



// IDP AS A SERVICE: MANAGING TENANTS EFFICIENTLY USING GITOPS

Johannes Schnatterer, Clouddogu GmbH

Slides



 @schnatterer@floss.social

 in/jschnatterer

Version: 202511141156-5ae57ae

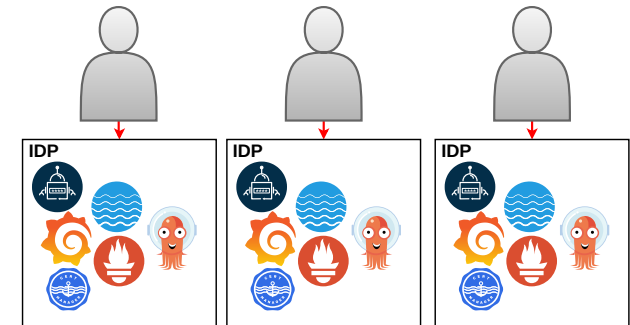
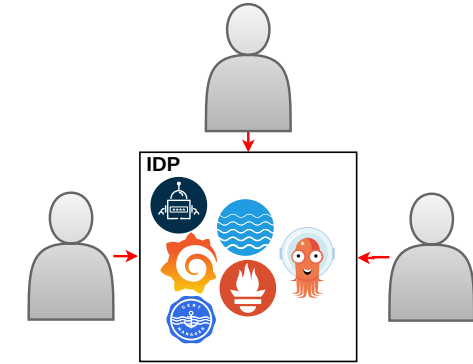
Agenda

- Shared IDP Instance
- Dedicated IDP Instances (IDPaaS)
- Multiple Environments per Tenant

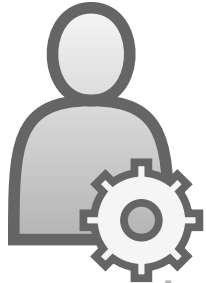


Multi-tenancy strategies

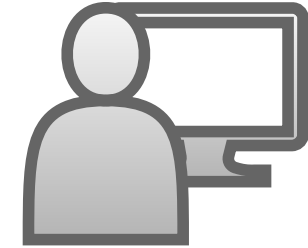
- Shared instance
- Dedicated instances



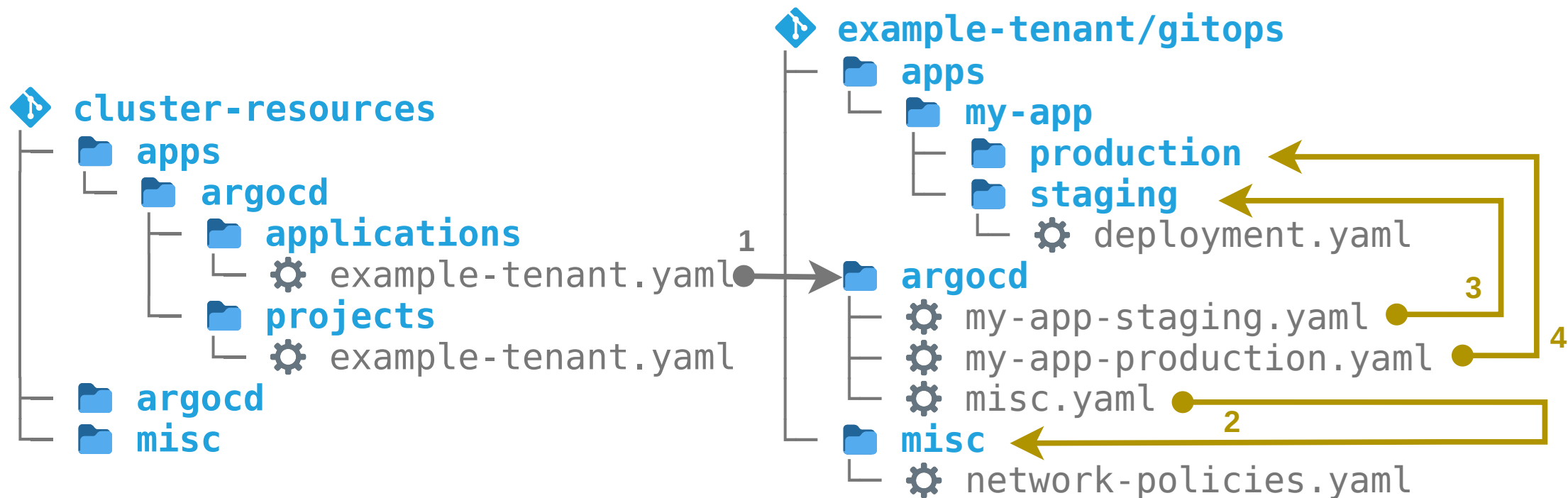
Shared Instance: A first approach



Platform engineer



Software engineer



 [cloudogu/gop-multi-tenant-shared-example](https://github.com/cloudogu/gop-multi-tenant-shared-example)

