Alcide kAudit

Real-time, Automated Kubernetes Forensics and Analysis

Challenges of Auditing a Kubernetes Cluster

The dynamic, distributed and ephemeral nature of Kubernetes deployments results in workloads being added, removed or modified at a fast pace. Security teams' demands for safeguarding Kubernetes deployments are many, and increasing, and also include the swift identification of users, and roles, with legitimate reasons for accessing sensitive database-workloads at any given time. This calls for a solution that can monitor and conform to the organization's compliance and policies in order to: **Identify anomalous behaviors and suspicious activity patterns**, such as unknown suspicious eventsevents; and **focus compliance investigations** on Kubernetes misuses, for example, known organization policy violation events.

Finding interesting results is just a matter of finding the specific entries in the log that are known in advance to correlate to undesirable activity. However, finding suspicious but previously unknown activity in the logs requires a different set of tools and skills; especially if this suspicious behavior can only be understood from a wider context over a prolonged period, and not just one or two related log entries.

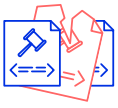
Focus on Real Incidents. Reduce Time to Detect.

Alcide kAudit identifies anomalous behaviors and suspicious activity patterns, observing them with extended context, beyond configured rules. These use cases include:

Stolen credentials, which aim to gain initial access to K8s-based clusters or pods; or seek to capture credentials earlier in their reconnaissance process through social engineered access to cluster resources.

Stolen tokens or misconfigured RBAC, which allow lateral cluster or pod movement, privilege escalation, data access and/or data manipulation.

Exploited vulnerabilities in the Kubernetes API Server, such as authentication, authorization, admission control or validation requests breaches, which see to gain access to privileged and sensitive resources.



Violated security policies in conflict with compliance best practices.

How it Works

kAudit is an agentless service for the Kubernetes audit. It can be activated remotely to the K8s cluster or deployed locally as a standalone container.

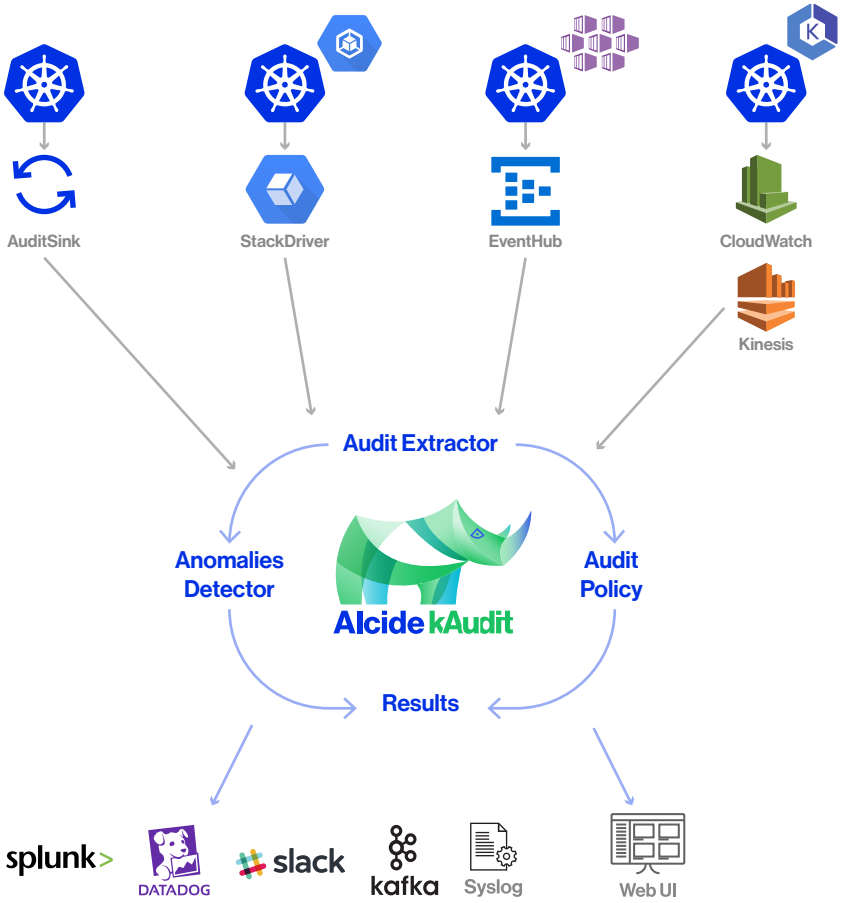
Depending on the monitored Kubernetes cluster, the cluster's environment should be set up to give kAudit access to the audit logs:

- **GKE:** through Google Stackdrvier
- **EKS:** through AWS CloudWatch and Kinesis
- **AKS:** through Azure EventHub
- **Native Kubernetes:** through Kubernetes Audit Policy configuration

kAudit's findings, detected anomalies in the audit log, as well as the audit entries matching the user's policy, can be viewed through a web UI and may be exported for integration with external systems and consumption channels.

These export options include:

- Slack Channel
- Splunk HTTP Event Collector
- Syslog
- Kafka topic



The Benefits

- Automate the entire security of their pipeline
- Reduce noise
- An advanced investigation dashboard that allows deep investigation instead of sifting through raw logs

Get a first view of kAduit

Sign up to early access program

Sign up