Portable, Universal, Single Sign-On for Your Clusters

Miguel Martinez @migmartri
May 21st, Kubecon EU

bitnami

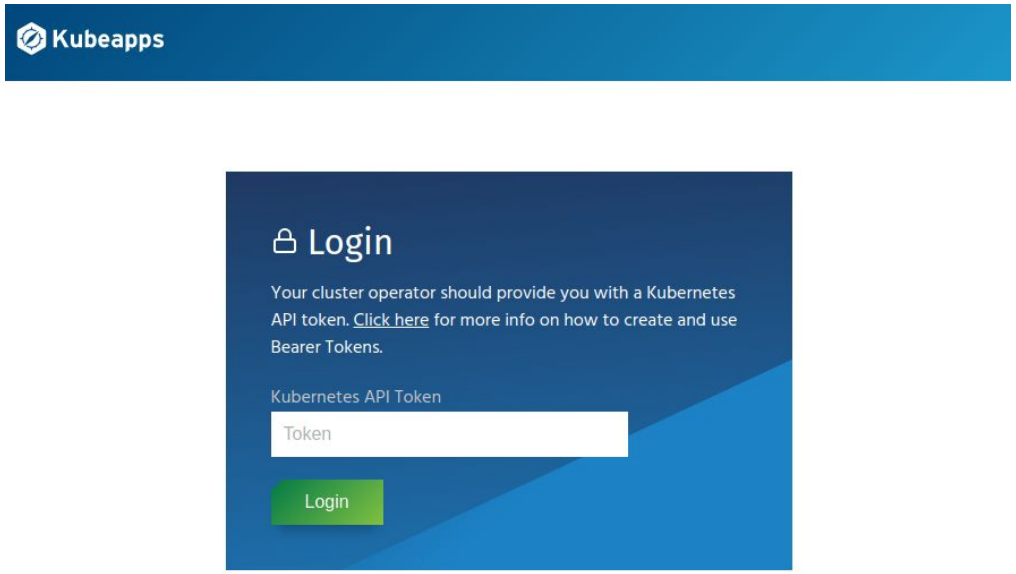
Hi, I am Miguel!

- Spaniard in San Francisco, obsessed with Mexican food
- Full-stack developer at Bitnami
- Core contributor of Kubeapps and Monocular
- Emeritus core maintainer in Helm

@migmartri

Our problem

Support Single Sign-on in Kubeapps



- Only supported service accounts
- Adoption barrier
- Best practices blocker, RBAC is hard

