モニタリング

この章の内容は、次のとおりです。

障害、エラー、イベント、監査ログ

（注） 障害、イベント、エラー、およびシステム 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 Error Messages User 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。

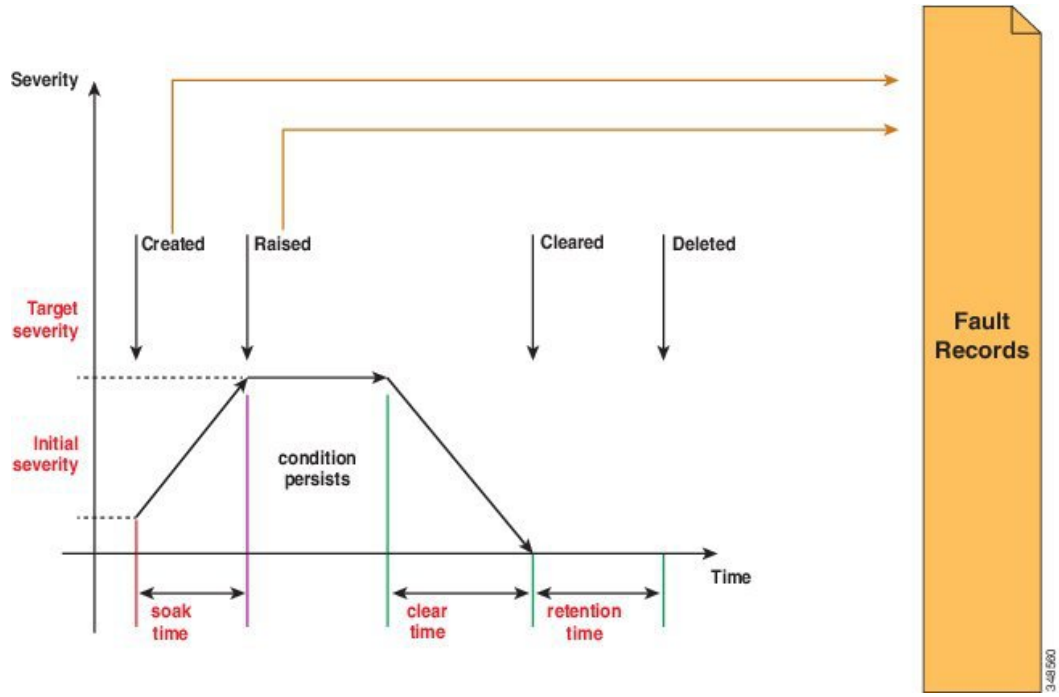
障害

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。

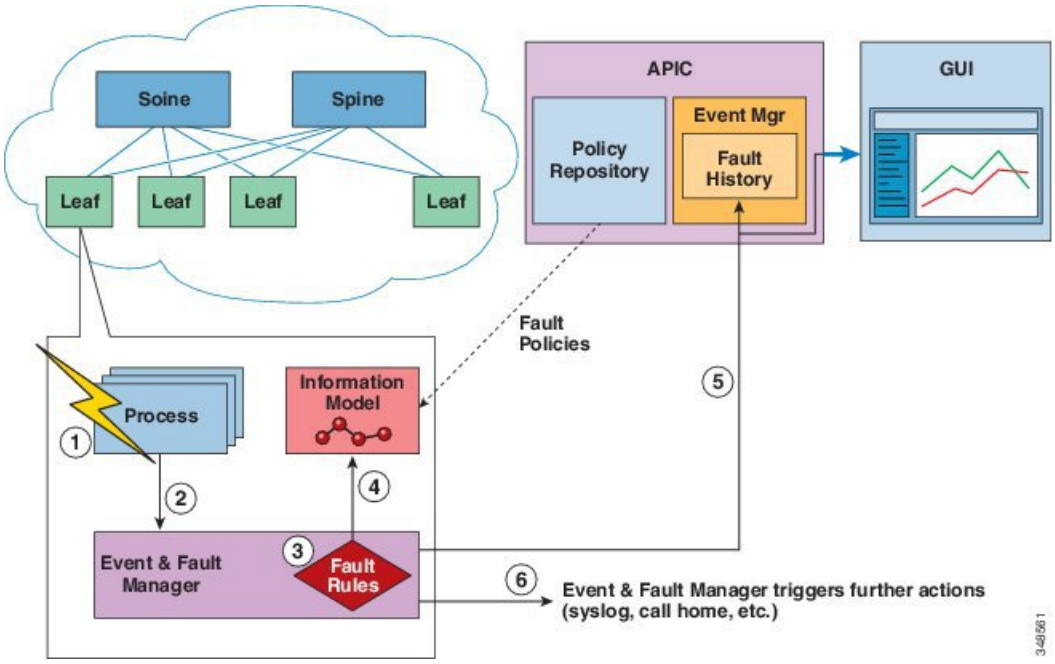
重大度は、サービスを提供するシステムの機能に対するその状態の影響の概算値です。 考えられる値は、Warning、Minor、Major および Critical です。 Warning に相当する重大度の障害は、導入されているサービスには現在影響を与えていない潜在的な問題を示します（たとえば、不完全または矛盾した設定など）。 Minor および Major の障害は、提供されるサービスが低下する可能性があることを示します。 Critical は、大規模な停電がサービスを著しく低下させていたり、同時にサービスが悪化していることを意味します。 説明には、追加情報を提供したりトラブルシューティングに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

