~~Tech Talks~~ KCD Austria 2nd Chance Edition

SSO for Kubernetes Using Dex

Let's get authenticated!

$ whoami

Martin Nirtl

Solution Architect

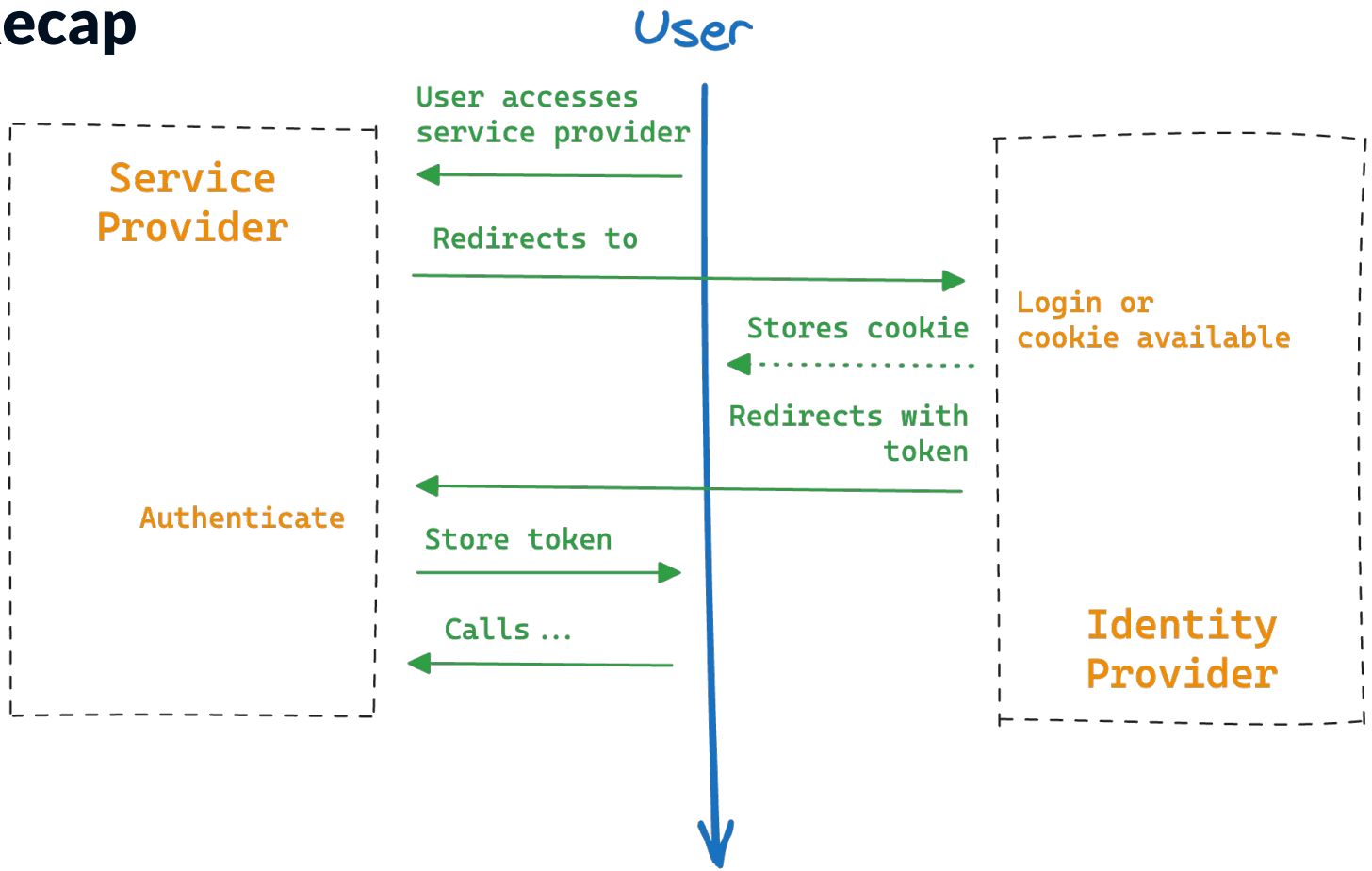
I am an IT engineer 👨‍💻 with strong backgrounds in software, DevOps/platform and electronic engineering working for Mirantis as a pre-sales solution architect. Next to my job, my main side-hustles are all around Kubernetes ⛵, IaC and automating things. From time to time, I even build little apps in Go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

martinnirtl martinnirtl martinnirtl

Single Sign-On

Let’s do a quick recap!

