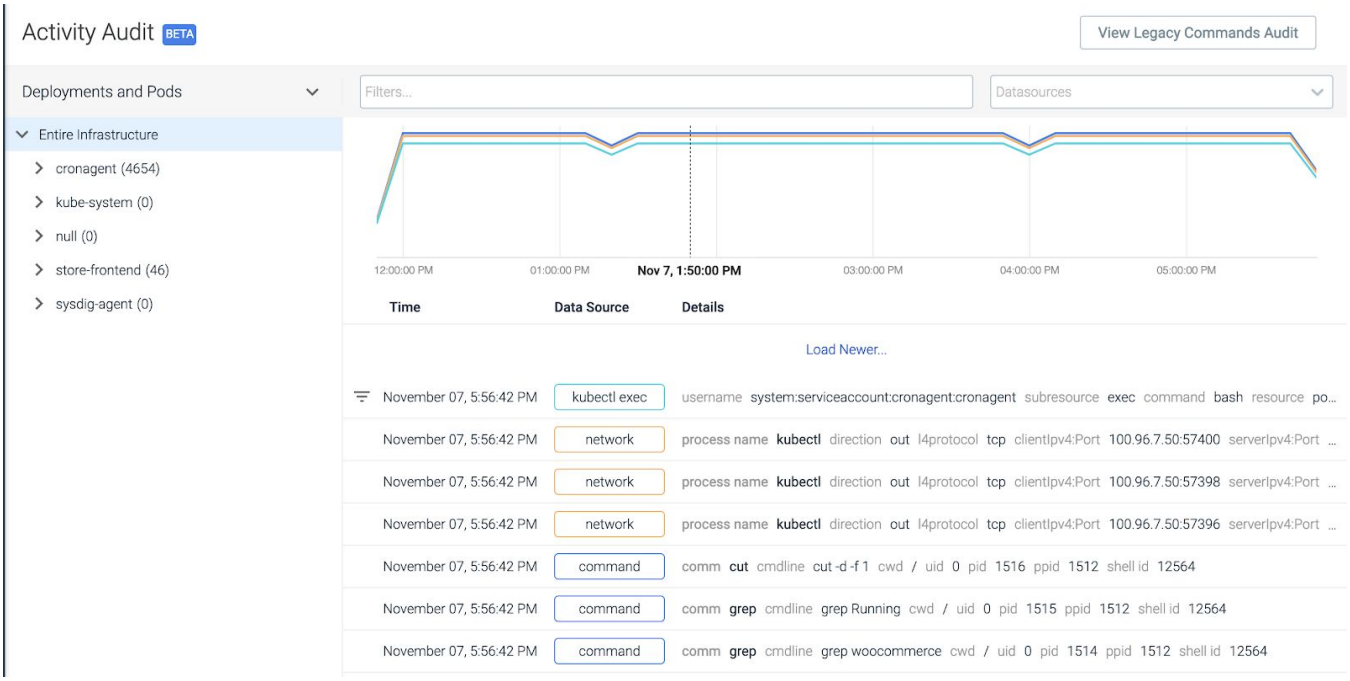
[Beta] Activity Audit
アクティビティ監査

本文の内容は、ベータ版としてリリースしていますActivity Auditのドキュメント(https://docs.sysdig.com/en/-beta--activity-audit.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。

アクティビティ監査について

アクティビティ監査は、キャプチャから価値の高いデータを取得し、常に有効にして検索可能にし、クラウド固有のアセットに対してインデックスを作成します。このストリームには、実行されたコマンド、ネットワークアクティビティ、およびKubernetes APIへのkube exec リクエストが含まれます。



