sysdig

ポリシー

本文の内容は、Sysdig Secure ポリシーのドキュメント(https://docs.sysdig.com/en/policies.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。

ポリシー

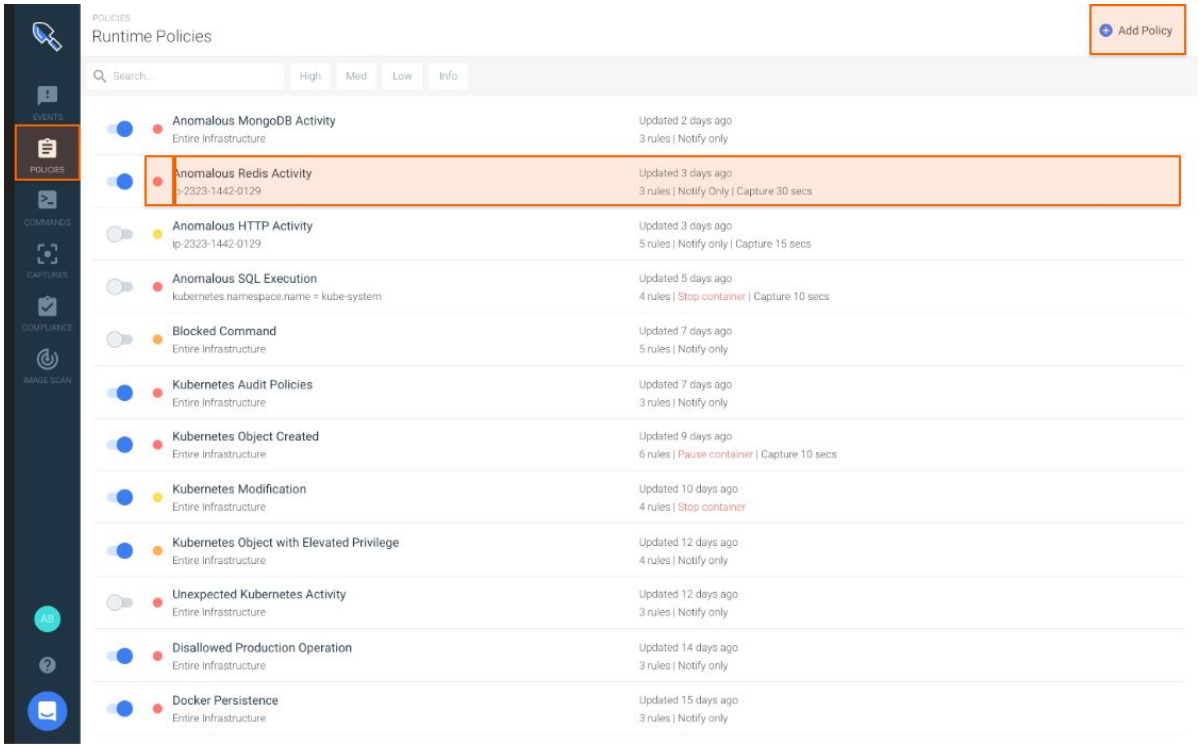
このページでは、Sysdigポリシーとそれらを構成するルールを紹介し、自分の環境でセキュリティポリシーを作成、編集、および適用するために必要な概念的背景を提供します。

Sysdigセキュアポリシーについて

Sysdig Secureポリシーは、企業が環境内で検出したいアクティビティ、ポリシールールに違反した場合に実行するアクション、および潜在的に送信する必要がある通知に関するルールの組み合わせです。すぐに使用できる多数のポリシーが提供されており、必要に応じてそのまま使用したり、複製したり、編集したりできます。 定義済みのルールを使用するか、カスタムルールを作成して、ポリシーを最初から作成することもできます。

ランタイムポリシーUIの確認

`Policies > Runtime Policies` を選択して、Sysdig Secureに含まれるデフォルトポリシーを確認します。



上記の概要から、次のことができます

一目で確認

- **重大度レベル** デフォルトポリシーには、編集可能な高、中、低、または情報レベルの重大度が割り当てられます。

- **有効/無効** は切り替えトグルで表示されます
- **ポリシーの概要は、**
  更新ステータス、ルールの数、影響を受けるコンテナで実行する割り当てられたアクション（`Stop | Pause | Notify`）、およびキャプチャの詳細（ある場合）が含まれます。

操作

このパネルでは以下も操作できます。

- ポリシーの詳細へのドリルダウン（および 編集 ）

- ポリシー名、または重大度レベルによるポリシーの検索とフィルター

- トグルを使用したポリシーの有効化/無効化

- `+Add Policy`ボタンで新規ポリシーの作成

Sysdig Secure Rulesの理解する

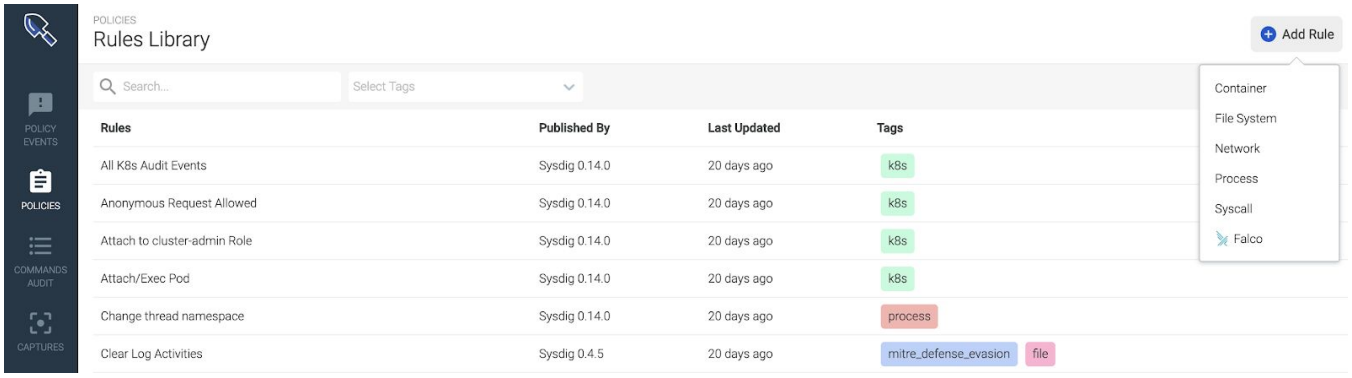
ルールは、セキュリティポリシーを作成するために使用する基本的な構成要素です。ルールは、企業が環境内で検出したいあらゆるタイプのアクティビティを表現します。

ルールは次の2つの形式で表現できます

- **Falcoルール 構文**

- ファストルール 構文 これはシンプルなホワイトリスト/ブラックリストです。
  ファストルールは、コンテナイメージ、ファイルシステム、ネットワーク、プロセス、およびSyscallの5つのタイプにグループ化されます。

Sysdig Secure UIはルールをさまざまなタイプにグループ化し、各タイプに適切なルール作成入力画面を提供します。（参照：ルールの作成。）



注

Sysdigが作成したデフォルトのルールは、[Published By]列にSysdigが表示されます。 自分で作成したルールには、[Published By]列にSecure UIが表示されます。

