



アラート

図 1: アラートタイプとパブリッシャの設定

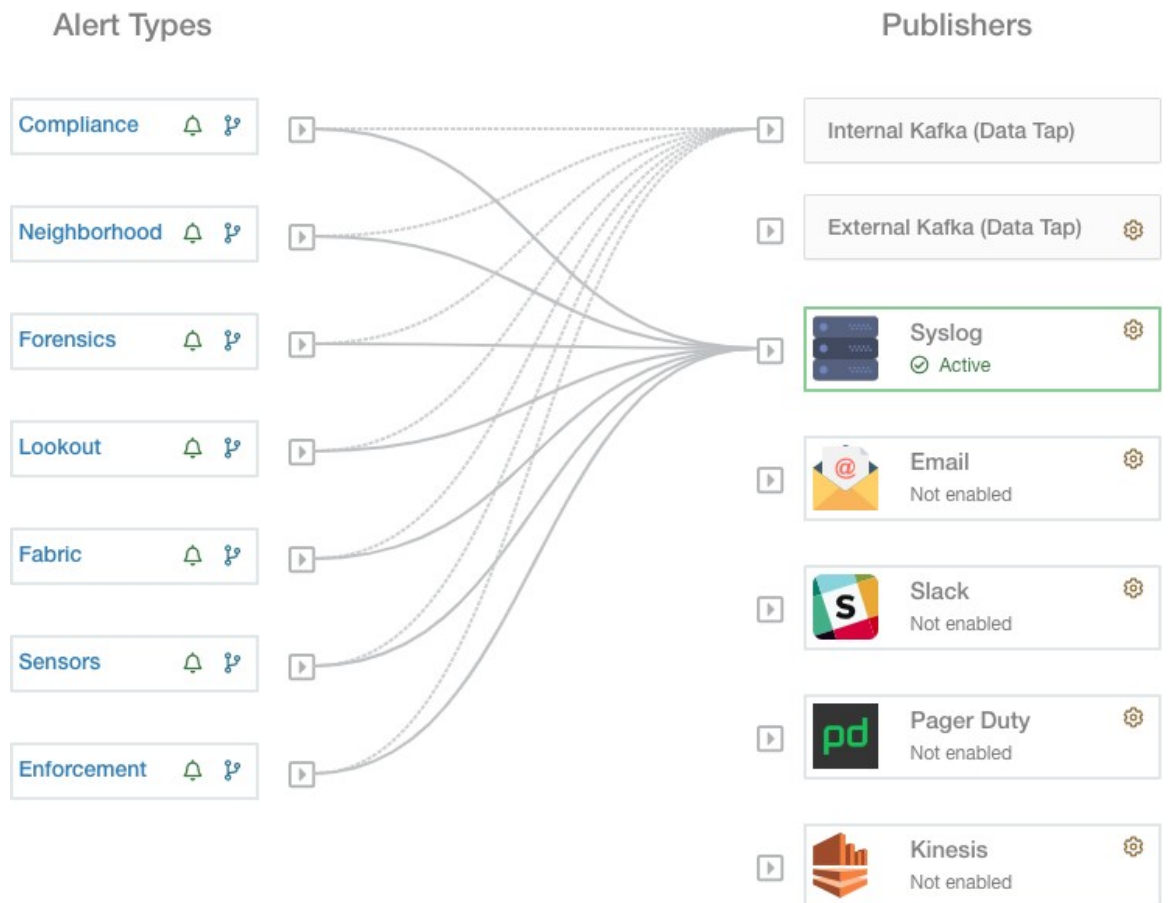


図 2: アラートタイプとパブリッシャの設定

The screenshot shows the 'Alerts - Configuration' page. On the left, 'Alert Types' lists seven categories: Compliance, Forensics, Sensors, Enforcement, Federation, Connector, and Platform. In the middle, 'Publishers' lists six options: Alerts, Syslog, Email, Slack, Pager Duty, and Kinesis, each with a 'Not enabled' status. On the right, 'Alerts Trigger Rules' displays a table of configurations. The table has columns for 'alert type', 'Configuration', and 'actions'. The configurations include rules for ENFORCEMENT (Agent not reachable, Firewall - Off, Policy - Deviated) and SENSORS (Agent Upgrade Status, Agent Flow Export Status, Agent Check-In Service, memory usage, and CPU Quota).

alert type	Configuration	actions
ENFORCEMENT	Scope: Default when Agent not reachable (seconds) > 300	
ENFORCEMENT	Scope: Default when Firewall - Off	
ENFORCEMENT	Scope: Default when Policy - Deviated	
SENSORS	Scope: Default when Agent Upgrade Status = Failed	
SENSORS	Scope: Default when Agent Flow Export Status = Stopped	
SENSORS	Scope: Default when Agent Check-In Service = Inactive	
SENSORS	Scope: Default when Deep visibility memory usage (MB) > 512 and Enforcement memory usage (MB) > 512 and Forensic memory usage (MB) > 256	
SENSORS	Scope: Default when Deep visibility CPU Quota (%) > 3 and Enforcement CPU Quota (%) > 3 and Forensic CPU Quota (%) > 3	
SENSORS	Scope: Default when Amount of flow observations > 500000	
SENSORS	Scope: Default when Agent Uninstalled = On	
SENSORS	Scope: Default when Alert before removal (minutes) = 5	

Cisco Secure Workload 内のアラートは、多くの統合コンポーネントで構成されています。コンポーネントは、大まかに次のように分類できます。

Visibility:

- [アラート (Alerts)] ページ : [Investigate] > [アラート (Alerts)] にあります。このページは、DataTap に送信されたアラートのプレビューで構成されます。

アラートの送信元と設定 :

- [アラート設定 (Alert Configuration)] : アプリケーション/コンポーネントによって判断されますが、多くの場合、DataTap の構成やサマリーアラートオプションなどの機能を備えた共通のインターフェイス (「アラート設定モジュール」と呼ばれる) が使用されます。
- [アラート設定 (Alerts Configuration)] ページ : [管理 (Manage)] > [アラート設定 (Alerts Config)] にあります。このページには、共通のモジュールを使用して構成されたアラート設定と、アラートパブリッシャおよび通知者の設定の両方が表示されます。

アラートの送信先 :

- 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 DataTap 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、実質的に送信するアラートを判断します。
- アラートパブリッシャ : UI に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 DataTap) 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。
- [アラートの設定 \(3 ページ\)](#)
- [現在のアラート \(20 ページ\)](#)
- [アラート詳細 \(25 ページ\)](#)

アラートの設定

[アラート設定 (Alerts Configuration)] ページでは、アラートトリガールールを設定し、アラートを送信するパブリッシャを選択できます。このページに表示されるアラートタイプは、ユーザーロールによって異なります。アラートのパブリッシャは、Kafka (データタップ) または Notifier のいずれかです。

[アラート設定 (Alerts Configuration)] ページでは、アラートトリガールールを設定し、アラートを送信するパブリッシャを選択できます。このページに表示されるアラートタイプは、ユーザー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) アラートとコンプライアンス アプリケーションは、リリース 3.0 以降、Secure Workload App Store から削除されます。アラートアプリインスタンスやコンプライアンス アプリ インスタンスを作成しなくても、このページでコンプライアンスアラートをはじめとするアラートを設定できます。
-

