モニタリング

この章は、次の内容で構成されています。

障害、エラー、イベント、監査ログ

（注） 障害、イベント、エラー、システム メッセージについては、Web ベースのアプリケーションである『*Cisco APIC Faults, Events, and System Messages Management Guide*』および『*Cisco APIC Management Information Model Reference*』を参照してください。

APIC は、MO の集合形式で ACI ファブリック システムの管理および操作状態の包括的な現在のランタイム表現を維持します。システムは、これらのプロセスを管理するためにシステムとシステムおよびユーザーが作成するポリシーのランタイム状態に従って、障害、エラー、イベント、および監査ログ データを生成します。

APIC GUI を使用すると、ファブリック スイッチのカスタマイズされた「履歴レコード グループ」を作成できます。これに、カスタマイズされたスイッチ ポリシーを割り当てて、それらのグループのスイッチ用に維持する監査ログ、イベント ログ、正常性ログ、および障害ログのカスタマイズされたサイズと保持期間を指定できます。

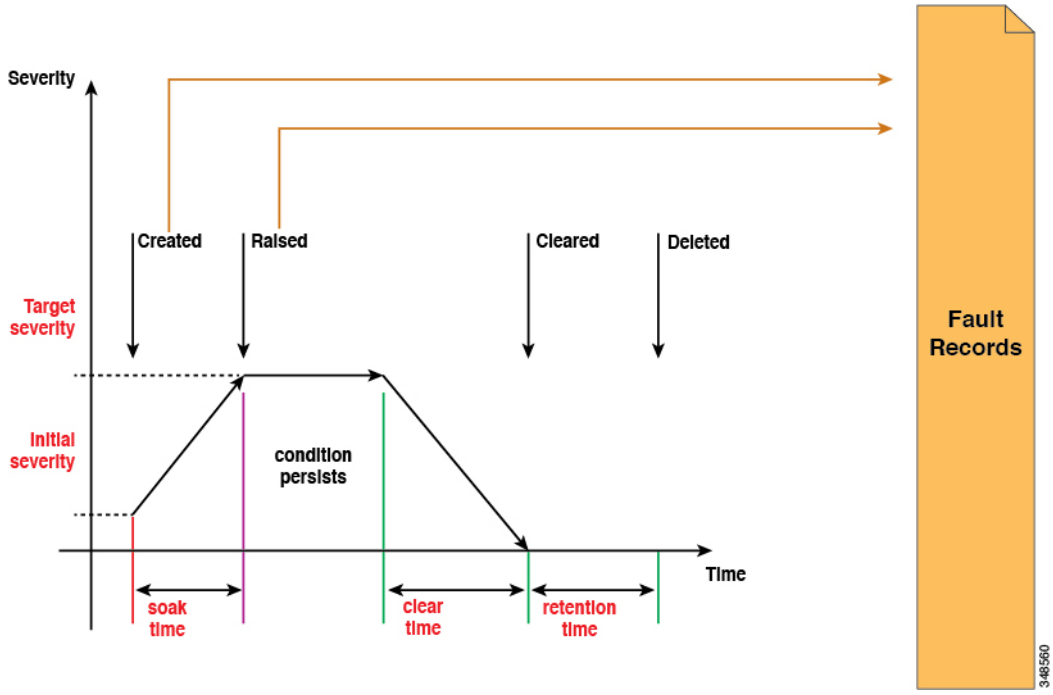
APIC GUI を使用すると、このファブリック上のコントローラに対して維持される監査ログ、イベント ログ、正常性ログ、および障害ログのサイズと保持期間を指定するグローバル コントローラ ポリシーをカスタマイズすることもできます。

障害

システムの実行時の状態に基づいて、APICは自動的に異常を検出し、障害を表す障害オブジェクトを作成します。障害オブジェクトには、ユーザが問題を診断してその影響を評価するのに役立ち、解決策を提供するように作られているさまざまなプロパティが含まれます。

たとえば、高いパリティエラー率などポートに関連する問題をシステムが検出すると、障害オブジェクトが自動的に作成され、ポートオブジェクトの子として管理情報ツリー（MIT）内に配置されます。同じ状況が複数回検出される場合、障害オブジェクトの追加インスタンスは作成されません。障害を引き起こした状況が修正された後、障害オブジェクトは障害のライフサイクルポリシーで指定された一定期間保存され、最終的に削除されます。次の図を参照してください。