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

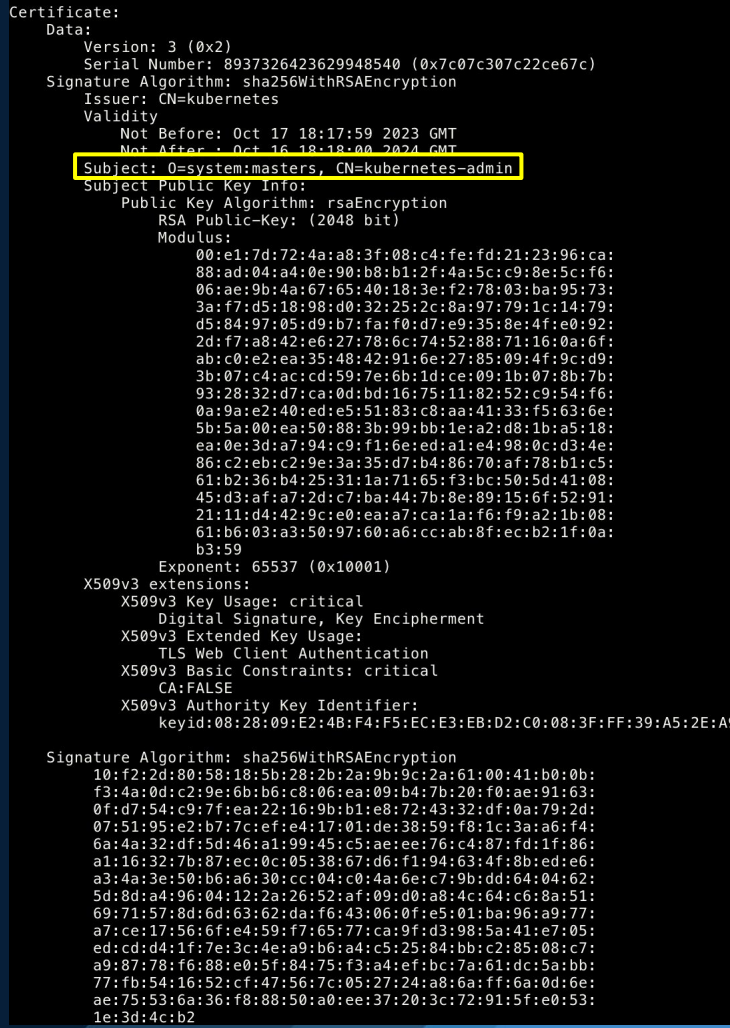
Documentation

Kubernetes Authentication

Reminder for Martin: Don’t talk too much!

X509 Client Certs

- User Info stored in Cert Subject
  - Username: Common Name (CN=)
  - Groups: Organization fields (O=)
- Requires API-Server Params
  - `client-ca-file`
  - `tls-cert-file`
  - `tls-private-key-file`
- Generate certificates manually
- Use certificates.k8s.io API



Bootstrap Tokens

- Bootstrapping new Clusters
  - Joining nodes, etc.
- Token Format
  - `<token-id>.<token-secret>`
  - `[a-z0-9]{6}\.[a-z0-9]{16}`
  - `abcdef.0123456789abcdef`
- Requires API-Server Params
  - `enable-bootstrap-token-auth`
- Authorization
  - `Bearer <token>`

Sample Bootstrap Token

Source: https://kubernetes.io/...

```yaml
apiVersion: v1
kind: Secret
metadata:
  # Name MUST be of form "bootstrap-token-<token id>"
  name: bootstrap-token-07401b
  namespace: kube-system
# Type MUST be 'bootstrap.kubernetes.io/token'
type: bootstrap.kubernetes.io/token
stringData:
  # Human readable description. Optional.
  description: "The default bootstrap token generated by 'kubeadm init'."
  # Token ID and secret. Required.
  token-id: 07401b
  token-secret: f395accd246ae52d
  # Expiration. Optional.
  expiration: 2017-03-10T03:22:11Z
  # Allowed usages.
  usage-bootstrap-authentication: "true"
  usage-bootstrap-signing: "true"
  # Extra groups to authenticate the token as. Must start with "system:bootstrappers:"
  auth-extra-groups: system:bootstrappers:worker,system:bootstrappers:ingress
```