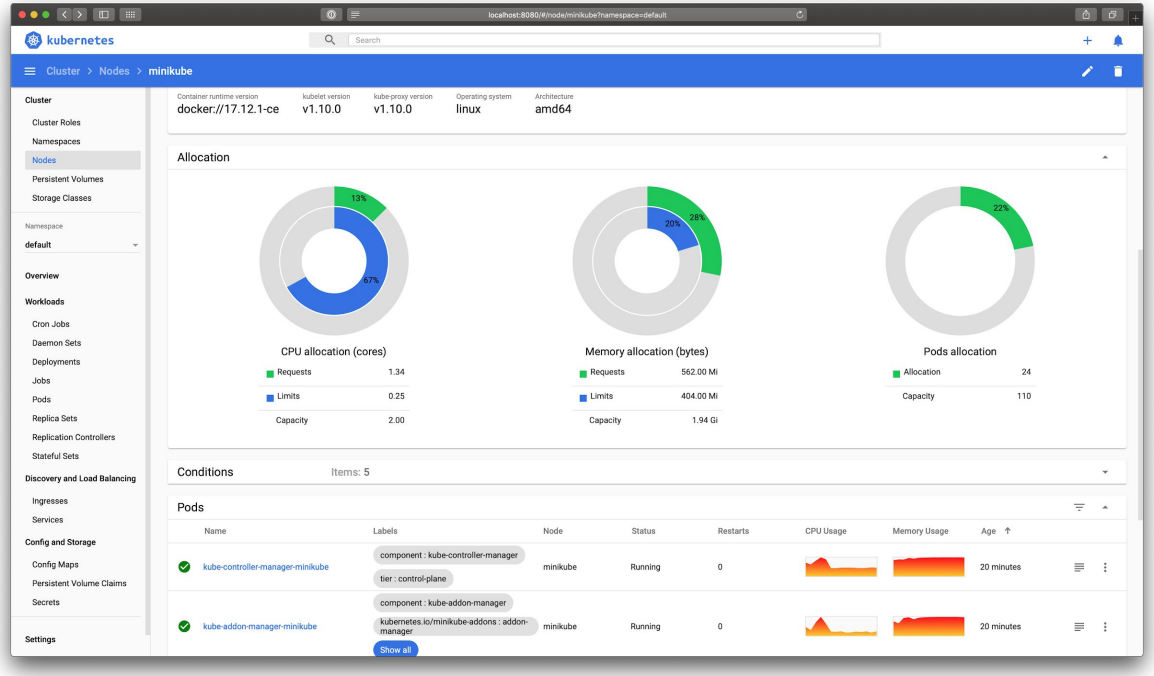
Single sign-on, most requested feature

bitnami

Kubeapps OIDC support in-depth design document

Our problem

General Statement



Application (YourApp) that

1. AuthN users via Single sign-on
2. **Talks to the k8s API server**

i.e kubectl, Kubernetes Dashboard, Kubeapps

bitnami

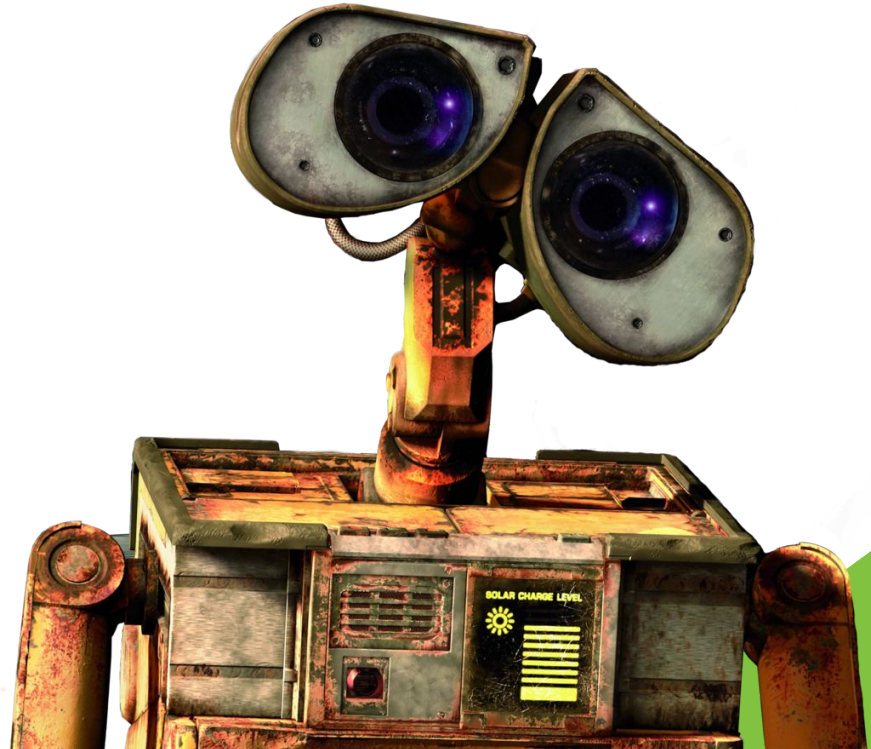
Our problem

Solution Scope and Caveats

AuthN vs ~~AuthZ~~

Platform ~~dependent~~ vs Independent

~~Robots~~ vs Humans



bitnami

AuthN in Kubernetes

User Authentication Overview

	Self-serve	Rotation	Revocation	UX
X509 Client Certs				
Token (SA or Static)				
Basic Auth				
Single sign-on - OpenID Connect				

SSO in Kubernetes

Why?

