kube-rbac-proxy

github.com/brancz/kube-rbac-proxy

Securing Kubernetes cluster communication with RBAC

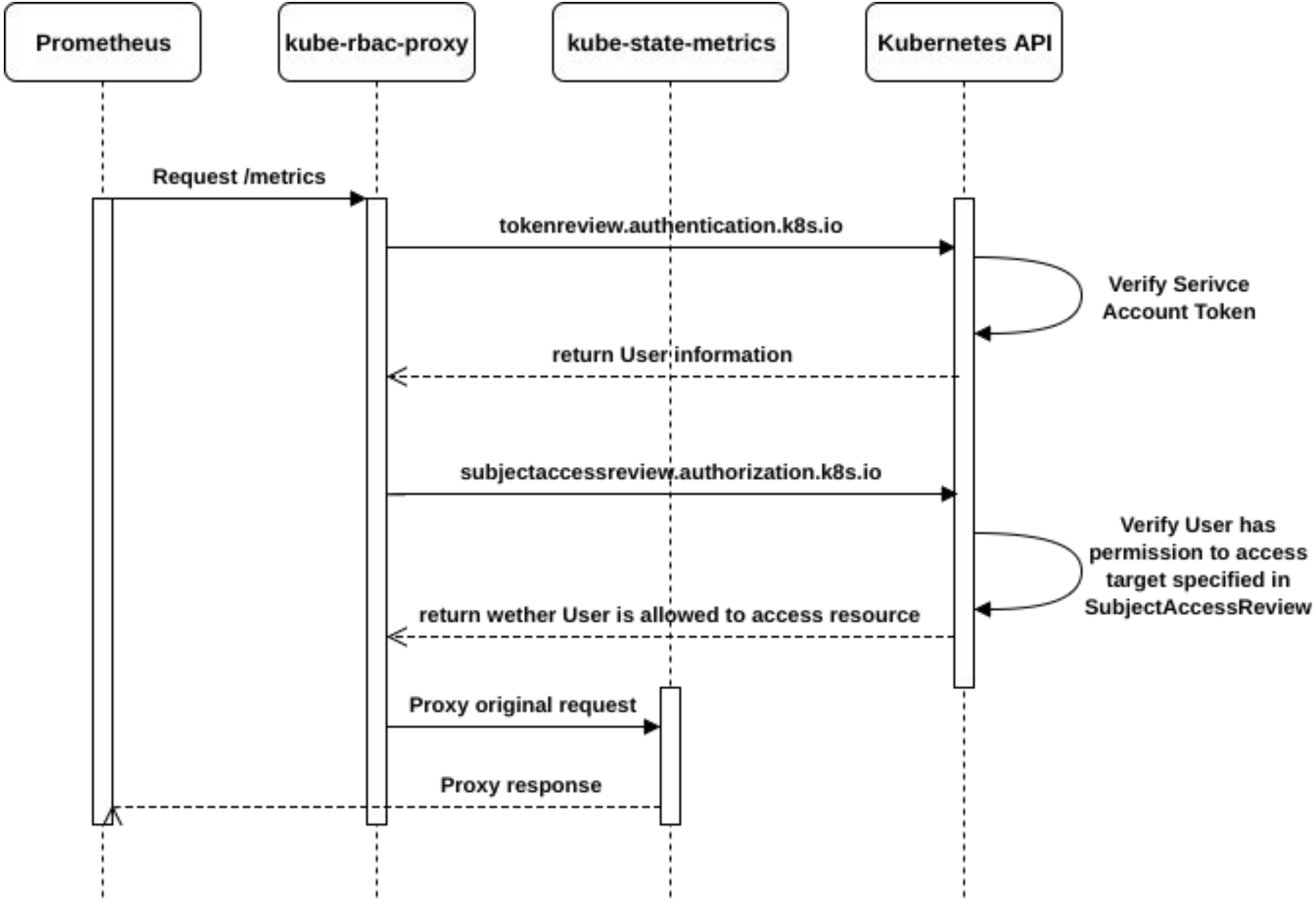
By Frederic Branczyk @fredbrancz

Problem

- Scraping metrics with Prometheus
- Recurring theme: How to authenticate and authorize?

By example: apiserver & kubelet

- AuthN: Use a Kubernetes supported authentication mean to authenticate a client
  - Client certificate auth (verified with cluster CA)
  - ServiceAccount token (verified with TokenReview)
- AuthZ: Verify a previously authenticated user is allowed to access the requested resource
  - Verify via SubjectAccessReview


Prometheus
kube-rbac-proxy
kube-state-metrics
Kubernetes API
Request /metrics
tokenreview.authentication.k8s.io
Verify Serivce Account Token
return User information
subjectaccessreview.authorization.k8s.io
Verify User has permission to access target specified in SubjectAccessReview
return wether User is allowed to access resource
Proxy original request
Proxy response

What can authZ look like?

- Resource based
    - Can user X proxy through service X
    - Can user X get service X
    - Can user X access namespace X
- Non-resource URLs
    - /metrics
    - /google.pubsub.v2.PublisherService/CreateTopic

Demo

Future work

- Verifying Token audience
    - Prevent impersonation with Kubernetes API
- Unprivileged SubjectAccessReviews
- Human user authN methods, such as oauth/OIDC

Thanks!

kube-rbac-proxy

github.com/brancz/kube-rbac-proxy

Follow me! :) @fredbrancz