アラートの設定

この章では、Secure Workload内でのアラートの設定に焦点を当て、重要なイベントと異常を管理者に通知することで予防的なセキュリティ対策を強化します。Secure Workload内でフォレンジックイベントを構成および監視し、徹底的な調査のためにセキュリティインシデントに関するインサイトを提供する方法について説明します。組織のニーズに基づいてアラートパラメータをカスタマイズすると、通知の関連性と有効性が向上します。

Cisco Secure Workload のアラートは、ワークロードのセキュリティをモニターし、潜在的な脅威に対応するのに役立ちます。アラートのさまざまなコンポーネントが連携して、可視性、アラートの送信元と設定、およびパブリッシャからアラートを送信する機能を提供します。アラートを設定し、アラートトリガールールを表示し、アラートを送信するパブリッシャを選択できます。設定ページに表示されるアラートは、ユーザーのロールによって異なります。アラートのパブリッシャは、アラートまたは Notifier のいずれかです。

注目 最近の GUI の更新により、ユーザーガイドで使用されているイメージやスクリーンショットの一部に、製品の現在の設計が完全に反映されていない可能性があります。最も正確に視覚的に参照するには、このガイドを最新バージョンのソフトウェアと組み合わせて使用することを推奨します。

表 *1:* 機能情報

機能名	リリース	機能説明	どこにあるか
アラートの拡張機能	3.9	**[Investigate]** > **[アラート（Alerts）]** ページ。その他の拡張機能： • [アラート名（Alert Name）] フィールドの導入：新しいフィールド [アラート名（Alert Name）] が導入され、アラート管理への構造化されたアプローチが容易になり、アラートに一意の名前を割り当てられます。 • [アラートタイプ（Alerts Type）] のドロップダウンの導入：新しいドロップダウンである [アラートタイプ（AlertType）] が [アラート - 設定（Alerts – Configs）] ページに導入され、迅速なフィルタリングが容易になりました。 • アイコンの更新：[アラート – 設定（Alerts – Configs）] ページで新しい [+] アイコンを選択して、アラートの設定を開始できるようになりました。	アラート設定モーダル（7 ページ）

機能名	リリース	機能説明	どこにあるか
		アラートのフィルタリングオプションが強化されたマルチサーチ機能。	現在のアラート （18 ページ）

（注） Cisco Secure Workload 3.0 リリース以降、Secure WorkloadApp Store はアラートとコンプライアンス アプリケーションをサポートしていません。アラート アプリケーション インスタンスやコンプライアンス アプリケーション インスタンスを作成せずに、このページでアラートとコンプライアンスアラートを設定できます。

- アラートタイプとパブリッシャ （3 ページ）
- アラートの作成 （5 ページ）
- アラート設定モーダル （7 ページ）
- テストアラートの生成 （16 ページ）
- 現在のアラート （18 ページ）
- アラート詳細 （20 ページ）

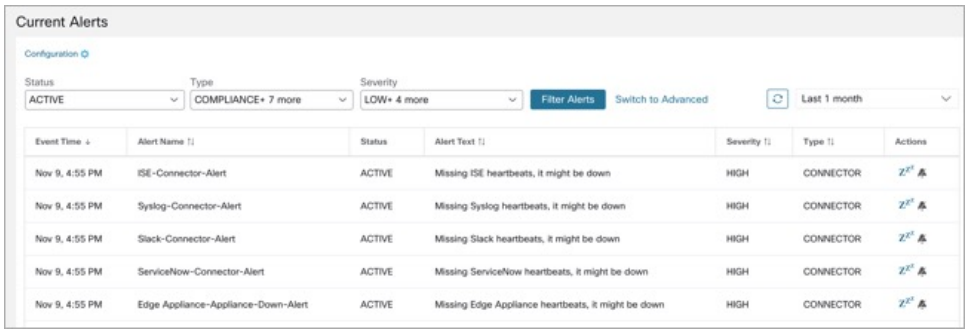
アラートタイプとパブリッシャ

Secure Workload のアラートでは、重大なシステムアラート、ポリシー違反、ワークロードの動作で検出された異常など、アラートがさまざまなタイプに分類されます。各タイプは、セキュリティの整合性を維持するための特定の目的を果たします。アラート基準の定義から通知方法（電子メールや SMS など）を指定するまで、アラートを設定するためのプロセスが定義されています。アラートは、既存の監視ソリューションと統合され、セキュリティの状況に関する包括的なビューを提供します。

Secure Workload のアラートは、次のコンポーネントで構成されています。

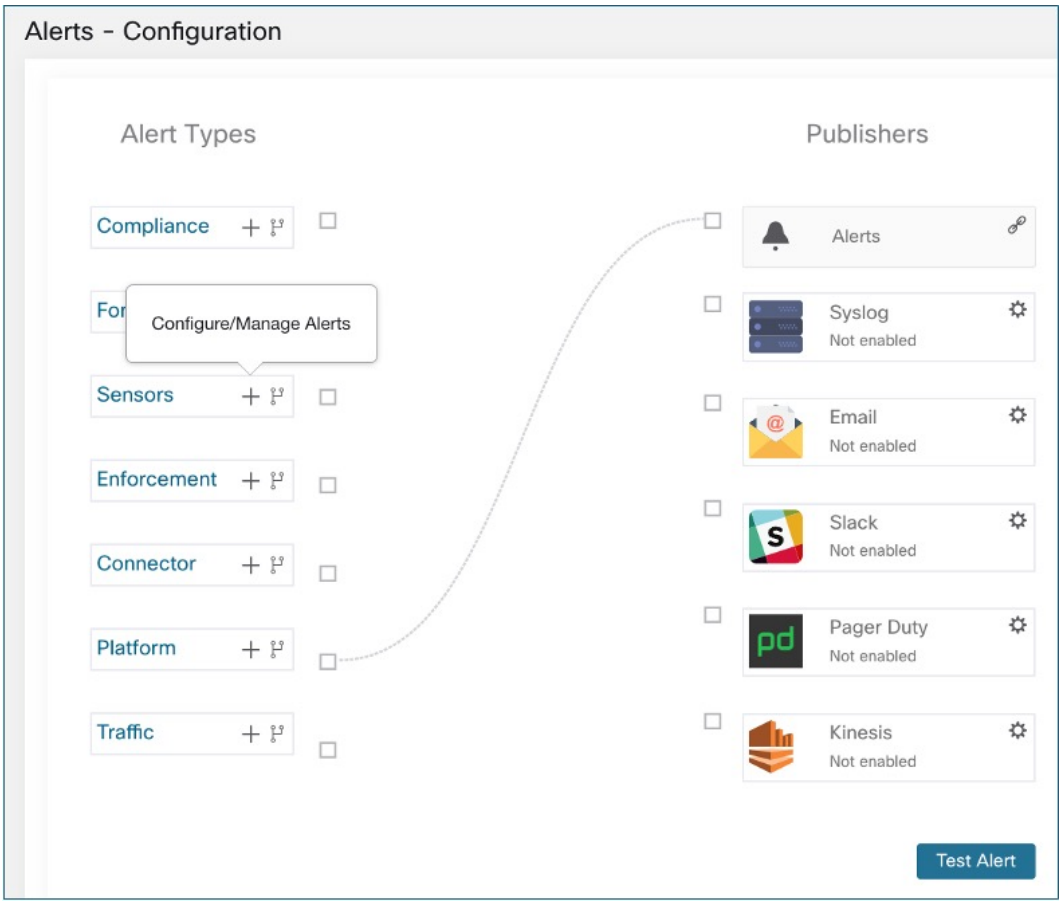
- **アラートの可視性**
  - **現在のアラート**：ナビゲーションウィンドウから、**[Investigate]**>**[アラート（Alerts）]** の順に選択します。アラートのプレビューはデータタップに送信されます。

図 *1* : 現在のアラート



- アラートの送信元と設定：
  - **アラート - 設定**：ナビゲーションウィンドウで、**[管理（Manage）]** > **[ワークロード（Workloads）]** > **[アラート設定（Alert Configs）]** の順に選択します。共通のモーダルとアラートパブリッシャを使用して設定されているアラート設定、および通知者の設定の両方が表示されます。