For Users

- Familiar AuthN mechanism
- No need to have additional set of credentials
- Self-serve

For Cluster Operators

- No manual generation or transfer of credentials
- Built-in rotation and revocation methods
- AuthN delegation
- Support for groups and scopes

SSO in Kubernetes

Kubernetes API understands
OpenID Connect (OIDC)

OAuth2 != OIDC!

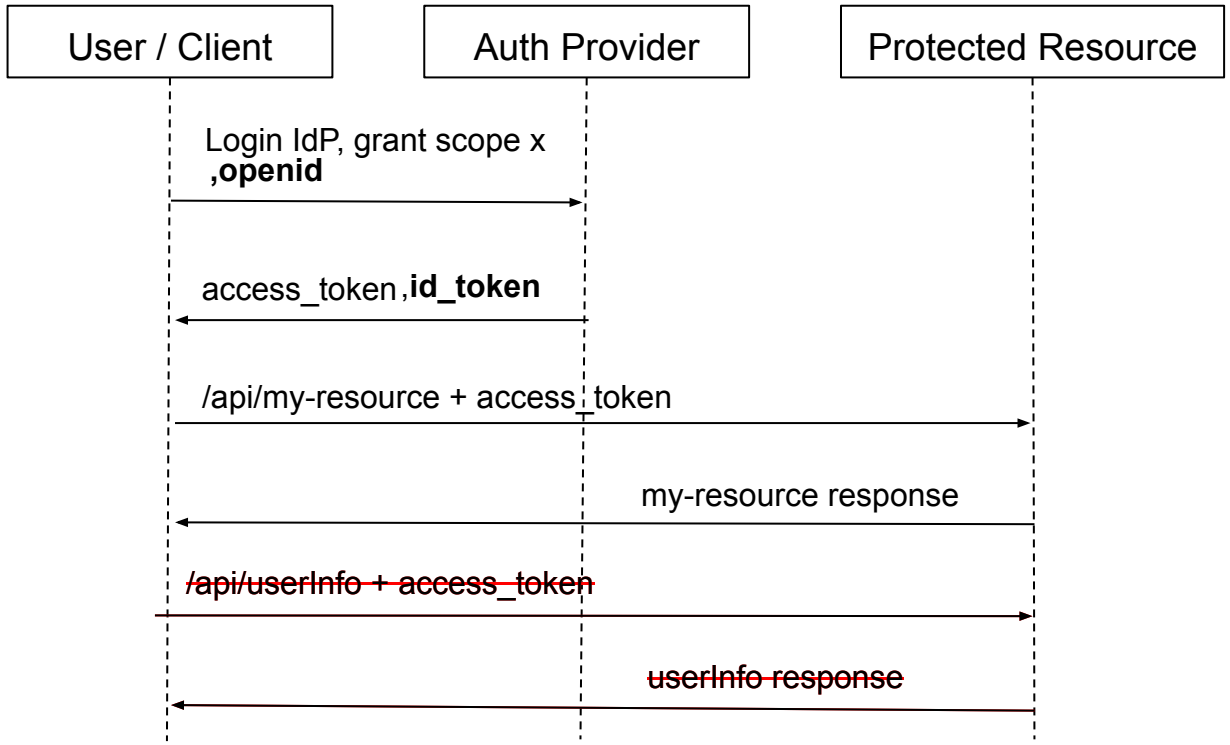
bitnami

SSO in Kubernetes

OpenID Connect (OIDC)

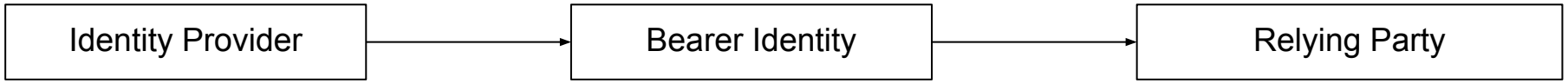
Identity layer **on top of** the OAuth 2.0 protocol