イベント

イベント レコードは、ユーザにとって重要な可能性がある特定の状態の発生を記録するためにシステムによって作成されるオブジェクトです。 レコードには、影響を受けるオブジェクトの完全修飾ドメイン名（FQDN）、タイムスタンプおよび状態の説明が含まれます。 例には、リンクの状態遷移、プロトコルの開始と停止、および新しいハードウェア コンポーネントの検出が含まれます。 イベント レコードは、作成後は変更されることはなく、レコード数がイベント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。

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）。

エラー

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。

- 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。
- 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。

監査ログ

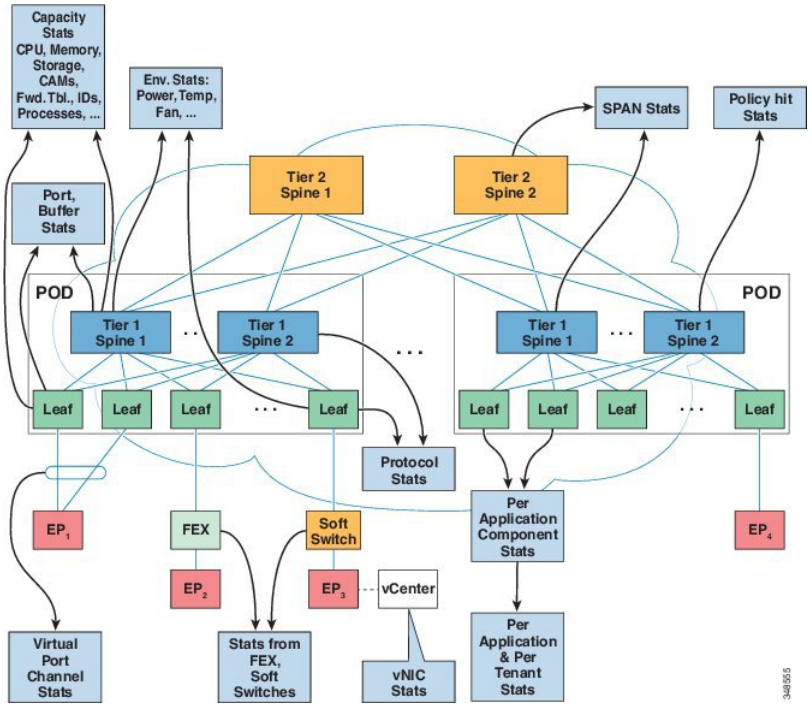
監査レコードは、ログイン/ログアウトや構成の変更などのユーザが開始するアクションを記録するためにシステムにより作成されるオブジェクトです。 レコードには、アクションを実行したユーザの名前、タイムスタンプ、アクションの説明、また該当する場合は影響を受けたオブジェクトのFQDNが含まれます。 監査レコードは、作成後は変更されることはなく、レコード数が監査保持ポリシーで指定された最大値を超えた場合にのみ削除されます。

