MIRANTIS | LABS

Tech Talks

SSO for Kubernetes using Dex

A Federated OpenID Connect Provider

Disclaimer

The content contained herein is for informational purposes only, may not be referenced or added to any contract, and should not be relied upon to make purchasing decisions. It is not a commitment, promise, or legal obligation to provide any features, functionality, capabilities, code, etc. or to provide anything within any schedule, date, time, etc. All Mirantis product and service decisions remain at Mirantis sole and exclusive discretion.

Whoami

Martin Nirtl

Solution Architect

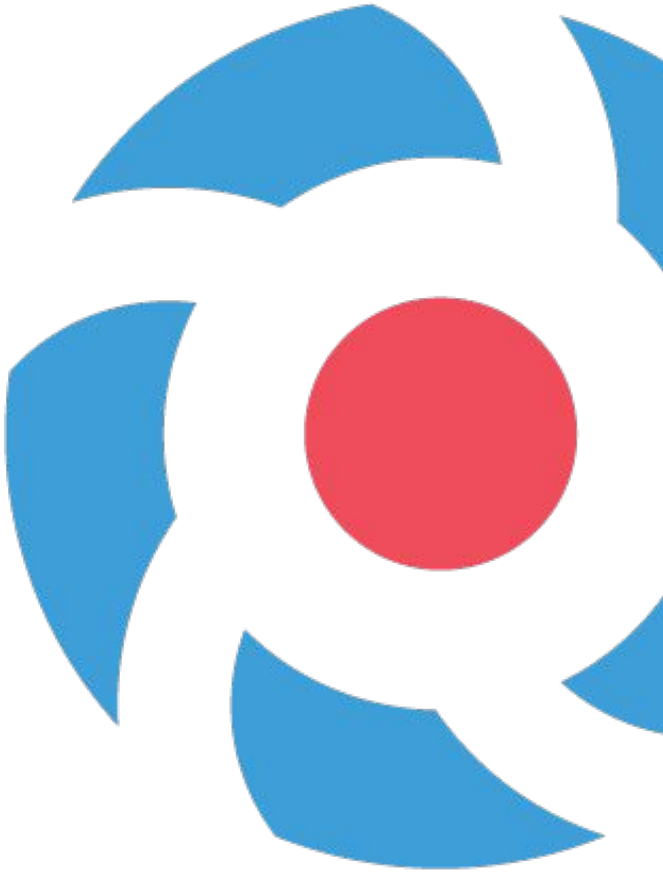
I am an IT engineer 👨‍💻 with strong backgrounds in software, DevOps/platform and electronic engineering working for Mirantis as a pre-sales solution architect. Next to my job, my main side-hustles are all around Kubernetes ⛵, IaC and automating things. From time to time, I even build little apps in Go or other languages.