図 *1*: 障害のライフサイクル



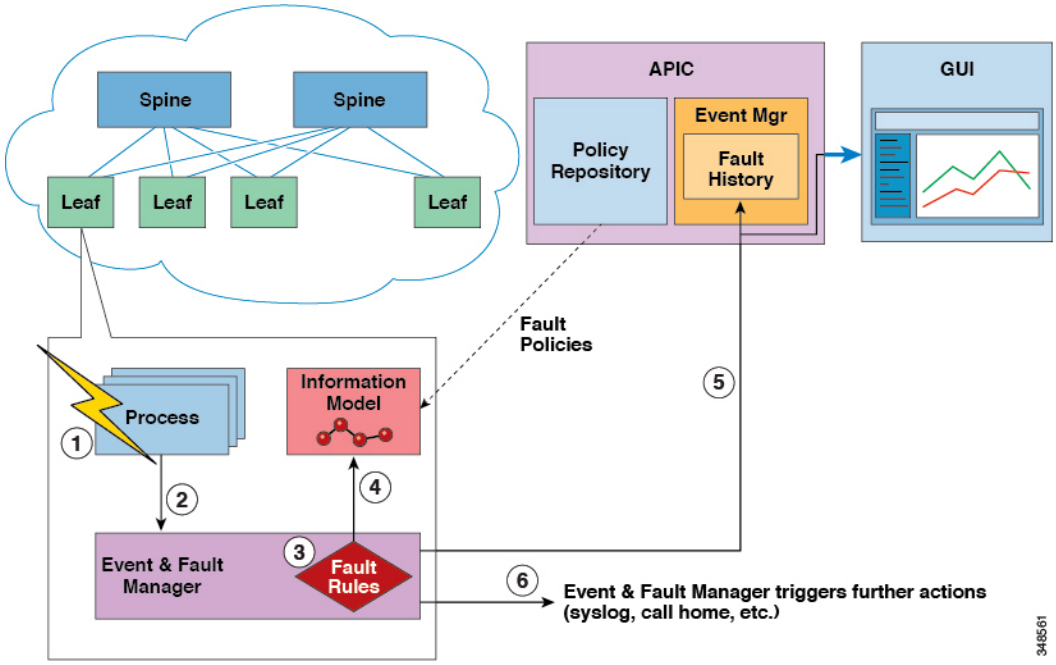
ライフサイクルは問題の現在の状態を表します。サイクルは問題が最初に検出されると、そのソーク時間で開始され、提起された状態へと変わって、問題がまだ存在するとその状態のままになります。状態がクリアされると、「raised-clearing」と呼ばれるステータスに移行します。そのステータスでは、その状態がまだ存在する可能性があると見なされます。次に、「clearing time」に移行し、最終的に「retaining」に移行します。この時点で、問題は解決されたと見なされ、ユーザが最近解決された問題を確認できるようにする目的のために障害オブジェクトは保持されます。

ライフサイクルの移行が発生するたびに、システムは自動的にそれを記録する障害記録オブジェクトを作成します。障害レコードは、作成後は変更されることはなく、レコード数が障害保持ポリシーで指定された最大値を超えた場合にのみ削除されます。

シビラティ（重大度）は、サービスを提供するシステムの機能に対するその状態の影響の概算値です。考えられる値は、Warning（注意）、Minor、Major および Critical です。Warning（注意）に相当するシビラティ（重大度）の障害は、導入されているサービスには現在影響を与えていない潜在的な問題を示します（たとえば、不完全または矛盾した構成など）。Minor および Major の障害は、提供されるサービスが低下する可能性があることを示します。Critical は、大規模な停電がサービスを著しく低下させていたり、同時にサービスが悪化していることを意味します。説明には、追加情報を提供したりトラブルシューティングに役立てるために用意された人間に解読可能な問題の説明が含まれます。

次の図は、障害とイベントに関するレポートを作成するプロセスを示します。

図 *2*: 障害およびイベントのレポート/エクスポート



1. プロセスが障害のある状態を検出します。
2. プロセスが Event and Fault Manager に通知します。
3. Event and Fault Manager は障害ルールに従って通知を処理します。
4. Event and Fault Manager は、MIM で障害インスタンスを作成し、障害ポリシーに従ってそのライフ サイクルを管理します。
5. Event and Fault Manager は、APIC および接続されたクライアントに状態遷移を通知します。
6. Event and Fault Manager は、追加のアクションをトリガーします（syslog や call home など）。

ログ レコード オブジェクト

ログ レコード オブジェクトについて

Cisco Application Centric Infrastructure（ACI）ファブリックのイベント（生成された障害、クリアされた障害など）、Cisco Application Policy Infrastructure Controller（APIC）またはスイッチのイベントなど、すべてのイベントがデータベースに記録されるため、ユーザはステータス遷移の履歴、イベントなどをレビューすることが可能です。Cisco APIC ノードおよびスイッチ ノードはどちらも、障害、イベントなどを自ら生成して保存します。ただし、スイッチ ノードからのログ レコードは Cisco APIC にも複製されるため、Cisco APIC ノードおよびスイッチ ノードを含むファブリック全体のログ レコードを Cisco APIC から表示できます。さらに、Cisco APIC データベースは、Cisco APIC をアップグレードした後でも、Cisco APIC ノードおよびスイッチ ノードの両方のログ レコードを保持します。対照的に、スイッチをアップグレードすると、スイッチのログ レコードは失われます。

ログ レコード オブジェクトはシステムによって作成され、ユーザが変更または削除することはできません。ログ レコード オブジェクトのライフサイクルは、保持ポリシーによって制御されます。クラスごとのログ レコード オブジェクトの数が保持ポリシーの最大制限に達すると、最も古いログ レコード オブジェクトがデータベースから削除され、新しいレコード用のスペースが確保されます。

ログ レコード オブジェクトは、次のログ レコード クラスに分類されます。

- **[障害記録（Fault Records）]**：障害記録は、ライフサイクル変更の履歴を示します。障害ルールは、管理対象オブジェクト クラスで定義されます。管理対象オブジェクトに障害がある場合、障害が発生し、管理対象オブジェクトに関連付けられます。障害状態がなくなると、障害はクリアされます。障害が発生またはクリアされるか、ライフサイクル状態が変更されるたびに、FAULT 状態の変化を記録するために障害レコード オブジェクトが作成されます。