図 *2* : アラート - 設定

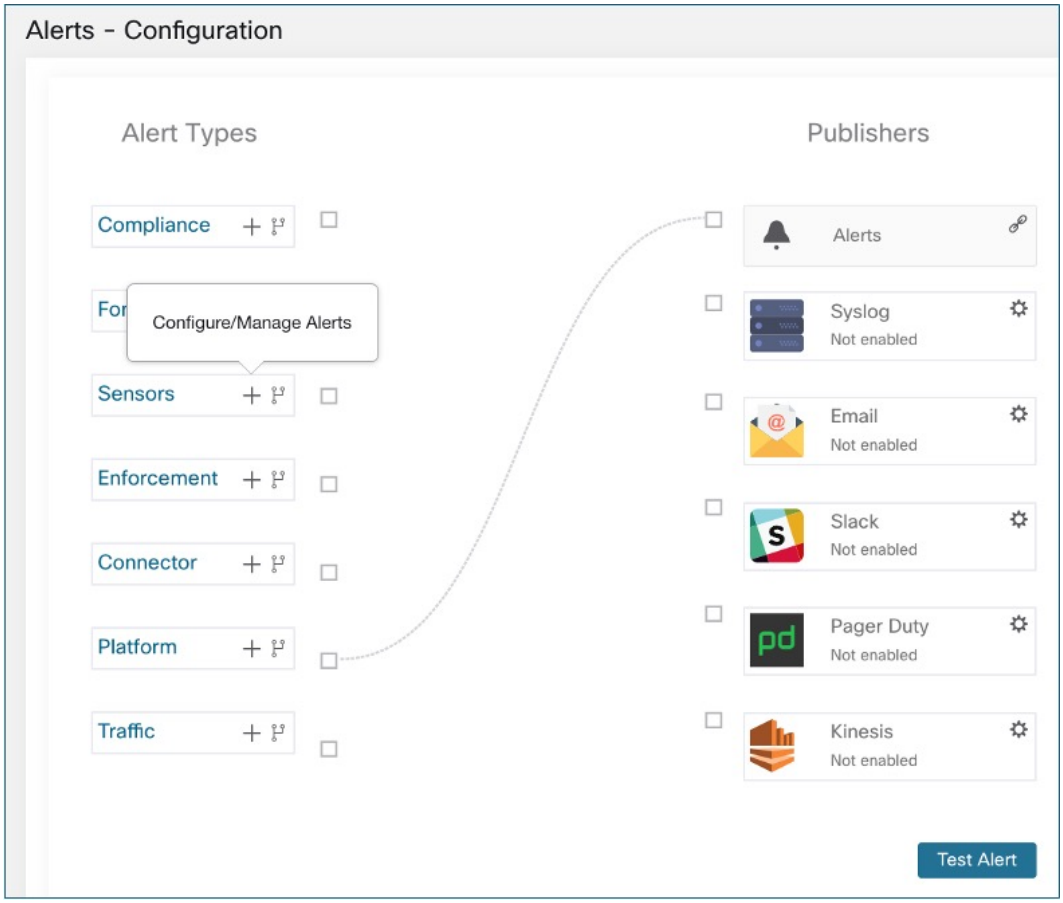


- アラートの送信：
  - **アラートアプリケーション**：生成されたアラートを設定済みのデータタップに送信する暗黙的なSecure Workloadアプリケーション。アラートアプリケーションは、**スヌーズ**や**ミュート**などの機能を処理します。
  - **アラートパブリッシャ**：表示されるアラートの数を制限し、外部で使用できるようにアラートをKafka（MDTまたはデータタップ）にプッシュします。
  - **Edgeアプライアンス**：Slack、PagerDuty、Emailなどの他のシステムにアラートをプッシュします。

アラートの作成

ナビゲーションウィンドウで、**[アラート（Alerts）]** > **[設定（Configuration）]**の順に選択して、次のアラートタイプを設定します。

図 *3:* アラートまたはトリガールールの作成



- 適用アラート

- エージェントの到達可能性
- ワークロード ファイアウォール
- ワークロードポリシー

- **センサーアラート**
  - エージェントのアップグレード
  - エージェントフローのエクスポート
  - エージェントのチェックイン
  - エージェントのメモリ使用率
  - エージェント CPU クォータ
  - フロー観測量
  - 新しいエージェントの登録
  - Pcap ステータス
  - エージェントのアンインストール
  - 推奨されない暗号
  - 廃止された TLS バージョン
  - エージェントの自動削除

- **コンプライアンスアラート**
  - 適用ポリシー
  - ライブ分析ポリシー

（注）
- 適用およびセンサーアラートタイプの場合、アラートトリガールールは、現在選択されているルート範囲に適用されます。
- コンプライアンス アラート タイプの場合、アラートトリガールールを作成するには、現在選択されている範囲で適用機能を使用できる必要があります。

次のアラートタイプには、設定モーダルがありません。

- フォレンジック
- コネクタ
- トラフィック

トラフィックアラート

ワークロードが既知の悪意のある IPv4 アドレスと通信したときに通知される**トラフィック**アラートを作成できます。

デフォルトでは、悪意のあるアドレスを検出するオプションは無効になっています。オプションを有効にするには、「既知の悪意のある IPv4 アドレスの可視性」セクションを参照してください。

使用可能なアラート条件は、次のとおりです。

- **悪意のあるフローが観測された**：既知の悪意のある IPv4 アドレスの通信が観測されました。
- **悪意のあるフローが許可された**：この条件は、ポリシーの分析および適用の後に、許可された悪意のあるフローについて通知します。
- **悪意のあるフローが拒否された**：この条件は、ポリシーの分析および適用の後に、拒否された悪意のあるフローについて通知します。

アラート設定モーダル

アラート設定モーダルは、次のセクションで構成されています。

- [アラート名（Alert Name）]：アラート名を使用すると、アラート管理への構造化されたアプローチが容易になり、アラートに一意の名前を割り当てられます。
- [アラートタイプ（Alert Types）]：[コンプライアンス（Compliance）]、[フォレンジック（Forensics）]、[適用（Enforcement）]、[コネクタ（Connector）]、[プラットフォーム（Platform）]、および [トラフィック（Traffic）] に分類されるさまざまなタイプのアラート。
- [件名（Subject）]：アラートの**件名**はアプリケーションによって異なり、アラートのモーダルがコンテキストの場合は事前に入力されている場合があります。
- [アラート条件（Alert Condition）]：アラートがトリガーされるアラートの条件。**情報**アイコンにカーソルを合わせると、使用可能な条件のリストが表示されます。

（注） 複数のアラートが生成された場合、重大度の高いアラートが、重大度の低いアラートよりも優先的に表示されます。

- その他の設定オプションについては、[詳細設定の表示（Show Advanced Settings）] をクリックしてください。

（注）

- アップグレードが完了すると、現在のテナントにある既存のすべてのアラート設定ルールに、事前定義された形式に基づいて [アラート名（Alert Name）] が割り当てられます。[アラート名（Alert Name）] がない場合、使用される形式は Alert_SubType_{DatabaseID} です。次の例を参考にしてください。

  ```
  Workload_Firewall_64bf9b8493dfc94ca0095718
  ```

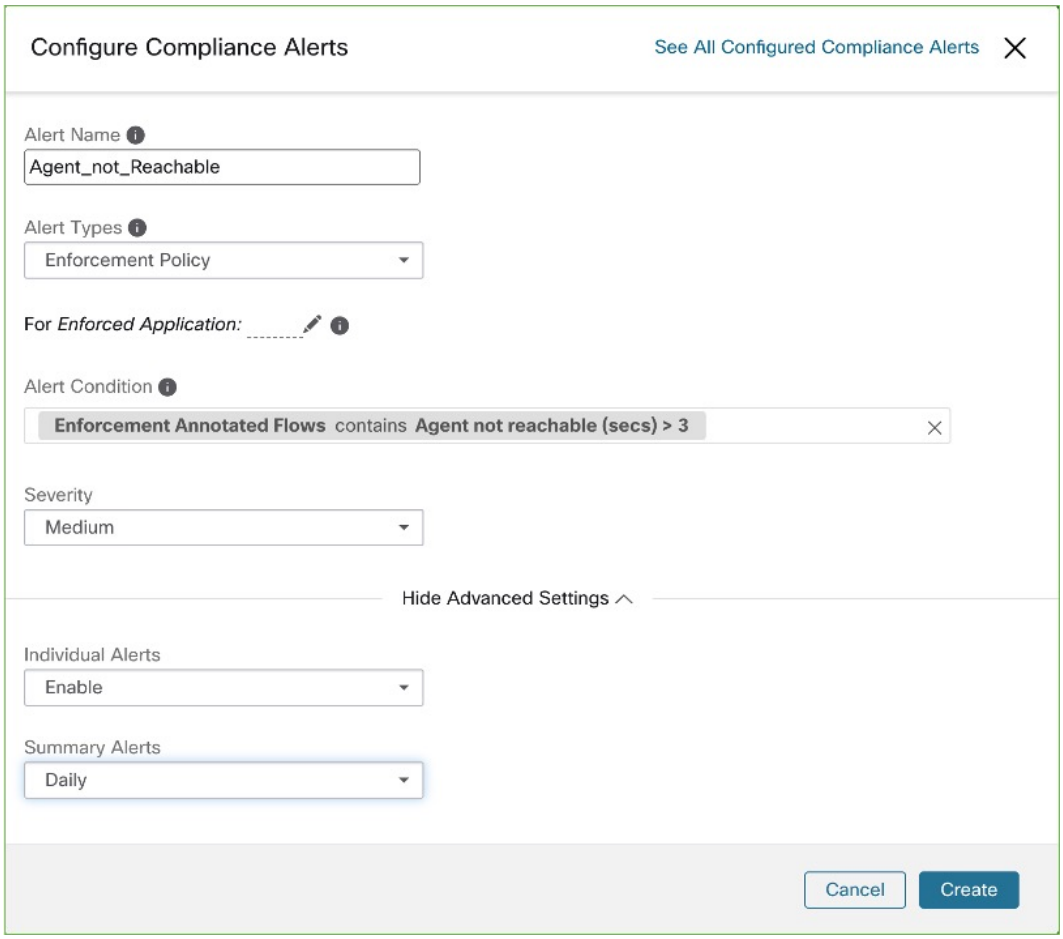
  .