アラートの作成

図 3: アラート（トリガールール）の作成

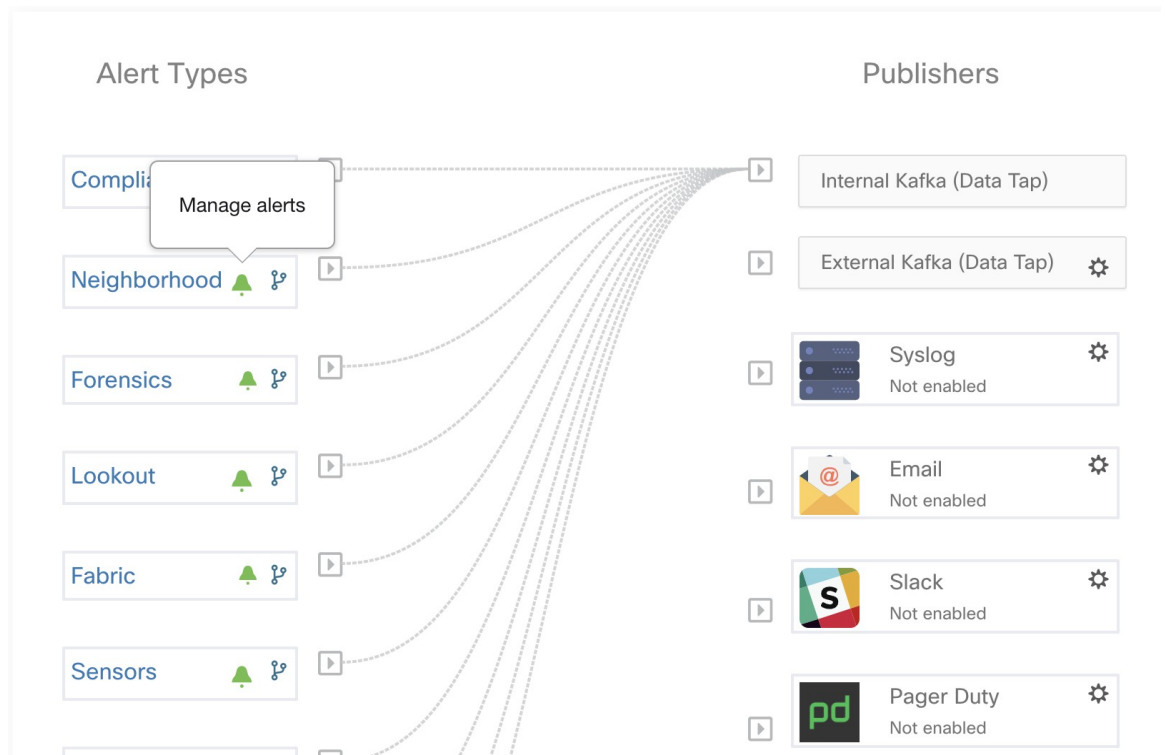
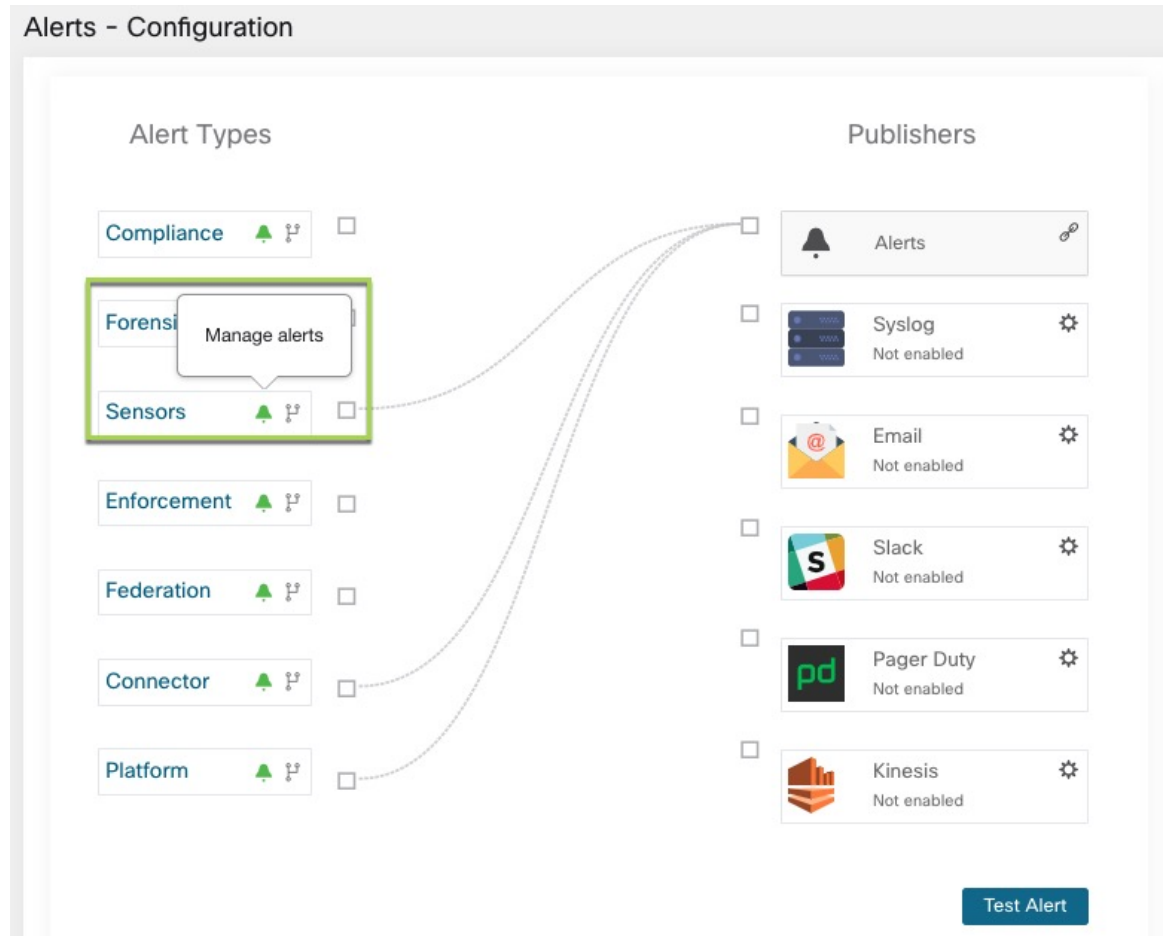


図 4: アラート（トリガールール）の作成



いくつかのコンポーネントは、アラートを設定するため、共通のアラート設定モデルを使用します。現時点では、設定モデルには次のものが含まれます（特定のアラート設定の詳細については、各ユーザーガイドを参照してください）。

- [近隣](#)
- [施行](#)
- [\[センサー \(Sensors\)\]](#)
- [施行](#)
- [\[センサー \(Sensors\)\]](#)



(注) コンプライアンス アラート タイプの場合、現在選択されている範囲で最低限「適用」機能を使用可能なユーザーのみが、アラートトリガールールを作成できます。





(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。

次のタイプには、設定モーダルがありません。

- **フォレンジック** : フォレンジックルールを使用して設定
- **コネクタ**


アラート設定モーダル

アラート設定モーダルは、次の6つのセクションで構成されています。

1. アラートのタイプ。注：これは、アラートの設定が件名に応じて異なる場合にのみ表示されます（現在、近隣アラートに対してのみ表示されます）。
 2. アラートの件名: 「何をアラートするか」を示します。これはアプリによって異なり、アラートモーダルがコンテキスト型の場合は事前に入力されている可能性があります。
 3. アラートがトリガーされる条件: 「いつアラートを生成するか」を示します。にカーソルを合わせると、指定できる条件の一覧が表示されます。注：この一覧には、現在設定されているアラートタイプに特化した条件が表示されます。
 4. アラートのシビラリティ（重大度）の選択。多くのアラートが生成された場合、シビラリティ（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UIに表示されます。
 5. サマリーアラートオプションで構成される追加の設定オプション。[詳細設定を表示する (Show Advanced Settings)] をクリックして展開します。
 6. モーダルを閉じる：新しいアラートと指定したすべての設定オプションを追加する場合は、[作成 (Create)] を選択します。または、新しいアラートを追加しない場合は [取り消し (Dismiss)] を選択します。
1. アラートのタイプ。注：これは、アラートの設定が件名に応じて異なる場合にのみ表示されます。
 2. アラートの件名: 「何をアラートするか」を示します。これはアプリによって異なり、アラートモーダルがコンテキスト型の場合は事前に入力されている可能性があります。
 3. アラートがトリガーされる条件: 「いつアラートを生成するか」を示します。にカーソルを合わせると、指定できる条件の一覧が表示されます。注：この一覧には、現在設定されているアラートタイプに特化した条件が表示されます。

4. アラートのシビラリティ（重大度）の選択。多くのアラートが生成された場合、シビラリティ（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 UI に表示されます。
5. サマリーアラートオプションで構成される追加の設定オプション。[詳細設定を表示する（Show Advanced Settings）] をクリックして展開します。
6. モーダルを閉じる：新しいアラートと指定したすべての設定オプションを追加する場合は、[作成（Create）] を選択します。または、新しいアラートを追加しない場合は [取り消し（Dismiss）] を選択します。

図 5: アラート設定モーダル

 にカーソルを合わせると、アラートトリガーを作成するために使用できるプロパティのリストが表示されます。このリストは、選択したアラートのタイプに依存するコンテキストです。

[詳細設定を表示する (Show Advanced Settings)] をクリックすると表示される追加の設定オプション:

1. **[詳細設定を表示しない (Hide Advanced Settings)]** をクリックすると、展開が折りたたまれます。
2. サマリーアラートオプション (利用可能な場合)。アラートを生成するアプリによって、利用できるかどうかが決まります。詳細については、「[サマリーアラート](#)」を参照してください。

図 6: アラート設定モーダルの詳細オプション

サマリーアラート

一部のアプリケーションではサマリーアラートが許可されており、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。

- 個別のアラートとは、一般的に、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るアラートを指し、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、送信されることを意味するわけではないことに注意してください。個別のアラートは引き続き [アプリの頻度 (App Frequency)] 間隔で生成されます。

- サマリーアラートとは、1時間の間に生成されたメトリックに対して生成されたアラート、または頻度の低いアラートのサマリーを指します。

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	はい：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
近隣	Hourly	—	対応	毎時アラートのサマリー
施行	毎分	はい：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	はい：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

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	はい：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	はい：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	はい：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 UI に表示されるイベント時間は、過去 1 時間または指定された間隔ウィンドウ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。

自動要約とスヌーズの違いに関する注記

自動要約はアラート設定に従って生成された全アラートに適用され、スヌーズは特定のアラートに適用されます。アラート設定が非常に具体的である場合、この差はわずかですが、アラート設定が広範囲である場合、差は大きくなります。