アクティビティ監査の使用方法を理解する

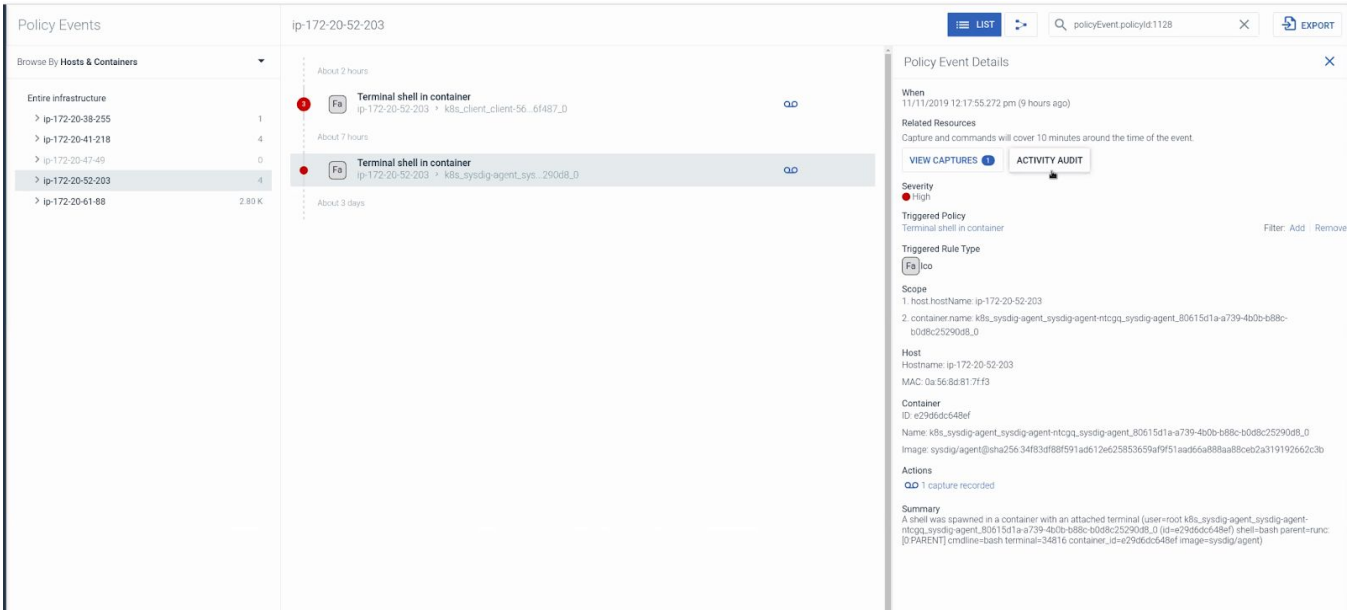
アクティビティ監査を使用すると、ユーザーはさまざまなデータソースを詳細に表示して、監視、トラブルシューティング、診断を行ったり、規制コントロールに対応したりできます。

トラブルシューティング

システム調査は、Sysdigによって生成されたイベント、または別のツールまたは人からのアラートによってトリガーされる場合があります。

- コンテキスト化された関連データの検索アクティビティ監査により、基になるデータに簡単にアクセスして、イベントの追跡、その影響の評価、および問題の解決に役立てることができます。

Sysdig Secureのポリシーイベントから、関連するアクティビティ監査に直接ジャンプして詳細を調査します。



- ユーザーへのコマンドと接続のトレースアクティビティ監査は、Kubernetesユーザーからの対話型要求をコンテナ内で実行されるコマンドとネットワーク接続に関連付けることができ、オペレーターはこのアクティビティをユーザーIDにトレースバックできます。

規制

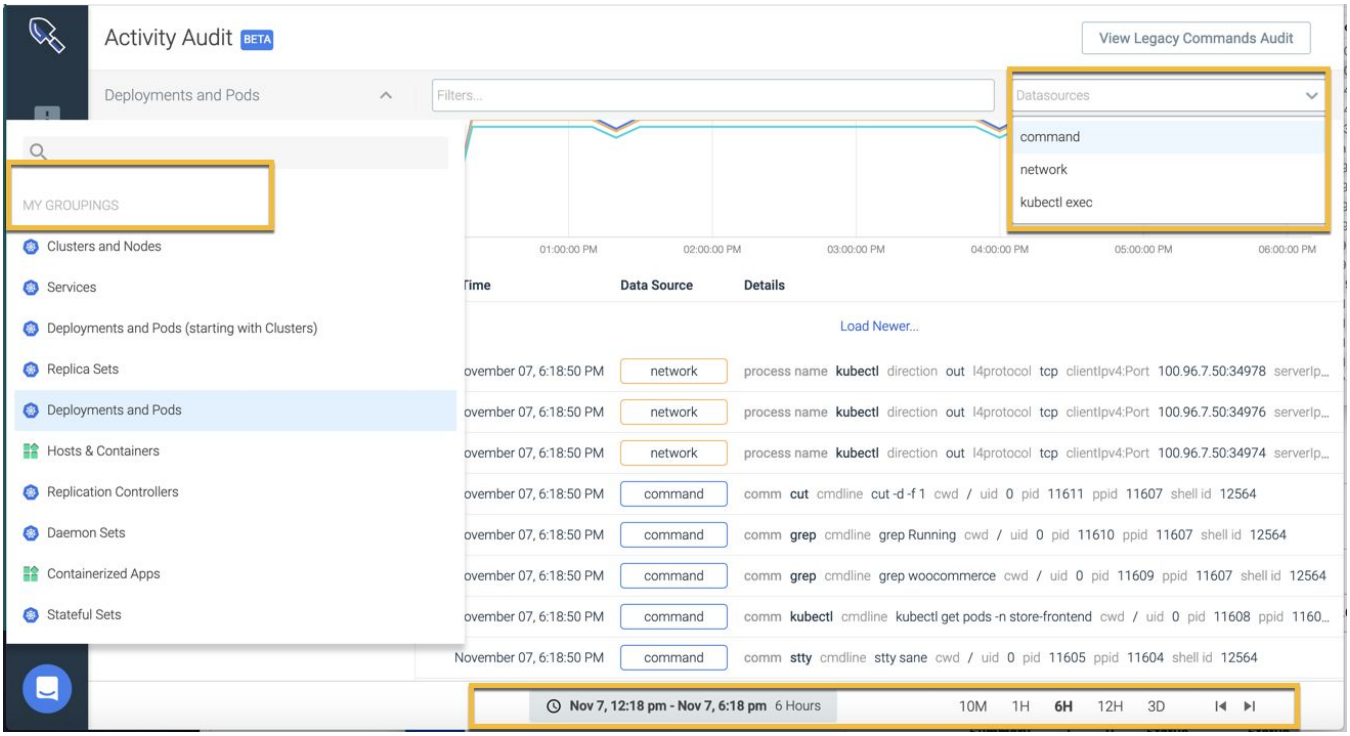
アクティビティ監査は、適切なデータの可視性とセキュリティ対策が実施されていることを監査人に証明するのに役立つインフラストラクチャに関するデータも提供できます。

