イベント
Events

本文の内容は、Eventsのドキュメント(https://docs.sysdig.com/en/events.html)を元に日本語に翻訳・再構成した内容となっております。

イベント

Sysdigモニターイベントモジュールは、環境内で発生した監視とセキュリティの両方のイベントの包括的な統合リストをライブイベントフィードとして表示します。フィードは、トリガーされたアラートによって作成された、インフラストラクチャーサービスからプルされた、ポリシーやイメージスキャンなどのSysdig セキュアによって開始された、またはユーザーによって定義されたイベントを表示し、ユーザーが問題を確認、追跡、および解決できるようにします。各イベントは豊富なメタデータで強化されており、イベントを検索すると、監視対象のシステム内の関係全体が構築されます。統合されたイベントストリームにより、Sysdig モニターを活用する事で、セキュリティおよびアラートの監視のためのスタンドアロンツールを使用する必要がなくなるでしょう。

Sysdigモニターイベントの詳細については、次のセクションをご覧ください：

- イベントの種類
- カスタムイベント
- 重大度とステータス
- イベントの範囲
- イベントのフィルタリングと検索
- イベントアラートの設定
- イベントの確認

イベントの種類

イベントフィードには、アラートイベント、インフラストラクチャーイベント、セキュリティイベント、カスタムイベントの4つの主要なタイプのイベントが表示されます。

アラートイベント

アラートイベントは、ユーザーが設定したアラートによってトリガーされます。 アラートの設定の詳細については、Sysdigモニターアラートのドキュメントを参照してください。

インフライベント

イベントは、実稼働環境内のサポートされているサービスから収集できます。 Sysdigエージェントはこれらのサービスを自動的に検出し、デフォルトで選択したイベントのグループのイベントデータを収集するように構成されています。 dragent.yamlファイルを設定することで、リストにイベントを追加できます。

Sysdigは現在、以下のインフラストラクチャーサービスのイベント監視をサポートしています。

- Docker
- Kubernetes

*でマークされたイベントは、デフォルトで有効になっています。 追加のインフラストラクチャイベントの構成の詳細については、イベントデータの有効化/無効化を参照してください。

Dockerイベント

次のDockerイベントがサポートされています。

```
docker:
    container:
      - attach        # Container Attached      (information)
      - commit        # Container Committed     (information)
      - copy          # Container Copied        (information)
      - create        # Container Created       (information)
      - destroy       # Container Destroyed     (warning)
      - die           # Container Died          (warning)
      - exec_create   # Container Exec Created  (information)
      - exec_start    # Container Exec Started  (information)
      - export        # Container Exported      (information)
      - kill          # Container Killed        (warning)*
      - oom           # Container Out of Memory (warning)*
      - pause         # Container Paused        (information)
      - rename        # Container Renamed       (information)
      - resize        # Container Resized       (information)
      - restart       # Container Restarted     (warning)
      - start         # Container Started       (information)
      - stop          # Container Stopped       (information)
      - top           # Container Top           (information)
      - unpause       # Container Unpaused      (information)
      - update        # Container Updated       (information)
    image:
      - delete # Image Deleted  (information)
      - import # Image Imported (information)
      - pull   # Image Pulled   (information)
      - push   # Image Pushed   (information)
      - tag    # Image Tagged   (information)
      - untag  # Image Untaged  (information)
    volume:
```

```
    - create  # Volume Created    (information)
    - mount   # Volume Mounted    (information)
    - unmount # Volume Unmounted  (information)
    - destroy # Volume Destroyed  (information)
  network:
    - create     # Network Created       (information)
    - connect    # Network Connected     (information)
    - disconnect # Network Disconnected  (information)
    - destroy    # Network Destroyed     (information)
```