デフォルトのルールは削除できず、編集できるものに制限があります。 詳細については、ルールの編集を参照してください。

Falcoルール

Falcoの概要については、Sysdig Secure内でのFalcoの使用を参照してください。

Falcoルールは、ファストルールタイプよりも複雑で繊細な場合があることに注意してください。

ファストルール

ファストルールは、プロセス、ネットワーク接続、およびその他の操作の簡単な検出を実現します。
例：

- このプロセスが検出された場合、警告してください。
  または
- xポートでネットワーク接続が検出された場合は、警告してください。

Falcoルールとは異なり、ファストルールタイプは、「y IPアドレスからxポートで接続が検出された場合...」などの複雑なルールの組み合わせはできません。

5つのファストルールタイプを以下に説明します。

コンテナルール

これらのルールは、特定のイメージ名が環境で実行されているかどうかを通知するために使用されます。

ファイルシステムルール

これらのルールは、特定のディレクトリ/ファイルへの書き込みアクティビティがあるかどうかを通知するために使用されます。

ネットワークルール

これらのルールは、次の目的で使用します。

- 特定のリストの信頼できるリスト外のポートでアクティビティを検出する
- 予期しないインバウンド/アウトバウンド接続の場合に通知する

プロセスルール

これらのルールは、SSHなどの特定のプロセスが環境の特定の領域で実行されているかどうかを検出するために使用されます。

システムコールルール

注意

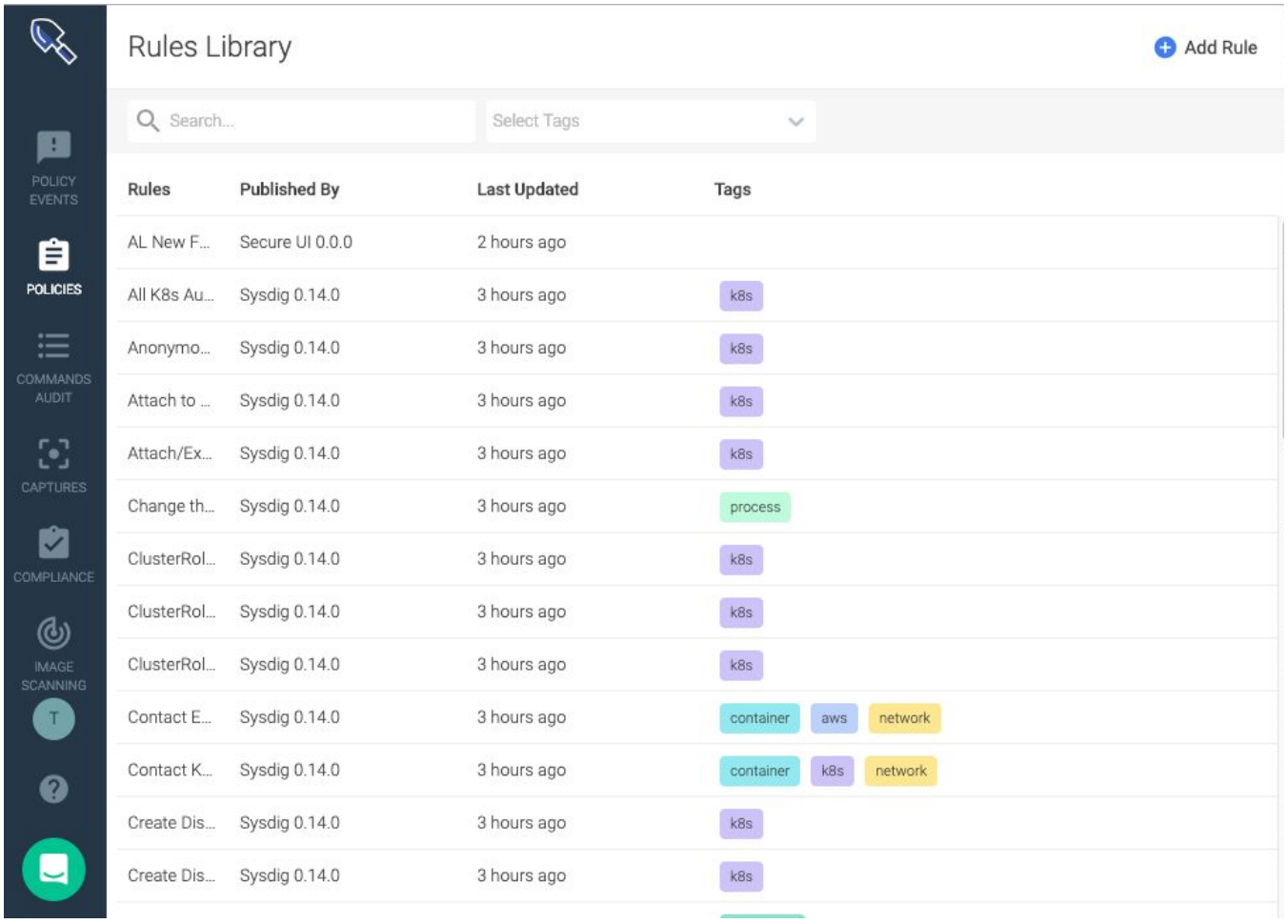
システムコールルールタイプは、ユーザーが作成したポリシーにはほとんどデプロイされません。以下の定義は情報提供のみを目的としています。

これらのルールは（内部的に）使用され：

- 特定のsyscallがリストで発生した場合に通知する
- 信頼できるリスト以外のシステムコールが環境で発生した場合に通知する

ルールライブラリについて

ルールライブラリには、ポリシーで参照できるすべての作成済みルールが含まれています。 Sysdigの脅威調査チーム、Falcoのオープンソースコミュニティルール、およびCISやMITER ATT&CKなどの国際的なセキュリティベンチマークによって開発されたコンテナ固有のルール（および定義済みポリシー）を備えた包括的なランタイムセキュリティライブラリを提供します。



監査に適した機能

ルールライブラリインターフェースでは、一目で以下を確認できます。

- 発行者：
- 最終更新日

により、トレーサビリティと監査が強化されています。

タグ

ルールはタグで分類されているため、機能、セキュリティ標準、ターゲット、または組織にとって意味のあるスキーマでグループ化できます。

さまざまなタグが事前定義されており、ポリシーを作成または編集するときにルールを論理グループとして整理するのに役立ちます。

検索

上部の検索ボックスを使用して、ルール名またはタグで検索します。

Sysdig Secure内でFalcoを使用する

Falcoとは

Falcoは、オープンソースの侵入検知およびアクティビティ監視プロジェクトです。 Sysdigによって設計されたこのプロジェクトは、クラウドネイティブコンピューティング財団に寄付されており、コミュニティによって引き続き開発および強化されています。 Sysdig Secureは、ポリシーおよびコンプライアンスモジュールの一部としてFalcoルールエンジンを組み込んでいます。

Sysdig Secureのコンテキスト内で、ほとんどのユーザーは、主に環境のポリシーにデプロイされたルールを作成またはカスタマイズすることでFalcoと対話します。

Falcoルールは、アラートを生成する条件と、アラートとともに送信する出力文字列で構成されます。

条件

- Falcoルールは、Sysdigフィルタリング構文を使用します。
  （Falcoの残りのドキュメントの多くは、ほとんどのSysdig Secureユーザーには適用されない自立型ツールとしてのインストールと使用について説明しています。）

- ルール条件は通常、マクロとリストで構成されます。

- マクロ は、ルールやその他のマクロ内で再利用できる単純なルール条件スニペットであり、一般的なパターンを除外して名前を付ける方法を提供します。
- リストリスト は、ルール、マクロ、または他のリストに含めることができるアイテムのです（サプライズ！）。ルール/マクロとは異なり、Sysdigフィルタリング式として解析することはできません。

背後ににおいて、 falco_rules.yaml ファイルには、Falcoマクロやリストなど、環境内のすべてのFalcoルールの未加工コードが含まれています。

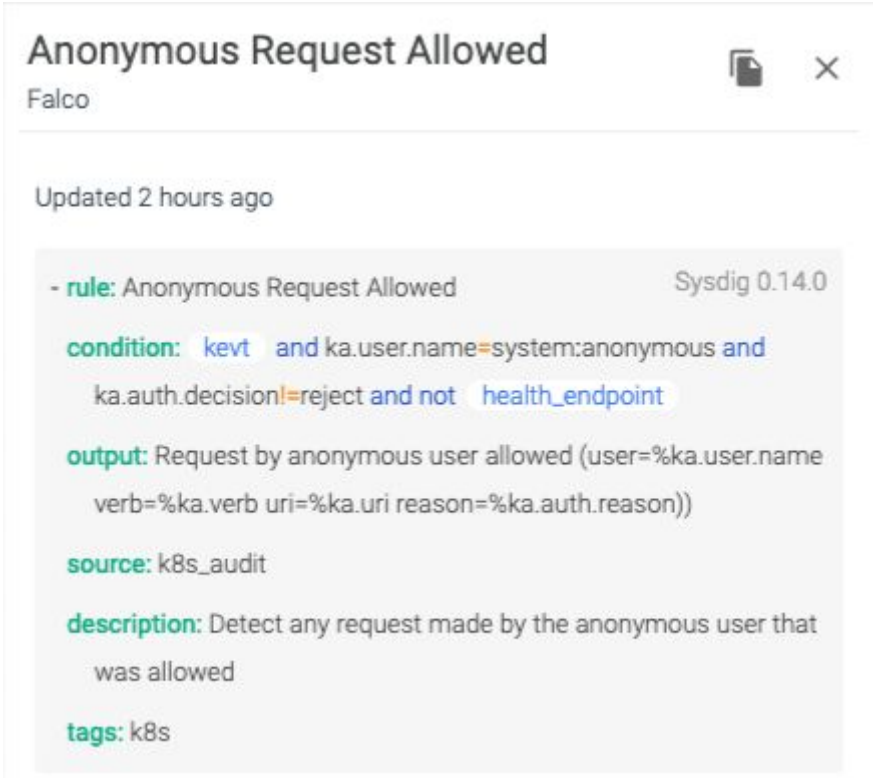
Falcoルールの構造

すべてファルコルール、以下の基本パラメータを含みます：

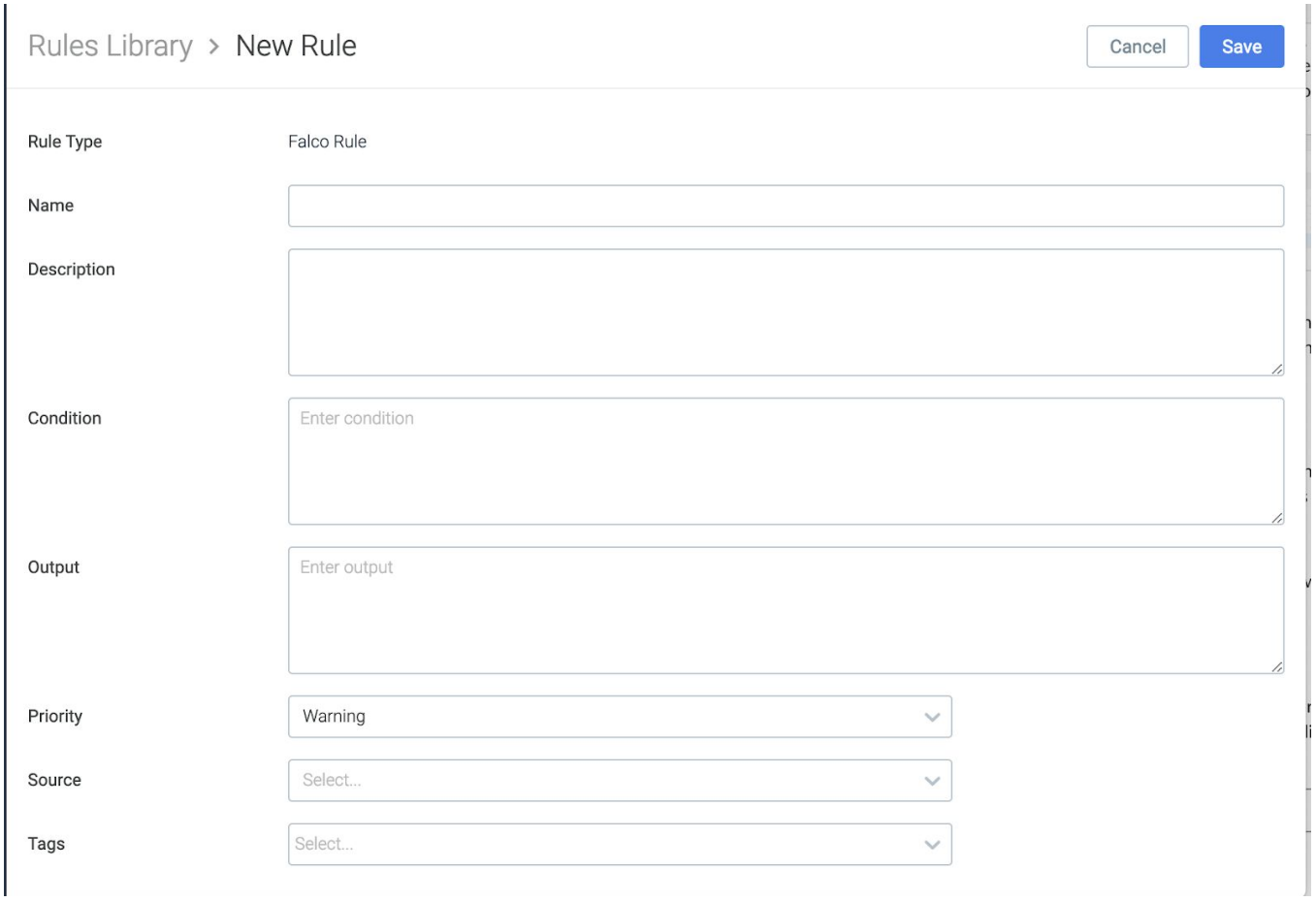
- **rule name**： デフォルトまたはユーザーが割り当てます
- **condition**： ルール作成に使用されるフィールドおよび引数のコマンドラインコレクション
- **output**：
- **source**：
- **description**：
- **tags**： 検索およびソート用
- **priority**：