- たとえば、コンプライアンス設定は非常に幅広く、アプリケーションのワークスペースからアラート生成の対象にする違反タイプに関するものまであります。したがって、自動要約は「エスケープ」条件によってトリガーされたすべてのアラートに適用されますが、スヌーズは非常に特定のコンシューマ範囲、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されます。

- 反対に、送信元範囲と宛先範囲間のパスでホップカウントが一定数未満の場合に警告するように設定された近隣アラートは、非常に特定のアラートを生成します。
- たとえば、コンプライアンス設定は非常に幅広く、アプリケーションのワークスペースからアラート生成の対象にする違反タイプに関するものまであります。したがって、自動要約は「エスケープ」条件によってトリガーされたすべてのアラートに適用されますが、スヌーズは非常に特定のコンシューマ範囲、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されます。
- 反対に、送信元範囲と宛先範囲間のパスでホップカウントが一定数未満の場合に警告するように設定されたプラットフォームアラートは、非常に特定のアラートを生成します。

その他の違い

- スヌーズ間隔が経過した後新しいアラートが生成される際、スヌーズで生成されるのは送信するアラートのみです。スヌーズ間隔中に抑制された可能性のあるアラートの数は示されません。
- 特定の間隔でアラートが生成されている限り、アラートサマリは指定した頻度で生成されます。アラートサマリでは、期間内でトリガーされたアラート数が、集計メトリックや範囲メトリックとともに示されます。

Cisco Secure Workload Alerts Notifier (TAN)



- (注) リリース 3.3.1.x では、TAN に代わって **Cisco Secure Workload Edge アプライアンス** が使用されています。

Alerts 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。必要な資格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のみ設定できます。Secure Workload Edge アプライアンスの展開方法の詳細については、「[コネクタ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 アプライアンスのセットアップ後は、アラートタイプと内部 Kafka (データタップ) を結ぶ破線が表示されることに注意してください。これは、通知機能が内部 Kafka (データタップ) 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、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 アプライアンスのセットアップ後は、アラート

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ることに注意してください。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。

各アラート通知機能の設定方法の詳細については、「アラート通知用のコネクタ」を参照してください。

[アプリの頻度 (App Frequency)] は、アプリが実行されてアラートを生成す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。

ファブリックアラートは、アプリの実行時に1時間ごとに生成されます ([アプリの頻度 (App Frequency)] は1時間ごとであることを注意してください)。そのため、個々のアラートオプションで「1分間」のデータを指定していても、実際のファブリックアラートは「1時間」のデータの処理が終わったあとでバッチ単位で生成および送信されます。つまり、データが1分あたり2個のアラートを生成する場合、実際には120個のアラートすべてが1時間の最後に生成および送信され、UIにアラートサマリーとして表示される可能性があります。

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。

図 7: アラートのパブリッシャーの選択

The screenshot displays the configuration interface for alerts, divided into two main sections: Alert Types and Publishers.

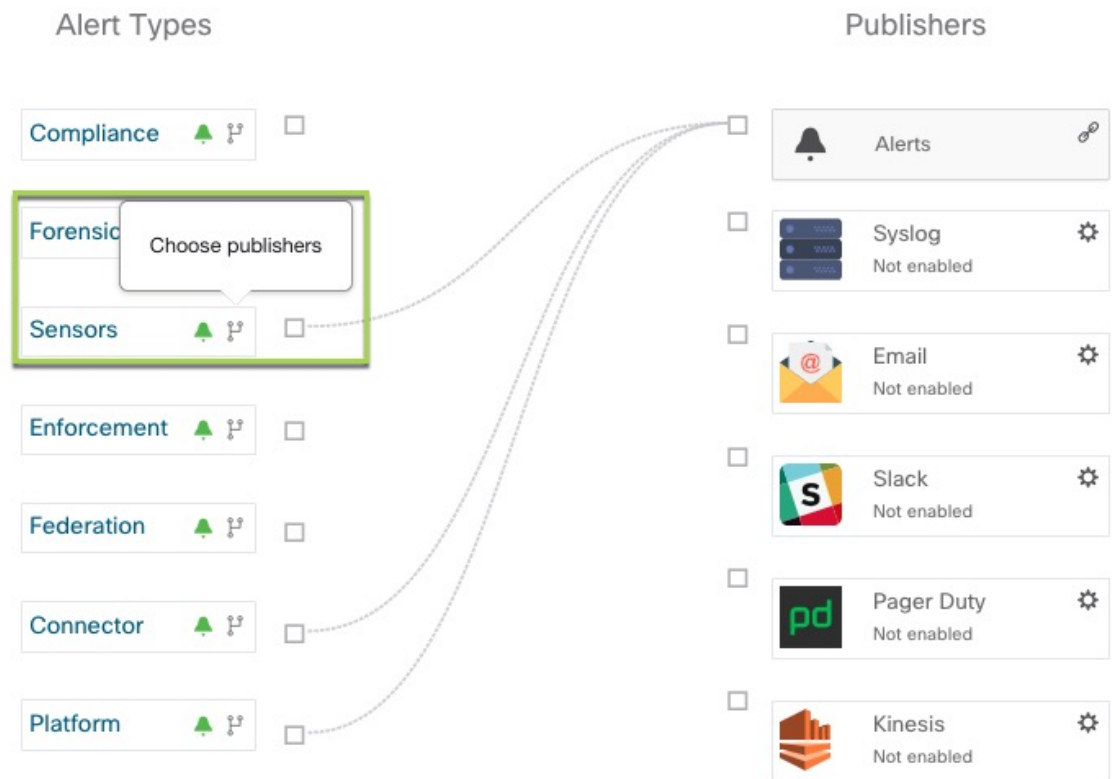
Alert Types: This section lists various alert categories, each with a dropdown arrow and a bell icon. A tooltip labeled "Choose publishers" is shown over the "Compliance" alert type.

Alert Type	Icon	Action
Compliance	Bell icon	Dropdown arrow
Neighborhood	Bell icon	Dropdown arrow
Forensics	Bell icon	Dropdown arrow
Lookout	Bell icon	Dropdown arrow
Fabric	Bell icon	Dropdown arrow
Sensors	Bell icon	Dropdown arrow
Enforcement	Bell icon	Dropdown arrow
Federation	Bell icon	Dropdown arrow
Connector	Bell icon	Dropdown arrow

Publishers: This section lists various notification channels, each with a dropdown arrow, a status indicator, and a settings gear icon.

Publisher	Status	Action
Internal Kafka (Data Tap)	Enabled	Dropdown arrow
External Kafka (Data Tap)	Enabled	Dropdown arrow
Syslog	Not enabled	Dropdown arrow
Email	Not enabled	Dropdown arrow
Slack	Not enabled	Dropdown arrow
Pager Duty	Not enabled	Dropdown arrow
Kinesis	Not enabled	Dropdown arrow

図 8: アラートのパブリッシャの選択



(注) サイト管理者と範囲所有者のみが、アラートを送信するパブリッシャを選択できます。

図 9: 選択可能なすべてのパブリッシャがこのモーダルに表示されます

選択できるすべてのパブリッシャ（アラートやアクティブな通知ツールなど）がこのモーダルに表示されます。送信ボタンを切り替えて、アラートタイプのパブリッシャを選択できます。アラートの最低シビラティ（重大度）は、重大度レベルを指し、ある特定の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。



- (注) 外部データタップを選択すると、処理できるアラートの最大数に影響を与える可能性があります。処理できるアラートの最大数は、1 分間のバッチあたり最大 14000 アラートまで削減できます。

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、ユーザー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。デフォルトのルート範囲で Secure Workload Edge アプライアンスを設定したら、syslog サーバーを以下のように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。

