swisscom

Enterprise-grade Infrastructure as a Service in a Cloud Native Way

Our journey of the «Cloud Native Infrastructure Platform»

The Mission

« *Building a new Infrastructure Platform for hosting Swisscom's CAAS offering.*

Highly scalable, secure and stable.

Avoiding vendor lock-in.

Leveraging open source and Cloud Native Technologies. »

Key Features

Entire stack based on ***Cloud Native*** *and other* open-source technology

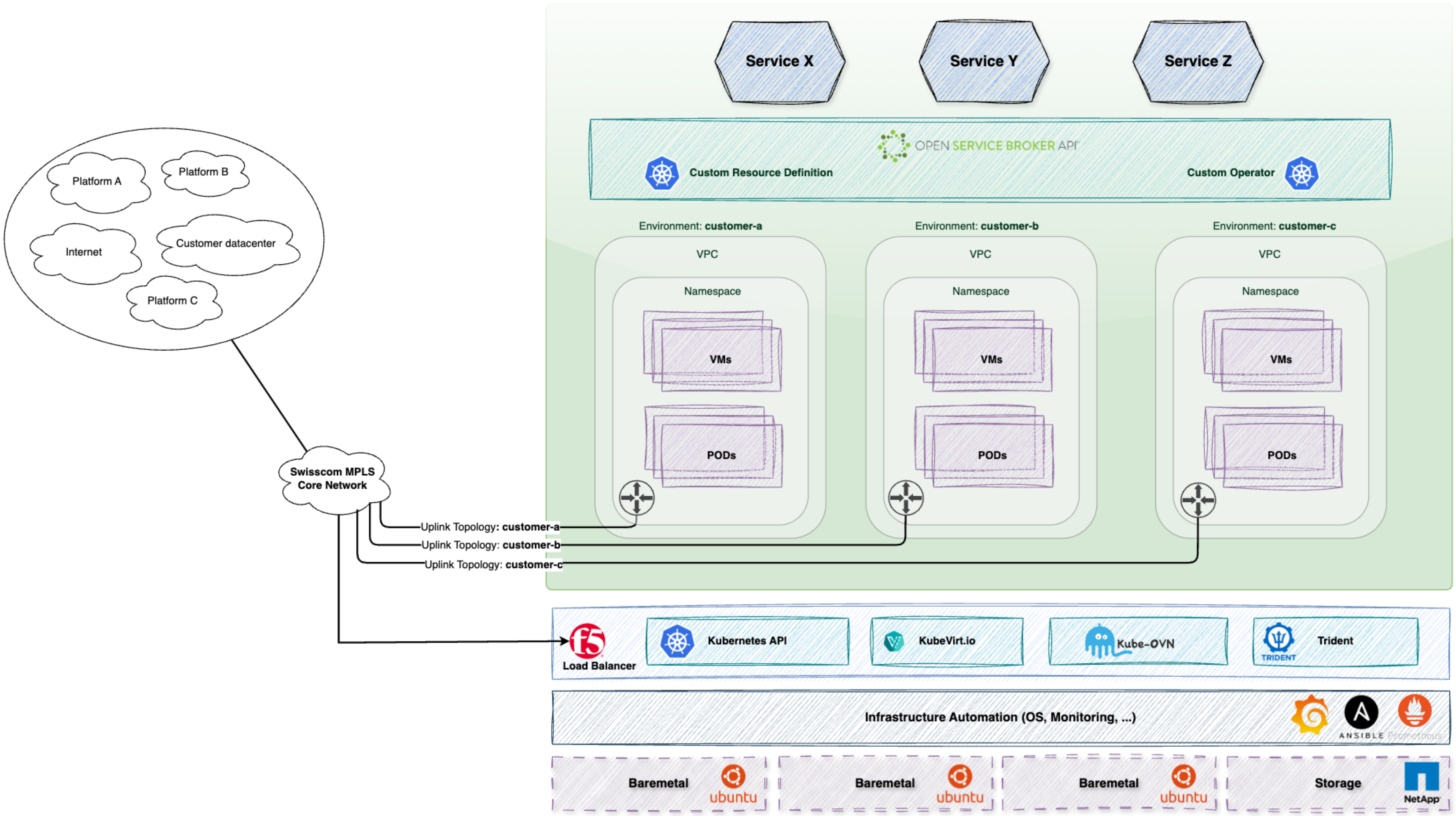
Kubernetes based platform, running on **bare metal** hosts all over Switzerland in 4 datacenters

Infrastructure Clusters that are supporting multiple services and are **shared among customers**