Kubernetesイベント

次のKubernetesイベントがサポートされています。

```
kubernetes:
  node:
    - TerminatedAllPods       # Terminated All Pods      (information)
    - RegisteredNode          # Node Registered          (information)*
    - RemovingNode            # Removing Node            (information)*
    - DeletingNode            # Deleting Node            (information)*
    - DeletingAllPods         # Deleting All Pods        (information)
    - TerminatingEvictedPod   # Terminating Evicted Pod  (information)*
    - NodeReady               # Node Ready               (information)*
    - NodeNotReady            # Node not Ready           (information)*
    - NodeSchedulable         # Node is Schedulable      (information)*
    - NodeNotSchedulable      # Node is not Schedulable  (information)*
    - CIDRNotAvailable        # CIDR not Available       (information)*
    - CIDRAssignmentFailed    # CIDR Assignment Failed   (information)*
    - Starting                # Starting Kubelet         (information)*
    - KubeletSetupFailed      # Kubelet Setup Failed     (warning)*
    - FailedMount             # Volume Mount Failed      (warning)*
    - NodeSelectorMismatching # Node Selector Mismatch   (warning)*
    - InsufficientFreeCPU     # Insufficient Free CPU    (warning)*
    - InsufficientFreeMemory  # Insufficient Free Mem    (warning)*
    - OutOfDisk               # Out of Disk              (information)*
    - HostNetworkNotSupported # Host Ntw not Supported   (warning)*
    - NilShaper               # Undefined Shaper         (warning)*
    - Rebooted                # Node Rebooted            (warning)*
    - NodeHasSufficientDisk   # Node Has Sufficient Disk (information)*
    - NodeOutOfDisk           # Node Out of Disk Space   (information)*
    - InvalidDiskCapacity     # Invalid Disk Capacity    (warning)*
    - FreeDiskSpaceFailed     # Free Disk Space Failed   (warning)*
  pod:
    - Pulling           # Pulling Container Image          (information)
    - Pulled            # Ctr Img Pulled                   (information)
    - Failed            # Ctr Img Pull/Create/Start Fail   (warning)*
    - InspectFailed     # Ctr Img Inspect Failed           (warning)*
    - ErrImageNeverPull # Ctr Img NeverPull Policy Violate (warning)*
    - BackOff           # Back Off Ctr Start, Image Pull   (warning)
    - Created           # Container Created                (information)
    - Started           # Container Started                (information)
    - Killing           # Killing Container                (information)*
    - Unhealthy         # Container Unhealthy              (warning)
```

```
    - FailedSync        # Pod Sync Failed                  (warning)
    - FailedValidation  # Failed Pod Config Validation     (warning)
    - OutOfDisk         # Out of Disk                      (information)*
    - HostPortConflict  # Host/Port Conflict               (warning)*
  replicationController:
    - SuccessfulCreate    # Pod Created        (information)*
    - FailedCreate        # Pod Create Failed  (warning)*
    - SuccessfulDelete    # Pod Deleted        (information)*
    - FailedDelete        # Pod Delete Failed  (warning)*
```

セキュリティイベント

イベントモジュールは、Sysdig セキュアによって開始されたイベントを表示します。イベントのライブストリームにより、ポリシー違反とイメージスキャンの結果がすぐに通知されます。 Sysdig モニターは、次のタイプのセキュリティイベントをサポートしています。

スキャン

スキャンイベントは、脆弱性、シークレット、ライセンス違反などを通知します。たとえば、スキャンされていないイメージが環境に追加された場合、イメージがポリシー評価に失敗した場合、スキャン結果が変更された場合、またはCVEが更新された場合に、イベントが生成されます。詳細については、イメージスキャンを参照してください。

ポリシー

ポリシーイベントは、ポリシーに違反したときにトリガーされます。たとえば、特定のコマンドやプロセスの不正な実行、読み取り/書き込み操作、システムコール、ブラックリストに登録されたコンテナイメージのダウンロードによってイベントがトリガーされます。詳細については、「ポリシーイベント」を参照してください。

カスタムイベント

追加のイベントは、Sysdigエージェントによって収集され、イベントモジュールに表示されますが、より包括的な設定手順が必要です。これらのカスタムイベントは、次の方法で統合できます。

- SysdigモニターSlackbot
- Pythonスクリプト（Sysdigによって事前に作成されたか、ユーザーが作成したもの）
- CURLリクエスト

他のカスタムイベントの設定に関する簡単なサンプルスクリプトについては、カスタムイベントを参照してください。詳細については、Sysdigサポートにお問い合わせください。

カスタムイベント

Sysdig モニターは、コードのデプロイ、自動スケーリングアクティビティ、ビジネスレベルのアクションなど、作成されたカスタムイベントを取り込むことができます。これらのイベントは、すべてのパフォーマンスデータを簡単に関連付けるために、チャートとグラフに自動的にオーバーレイされます。以下のセクションでは、カスタムイベントをSysdigモニターに送信するさまざまな方法の概要を説明します。

アプリケーション統合

Sysdig モニターは、デフォルトで特定のアプリケーションとのイベント統合をサポートしています。Sysdigエージェントはこれらのサービスを自動的に検出し、それらからイベントデータの収集を開始します。詳細については、イベントのドキュメントを参照してください。