- クラスタの展開またはアップグレードに続いて、すべてのデフォルトのアラート設定ルール（新しいテナントの開始時に作成されたルール）に、事前定義された形式（Alert_SubType）で [アラート名（Alert Name）] が割り当てられます。次の例を参考にしてください。

  ```
  Upgrade_Status
  ```

  .

図 *4:* アラートの設定



サマリーアラート

サマリーアラートは、一部のアプリケーションでのみ使用でき、一部の設定オプションはアプリケーションによって異なります。

- **個別のアラート**は、集約されていない（または最小限に集約された）情報に対して生成され、時間範囲は 1 分間である可能性が高いです。ただし、アラートが必ずしも 1 分間隔で実際に生成され、送信されるわけではありません。個別のアラートは[アプリの頻度（App Frequency）] 間隔でも生成されます。
- **サマリーアラート** は、設定されているアラートルールに基づいて、1 時間または日ごとにすべてのエージェントに対して生成されます。たとえば、センサーアラートと適用アラートはエージェントに対して要約され、コンプライアンスアラートは設定されたアラートルールのすべてのフローで要約されます。

App	アプリの頻度 1	個別のアラート	毎時アラート	毎日のアラート
コンプライアンス	毎分	アプリの頻度で	個別のアラートのサマリー	個別のアラートのサマリー
施行	毎分	アプリの頻度で	個別のアラートのサマリー	個別のアラートのサマリー
Sensor	毎分	アプリの頻度で	個別のアラートのサマリー	個別のアラートのサマリー
トラフィック	毎分	アプリの頻度で	個別のアラートのサマリー	個別のアラートのサマリー

（注） サマリーアラートの**イベント時間**は、過去1時間または指定された間隔における同じタイプのアラートの最初の発生時間を表します。

アラートのスヌーズとミュート

アラートアプリケーションでは、アラートキーで分類されたアラートを、選択した期間スヌーズできます。

（注） 現時点では、ユーザーアプリケーションで作成されたアラートはスヌーズまたはミュートできません。

アラートをスヌーズするには、次の手順を実行します。

1. [アクション（Action）] で、[スヌーズ（Snooze）] アイコンをクリックします。
2. [間隔（Interval）] ドロップダウンリストから適切な間隔を選択します。
3. [スヌーズ（Snooze）] をクリックします。

図 *5:* 現在のアラート

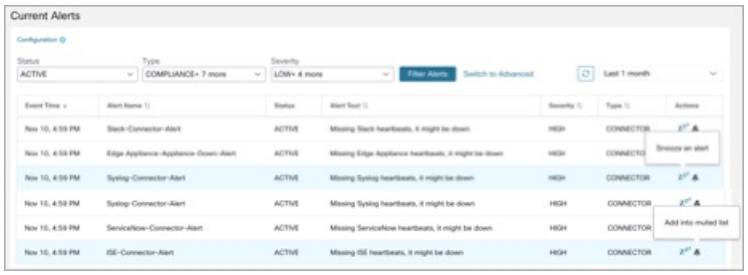
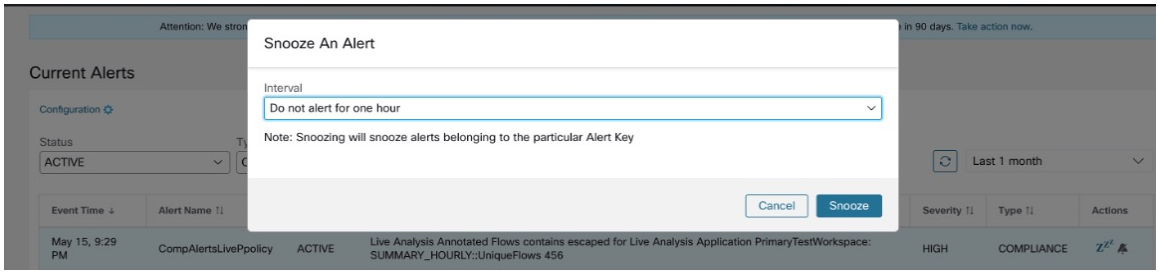


図 *6:* アラートをスヌーズする



アラートをミュートするには、次の手順を実行します。

アラートの受信を停止するには、[ミュート（Mute）] オプションを使用します。

1. [アクション（Action）] で、[ミュート（Mute）] アイコンをクリックします。
2. 確認するには、[はい（Yes）] をクリックします。
3. （オプション）アラートのミュートを解除するには、ミュートリストからアラートを削除します（すべての [ミュート済み（MUTED）] アラートを表示するには、[ステータス（Status）] フィルタ ドロップダウン リストを使用します）。
4. アラートのミュートを解除するには、ミュートリストからアラートを削除します。[ステータス（Status）] フィルタドロップダウンを使用して、すべての [ミュート済み（MUTED）] アラートを表示し、必要な変更をミュート解除します。

（注） 1 つの範囲で最大 5,000 のミュートまたはスヌーズされたアラートを表示できます。

アドミラルアラート

アドミラルは、以前のリリースの Bosun に代わる統合アラートシステムです。詳細については、「アドミラルアラート」を参照してください。

自動要約とスヌーズの対比

アラートの自動要約はアラート設定に基づくすべてのホストに適用され、スヌーズは特定のアラートに適用されます。

両者のいくつかの相違点は、次のとおりです。

- たとえば、コンプライアンス設定は、アプリケーションのワークスペースや、アラート生成の対象にする違反タイプに依存します。したがって、自動要約はアラートルール（たとえば、エスケープ条件）に基づくすべてのホストに適用できますが、スヌーズは非常に特定的なコンシューマ範囲、プロバイダー範囲、プロバイダーポート、プロトコル、およびエスケープ条件に適用できます。

- 特定の間隔で生成されるアラートにより、アラートサマリは指定した頻度で生成されます。サマリーアラートでは、指定された頻度内で生成されたアラートの数が、その範囲に含まれるすべてのエージェントの自動要約とともに示されます。
- スヌーズ間隔が経過した後に新しいアラートが生成される際、アラートのスヌーズで生成されるのは送信するアラートのみです。さらに、ホップカウントが一定数未満の送信元範囲と宛先範囲間のパスで設定されたプラットフォームアラートは、非常に特定的なアラートを生成します。

Cisco Secure Workload Alerts Notifier (TAN)

（注） Cisco Secure Workload リリース 3.3.1.x 以降、TAN は **Cisco Secure Workload Edge アプライアンス**に移行します。

Alert Notifier は、現在選択されている範囲で Amazon Kinesis、電子メール、Syslog、Slack などの各種ツールを介してアラートを送信する機能を備えています。必要なログイン情報や通知アプリケーションに固有のその他の情報を使用して、それぞれの通知者を範囲の所有者やサイト管理者として設定できます。

