TALOSCON 2025

HOSTED BY SIDERO

# From Zero to Scalable:
# Accelerated On-Premise Infrastructure with Omni and GitOps

## About us

### Alexandre Ferreira

SRE/DevOps engineer @ Promptly Health

On the web:

github.com/brancof

### Paulo Araújo

SRE/DevOps engineer @ Promptly Health

On the web:

github.com/paulob122

Portugal

Sllllluuu

## Challenge

"Build a Federated Health Data Network spread across different regions…"

*Promptly Health*

### Requirements:

- *Infrastructure* ***agnostic*** - Cloud, Virtualized or Bare Metal platforms.
- **Isolation** - *Secure data governance*.
- *Scalable* - Hundred of clusters.
- **Reproducible** - "Define once apply multiple" using **GitOps**.
- Secure by design - Minimal connection and Immutable OS.
- Portable - **Kubernetes**.
- Uniform infrastructure and application management.

### Technology used:

Sidero Omni

+

Talos Linux

## Omni

### Capabilities:

- Built-in Image Factory.
- Wireguard link to each node.
- Control Plane backups.
- Full cluster lifecycle management.
- Cluster template - **Cluster as code**.

```
kind: Cluster
name: demo
kubernetes:
    version: v1.32.2
talos:
    version: v1.10.5
features:
    enableWorkloadProxy: true
    backupConfiguration:
        interval: 24h
patches:
  - name: Deploy Cilium CNI
    annotations:
      description: Set up Cilium CNI on Talos
      name: Deploy Cilium CNI
    file: patches/cluster/cni.yaml
  - name: Audit Logging
    annotations:
      description: Enable audit logging on Talos
      name: Audit Logging
    file: patches/cluster/audit-logging.yaml

---
```

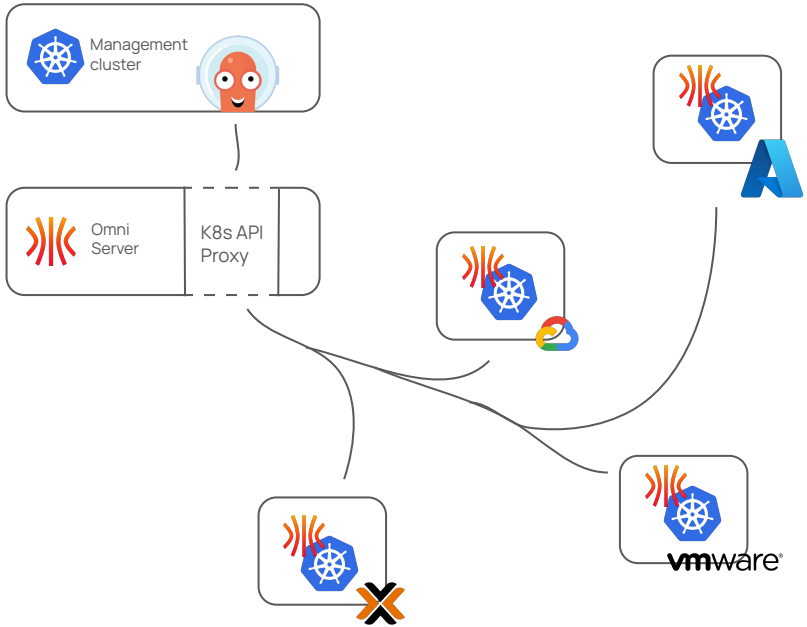
```
kind: ControlPlane
machines:
  - c6xxxx
---
kind: Workers
machines:
- 5fyyy
- bfyyy
- b7yyy
- e3yyy
```

Omni v1.1.x

# GitOps

## How we manage GitOps?

- ArgoCD w/ Hub-Spoke model:
  - Central management for every application.
- Applications as code:
  - Helm templates.
  - Custom configurations per client.
- Clusters as code.