SysdigモニターSlackbot

Sysdigbot（Sysdig Monitor Slackbot）を使用すると、ユーザーはSlackボットとのチャットを通じてカスタムイベントを直接Sysdigクラウドに投稿できます。

ビルド済みPythonスクリプト

Sysdig Pythonスクリプトは、次のコマンド構造を使用して、コマンドラインから直接Sysdig Monitorにイベントを送信する方法を提供します。

```
python post_event.py SYSDIG_TOKEN NAME [-d DESCRIPTION] [-s SEVERITY] [-c SCOPE] [-t TAGS]
[-h]
```

詳細については、Sysdig Githubリポジトリを参照してください。

Pythonサンプルクライアント

Sysdig モニター pythonクライアントは、Sysdig Monitor REST APIのラッパーとして機能し、REST API機能のほとんどを公開して、使いやすくインストール可能なpythonインターフェースを提供します。post_eventx( )関数を使用して、カスタムスクリプトからSysdig Monitorにイベントを送信できます。スクリプトの例を以下に示します。

```
import os
import sys

sys.path.insert(0, os.path.join(os.path.dirname(os.path.realpath(sys.argv[0])), '..'))

from sdcclient import SdcClient

# Parse arguments
sdc_token = sys.argv[1]
name = sys.argv[2]

# Instantiate the SDC client
sdclient = SdcClient(SDC_TOKEN)

# Post the event using post_event(self, name, description=None, severity=None,
event_filter=None, tags=None)
res = sdclient.post_event(NAME)
```

Curlサンプルクライアント

Sysdig Monitor REST APIは、APIを介してSysdig Monitorアプリの全機能を提供し、REST APIを介してカスタムイベントをSysdigクラウドに直接送信できるようにします。以下の例は、curlリクエストです。

```
#!/bin/bash
SDC_ACCESS_TOKEN='626abc7-YOUR-TOKEN-HERE-3a3ghj432'
ENDPOINT='app.sysdigcloud.com'

curl -X POST -s 'https://'"${ENDPOINT}"'/api/events' \
-H 'Content-Type: application/json; charset=UTF-8' \
-H 'Accept: application/json, text/javascript, */*; q=0.01' \
-H 'Authorization: Bearer '"${SDC_ACCESS_TOKEN}"'' \
--data-binary '{"event":{"name":"Jenkins - start wordpress
deploy","description":"deploy","severity":"6","tags":{"build":"89"}}}' --compressed
sleep 5s
```

イベントデータの有効化/無効化も参照してください。

重大度とステータス

イベントの重大度

イベントの重大度はSysdigモニターUIで4つのカテゴリーに分類され、問題の優先順位を視覚化し、フィルター操作を容易にします。

注意

新しいカテゴリはこれらの値の単純化されたグループであるため、以前の重大度の値（0〜7）を使用したスクリプトは引き続き期待どおりに機能します。

以下の画像は、重大度の値の内訳を示しています。

イベントステータス

主なイベントステータスには、トリガーと解決の2つがあります。さらに、フィルタリング方法を改善するために利用可能な2つの追加ステータスがあります。

注意

イベントフィードのフィルタリングの詳細については、「イベントのフィルタリング」セクションを参照してください。

イベントステータス	説明
Triggered	イベントをトリガーした状況はそのまま残ります（たとえば、ノードはダウンしたままになります）。
Resolved	イベントをトリガーした状況が整っていません（たとえば、メトリクス値が通常の範囲内に戻ったなど）。
Acknowledged	イベントフィードをさらにフィルタリングするのに役立つ手動ラベル。 **注意**：確認済みラベルは純粋に視覚的なマーカーであり、イベントの現在の状態（トリガー/解決済み）を反映していません。 カスタムイベントを確認済みとしてマークすることはできません。
Unacknowledged	イベントフィードをさらにフィルタリングするのに役立つ手動ラベル。 **注意**：すべてのイベントは、デフォルトで未確認としてマークされます。

イベントスコープ

デフォルトでは、イベントフィードには環境全体のイベントが表示されます。ただし、その環境内の特定のスコープからのイベントのみを表示するようにフィードを設定できます。イベントフィードのスコープは、ラベルで設定できます。