Shared vs Dedicated Instance

- Lower infra usage
- Easier to maintain
- Higher isolation
- Easier to configure (RBAC) 

 blog.argoproj.io/best-practices-for-multi-tenancy-in-argo-cd-273e25a047b0

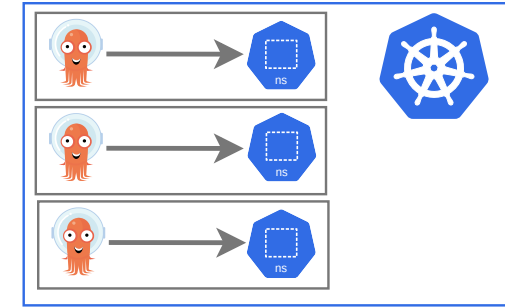
Dedicated instances: Options

Topology:

- Instance per Namespace
- Instance per Cluster

Management:

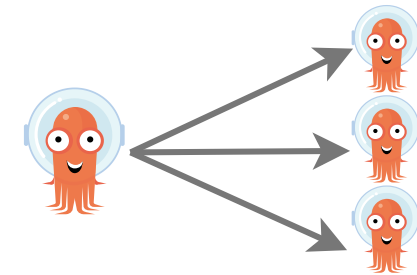
- Standalone
- Hub and Spoke (IDP as a Service)
 - 💡 Argo CD AppSets