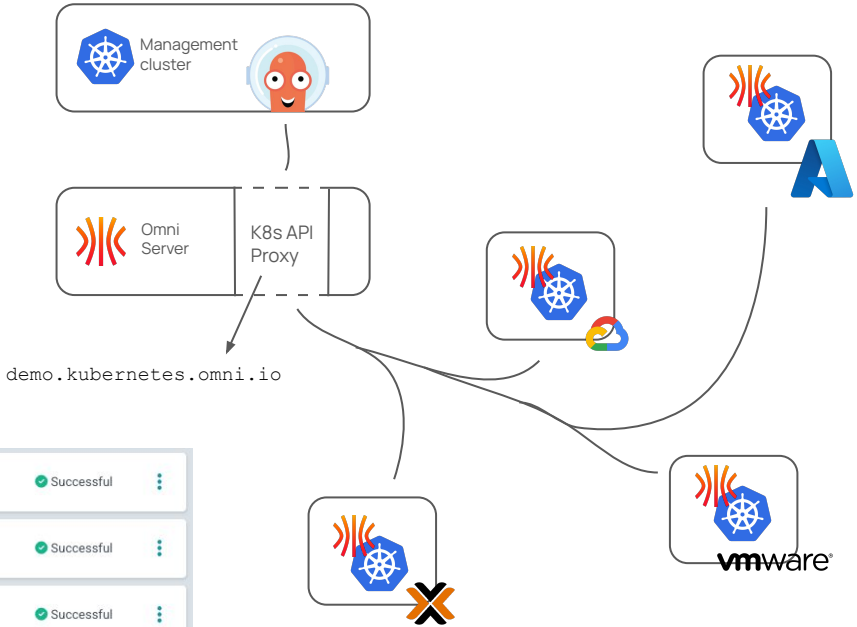
## GitOps

### ArgoCD problem:

- Common server name among clusters == Failure.
- ArgoCD cluster identifier (key) is the server url.

-

- Breaks reconciliation.




Server URL

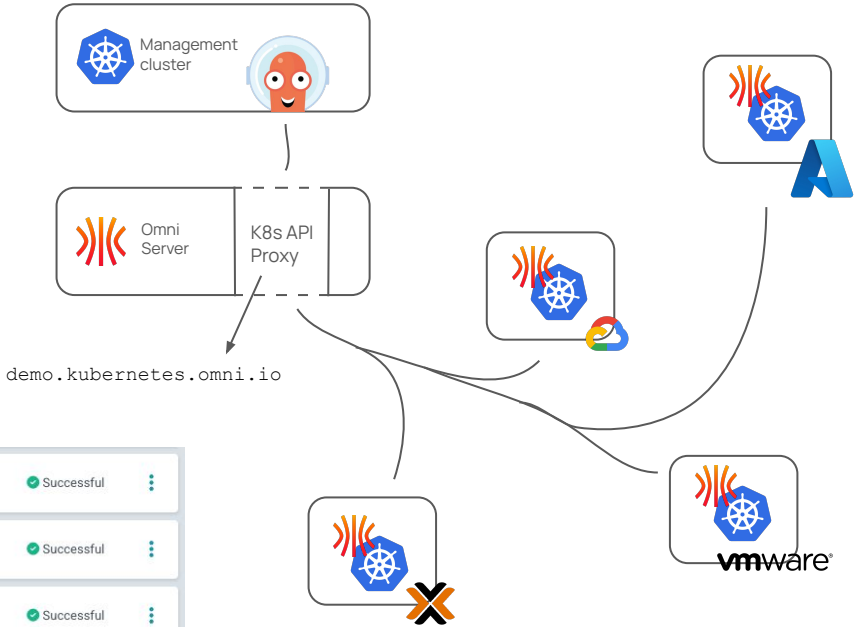
| | | | |
|---|---|---|---|
| demo1 | https://demo.kubernetes.omni.io | 1.32 | Successful |
| demo2 | https://demo.kubernetes.omni.io | 1.32 | Successful |
| demo3 | https://demo.kubernetes.omni.io | 1.32 | Successful |

## GitOps

**Fix:**

- Add query parameters to the server URL.
- ArgoCD clusters "keys" will be different.
- Query parameters are ignored when connecting to the Kubernetes API.

