



iits

**Innovation
as a Team**

From Zero to Hero

Best-Practices from cloud-native GitOps projects



About the Speaker

Victor Getz

CTO and Founder at iits-consulting



The logo for iits, consisting of the lowercase letters "iits" in white on a red square background.

Founded in 2019

We provide agile development teams that help businesses automate their complex processes

100+ people are working for us

The logo for "Beste Arbeitgeber NRW", featuring the text "Beste Arbeitgeber™ NRW" in black on a white background, which is part of a larger orange and white graphic.The logo for "Great Place To Work", featuring the text "Great Place To Work®" in white on a red background, which is part of a larger orange and white graphic.

Deutschland



elastic



kubernetes

The HashiCorp logo icon, which is a stylized "H" made of two interlocking shapes.

HashiCorp



CLOUD NATIVE
COMPUTING FOUNDATION

...

Purpose of this talk



Share Lessons Learned



**Provide a bootstrapping
architecture**

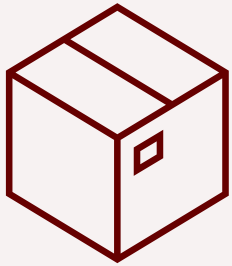


**Share our
knowledge**



**Introduce the
workshop**

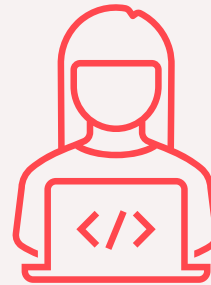
Quick audience check



Who is using Kubernetes ?

Who is using Helm ?

Got problems with merging Lists?