ラベルは、Sysdigモニターによって定義された意味のあるキーと値のペア（ホワイトリスト）のセットを指します。ユーザーは、ホワイトリストを設定できます。たとえば、ECSを使用していて、定義済みのカスタムコンテナラベルがある場合、ホワイトリストを構成して必要なラベルを追加することができます。完了すると、コンテナに関連するすべてのインフラストラクチャイベントがこれらのラベルで強化され、イベントスコープに関連するメタデータが表示されます。

スコープの詳細については、メトリクスのグループ化、スコープ、およびセグメント化のドキュメントを参照してください。

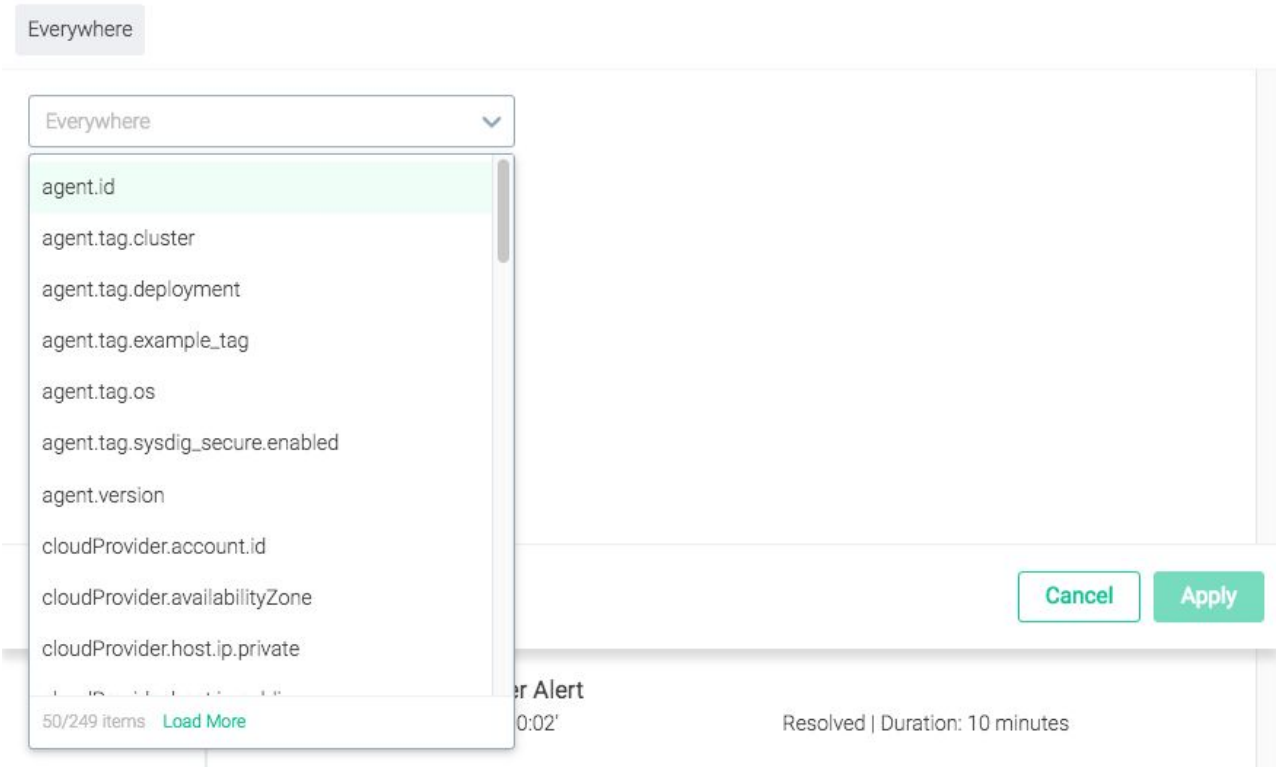
イベントスコープの設定

イベントフィードのスコープを設定するには：

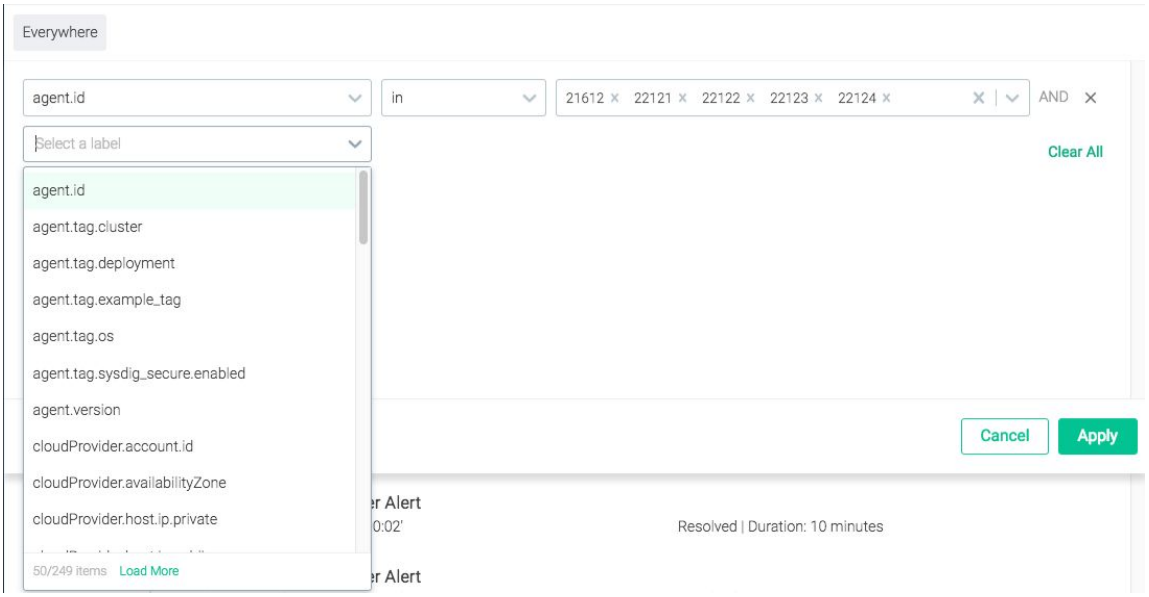