- **[イベント レコード（Event Records）]**：Cisco APIC によって管理されるイベントです。各イベント レコードは、スイッチまたは Cisco APIC ノードで発生したイベントを表します。イベント ルールは、管理対象オブジェクト クラスで定義されます。管理対象オブジェクトの状態がイベント ルールに一致すると、イベント（または `eventRecord` オブジェクト）が作成されます。たとえば、スイッチからカードを抜くと、スイッチ イベント マネージャはユーザ操作のイベント通知を生成します。

- **[監査ログ（Audit Logs）]**：監査ログは、管理対象オブジェクトが変更されたときに記録される履歴レコードであり、変更を行ったユーザが含まれます。監査ログには、システムによって内部的に変更された管理対象オブジェクトも記録されます。

- **[セッション ログ（Session logs）]**：セッション ログは、ユーザが Cisco APIC またはスイッチにログインまたはログアウトしたときに記録される履歴レコードであり、クライアントの IP アドレスが含まれています。

- **[正常性レコード（Health Records）]**：正常性レコードは、管理対象オブジェクトの正常性スコア変更の履歴レコードです。管理対象オブジェクトの正常性スコアが 5 ポイント変化するたびに、正常性レコード オブジェクトが作成されます。

ファブリック内の各ログ レコード オブジェクトの最大数は、保持ポリシーによって定義されます。これは、ファブリック全体で数百万になる可能性があります。このような大量のデータをクエリすると、クエリへの応答が遅くなり、最悪の場合、クエリが失敗する可能性があります。これを防止するために、Cisco APIC リリース 5.1(1) 以降、ログ レコード オブジェクトの応答が大幅に高速化されるように、特にリーダープロセスが強化されました。ただし、トレードオフとして、クエリ（ページ）間の並べ替えは保証されません。

クエリ パフォーマンスの向上と新しい制限は、このセクションで説明されているログ レコード オブジェクトのクエリにのみ適用されます。

Cisco APIC リリース 5.2(3) 以降、ログ レコード オブジェクトに対してのみサポートされる新しい API クエリ オプションの `time-range` を使用すると、Cisco APIC はページ間のソートを維持しながら、ログ レコード オブジェクトの API クエリにはるかに高速に応答できます。Cisco APIC GUI はまた、`time-range` オプションを使用することでパフォーマンスとソートを向上します。ログ レコード オブジェクトのクエリの詳細については、『*Cisco APIC REST API* 構成ガイド』リリース *4.2(x)* 以降）を参照してください。

GUI を使用したログ レコード オブジェクトの表示

Cisco Application Policy Infrastructure Controller（APIC）GUI を使用して、Cisco APIC または スイッチのデータベースからログ レコードオブジェクトを表示できます。5.2(3) リリース以降、次のいずれかの方法を使用してログ レコード オブジェクトを表示します。

- ファブリック内のすべての Cisco APIC およびスイッチについて、**[システム（System）] > > [履歴（History）]**タブに移動し、**[作業（Work）]** ペインでいずれかのログ レコード タブを選択します。
- 特定のスイッチについては、**[ファブリック（Fabric）]< >[インベントリ（Inventory）]**タブに移動します。**[ナビゲーション（Navigation）]** ペインで、**[*pod_id*] > > [*leaf_name]*** に移動します。**[作業（Work）]** ペインで、**[履歴（History）]** タブを選択してから、ログ レコード サブタブの 1 つを選択します。

レコードは作成日時の降順で表示されます。**[過去 *x time_measurement* 内の履歴（History within the last x time_measurement）]** の右側にある下矢印をクリックして期間を選択することで、期間に基づいて表示されるログ レコードを絞り込むことができます。**[カスタム（custom）]** 選択により、任意の範囲の日付を指定できます。

1 つ以上のフィルタを作成して、表示されるログ レコードを絞り込むこともできます。**[属性でフィルタ（Filter by attributes）]** フィールドをクリックし、属性を選択し、演算子を選択してから、値を選択または入力します（属性に応じて）。作成するフィルタごとにこのプロセスを繰り返します。

または、レコードのテーブルの値にカーソルを合わせると、値の右側にフィルタアイコン（じょうごで表される）が表示され、アイコンをクリックします。これで、適切なパラメータを持つフィルタが自動的に作成されます。たとえば、障害レコードを表示しているときに障害コード F103824 のフィルタ アイコンをクリックすると、次のパラメータを使用してフィルタが作成されます。`Code == F103824` 自動作成されたフィルタは、`==` 演算子のみをサポートします。

[作業（Work）] ペインの下部にある **[行（Rows）]** ドロップダウン リストを使用して、1 ページに表示するレコードの数を選択します。**[行（Rows）]** の値を大きくすると、GUI の応答時間が遅くなる可能性があります。別のログ レコード クラスをクリックすると、**[行（Rows）]** の値はデフォルトの 10 にリセットされます。

[アクション（Actions）] メニューでは、次のアクションを実行できます。

- **[すべてダウンロード（Download All）]**：選択したクラスのすべてのレコードをローカル システムにダウンロードします。指定した時間範囲とフィルタは無視されます。レコードは XML または JSON ファイルとしてダウンロードできます。

