をすばやくデバッグして分離できます。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。アトミック カウンタは、IPv6 または IPv4 の送信元アドレスと宛先アドレスに対して機能しますが、異なるアドレス ファミリ間では機能しません。

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。送信元と接続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スイッチにドリル 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。

- ドロップ、承認および超過パケットのカウント
- 最後の 30 秒などの短期間のデータ収集、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 未満の場合にのみ使用可能）
- 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。

テナントのアトミック カウンタは次を提供できます。

- ドロップ、承認および超過パケットを含む、ファブリック全体のトラフィックのアプリケーション固有カウンタ
- モードは次を含みます。
  - Endpoint-to-endpoint アドレス、または Endpoint-to-endpoint IP アドレス。1 つのターゲット エンドポイントに複数の IP アドレスが関連付けられている可能性があることに注意してください。
  - EPG から EPG
  - EPG からエンドポイント
  - EPG から *（任意）
  - エンドポイントから外部 IP アドレス

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

（注） 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仮想ルート転送（VRF）インスタンス（コンテキストまたはプライベートネットワークとも呼ばれます）にある場合はサポートされません。アトミック カウンタは IPv6 の送信元と接続先で動作しますが、IPv4 アドレスと IPv6 アドレスを混在させて送信元 IP アドレスと宛先 IP アドレスを構成することはできません。

エンドポイントが同じ EPG に属している場合、IPv6 ヘッダーを持つレイヤ 2 ブリッジド トラフィックの、それらのエンドポイント間でのアトミック カウンタ統計は報告されません。

EPG または ESG から L3Out EPG に流れるトラフィックに対してアトミック カウンタが機能するには、すべてのプレフィックスとマッチさせるため、0/0 ではなく 0/1 および 128/1 を使用して L3Out EPG を設定します。

デジタル オプティカル モニタリング（DOM）について

リアルタイムのデジタル オプティカル モニタリング（DOM）データは SFP、SFP+、および XFP から定期的に収集され、警告およびアラームのしきい値テーブル値と比較されます。収集された DOM データは、トランシーバ送信バイアス電流、トランシーバ送信電力、トランシーバ受信電力、およびトランシーバ電源電圧です。

ヘルススコア

ACIファブリックは、ポリシーモデルを使用してデータを正常性スコアに組み入れます。正常性スコアは、システム、インフラストラクチャ、テナント、アプリケーション、またはサービスなどのさまざまなエリアに集約できます。

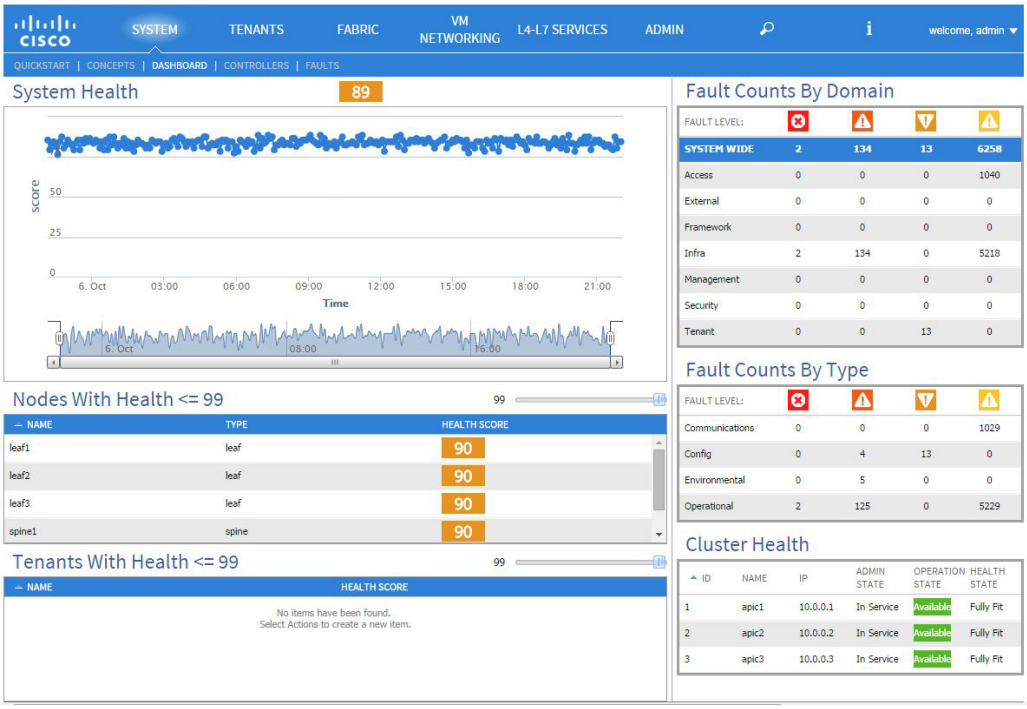
ACI ファブリック ヘルス情報は、システムの次の表示画面で見ることができます。