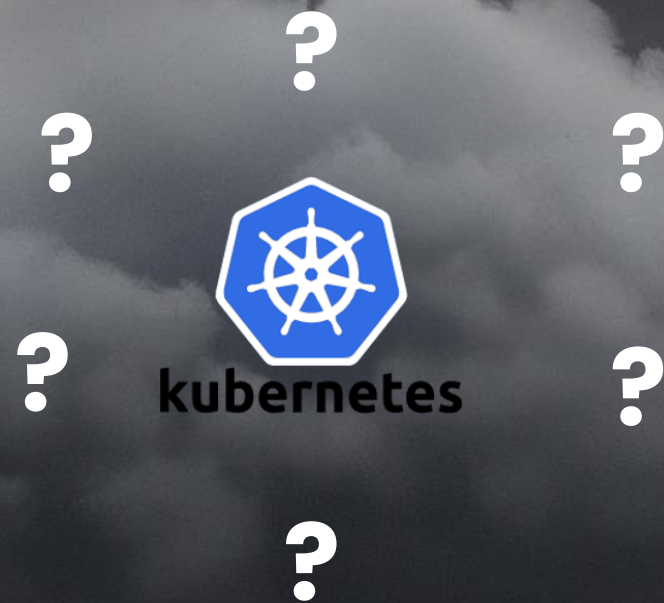


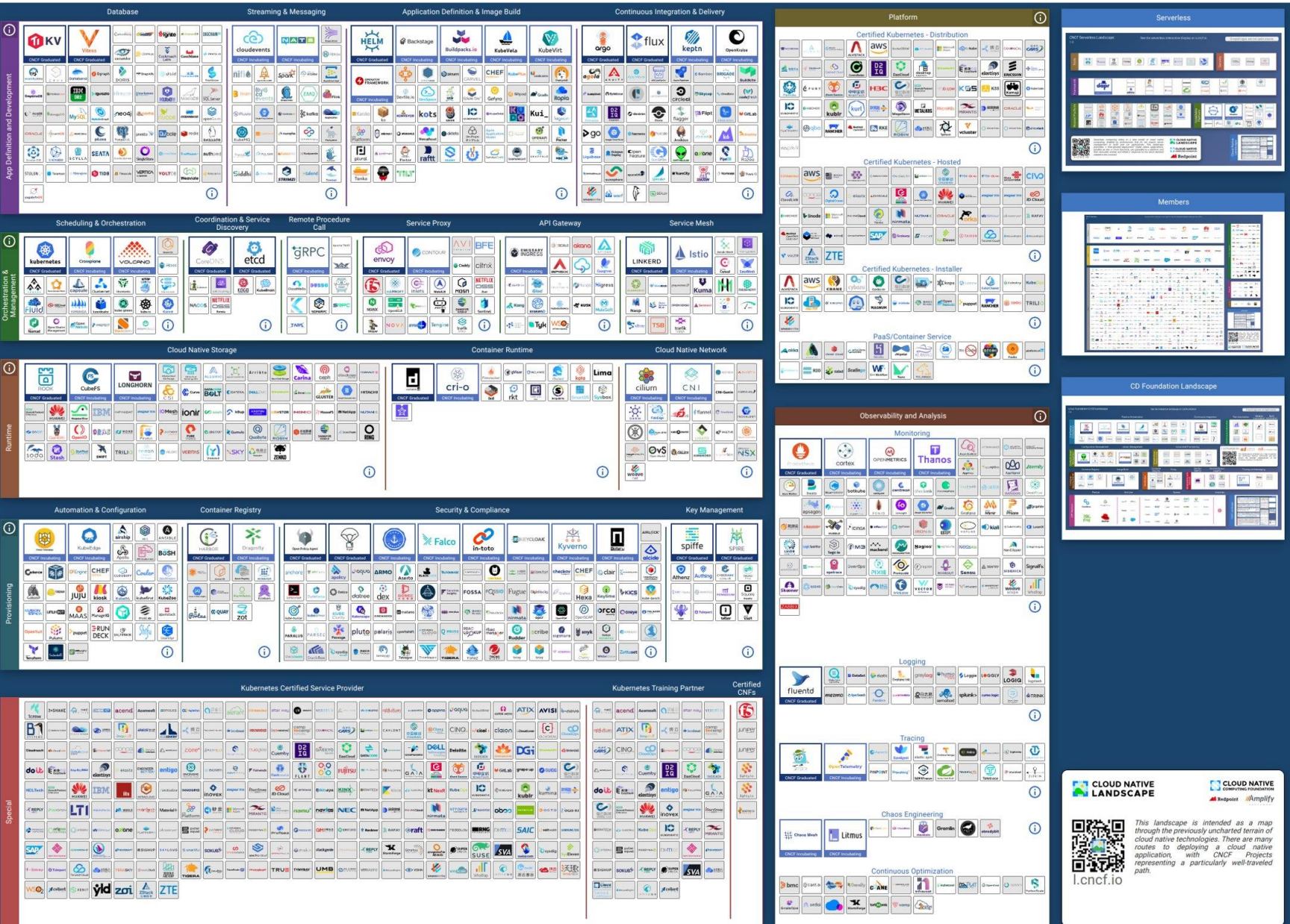
Who is using GitOps ?

Who is using Argo ?

Who is using Flux?

**Why is
CloudOps so
hard?**





CNCF Landscape

CLOUD NATIVE LANDSCAPE









This landscape is intended as a map through the previously uncharted terrain of cloud native technologies. There are many routes to deploying a cloud native application, with CNCF Projects representing a particularly well-traveled path.