[システム（System）] > **>[履歴（History）]** タブからログ レコード オブジェクトを表示している場合は、行の右端にある 3 つのドットをクリックして、その特定のレコードで追加のアクションを実行できます。 イベント レコードの場合、可能なアクションは次のとおりです。

- **[シビラティ（重大度）の変更（Change Severity）]**：イベントのシビラティ（重大度）を選択するシビラティ（重大度）に変更します。同じイベント コードを持つすべての新しいイベントにも、選択したシビラティ（重大度）が適用されます。同じイベント コードを持つ他のすべての既存のイベントのシビラティ（重大度）は変更されません。
- **[イベントを無視（Ignore Event）]**：イベントは表示されなくなり、同じイベント コードを持つすべての新しいイベントは表示されません。同じイベント コードを持つ他のすべての既存のイベントは引き続き表示されます。
- **[Object Store Browser で開く（Open in Object Store Browser）]**：Object Store Browser の特定のレコードを新しい Web ブラウザ タブで開きます。
- **[名前を付けて保存（Save As）]**：特定のレコードをローカル システムにダウンロードします。レコードは XML または JSON ファイルとしてダウンロードできます。

他のすべてのログ レコード クラスの場合、可能なアクションは次のとおりです。

- **[Object Store Browser で開く（Open in Object Store Browser）]**：Object Store Browser の特定のレコードを新しい Web ブラウザ タブで開きます。
- **[名前を付けて保存（Save As）]**：特定のレコードをローカル システムにダウンロードします。レコードは XML または JSON ファイルとしてダウンロードできます。

Errors

APIC エラー メッセージは通常、APIC GUI および APIC CLI に表示されます。これらのエラー 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。

- Informational（情報提供）メッセージ。実行しているアクションのヘルプおよびヒントを提供します。
- 警告メッセージ。ユーザが構成または管理しているオブジェクト（ユーザー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。

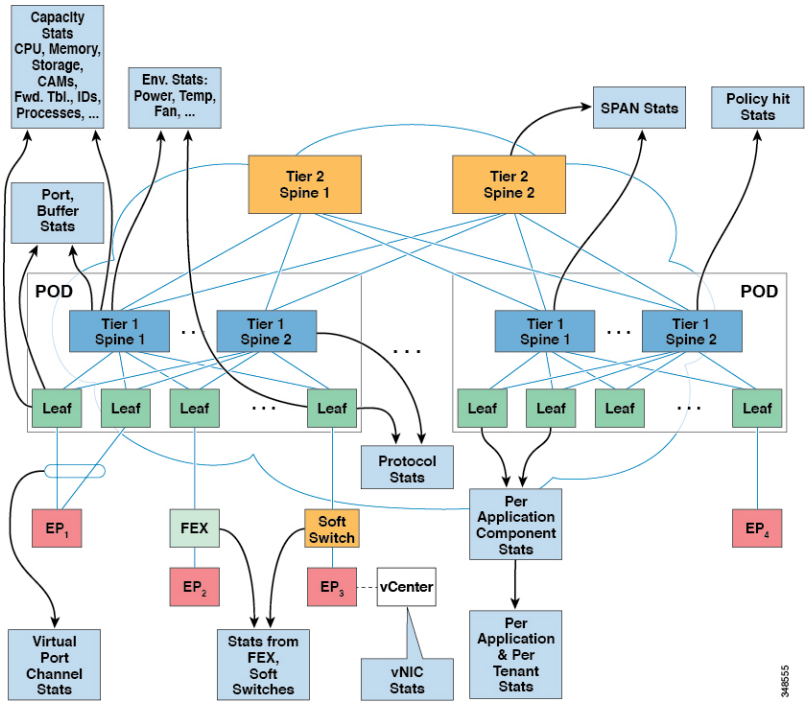
- Finite State Machine（FSM）のステータスメッセージ。FSM 段階のステータスに関する情報を提供します。

多くのエラーメッセージには、1つまたは複数の変数が含まれます。これらの変数を置き換えるために APIC が使用する情報は、メッセージのコンテキストによって決まります。一部のメッセージは、複数のタイプのエラーによって生成される場合があります。

統計プロパティ、階層、しきい値およびモニタリング

統計により、トレンド分析とトラブルシューティングが可能になります。統計収集は、継続的またはオンデマンドの収集用に構成できます。統計により、監視対象オブジェクトのリアルタイム測定が提供されます。統計は、累積カウンタとゲージで収集できます。

図 *3*：統計のさまざまな送信元



ポリシーは、収集する統計の種類、間隔、実行するアクションを定義します。たとえば、入力 VLAN でドロップされたパケットのしきい値が毎秒 1000 を超える場合、ポリシーは EPG 上で 1 つの障害を生成することができます。

統計データは、インターフェイス、VLAN、EPG、アプリケーションプロファイル、ACL ルール、テナント、内部 Cisco Application Policy Infrastructure Controller（APIC）プロセスなどのさまざまな送信元から収集されます。統計は、5 分、15 分、1 時間、1 日、1 週間、1 か月、1 四半期、または1年のサンプリング間隔でデータを蓄積します。短い期間の間隔によって、長い間隔が与えられます。