統計情報プロパティ、階層、しきい値およびモニタリング

統計情報により、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。 統計情報収集は、収集を継続的にまたはオンデマンドベースで行うように設定できます。 統計情報により、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。 統計情報は、累積カウンタとゲージで収集できます。 次の図を参照してください。

ポリシーは、収集する統計情報の種類、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。

図 *3*：統計情報のさまざまな送信元



統計情報データは、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 APIC プロセスなどのさまざまな送信元から収集されます。 統計情報は、5 分、15 分、1 時間、1 日、1 週間、1 か月、4 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。

さまざまな統計情報プロパティを利用でき、[last value]、[cumulative]、[periodic]、[rate of change]、[trend]、[maximum]、[min]、[average] などがあります。 収集/保持時間は設定できます。 ポリシーは、統計情報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 分間の統計情報が追加され、一番最初の 5 分間に収集されたデータが放棄されます。

モニタリング ポリシーの設定

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

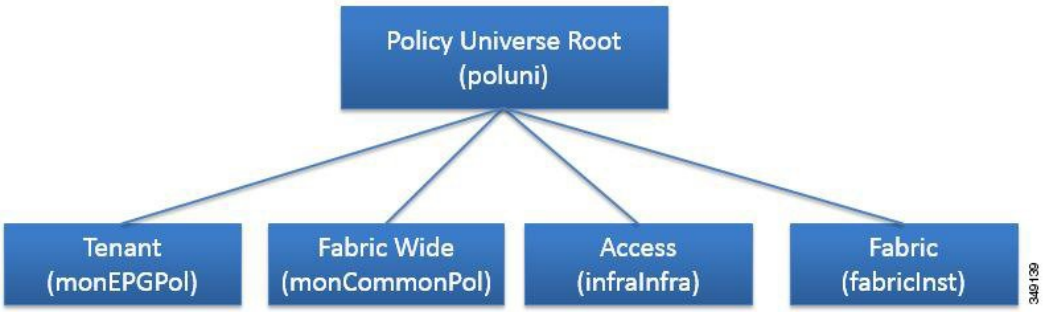
APIC には、デフォルトのモニタリング ポリシーの次の 4 つのクラスが含まれます。

- monCommonPol（uni/fabric/moncommon）：ファブリック インフラストラクチャ階層とアクセス インフラストラクチャ階層の両方に適用されます。
- 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。