Separation between management- and workload-clusters (internal and customer environments)

Full **multi-tenancy** based on K8s Namespaces, Role-based Access Control (RBAC) and Kube-OVN VPCs for network isolation

High Level Architecture



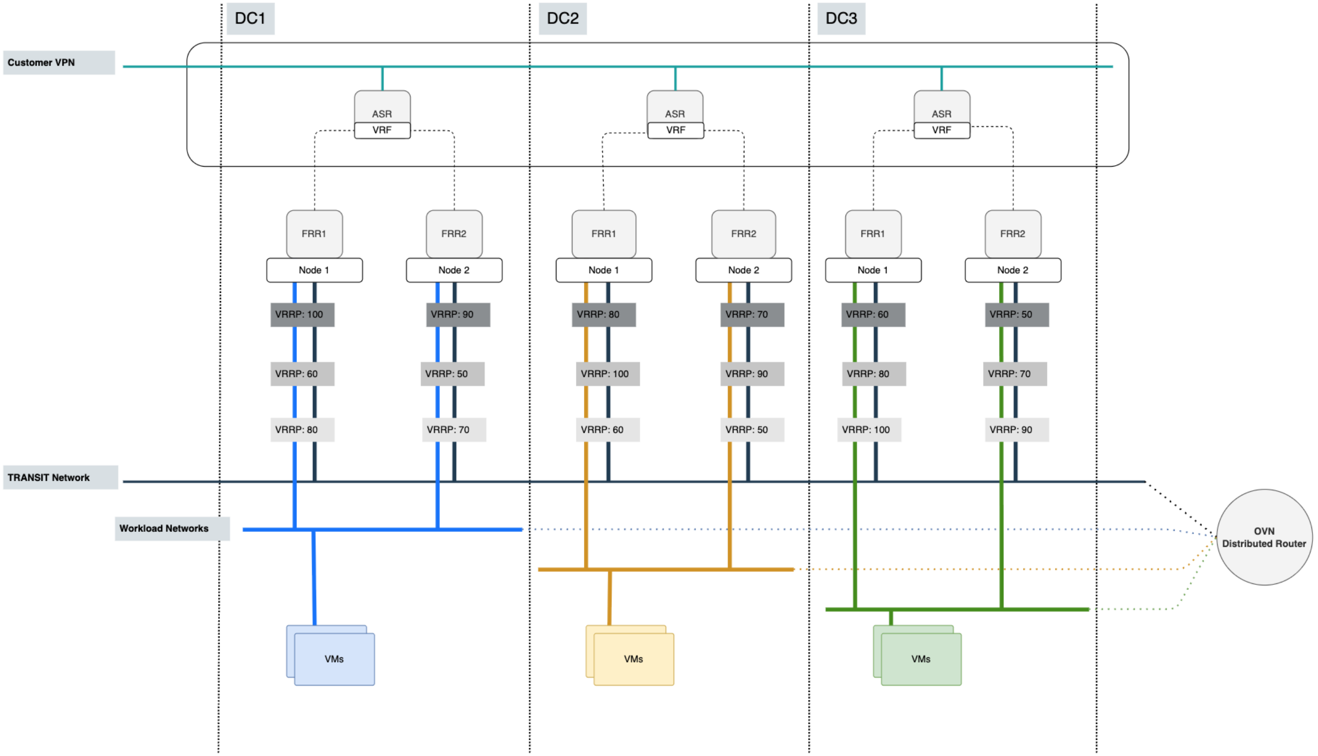
Network Design *(simplified…)*

- Subnets per Availability Zone, **prioritizing** the local router gateway - using **VRRP** with different priorities