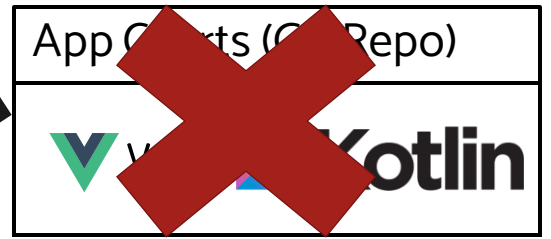
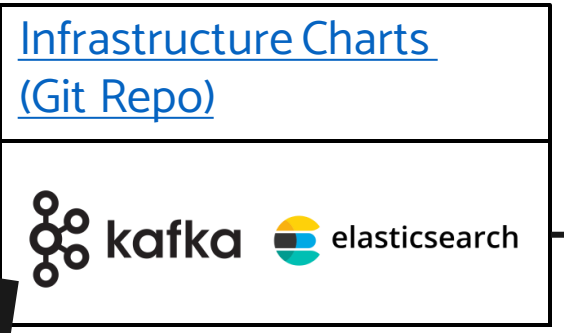
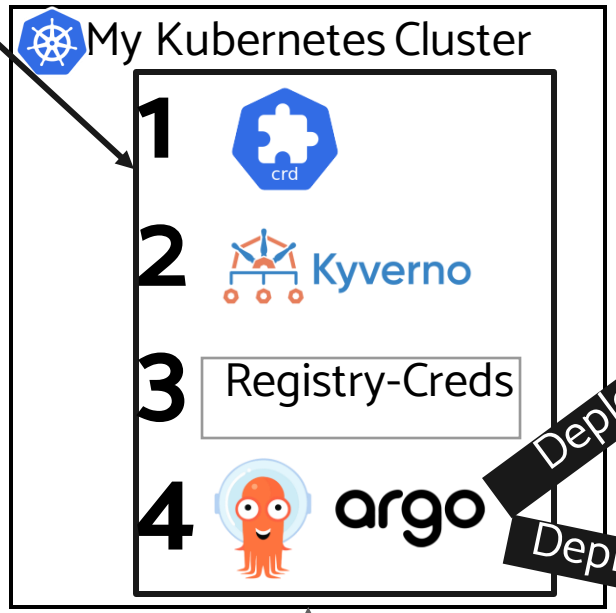
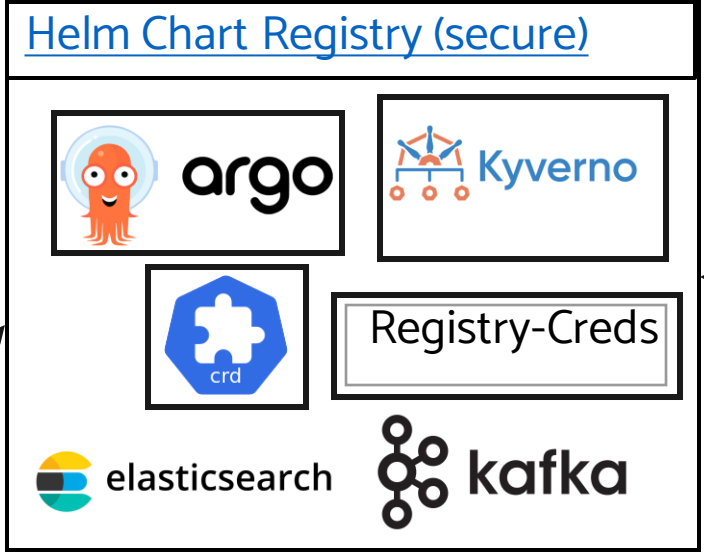
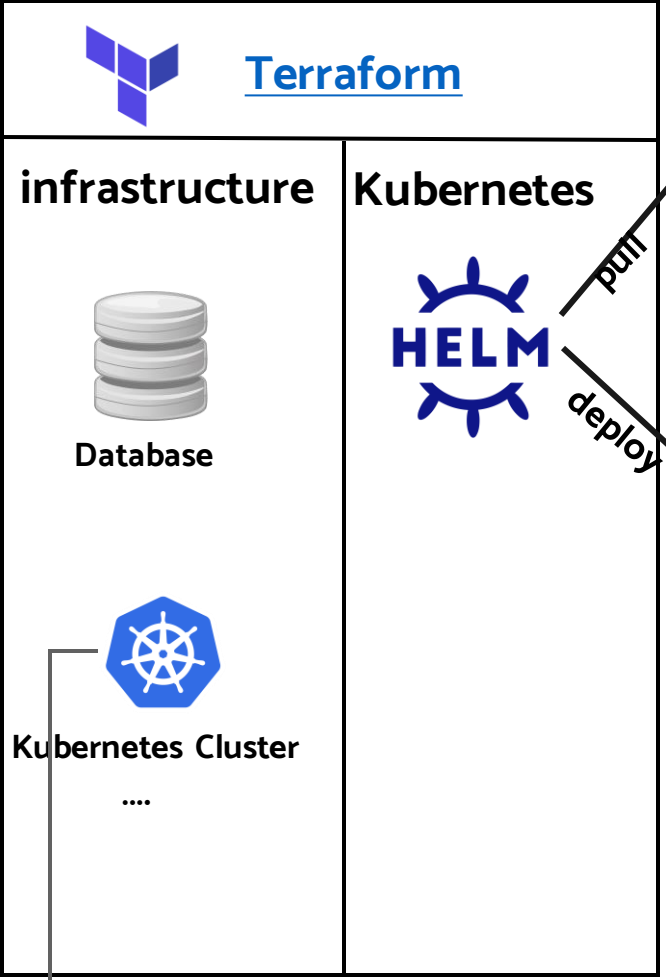
l.cncf.io