- System：ポッドの正常性スコア、テナントの正常性スコア、ドメインおよびタイプごとのシステム エラー数、APIC クラスタの正常性の状態など、システム全体の正常性の集約を示します。
- Pod：ポッド（スパインおよびリーフスイッチのグループ）の正常性スコアの集約、ドメインおよびタイプごとのポッド全体のエラー数を示します。
- Tenant：テナント固有のアプリケーションおよびEPGなどのオブジェクトのパフォーマンスデータを含むテナントの正常性スコアの集約、ドメインおよびタイプごとのテナント全体のエラー数を示します。
- Managed Object：管理対象オブジェクト（MO）（独立 MO および関連 MO を含む）の正常性スコア ポリシーを示します。これらのポリシーは、管理者によりカスタマイズできます。

システムおよびポッドの正常性スコア

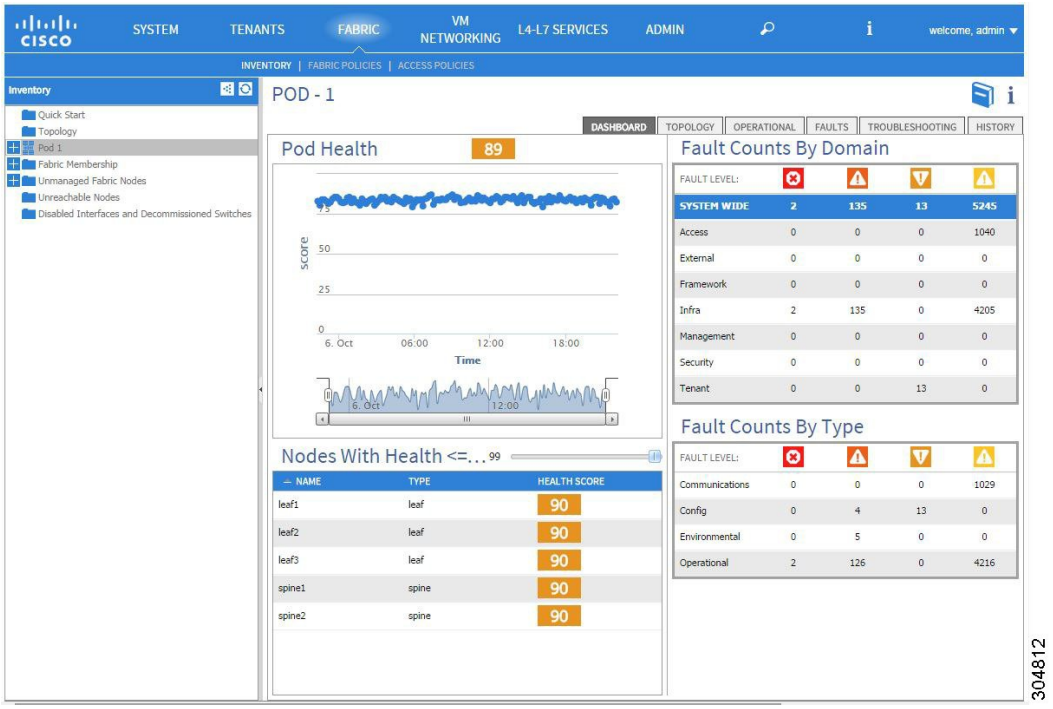
システムとポッドの正常性スコアは、リーフスイッチとスパインスイッチの正常性スコア、およびリーフスイッチで学習されたエンドポイントの数に基づいています。GUI システム ダッシュボードには、ドメイン タイプごとのシステム全体の障害数、およびノードごとのAPICクラスタの管理状態、動作状態、および正常性の状態も表示されます。

図 *3 :* システム正常性スコア



ポッドの正常性スコアは、リーフスイッチとスパインスイッチのへ正常性スコア、およびリーフスイッチで学習されたエンドポイントの数に基づいています。GUI ファブリック ポッド ダッシュボード画面には、ドメインおよびタイプごとのポッド全体の障害数も表示されます。

図 *4:* ポッド正常性スコア



304812

システムとポッドの正常性スコアは同じ方法で計算されます。この計算は、リーフ正常性スコアの加重平均を、リーフスイッチの学習済みエンドポイントの総数で割った値に、スパインの数とその正常性スコアから得られるスパイン係数を掛けたものに基づいています。