ルールライブラリからルールを選択して、その基本構造を表示または編集します。 新しいFalcoルールを作成し、それをライブラリに追加するときにも同じ構造が適用されます。

既存ルール


Anonymous Request Allowed
Falco
Updated 2 hours ago
- rule: Anonymous Request Allowed
Sysdig 0.14.0
condition: kevt and ka.user.name=system:anonymous and ka.auth.decision!=reject and not health_endpoint
output: Request by anonymous user allowed (user=%ka.user.name verb=%ka.verb uri=%ka.uri reason=%ka.auth.reason))
source: k8s_audit
description: Detect any request made by the anonymous user that was allowed
tags: k8s

ルールの作成



注意

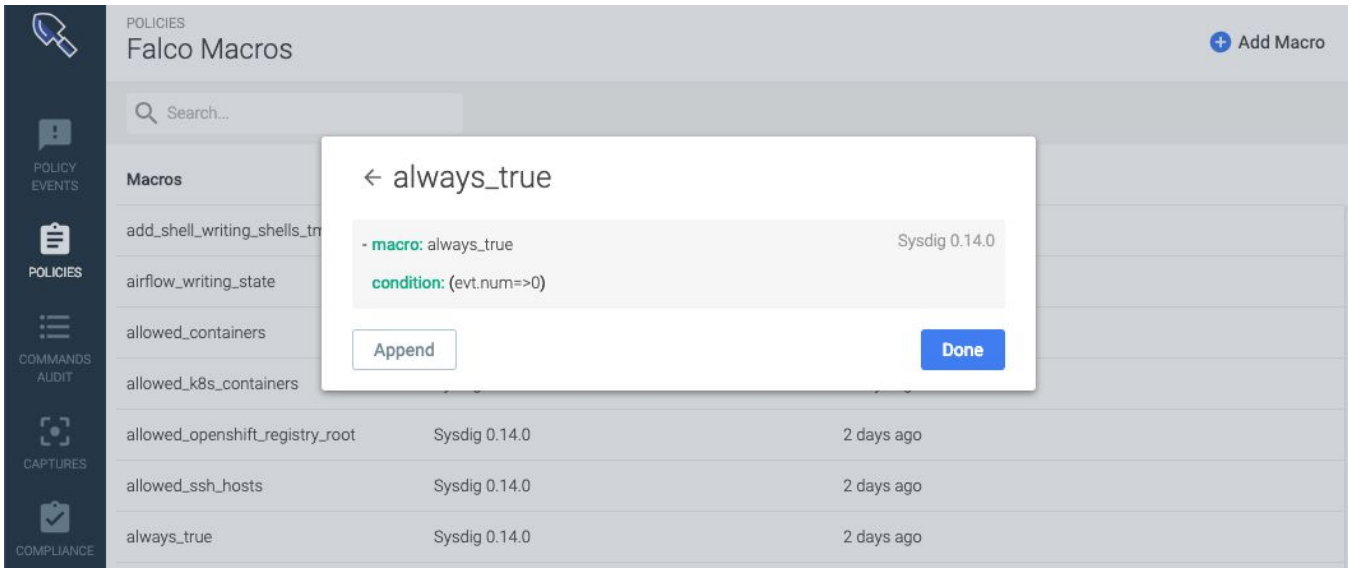
k8s_auditのFalcoルールでは、使用するためにはKubernetes audit ログを有効にする必要があります。

Falcoマクロについて

ルールライブラリのFalcoルールの多くには、条件コードにFalcoマクロが含まれています。

Falcoマクロリストを参照したり、マクロの基になるコードを調べたり、独自のマクロを作成したりできます。デフォルトのFalcoルールセットは、ルールの記述を開始しやすくする多数のマクロを定義し

ます。これらのマクロは、多くの一般的なシナリオのショートカットを提供し、ユーザー定義のルールセットで使用できます。



Sysdig Secureポリシーおよびルールに含まれるデフォルトマクロの動作をオーバーライドするには、使用し ルールエディターが使用できます。

Falcoリストについて

デフォルトのFalcoリストが追加され、環境のカスタムルールの記述に関するユーザーエクスペリエンスが向上しました。

たとえば、リスト`allow.inbound.source.domains`はカスタマイズでき、ルール内で簡単に参照できます。

（On-Premのみ）ルールインストーラーを使用してFalcoルールをアップグレード

Sysdig Secure SaaSは、常に最新のFalcoルールセットを使用しています。

Sysdig Secure On-Premの場合は、Falcoルールセットを定期的にアップグレードする必要があります。

ルールインストーラー

Docker pullコマンドと手順は、ルールインストーラー
(https://hub.docker.com/r/sysdig/falco_rules_installer)をご参照ください。

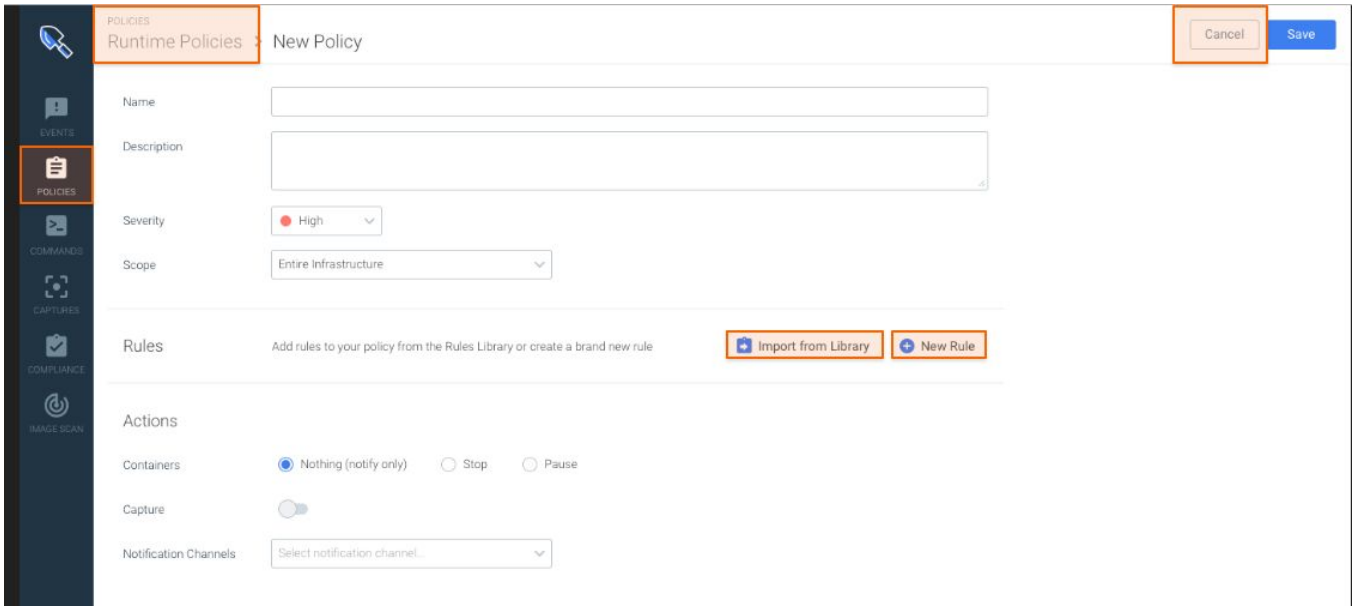
ポリシーの管理

ルールは、ランタイムポリシーに追加されるまで実行できません。

ポリシーを作成する

1. [`Policies`]を選択し、[`+Add Policy`]をクリックします。
2. 以下の説明に従ってフォームに入力し、[`Save`]をクリックします。

以下の手順は、基本パラメーター、ルール、およびアクションに分かれています。



基本パラメーターの定義

- 名前と説明：意味のある検索可能な記述子を提供します
- ポリシーの重大度：ランタイムポリシーUIで表示する適切な重大度レベルを選択します。

  ポリシーの重大度は主観的であり、Sysdig Secureインスタンス内のポリシーをグループ化するために使用されます。

  注：基本となるルールの優先度とポリシーに割り当てる重大度の間には継承はありません。

- ポリシーのスコープ：ポリシーが適用されるスコープを定義します。 例：

- cluster.nameコンテナが「Prod」のクラスタにのみPrivileged Containerポリシーを適用します
- Shell in Containerポリシーのみをkubernetes.namespace.name = billingに適用します