Static Token File

- Indefinitely lasting Tokens
- CSV File
  - `<token>,<username>, <uid>,"<groups...>"`
  - File on controller nodes
- Requires API-Server Params
  - `token-auth-file`
- API restart after update required
- Authorization Header
  - `Authorization: Bearer <token>`

Webhook Token Auth

- Arbitrary Auth-API
  - Receives TokenReview Object holding opaque token
  - Responds with TokenReview Object
- User fields in TokenReview
  - `Required: username`
  - `Optional: uid, groups, extra`
- Required API-Server Params
  - `authentication-token-webhook-config-file`

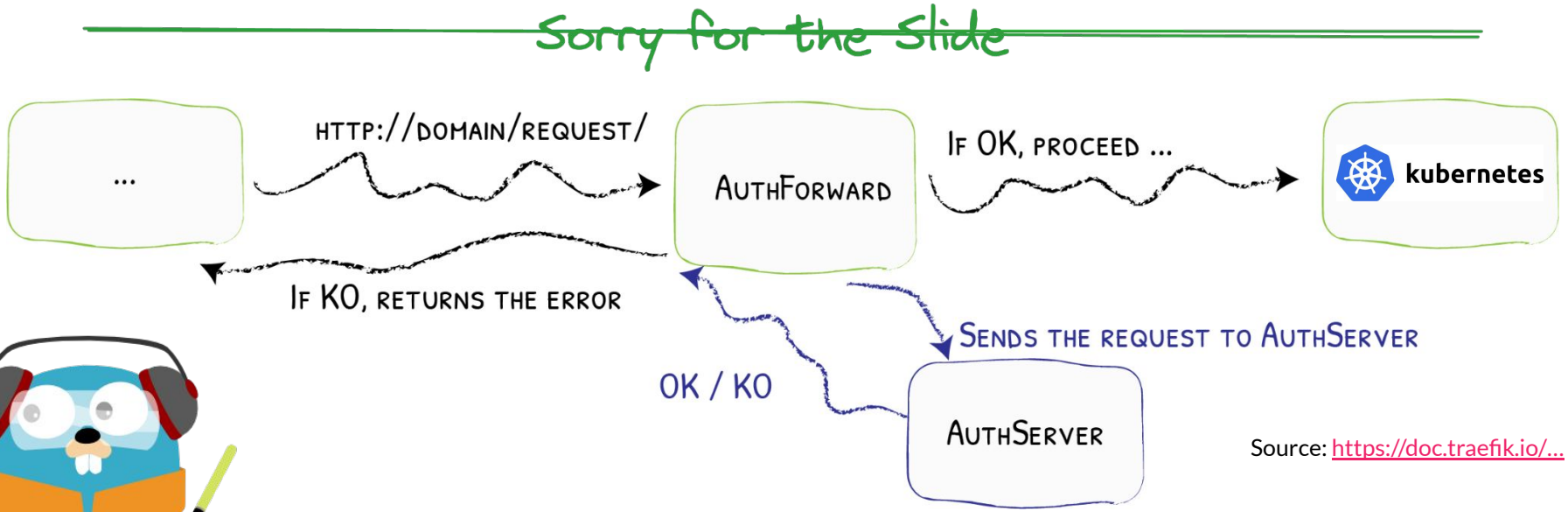
Source: https://kubernetes.io/...

```
{
  "apiVersion": "authentication.k8s.io/v1beta1",
  "kind": "TokenReview",
  "status": {
    "authenticated": true,
    "user": {
      # Required
      "username": "janedoe@example.com",
      # Optional
      "uid": "42",
      # Optional group memberships
      "groups": ["developers", "qa"],
      # Optional additional information provided by
      # This should not contain confidential data,
      # or API objects, and is made available to ad
      "extra": {
        "extrafield1": [
          "extravalue1",
          "extravalue2"
        ]
      }
    },
    # Optional list audience-aware token authentica
    # containing the audiences from the `spec.audie
    # If this is omitted, the token is considered t
    "audiences": ["https://myserver.example.com"]
  }
}
```