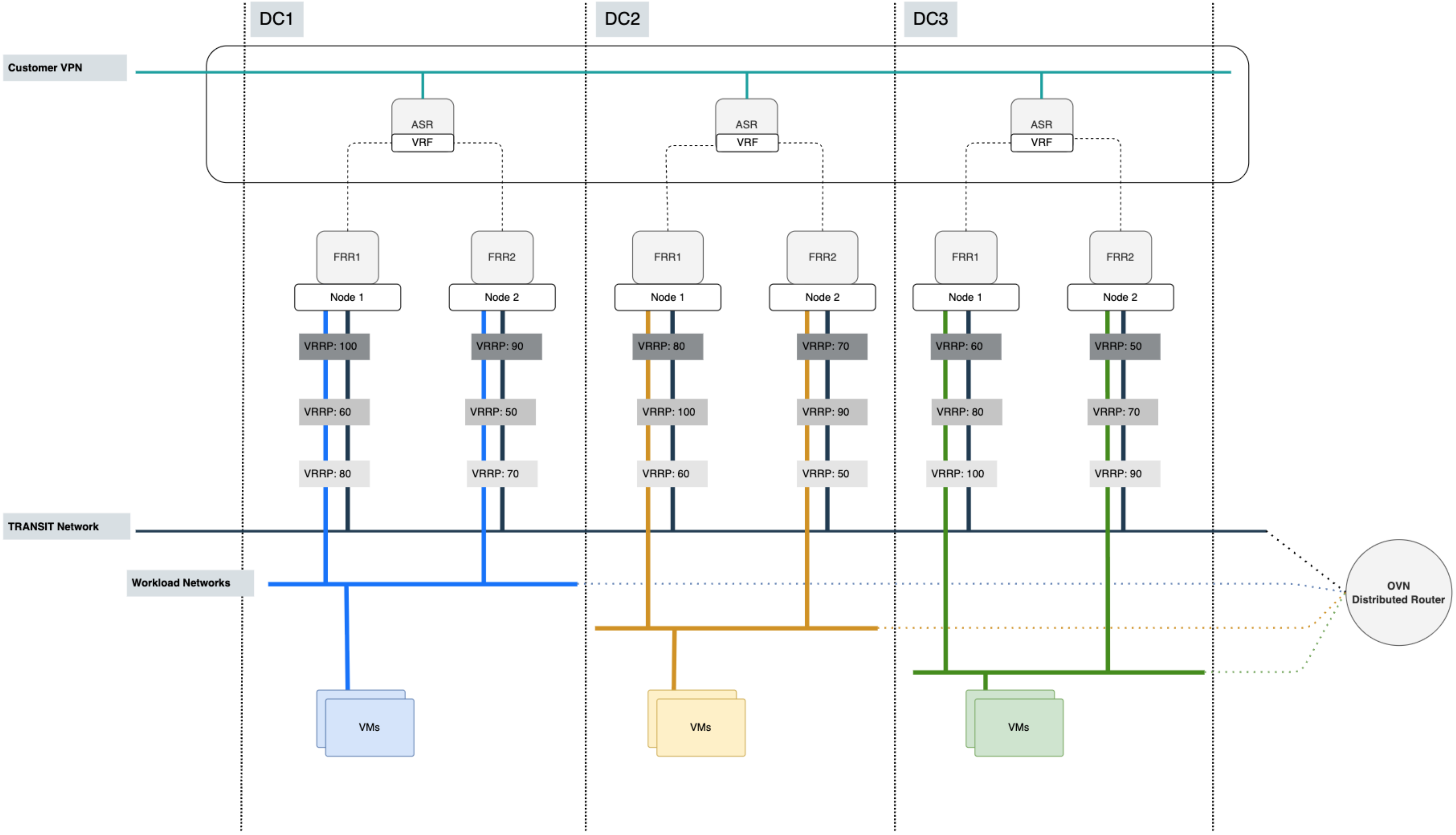
- Router-pair consisting of **2 Routers** (based on FRR) per site running on **separate nodes**

→ Fail-over capability **within** an availability zone or to **any other zone**

- All networks fully routed through the **OVN distributed router**



Network Design *(simplified…)*



KubeVirt, Kube-OVN and Kyverno

Leveraging the power of Cloud Native

KubeVirt

- Operator with CRDs to run Virtual Machines in Kubernetes
- VMs are running within a pod
  - Each Pod runs its own KVM, QEMU etc.
  - The VM is a process in the Pod, therefore decoupled from pod lifecycle
  - Volumes, IPs, Resources etc. Are the same as for a regular pod
- IaaS specific features
  - virtctl CLI
  - Hot-plugging of network interfaces, disks, CPU, memory
  - Live migrations

https://kubevirt.io/

Kube-OVN

- Operator with CRDs to create VPCs, Subnets, etc. in Kubernetes
- Allows to place pods in different Subnets
- In combination with Multus, multiple network interfaces can be added to one Pod
- KubeVirt Integration
  - Support for static IPs and Mac-Addresses
  - Live Migration optimizations (network downtime below 0.2 seconds)