注意

ポリシーの処理を簡素化するために、ポリシーを複製して別のスコープを割り当てると便利な場合があります。

ルールの追加

ライブラリから既存のルールを選択するか、その場で新しいルールを作成してポリシーに追加できます。

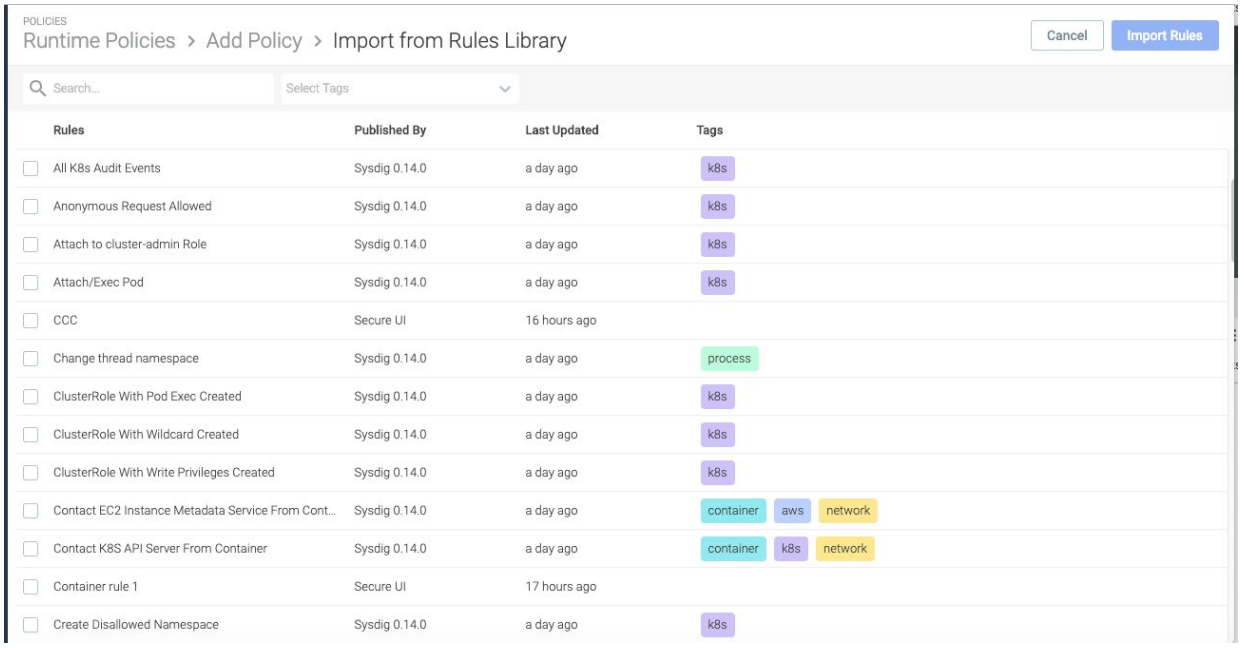
Policy Editorインターフェースは、ポリシーにルールを追加したり、ポリシーからルールを削除したりするための多くの柔軟な方法を提供します。 以下の手順は1つの方法を示しています。

参照：ルールの管理

ライブラリからインポート

1. [**New Policy**]（または[ポEdit Policy]）ページで、[`Import from Library`]をクリックします。

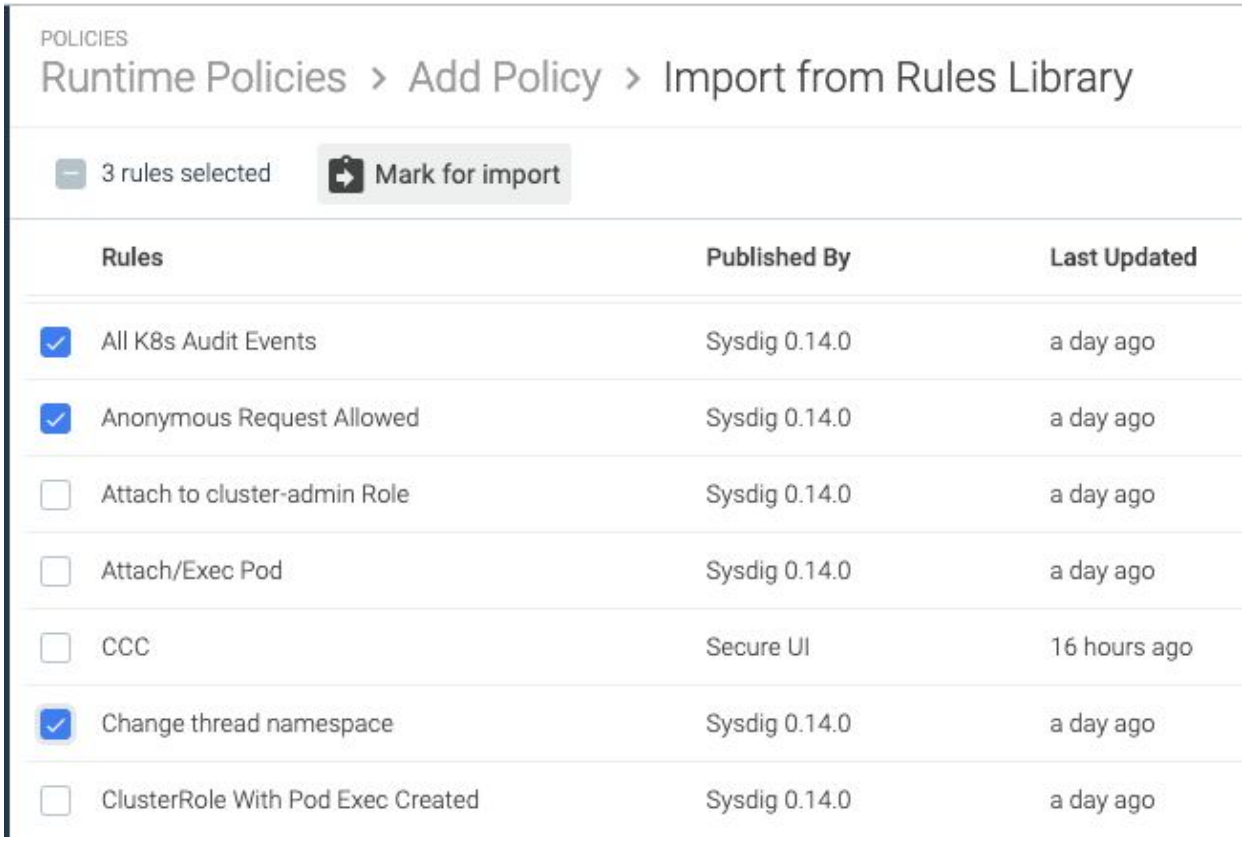
[**Import from Rules Library**]ページが表示されます。



2. インポートするルールのチェックボックスを選択します。

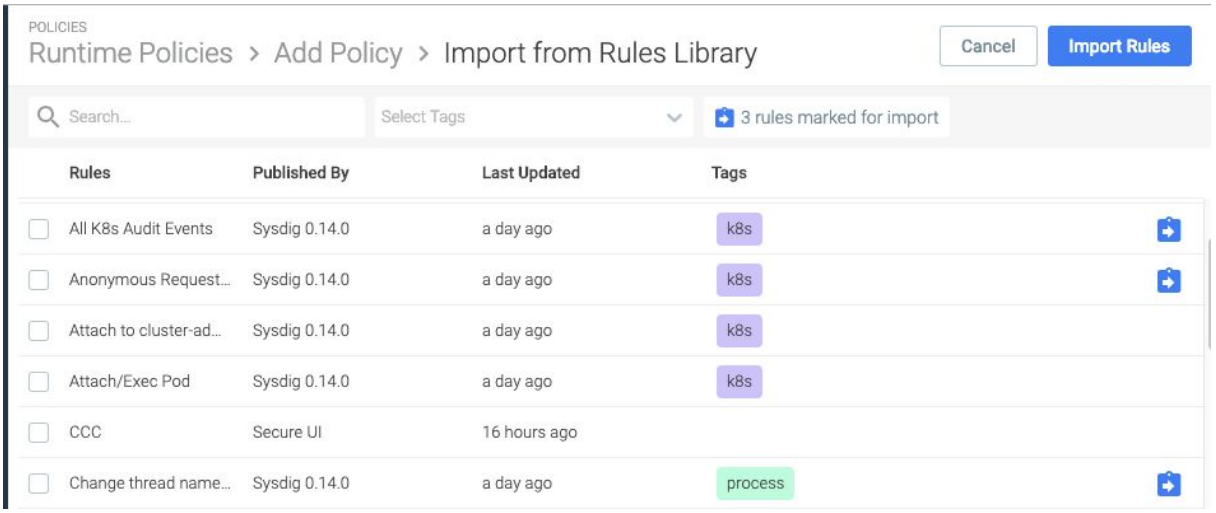
> **ヒント**
>
> 特定のキーワードまたはタグを検索するか、色付きのタグアイコンをクリックして、ルールのコレクションを事前にソートできます。