1. [`Events`]モジュールで、[`Edit Scope`]リンクをクリックします。

2. トップレベルのドロップダウンメニューを開きます。

3. リストをスクロールするか、検索バーに名前/部分的な名前を入力して選択することにより、目的のラベルを選択します。



4. [`Operator`]ドロップダウンメニューを開き、関連するオプションを選択します。
5. [`Value`]ドロップダウンメニューを開き、関連するオプションを選択します。
6. オプション：次のレベルのドロップダウンメニューを開き、手順3〜5を繰り返します。



7. オプション：必要なスコープの追加レイヤーごとにステップ6を繰り返します。

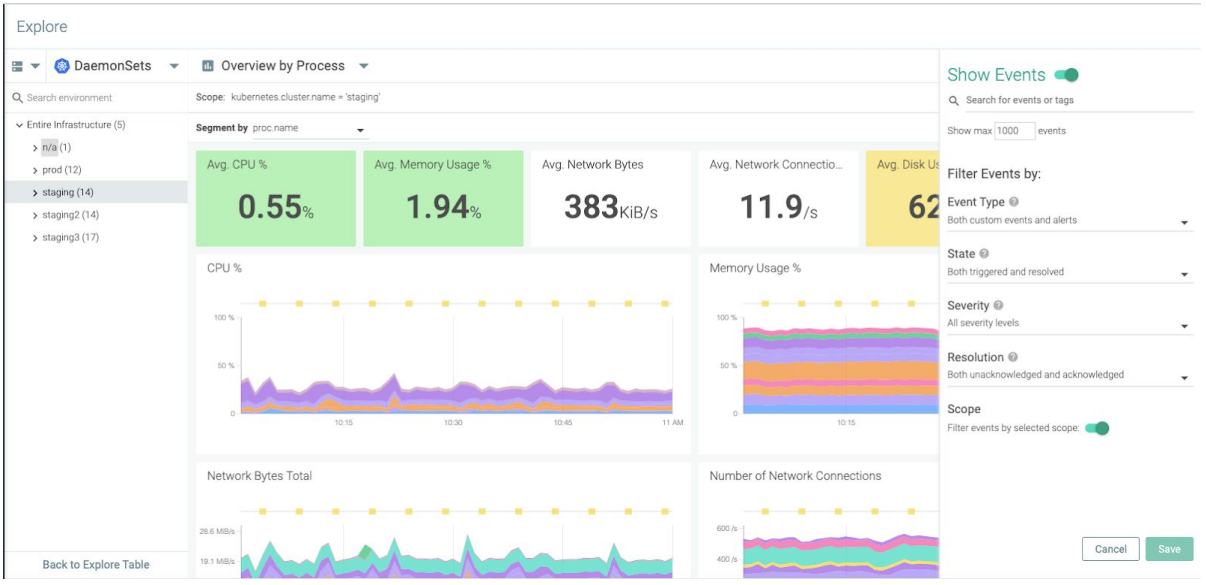
> **注意**
>
> 必要に応じて、関連するレイヤーの横にある`Delete`（x）アイコンをクリックして、スコープの個々のレイヤーを削除できます。