Authenticating Proxy

- Reverse Proxy in front of API-Server
- Example below: Traefik

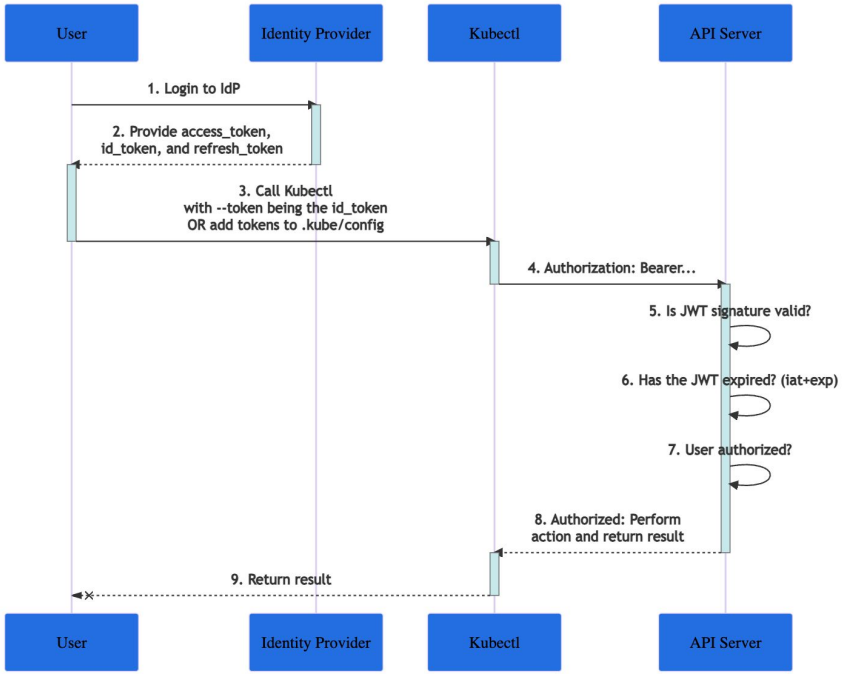
- API-Server Params
  - `Required: requestheader-username-headers`
  - `requestheader-group-headers`
  - `requestheader-extra-headers-prefix`
  - `Required: requestheader-client-ca-file`
  - `requestheader-allowed-names`



Source: https://doc.traefik.io/...

OpenID Connect Tokens 💝

- Allows SSO Flow
  - Integrate Directory Services & IAM
  - Central User Management
- OIDC extends OAuth2
  - Uses `id_token` (not `access_token`)
  - JSON Web Token (JWT)
- API-Server Params
  - `oidc-issuer-url`
  - `oidc-client-id`



Service Account Tokens

- Associated with Pods
  - Operators, Controllers, etc.
- Workload Identity
  - `service-account-issuer`
  - `service-account-jwks-uri`
- Optional API-Server Params
  - `service-account-key-file`
  - `service-account-lookup`
- JSON Web Token (JWT)
- Can be stored in Secrets!

Kube Auth Strategies Docs

- X509 Client Certs
- Bootstrap Tokens
- Static Token File
- Webhook Token Auth
- Authenticating Proxy
- OpenID Connect Tokens
- Service Account Tokens
- Anonymous Requests

Good to know:

➔ Multiple modules possible

➔ First success short-circuits evaluation

➔ API server does not guarantee order

➔ Enable at least SA tokens and one user auth module

Comparison

OpenID Connect Tokens	X509 Client Certs
✅ Central	❌ Distributed
✅ Short living	❌ Long-living
✅ Easy to manage	❌ Hard to manage
✅ No	❌ Easy to lose
Enterprise-grade Tooling ✌️	Can be automated 😅 (Look left)

Dex

A Federated OpenID Connect Provider

Dex

dexidp.io

- CNCF Project
- Federated OIDC Provider
- Integrate any Identity Provider
  - One Tool to Rule Them All 💍
  - Easy ✌
- Integrates with Kubernetes
  - Via kubelogin

