It's My HomeLab

Why Would I Want SSO?

Matt Williams – Evangelist @ Infra
matt@infrahq.com | @technovangelist

infra

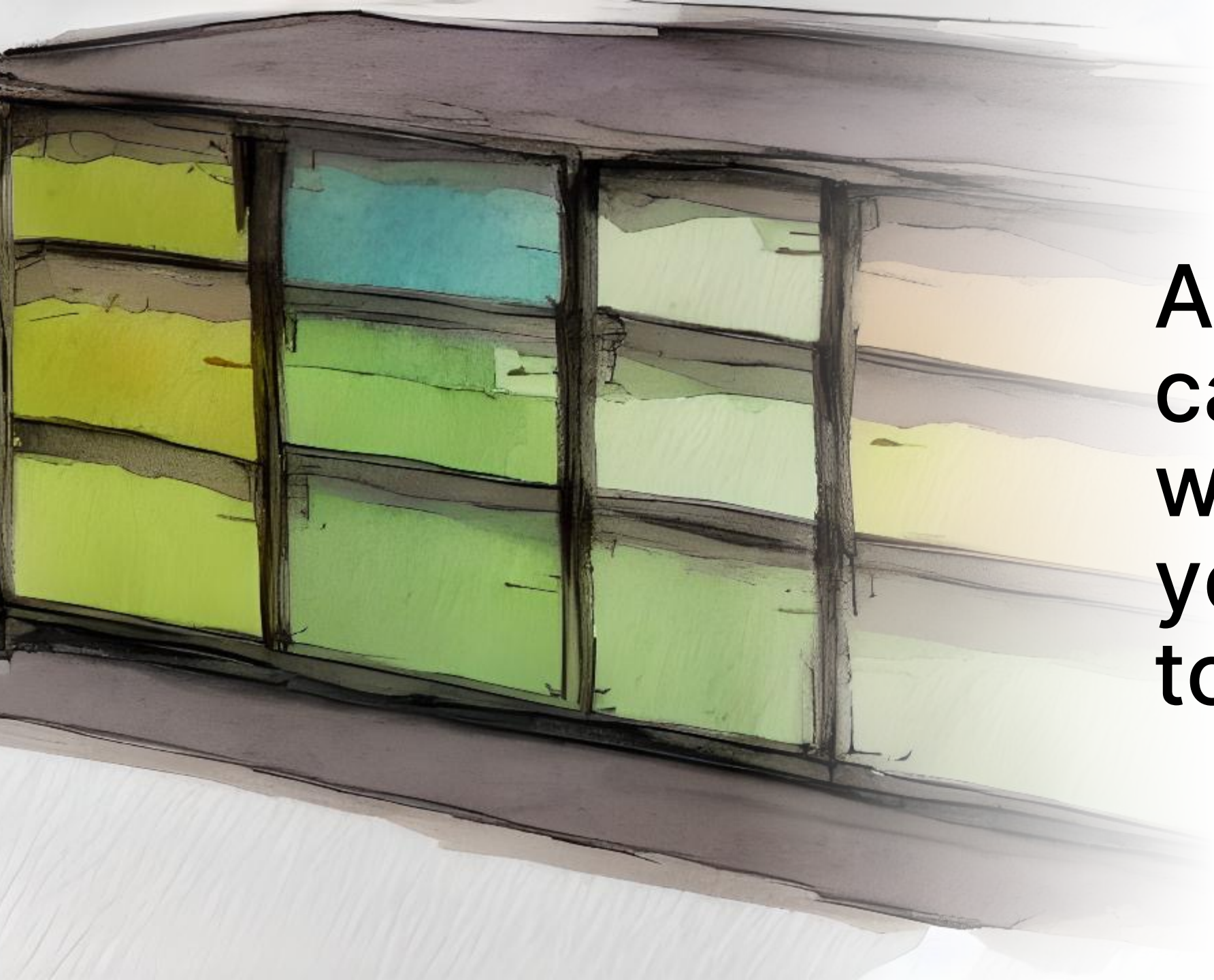
It's My HomeLab

Why Would I Want Single Sign On? Or Roles? Or Users?