平均、最小、最大、傾向、変化のペースなど、さまざまな統計プロパティを使用できます。収集/保持時間は構成できます。ポリシーは、統計をシステムの現在の状態から収集するか、履歴的に蓄積するか、またはその両方かを指定できます。たとえば、ポリシーは、履歴統計を 1 時間にわたって 5 分間隔で収集するように指定できます。1 時間は移動ウィンドウです。1 時間が経過すると、次の 5 分間の統計が追加され、一番最初の 5 分間に収集されたデータが放棄されます。

（注） 5 分の粒度サンプル レコードの最大数は 3 サンプル（15 分の統計）に制限されています。他のすべてのサンプル間隔は、1,000 サンプル レコードに制限されています。たとえば、1 時間の粒度統計は 41 日間まで保持できます。統計は、これらの制限を超える期間は保持されません。長期間にわたって統計を収集するには、エクスポートポリシーを作成します。

統計データについて

次のタイプの管理対象オブジェクト（MO）は、オブザーバ モジュールによって収集される統計データに関連付けられています。

- 履歴データ
- 現在のデータ

これらのオブジェクトに対応する MO 名は、HD または CD の 2 文字のプレフィックスで始まります。HD は履歴データを示し、CD は現在のデータを示します。たとえば、「CDl2IngrBytesAg15min」です。MO 名は、データが収集される時間間隔の指標でもあります。たとえば、「CDl2IngrBytesAg15min」は、MO が 15 分間隔に対応することを示します。

CD オブジェクトは現在実行中のデータを保持しており、オブジェクトが保持する値は時間の経過とともに変化します。ただし、指定された時間間隔の最後に、CD オブジェクトで収集されたデータが HD オブジェクトにコピーされ、CD オブジェクトの属性が 0 にリセットされます。たとえば、指定された 15 分間隔の最後に、CDl2IngrBytesAg15min オブジェクトのデータが HDl2IngrBytesAg15min オブジェクトに移動され、CDl2IngrBytesAg15min オブジェクトがリセットされます。

CD...15min オブジェクト データを 15 分以上注意深く観察すると、値が 0 になり、その後 2 回増分され、再び 0 になることがわかります。これは、値が 5 分ごとに更新されるためです。データは HD オブジェクトにロールアップされ、その更新が発生するとすぐに CD オブジェクトがリセットされるため、3 回目の更新（15 分の経過後）は気付かれません。

CD...15min オブジェクトは 5 分ごとに更新され、CD...5min オブジェクトは 10 秒ごとに更新されます。CD...15min オブジェクトは HD...15min オブジェクトとしてロールアップされ、CD...5min オブジェクトは HD...5min オブジェクトとしてロールアップされます。

CD オブジェクトが保持するデータは動的であり、実際には内部データであると見なされる必要があります。HD データ オブジェクトは、さらなる分析目的に使用でき、公開データまたは静的データと見なすことができます。

HD オブジェクトも時間の経過とともにロールアップされます。たとえば、3 つの連続する HD...5min データ オブジェクトは、1 つの HD...15min オブジェクトに寄与します。1 つの HD...5 分オブジェクトがシステムに存在する時間の長さは、統計収集ポリシーによって決定されます。

モニタリング ポリシーの構成

管理者は、次の 4 つの広い範囲でモニタリング ポリシーを作成できます。

- ファブリック全体：ファブリック オブジェクトとアクセス オブジェクトの両方が含まれます。
- アクセス（別名インフラストラクチャ）：アクセス ポート、FEX、VM コントローラなど
- ファブリック：ファブリック ポート、カード、シャーシ、ファンなど
- テナント：EPG、アプリケーション プロファイル、サービスなど

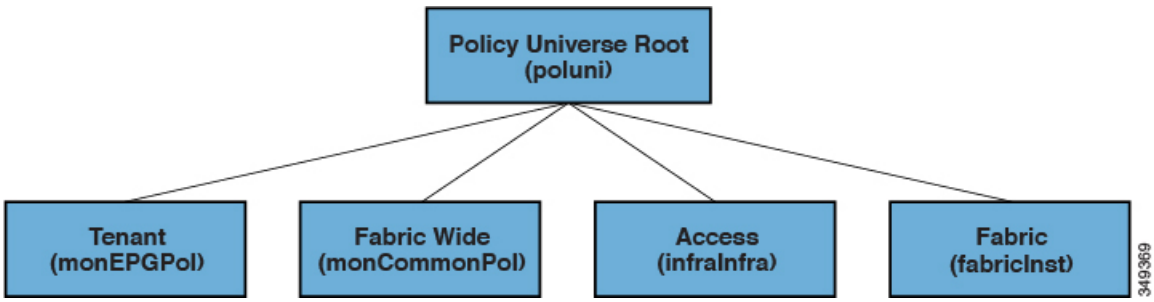
Cisco Application Policy Infrastructure Controller（APIC）には、デフォルトのモニタリング ポリシーの次の 4 つのクラスが含まれます。

- `monCommonPol`（uni/fabric/moncommon）：すべてのファブリック、アクセス、およびテナント階層に適用されます。
- `monFabricPol`（uni/fabric/monfab-default）：ファブリック階層に適用されます。
- `monInfraPol`（uni/infra/monifra-default）：アクセス インフラストラクチャ階層に適用されます。
- `monEPGPol`（uni/tn-common/monepg-default）：テナント階層に適用されます。

