External authentication with managed Kubernetes

Juho Saarinen
Mavericks Software OY

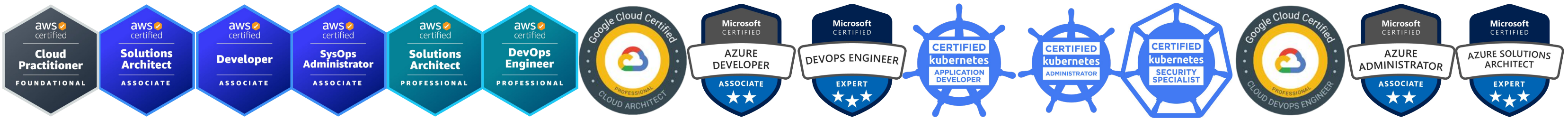
mavericks

a Witted Company

SENIOR SOFTWARE CONSULTANTS FOR DIGITAL DEVELOPMENT PROJECTS

About me

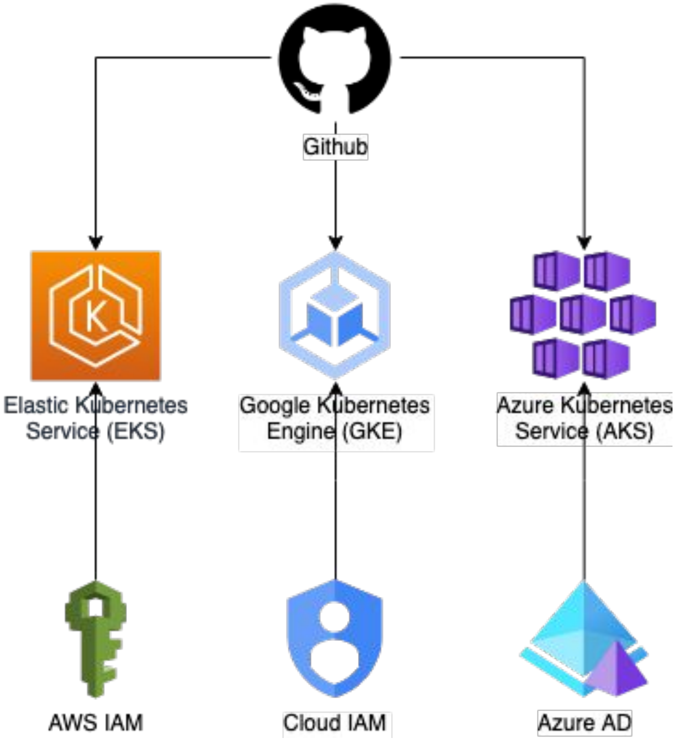
- Test & DevOps Architect at Mavericks
- Consultant since 2007
- Master of Science (M. Sc.) 2013 from University of Helsinki
- Major physics, minors mathematics, theoretical physics
- Open source contributor e.g. Robot Framework, Projen, AWS CDK
- DevOps, testing and Cloud enthusiastic


aws certified Cloud Practitioner FOUNDATIONAL
aws certified Solutions Architect ASSOCIATE
aws certified Developer ASSOCIATE
aws certified SysOps Administrator ASSOCIATE
aws certified Solutions Architect PROFESSIONAL
aws certified DevOps Engineer PROFESSIONAL
Google Cloud Certified PROFESSIONAL CLOUD ARCHITECT
Microsoft CERTIFIED AZURE DEVELOPER ASSOCIATE
Microsoft CERTIFIED DEVOPS ENGINEER EXPERT
CERTIFIED kubernetes APPLICATION DEVELOPER
CERTIFIED kubernetes ADMINISTRATOR
CERTIFIED kubernetes SECURITY SPECIALIST
Google Cloud Certified PROFESSIONAL CLOUD DEVOPS ENGINEER
Microsoft CERTIFIED AZURE ADMINISTRATOR ASSOCIATE
Microsoft CERTIFIED AZURE SOLUTIONS ARCHITECT EXPERT

Issue: Multi-cloud managed Kubernetes clusters’ authentication

Environment

- Developers mostly only at GitHub
- Kubernetes services use cloud provider own IAM
    - EKS allows to use external OAuth IdP as long as endpoint is publicly available


Github
Elastic Kubernetes Service (EKS)
Google Kubernetes Engine (GKE)
Azure Kubernetes Service (AKS)
AWS IAM
Cloud IAM
Azure AD

Solution:
Kube-oidc-proxy

A bit more about solution

- Kubernetes supports OIDC authentication through master configuration
  - Managed Kubernetes doesn’t reveal masters
  - Note: Elastic Kubernetes Service (EKS at AWS) allows to use external OIDC authentication
- Kube-oidc-proxy solves this by proxying traffic
  - Forked by Tremolo Security
- Gangway offers nice UI to make login
  - Archived project

Demo

mavericks

Issue: Some Kubernetes services don’t offer authentication

Kubernetes “basic” tooling

- “All” clusters have tools that doesn’t support authentication
  - Prometheus
  - AlertManager
  - Thanos
  - WeaveScope
  - Test versions of applications
- Can be handled by closing basic UIs
  - Reduces usability of e.g. AlertManager alert links
    - Point to AlertManager
    - AlertManager links to Prometheus