アクティビティ監査は、多くのコンプライアンス標準の重要な要件です。

- SOC2
- PCI
- HIPAA
- NIST 800-53

監査インターフェイスをナビゲートする

アクティビティ監査には、継続的に更新されるアクティビティのリストが表示されます。 UI 機能を使用して、必要な情報を見つけてフィルタリングします。



グルーピング

ドロップダウンメニューから事前に定義されたグループでアクティビティをフィルタリングします。

グループ内の各要素には、そのエンティティのアクティビティエントリの概要が表示されることに注意してください。この番号を使用して、アクティビティの多い領域を発見できます。 フィルタリングは数値を変更します。

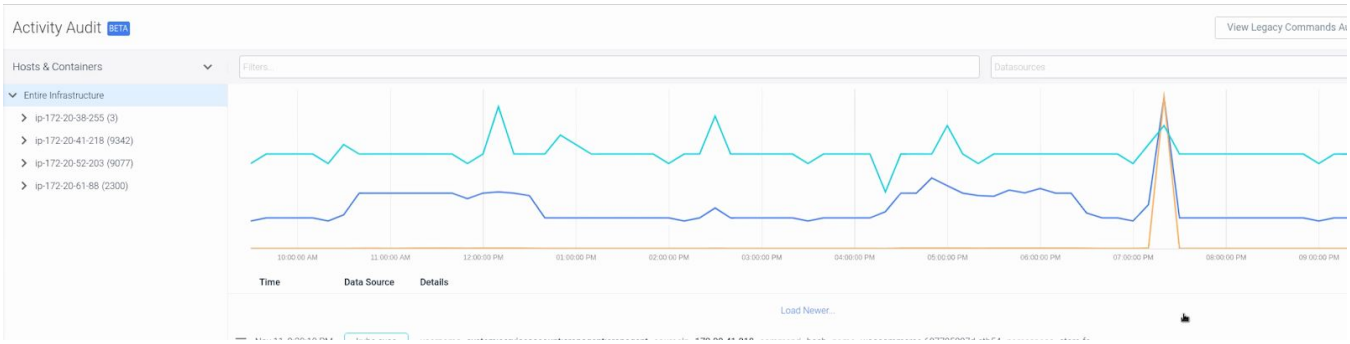
データソース

右上のドロップダウンを使用して、特定のデータセットから情報をフィルタリングします。 現在のデータソースは次のとおりです。

- ユーザコマンド
- ネットワークコネクション
- Kube exec コマンド

度数グラフ

グラフには、各データソースのアクティビティ頻度が表示されるため、ユーザーは異常を簡単に把握できます。



上の画像は、午後7時から午後8時までのネットワークアクティビティ（オレンジ色の線）の急上昇を示しています。

ピーク上でマウスをドラッグして、時間枠で自動ズームし、詳細を確認します。

タイムナビゲーションボタン

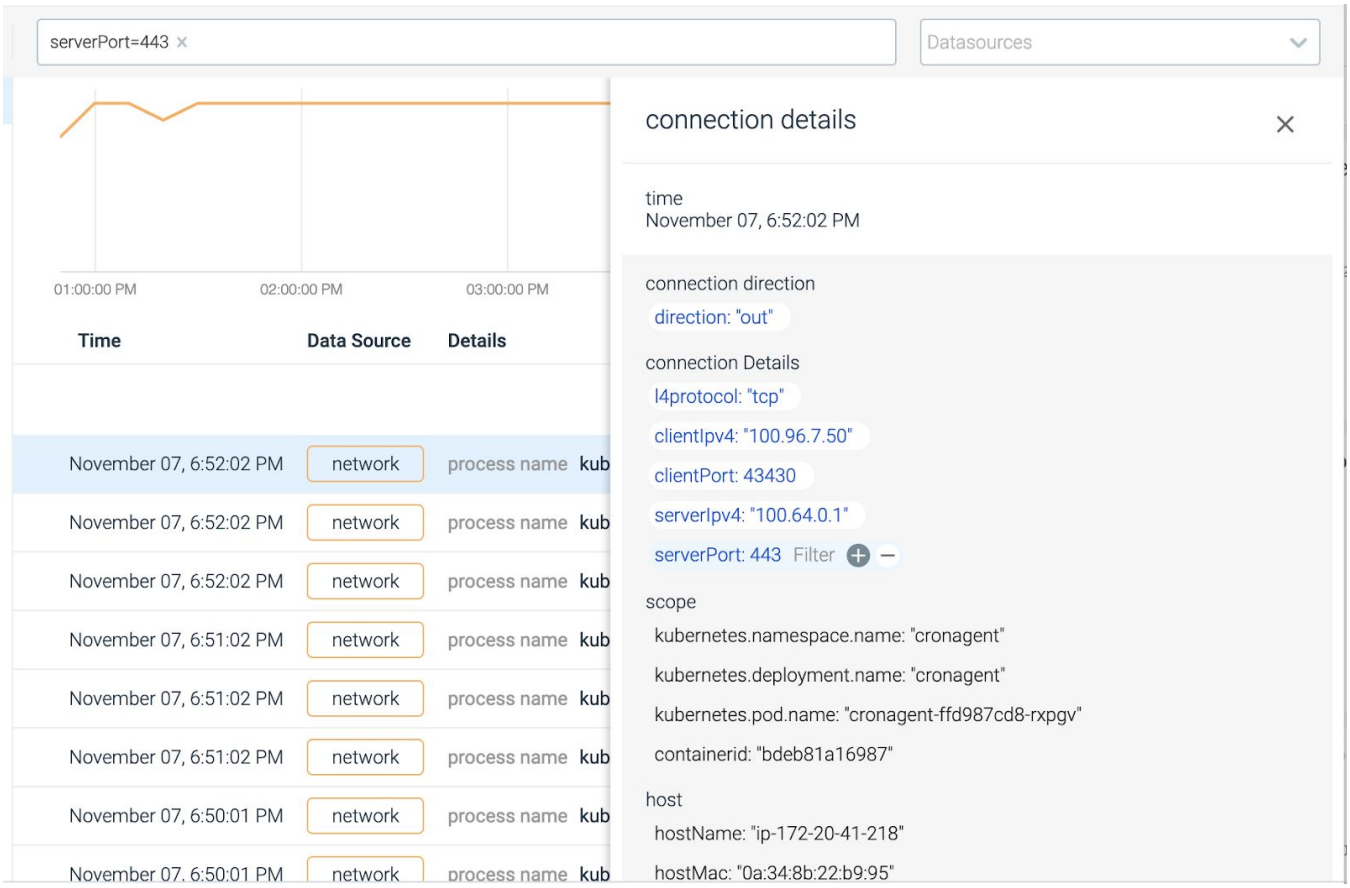
タイムウィンドウのナビゲーションバーを使用して、そのウィンドウ内で実行されるアクティビティのみを表示します。（詳細については、時間ウィンドウも参照してください。）