モニタリング ポリシーの 4 つのクラスそれぞれにおいて、デフォルト ポリシーは特定のポリシーによって上書きできます。たとえば、Solar テナント（*tn-solar*）に適用されたモニタリング ポリシーは、他のテナントがまだデフォルト ポリシーによってモニタされている一方で、Solar テナントのデフォルト ポリシーを上書きします。

次の図の 4 つのオブジェクトのそれぞれには、モニタリングのターゲットが含まれます。

図 *4:* デフォルト モニタリング ポリシーの *4* つのクラス



インフラ モニタリング ポリシーには monInfra ターゲットが含まれ、ファブリック モニタリング ポリシーには monFab ターゲットが含まれ、テナント モニタリング ポリシーには monEPG ターゲットが含まれます。各ターゲットは、この階層内のオブジェクトの対応するクラスを表します。たとえば、monInfra-default モニタリング ポリシーには、FEX ファブリック対面ポートを表すターゲットがあります。これらの FEX ファブリック対面ポートのモニタリング方法に関するポリシーの詳細はこのターゲットに含まれています。ターゲットに適用できるポリシーのみがそのターゲット下で許可されます。考えられるターゲットすべてがデフォルトで自動作成されるわけではないことに注意してください。管理者は、ターゲットがない場合にポリシー下でターゲットを追加できます。

共通モニタリング ポリシー（monCommonPol ）は、グローバル ファブリック全体の範囲を持ち、Cisco APIC を含むファブリック内のすべてのノードに自動的に展開されます。共通のモニタリング ポリシーの下にある送信元（syslog、callhome、SNMP など）は、すべての障害、イベント、監査、および正常性の発生をキャプチャします。単一の共通モニタリング ポリシーは、ファブリック全体をモニタします。syslog および snmp のシビラティ（重大度）のしきい値、または callhome の緊急度は、ファブリック管理者が適切であると判断した詳細レベルに従って構成できます。

複数のモニタリング ポリシーを使用して、ファブリックの個々の部分を個別にモニタできます。たとえば、グローバル モニタリング ポリシーの下にある送信元は、グローバル ビューを反映します。一部のノードにのみ展開されたカスタム モニタリング ポリシーの下にある別の送信元は、電源を詳しくモニタできます。または、異なるテナントの特定の障害またはイベントの発生は、n.jpgy 特定のオペレーターにリダイレクトできます。

他のモニタリング ポリシーの下にある送信元は、より小さな範囲内で障害、イベント、および監査をキャプチャします。モニタリング ポリシーの直下にある送信元は、範囲内（ファブリックやインフラなど）のすべての発生をキャプチャします。ターゲットの下にある送信元は、そのターゲットに関連するすべての発生をキャプチャします（たとえば、電源の eqpt:Psu）。障害/イベントの重大度の割り当てポリシーの下にある送信元は、その特定の障害またはイベントに一致する発生のみを、障害/イベント コードによって ide.jpgied としてキャプチャします。

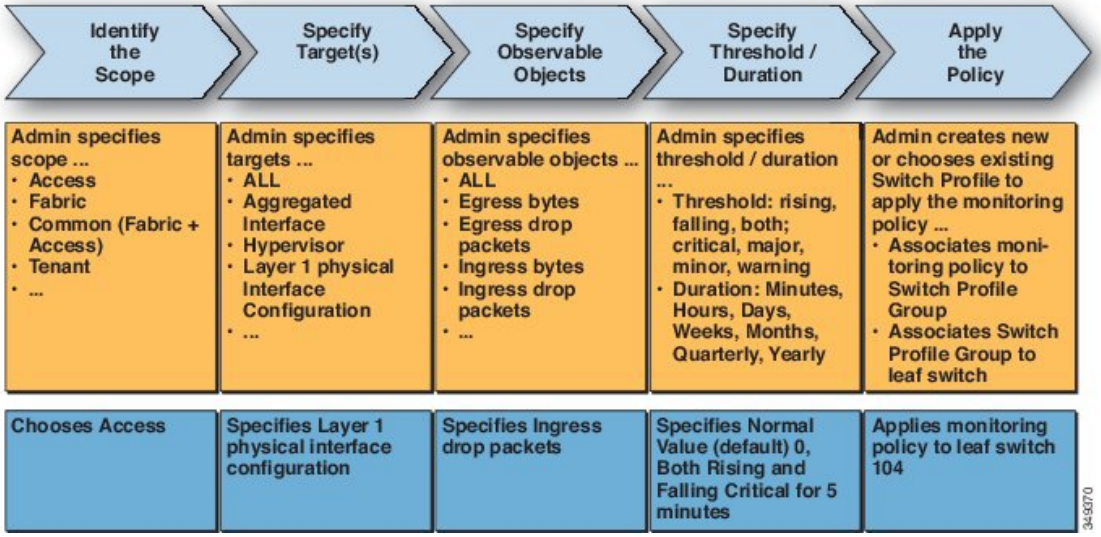
障害/イベント/監査が生成されると、該当するすべての送信元が使用されます。たとえば、次のようなコンフィギュレーションがあるものとします。

- syslog グループ 4 を指す syslog 送信元 4 は、障害 F0123 に対して定義されています。
- ターゲット電源（eqpt:Psu）に対して、syslog グループ 3 を指す syslog 送信元 3 が定義されています。
- syslog グループ 2 を指す syslog 送信元 2 は、範囲インフラ用に定義されています。
- syslog グループ 1 を指す syslog 送信元 1 は、共通の監視ポリシーに定義されています。