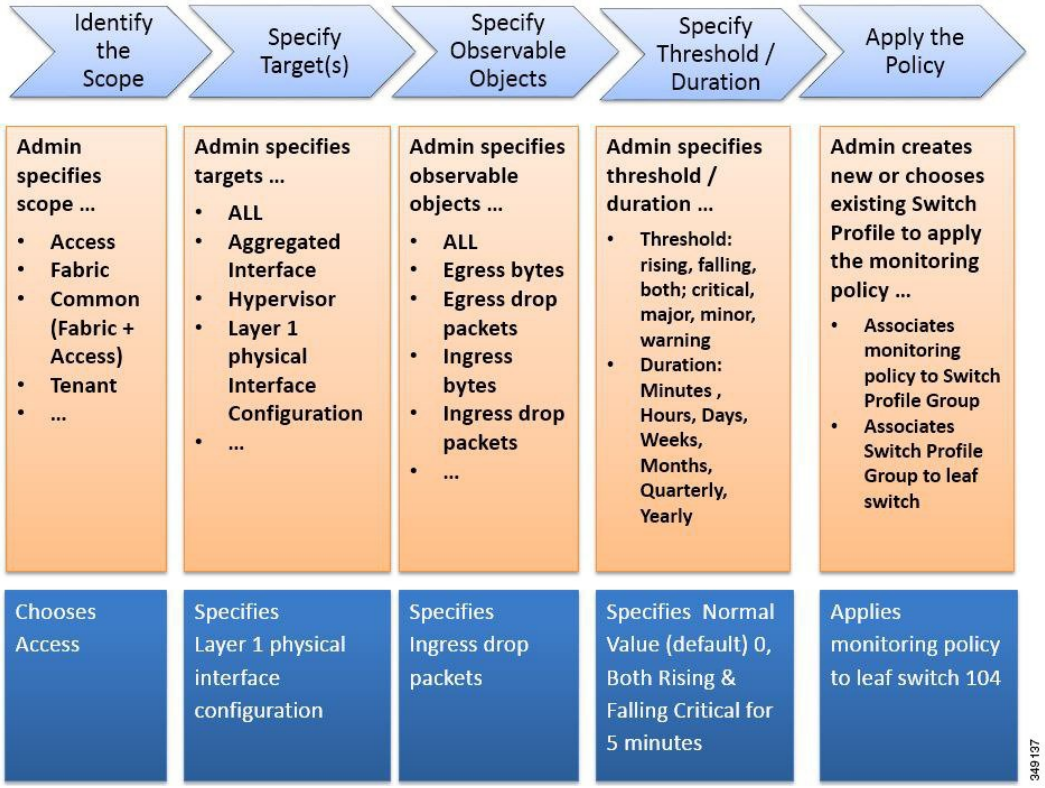
図 *4*: デフォルト モニタリング ポリシーの *4* つのクラス



インフラ モニタリング ポリシーには monInfraTargets が含まれ、ファブリック モニタリング ポリシーには monFabTargets が含まれ、テナント モニタリング ポリシーには monEPGTargets 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。

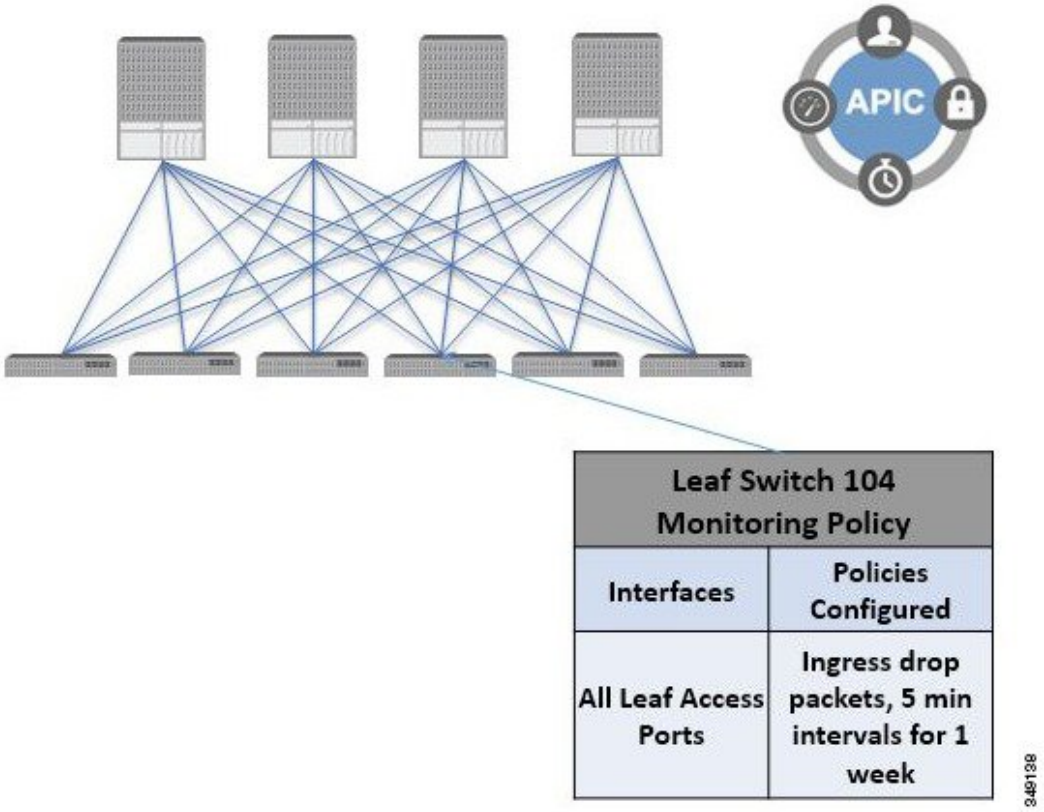
次の図は、統計情報用のファブリック モニタリング ポリシーを設定するプロセスがどのように動作するかを示します。

