Inspect your Cluster with osquery

Prateek Sahu

prateeks@utexas.edu

What is osquery?

osquery is an operating systems instrumentation framework

- Developed by Facebook
- Used for performant low-level OS analytics and monitoring
- Exposes the OS as a high performant Relational DB
- SQL queries to explore system data like processes, kernel modules, network conn, hardware events
- Available for Windows, OS X, Linux and FreeBSD

osquery Features

- High performance and low-footprint distributed host monitoring tool.
- Allows queries to be executed across the entire infrastructure.
- Tool aggregates query results and logs state changes in infrastructure.
- Insight into security, performance, configuration and state of infrastructure.
- Monitors systems operational problem or incident response at runtime.
- Extensive tooling documentation to be used as a plugin to any toolchain.

Monitoring of System

- Exposes whole of `/proc` filesytem as a Relational DB
  - Easy to compose queries across files and processes using SQL commands like `JOIN`.
  - High performant search through running processes using `LIKE` or = operations given by SQL.
  - Useful to monitor Containerd and Docker containers since these apps are processes logged under `/proc` filesystem.

Installation steps: osquery

- Installation steps (https://www.osquery.io/downloads/official/4.0.2)

```
$ export OSQUERY_KEY =
1484120AC4E9F8A1A577AEEE97A80C63C9D8B80B

$ sudo apt-key adv -keyserver keyserver.ubuntu.com
-recv-keys $OSQUERY_KEY

$ sudo add-apt-repository 'deb [arch=amd64]
https://pkg.osquery.io/deb deb main'

$ sudo apt-get update

$ sudo apt-get install osquery
```

Demo

- `$ sudo osqueryi`
- `.tables`
- Run a docker container: `docker run -d --name web01 --privileged --user root nginx:latest`
- `SELECT name, image, status FROM docker_containers WHERE privileged=1;`
- Lets check the environment variables for the database we deploy in lab2. `SELECT name, env_variables FROM docker_containers WHERE env_variables LIKE "%PASSWORD%";`
- Can check various security enhancement features: AppArmor, SELinux enabled, plaintext secret usages.

Demo

Kubernetes

- Select kubernetes namespaces or process informations.
- `SELECT pid FROM processes WHERE name LIKE "%sql%";`
- `SELECT pid_namespace FROM process_namespaces WHERE pid IN (SELECT pid FROM processes WHERE name LIKE "%sql%");`
- `SELECT name,pid FROM processes WHERE pid IN (SELECT pid FROM process_namespaces WHERE pid_namespace=<namespace>);`
- Can monitor various metrics like startup process logs to gather data/analyse anomalies
  - Anomaly Detection: https://osquery.readthedocs.io/en/stable/deployment/anomaly-detection/
  - Auditing : https://osquery.readthedocs.io/en/stable/deployment/process-auditing/