Instance per Namespace

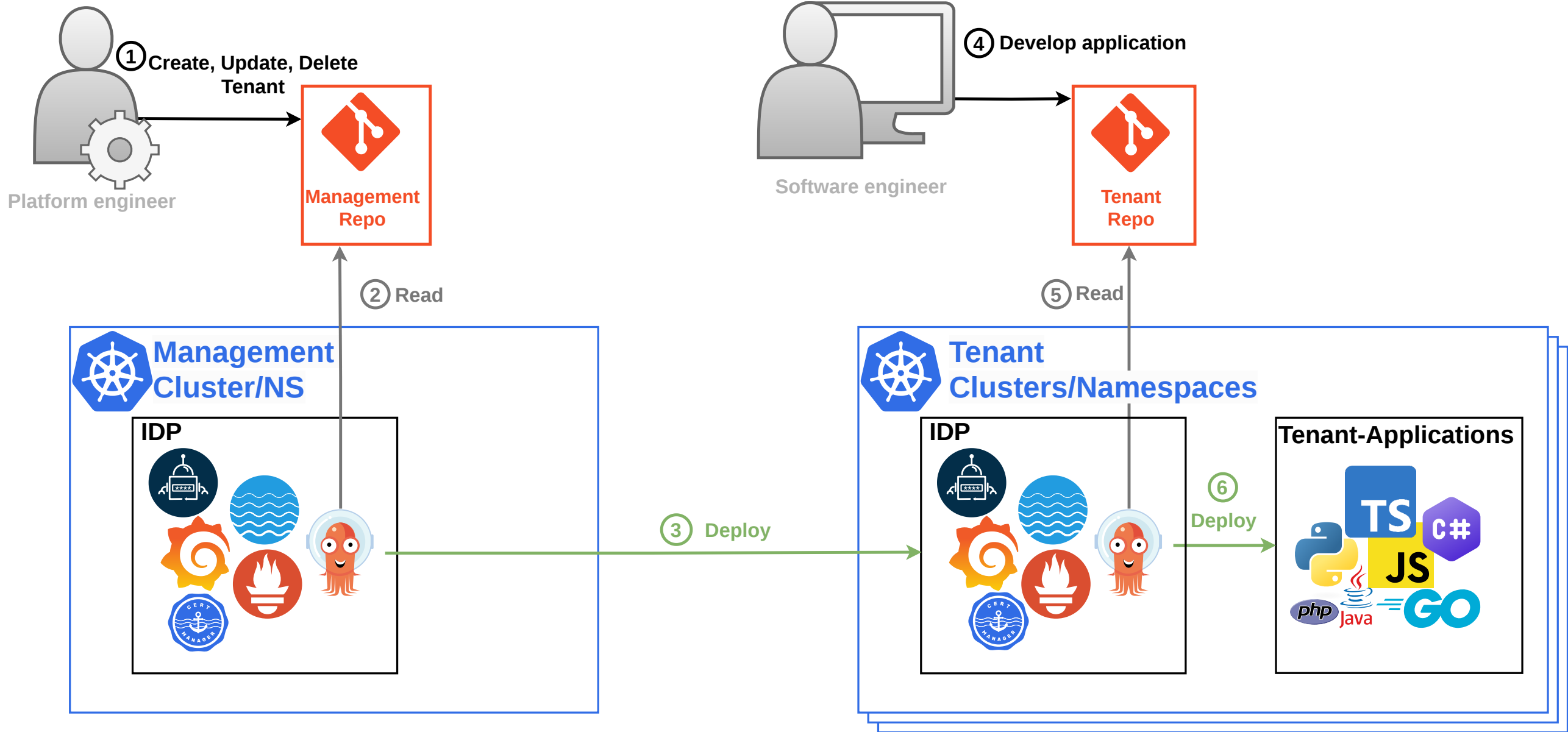


Instance per Cluster

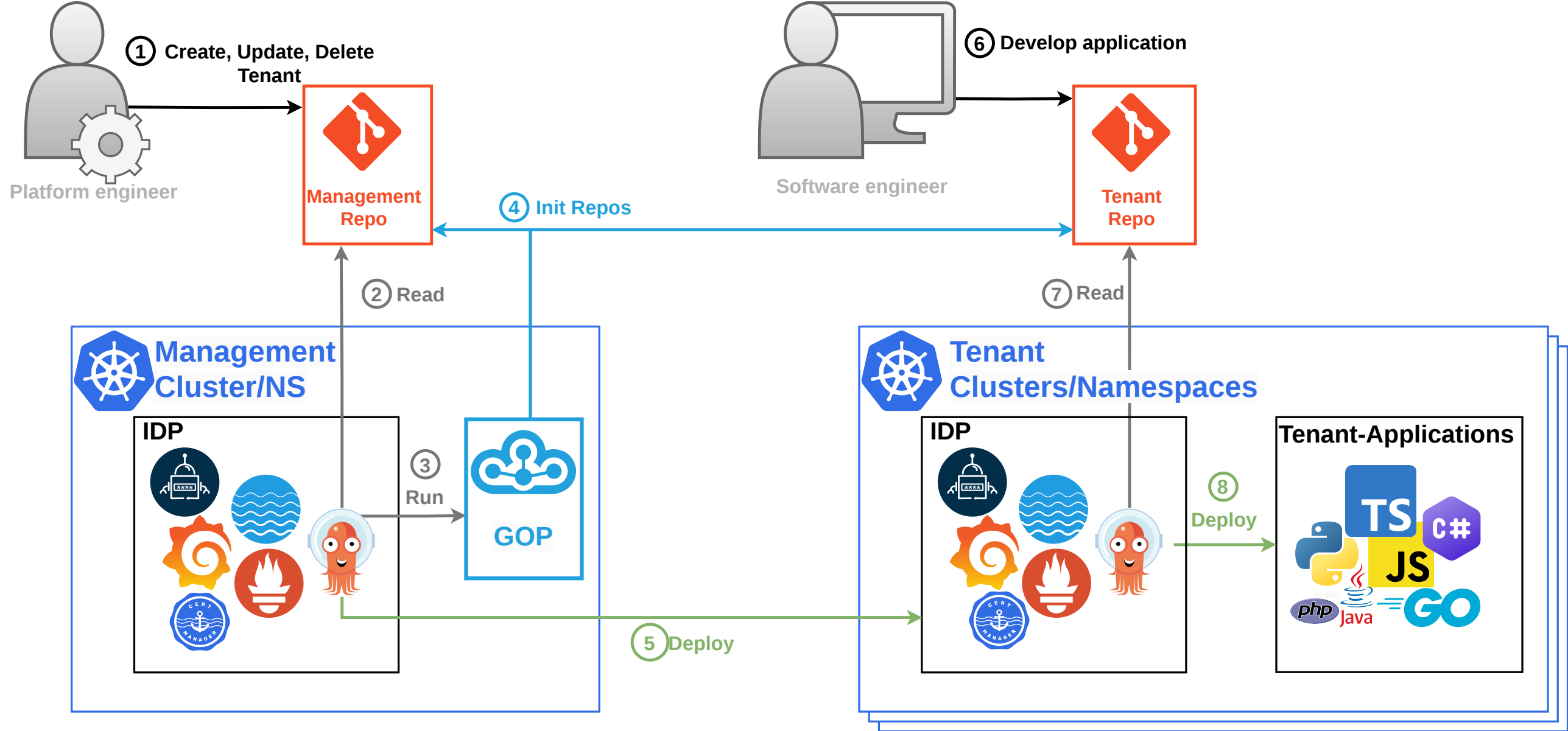