3. Mark for Importをクリック



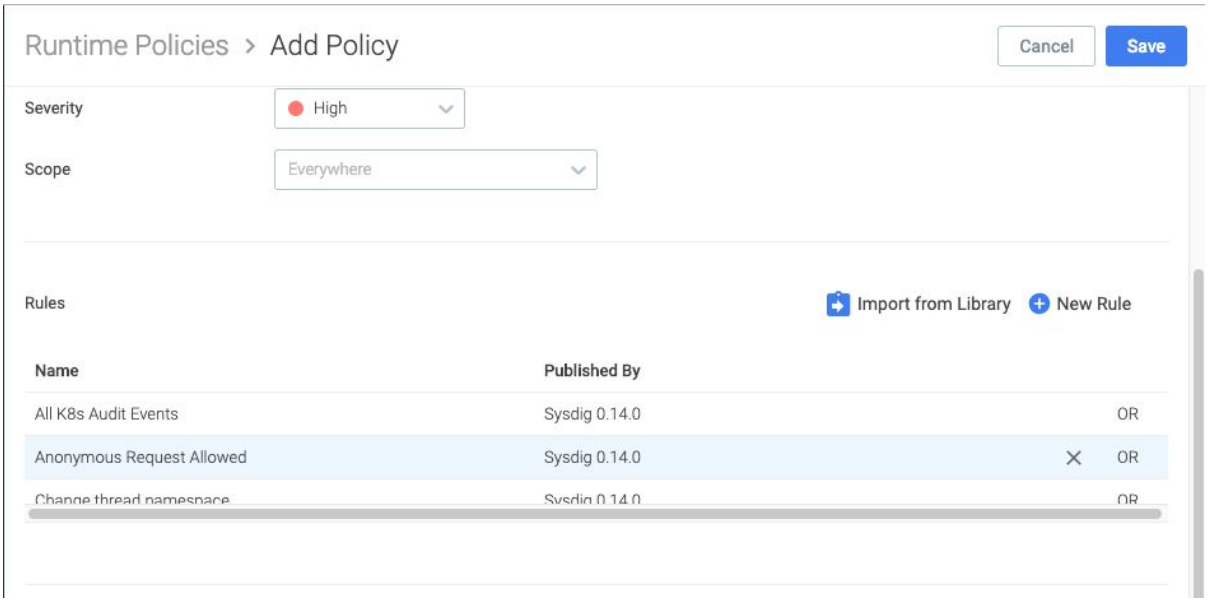
青い`Import`アイコン

選択したルールの右側に表示され、[`Import Rules`]ボタンがアクティブになります。



4. [Import Rules]をクリックします。

[Policy]ページが表示され、選択したルールが一覧表示されます。



ヒント

リスト内のルールの横にあるXをクリックすると、ポリシーからルールを削除できます。

ポリシーエディターからルールを作成する

[Import from Library]ではなく[New Rule]をクリックすると、ルールの作成で説明されている手順にリンクされます。

アクションの定義

ポリシーに違反した場合の対処方法を決定します。

- コンテナ：ポリシールールに違反した場合、影響を受けるコンテナに何が起こるかを選択します。
  - `Nothing (alert only)`：コンテナの動作を変更しないでください。通知チャネル設定に従って通知を送信します。
  - `Stop`：実行中の1つ以上のコンテナーを停止/強制終了します。
  - **`Pause`**：指定したコンテナ内のすべてのプロセスを一時停止します。
- キャプチャ：イベント発生時にキャプチャを作成する場合はキャプチャをオンに切り替え、スナップショットにあるイベントの前後の秒数を定義します。

  参照：キャプチャ

- 通知チャネル：イベントの通知を適切な担当者に送信するために、ドロップダウンリストから通知チャネルを選択します。

  参照：通知チャネルの設定

ポリシーを編集する

デフォルトポリシーとユーザー定義ポリシーの両方を自由に編集できます。上記で定義したように、ポリシーを選択して詳細を表示します。

ポリシーを削除する

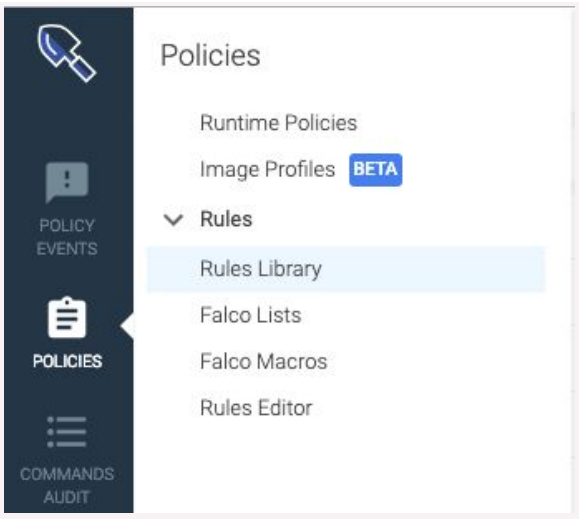
ポリシーは、Sysdig Secureが最初にインストールされたときにのみ自動インストールされます。デフォルトのポリシーを削除してからアップグレードした場合、そのポリシーは再作成されません。

ルールの管理

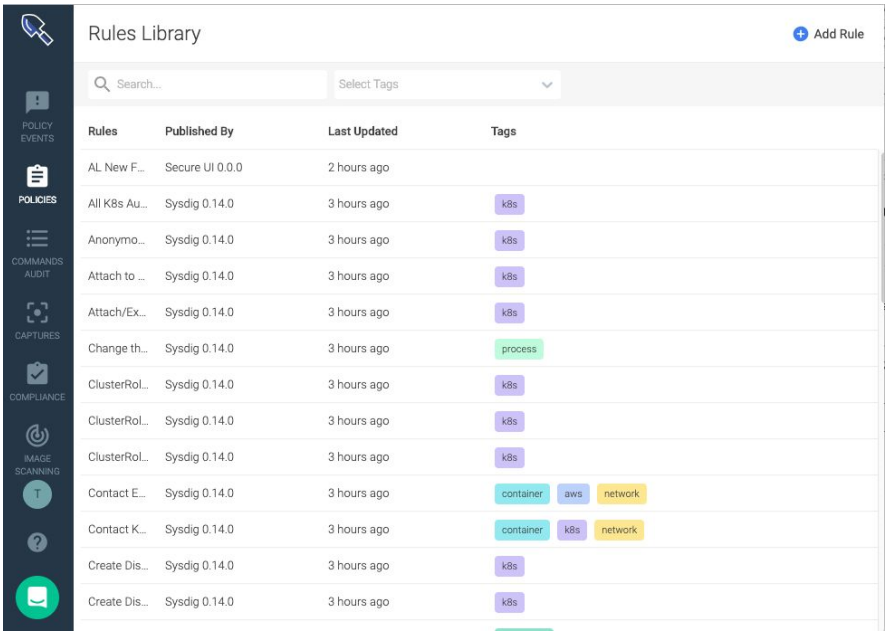
Sysdig Secure Rulesを理解しましょう。特にRules Libraryの理解を確認して開始してください。

ルールライブラリにアクセスする

1. `Policies > Rules Library`を選択します。



2. ルールライブラリが表示されます。

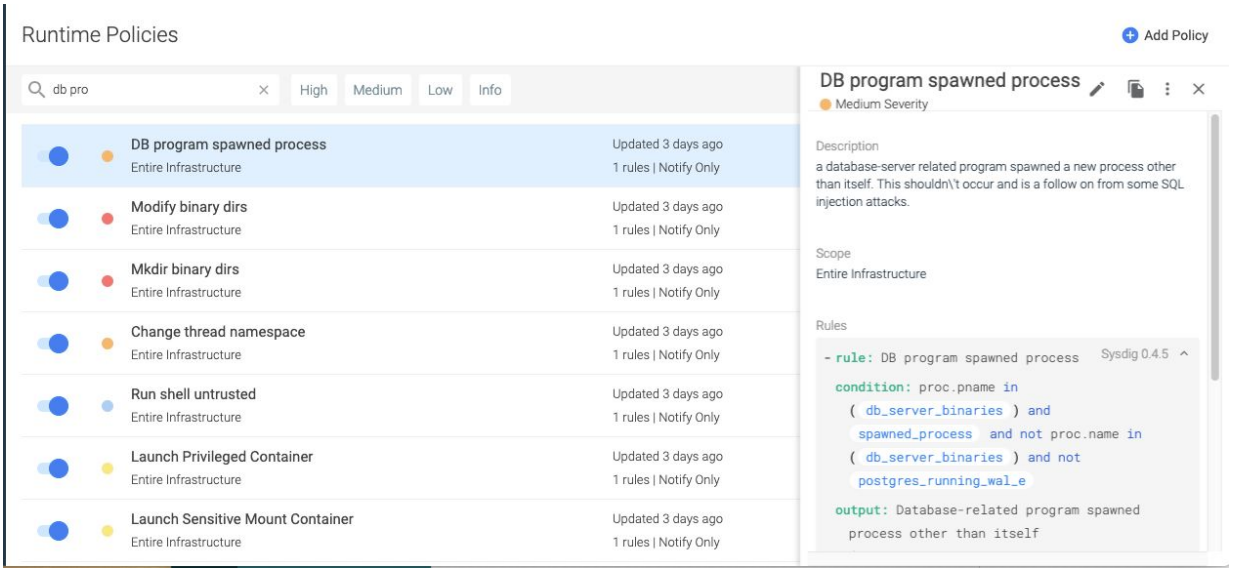


ルールを編集する

Sysdigによって公開されたルールはデフォルトであり、読み取り専用です。リストとマクロに追加できますが、コアパラメーターは変更できません。デフォルトのルールは削除できません。

自作のルールは自由に編集できます。

1. [`Policies`]> [`Rules Library`]を選択し、ルールを選択します。
2. **Rule Details**パネルが右側に開きます。 必要に応じて、パラメーターを確認し、インラインでマクロとリストに追加できます。