詳細ビュー

アクティビティ行を選択して、フィルタリング可能な属性（ホワイトリスト/ブラックリスト）などの詳細を表示します。

各データソースの属性については、アクティビティの詳細を確認するをご覧ください。

詳細ビューからホワイトリスト（+）/ブラックリスト（-）属性フィルターを使用することもできます。



ホワイトリスト（+）およびブラックリスト（-）の属性オプション

詳細ビューの属性の横には、フィルタリングに使用される+/-記号があります。

+をクリックして属性を含めます。 クリック-フィルターから属性を除外します。

トレースボタン(kube exec アクティビティ)

各kube exec項目の横には、トレースボタンがあります。

この機能を使用すると、コンテナのアクティビティを元のKubernetesユーザーとIPに関連付けることができます。 kubectl exec Traceの追跡を参照してください。

フィルタ

フィルタリングは、アクティビティ監査のパワーの中心です。フィルターを使用すると、意味のあるデータと接続を必要に応じて検索、並べ替え、解析、表示できます。

アクティビティデータをフィルタリングする方法：

- データソース：ドロップダウンからデータソースを選択します：ネットワークアクティビティ、コマンド、kubectl exec。
- 属性（+/-）：属性の横にある+または-を選択して、フィルターからその属性を含める/除外する
- 属性（手動）：属性がわかっている場合は、次の構文を使用して、フィルターボックスに手動で入力できます。