次の式は、この計算がどのように行われるかを示しています。

図 *5:* システムおよびポッドの正常性スコアの計算

$$Health_{Fabric} = \frac{\sum_{i=1}^{N_{Leaf}} Health_{Leaf_i} \times Weight_{Leaf_i}}{\sum_{i=1}^{N_{Leaf}} Weight_{Leaf_i}} \times \left(1 - \left(1 - \frac{\sum_{i=1}^{N_{Spine}} Health_{Spine_i}}{N_{Spine} \times 100}\right)^{N_{Spine}}\right)$$

304814

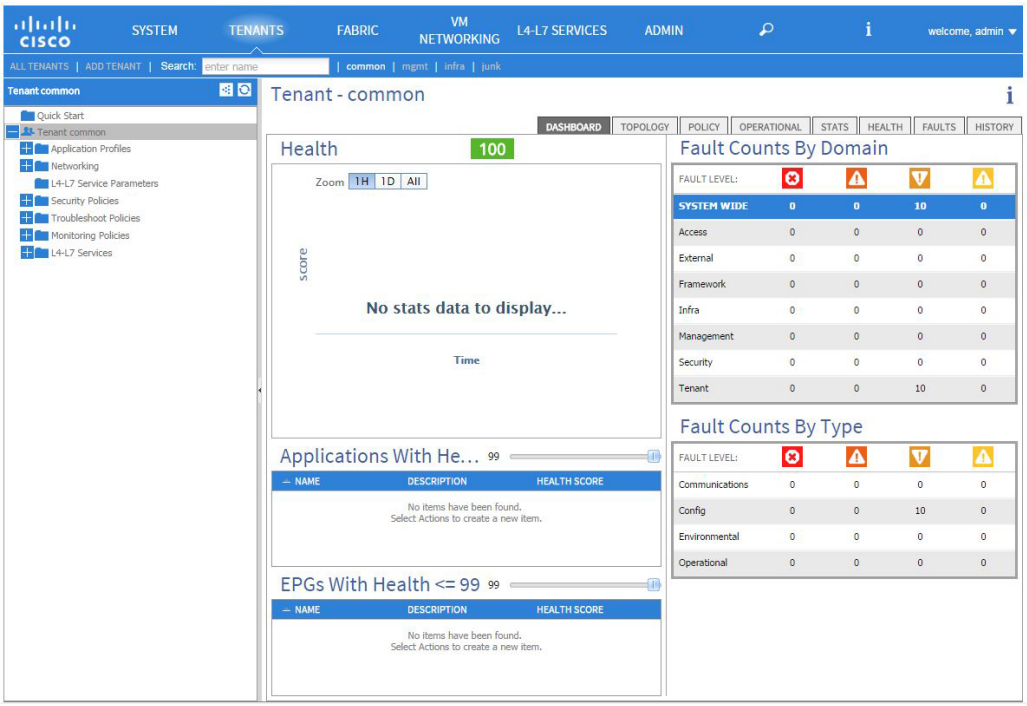
次の凡例は、方程式のコンポーネントを定義します。

- 正常性 $_{\text{Leaf}\,i}$ は、リーフスイッチの正常性スコアです。
- 重み $_{\text{Leaf}\,i}$ は、リーフスイッチのエンドポイントの数です。
- N $_{\text{Leaf}}$は、ファブリック内のリーフスイッチの数です。
- 正常性 $_{\text{Spine}\,i}$ は、スパイン スイッチの正常性スコアです。
- N $_{\text{Spine}}$ は、ファブリック内のスパイン スイッチの数です。

テナントの正常性スコア

テナントの正常性スコアは、テナントが使用するインフラストラクチャ全体のテナント全体の論理オブジェクトの正常性スコアを集計します。GUI テナント ダッシュボード画面には、ドメインおよびタイプごとのテナント全体の障害数も表示されます。