8. [`Apply`]ボタンをクリックして、新しいスコープを保存します。

スコープによるイベントのフィルタリング

イベントはデフォルトでダッシュボードとエクスプローラのスコープでフィルタリングされ、選択したスコープに関連する最も関連性の高いイベントが表示されます。この機能により、対象となる領域の潜在的な問題をすばやく絞り込むことができます。ただし、フィルタリングをオフにして、完全なスコープからイベントを表示できます。エクスプローラーでこれを行うには：

1. エクスプローラーモジュールで、オプション（3つのドット）アイコンをクリックし、[**Events**]を選択します。



[Events]パネルが表示されます。次のことができます。

- イベントを表示するかどうかを決定します。
- エクスプローラーテーブルに表示されるイベントの最大数を決定します。
- イベントをフィルターする
    - タイプ：サポートされるイベントのタイプは、カスタムイベントとアラートです。詳細については、イベントタイプを参照してください。
    - ステート：サポートされるイベントのタイプがトリガーされ、解決されます。詳細については、重大度とステータスを参照してください。
    - 重大度：サポートされる重大度レベルは、すべての重大度タイプ、高重大度、および高レベルと中レベルの両方です。詳細については、重大度とステータスを参照してください。
    - 解決策：サポートされる解決策は、確認済みと未確認の両方、確認済みのみ、未確認のみです。詳細については、重大度とステータスを参照してください。
- イベントをスコープ別に表示するかどうかを決定します。トグルボタンを使用して、スコープによるフィルタリングをオフにします。
- このオプションを無効にすると、エクスプローラーテーブルには、選択したスコープに関係のないイベントを含め、インフラストラクチャ内のすべてのイベントのフィードが表示されます。[**Filter events by selected scope**]オプションを有効のままにして、関連するイベントのみを表示します。
- **Save**をクリックします。

  同様に、ダッシュボードでスコープによるイベントのフィルタリングをオフにすることができます。

環境スコープをリセットする

スコープを環境全体でリセットするには：

1. [Events]モジュールで、[`Edit Scope`]リンクをクリックします。

2. [Clear All]リンクをクリックします。

3. [Apply]ボタンをクリックして変更を保存します。

イベントアラートを設定する

[Event Details]パネルから、イベントアラートを作成（カスタムイベントの場合）および設定が（アラートイベント、および以前に作成したアラートのあるカスタムイベントの場合）できます。

1. [Events]モジュールで、フィードからイベントを選択して[Event Details]パネルを開きます。
2. 「Configure Alert」パネルを開きます。
    a. 既存のアラートの場合は、[Edit Alert]リンクをクリックします。
    b. 新しいアラートについては、[Edit Alert]ボタンをクリックします。
3. 必要に応じてアラートを設定します。アラートの設定の詳細については、アラートのドキュメントを参照してください。

> **注意**
>
> 新しいアラートには、カスタムイベントの情報が自動的に入力されます。

新しいアラートの場合は[`Create button`]ボタンをクリックし、既存のアラートの場合は[`Save`]ボタンをクリックします。

イベントのフィルタリングと検索

イベントのフィルタリング

イベントフィードは、複数の方法でフィルタリングして、環境の履歴にドリルダウンし、表示されるイベントを絞り込むことができます。フィードは、重大度、タイプ、ステータスでフィルタリングできます。 それぞれの例を以下に示します。