範囲インフラ内のクラス eqpt:Psu の MO で障害 F0123 が発生した場合、メッセージのシビラティ（重大度）が各送信元および接続先に定義された最小値以上であると想定して、syslog メッセージが syslog グループ 1 ～ 4 のすべての接続先に送信されます。 この例は syslog 構成を示していますが、callhome および SNMP 構成は同じように動作します。

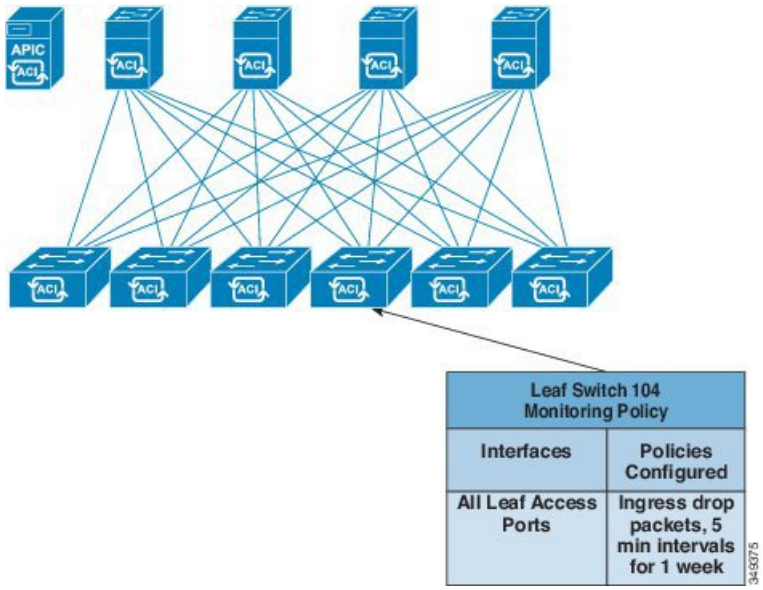
次の図は、統計用のファブリック モニタリング ポリシーを構成するプロセスがどのように動作するかを示します。

図 *5:* アクセス モニタリング ポリシーを構成するワークフロー



Cisco APIC は、次の図に示すように、このモニタリング ポリシーを適用します。

図 *6:* サンプルのアクセス モニタリング ポリシーの結果



モニタリングポリシーは、障害や正常性スコアなどの他のシステム操作に対しても構成できます。この階層へのモニタリング ポリシー マップの構造

ポリシーのモニタリング

- 統計のエクスポート
- 収集ルール
- モニタリング ターゲット

- 統計のエクスポート
- 収集ルール
- 統計情報
  - 収集ルール
  - しきい値ルール
  - 統計のエクスポート

次の図の [統計のエクスポートポリシー（Statistics Export policies）] オプションは、エクスポートする統計のフォーマットと接続先を定義します。出力は、FTP、HTTP、または SCP プロトコルを使用してエクスポートできます。形式は JSON または XML です。ユーザまたは管理者は、出力を圧縮することもできます。エクスポートは、[統計（Statistics）]、[モニタリング ターゲット（Monitoring Targets）] または最上位のモニタリング ポリシー下で定義できます。統計のエクスポートの上位レベルの定義は、定義された下位レベルのポリシーが存在しない限り優先されます。

モニタリング ポリシーは、セレクタまたは関係を使用して、特定の監視可能なオブジェクト（ポート、カード、EPG、テナントなど）または監視可能なオブジェクトのグループに適用されます。モニタリング ポリシーは次を定義します。

- 統計が収集され、履歴に保持されます。
- しきい値超過障害がトリガーされます。
- 統計がエクスポートされます。

収集ルールは、精密に指定されたサンプリング間隔ごとに定義されます。ルールでは、統計の収集をオンまたはオフにする必要があるかどうか、またオンにした場合、履歴保持期間をどうするべきかを構成します。モニタリング ターゲットは、監視可能なオブジェクトに相当します（ポートや EPG など）。収集ルールは、[統計（Statistics）]、[モニタリング ターゲット（Monitoring Targets）] または最上位のモニタリング ポリシー下で定義できます。収集ルールの上位レベルの定義は、定義された下位レベルのポリシーが存在しない限り優先されます。

統計は、統計カウンタのグループに相当します（入力カウンタ、出力カウンタ、またはドロップ カウンタなど）。

しきい値ルールは収集ルール下で定義され、親レベルの収集ルールで定義された、対応するサンプリング間隔に適用されます。

Tetration Analytics

Cisco Tetration Analytics エージェントのインストールについて

Cisco Tetration エージェントのインストールは、RPM Package Manager（RPM）ファイルを Cisco Tetration クラスタからダウンロードし、APIC にアップロードすることによって実行されます。Cisco Tetration クラスタは、Cisco Tetration エージェントの新しいバージョンがアップロードされるたびに、スイッチに通知を送信します。

スイッチへのイメージのインストールに関しては、次の 2 つのシナリオが考えられます。

- Cisco Tetration イメージがスイッチにインストールされていません。スイッチは APIC から通知を受信し、スイッチのコンテナに Cisco Tetration エージェント イメージをダウンロードしてインストールします。
- Cisco Tetration イメージがスイッチにインストールされ、スイッチが APIC から通知を受信します。このスイッチは、APIC バージョンが既にインストールされているエージェント イメージのバージョンよりも高いかどうかを確認します。バージョンが高い場合、スイッチは最新の Cisco Tetration イメージをダウンロードして、スイッチのコンテナにインストールします。