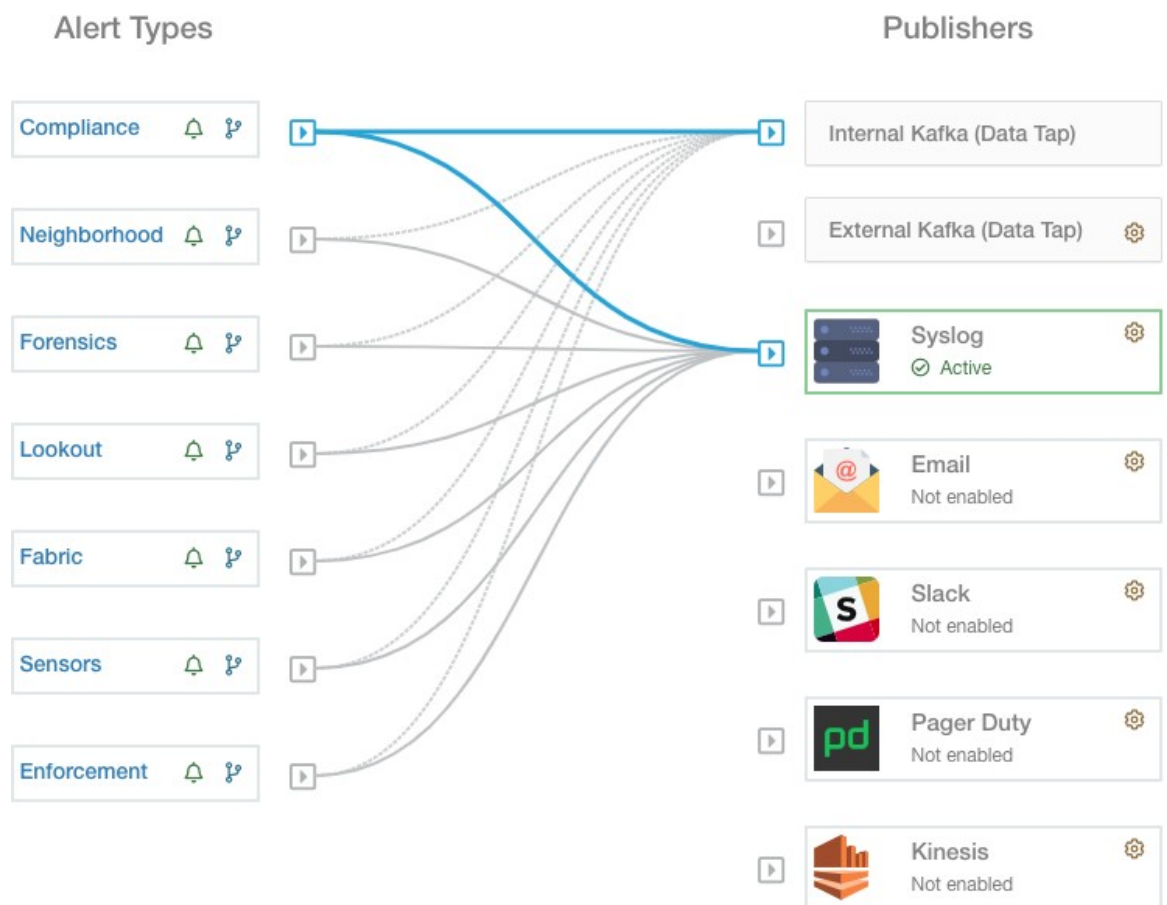
Syslog の設定方法の詳細については、「[Syslog コネクタ](#)」を参照してください。

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を注意してください。

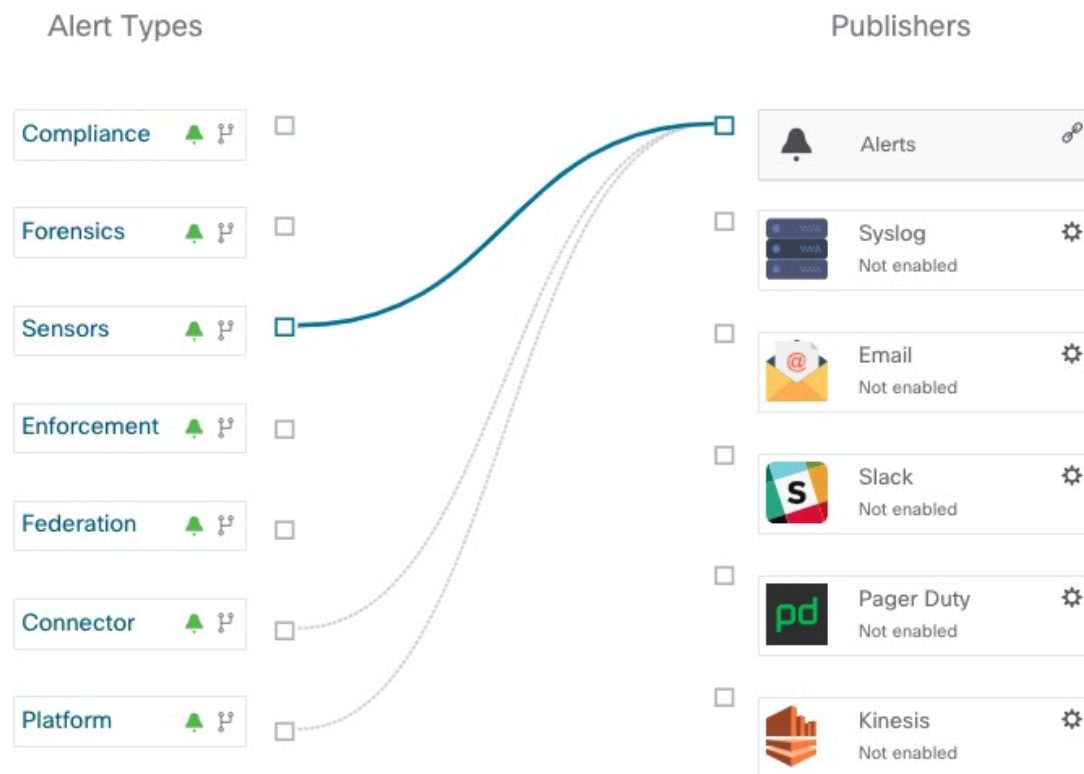
接続図には、アラートタイプとパブリッシャの間の接続が表示されます。任意のアラートタイプのパブリッシャを選択すると、そのアラートタイプとパブリッシャの間に線が確立されます。アラートのパブリッシャを指す線は、アラート通知構築の基盤となる内部メカニズムを表すため、常に破線であることを注意してください。

図 10: 接続図



この図に示すように、**Syslog**が近接アラートのパブリッシャとして選択されると、それらの間に線が確立されます。図の丸で囲まれた領域にカーソルを合わせると、近隣アラートにのみ関連付けられている接続が強調表示されることに注意してください。

図 11: 接続図



(注) ユーザーアプリケーションで生成されたアラートは、[アラート設定 (Alert Configuration)] ページに表示されません。ユーザーアプリケーションは、構成された任意のデータタップにメッセージとアラートを送信できます。

アラートトリガー規則の表示

設定されているすべてのアラートトリガー規則のリストが、接続チャートの下の表に表示されます。

図 12: アラートトリガールールの表示

The screenshot displays the Alerts Configuration interface. On the left, there are two columns: 'Alert Types' and 'Publishers'. 'Alert Types' includes Compliance, Neighborhood, Forensics, Lookout, Fabric, Sensors, Enforcement, and Federation. 'Publishers' includes Internal Kafka (Data Tap), External Kafka (Data Tap), Syslog (Not enabled), Email (Not enabled), Slack (Not enabled), Pager Duty (Not enabled), and Kinesis (Not enabled). Lines connect various alert types to publishers. On the right, the 'Alerts Trigger Rules' table is shown, listing rules for different alert types and their configurations.

Alert Type	Configuration	Actions
ENFORCEMENT	Scope: Default when Agent not reachable (seconds) > 300	
ENFORCEMENT	Scope: Default when Firewall = Off	
ENFORCEMENT	Scope: Default when Policy = Deviated	
SENSORS	Scope: Default when Agent Upgrade Status = Failed	
SENSORS	Scope: Default when Agent Flow Export Status = Stopped	
SENSORS	Scope: Default when Agent Check-In Service = Inactive	
SENSORS	Scope: Default when Deep visibility memory usage (MB) > 512 and Enforcement memory usage (MB) > 512 and Forensic memory usage (MB) > 256	
SENSORS	Scope: Default when Deep visibility CPU Quota (%) > 3 and Enforcement CPU Quota (%) > 3 and Forensic CPU Quota (%) > 3	

図 13: アラートトリガールールの表示

The screenshot displays the Alerts Configuration interface. On the left, there are two columns: 'Alert Types' and 'Publishers'. 'Alert Types' includes Compliance, Forensics, Sensors, Enforcement, Federation, Connector, and Platform. 'Publishers' includes Alerts, Syslog (Not enabled), Email (Not enabled), Slack (Not enabled), Pager Duty (Not enabled), and Kinesis (Not enabled). Lines connect various alert types to publishers. On the right, the 'Alerts Trigger Rules' table is shown, listing rules for different alert types and their configurations.