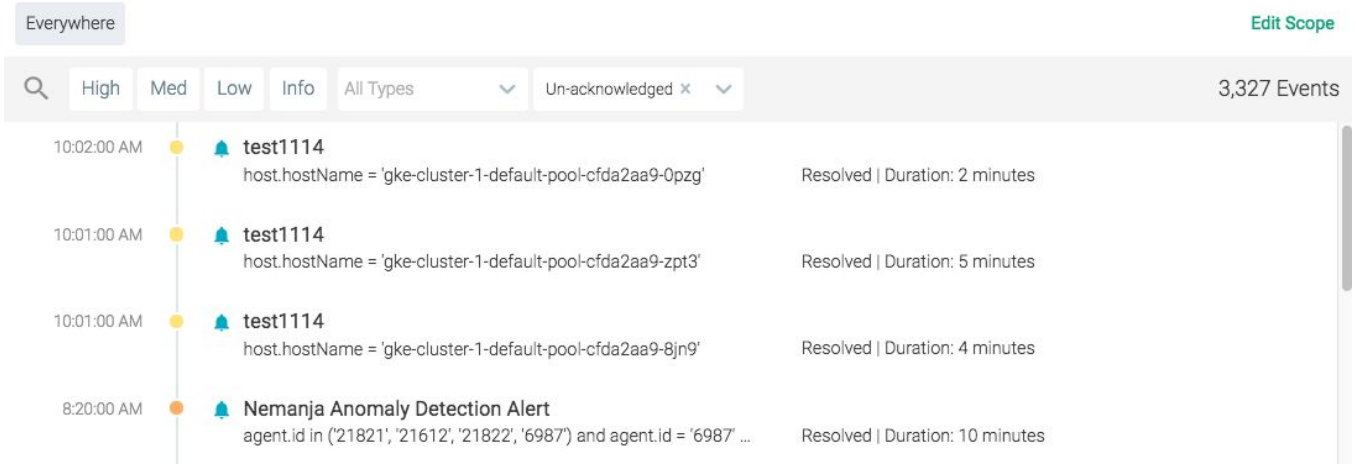
以下の例は、重大度が高および中のイベントのみを示しています。

以下の例は、Kubernetesイベントのみを示しています。

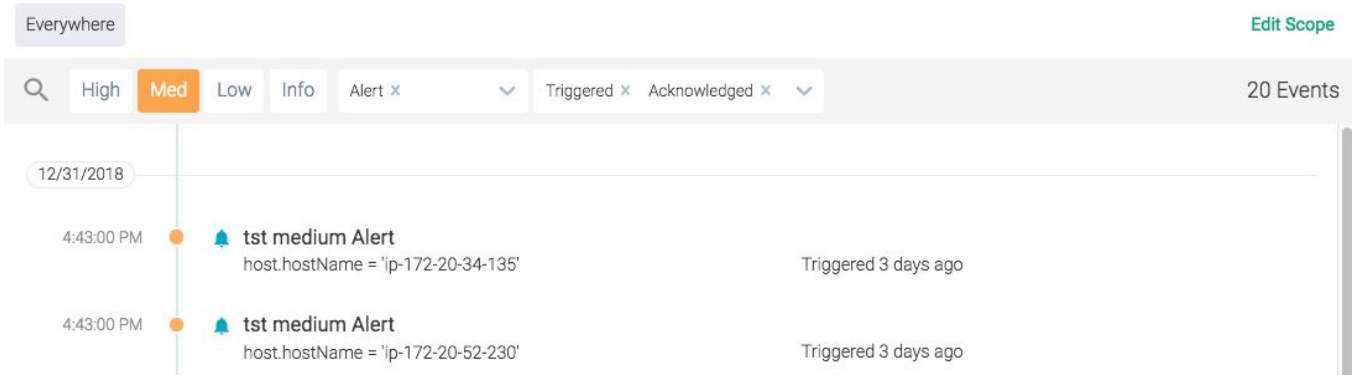
以下の例は、未確認のイベントのみを示しています。

注意

Acknowledgedラベルは純粋に視覚的なマーカーであり、イベントの現在の状態（トリガー/解決済み）を反映していません。 デフォルトでは、すべてのイベントは未確認です。