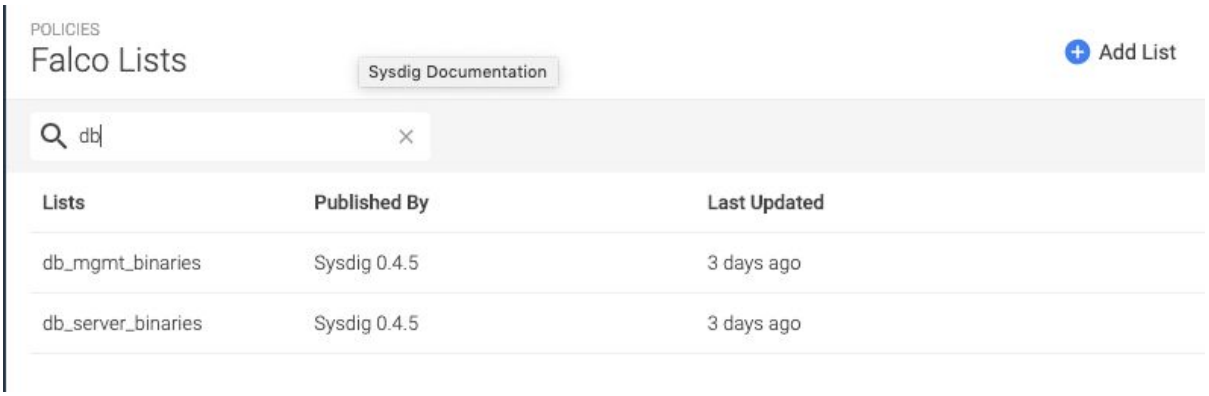
Falcoマクロとリストに追加する

デフォルトのFalcoルールには、さまざまなマクロとリストが埋め込まれています。 これらはデフォルトルールから削除できませんが、追加情報を追加できます。

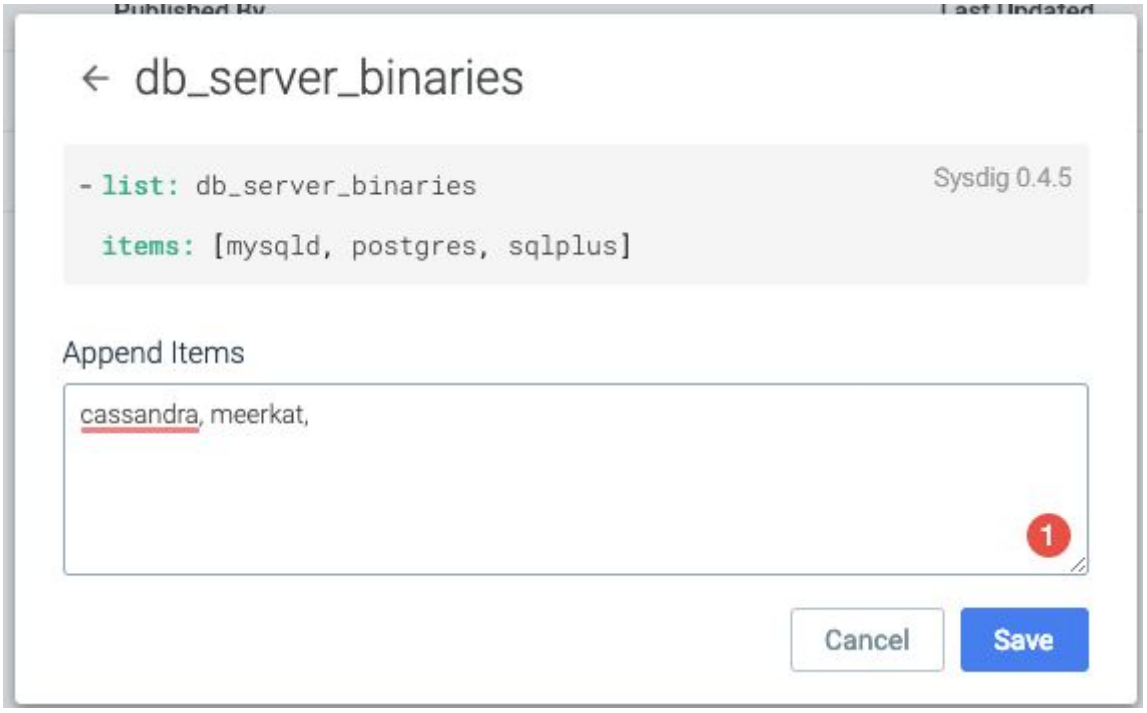
たとえば、上記のスクリーンショットのPolicy DB Program Spawned Processを検討してください。 組み込みルールは、データベースが不正プロセスを引き起こしていないことを確認するために使用されます。 ルール条件でFalcoリストdb_server_binariesを確認できます。

デフォルトのリストにアイテムを追加するには：

1. ルール条件の青いリストテキストをクリックするか、[Policies]>[Falco Lists]に移動して、名前で検索します。



2. リストの内容が表示されます。Appendをクリックします。



3. ルールに含める追加のアイテム（データベースなど）を入力し、[Save]をクリックします。

   同じプロセスがマクロに適用されます。

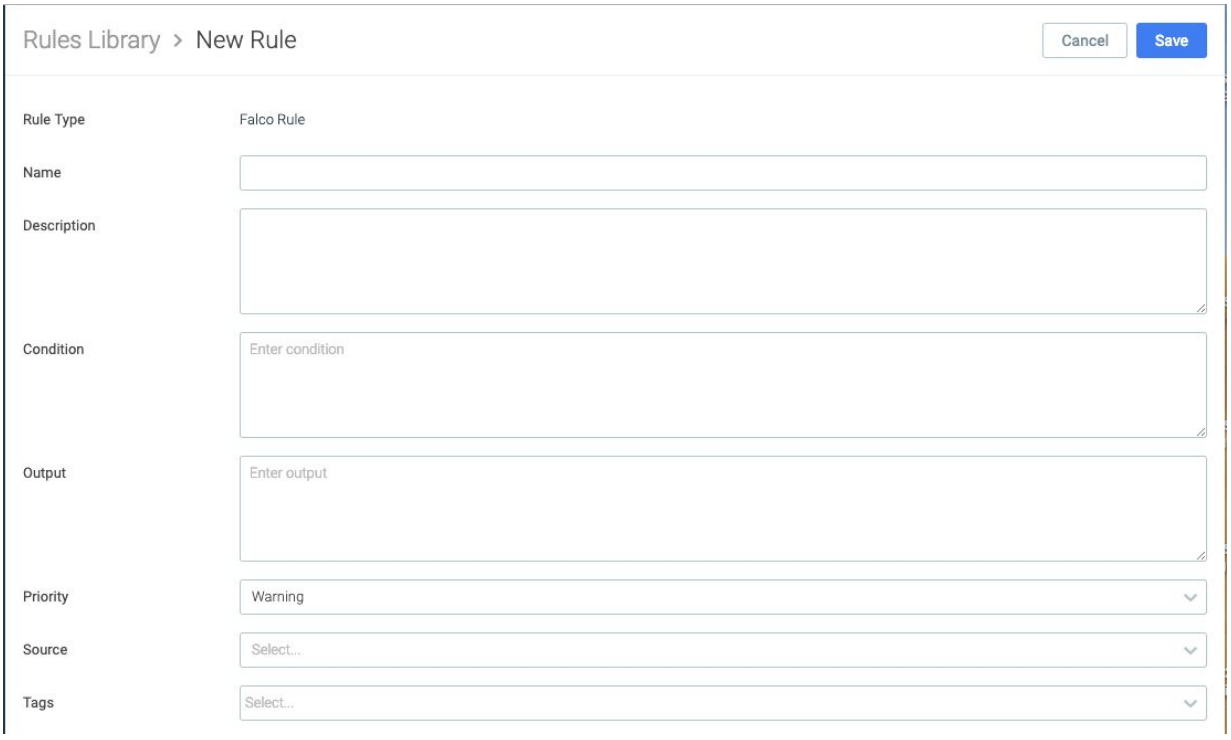
ルールを作成する

Falcoルールとファストルールを作成するためのさまざまなインターフェイスがあります。

Falcoルールを作成する

1. [**Rules Library**]ページで、[`+Add Rule`]をクリックし、ドロップダウンから[Falco]を選択します。

   Falcoルールタイプの[**New Rule**]ページが表示されます。

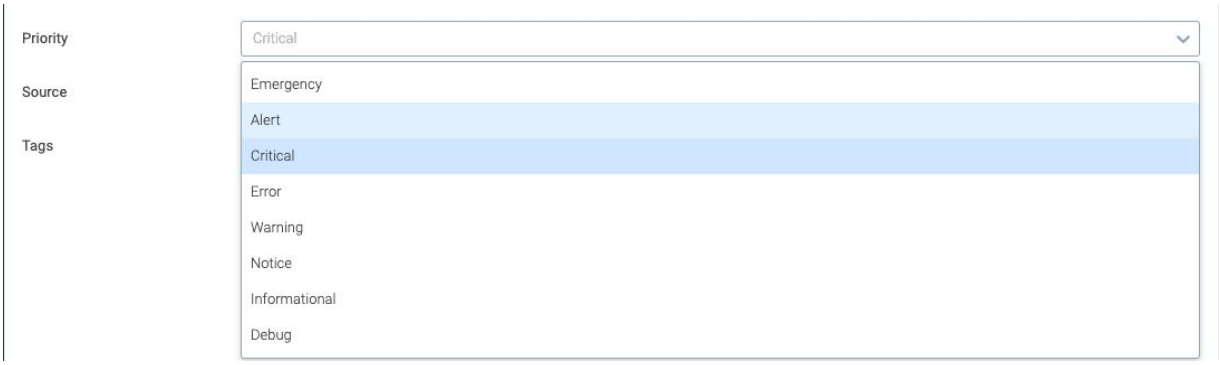


2. パラメーターを入力します。

   Name and Description：ルールの名前と意味のある説明を作成します

   Condition and Output：必要な条件コードと出力を記述します。 詳細については、サポートされているフィールド(https://falco.org/docs/rules/supported-fields/)を参照してください。