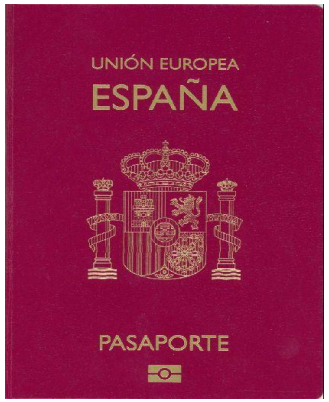
Authentication Info **standardized** in a **cryptographically signed JWT token** called id_token



SSO in Kubernetes

OpenID Connect - Trust Chain In Real Life





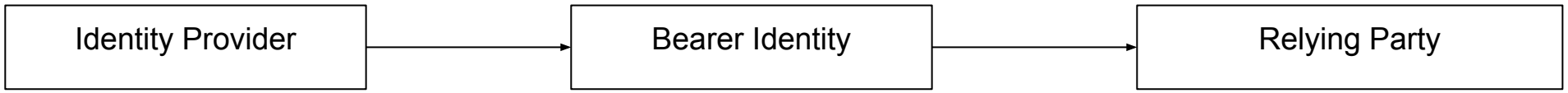
- Verify Identity
- Craft Passport

- It is from a trusted source
- It has not been tampered with (ePassport)
- It is not expired

The relying party does not contact the identity provider

SSO in Kubernetes

OpenID Connect - Trust Chain in Kubernetes



ID Token (JWT)

- Header
- Payload
  - Identity (sub/email)
  - Who provisioned this token (**iss**)
  - Intended client audience (**aud**)
  - Expiration time (**exp**)
  - Claims (name, email, ...)
- **Signature**

K8s API Server

3rd party app

- It has not been tampered with (**signature**)
- It is from a trusted source (**iss**)
- I am the receiver (**aud**)
- It is not expired (**exp**)
- **DOES NOT contact the IdP (except to retrieve the Public Key)**

SSO in Kubernetes

Integration

You need to configure the K8s API server
to trust an OIDC Identity Provider

```
# API server flags

--oidc-issuer-url https://my-oidc-idP.com # .../.well-known/openid-configuration
--oidc-client-id my-client-id
--oidc-username-claim email
--oidc-groups-claim groups

# oidc-issuer.match(id_token.iss) && oidc-client-id.match(id_token.aud)
```

```
$ curl https://api-server -H "Authorization: Bearer ${id_token}"

$ kubectl --token ${id_token}
```

bitnami https://kubernetes.io/docs/reference/access-authn-authz/authentication/

Problem Statement

Summary

Application (YourApp) that:

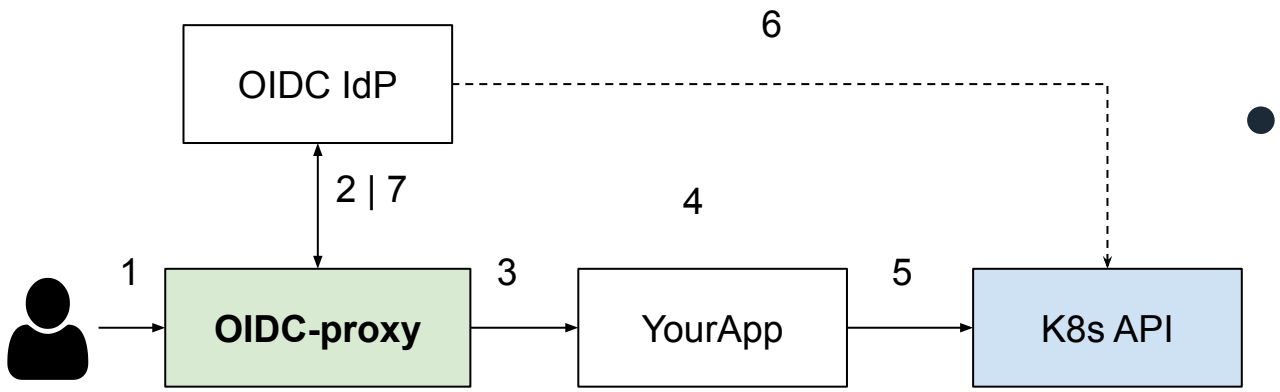
1. AuthN users via OIDC single sign-on
2. Talks directly to the k8s API server