図 *5* : アクセス モニタリング ポリシーを設定するワークフロー



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、障害やヘルス スコアなどの他のシステム操作に対しても設定できます。 この階層へのモニタリング ポリシー マップの構造

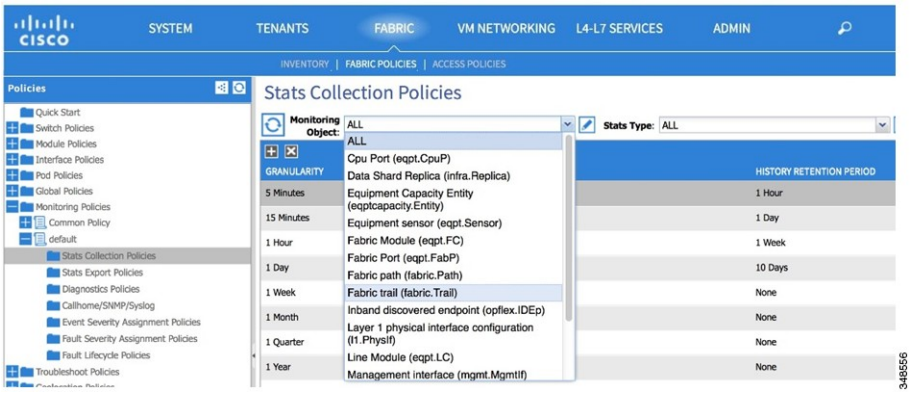
モニタリング ポリシー

- **統計情報のエクスポート**
- **収集ルール**
- **モニタリング ターゲット**
  - **統計情報のエクスポート**
  - **収集ルール**
  - **統計情報**
    - **収集ルール**
    - **しきい値ルール**
    - **統計情報のエクスポート**

次の図の [Statistics Export policies] オプションは、エクスポートする統計情報の形式と宛先を定義します。 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、[Statistics]、[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。 統計情報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。

次の図に示すように、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。

図 *7*: ファブリック統計情報収集ポリシー



モニタリング ポリシーは次を定義します。

- 統計情報が収集され、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。
- 統計情報がエクスポートされます。

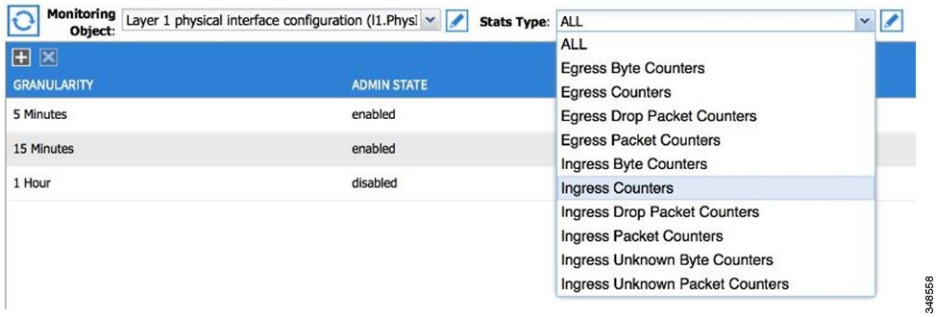
次の図に示すように、収集ルールは、サンプリング間隔ごとに定義されます。

図 *8*：統計情報モニタリング間隔

情報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設定します。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）。

統計情報は、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）。

図 *9*：統計情報タイプ



収集ルールは、[Statistics]、[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。

次の図に示すように、しきい値ルールは収集ルール下で定義され、親収集ルールで定義される対応するサンプリング間隔に適用されます。

図 *10*：統計情報しきい値