Alert Type	Configuration	Actions
ENFORCEMENT	Scope: Default when Agent not reachable (seconds) > 300	
ENFORCEMENT	Scope: Default when Firewall = Off	
ENFORCEMENT	Scope: Default when Policy = Deviated	
SENSORS	Scope: Default when Agent Upgrade Status = Failed	
SENSORS	Scope: Default when Agent Flow Export Status = Stopped	
SENSORS	Scope: Default when Agent Check-In Service = Inactive	
SENSORS	Scope: Default when Deep visibility memory usage (MB) > 512 and Enforcement memory usage (MB) > 512 and Forensic memory usage (MB) > 256	
SENSORS	Scope: Default when Deep visibility CPU Quota (%) > 3 and Enforcement CPU Quota (%) > 3 and Forensic CPU Quota (%) > 3	
SENSORS	Scope: Default when Amount of flow observations > 500000	
SENSORS	Scope: Default when Agent Uninstalled = On	
SENSORS	Scope: Default when Alert before removal (minutes) = 5	

[アラートトリガールール (Alerts Trigger Rules)] テーブルを使用して、アラートタイプ、アラート頻度、およびアラート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できます。



(注) アラートトリガー条件は完全一致条件です。

アラートトリガー規則の詳細

アラートトリガー規則テーブルの各行をクリックして、設定の詳細を展開できます。

図 14: 展開されたアラート設定

The screenshot shows the configuration interface for alert triggers. It is divided into two main sections: ENFORCEMENT and SENSORS. The SENSORS section is expanded to show details for a specific rule. The rule's configuration is as follows:

ENFORCEMENT	
Scope:	Default when Policy = Deviated
Details	
Severity	Medium
Individual Alerts	Enable
Summary Alert Freq.	None

SENSORS	
1	Scope: Default when Agent Upgrade Status = Failed 2
Details	
3	Severity: Medium
4	Individual Alerts: Enable
	Summary Alert Freq.: None

1. 件名：アラートの内容
2. トリガー：アラートが生成されるタイミング
3. アラートに割り当てられた重大度（同時に生成されたアラートが多くある場合、UIに表示されるアラートに影響する可能性があります）
4. アラートの頻度：個別アラートやサマリーアラートが生成されるかどうか。

テストアラートの生成

サンプルアラートを設定して、アラートの設定の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することができます。主な用途は、パブリッシャとの接続を確認することです。



- (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、次の手順に従います。

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)] をクリックします。

ステップ2 テストアラートを設定するために、[テストアラート (Test Alert)] ボタンをクリックします。

図 15: テストアラートの設定ページ

The screenshot shows the 'Test Alert' configuration window. On the left, there is a sidebar with four tabs: 'Keys', 'Scope', 'Details', and 'Configuration'. The 'Keys' tab is selected. The main area contains the following fields:

- Alert Key:** A text input field containing 'Aa1234Zz'.
- Event Time:** A date and time picker showing '29/03/2023, 08:59:50.628 PM'.
- Alert Time (optional):** A date and time picker showing '29/03/2023, 08:59:50.628 PM'.
- Alert Severity:** A dropdown menu currently set to 'LOW'.
- Alert Type:** A dropdown menu with 'COMPLIANCE' selected. Other options include 'FORENSICS', 'SENSORS', 'ENFORCEMENT', 'FEDERATION', and 'CONNECTOR'.

At the bottom right of the window, there are two buttons: 'Cancel' and 'Test'.

[テストアラート (Test Alert)] ページが表示されます。

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 [範囲 (Scope)] タブで、[範囲ID (Scope ID)] と [テナントID (Tenant ID)] の値が、現在の範囲に基づいて自動生成されます。

(注) [テナントID (Tenant ID)] が [テナントID VRF (Tenant ID VRF)] と同じである場合は、[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、文字列値またはJSON形式のデータを指定できます。

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。

アラート頻度は、自動的に[個別 (INDIVIDUAL)]の頻度を選択されます。

(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。

サマリーアラートは、自動的に[なし (NONE)]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ーに送信されます。

現在のアラート

[アラート (Alerts)] ページは次のように構成されています。アラートは、タイプ、ステータス (アクティブまたはスヌーズ) 、および重大度 (クリティカル、高、中、低) でフィルタリングできます。デフォルトでは、リストされているアラートはアクティブなアラートにフィルタリングされています (スヌーズおよびミュートされたアラートは、デフォルトでは表示されません) 。



警告 [アラート (Alerts)] ページには、重大度の値が低 (LOW) 、中 (MEDIUM) 、または高 (HIGH) のアラートのみが表示されます。重大度の値を問わず、すべてのアラートは必ず設定済みの Kafka ブローカーに送信されます。

図 16: 現在のアラートリスト

Event Time [↑]	Status [↑]	Alert Text [↑]	Severity [↑]	Type [↑]	Actions [↑]
Aug 9, 10:22 PM	ACTIVE	eg-tet36-win16 MSServer2016Datacenter Flow Export Stopped	MEDIUM	SENSOR	🔍 ⏹
Aug 9, 10:20 PM	ACTIVE	eg-tet36-win16 MSServer2016Datacenter Flow Export Stopped	MEDIUM	SENSOR	🔍 ⏹
Aug 9, 10:18 PM	ACTIVE	eg-tet36-win16 MSServer2016Datacenter Flow Export Stopped	MEDIUM	SENSOR	🔍 ⏹
Aug 9, 10:16 PM	ACTIVE	eg-tet36-win10 MSWindows10Pro Flow Export Stopped	MEDIUM	SENSOR	🔍 ⏹
Aug 9, 10:12 PM	ACTIVE	eg-tet36-win19-2 MSServer2019Datacenter Flow Export Stopped	MEDIUM	SENSOR	🔍 ⏹
Aug 9, 10:12 PM	ACTIVE	eg-tet36-win19 MSServer2019Datacenter Flow Export Stopped	MEDIUM	SENSOR	🔍 ⏹
Aug 9, 10:12 PM	ACTIVE	eg-tet36-win12r2 MSServer2012R2Datacenter Flow Export Stopped	MEDIUM	SENSOR	🔍 ⏹
Aug 9, 10:10 PM	ACTIVE	eg-tet36-win12r2 MSServer2012R2Datacenter Flow Export Stopped	MEDIUM	SENSOR	🔍 ⏹
Aug 9, 10:10 PM	ACTIVE	eg-tet36-win19 MSServer2019Datacenter Flow Export Stopped	MEDIUM	SENSOR	🔍 ⏹

アラート詳細の展開

特定のアラートの詳細が必要な場合は、アラートをクリックするだけで詳細情報が表示されます。

図 17: アラートの詳細

Event Time [↑]	Status [↑]	Alert Text [↑]	Severity [↑]	Type [↑]	Actions [↑]
Aug 9, 10:22 PM	ACTIVE	eg-tet36-win16 MSServer2016Datacenter Flow Export Stopped	MEDIUM	SENSOR	🔍 ⏹
Details					
<p>Host Name eg-tet36-win16</p> <p>Agent Type ENFORCER</p> <p>Agent UUID fb44f417c1a5bed633afcbfc16aca3b8bb046253</p> <p>Current Version 3.6.1.42.win64-enforcer</p> <p>Desired Version</p> <p>BIOS 88C60842-C4A1-FC1C-2F70-5C4AE929155D</p> <p>IP 172.31.182.228</p> <p>Platform MSServer2016Datacenter</p> <p>Scope Default</p> <p>Vrf ID 1</p>					

UI でのアラートの表示に関する注意事項

- UI に表示されるのは、ルート範囲当たり毎分 60 件のアラートのみです。アラートの量が増えると、UI に上述のサマリーアラートが表示されます。
- クリティカルアラート、次に重大度が高いアラート、次に重大度が中、最後に重大度が低いアラートの順に優先度が与えられます。
- ある時点で UI に表示されるアラートには最大数が設定されています。新しいアラートが届くと、古いアラートは削除されます。

「[制限](#)」を参照してください。

アラートのスヌーズ



(注) 現時点では、ユーザーアプリで作成されたアラートをスヌーズまたは無視（ミュート）することはできません。

Alerts アプリでは、同じ「タイプ」のアラートを、選択した時間だけスヌーズ（抑制）できます。「アラートのタイプ」の定義は、アラートが現在構成されているワークスペースに応じて異なることに注意してください。例としてコンプライアンスのアラートでは、「アラートのタイプ」は、コンシューマ範囲、プロバイダー範囲、プロトコル、プロバイダーポートの4つのタプルとして定義されます。

アラートのこれらのフィールドを表示するには、問題のアラートをクリックします。これだけで、アラートの詳細が表示されます。

図 18: アラートの詳細

Details	
Application Ids	test
Consumer Scope	Tetration
Flow Count	12
Fwd Categories	Escaped
Protocol	TCP
Provider Port	8301
Provider Scope	Tetration
Rev Categories	Escaped
Time Range	Aug 28 02:48:00 pm (PDT) → Aug 28 02:48:59 pm (PDT)

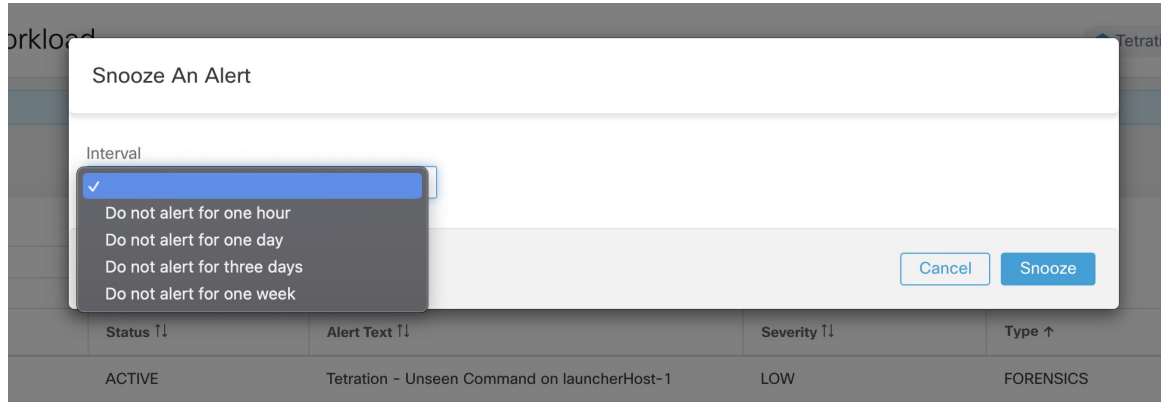
アラートのスヌーズ

アラートをスヌーズするには、スヌーズする特定のアラートタイプの[アクション (Actions)]の下にあるスヌーズボタンをクリックし、期間を指定します。

図 19: アラートのスヌーズ

Event Time ↑↓	Status ↑↓	Alert Text ↑↓	Severity ↑↓	Type ↑↓	Actions ↑↓
Aug 9, 10:22 PM	ACTIVE	eg-tet36-win16 MSServer2016Datacenter Flow Export Stopped	MEDIUM	SENSOR	Snooze an alert
Aug 9, 10:20 PM	ACTIVE	eg-tet36-win16 MSServer2016Datacenter Flow Export Stopped	MEDIUM	SENSOR	z# ○