Solution: Oauth2-proxy

A bit more about solution

- As (usually) external traffic comes through Ingress, it's easy point to authenticate
- Oauth2-proxy allows to use annotations to enable authentication
  - Transparently authenticates user at the ingress
  - Authorization possible with groups
    - Just at generic access level, as application's doesn't know anything about this

Demo

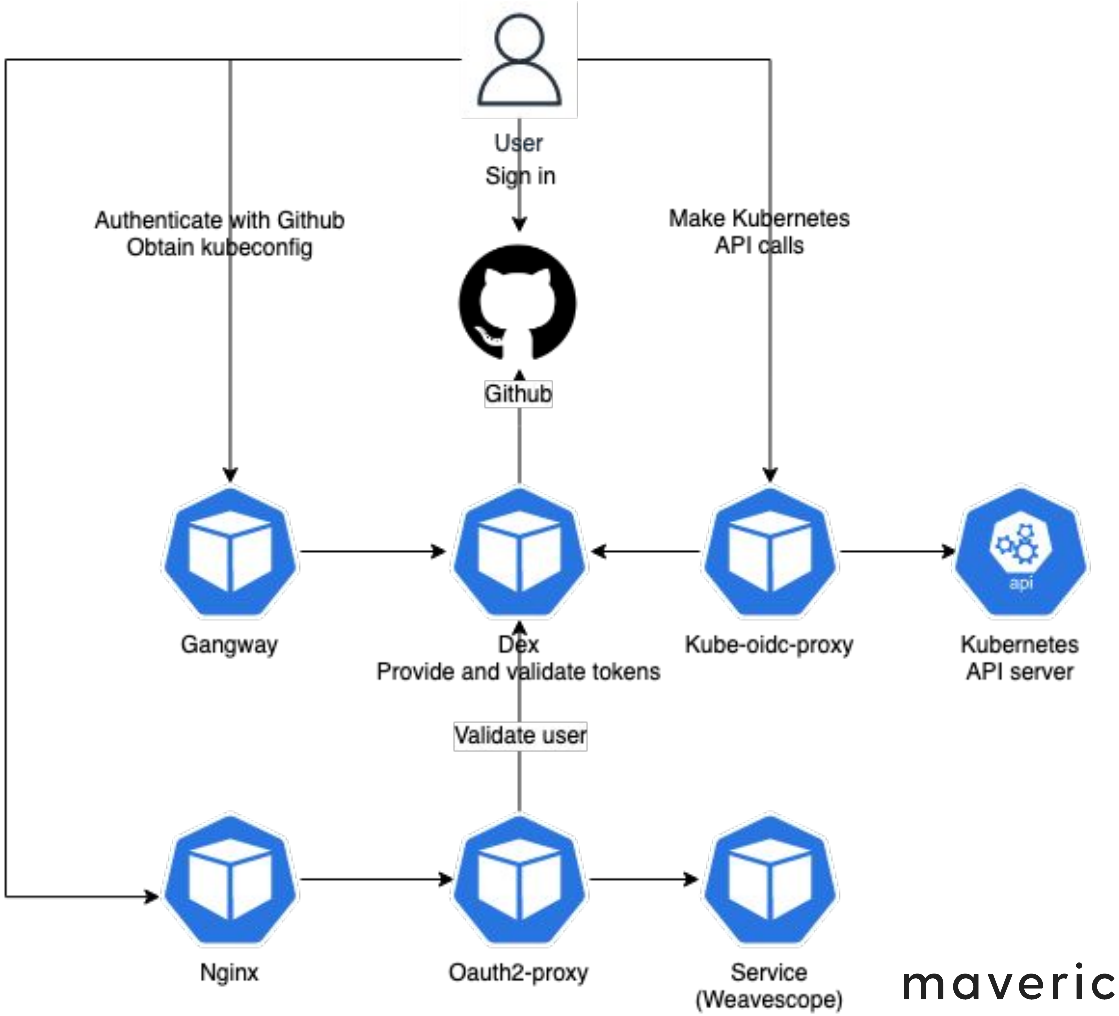
Issue: Multiple OAuth secrets per cluster

mavericks

Solution: Dex

A bit more about solution

- As each OAuth application (URL) requires own registration, it might be hard to get those for multiple different addresses
- Here we have just 2 applications, but having Dex allows easier management of applications
- Also allows to use multiple authentication backends without need to change applications



@hifi_fi jjsaarinen

mavericks

Final experience

- Users can use both Kubernetes API and application with GitHub credentials
    - Rights defined with GitHub group memberships
- No need to give Gcloud or MS or AWS credentials to anyone
- User rights management at own hands
    - Also for external applications, like Cloud Run running Hashicorp Vault

Alternatives

- Rancher
  - Can be installed just to manage cluster
  - Productized but heavier as used solution
  - Not providing ingress authentication as oauth2-proxy
- OpenUnison (Tremolo Security)
  - Productized way to get everything presented here
  - Contollable through CRDs
    - Dex has CRDs, but those are not meant for user to utilize directly

Links