イメージは永続メモリにインストールされます。再起動時に、APIC からコントローラ通知を受信した後、スイッチは APIC で使用可能なイメージに関係なく Cisco Tetration エージェントを開始します。

NetFlow

NetFlow について

NetFlow テクノロジは、ネットワーク トラフィック アカウンティング、従量制のネットワーク課金、ネットワーク プランニング、そしてサービス拒絶に対する監視機能、ネットワーク監視、社外マーケティング、およびサービス プロバイダと企業顧客向け両方のデータ マイニングなど、主要な一連のアプリケーションの計測基盤を効果的にします。Cisco は NetFlow エクスポート データの収集、データ量削減、ポスト プロセッシングを行う一連の NetFlow アプリケーションを提供し、エンド ユーザー アプリケーションが NetFlow データへ簡単にアクセスできるようにします。この機能により、同じレベルを介したトラフィックのモニタリングを実行する、NetFlow がデータ センターを通過するトラフィックのモニタリングを有効にすると、Cisco Application Centric Infrastructure (Cisco ACI) ファブリック。

ハードウェアがレコードからコレクタに直接エクスポートする代わりに、レコードはスーパーバイザ エンジンで処理され、必要な形式で標準の NetFlow コレクタにエクスポートされます。

仮想マシン ネットワークでの NetFlow の構成については、『*Cisco ACI Virtualization Guide*』を参照してください。

NetFlow に関するサポートおよび制限事項

次のリストは、NetFlow で利用可能なサポートとそのサポートの制限に関する情報を提供します。

- EX、FX、FX2 以降のスイッチは NetFlow をサポートしています。特定のリリースでサポートされるスイッチ モデルの完全なリストについては、そのリリースの「*Cisco Nexus 9000 ACI* モード スイッチ リリース ノート」を参照してください。
- Cisco Application Policy Infrastructure Controller（APIC）リリース 4.0(1) 以降では、リモート リーフスイッチの NetFlow はサポート対象です。
- Cisco Application Centric Infrastructure（ACI）は NetFlow の入力のみをサポートし、NetFlow の出力はサポート対象外です。ブリッジドメインでは、NetFlow はスパイン スイッチから入ってくるパケットを確実にキャプチャできません。
- スパイン スイッチは NetFlow をサポートしていないため、スパイン スイッチのパケットからテナント レベルの情報をローカルに取得することはできません。
- ハードウェアは、アクティブ/非アクティブ タイマーをサポートしていません。フロー テーブル レコードはテーブルがフラッシュされると集約され、レコードは毎分エクスポートされます。
- すべてのエクスポート間隔で、ソフトウェア キャッシュがフラッシュされ、フローが長期間有効であっても、次の間隔でエクスポートされるレコードには、リセットされたパケット/バイト カウントおよびその他の統計が含まれます。
- フィルタ TCAM には、ブリッジドメインまたはインターフェイスのラベルがありません。NetFlow モニターを 2 つのブリッジドメインに追加すると、NetFlow モニターは IPv4 の場合は 2 つのルール、IPv6 の場合は 8 つのルールを使用します。そのため、スケールは 1K フィルタ TCAM で制限されます。
- ARP/ND は IP パケットとして処理され、それらのターゲット プロトコル アドレスは、プロトコル範囲として 249 から 255 までのいくつかの特別なプロトコル番号とともに IP フィールドに配置されます。NetFlow コレクタは、この処理を理解していない可能性があります。
- ICMP チェックサムはフロー レコードのレイヤ 4 src ポートの一部であるため、ICMP レコードの場合、他の非 TCP/UDP パケットと同様に、これがマスクされていないと多くのフロー エントリが作成されます。
- Cisco ACI-mode スイッチは、2 つのアクティブなエクスポータのみをサポートします。
- スイッチが CPU 生成パケットの VRF インスタンス間ルーティングを実行できないため、リーフスイッチからの NetFlow トラフィックがコレクタに到達できないことがあります。回避策として、NetFlow コレクタに使用される L3Out と同じ VRF インスタンスですでに構成されている EPG の偽の静的パスを作成します。偽のパスにより、トラフィックはコレクタに到達できます。

- 混合モードで NetFlow エクスポータ ポリシーを構成する場合、特定の VRF インスタンスのサブネットを構成できます。フロー テレメトリは、EPG に関連付けられているすべてのテナントを追跡します。サブネットごとに個別のポリシーを構成する必要はありません。

  たとえば、**t1:ctx2** VRF インスタンスのサブネットとして **0.0.0.0/0** を指定すると、フロー テレメトリは、関連付けられている VRF インスタンスに関係なく、すべての IPv4 フローを追跡します。

- NetFlowエクスポータ エンドポイントがブリッジ ドメインの背後にある場合は、ブリッジ ドメインのユニキャスト ルーティング ノブを有効にして、ブリッジ ドメイン サブネットの URIB ルートをインストールする必要があります。ノブが無効になっている場合、パケットはコレクタに転送されず、コレクタ ポリシーに対して operSt が無効になります。

- NetFlow とフロー テレメトリを同時に有効にすることはできません。

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。