* Specific to Kubernetes

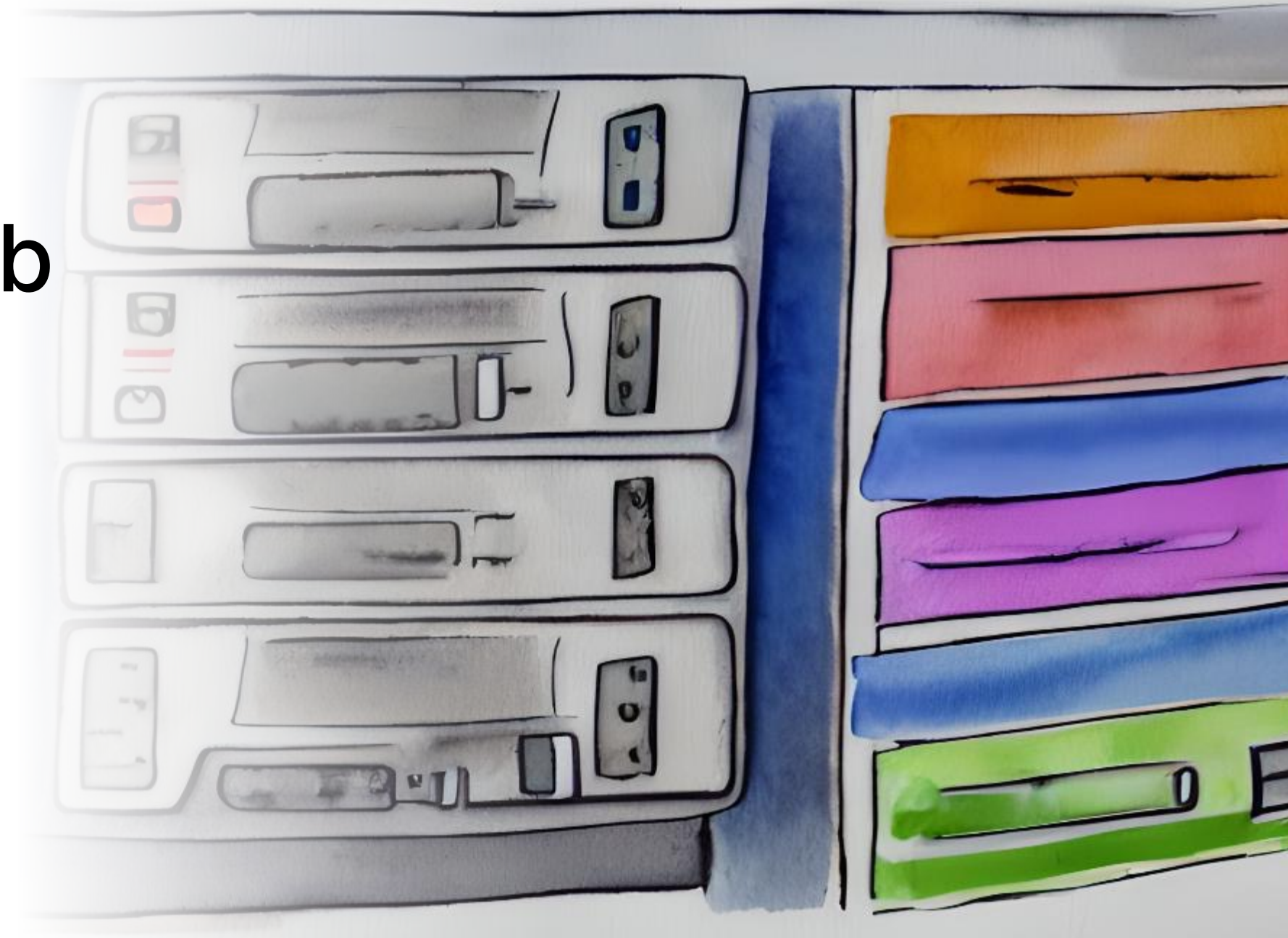
Matt Williams – Evangelist @ Infra
matt@infrahq.com | @technovangelist

infra



A HomeLab can be whatever you want it to be.