通知機能の設定

通知機能を設定するには、アラート関連のコネクタを設定する必要があります。このコネクタは、Secure Workload Edge アプライアンスが展開された後にのみ設定できます。Secure Workload Edge アプライアンスの展開の詳細については、「コネクタ用の仮想アプライアンス」を参照してください。

Secure Workload Edge アプライアンスをセットアップしたら、各通知機能に固有の必須入力情報を指定して設定できます。Secure Workload Edge アプライアンスをセットアップしたら、アラートタイプとアラートのパブリッシャを結ぶ破線が表示されます。これは、通知機能がアラートのパブリッシャに基づいているためです。

Secure Workload Edge アプライアンスをセットアップしたら、必要な入力情報を指定して各通知機能を設定できます。Secure Workload Edge アプライアンスをセットアップしたら、アラートタイプとパブリッシャを結ぶ破線が表示されます。これは、通知機能がパブリッシャに基づいているためです。

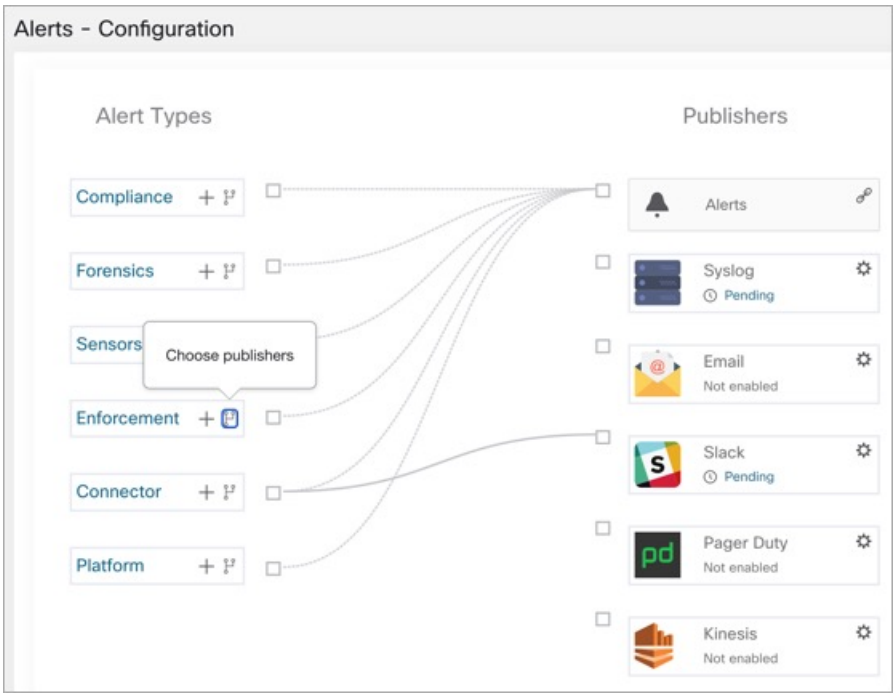
[アプリの頻度（App Frequency）] は、アプリケーションが実行されてアラートが生成されるおおよその頻度です。たとえば、コンプライアンスには柔軟な実行頻度が設定されており、実際には数分間にわたってアラートを計算する場合があります。

アラートのパブリッシャの選択

範囲の所有者と**サイト管理者**は、アラートを**送信**する**パブリッシャ**を選択できます。**パブリッシャ**には、Kafka（データタップ）と**通知ツール**があります。

アラートや**アクティブな通知ツール**を含む選択可能なすべてのパブリッシャが、[アラート - 設定（Alerts - Configuration）] ウィンドウに表示されます。[送信（Send）] アイコンを切り替えて、アラートタイプに [パブリッシャ（Publishers）] を選択できます。[アラートの最低重大度（Minimum Alert Severity）] は重大度レベルを指し、アラートがこのレベルに達すると、**パブリッシャ**経由でアラートが送信されます。

図 7: アラートのパブリッシャの選択



（注） TaaS クラスタにはアラートの最大数があり、1 分間のバッチあたり最大 14000 アラートを処理できます。これは、外部データタップを選択して削減することもできます。

外部 Syslog トンネリングの TAN への移行

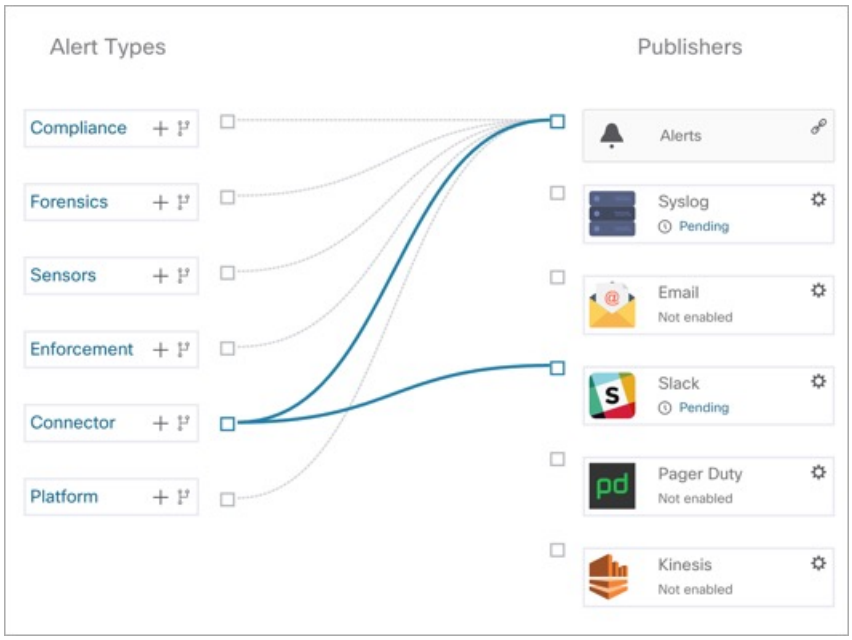
（注） 3.1.1.x リリース以降、syslog トンネリング機能は TAN に移行します。プラットフォームレベルの Syslog イベントを取得するために Syslog を設定するには、デフォルトのルート範囲の Secure Workload Edge アプライアンスで TAN を設定する必要があります。Secure Workload Edge アプライアンスがデフォルトのルート範囲で設定されている場合は、Syslog サーバーをセットアップできます。プラットフォームアラートを有効にするには、プラットフォームの syslog 通知を有効にします。これは、プラットフォーム Syslog 接続を有効にすることで実行できます。

Syslog の設定方法の詳細については、「Syslog コネクタ」を参照してください。

接続チャート

接続図には、**アラートタイプ**と**パブリッシャ**の間の接続が表示されます。任意のアラートタイプのパブリッシャを選択すると、そのアラートタイプとパブリッシャの間に青色の線が確立されます。内部 Kafka（データタップ）を指す線は、アラート通知構築の基盤となる内部メカニズムを表すため、常に破線であることに注意してください。