martinnirtl martinnirtl

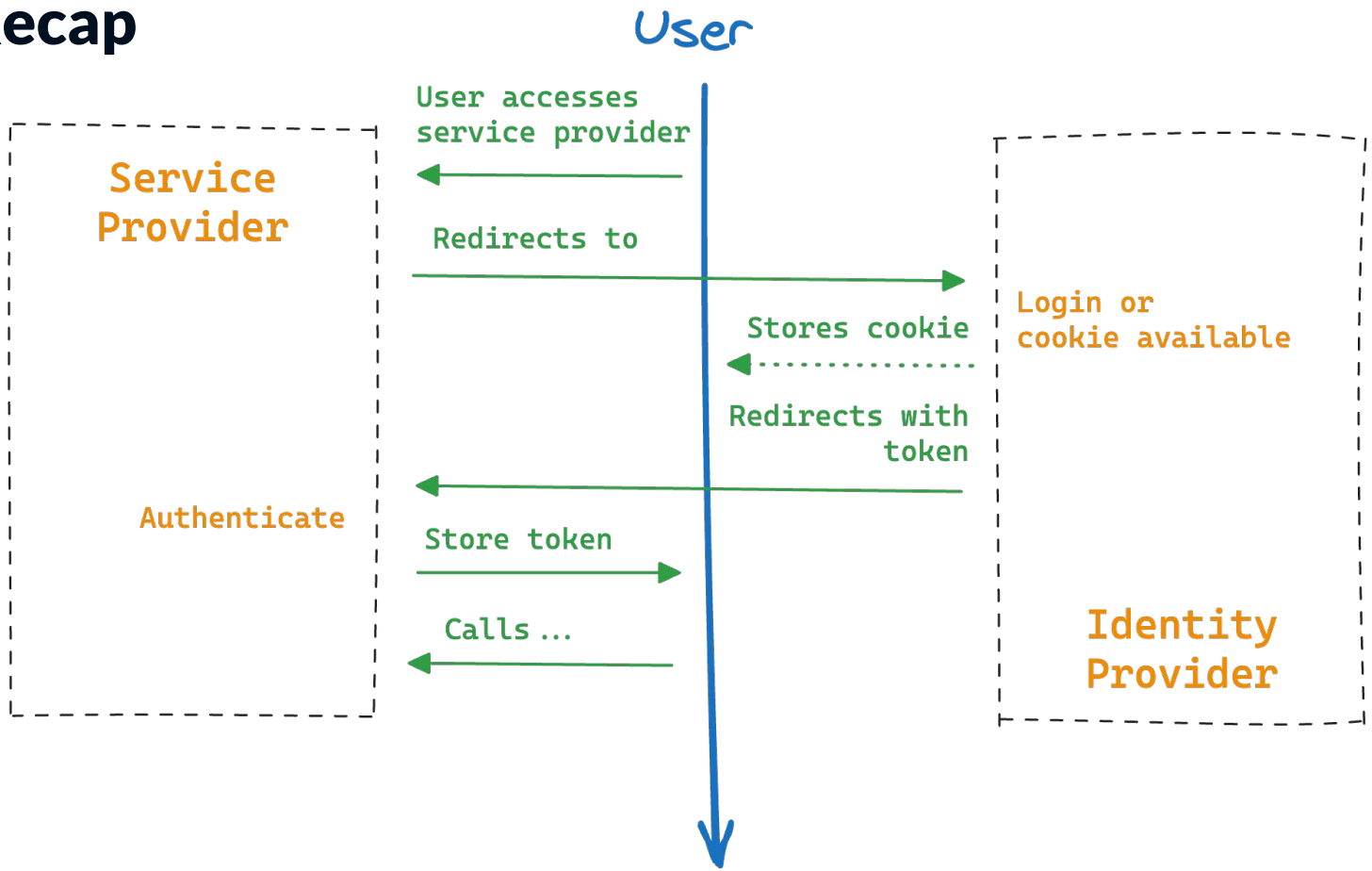
martinnirtl

Agenda

- SSO Recap
- SSO for Kubernetes
- Dex
- Beyond Authentication
- Demo



SSO Recap


User
User accesses service provider
Service Provider
Redirects to
Login or cookie available
Stores cookie
Redirects with token
Authenticate
Store token
Calls ...
Identity Provider

SSO for Kubernetes

- Why SSO for Kubernetes?
- Why is certificate-based authentication not good (enough)?
  - Long-living and cannot be revoked
  - Hard-to-manage and easy-to-lose access key
- Kubernetes Authentication Strategies
  - Client Certs, OIDC Tokens 😍, etc.

Dex

- CNCF Project
- Federated OIDC Provider
- Integrate any identity provider
  - One provider to rule them all
  - Easy ✌
- Integrates with Kubernetes
  - Via kubelogin

Name	supports refresh tokens	supports groups claim	supports preferred_username claim	status	notes
LDAP	yes	yes	yes	stable	
GitHub	yes	yes	yes	stable	
SAML 2.0	no	yes	no	stable	
GitLab	yes	yes	yes	beta	
OpenID Connect	yes	yes	yes	beta	Includes Salesforce, Azure, etc.
OAuth 2.0	no	yes	yes	alpha	
Google	yes	yes	yes	alpha	
LinkedIn	yes	no	no	beta	
Microsoft	yes	yes	no	beta	
AuthProxy	no	no	no	alpha	Authentication proxies such as Apache2 mod_auth, etc.
Bitbucket Cloud	yes	yes	no	alpha	
OpenShift	no	yes	no	stable	
Atlassian Crowd	yes	yes	yes *	beta	preferred_username claim must be configured through config
Gitea	yes	no	yes	alpha	
OpenStack Keystone	yes	yes	no	alpha	