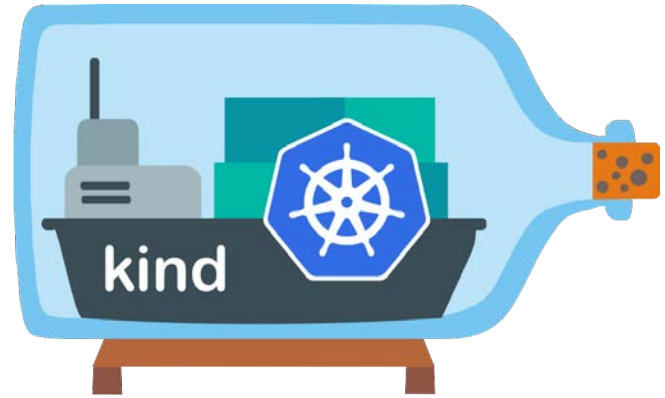
A HomeLab can be made of whatever you have



My first HomeLab was...

My HomeLab Today

PROXMOX

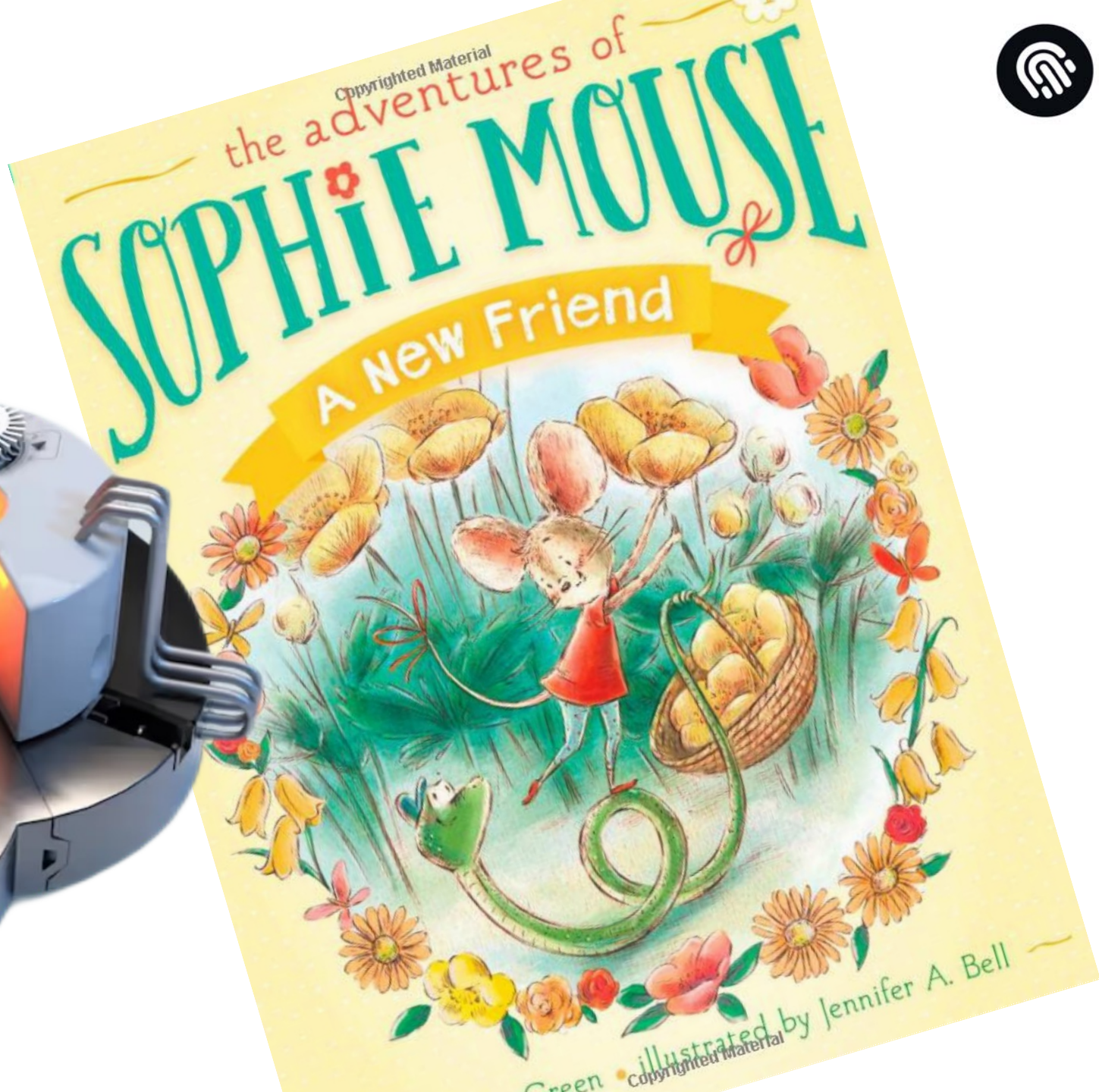


TrueNAS
OPEN STORAGE

portainer.io

K3S


TEKIT


Copyrighted Material
the adventures of
SOPHIE MOUSE
A New Friend
illustrated by Jennifer A. Bell
Copyrighted Material


6:55 PM Thu Oct 13
100%
Trash
10/19/2022 in 6 days
Recycling
10/19/2022 in 6 days
Yard Waste
10/26/2022 in 13 days
Living Rm
Dining Rm
Chandelier
Accent
Morning
Cook/Prep
Dine
Entertain


amazon
web services


ORACLE
CLOUD

Kubernetes in the HomeLab

Can take advantage of a hodgepodge of machines

Kubernetes in the HomeLab

Consistent Deployments

Why Users and Roles in K8S at Home?

Kubernetes: What is a User?

- They don’t exist

  - or –

- A signed certificate in a kubeconfig file

```
apiVersion: v1
clusters:
- cluster:
    certificate-authority-data: certgoeshere
    server: https://clusterendpoint.k8s.ondigitalocean.com
  name: mycluster
contexts:
- context:
    cluster: mycluster
    user: do-sfo3-matt-primary-admin
  name: mycontext
current-context: mycontext
kind: Config
preferences: {}
users:
- name: do-sfo3-matt-primary-admin
  user:
    token: dop_v1_dea9d7ff2b8eb092f53ffebogus31d2bd4602a62a19b5ac4
```

```
apiVersion: v1
clusters:
- cluster:
    certificate-authority-data: certgoeshere