図 *8*: 接続チャート

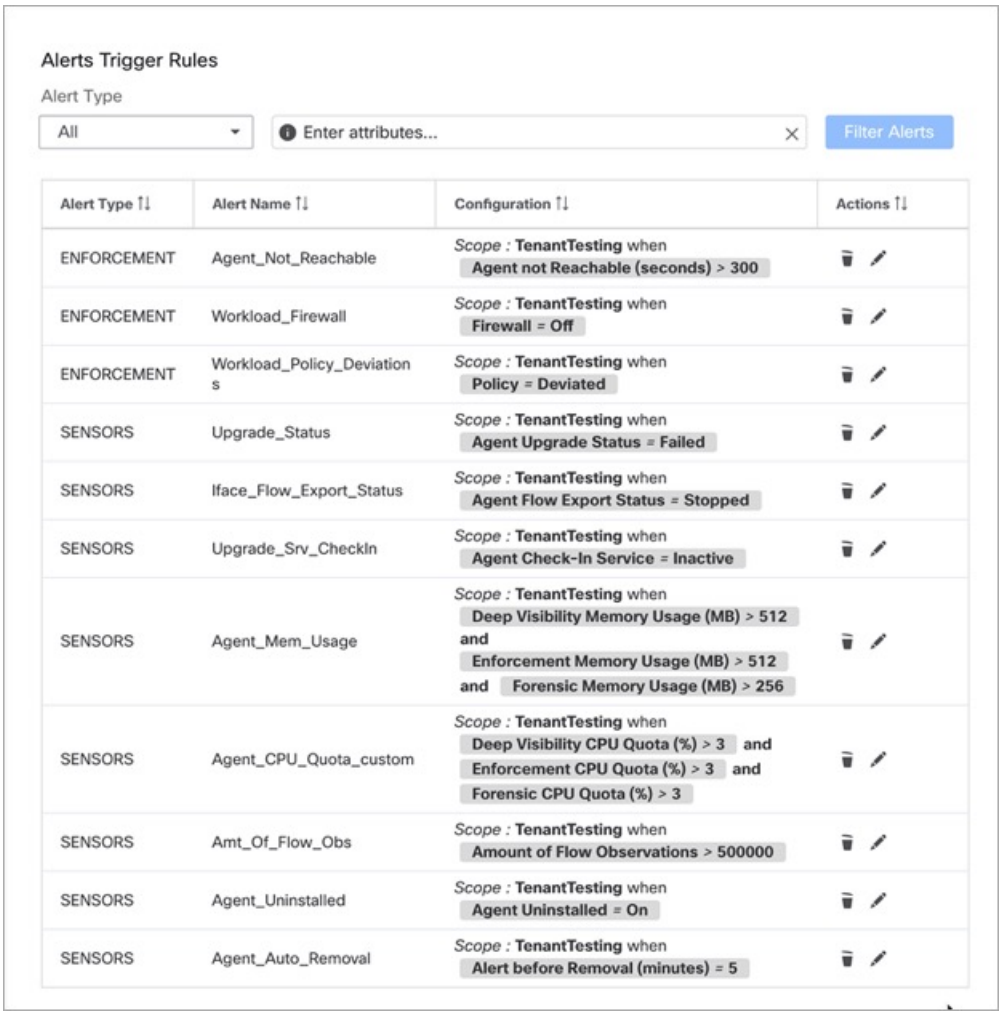


アラートトリガールールの表示

[アラート - 設定（Alerts - Configuration）] ページで、設定済みのすべてのアラートトリガールールのリストを確認できます。また、次のタスクも実行できます。

- ルールは、[アラートタイプ（Alert Type）] やその他のプロパティでフィルタできます。
- [アクション（Actions）] 列で、**鉛筆**アイコンをクリックして、[アラート名（Alert Name）]、[アラートタイプ（Alert TYpe）]、[アラート条件（Alert Condition）]、[重大度（Severity）] などの詳細を変更します。
- 選択した [アラートタイプ（Alert Type）] のすべてのアラートを新しいタブに表示するには、[設定済みの[アラートタイプ]アラートをすべて表示（See All Configured [alert type] Alerts）] をクリックします。

図 *9:* アラートトリガールールの表示



[アラートトリガールール（Alerts Trigger Rules）] ウィンドウを使用して、アラートタイプとトリガー条件でアラートトリガールールをフィルタ処理します。

（注） アラートトリガー条件は完全一致条件です。

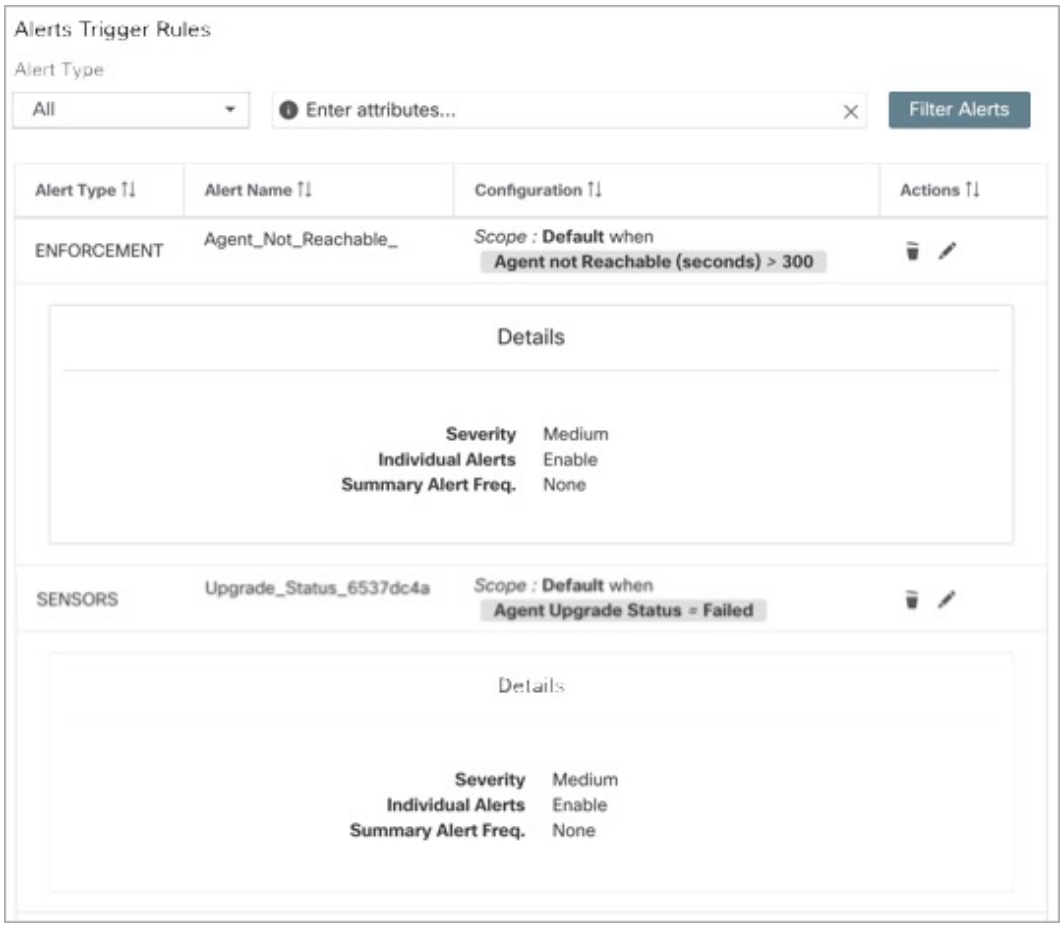
アラートトリガールールの詳細

[アラートトリガールール（Alerts Trigger Rules）] セクションの行をクリックして、設定の詳細を表示します。

1. [アラートタイプ（Alert Type）] : アラートのタイプ。
2. [アラート名（Alert Name）] : アラートの名前。
3. [設定（Configuration）] : アラートが特定の範囲でトリガーされる条件。

[重大度（Severity）]、[個別アラート（Individual Alerts）]、[サマリーアラート頻度（Summary Alert Frequency）] などの詳細も表示できます。

図 *10 :* アラート設定の詳細



テストアラートの生成

テストアラートは、主にパブリッシャとの接続を確認するために生成します。テストアラートを設定して、アラートの設定におけるアラートタイプとリンクされたパブリッシャに基づいてアラートを送信できます。

（注）

- テストアラートの生成は、実際の送信元からは生成されず、テスト目的でのみ生成されます。
- テストアラートは、少なくとも1つのパブリッシャにリンクされているアラートタイプに対して生成できます。

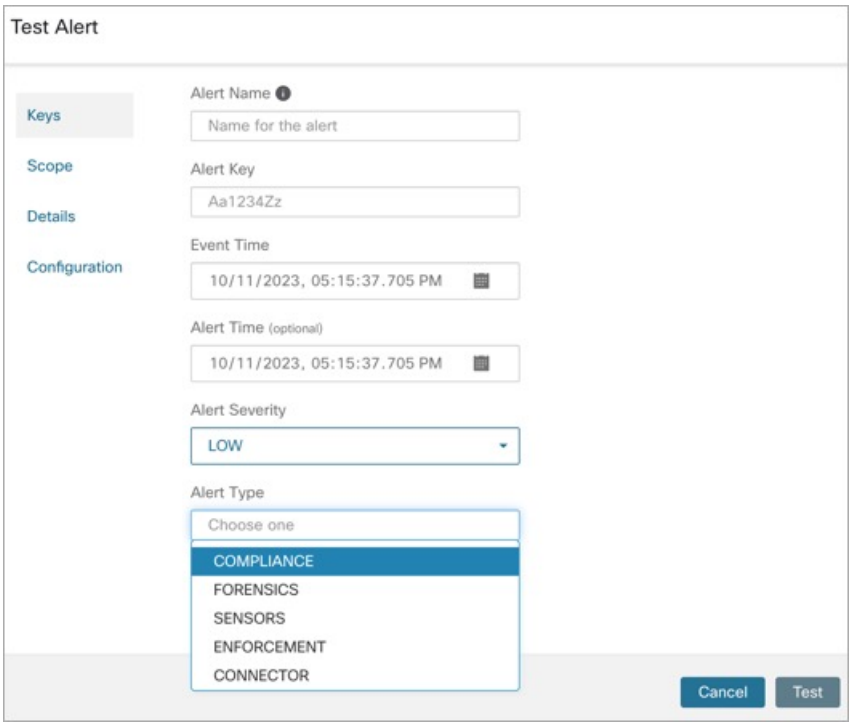
テストアラートを生成するには、次の手順を実行します。

手順

ステップ 1 ナビゲーションウィンドウで、**[管理（Manage）]** > **[ワークロード（Workloads）]** > **[アラート設定（Alerts Config）]** の順に選択します。