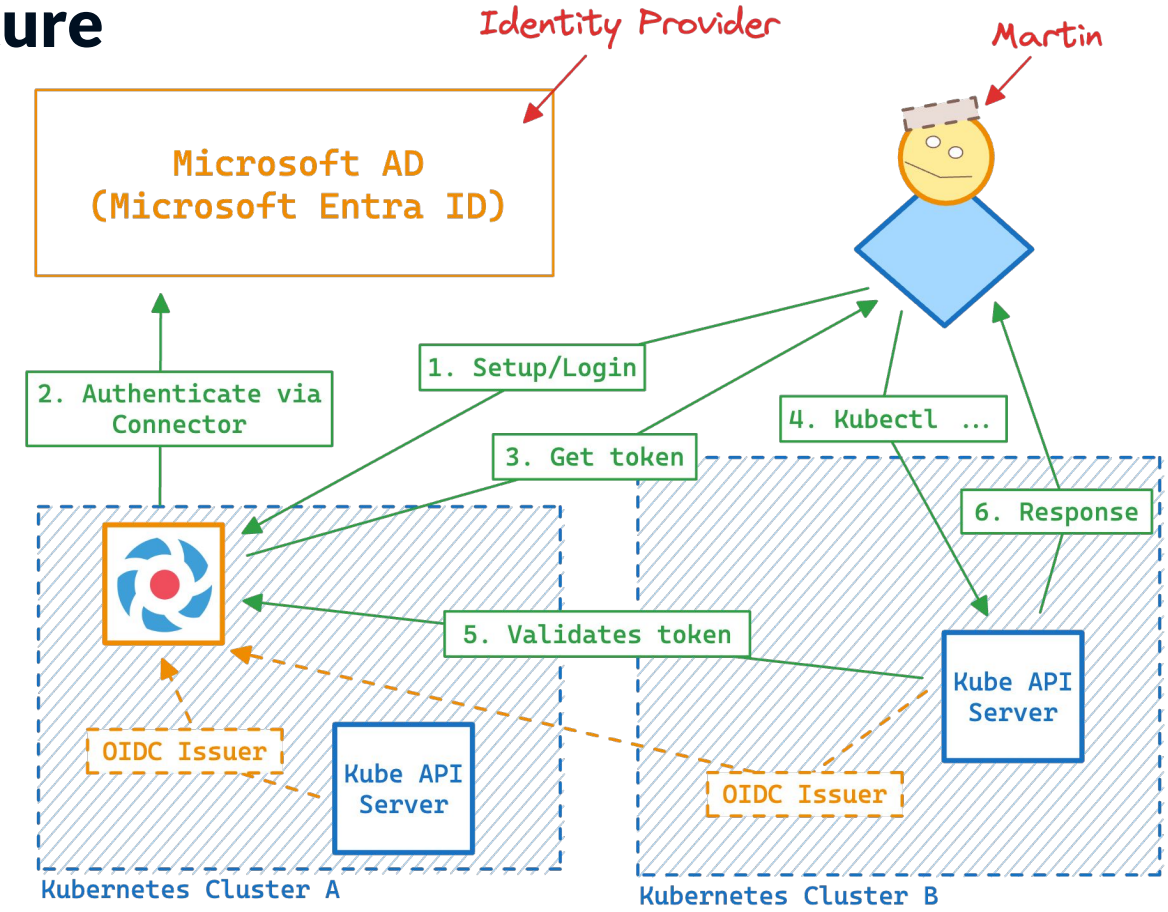
Beyond Authentication

- Authentication (authn) vs. Authorization (authz)
- CENTRAL MANAGEMENT IS KEY
- Nice tools to keep you sane (and reduce effort) 😎
  - Fairwinds RBAC Manager - Roles and Bindings on Steroids
  - Audit2RBAC - Create roles from audit logs
  - Paralus - Zero trust Kubernetes with zero friction
  - Teleport - Open Infrastructure Access Platform

Demo

Let’s get authenticated!