図 20: スヌーズ期間



図に示すように、アラートは4つの異なる期間（1時間、1日、3日、または1週間）でスヌーズできます。アラートのミュートは、本質的に永久にスヌーズするアクションであり、そのボタンも [アクション (Actions)] の下にあります。

図 21: ミュートリストに追加してアラートをミュートする

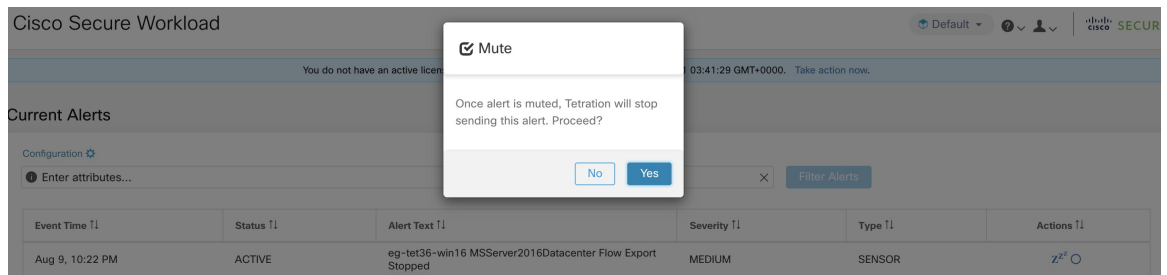
Configuration

Enter attributes... Filter Alerts

Event Time	Status	Alert Text	Severity	Type	Actions
2:57 PM	ACTIVE	Tetration - Unseen Command on launcherHost-1	LOW	FORENSICS	z o
2:56 PM	ACTIVE	Tetration - Raw Socket on collectorDatamover-1	HIGH	FORENSICS	z o
2:56 PM	ACTIVE	Tetration - Raw Socket on collectorDatamover-1	HIGH	FORENSICS	z o
2:56 PM	ACTIVE	Tetration - Raw Socket on collectorDatamover-1	HIGH	FORENSICS	z o
2:56 PM	ACTIVE	Tetration - Raw Socket on collectorDatamover-2	HIGH	FORENSICS	z o
2:56 PM	ACTIVE	Tetration - Raw Socket on collectorDatamover-2	HIGH	FORENSICS	z o
2:56 PM	ACTIVE	Tetration - Raw Socket on collectorDatamover-1	HIGH	FORENSICS	z o
2:56 PM	ACTIVE	Tetration - Raw Socket on collectorDatamover-1	HIGH	FORENSICS	z o
2:56 PM	ACTIVE	Tetration - Raw Socket on collectorDatamover-1	HIGH	FORENSICS	z o
2:56 PM	ACTIVE	Tetration - Raw Socket on collectorDatamover-2	HIGH	FORENSICS	z o
2:56 PM	ACTIVE	Tetration - Raw Socket on collectorDatamover-2	HIGH	FORENSICS	z o

Add into muted list

図 22: アラートのミュートの確認

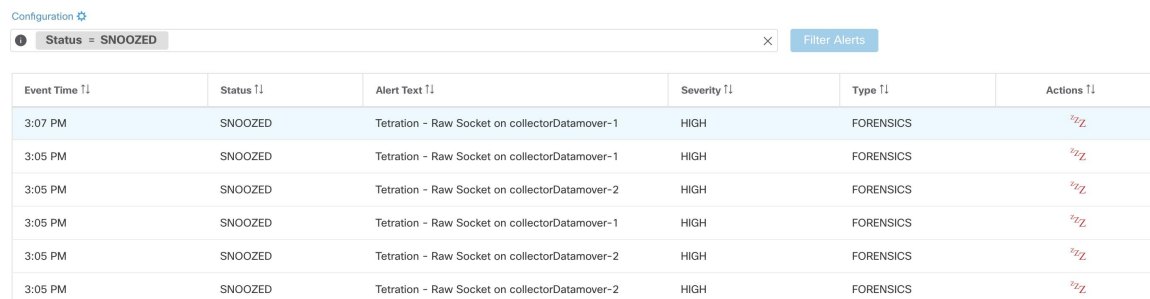


アラートが「ミュート」されている場合、アラートがミュートリストから削除されるまで、このタイプのアラートはユーザーに送信されません。

スヌーズまたはミュート状態の解除

以前にスヌーズされたアラートタイプのスヌーズを解除するには、最初のスヌーズされたアラートをフィルタで抽出して、スヌーズされたアラートのみが表示されるようにします。

図 23: スヌーズされたアラートフィルタ



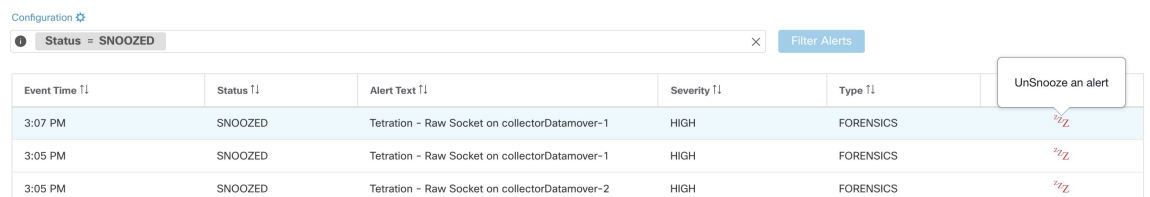
Configuration [✦](#)

Status = SNOOZED Filter Alerts

Event Time ↑↓	Status ↑↓	Alert Text ↑↓	Severity ↑↓	Type ↑↓	Actions ↑↓
3:07 PM	SNOOZED	Tetration - Raw Socket on collectorDatamover-1	HIGH	FORENSICS	
3:05 PM	SNOOZED	Tetration - Raw Socket on collectorDatamover-1	HIGH	FORENSICS	
3:05 PM	SNOOZED	Tetration - Raw Socket on collectorDatamover-2	HIGH	FORENSICS	
3:05 PM	SNOOZED	Tetration - Raw Socket on collectorDatamover-1	HIGH	FORENSICS	
3:05 PM	SNOOZED	Tetration - Raw Socket on collectorDatamover-2	HIGH	FORENSICS	
3:05 PM	SNOOZED	Tetration - Raw Socket on collectorDatamover-2	HIGH	FORENSICS	

次に、次の図のように [アクション (Actions)] で目的のアラートのスヌーズ解除ボタンをクリックし、アクションを確認します。

図 24: アラートのスヌーズ解除

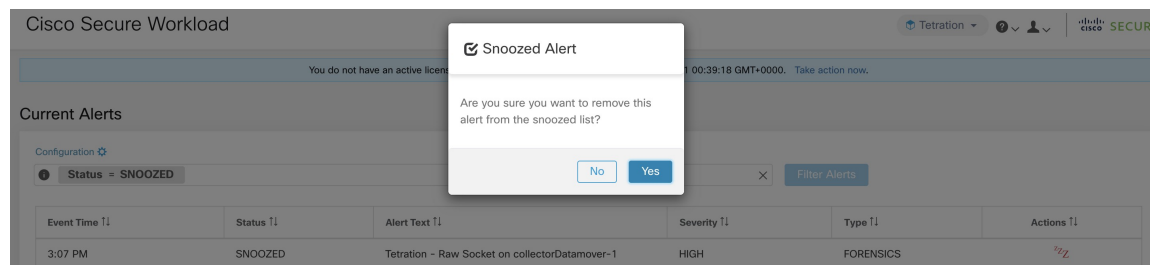


Configuration [✦](#)

Status = SNOOZED Filter Alerts

Event Time ↑↓	Status ↑↓	Alert Text ↑↓	Severity ↑↓	Type ↑↓	Actions ↑↓
3:07 PM	SNOOZED	Tetration - Raw Socket on collectorDatamover-1	HIGH	FORENSICS	
3:05 PM	SNOOZED	Tetration - Raw Socket on collectorDatamover-1	HIGH	FORENSICS	
3:05 PM	SNOOZED	Tetration - Raw Socket on collectorDatamover-2	HIGH	FORENSICS	

図 25: アラートのスヌーズ解除の確認



Cisco Secure Workload

You do not have an active license. Tetration - 00:39:18 GMT+0000. Take action now.

