Kubernetes

*Kubernetes* is an open-source system for automating deployment, scaling, and management of containerized applications.

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

Data application

When your Splunk deployment is ingesting Kubernetes data, you can use it to achieve the following Security use cases:

- Detecting Kubernetes scanning activity
- Monitoring Kubernetes sensitive role activities
- Monitoring Kubernetes sensitive object access

You can also use the data to achieve the following Observability use cases:

- Maximizing infrastructure performance in Kubernetes environments
- Monitoring Kubernetes pods
- Deploying the Splunk OpenTelemetry Collector to gather Kubernetes metrics
- Instrumenting Java apps in Amazon EKS and non-EKS environments
- Becoming more effective monitoring Kubernetes at scale