i.e kubectl, Kubernetes Dashboard, Kubeapps

Problem Statement

Solution

Proxy configured with the **same OIDC IdP than the k8s API server ***

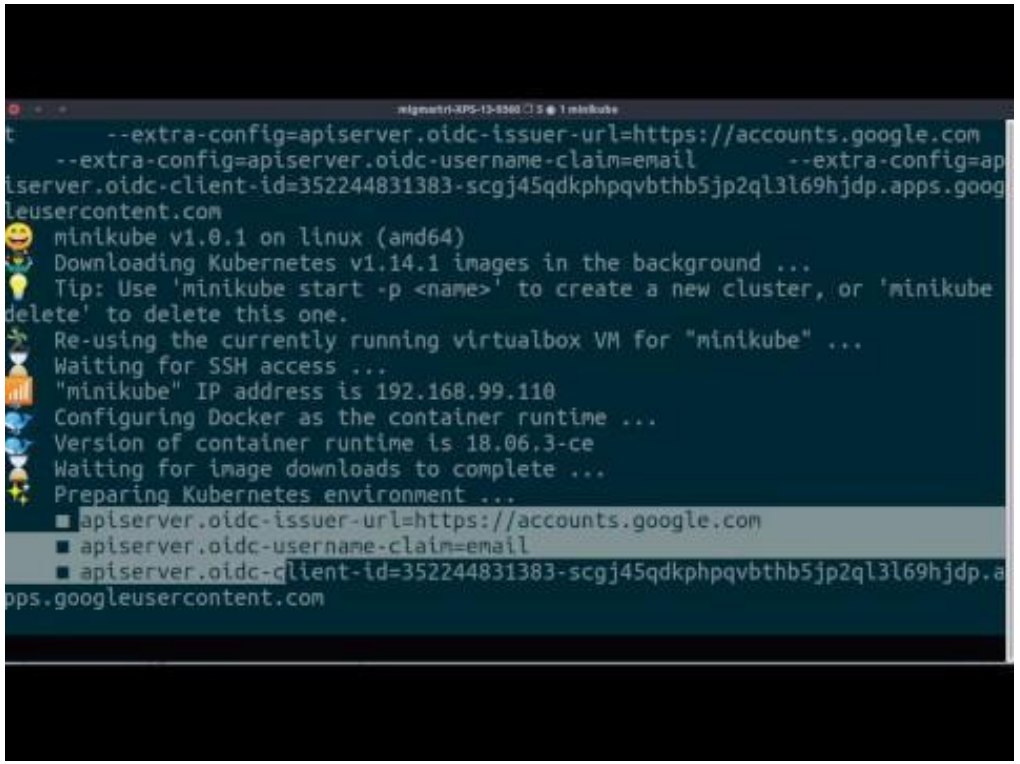


- Enforce AuthN with an external IdP
- Takes care of the OAuth2 dance, token exchange and refresh
- Inject ID Headers and forward them upstream

Problem Statement

Demo, Exclamation Mark

SSO-enabled Kubernetes Dashboard
+ Google's IdP on Minikube



Problem Statement

We Are Not Done Yet

The solution does not work in all platforms

- K8s provider API server lockdown
- Ops do not want OIDC enabled in k8s API
- IdP or authN requirements mismatch (LDAP)
- IdP groups/user claim support

Problem Statement

Challenge 1: K8s API Server OIDC Customisation

Kubernetes Distro	API Server OIDC Customization
GKE (Google)	No
EKS (AWS)	No
AKS (Azure)	Active Directory
OKE (Oracle)	Oracle Identity Cloud Service
Minikube	Any
Kops	Any
kubeadm	Any

Problem Statement

Challenge 2: Identity Providers and Group Claims

```
subjects:
- kind: Group
  name: "kubeapps:developer"
  apiGroup: rbac.authorization.k8s.io
```