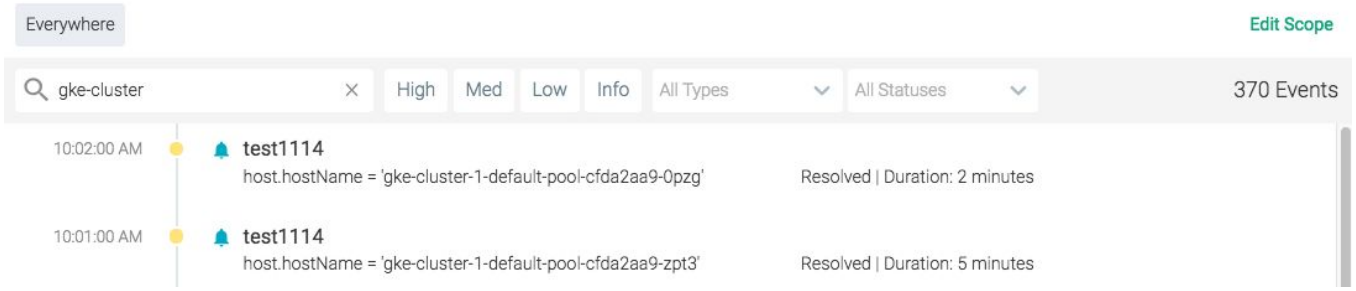


以下の例は、トリガーされたままであるが確認された中程度の重大度のアラートイベントを示しています。



イベントを検索

イベントフィードは、上部のバーにある検索アイコンを使用して検索できます。



イベントの確認

フィードのイベントリストをクリックすると、イベントを詳細に確認できます。

イベント発生時の環境を詳細に確認するには、[Explore]ボタンをクリックして[Explore]モジュールに移動します。Exploreモジュールは、影響を受ける環境オブジェクトに自動的にドリルダウンします。

イベント詳細パネル

「Event Details」パネルには、イベントに関する詳細情報が含まれています。 この情報は、イベントがアラートイベントかカスタムイベントかによって異なります。

アラートイベント

以下の例は、アラートイベントです。

メタデータ	説明
Event ID	イベントのユニークID
Severity	イベントの重大度（High, Medium, Low, Info）
State	イベントの現在の状態（Triggered, Resolved）
Duration	イベントが継続した時間の長さ
Acknowledged	イベントが承認されたかどうか
Trigger	イベントの原因（たとえば、定義された範囲を超えたメトリクスおよび到達した値）
Entity	イベントが発生したエンティティ
Start Time	イベントが開始した日時
End Time	イベントが終了した日時
Alert Name	トリガーされたアラートの名前
Type	アラートのタイプ
Metrics	影響を受けたメトリクス
Trigger Condition	アラートをトリガーするために満たされた条件
Scope	アラートの範囲
Segment	アラートに適用されるセグメンテーション

注意

イベントを作成したアラートを設定するには、[Event Details]パネルの[`Edit Alert`]リンクをクリックします。 アラートの詳細については、アラートのドキュメントを参照してください。

セキュリティイベント

ポリシー

この例は、コンテナ内で無許可のターミナルシェルを通知するイベントを示しています。 ポリシーアラートの詳細については、「ポリシーイベントの詳細」を参照してください。

メタデータ	説明
Event ID	イベントのユニークID
Severity	イベントの重大度（High, Medium, Low, Info）
Date / Time	イベントが発生した日時
Host	ホスト名と物理アドレス（MAC）
Container	コンテナ名、ユニーク識別子、およびイメージ
Summary	発生したことの詳細な説明

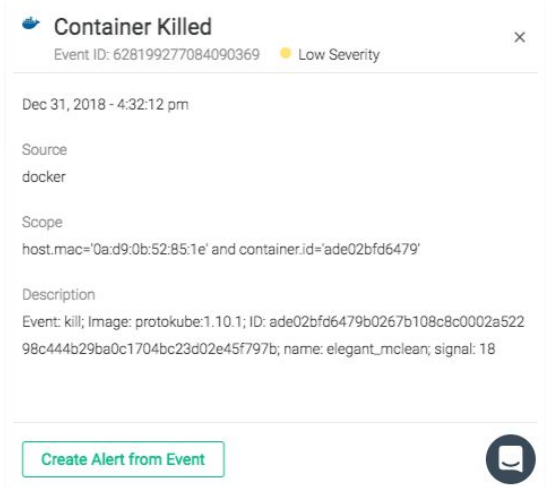
スキャン

例は、Quayのelasticsearchイメージのスキャン結果の変化を警告する重大度の高いイベントです。 スキャンの詳細については、「スキャンアラート」を参照してください。

メタデータ	説明
Event ID	イベントのユニークID
Severity	イベントの重大度（High, Medium, Low, Info）
Date / Time	イベントが発生した日時
Image Registry	イメージが存在するリポジトリー（例えば、Quay）
Tag	イメージに関連付けられたイメージ名
Image ID	イメージのユニーク識別子。
Digest	イメージのJSON設定オブジェクトのSHA256ハッシュを含む、コンテンツアドレス可能な識別子

インフラストラクチャーとカスタムイベント

インフラストラクチャイベントとカスタムイベントは、[`Event Details`]パネルに同じ情報セットを表示します。 以下の例は、Dockerイベントです。



メタデータ	説明
Event ID	イベントのユニークID
Severity	イベントの重大度（High, Medium, Low, Info）
Date / Time	イベントが発生した日時
Source	イベントのソース（Dockerなど）
Scope	イベントのスコープ
Description	発生したことの詳細な説明