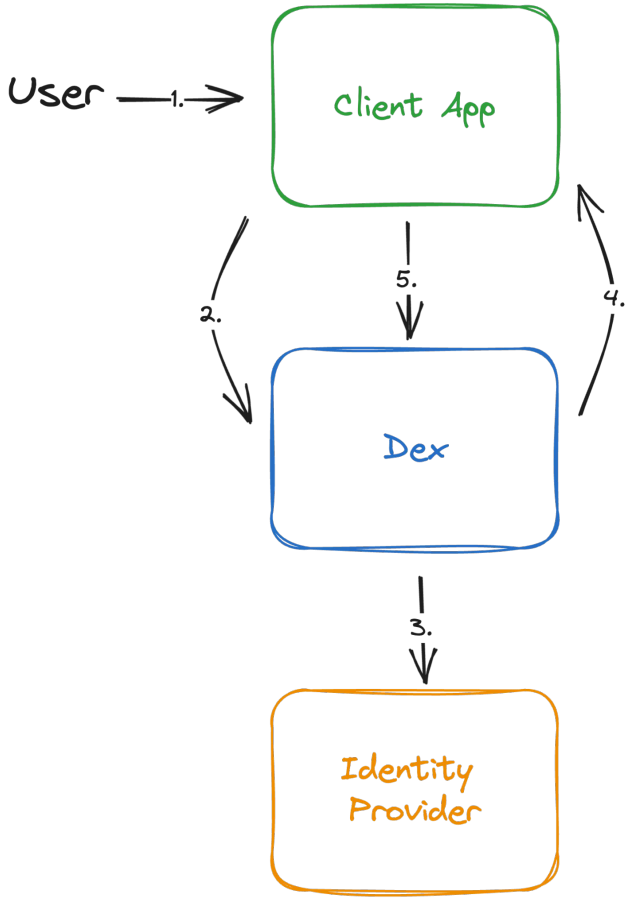
Source: https://dexidp.io/...

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	

Dex Flow 🏄 Read more...

1. User visits client app
2. App redirects user to Dex with OAuth2 request
3. Dex determines user's ID
4. Dex redirects user back with a code
5. App uses code to exchange for a token (ID token)

Dex is not bound to Kubernetes!