Current Alerts

Configuration [✦](#)

Status = SNOOZED Filter Alerts

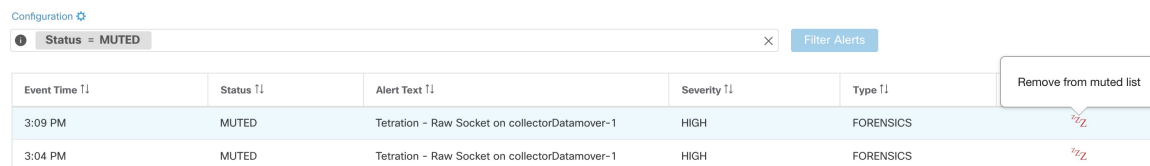
Event Time ↑↓	Status ↑↓	Alert Text ↑↓	Severity ↑↓	Type ↑↓	Actions ↑↓
3:07 PM	SNOOZED	Tetration - Raw Socket on collectorDatamover-1	HIGH	FORENSICS	

Snoozed Alert

Are you sure you want to remove this alert from the snoozed list?

このプロセスは、ミュートされたアラート以外を除外するフィルタを使用して、ミュートリストからアラートを削除する場合も同じです。

図 26: 「ミュートされた」アラートの選択とミュートリストからの削除

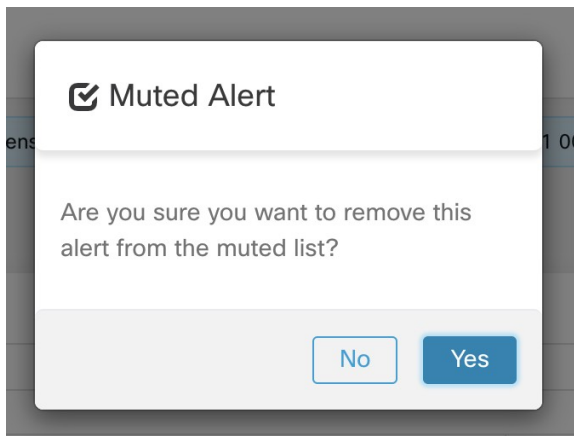


Configuration [✦](#)

Status = MUTED Filter Alerts

Event Time ↑↓	Status ↑↓	Alert Text ↑↓	Severity ↑↓	Type ↑↓	Actions ↑↓
3:09 PM	MUTED	Tetration - Raw Socket on collectorDatamover-1	HIGH	FORENSICS	
3:04 PM	MUTED	Tetration - Raw Socket on collectorDatamover-1	HIGH	FORENSICS	

図 27: アラートのミュート解除の確認



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、後述する「[アドミナルアラート](#)」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が、アラートの詳細はアラートの種類ごとに異なります。

一般的な構造は次のとおりです。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、FABRIC、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リティ（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。String-ified 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、string-ified ではありません。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。
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。
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。

フィールド	フォーマット	バージョン情報
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。
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。

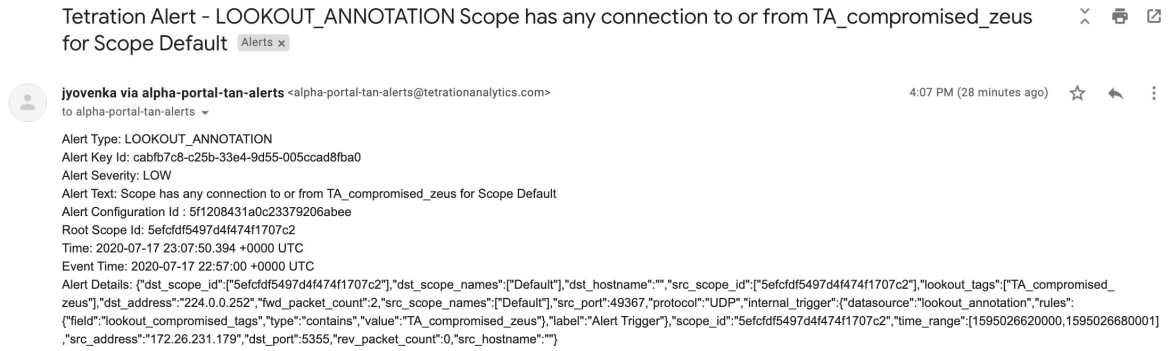
フィールド	フォーマット	バージョン情報
alert_details	string	構造化データ。String-i-fied json。このフィールドの正確な構造はアラートのタイプによって異なるため、特定のアラートタイプについては機能の詳細を参照してください。
alert_details_json	json	alert_details と同じ内容ですが、string-i-fied ではありません。コンプライアンスアラートにのみ存在し、Kafka を介してのみ使用できます。
tenant_Id	string	root_scope_id に対応する vrf を含む場合があります。または、デフォルト値として 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_details 内のフィールドは、アラートのタイプによって異なります。説明とフィールドのリストについては、各機能のセクションを参照してください。

- コンプライアンス : [lab-compliance-alert-details](#)
- 近接 : [アラートの詳細](#)
- フォレンジック : [例およびフォレンジック イベント フィールド](#)
- センサー : [センサーアラートの詳細](#)
- 適用 : [適用アラートの詳細](#)
- コネクタ : [アラートの詳細](#)
- コンプライアンス : [lab-compliance-alert-details](#)
- フォレンジック : [例およびフォレンジック イベント フィールド](#)
- センサー : [センサーアラートの詳細](#)
- 適用 : [適用アラートの詳細](#)
- コネクタ : [アラートの詳細](#)

オンプレミスクラスタにおける追加のアラートタイプ

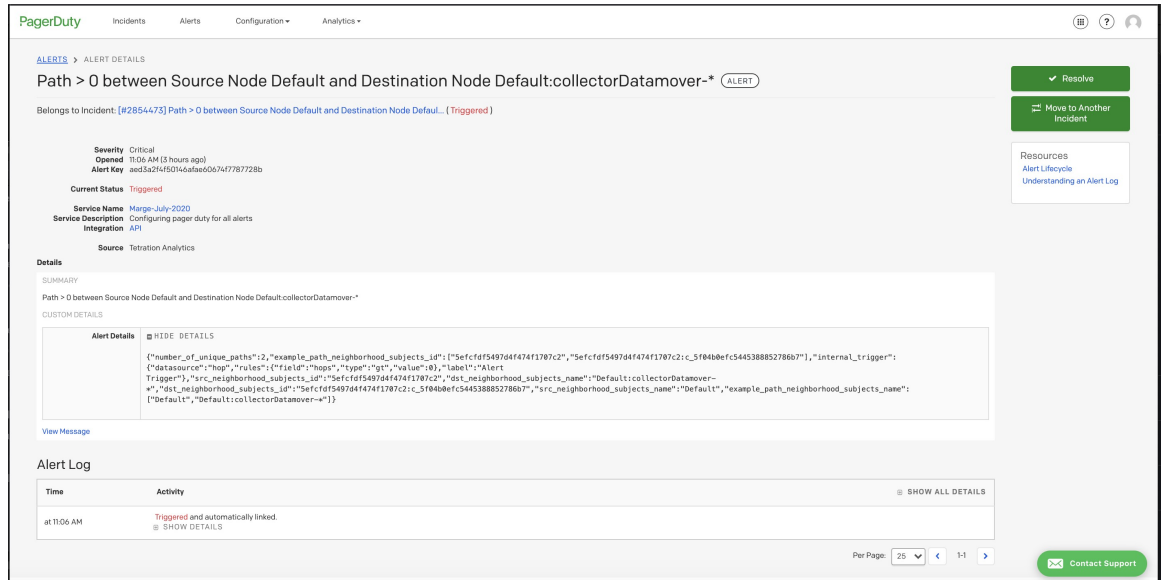
図 28: Eメール送信が設定されている場合の Cisco Secure Workload アラートの例



PagerDuty

PagerDuty アラートの設定に関する情報: [PagerDuty コネクタ](#)

図 29: 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 に基づく同じアラートの再トリガーと見なされません。

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 のシビラリティ（重大度）
IMMEDIATE_ACTION	critical
CRITICAL	critical
HIGH	error

Cisco Secure Workload のシビラリティ (重大度)	PagerDuty のシビラリティ (重大度)
MEDIUM	warning
LOW	info