[illegible][illegible]



**CloudOps
should be
like this**

Infrastructure	Infrastructure Charts/Services	App Charts/Services or Business Charts/Services
  kubernetes  mongoDB® Cloud SaaS service	   Grafana	 



reference/local or third party

Will not be shown today

Install



pull

deploy

Deploy

Deploy

Showtime

```
mirror_mod = modifier_ob.  
#set mirror object to mirror  
mirror_mod.mirror_object =  
operation == "MIRROR_X":  
mirror_mod.use_x = True  
mirror_mod.use_y = False  
mirror_mod.use_z = False  
operation == "MIRROR_Y":  
mirror_mod.use_x = False  
mirror_mod.use_y = True  
mirror_mod.use_z = False  
operation == "MIRROR_Z":  
mirror_mod.use_x = False  
mirror_mod.use_y = False  
mirror_mod.use_z = True
```

```
#selection at the end -add  
mirror_ob.select= 1  
modifier_ob.select=1  
context.scene.objects.active  
("Selected" + str(modifier_ob.  
mirror_ob.select = 0  
= bpy.context.selected_object  
data.objects[one.name].select  
print("please select exactly
```

--- OPERATOR CLASSES ---

```
types.Operator):  
X mirror to the selected  
object.mirror_mirror_x"  
mirror X"
```

```
context):  
context.active_object is not
```

**And the Cloud
lived happily
ever after**

Right ?






Which tool to use for which purpose ? (tech radar)

**Unfortunately,
not ...**

Secret Management

- Example: Azure
 - Keyvault + `akv2k8s.io`
- If their Cloud does not have a Secret Management Service
 - HashiCorp Vault + Bank Vaults

Ingress Controller

- Default Ingress 
- Nginx 
- Traefik 

```
1  apiVersion: traefik.containo.us/v1alpha1
2  kind: IngressRoute
3  metadata:
4    name: grafana
5  spec:
6    entryPoints:
7      - websecure
8      - web
9    routes:
10     - kind: Rule
11       match: "HostRegexp(`{host:grafana.iits.tech}`) && (PathPrefix(`/`))"
12       middlewares:
13         - name: https-redirect
14           namespace: default
15       services:
16         - kind: Service
17           name: grafana
18           namespace: default
19           passHostHeader: true
20           port: 80
21     tls:
22       secretName: grafana-cert
23       domains:
24         - main: grafana.iits.tech
25
```

Traefik

GitOps Tools



- Better UI
- Bigger Community
- No easy Bootstrapping
- No native Helm support



- Nice Bootstrapping
- KISS
- UI not so powerful

The *lookup* function can be used to look up resources in a running cluster.