https://www.kube-ovn.io/

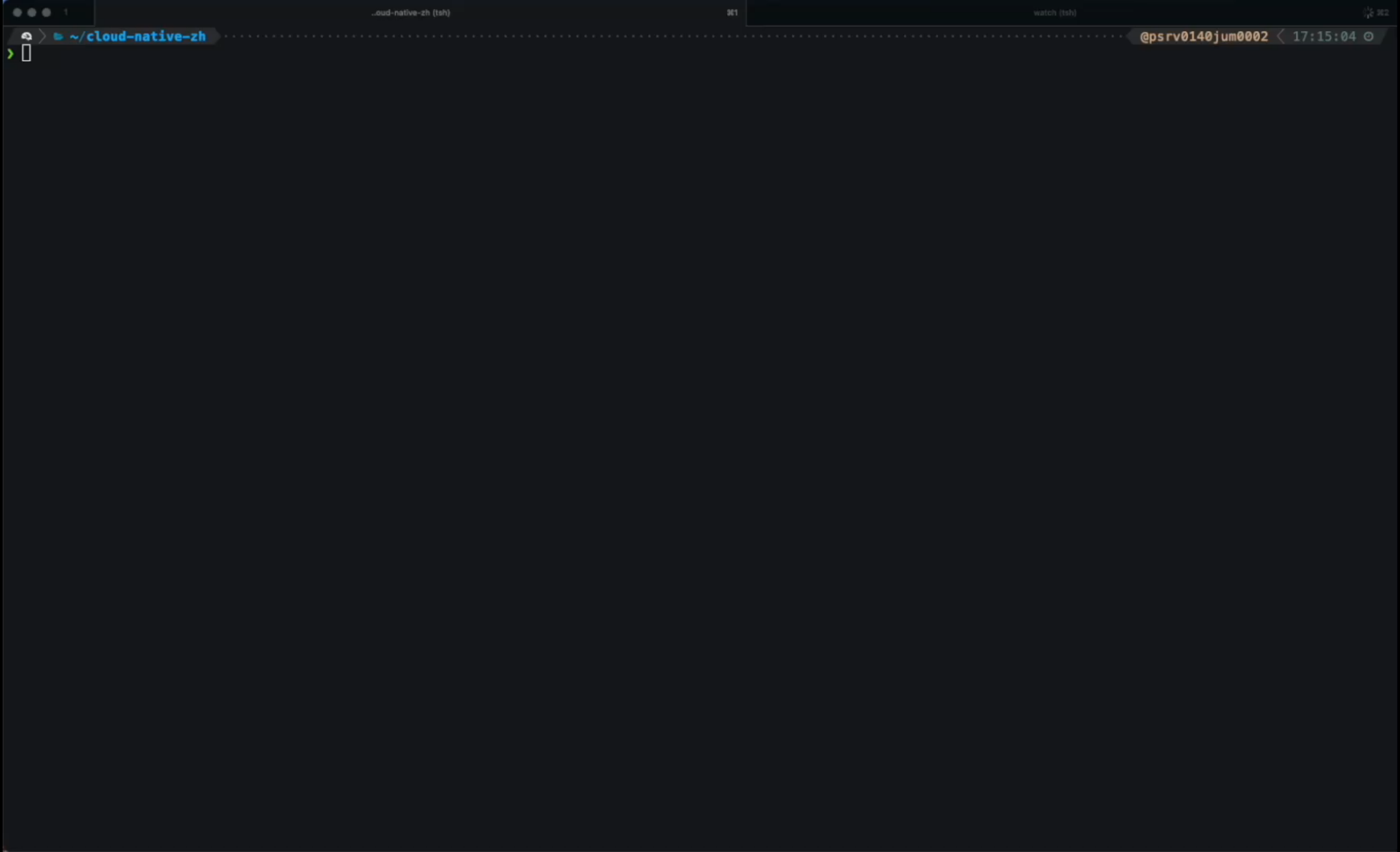
Kyverno

- Operator with CRDs for Policy-as-Code in Kubernetes
- Kyverno policies can **validate, mutate, generate, and cleanup** any Kubernetes resource
- Used to enforce settings for example
  - Enforce RWX accessMode
  - Inject DNS Configs from namespace's annotations to Pods
- Policies can be created and released very fast
  - Used to fix bugs / missing features

https://kyverno.io/

Demo time

Create a Virtual Machine on KubeVirt



```
~/cloud-native-zh ··························································· @psrv0140jum0002 < 17:15:04
❯ 
```

Summary

- Multi-Tenant Environment across multiple Availability Zones
- Kubernetes on Baremetal to run Virtual Machines with KubeVirt
- Kube-OVN to sperate Pods/VMs in different VPCs & Subnets

Visit us and learn more on our stand!

Thanks to our partners on that journey…

KUBERMATIC

tim&
koko

bespinian