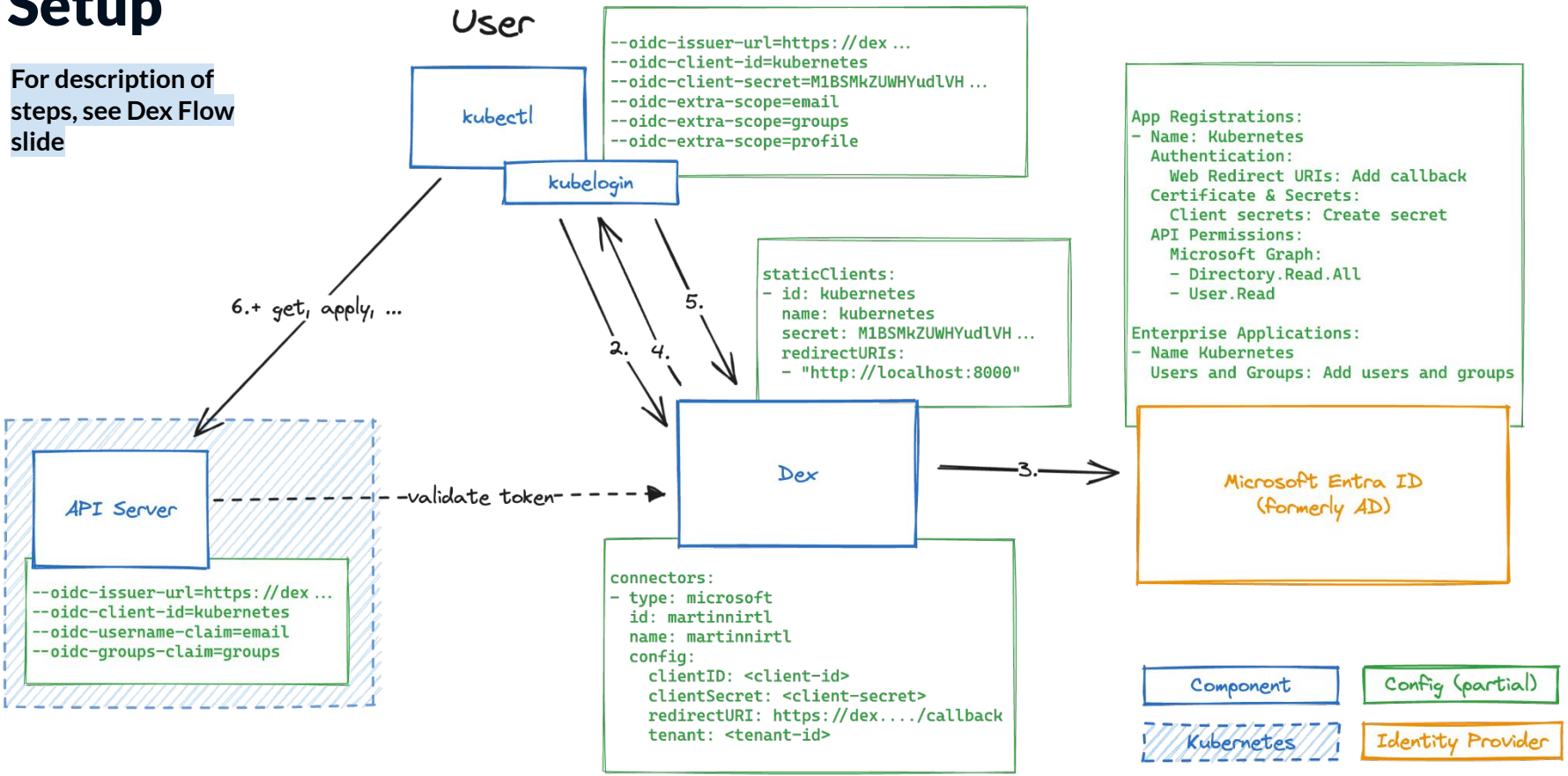


Demo

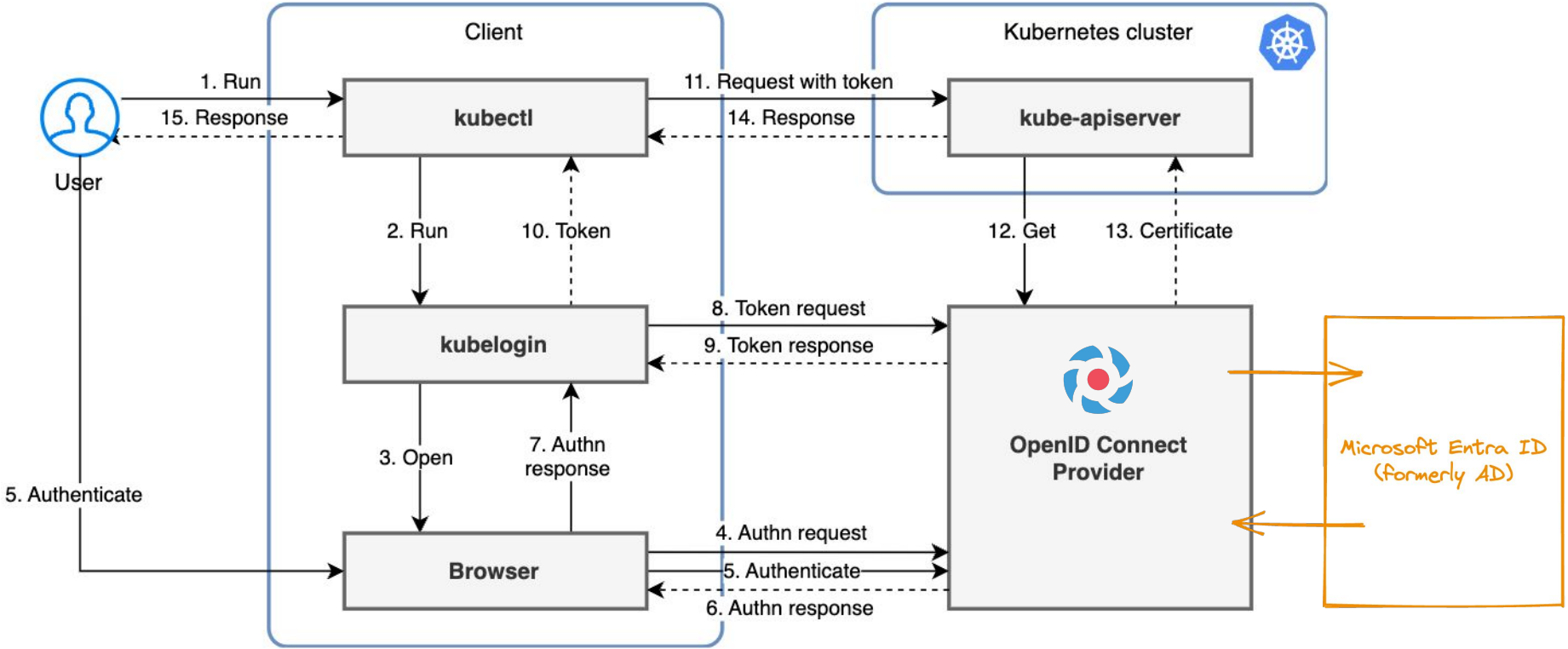
Let’s get authenticated!