Nope not working 😊

**Argo
Fails
–
Helm**

Argo Fails – Helm

iits



Our Fails/Issues in the past

- ArgoCD Image Updater -> Checkout the project, change commit and push

- ```
Grafana Secret Injection
vault.hashicorp.com/agent-inject-secret-1-service-default-secrets.sh: "secret/data/grafana"
```

- Argo Sync Waves and CRDs
- Local vs Remote Charts
- Bootstrapping business ArgoCD projects

**Argo  
Fails  
–  
Helm**

# Helm List Issue

values.yaml

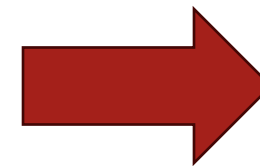
```
traefik:
 namespace: routing
 targetRevision: 10.22.0-https-redirect
 parameters:
 - name: traefik.deployment.replicas
 value: "1"
```

values-dev.yaml

```
traefik:
 parameters:
 - name: "muh"
 value: "kuh"
```

How does the result of this command look like?

*helm template -f values-dev.yaml.*



```
parameters:
 - name: muh
 value: kuh
```

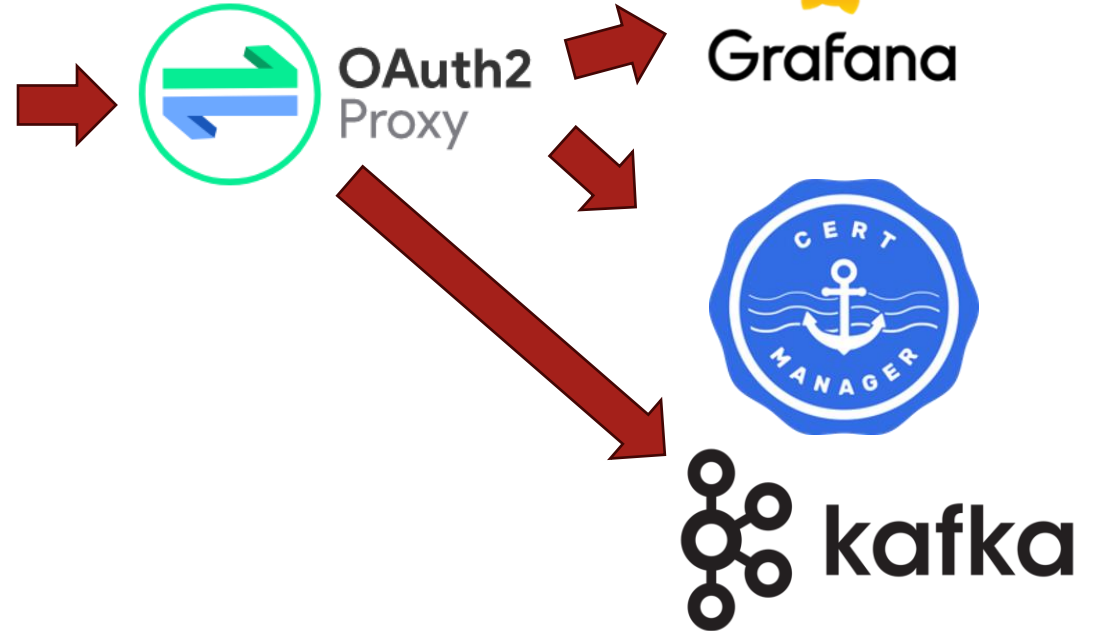
# Zitadel vs. Keycloak

- Zitadel is a really nice project but has a lot of bugs at the moment
- Keycloak has a lot of functionality but is really complex and hard to configure with Infrastructure as Code

**Identity and  
Access  
Management  
Tools**

# OAuth2 Proxy

admin.dev.my-  
subdomain.iits.tech



dev.my-  
subdomain.iits.tech





# OPA vs. Kyverno

- OPA is really mighty but way too complex
- Kyverno offers a lot of predefined policies
  - Only allow pulls from certain registries
  - Only allow images which are signed by cosign
  - Several out of the box container security policies

**Policies &  
Security**

**Workshop  
tomorrow**

# OTC Cloudland Workshop

iits

- Hands On Training with OpenTelekomCloud
- Talk with my CloudOps Team
- Friday 23.06.2023 | 12:00 - 15:45 | Orange Lounge



**Questions**