図 *6*:テナントの正常性スコア

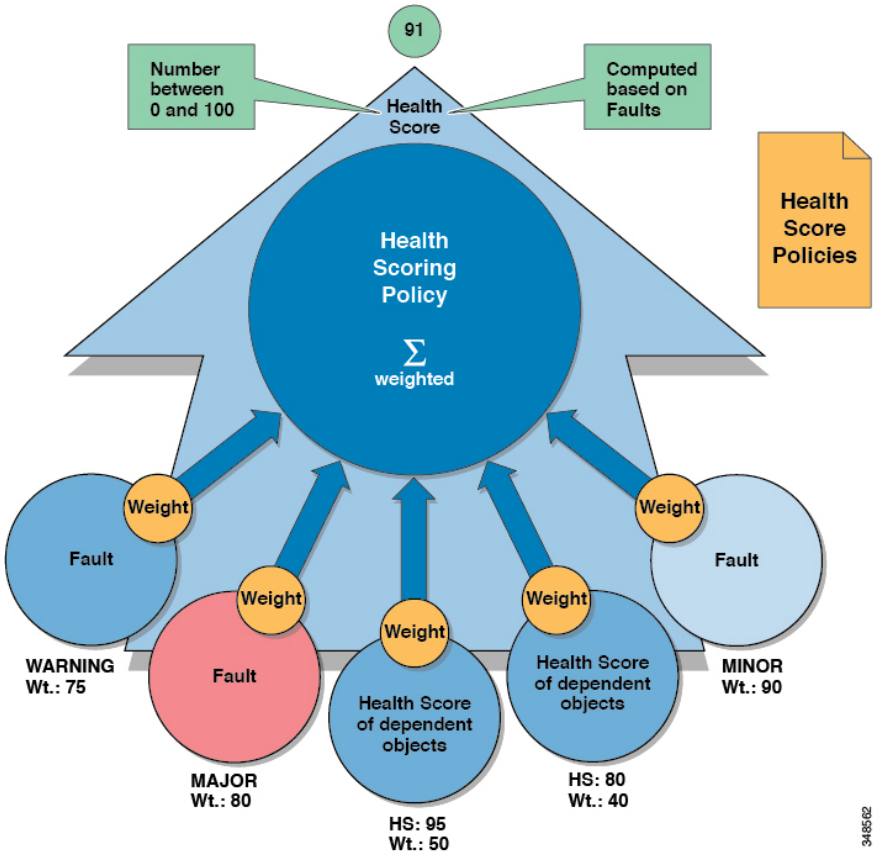


たとえば、EPGは2つのリーフスイッチのポートを使用している可能性があります。各リーフスイッチには、展開された EPG コンポーネントが含まれます。学習されたエンドポイントの数は、重み係数です。各ポートは、学習されたエンドポイントの数が異なる場合があります。したがって、EPG 正常性スコアは、各 EPG コンポーネントの正常性スコアとそのリーフで学習されたエンドポイントの数を合計し、EPGが使用するリーフスイッチ全体で学習されたエンドポイントの総数で割ったものになります。

MO 正常性スコア

各管理対象オブジェクト（MO）は、正常性スコアのカテゴリに属しています。デフォルトでは、MO の正常性スコアのカテゴリは MO のクラス名と同じです。

図 *7: M0* 正常性スコア



各正常性スコア カテゴリには影響レベルが割り当てられます。正常性スコアの 5 つの影響レベルは、Maximum、High、Medium、Low および None です。たとえば、ファブリック ポートのデフォルトの影響レベルは Maximum で、リーフ ポートのデフォルトの影響レベルは High です。子 MO の特定のカテゴリは、正常性スコアの影響レベル None を割り当てることで、親 MO のヘルス スコアの計算から除外できます。これらのオブジェクト間の影響レベルは、ユーザが構成できます。ただし、デフォルトの影響レベルが None の場合は、管理者はこれを上書きできません。

次の係数は、さまざまな影響レベルです。

Maximum：100% High：80% Medium：50% Low：20% None：0%

カテゴリ正常性スコアは、Lp ノルム式を使用して計算されます。正常性スコア ペナルティは、100 - 正常性スコアと等しくなります。正常性スコア ペナルティは、所定のカテゴリに属し、正常性スコアが計算される MO の子または直接親族である MO のセットの全体的な正常性スコア ペナルティを表します。

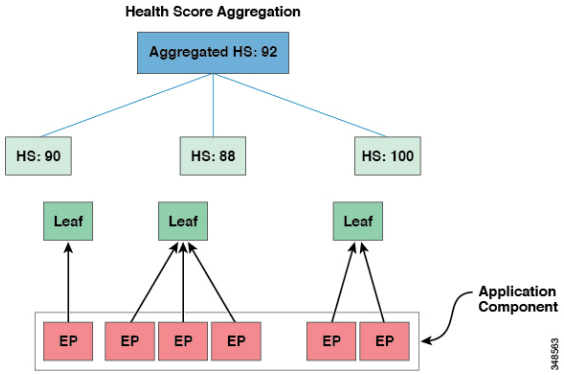
MO クラスの正常性スコアのカテゴリは、ポリシーを使用して変更できます。たとえば、リーフ ポートのデフォルトの正常性スコア カテゴリは `eqpt:LeafP` で、ファブリック ポートのデフォルトの正常性スコア カテゴリは `eqpt:FabP` です。ただし、リーフ ポートとファブリック