Hub and Spoke

IDP as a Service using Argo CD AppSets



IDP as a Service using Argo CD AppSets





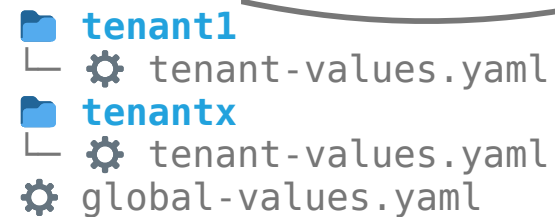
1



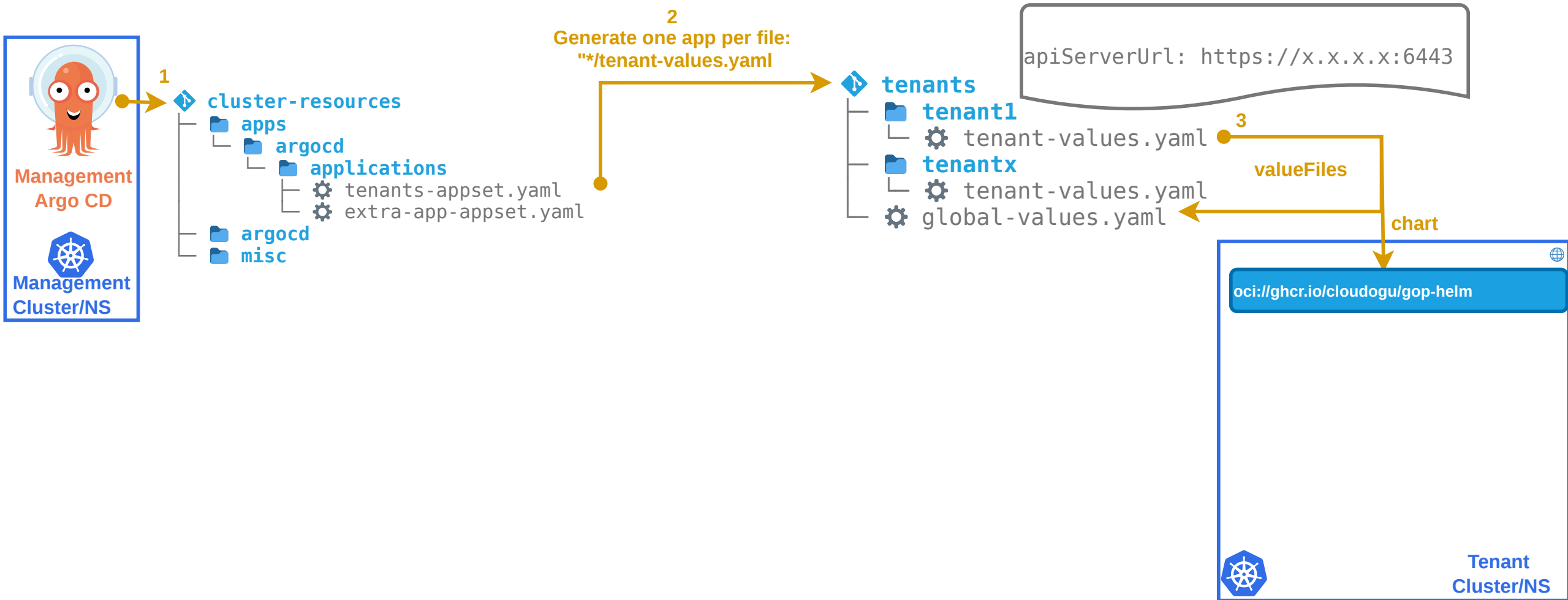
2
Generate one app per file:
"/tenant-values.yaml"