Priority：これは、Falcoルールの構文を満たすための必須フィールドです。



Source：ルールがKubernetes Auditデータソースまたは標準のsyscallメカニズムを使用してイベントを検出するかどうかを定義します

Tags：ドロップダウンから関連するタグを選択するか、独自のカスタムタグを追加します

3. `Save`をクリック

> **注意**
>
> ソースk8s_auditのFalcoルールでは、使用するためにKubernetes Auditログを有効にする必要があります。

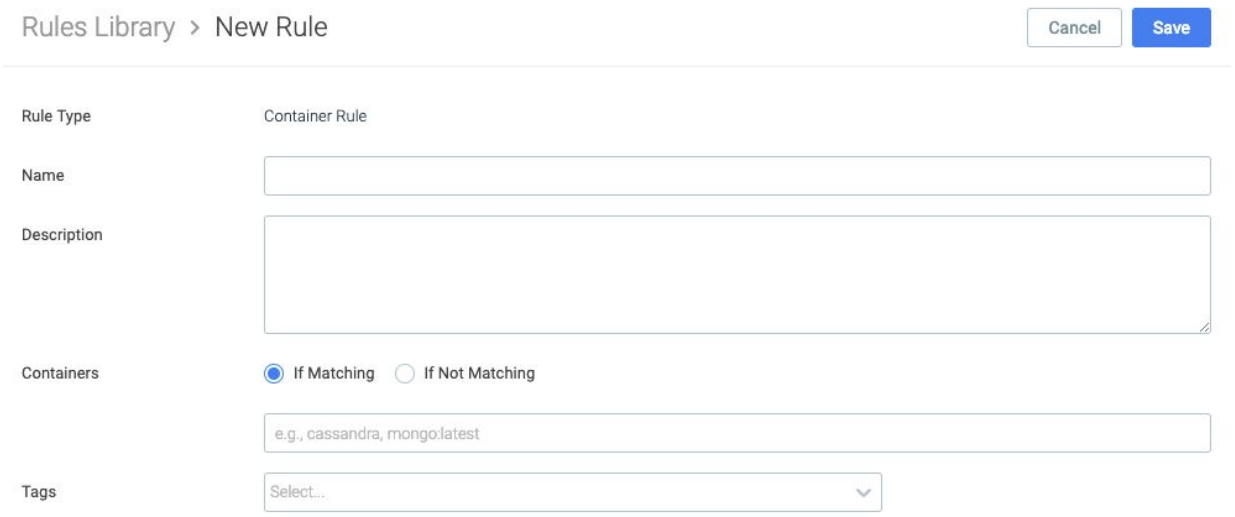
ファストルールの作成：コンテナタイプ

ファストルールは、本質的にホワイトリスト/ブラックリストルールです。

環境で許可される特定のCassandraデータベースイメージを項目化し、指定されていないものをブラックリストに登録するとします。この場合、コンテナルールが適切です。（他のファストルールタイプには、タイプに応じて同様の入力フィールドがあります。）

1. [Rules Library]ページで、[`+Add Rule`]をクリックし、ドロップダウンから[`Container`]を選択します。

コンテナルールタイプの[New Rule]ページが表示されます。



2. パラメーターを入力します。

   Name：名前を入力します例： Cassandraイメージを許可しました。

   Description：説明を入力します。 許可されているCassandraイメージのリスト。 ブラックリストに登録される他のすべて

   If Matching/ If Not Matching：この場合、[`If Not Matching`]を選択して、以下のエントリと一致しないCassandraコンテナのブラックリストアクションを自動的にトリガーします。

   Containers：許可されているCassandraコンテナー名を追加します。 例: cassandra.myorg.3.0

   Tags：ドロップダウンから関連するタグを選択します。 データベースとコンテナ。

3. 保存をクリックします。

[ベータ] ポリシーアドバイザー

Sysdig Secureは、ポリシーアドバイザーと呼ばれるKubernetesセキュリティを強化するためのツールを導入しました。現時点では、Kubernetesポッドセキュリティポリシー専用です。

[ベータ] ポッドセキュリティポリシー（PSP）

Kubernetesによると、「ポッドセキュリティポリシー[PSP]は、ポッド仕様のセキュリティセンシティブな側面をコントロールするクラスターレベルのリソースです。PodSecurityPolicyオブジェクトは、ポッドがシステムに受け入れられるために実行する必要がある一連の条件と、関連フィールドのデフォルトを定義します。」

詳細は、Kubernetes PSPのドキュメント(https://kubernetes.io/docs/concepts/policy/pod-security-policy/)をご覧ください。

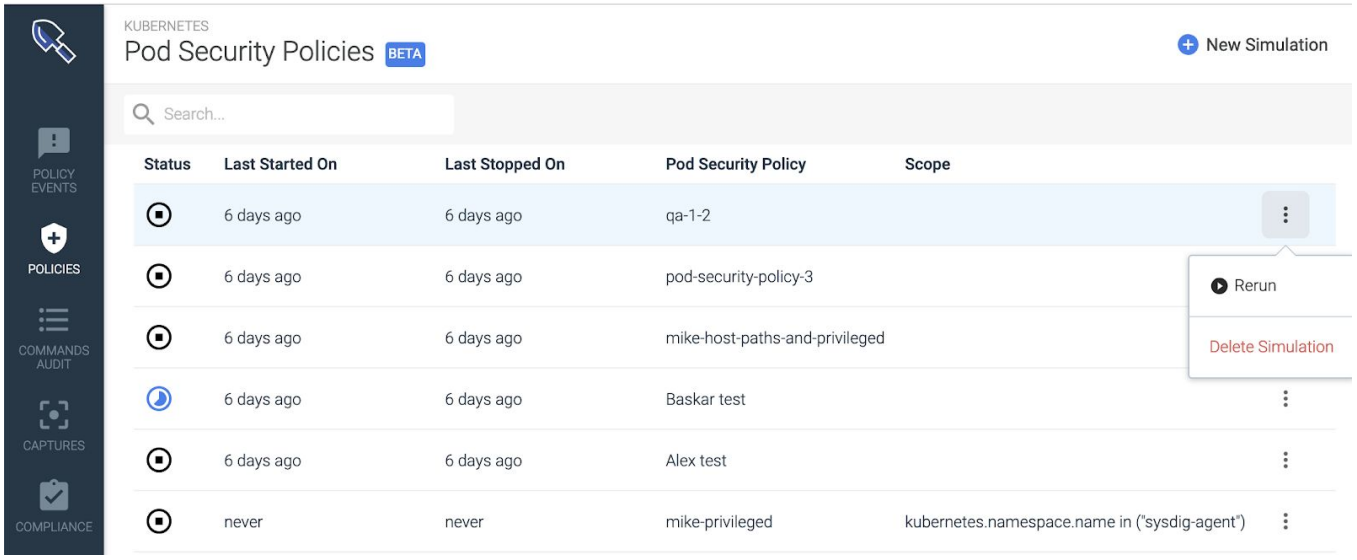
SysdigのKubernetes Policy Advisorを使用すると、ポッドセキュリティポリシーを自動生成し、それらを環境にコミットする前にそれらのドライテストまたは「シミュレーション」を実行できます。これらの機能にはいくつかの利点があります。

- PSPはセキュリティを強化するために最小特権を強制するのに役立ちます
- 自動生成により、Kubernetesポリシーの構成にかかる時間を大幅に短縮できます
- シミュレーションテストは、チームがPSPを調整して誤検知を回避し、PSPのデプロイメント中にアプリケーションが破損するのを防ぐのに役立ちます。

PSPワークフローを理解する

一般に、PSPを生成し、シミュレーションテストを実行し、結果を確認し、必要に応じてPSPを調整してから、シミュレーターをオフにして、実際のデプロイメントにポッドセキュリティポリシーを追加

します。



前提条件

- Kubernetes上のSysdig Secure v3.0+およびSysdig Agent v93.0+
- SysdigでKubernetes Audit Loggingを有効にする必要があります

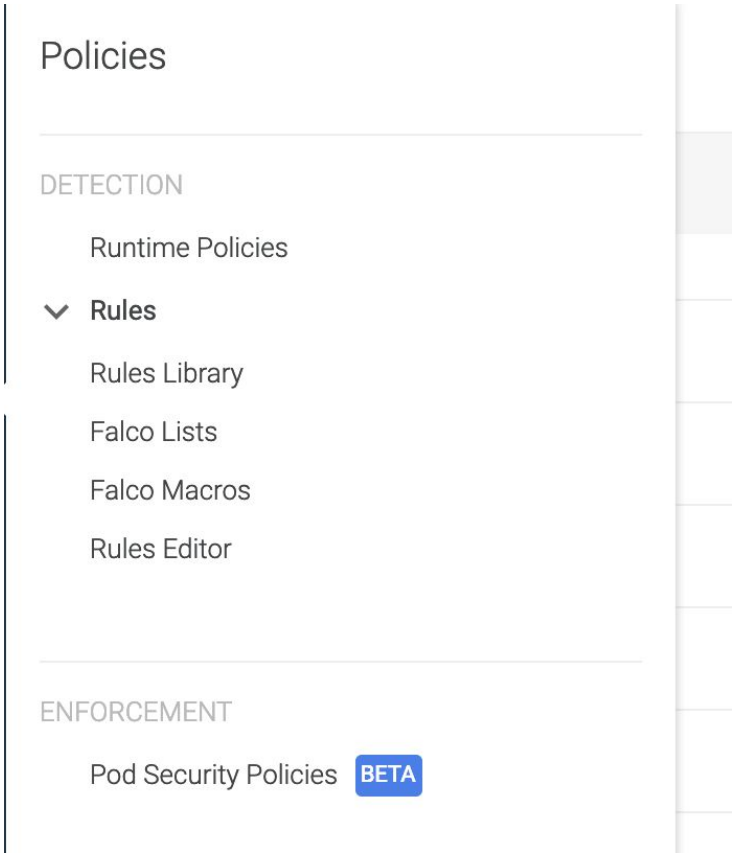
用語

Kubernetes Podセキュリティポリシーは、標準のSysdigセキュアポリシーとは異なり、通常のポリシーリストページには表示されないことに注意してください。