  属性を含める

  attribute_name = "attribute_value"　例： comm = "grep"

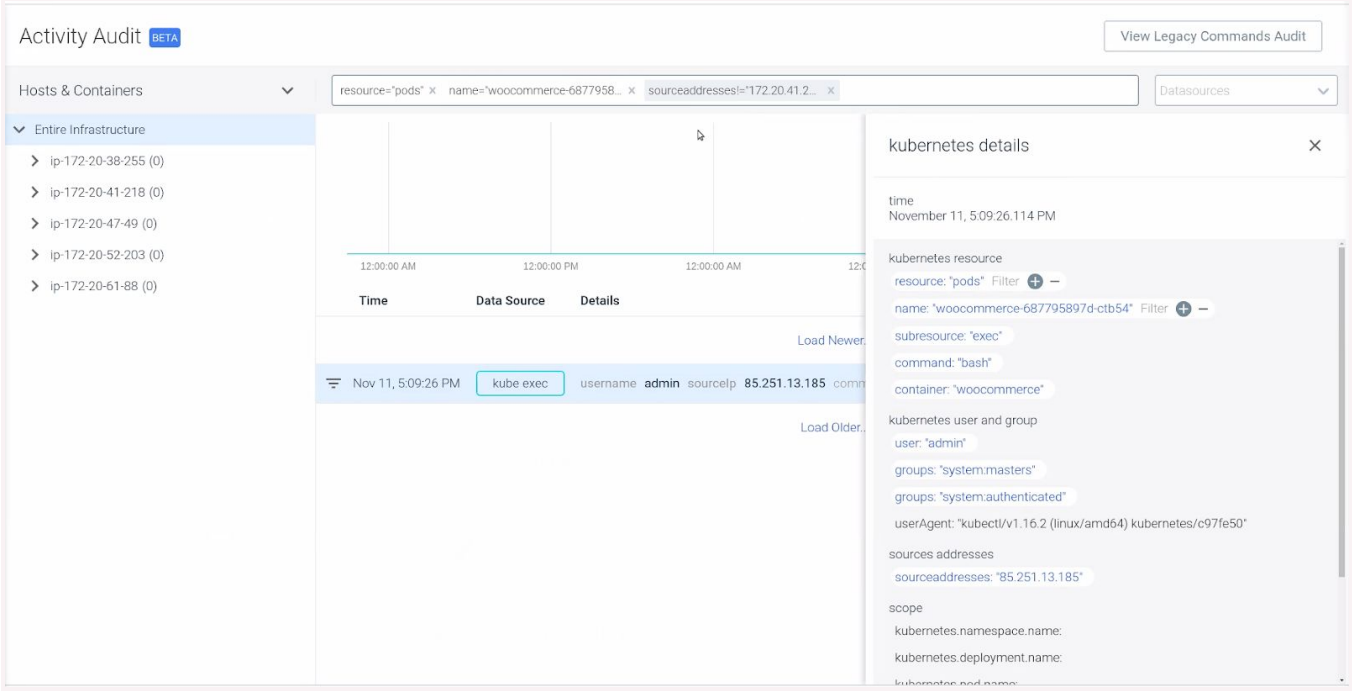
  属性を除外する

  attribute_name！= "attribute_value"　例： comm！= "grep"

- kube execエントリをトレースして、そのユーザーからのそのセッションのすべての関連アクティビティを表示します
- 時間グラフ：グラフのセクションを選択して、時間枠を拡大し、詳細なアクティビティを表示します
- 結合：これらの方法は、必要に応じて組み合わせることができます。

たとえば、下のフィルタは特定のポッドでアクティビティを表示しますが、通常のIPアドレスからアクティビティを除外します。

```
resource="pods" name="woocommerce-6877958" sourceaddresses!="172.20.41.2
```



アクティビティの詳細を確認する

コマンド詳細

名前	説明
When	コマンドが実行された日付と時刻
Command	実行されたコマンド
Full Command Line	すべての変数/オプションを含む完全なコマンド
Working Directory	コマンドが実行されたディレクトリ
Scope	コマンドによって影響を受けるインフラストラクチャ内のエンティティ
Host	コマンドが実行されたホストのホスト名とMACアドレス
Container	コマンドが実行されたコンテナーID、コンテナー名、およびイメージ
Additional Details	詳細なユーザー/ホスト情報： ● コマンドのプロセスID（PID） ● コマンドの親プロセスID（PPID） ● コマンドを実行したユーザーのユーザーID ● シェルID