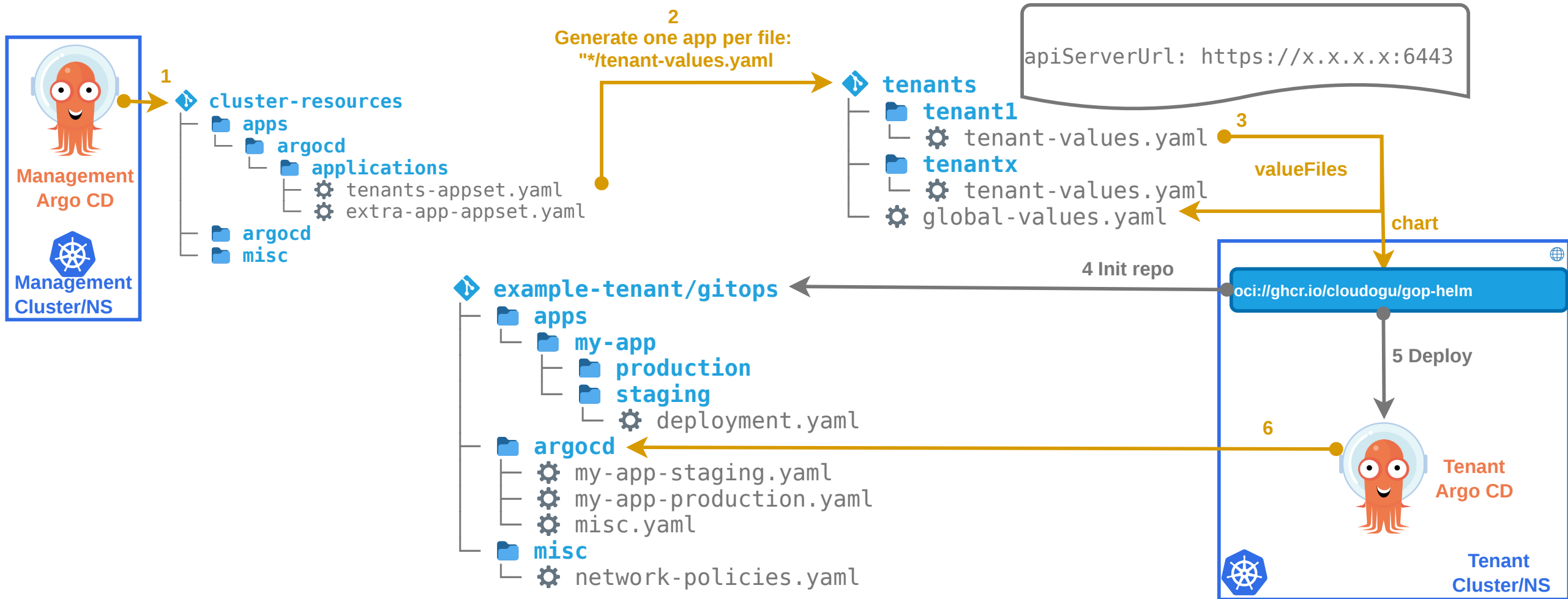


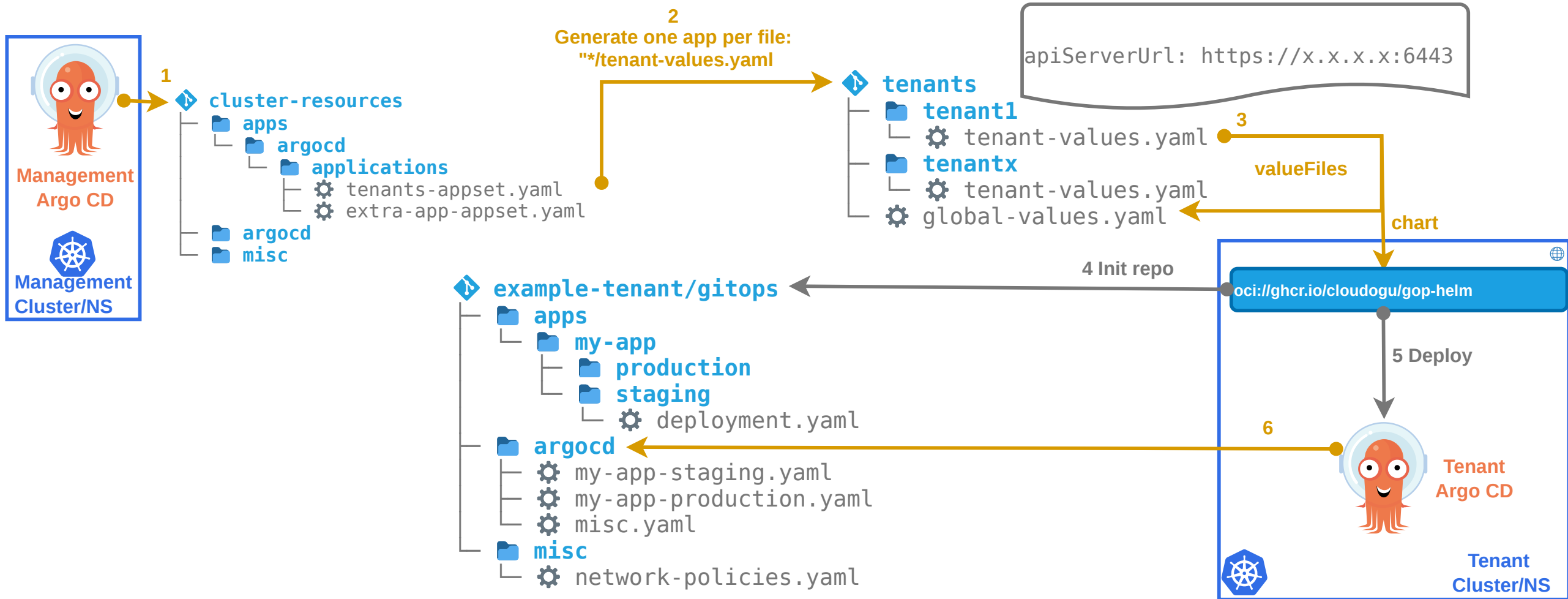
tenants



apiServerUrl: https://x.x.x.x:6443







 [cloudogu/gop-multi-tenant-multi-cluster-example](https://github.com/cloudogu/gop-multi-tenant-multi-cluster-example)