ステップ 2 テストアラートを設定するには、[テストアラート（Test Alert）] をクリックします。

図 *11* : テストアラートの設定



ステップ 3 [キー（Keys）] タブで、[アラートキー（Alert Key）] の値を入力し、[イベント時間（Event Time）]、[アラート時間（Alert Time）]、[アラートの重大度（Alert Severity）]、および[アラートタイプ（Alert Type）] の値を選択します。

ステップ 4 現在の範囲に基づいて、[範囲（Scope）] タブの下に、[範囲ID（Scope ID）] と [テナントID（Tenant ID）] の値が自動生成されます。

（注）
[テナントID（Tenant ID）] が [テナントID VRF（Tenant ID VRF）] と同じ場合は、[テナントID VRF（Tenant ID VRF）] チェックボックスが自動的にオンになります。

ステップ 5 [詳細（Details）] タブで、[アラートテキスト（Alert Text）]、[イベントの注釈（Event Notes）]、[アラート詳細（Alert Details）]、および[アラート設定ID（Alert Configuration ID）] の値を入力します。

（注）

[アラート詳細（Alert Details）] には、文字列または JSON 形式のデータを入力できます。

JSON コンテンツのオプションは次のとおりです。

1. そのアラートタイプで想定されているフィールドを含める。
2. そのアラートタイプでデフォルトの JSON フィールドが想定されていない場合は、任意のサンプル JSON データ。

   JSON の例：

   ```
   {"alert_name ":"sample","alert_category":{"severity": "dummy"}}
   ```

ステップ 6 [設定（Configuration）] タブで、[個別アラート（Individual Alert）]、[アラート頻度（Alert Frequency）]、および[サマリーアラート頻度（Summary Alert Frequency）] の値を選択します。

個別アラートについては、ドロップダウンから [有効（ENABLE）] または [無効（DISABLE）] を選択します。

アラート頻度には、[個別（INDIVIDUAL）] が自動的に選択されます。

（注）
個別アラートのみがサポートされ、集約は考慮されません。

サマリーアラートには、[なし（NONE）] が自動的に選択されます。

ステップ 7 テストアラートを生成するために、[テスト（TEST）] をクリックします。

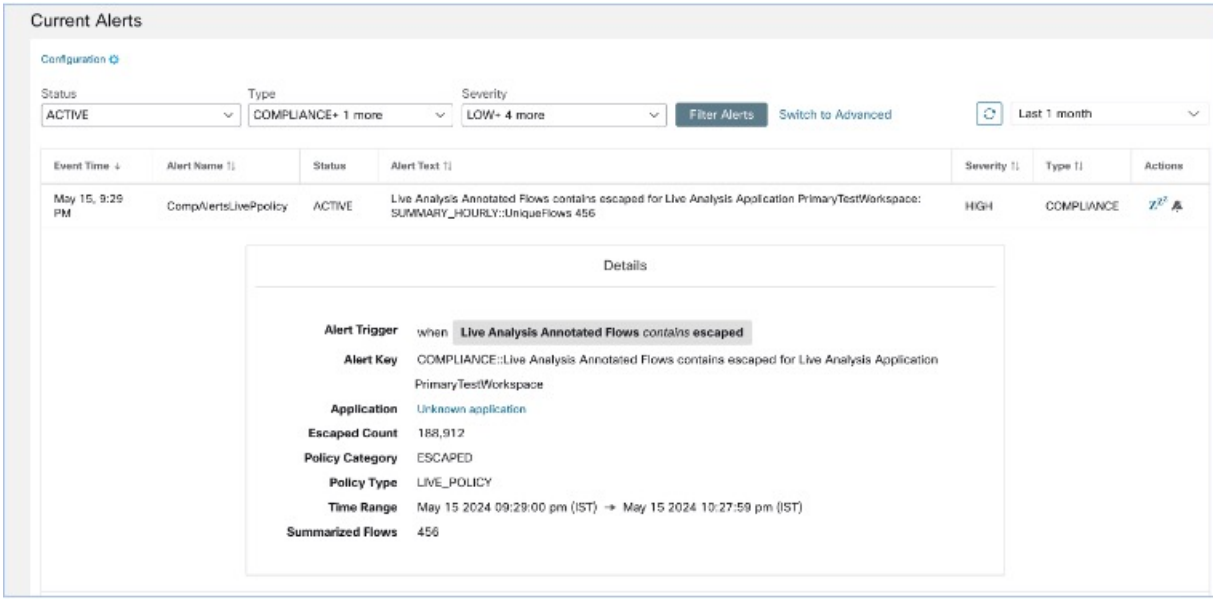
（注）
テストアラートが生成され、設定されたパブリッシャに送信されます。

現在のアラート

[Investigate] > [アラート（Alerts）] ページに移動して、すべてのアクティブアラートのリストを表示します。アラートは、[ステータス（Status）]、[タイプ（Type）]、[重大度（Severity）]、および [時間範囲（Time Range）] でフィルタ処理できます。

[現在のアラート（Current Alerts）] ページには、重大度が IMMEDIATE_ACTION、CRITICAL、HIGH、MEDIUM、または LOW に設定されているアラートのみが表示されます。重大度の値に関係なく、すべてのアラートは設定済みの Kafka Broker に送信されます。

図 *12 :* 現在のアラート



時間範囲によるアラートのフィルタ処理

1. ドロップダウンリストから範囲を選択します。デフォルト値は 1 か月です。
2. [カスタム（Custom）] をクリックし、[開始（From）] と [終了（To）] の日付を入力して、カスタム範囲を設定します。[適用（Apply）] をクリックします。カスタム時間範囲を選択すると、[更新（Refresh）] ボタンが無効になることに注意してください。

高度なフィルタリング

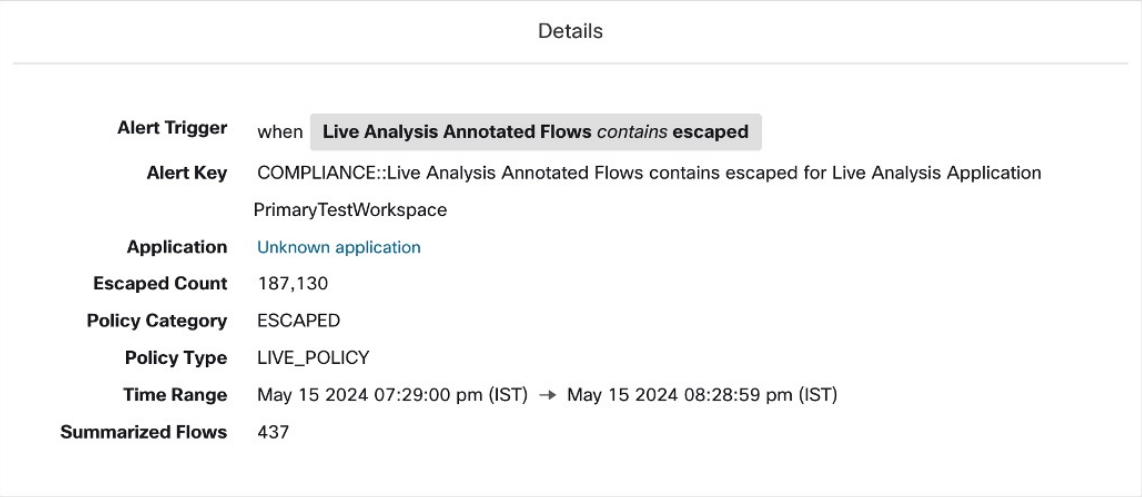
1. [詳細に切り替え（Switch to Advanced）] をクリックします。
2. フィルタ処理する属性を入力します。**情報**アイコンにカーソルを合わせると、フィルタ処理するプロパティが表示されます。