手順

通常、ワークフローは次のように進行します。

1. [**Policies**]> [**Pod Security Policies**]でモジュールにアクセスします。



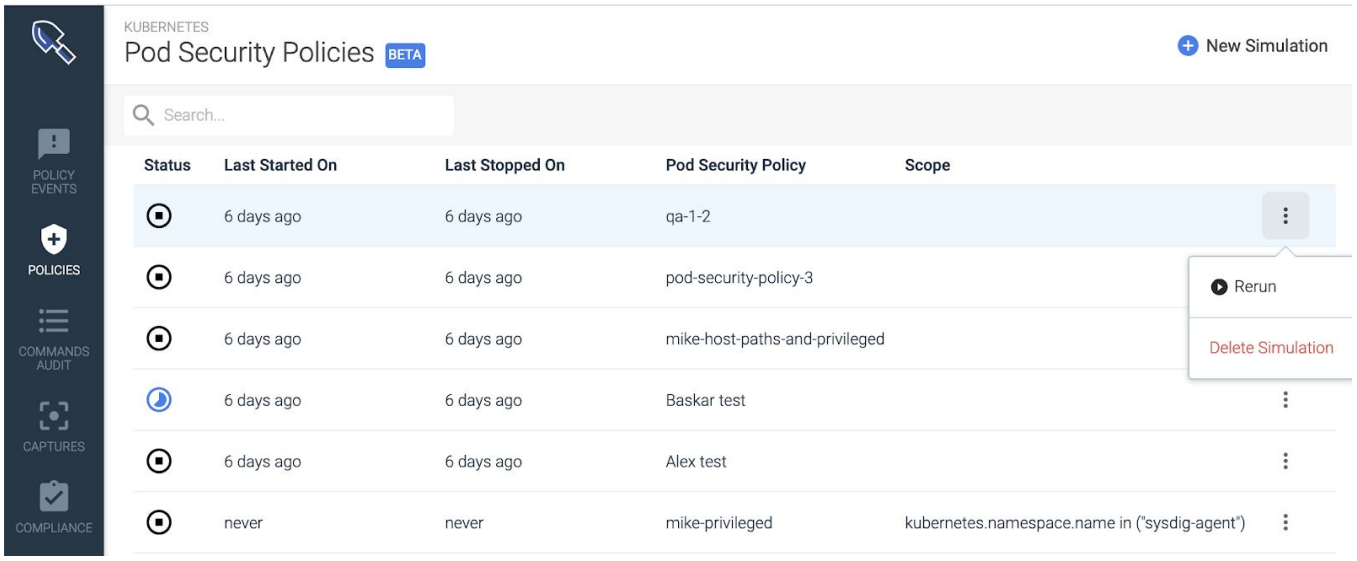
2. テストするポッドセキュリティポリシールールを作成します。既存のPSPをアップロードするか、ツールがPSPコンテンツを自動生成するyaml デプロイメントファイルをアップロードします。
3. **Start Simulation**をクリックします。
4. 環境内の適切なクラスターにポッドをデプロイします。 シミュレータが実行されているため、ドライテストとしてデプロイされ、結果のアラートがトリガーされます。
5. シミュレーション出力を確認し、必要に応じてPSPコンテンツを微調整します。
6. PSPルールが目的どおりに実行されたことを確認したら、[**Stop Simulation**]をクリックします。
7. これで、このPSPをクラスターに適用する準備ができました。 https://kubernetes.io/docs/concepts/policy/pod-security-policy/#enabling-pod-security-policies を参照してください。

ポッドセキュリティポリシーシミュレーションの管理

ポッドセキュリティポリシーのランディングページを確認する

[Policies]> [Pod Security Policies]からモジュールにアクセスします。

Pod Security Policies listページが表示されます。



少なくとも1つのシミュレーションが生成されると、リストにコンテンツが含まれます。

次の概要機能に注目してください。

- **Search Bar**：検索は、**Pod Security Policy column**に表示されるPSP **names**l の単語または文字で実行されます。
- **Status**：これは、PSP名に関連付けられたシミュレーションのステータスです。 Running または Stopped のいずれかです。

  シミュレーションは、手動で停止するまで継続的に実行されることに注意してください。「Running」記号は、「amount completed」を示していません。

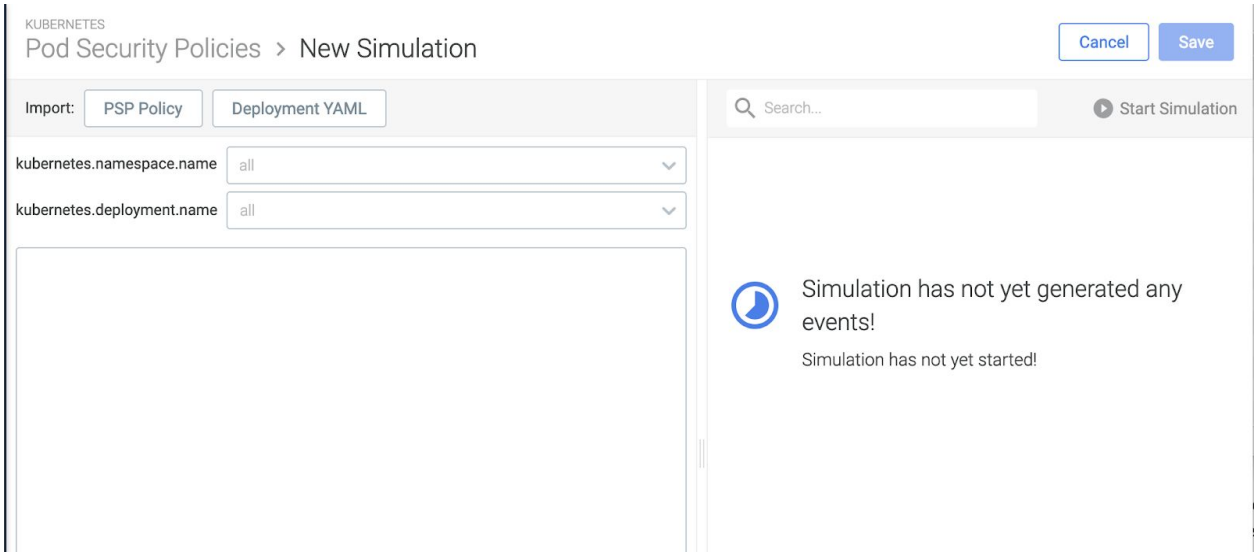
- **Pod Security Policy (name)**：PSP名は、自動的に継承されるか、アップロードされたPSPコンテンツの名前パラメーターから生成されます。 nameパラメーターを使用して、このタイトルを編集できます。

- **Scope**：[Scope]列には、シミュレーション用に定義されたKubernetes ネームスペース名とデプロイメント名が反映されます。
- **Rerun | Stop | Delete Simulation links**：右側の3つのドットを使用して、停止したシミュレーションを再実行、実行中のシミュレーションを停止、またはシステムからシミュレーションを削除します。

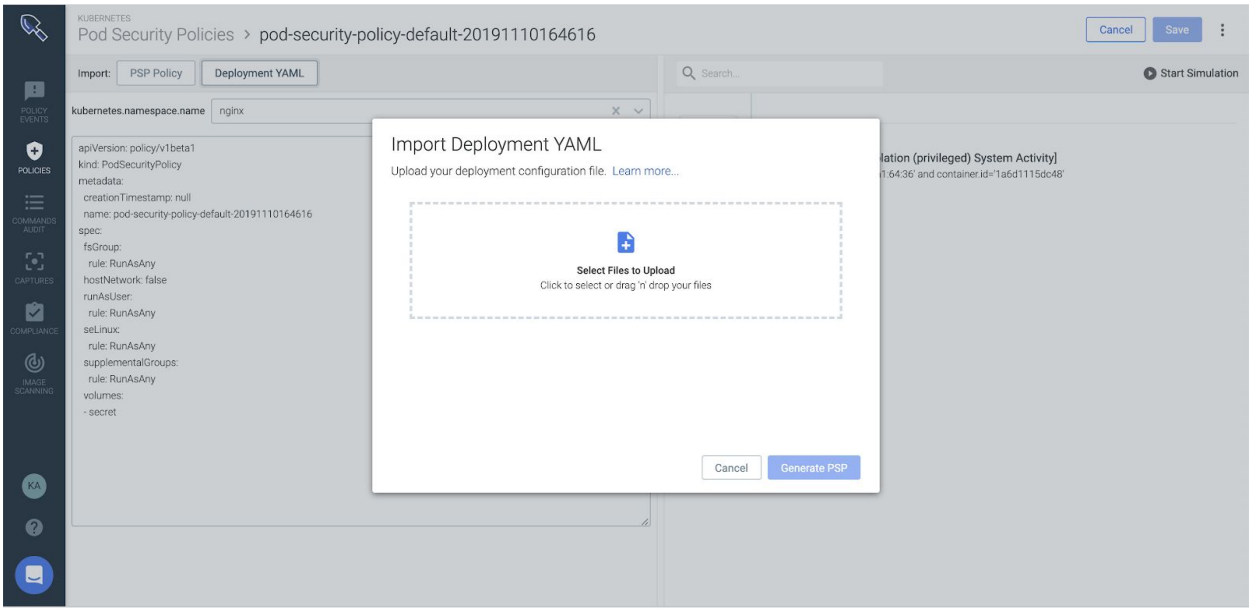
PSPシミュレーションを生成する

1. [Policies]> [Pod Security Policies]を選択し、[**New Simulation**]をクリックします。

   [New Simulation]ページが表示されます。



2. [Import]ボタンを使用して、既存のPSPポリシーまたはデプロイメントYAMLファイルをアップロードします。



3. [Generate PSP]をクリックします。

   PSPルールの内容は、下のテキストボックスに表示されます。 YAMLファイルを使用した場合、PSPルールのコンテンツはそのファイルから自動生成されて表示されます。

4. シミュレートされたPSPを実行するクラスターのnamespace.nameまたはdeployment.nameを入力するか、「all」を選択します。
5. **Save**をクリックします。

   PSPシミュレーションが定義され、PSPリストページに表示されます。

シミュレーションを実行し、出力イベントを確認する

1. PSPシミュレーションを生成したら、[**Start Simulation**]をクリックして開始します。

   メインのリストページまたはシミュレーションの詳細ページから[Start]ボタンにアクセスできます。

2. PSPをシミュレーターがテストする指定された環境にデプロイします。
3. 生成されたイベント出力を確認するには、実行中にシミュレーションを選択します。
4. 必要に応じてルールを編集し、必要に応じてシミュレーションを再開します。

シミュレーションを停止する

PSPテストの動作に満足したら。**Stop Simulation**をクリックします。

これで、このPSPをクラスターに適用する準備ができました。
https://kubernetes.io/docs/concepts/policy/pod-security-policy/#enabling-pod-security-policiesを参照してください。