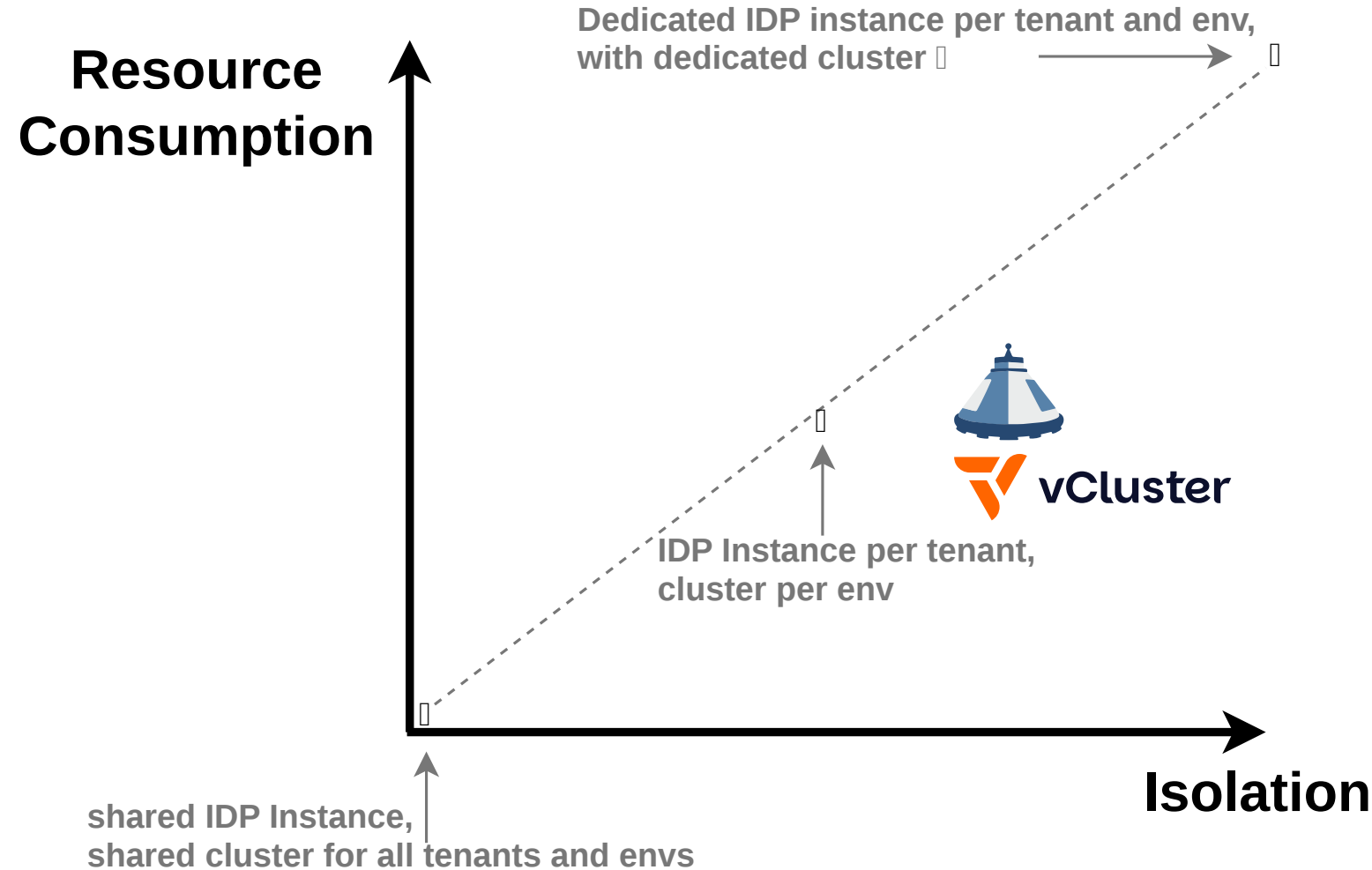
Instance per Namespace vs per Cluster

- Lower infra usage
- Easier to maintain
- Higher isolation
- Easier to configure    ...

 github.com/argoproj-labs/argocd-operator

What about env/stages?