OIDC Identity Provider	Group Claims Support
Okta	
Dex	Depends on Upstream
Keycloak	
Active Directory	
Google Accounts	
...	...

```
--oidc-groups-claim "groups" # API flag
```

bitnami

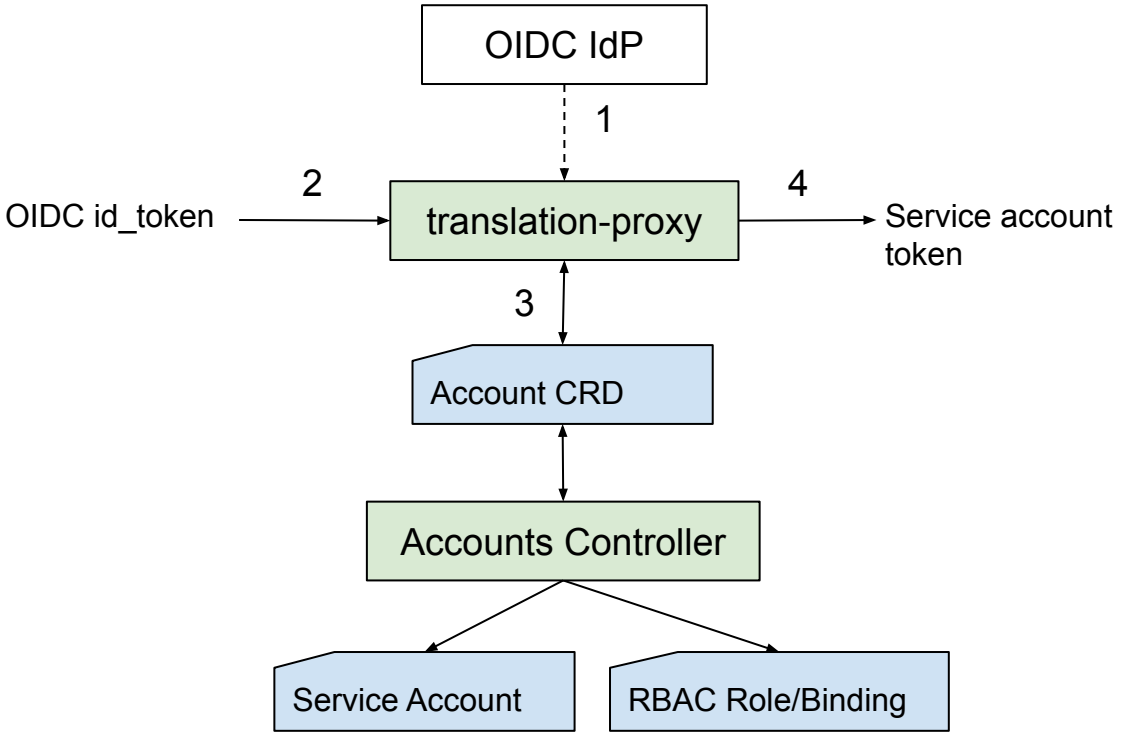
> Easy things should be easy, and hard things should be possible.

Larry Wall

Workaround 1

Translation to Service Accounts

Translate OIDC **id_tokens into service accounts** via a translation proxy and a custom controller



Workaround 2

Kubernetes Impersonation

```
$ kubectl get pods --as FooUser --as-group kubeapps-user


$ curl https://api-server/api/v1/pods \
  -H "Authorization: Bearer ${impersonator token}" \
  -H "Impersonate-User: FooUser"
  -H "Impersonate-Group: kubeapps-user"
```

Can ImpersonatorUser impersonate FooUser?

