alcide

Secure Microservices Workloads. Connect Cloud Citizens.

DATADOG TECHNOLOGY PARTNER

Alcide kAudit

Kubernetes Audit Logs Analysis Made Easy

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 and monitoring 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.

Alcide kAudit provides Kubernetes audit and anomaly monitoring services. Alcide's integration with Datadog enables DevOps and security personnel to focus on compliance violations and active security risks. This will allow companies to quickly limit the impact and fix the causes of such security issues in their Kubernetes clusters.

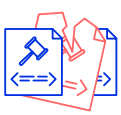
Focus on Real Incidents. Reduce Time to Detect.

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.