Teleport

Kubernetes Audit Log Best Practices

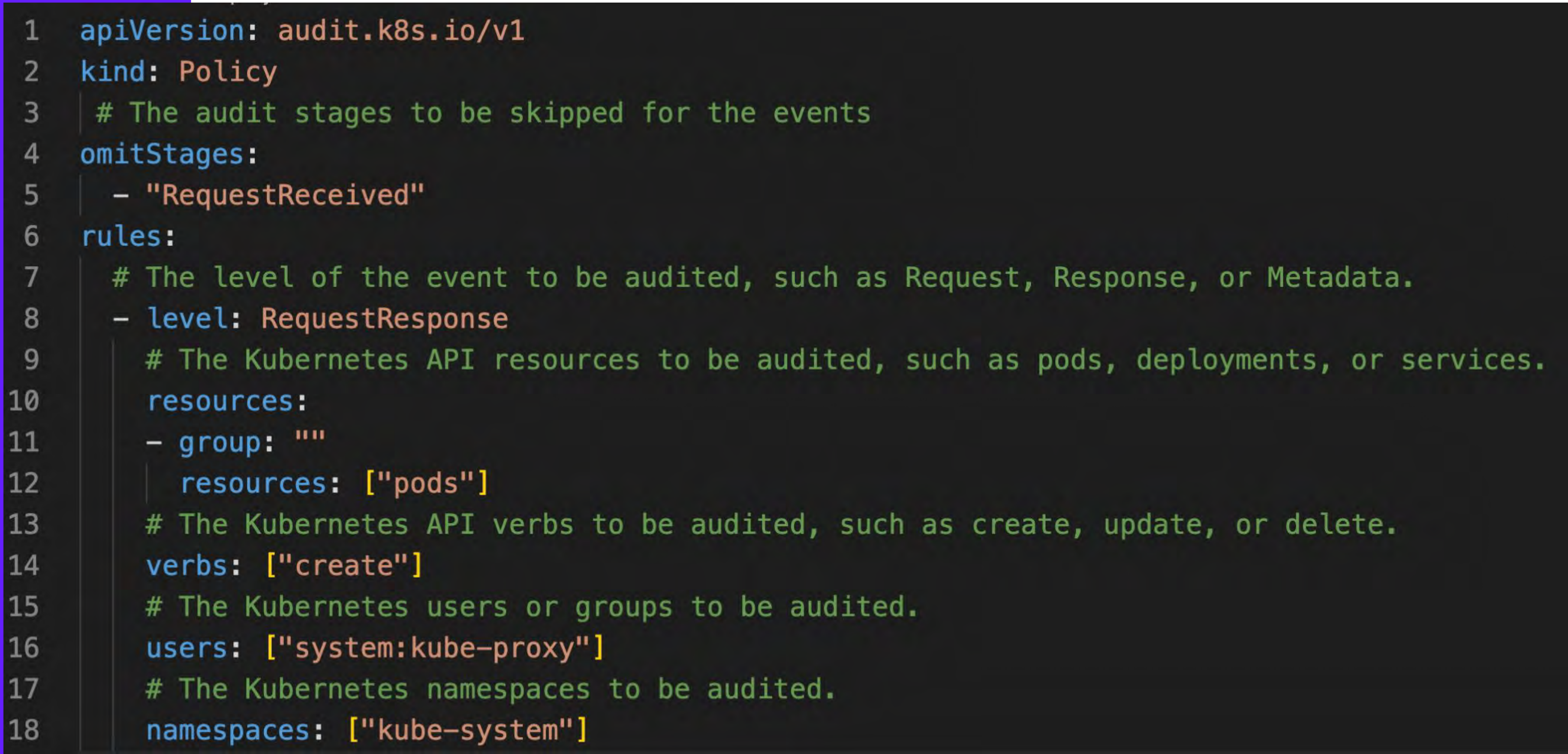
Kenneth DuMez

Teleport

Kubernetes Audit Policy

- Native Kubernetes object
  - Defined in YAML
- Defines rules and settings for all auditing events
- Key when configuring your audit logging strategy
- Extremely granular
  - Can filter events on different types of resources
  - Can configure what information you collect on those events
- Google Container-Optimized OS is a good starting point

Audit Policy “rules” fields



```yaml
apiVersion: audit.k8s.io/v1
kind: Policy
 # The audit stages to be skipped for the events
omitStages:
  - "RequestReceived"
rules:
  # The level of the event to be audited, such as Request, Response, or Metadata.
  - level: RequestResponse
    # The Kubernetes API resources to be audited, such as pods, deployments, or services.
    resources:
    - group: ""
      resources: ["pods"]
    # The Kubernetes API verbs to be audited, such as create, update, or delete.
    verbs: ["create"]
    # The Kubernetes users or groups to be audited.
    users: ["system:kube-proxy"]
    # The Kubernetes namespaces to be audited.
    namespaces: ["kube-system"]
```

Teleport

Audit Policy Best Practices

- Clearly define the audit policy scope
  - Limit the types of events you audit
    - Avoid performance issues
- Use meaningful audit rule names
- Regularly review audit logs
- Use a dedicated storage solution
- Aggregate your logs
  - Consolidate all of your audit logging into a central location

Open-Source Tooling

- Falco
  - Anomaly detection
  - Alerting
  - Allows extensive integration
- OpenRaven
  - Audit collection/aggregation
  - Compliance rule analysis (PCI, HIPAA, GDPR)
  - Real-time alerting
- Elastic
  - Centralized logging
  - Real-time analysis
  - Visualization

Multi-layer Comprehensive Solution

Teleport

Teleport Kubernetes Logging

- Ties each event in Kubernetes to an **Identity**
    - Centralized RBAC roles tied to identity for both machines and human engineers
- Centralizes audit logging for **ALL** of your resources
    - (not just Kubernetes)
- Allows for session playback of Kubernetes sessions conducted over SSH
    - Prevent obfuscation of attacks
    - See exactly what’s happening in your cluster

Demo!

Teleport

Thank you so much!

Teleport

goteleport.slack.com

https://goteleport.com