   基本オプションに再度切り替えた場合、アラートフィルタは保持されません。

追加アラートの詳細の表示

対応するアラートをクリックすると、そのアラートの詳細を確認できます。

図 *13 :* アラート詳細



- ルート範囲ごとに 1 分あたり 60 件のアラートのみが表示されます。
- アラートの量が多いと、アラートタイプが [アラートサマリー（Summary Alerts）] になり、表示されないアラートの数が表示されます。
- ある時点で表示されるアラートの数には上限があり、新しいアラートが届くと、古いアラートは削除されます。

  詳細については、「制限」を参照してください。

アラート詳細

一般的なアラート構造

すべてのアラートは、全体的な共通の構造に従います。この構造は、Kafka データタップを通じて使用可能な json メッセージ構造に対応します。

フィールド	フォーマット	バージョン情報
root_scope_id	string	範囲の階層における最上位の範囲に対応する範囲 ID。
key_id	string	「類似の」アラートを決定するために使用される ID フィールド。同一の key_id をスヌーズできます。

フィールド	フォーマット	バージョン情報
type	string	アラートのタイプ。文字列値の固定セット：COMPLIANCE、USERAPP、FORENSICS、ENFORCEMENT、SENSOR、PLATFORM、FEDERATION、CONNECTOR。
event_time	long	イベントがトリガーされたときのタイムスタンプ（またはイベントが範囲にまたがる場合は、範囲の開始点）。このタイムスタンプは、エポックミリ秒単位（UTC）です。
alert_time	long	アラートの送信が最初に試行されたときのタイムスタンプ。イベントの時間範囲の後になります。このタイムスタンプは、エポックミリ秒単位（UTC）です。
alert_text	string	アラートのタイトル。
alert_text_with_names	string	alert_text と同じ内容ですが、ID フィールドが対応する名前に置き換えられています。このフィールドは、すべてのアラートに存在するとは限りません。
severity	string	文字列値の固定セット：LOW、MEDIUM、HIGH、CRITICAL、IMMEDIATE_ACTION。このセットはアラートのシビラティ（重大度）です。一部のタイプのアラートでは、これらの値は設定可能です。
alert_notes	string	通常は設定しません。Kafka データタップを介して追加情報を渡すための特別なケースで存在する場合があります。

フィールド	フォーマット	バージョン情報
alert_conf_id	string	このアラートをトリガーしたアラート設定の ID。すべてのアラートに存在するとは限りません。
alert_details	string	構造化データ。文字列化されたJSON。このフィールドの正確な構造はアラートのタイプによって異なるため、特定のアラート タイプについては機能の詳細を参照してください。
alert_details_json	json	alert_details と同じ内容ですが、文字列化されていません。コンプライアンスアラートにのみ存在し、Kafka を介してのみ使用できます。
tenant_Id	string	root_scope_id に対応する vrf を含む場合があります。または、デフォルト値として 0 が含まれている場合があります。まったく存在しない場合もあります。
alert_id	string	内部で生成された一時的な ID。無視して構いません。
alert_name	string	アラートの名前。

- コンプライアンス：lab-compliance-alert-details
- フォレンジック：外部との統合およびフォレンジック イベント フィールド
- センサーアラートの詳細
- 適用アラートの詳細
- コネクタ：アラートの詳細
- フェデレーション：federation-alert-details
- プラットフォーム：アラートの詳細

通知機能別の全般アラート形式

以下に、さまざまな通知タイプでアラートがどのように表示されるかの例を示します。

（注） Cisco Secure Workload 3.9 以降、通知ツールの詳細に**アラート名**が含まれます。

Kafka（DataTap）

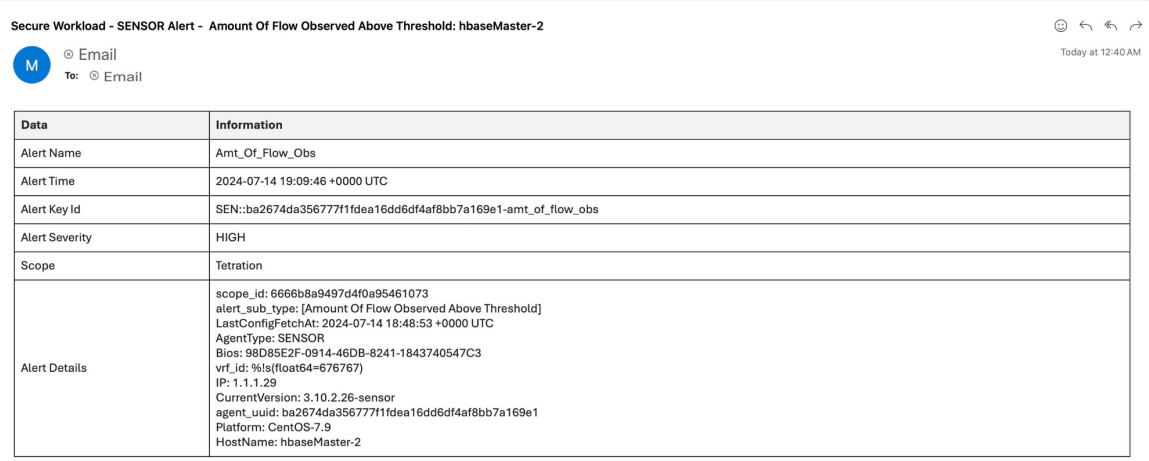
Kafka（DataTap）メッセージは JSON 形式です。以下に例を示します。その他の例については、前述の alert_details を参照してください。


```
{
"_id" : ObjectId("66969d9b89f8901091b54f29"),
"key_id" : "SEN::6c12d5738f083632ad99acb1ba7a6dc4968938be-amt_of_flow_obs",
"event_time" : NumberLong("1721146728000"),
"alert_time" : NumberLong("1721146779640"),
"alert_text" : "Amount Of Flow Observed Above Threshold: collectorDatamover-2",
"alert_text_with_names" : "Amount Of Flow Observed Above Threshold: collectorDatamover-2",
"severity" : "HIGH",
"tenant_id" : "676767",
"root_scope_id" : "6666b8a9497d4f0a95461073",
"type" : "SENSOR",
"alert_details" : "{\"details\":{\"AgentType\":\"SENSOR\",\"Bios\":\"819FAC8D-39DE-
4C56-8CF4-7EEE25CF3510\",\"CurrentVersion\":\"3.10.2.26-
sensor\",\"DesiredVersion\":\"3.10.2.26-sensor\",\"HostName\":\"collectorDatamover-
2\",\"IP\":\"1.1.1.36\",\"LastConfigFetchAt\":\"2024-07-16 15:49:50 +0000
 UTC\",\"Platform\":\"CentOS-
7.9\"},\"agent_uuid\":\"6c12d5738f083632ad99acb1ba7a6dc4968938be\",\"scope_na
me\":\"Tetration\",\"scope_id\":\"6666b8a9497d4f0a95461073\",\"vrf_id\":676767,\"h
ost_name\":{\"collectorDatamover-
2\":\"6c12d5738f083632ad99acb1ba7a6dc4968938be\"},\"alert_sub_type\":[\"Amount
Of Flow Observed Above Threshold\"]}",
"alert_name" : "Amt_Of_Flow_Obs"
}
```


E メール

E メールアラートの設定に関する情報：E メールコネクタ

図 *14 : Secure Workload* センサーアラートの例



Secure Workload - SENSOR Alert - Amount Of Flow Observed Above Threshold: hbaseMaster-2