Architecture



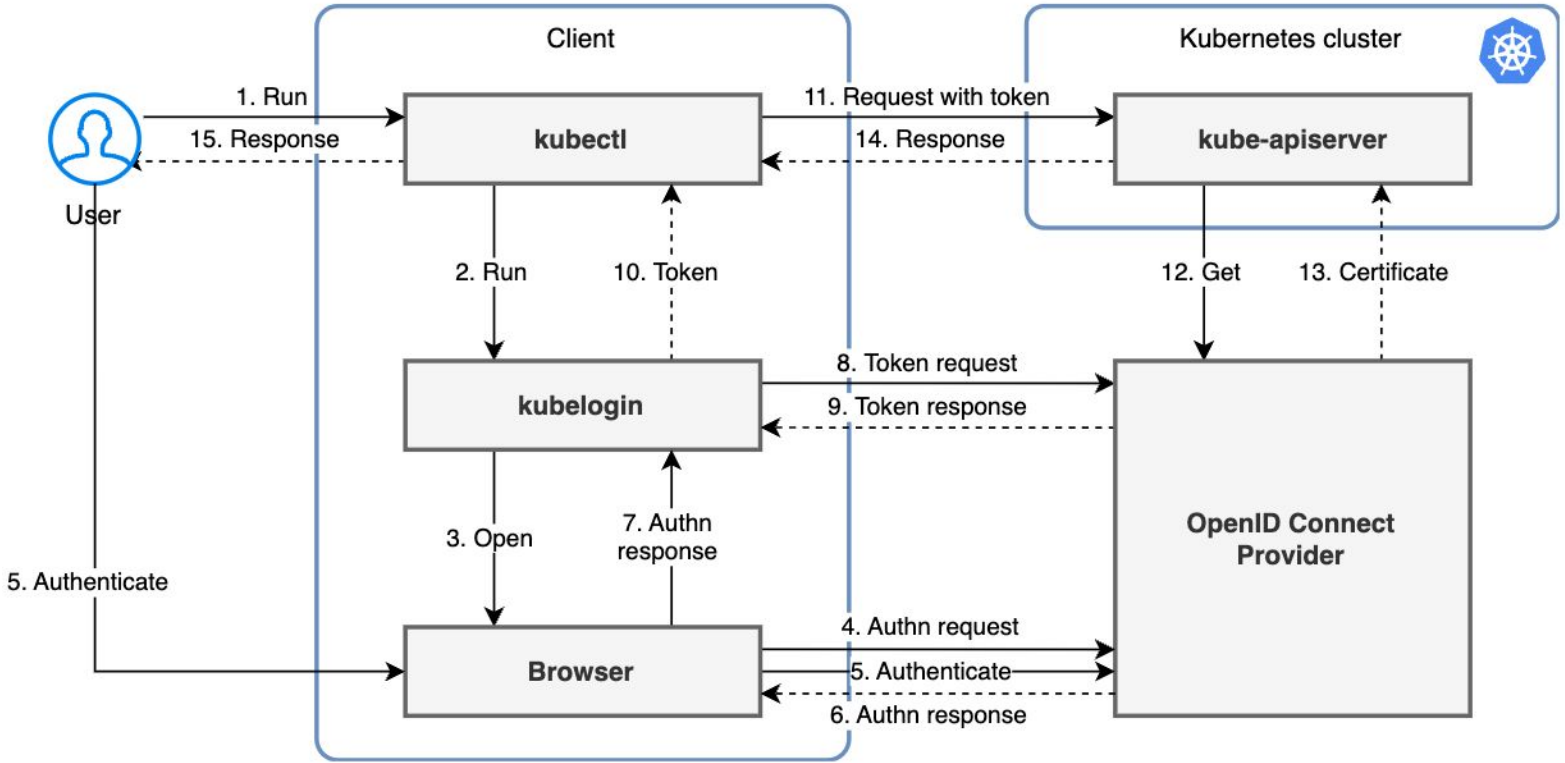
Setup and useful links

- Talk assets: https://github.com/martinnirtl/talks
  - Slides
  - Terraform files for AWS infra + k0s configuration
  - Kubernetes manifests
  - Step-by-step demo guide
- Documentation
  - Dex with Kubernetes
  - Dex with kubelogin and Microsoft AD
  - K0s configuration

Backup Slides

For disaster questions only!

Kubelogin Flow (source: https://github.com/int128/kubelogin)



Join us for Upcoming Webinars

Platform Engineering with Backstage: Getting Started

- Oct 17, 2023 at 5pm BST / 9am PST
- Featured presenters: Martin Nirtl, Solution Architect

Day 2 Operations: k0smotron & CAPI - Cluster Lifecycle Management

- Nov 14, 2023 at 5pm BST / 9am PST
- Featured presenters: Julian Hennig, Senior Solution Architect