    server: https://clusterendpoint.k8s.ondigitalocean.com
  name: mycluster
contexts:
- context:
    cluster: mycluster
    user: do-sfo3-matt-primary-admin
  name: mycontext
current-context: mycontext
kind: Config
preferences: {}
users:
- name: do-sfo3-matt-primary-admin
  user:
    token: dop_v1_dea9d7ff2b8eb092f53ffebogus31d2bd4602a62a19b5ac4
```

```
apiVersion: v1
clusters:
- cluster:
    certificate-authority-data: certgoeshere
    server: https://clusterendpoint.k8s.ondigitalocean.com
  name: mycluster
contexts:
- context:
    cluster: mycluster
    user: do-sfo3-matt-primary-admin
  name: mycontext
current-context: mycontext
kind: Config
preferences: {}
users:
- name: do-sfo3-matt-primary-admin
  user:
    token: dop_v1_dea9d7ff2b8eb092f53ffebogus31d2bd4602a62a19b5ac4
```

```
apiVersion: v1
clusters:
- cluster:
    certificate-authority-data: certgoeshere
    server: https://clusterendpoint.k8s.ondigitalocean.com
  name: mycluster
contexts:
- context:
    cluster: mycluster
    user: do-sfo3-matt-primary-admin
  name: mycontext
current-context: mycontext
kind: Config
preferences: {}
users:
- name: do-sfo3-matt-primary-admin
  user:
    token: dop_v1_dea9d7ff2b8eb092f53ffebogus31d2bd4602a62a19b5ac4
```

Kubernetes: What is a Role?

- Defines the level of access a ‘user’ has to the cluster
  - Resource
  - Verb

Kubernetes: What is a Role?