Email
To: Email

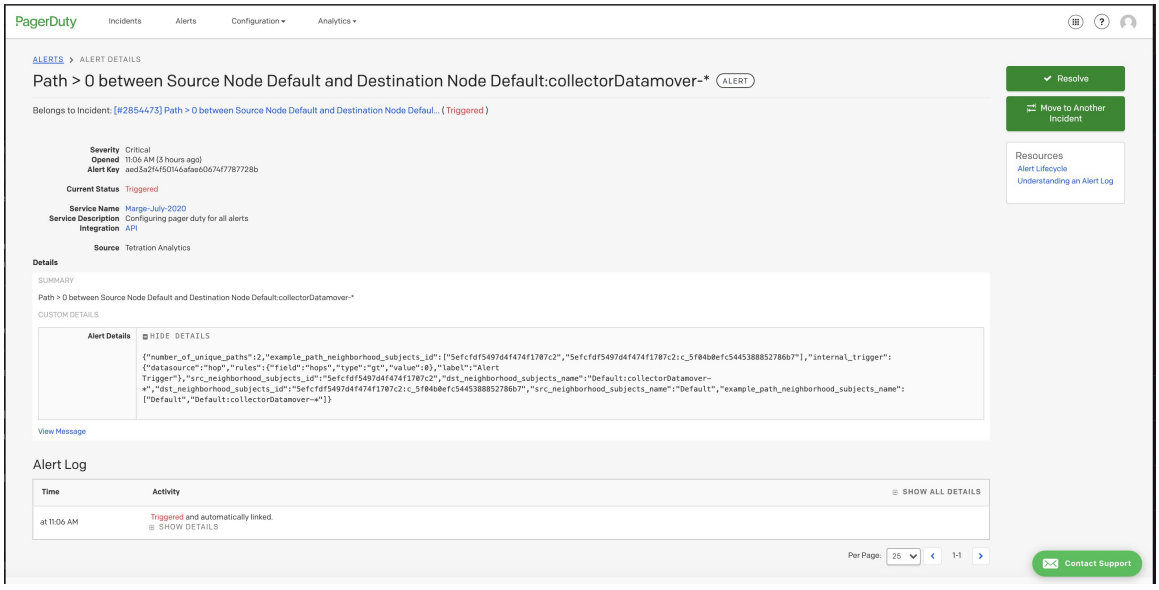
Today at 12:40 AM

Data	Information
Alert Name	Amt_Of_Flow_Obs
Alert Time	2024-07-14 19:09:46 +0000 UTC
Alert Key Id	SEN::ba2674da356777f1fdea16dd6df4af8bb7a169e1-amt_of_flow_obs
Alert Severity	HIGH
Scope	Tetration
Alert Details	scope_id: 6666b8a9497d4f0a95461073 alert_sub_type: [Amount Of Flow Observed Above Threshold] LastConfigFetchAt: 2024-07-14 18:48:53 +0000 UTC AgentType: SENSOR Bios: 98D85E2F-0914-46DB-8241-1843740547C3 vrf_id: %!s(float64=676767) IP: 1.1.1.29 CurrentVersion: 3.10.2.26-sensor agent_uuid: ba2674da356777f1fdea16dd6df4af8bb7a169e1 Platform: CentOS-7.9 HostName: hbaseMaster-2

PagerDuty

PagerDuty アラートの設定に関する情報：PagerDuty コネクタ

図 *15 : PagerDuty* における *Secure Workload* アラートの例



PagerDuty に送信されたアラートは、key_id に基づき再度トリガーされた同じアラートです。

シビラリティ（重大度）は、次のように PagerDuty のシビラリティ（重大度）にマッピングされます。

Cisco Secure Workload のシビラリティ（重大度）	PagerDuty のシビラティ（重大度）
IMMEDIATE_ACTION	critical

Cisco Secure Workload のシビラリティ（重大度）	PagerDuty のシビラティ（重大度）
CRITICAL	critical
HIGH	error
MEDIUM	warning
LOW	info

Syslog

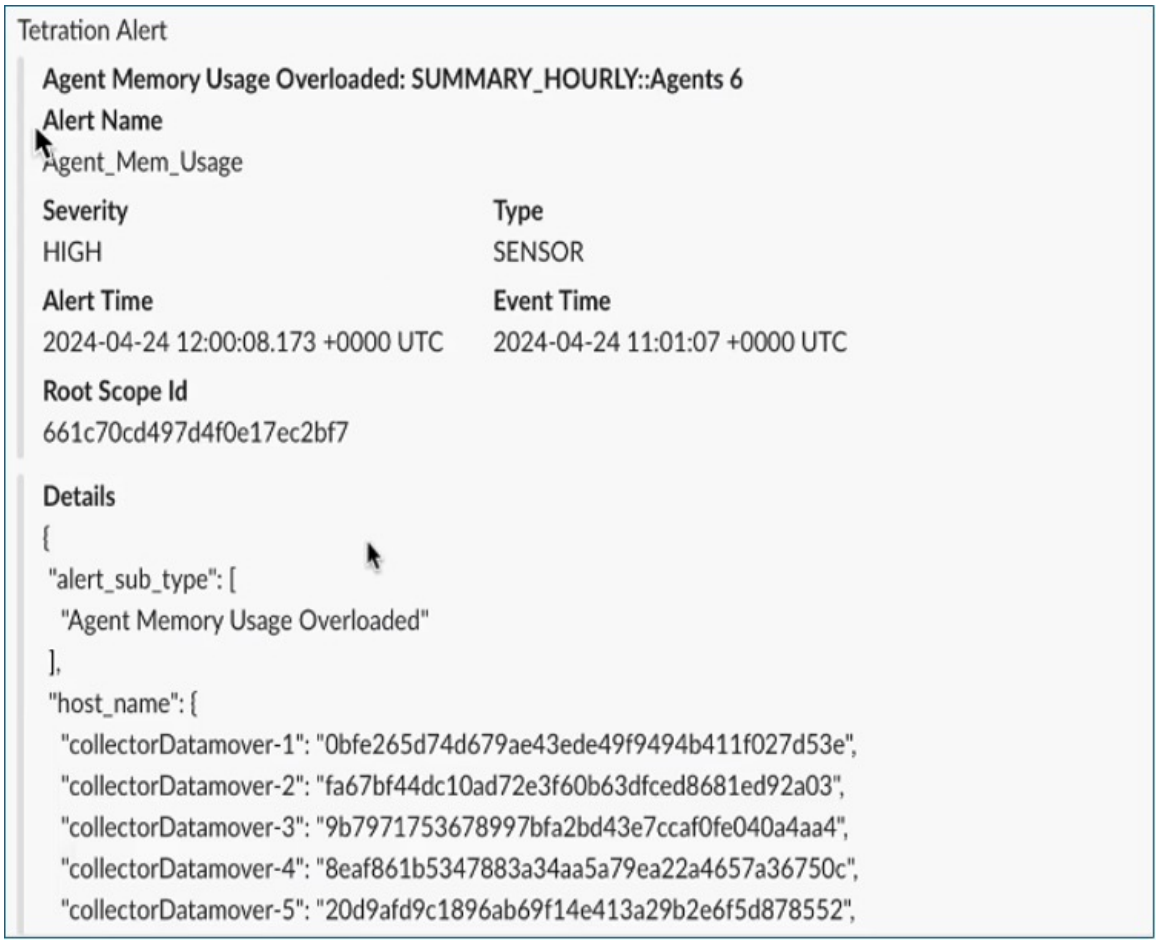
Syslogアラートの設定およびシビラリティ（重大度）のマッピングの調整については、「Syslog コネクタ」を参照してください。次に例を示します。

```
key_id : SEN::e1d41892afdd9a14d3355c30456ac7f835ab5bb6-upgrade_srv_check_in ;
event_time : 1757432813000 ;
alert_time : 1757432824809 ;
alert_text : Agent Inactive: chirmanj-red-hat03 ;
severity : MEDIUM ;
type : SENSOR ;
alert_details :
    {
        "details": {
        "AgentType": "ENFORCER",
        "Bios": "42C63242-56B6-9F8C-5E4C-7B03FFB72CA9",
        "CurrentVersion": "3.11.1.2.250831.22.6.mrpm.build.main.dev-enforcer",
        "DesiredVersion": "",
        "HostName": "chirmanj-red-hat03",
        "IP": "172.29.202.237",
        "LastConfigFetchAt": "2025-09-05 04:08:26 +0000 UTC",
        "Platform": "AlmaLinux-8.8"
        },
        "agent_uuid": "e1d41892afdd9a14d3355c30456ac7f835ab5bb6",
        "scope_name": "Default",
        "scope_id": "68b71e7416d0c2a1e73818d0",
        "vrf_id": 1,
        "host_name": {
            "chirmanj-red-hat03": "e1d41892afdd9a14d3355c30456ac7f835ab5bb6"
            },
        "alert_sub_type": [
            "Agent Inactive"
        ]
    } ;
individual_alert : ENABLE ;
summary_alert_freq : NONE ;
alert_grain : INDIVIDUAL ;
root_scope_id : 68b71e7416d0c2a1e73818d0 ;
alert_name : Upgrade_Srv_CheckIn ;
```

Slack

Slack アラートの構成に関する情報：Slack コネクタ

図 *16 : Slack* チャネルに送信される *Secure Workload* アラートの例



Kinesis

Kinesis アラートの構成に関する情報：Kinesis コネクタ

Kinesis アラートは、Kafka アラートに似ています。どちらもメッセージキューであるためです。

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。

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。

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。

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。

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。

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。