

Inspektor GadgetでKubernetesクラスタをデバッグしよう

2023/10/12 SRETT#7 satoken

- kubectlコマンドでがんばる
 - logs, describe
 - 適当なPod作ってデバッグ
- Dashboardで色々追う
 - ログ、メトリクス、トレース、 APM etc

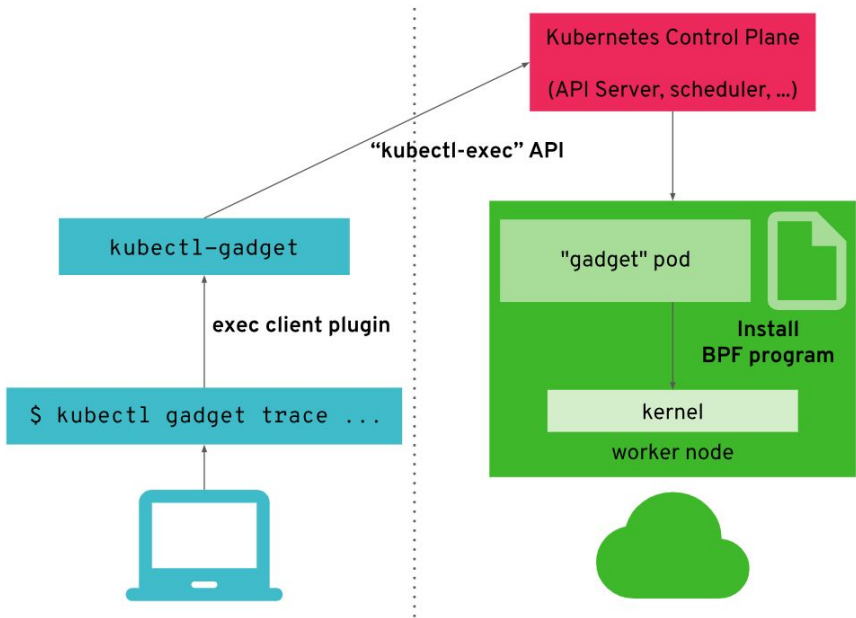


- eBPFを利用して k8sクラスタをデバッグするツール
 - <https://github.com/inspektor-gadget/inspektor-gadget>
 - <https://www.inspektor-gadget.io/docs/latest/>
- CNCFのSandbox Projectsの1つ
- krewでinstall
- kubectl gadget ~ サブコマンドが使えるようになる



**INSPEKTOR
GADGET**

- gadget deployコマンドで DaemonSetをインストール
- DaemonSetがNodeのカーネルに eBPFプログラムを接続し様々な情報を取得



```
$ kubectl gadget -h
Collection of gadgets for Kubernetes developers
```

```
Usage:
  kubectl-gadget [command]
```

Available Commands:

advise	Recommend system configurations based on collected information
audit	Audit a subsystem
completion	Generate the autocompletion script for the specified shell
deploy	Deploy Inspektor Gadget on the cluster
help	Help about any command
profile	Profile different subsystems
prometheus	Expose metrics using prometheus
script	Run a bpftrace-compatible scripts
snapshot	Take a snapshot of a subsystem and print it
sync	Synchronize gadget information with your cluster
top	Gather, sort and periodically report events according to a given criteria
trace	Trace and print system events
traceloop	Get strace-like logs of a container from the past
undeploy	Undeploy Inspektor Gadget from cluster
version	Show version

```
$ kubectl gadget trace -h
Trace and print system events
```

```
Usage:
  kubectl-gadget trace [command]
```

Available Commands:

bind	Trace socket bindings
capabilities	Trace security capability checks
dns	Trace DNS requests
exec	Trace new processes
fsslower	Trace open, read, write and fsync operations slower than a threshold
mount	Trace mount and umount system calls
network	Trace network streams
oomkill	Trace when OOM killer is triggered and kills a process
open	Trace open system calls
signal	Trace signals received by processes
sni	Trace Server Name Indication (SNI) from TLS requests
tcp	Trace TCP connect, accept and close
tcpconnect	Trace connect system calls
tcpdrop	Trace TCP kernel-dropped packets/segments
tcpretrans	Trace TCP retransmissions

ネットワークやプロセス
などいろいろなイベント
をトレース

```
$ kubectl gadget advise -h  
Recommend system configurations based on collected information
```

```
Usage:  
kubectl-gadget advise [command]
```

Available Commands:

```
network-policy    Generate network policies based on recorded network activity  
seccomp-profile   Generate seccomp profiles based on recorded syscalls activity
```

Network Policyやseccompの
ファイルを生成してくれる

- IaCは？
 - helm chartがあります
 - <https://artifacthub.io/packages/helm/gadget/gadget>
- 本番投入していますか？
 - していません。個人的に追っている &遊んでる状態
 - 特権の DaemonSetが立つという性質上、誰に使わせるなどルール決めが必要
 - eBPFのverifyがあるとはいえ gadget scriptで任意のコード実行できるので
 - 奥の手として使うのはありかも
 - Inspektor Gadgetの[Blog](#)にトラシューの実例が乗ってます
- 興味があればお試しください、おしまい
 - <https://www.inspektor-gadget.io/docs/latest/>