ネットワーク接続詳細

名前	説明
Time	ネットワーク接続の日付と時刻
Connection Direction	着信または発信接続
Connection Details	含む: • Transport-level protocol (Ip4) • Client address, server address (Ip4) • Client port, server port
Scope	ネットワーク接続の影響を受けるエンティティ
Host	接続が行われたホストのホスト名とMACアドレス
Additional Details	ネットワーク接続を起動または受信したプロセス名とID（親プロセスID / PID）

Kubectl Exec 詳細

名前	説明
Time	kubectlコマンドの日付と時刻

Kubernetes resource	含む: • resource: 影響を受けるKubernetesリソースの種類（現在はポッドのみ） • name: リソースの名前（ポッド名） • subresource: 現在の exec • command: 実行されたコマンド • container: コンテナ：Kubernetes定義の概要名
Kubernetes user and group	含む: • user: kubectlコマンドを実行するユーザー名。サービスアカウントまたは人間のユーザーのいずれかです。 • groups: ユーザーが属するグループ • userAgent: クライアントuserAgent
Sources addresses	接続を開始した外部IPアドレス
Scope	含む • Kubernetes namespace name • Kubernetes deployment name • Kubernetes pod name • Container ID
Host	Hkubectl execが作成されたホストのホスト名とMACアドレス

ユースケース例

ブラックリスト: コマンド

ノイズの多いコマンドが0.2秒ごとに発生していますが、これは私の環境ではまったく正常なことです。 私にはもっと疑わしい他のコマンドがあります：

Foo
Foo
Foo
Foo
Foo
Suspicious command - curl
Foo
Foo
Foo
... 200 Foo
Suspicious command - dpkg
.... 500 Foo
Suspicious command - shred