→

Can FooUser access pods in namespace x?

```
- apiGroups: [""]
  resources: ["groups"]
  verbs: ["impersonate"]
  resourceNames:
["developers","kubeapps-user"]
```

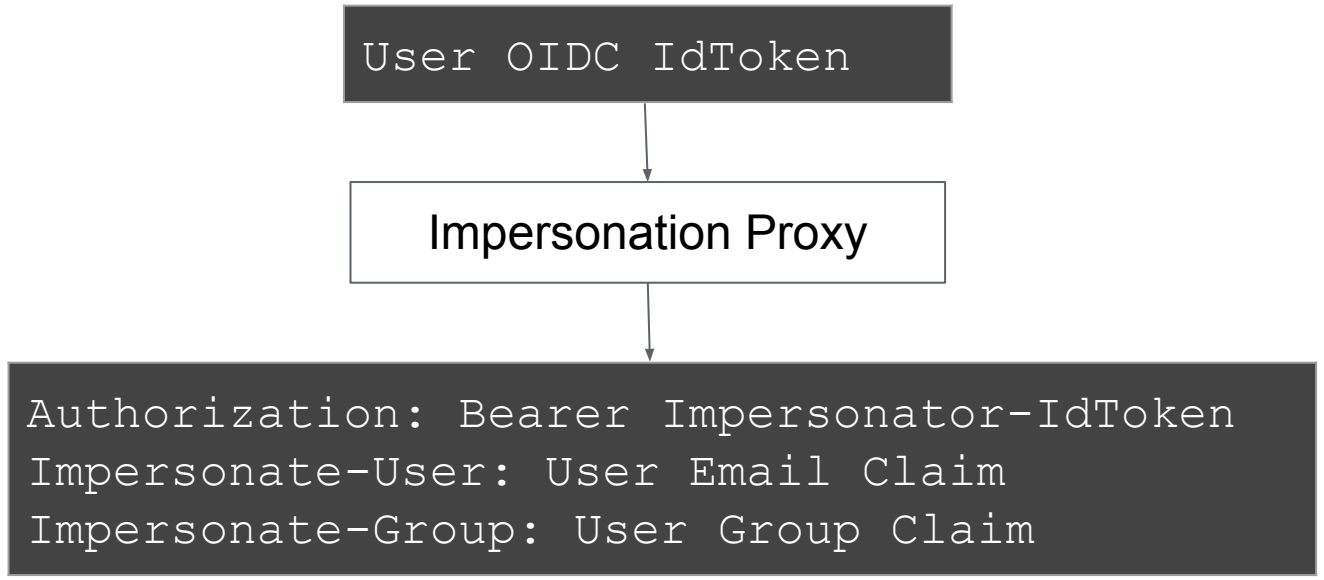
bitnami

https://kubernetes.io/docs/reference/access-authn-authz/authentication/#user-impersonation