ポートの両方を含むポリシーは、ポートと呼ばれる同じカテゴリの一部になるように作成できます。

正常性スコアの集約と影響

アプリケーションコンポーネントの正常性スコアは、次の図に示すように複数のリーフスイッチに分散できます。

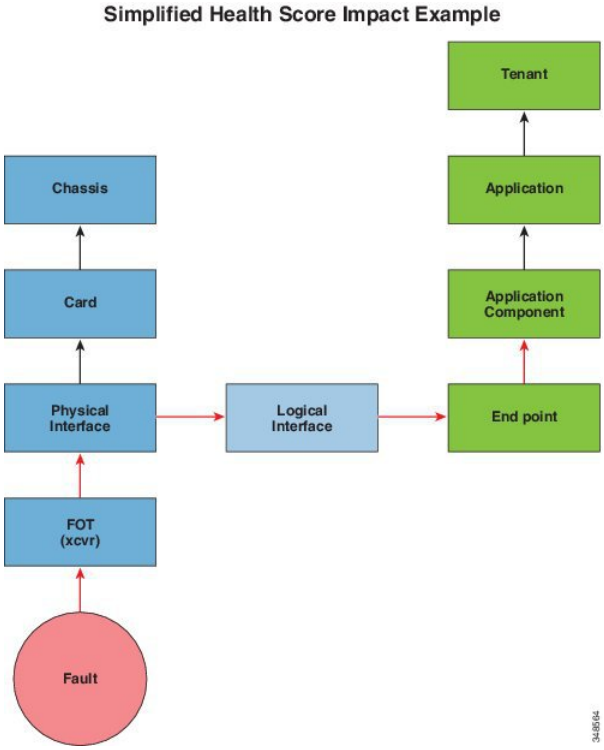
図 *8 :* 正常性スコアの集約



集約された正常性スコアは、APIC で計算されます。

次の図では、ハードウェアの障害が、アプリケーションコンポーネントの正常性スコアに影響します。

図 *9:* 簡略化した正常性スコアの影響の例



SPAN の概要

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

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

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

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

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

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。

その他の情報

SPAN の設定、使用、および制限の詳細については、*Cisco APIC Troubleshooting Guide* を参照してください。

SNMP について

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

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

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

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

Syslog について

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

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

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

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

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

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

Syslog の表示形式を NX-OS スタイル形式に変更できます。

これらのシステム メッセージを生成する障害またはイベントの詳細は、『*Cisco APIC Faults, Events, and System Messages Management Guide*』で説明しています。システム ログ メッセージのリストについては『*Cisco ACI System Messages Reference Guide*』を参照してください。

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

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 ウィザードを使用すると、ネットワークの動作を理解して可視化できるため、問題が発生した場合にネットワークに関する懸念を緩和できます。たとえば、2 つのエンドポイントで断続的なパケット損失が発生しているが、その理由がわからない場合があります。トラブルシューティング ウィザードを使用すると、問題を評価できるため、この問題のある動作の原因であると思われる各マシンにログオンするのではなく、問題を効果的に解決できます。

このウィザードを使用すると、管理ユーザは、選択した送信元と接続先の特定の時間枠に発生する問題のトラブルシューティングを行うことができます。デバッグを実行する時間枠を定義でき、TAC に送信できるトラブルシューティング レポートを生成できます。

関連トピック

トラブルシューティング ウィザードの開始
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

Cisco Nexus 9000 スイッチの安全な消去について

Cisco Nexus 9000 スイッチは、永続的なストレージを利用して、システム ソフトウェア イメージ、スイッチ構成、ソフトウェア ログ、および動作履歴を維持します。これらの各エリアには、ネットワーク アーキテクチャや設計の詳細など、ユーザ固有の情報と、潜在的な攻撃者からの目標ベクトルが含まれている可能性があります。安全な消去機能を使用すると、この情報を包括的に消去できます。これは、返品許可（RMA）を使用してスイッチを返品するとき、スイッチをアップグレードまたは交換するとき、または寿命に達したシステムを廃止するときに実行できます。

セキュア消去は、Cisco APIC リリース 6.0(x) からサポートされています。ファブリック内のすべてのリーフおよびスパイン スイッチは、APIC リリース 6.0(x) 以降である必要があります。

この機能は、次のストレージ デバイスのユーザ データを消去します。

- SSD
- EMMC
- MTD
- CMOS
- NVRAM

（注） すべてのスイッチ モデルにこれらすべてのストレージ デバイスがあるわけではありません。

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