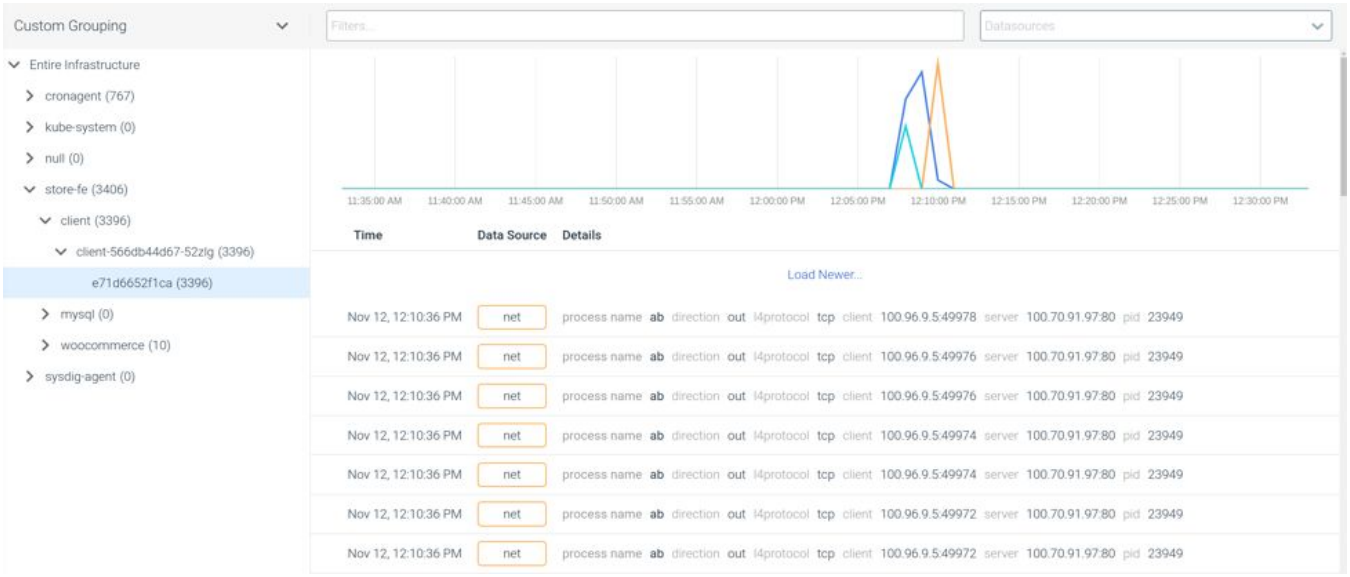
これは、「Foo」をブラックリストに登録し、残りに集中する明確なケースです。

インシデントレスポンスのフィルタリング

ポリシーイベントは、特定のポッドからのネットワーク接続に関して危険なピークを報告します。 この例では、根本原因を検索する1つの方法について説明します。

この問題を引き起こしたユーザーとアクティビティは何ですか？

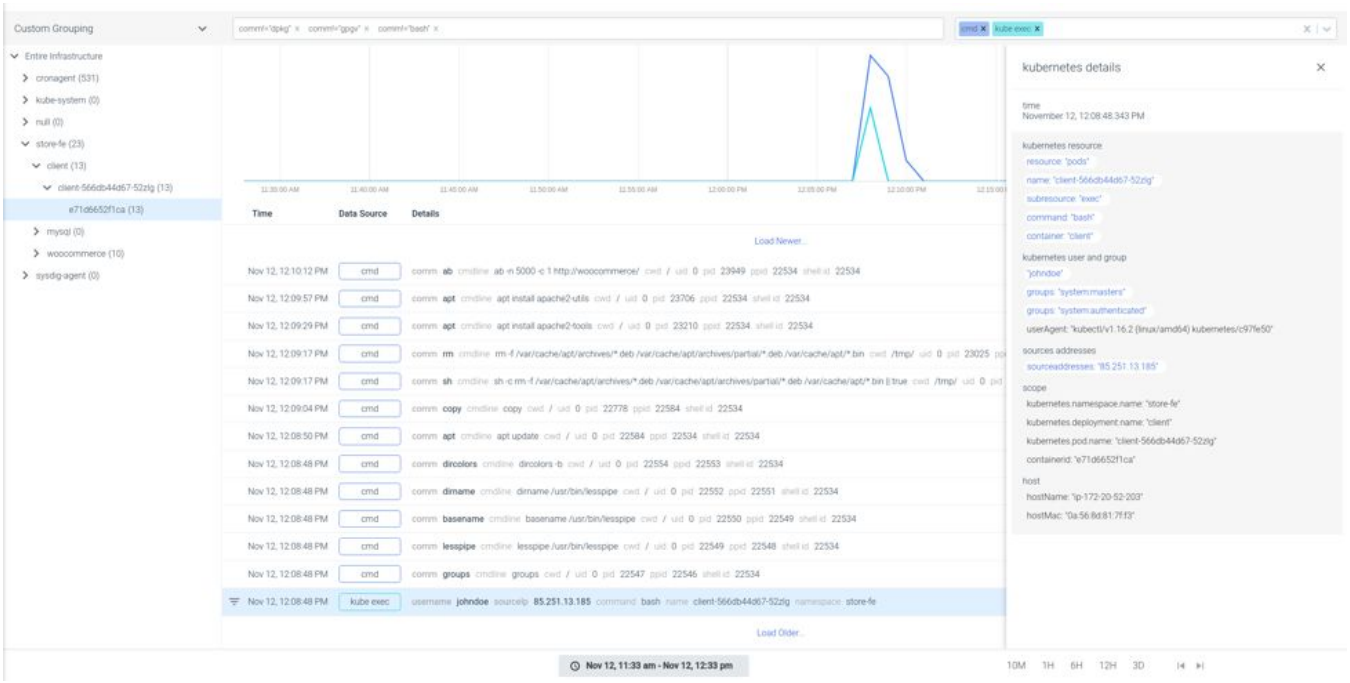
1. ポリシーイベントの横にある[アクティビティ監査]ボタンを使用して、関連する監査証跡に直接ジャンプします。



2. ここで一目で判断できます：

   - 高頻度のアクティビティが発生しているポッド/ネームスペース（3396ネットワークエントリがある場所）
   - アクティビティに関連するプロセス（この場合、ab、またはApache Benchmarkツール）
   - グラフ内の関連アクティビティ（cmdおよびkube exec行）
   - 除外できる繰り返しエントリ

3. フィルタリングによりビューを調整します。



- ネットワークデータソースからcmdおよびkube exeに切り替えます。
- ノイズの多い繰り返しのエントリを除外します（例：comm！= "bash"）
- ユーザー情報のkube execアイテムの詳細を調査します。

4. フィルタリング後、次の詳細を含む集中インシデントレポートが作成されます。

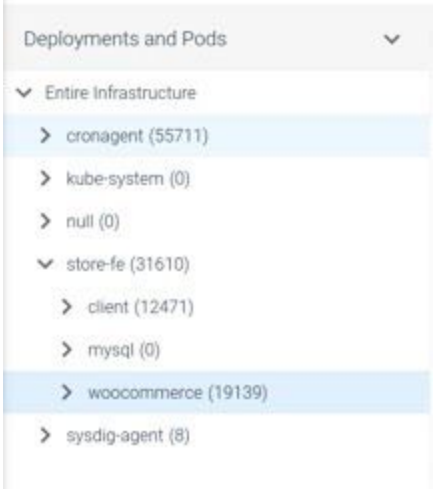
- Kubernetesユーザー「johndoe」
- 彼が接続に使用した外部IP
- Apache Benchmarkストレステストツールのインストールと起動に使用した一連のコマンド