Workaround 2

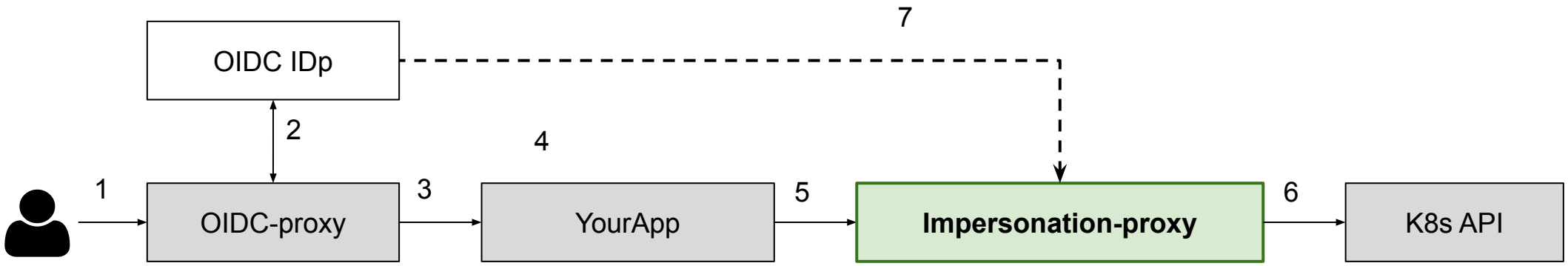
Kubernetes Impersonation

Proxy in charge of impersonating users and groups based on OIDC id_token claims



Workaround 2

Kubernetes Impersonation

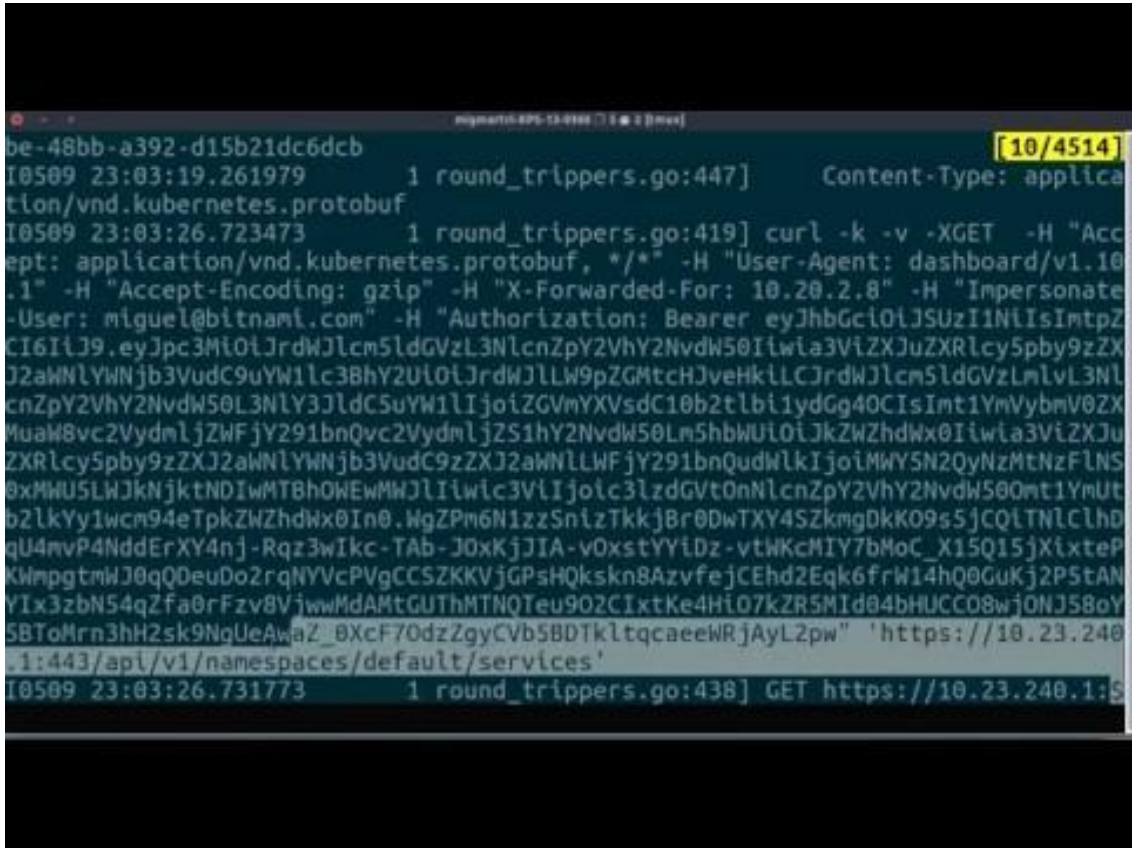


- Extracts OIDC verification logic from API server
- Prevent stale credentials
- Fewer moving pieces
- Single leak source

Workarounds

Kubernetes Impersonation

SSO-enabled Kubernetes Dashboard + Google's IdP on **GKE*** using impersonation



*** API server not configurable**

bitnami https://github.com/jetstack/kube-oidc-proxy

SSO in Kubernetes can be **vendor locked** but we can **workaround** it and offer a Universal, **Cross-Platform SSO experience**

Resources

- Kubeapps SSO in-depth document - https://bit.ly/30bi1zF
- SSO for Kubernetes talk by Joel Speed - https://bit.ly/2Hh6kQN
- kube-oidc-proxy - @jetstack - https://bit.ly/2Vip6uw
- Demo files repository - https://bit.ly/2HfV9GI
- This slide deck - https://bit.ly/2WD8YoT


@migmartri

Thank You