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: marketing-dev
  labels:
    app.infrahq.com/include-role: "true"
rules:
  - apiGroups: [""] # "" indicates the core API group
    resources: ["pods"]
    verbs: ["get", "watch", "list"]
```

Kubernetes: What is a Role?

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: marketing-dev
  labels:
    app.infrahq.com/include-role: "true"
rules:
  - apiGroups: [""] # "" indicates the core API group
    resources: ["pods"]
    verbs: ["get", "watch", "list"]
```

Kubernetes: What is a Role?

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: marketing-dev
  labels:
    app.infrahq.com/include-role: "true"
rules:
  - apiGroups: [""] # "" indicates the core API group
    resources: ["pods"]
    verbs: ["get", "watch", "list"]
```

Kubernetes: What is a Role?

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: marketing-dev
  labels:
    app.infrahq.com/include-role: "true"
rules:
  - apiGroups: [""] # "" indicates the core API group
    resources: ["pods"]
    verbs: ["get", "watch", "list"]
```

How to create a User

- Create the user key `(openssl genpkey…)`
- Create the CSR `(openssl req -new)`
- Submit the CSR to the cluster (yaml)
- Approve the request `(kubectl certificate approve…)`

How to create a User

- Get the approved request (`kubectl get csr…`)
- Build the kubeconfig (`kubectl --kubeconfig myuserconfig config set-credentials`, `kubectl --kubeconfig myuserconfig configset-context`)
- Then distribute the file

https://infrahq.com/blog/how-to-create-users

How to create a User

- And then repeat often
  - ensure bad parties can’t access

- And redistribute

Just give everyone admin???

- What happens when
  - User fired
  - User compromised

- Kubernetes is Remote Execution as a Service

Can we automate it?

master kubernetes-adduser / add-user.sh

Go to file ...

brendanburns Updates. Latest commit 6d53ffe on Nov 2, 2021 History

1 contributor

Executable File | 63 lines (51 sloc) | 1.41 KB

Raw Blame

```
#!/bin/bash

csr_name="my-client-csr"
name="${1:-my-user}"
cert_name="${name}-client"

if ! which cfssl; then
  echo "Can't find the cfssl tool, please install from https://pkg.cfssl.org/"
  exit 1
fi

if ! which cfssljson; then
  echo "Can't find the cfssljson tool, please install from https://pkg.cfssl.org/"
  exit 1
fi

echo "Generating signing request."
perl -p -e "s/%USER%/${name}/" cfssl.json.tmpl > cfssl.json

cfssl genkey cfssl.json | \
    cfssljson -bare ${cert_name}
```

What’s missing from the script

- Key / Config file distribution

How about something easier?

main | 68 branches | 89 tags | Go to file | Add file | Code

pdevine Require oldpassword (#3434) 05f7c58 3 hours ago **3,602** commits

.github	fix: postgres-dev to only listen on localhost	6 days ago
api	Require oldpassword (#3434)	3 hours ago
blog	improve: add blog post for creating users video (#30...	last month
docs	maintain: cli docgen fixes to clean up the resulting fil...	10 hours ago
helm	improve: add backwards compat for connector acces...	9 days ago
internal	Require oldpassword (#3434)	3 hours ago
metrics	maintain: update gofmt for go1.19	2 months ago
pki	improve: return our own type from NewDB	2 months ago
ui	Require oldpassword (#3434)	3 hours ago
uid	feat: add sql functions uidStrToInt and uidIntToStr (#...	last month

About

Infra manages access to infrastructure such as Kubernetes, with support for more connectors coming soon.

infrahq.com

go | kubernetes | infrastructure | golang | security | identity | login | iam | access | infra | oidc

Readme

View license

985 stars

16 watching

38 forks

Releases 89

Infra

- Two deployment options
  - Self Hosted
  - Use Infra Cloud (coming soon)

Demo

Summary

- HomeLabs let you practice
- You should be using Users/Roles/SSO with K8s
- Users in K8s are hard
- Infra is easy
- Infra lets you do the hard stuff without much thinking

It's My HomeLab

Why Would I Want SSO?

Matt Williams – Evangelist @ Infra
matt@infrahq.com | @technovangelist

infra