kubectl execトレースをフォローする

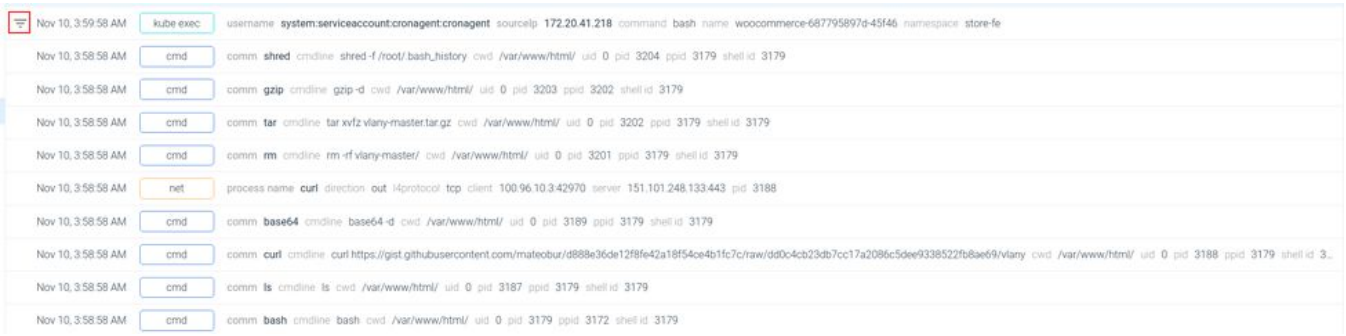
実稼働環境では、kubectl execコマンドは通常疑わしいです。また、そのようなコマンドは対話型セッションであるため、どの個人がコマンドを発行したか、およびその個人が実行した他のアクティビティを特定することは困難です。ここでSysdigのトレース機能が使用され、kubectl execコマンドと特定のユーザー、およびそのユーザーのセッションで実行されるネットワークとコマンドのアクティビティが関連付けられます。

この例では、疑わしいアクティビティが検出されたため、誰かがトロイの木馬をダウンロードして実行したかどうかを判断します。

1. グループを使用して、Kubernetes階層をネームスペースとデプロイメントごとに表示します。（カッコ内の数に基づいて）予期しない高頻度のアクティビティを表示するポッドに焦点を当てます。

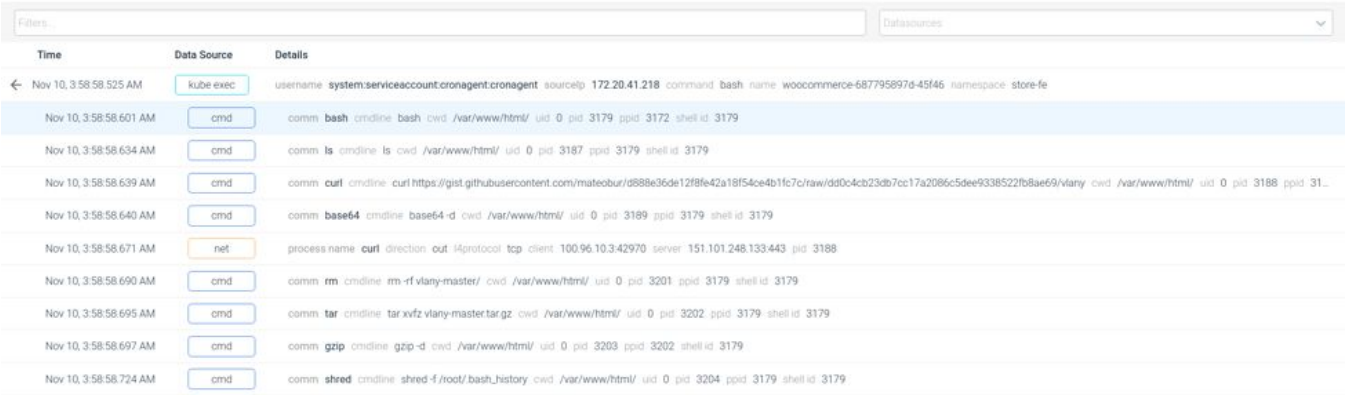


2. 対応するアクティビティグラフを確認すると、時間枠に焦点を合わせ、何百ものコマンドとネットワークイベントの中でkube execアクティビティを確認できます。



3. kube execアイテムを選択し、左側の[トレース]ボタンをクリックします。

   このセッショントレースは、ユーザーがコンテナ内で実行したコンテナアクティビティ（ネットワーク、コマンド）のフォーマットされたレポートを表示します。



   注意

   GKEクラスターで実行している場合、このボタンは表示されません。