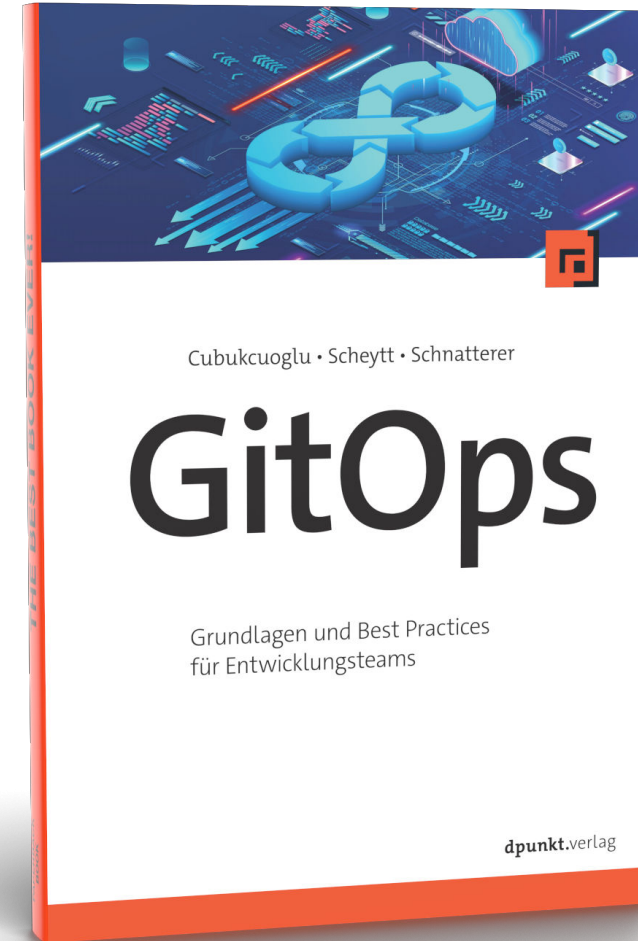
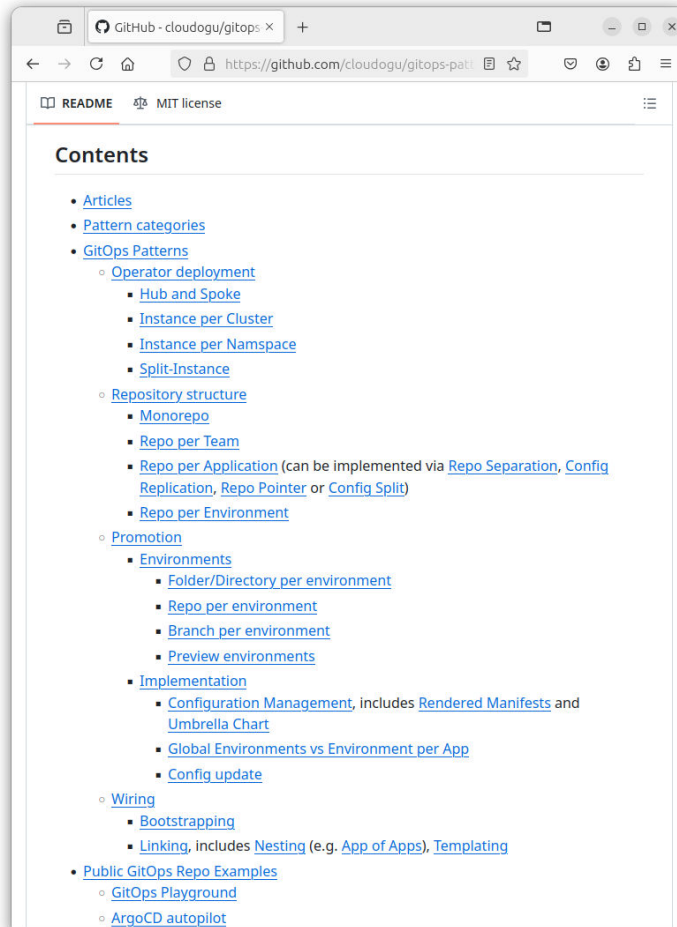
Each tenant might have multiple envs



My key experiences IDPs and tenants

- **Shared Instance:** 👍 for small settings. Lots of authz in tools.
- **Dedicated instances:** 🔒 Better isolation+UX but more effort
 - per Namespace: Less infra, but lots of RBAC, NetPols, etc. 
 - per Cluster: More infra+complexity, but authz easier.
 - IDPaaS using AppSets 🐙 great to have but hard to get.
- No silver bullet: Number of tenants/namespaces/clusters depends on requirements,
e.g. envs, security, regulation, onPrem/public cloud, etc.

Further reading



IDP Bootstrapping made simple: GOP

Creates a complete GitOps-based operational stack / IDP on your Kubernetes clusters

 [cloudogu/gitops-playground](https://github.com/cloudogu/gitops-playground)

Also runs locally



```
VERSION='0.12.1'
bash <(curl -s \
  "https://raw.githubusercontent.com/cloudogu/gitops-playground/$VERSION/scripts/init-cluster.sh") \
  && docker run --rm -t -u $(id -u) \
    -v ~/.config/k3d/kubeconfig-gitops-playground.yaml:/home/.kube/config \
    --net=host \
    ghcr.io/cloudogu/gitops-playground:$VERSION --yes --argocd --ingress-nginx --base-url=http://localhost
# More IDP-features: --monitoring --vault=dev --cert-manager --mailhog
# More features for developers: --jenkins --registry --content-examples
```

-  [cloudogu/gop-multi-tenant-shared-example](https://github.com/cloudogu/gop-multi-tenant-shared-example)

Try with GOP: •  [cloudogu/gop-multi-tenant-multi-cluster-example](https://github.com/cloudogu/gop-multi-tenant-multi-cluster-example)

Johannes Schnatterer, Cloudogu GmbH

 @schnatterer@floss.social

 in/jschnatterer

Slides



☒ Let's meet



Image sources

- Live Example:
<https://unsplash.com/photos/assorted-color-hot-air-balloons-during-daytime-DuBNA1QMpPA>
- More examples:
<https://unsplash.com/photos/XZc4f2XZc84>
- coloured-parchment-paper background by brgfx on Freepik:
https://www.freepik.com/free-vector/coloured-parchment-paper-designs_1078492.htm