Syslog

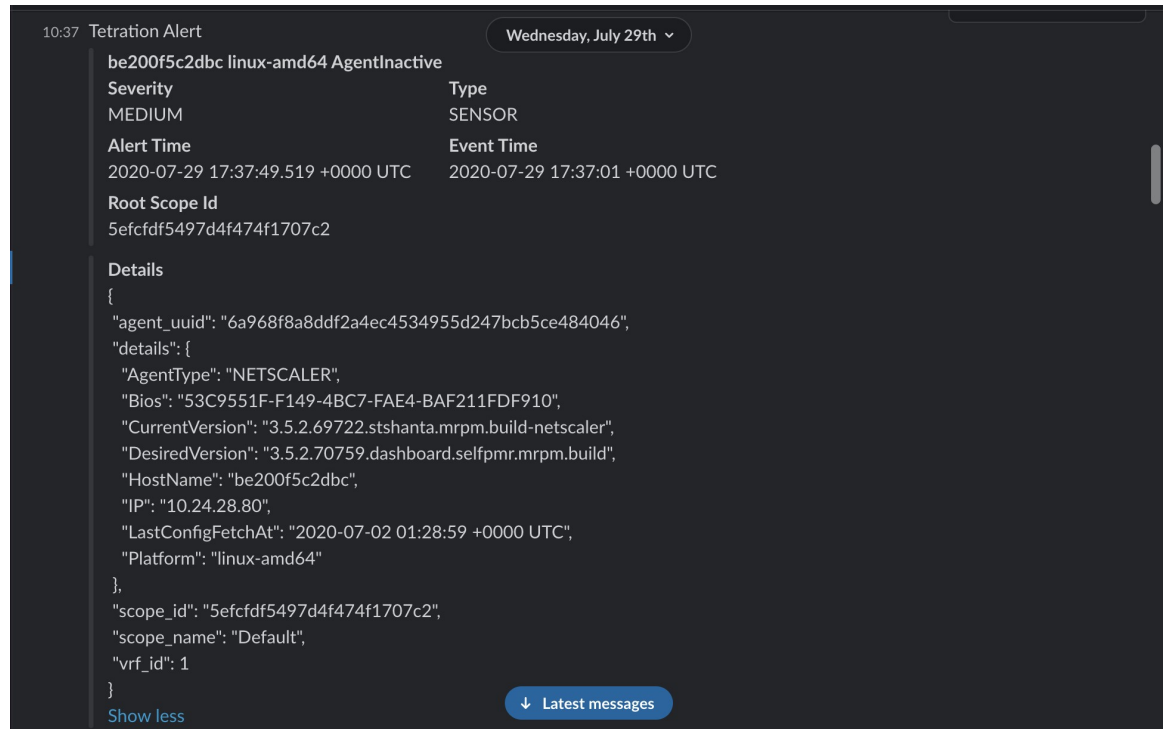
Syslog アラートの設定およびシビラリティ (重大度) のマッピングの調整については、「[Syslog コネクタ](#)」を参照してください。

図 30: Syslog に送信された *Secure Workload* アラートの例

```
Aug 2 18:45:21 tan-5f035bae1a0c231d5880d7f8-tac-demo-data-ingest Tetration Alert[26841]: [DEBUG] {"keyId":"9ee0d8b7-bc81-3427-9e84-6b9f8fedb98c","eventTime":"1596393720000","alertTime":"1596393968822","alertText":"Enforcement Annotated Flows contains escaped for \u003capplication_id:5f04b0b9755f024d4e36a279\u003e","severity":"LOW","tenantId":"","type":"COMPLIANCE","alertDetails":{"consumer_scope_ids":["5efcfd5497d4f474f1707c2"],"consumer_scope_names":["Default"],"provider_scope_names":["Default"],"provider_port":53,"application_id":"5f04b0b9755f024d4e36a279","constituent_flows":[{"consumer_port":37367,"protocol":"UDP","consumer_address":"172.31.163.139","provider_address":"171.70.168.183","provider_port":53,"consumer_port":39652,"protocol":"UDP","consumer_address":"172.31.163.137","provider_address":"171.70.168.183","provider_port":53,"consumer_port":63811,"protocol":"UDP","consumer_address":"172.31.163.136","provider_address":"171.70.168.183","provider_port":53,"consumer_port":57418,"protocol":"UDP","consumer_address":"172.31.163.138","provider_address":"173.36.131.10","provider_port":53,"consumer_port":12599,"protocol":"UDP","consumer_address":"172.31.163.141","provider_address":"173.36.131.10","provider_port":53,"consumer_port":7385,"protocol":"UDP","consumer_address":"172.31.163.140","provider_address":"173.36.131.10","provider_port":53}],"escaped_count":6,"provider_scope_ids":["5efcfd5497d4f474f1707c2"],"policy_type":"ENFORCED_POLICY","protocol":"UDP","internal_trigger":{"datasource":"compliance","rules":{"field":"policy_violations"},"type":"contains","value":"escaped"},"label":"Alert Trigger"},"time_range":{"start":1596393720000,"end":1596393779999},"policy_category":["ESCAPED"],"rootScopeId":"5efcfd5497d4f474f1707c2","alertConfId":"5f15cca71a0c231ebd66ca3b","alertTextWithNames":"Enforcement Annotated Flows contains escaped for Enforced Application j1"}
Aug 2 18:45:21 tan-5f035bae1a0c231d5880d7f8-tac-demo-data-ingest Tetration Alert[26841]: [DEBUG] {"keyId":"8f0cfc6b5-f8c1-3138-a669-3721b7d50159","eventTime":"1596393720000","alertTime":"1596393968822","alertText":"Enforcement Annotated Flows contains escaped for \u003capplication_id:5f04b0b9755f024d4e36a279\u003e","severity":"LOW","tenantId":"","type":"COMPLIANCE","alertDetails":{"consumer_scope_ids":["5efcfd5497d4f474f1707c2"],"consumer_scope_names":["Default"],"provider_scope_names":["Default"],"provider_port":5660,"application_id":"5f04b0b9755f024d4e36a279","constituent_flows":[{"consumer_port":17131,"protocol":"TCP","consumer_address":"172.26.231.193","provider_address":"172.31.163.140","provider_port":5660},"{"consumer_port":17131,"protocol":"TCP","consumer_address":"172.26.231.193","provider_address":"172.31.163.140","provider_port":5660}],"escaped_count":1,"provider_scope_ids":["5efcfd5497d4f474f1707c2"],"policy_type":"ENFORCED_POLICY","protocol":"TCP","internal_trigger":{"datasource":"compliance","rules":{"field":"policy_violations"},"type":"contains","value":"escaped"},"label":"Alert Trigger"},"time_range":{"start":1596393720000,"end":1596393779999},"policy_category":["ESCAPED"],"rootScopeId":"5efcfd5497d4f474f1707c2","alertConfId":"5f15cca71a0c231ebd66ca3b","alertTextWithNames":"Enforcement Annotated Flows contains escaped for Enforced Application j1"}
Aug 2 18:45:21 tan-5f035bae1a0c231d5880d7f8-tac-demo-data-ingest Tetration Alert[26841]: [DEBUG] {"keyId":"1ef4a974-be89-31de-abe9-dc71cb0170ad","eventTime":"1596393720000","alertTime":"1596393968822","alertText":"Enforcement Annotated Flows contains escaped for \u003capplication_id:5f04b0b9755f024d4e36a279\u003e","severity":"LOW","tenantId":"","type":"COMPLIANCE","alertDetails":{"consumer_scope_ids":["5efcfd5497d4f474f1707c2"],"consumer_scope_names":["Default"],"provider_scope_names":["Default"],"provider_port":443,"application_id":"5f04b0b9755f024d4e36a279","constituent_flows":[{"consumer_port":17792,"protocol":"TCP","consumer_address":"172.26.231.193","provider_address":"172.31.163.133","provider_port":443}],"escaped_count":1,"provider_scope_ids":["5efcfd5497d4f474f1707c2"],"policy_type":"ENFORCED_POLICY","protocol":"TCP","internal_trigger":{"datasource":"compliance","rules":{"field":"policy_violations"},"type":"contains","value":"escaped"},"label":"Alert Trigger"},"time_range":{"start":1596393720000,"end":1596393779999},"policy_category":["ESCAPED"],"rootScopeId":"5efcfd5497d4f474f1707c2","alertConfId":"5f15cca71a0c231ebd66ca3b","alertTextWithNames":"Enforcement Annotated Flows contains escaped for Enforced Application j1"}
```

Slack

Slack アラートの構成に関する情報: [Slack コネクタ](#)

図 31 : Slack チャンネルに送信される *Secure Workload* アラートの例

```
10:37 Tetration Alert Wednesday, July 29th
be200f5c2dbc linux-amd64 AgentInactive
Severity                                Type
MEDIUM                                 SENSOR
Alert Time                             Event Time
2020-07-29 17:37:49.519 +0000 UTC      2020-07-29 17:37:01 +0000 UTC
Root Scope Id
5efcfd5497d4f474f1707c2

Details
{
  "agent_uuid": "6a968f8a8ddf2a4ec4534955d247bcb5ce484046",
  "details": {
    "AgentType": "NETSCALER",
    "Bios": "53C9551F-F149-4BC7-FAE4-BAF211FDF910",
    "CurrentVersion": "3.5.2.69722.stshanta.mrpm.build-netscaler",
    "DesiredVersion": "3.5.2.70759.dashboard.selfpmr.mrpm.build",
    "HostName": "be200f5c2dbc",
    "IP": "10.24.28.80",
    "LastConfigFetchAt": "2020-07-02 01:28:59 +0000 UTC",
    "Platform": "linux-amd64"
  },
  "scope_id": "5efcfd5497d4f474f1707c2",
  "scope_name": "Default",
  "vrf_id": 1
}
Show less Latest messages
```

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。