Google: Kubernetes Engine (GKE)

Google Kubernetes Engine (GKE) provides a managed environment for deploying, managing, and scaling your containerized applications using Google infrastructure. The GKE environment consists of multiple machines (specifically, Compute Engine instances) grouped together to form a cluster.

Configuration

The Splunk OpenTelemetry Collector for Kubernetes is a Helm chart for the Splunk Distribution of OpenTelemetry Collector. This chart creates a Kubernetes DaemonSet along with other Kubernetes objects in a Kubernetes cluster and provides a unified way to receive, process and export metric, trace, and log data for:
- Splunk Enterprise
- Splunk Cloud Platform
- Splunk Observability Cloud

Check the Splunk Observability Cloud documentation for full details on Kubernetes configuration using the Splunk OpenTelemetry Collector for Kubernetes, including:

- Install on Kubernetes
- Advanced configurations for Kubernetes
- Collect Kubernetes data
- Supported integrations

Application

When your Splunk deployment is ingesting Google Kubernetes Engine data, you can use the data to achieve the following:

- Detecting Kubernetes sensitive object access activity