Setup

For description of steps, see Dex Flow slide



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



Beyond Authentication

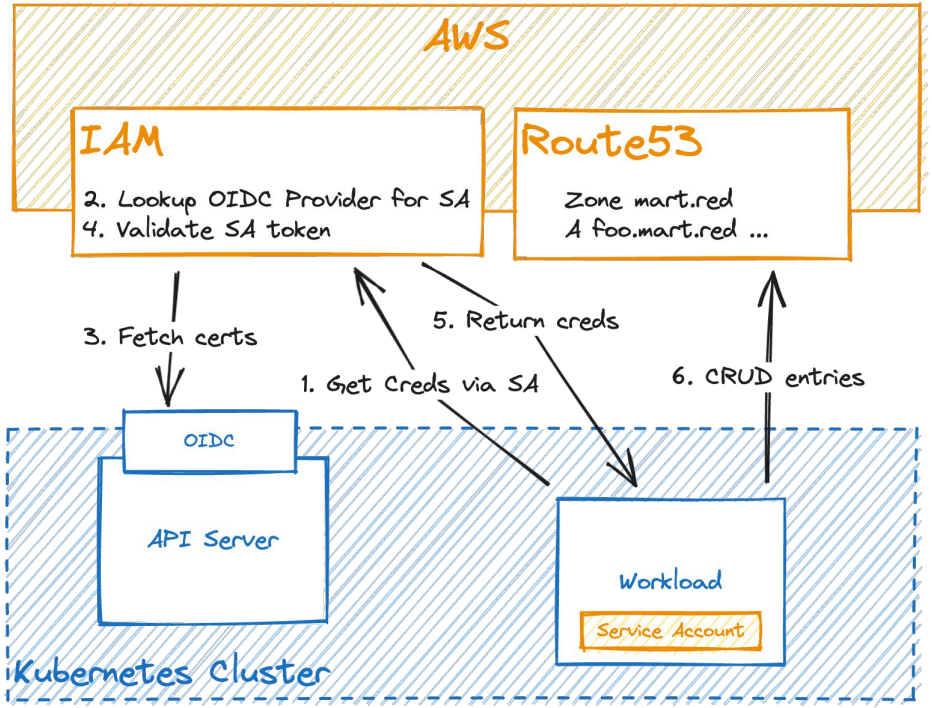
Hmm… What else could there be?

Authorization

- AUTHN vs. AUTHZ
- Central Management and Standardized Roles are Key!
- Nice tools to keep you sane (and reduce effort) 😎
  - Fairwinds' RBAC Manager - Roles and Bindings on Steroids
  - Fairwinds' RBAC Lookup - Search roles for a user, service-account or group
  - Audit2RBAC - Create roles from audit logs
  - Paralus - Zero trust Kubernetes with zero friction
  - Teleport - Open Infrastructure Access Platform

Workload Identity

- Assign identities to Workloads
  - E.g. Assume IAM role on AWS
  - Available on GKE & AKS as well
  - No explicit credentials needed
- Uses SA token to retrieve credentials
- OIDC used to verify token
  - OpenID Config Doc
  - JSON Web Key Set (JWKS)



SA... Service Account

Logout

Signed out successfully!