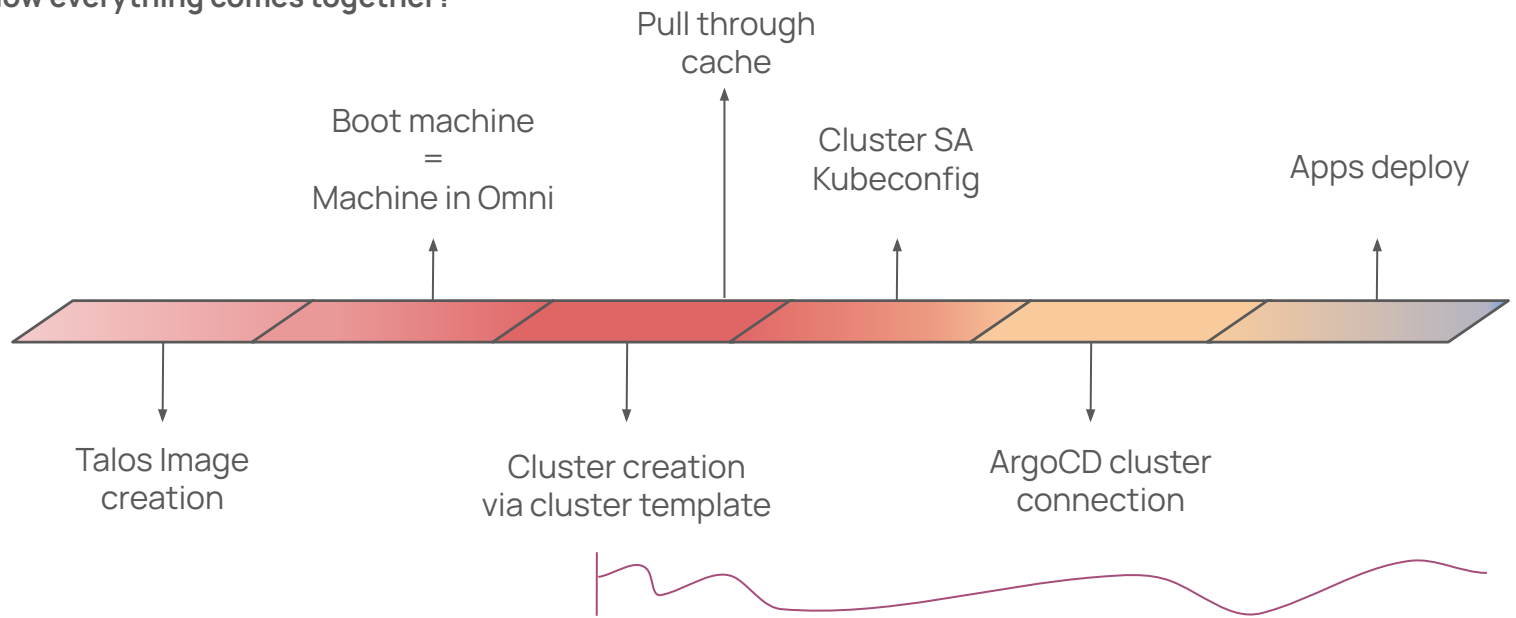
```
demo.kubernetes.omni.io ?__id=<cluster_name>
```




| | | | |
|---|---|---|---|
| demo1 | https://demo.kubernetes.omni.io?__id=demo1 | 1.32 | Successful |
| demo2 | https://demo.kubernetes.omni.io?__id=demo2 | 1.32 | Successful |
| demo3 | https://demo.kubernetes.omni.io?__id=demo3 | 1.32 | Successful |

## End 2 End Flow

How everything comes together?



## Automation

### Problem?

- Omni & Cluster template is good,
  but hard to scale by itself.
- Manual setup is error prune.
- Reduce repetitive tasks.
- Manually deploying each ArgoCD application.

### How to deploy tens of cluster for scale?

- SDKs to the rescue. 🛟

```go
// Getting all the machines from the Omni state.
machines, err := safe.StateList[*omni.MachineStatus](
    ctx,
    st,
    omni.NewMachineStatus(resources.DefaultNamespace, "").Metadata(),
)
if err != nil {
    log.Panicf("failed to get machines %s", err)
}

var (
    cluster string
    machine *omni.MachineStatus
)

for item := range machines.All() {
    log.Printf("machine %s, connected: %t", item.Metadata(), item.TypedSpec().Value.GetConnected())

    // Check cluster assignment for a machine.
    // Find a machine which is allocated into a cluster for the later use.
    if c, ok := item.Metadata().Labels().Get(omni.LabelCluster); ok && machine == nil {
        cluster = c
        machine = item
    }
}
```

Omni Go client example from
https://pkg.go.dev/github.com/siderolabs/omni/client/pkg/client

# Demo

Demo Placeholder

## Going further

### Integrations:

Harbor - Pull through Cache (Proxy) config in containerd.

Cilium CNI.

**Custom K8s controller + CRDs.**

**Omni crossplane provider?**

```
kind: Cluster
name: demo
kubernetes:
    version: v1.32.2
talos:
    version: v1.10.5
features:
    enableWorkloadProxy: true
    backupConfiguration:
        interval: 24h
patches:
  - name: Deploy Cilium CNI
    annotations:
      description: Set up Cilium CNI on Talos
      name: Deploy Cilium CNI
    file: patches/cluster/cni.yaml
  - name: Audit Logging
    annotations:
      description: Enable audit logging on Talos
      name: Audit Logging
    file: patches/cluster/audit-logging.yaml

---
```

Questions?

TALOSCON 2025

HOSTED BY SIDERO

# Thank you


Contact us

Name: Alexandre Ferreira
Role: Lead SRE/DevOps Engineer
Email: alexandre.branco@promptlyhealth.com

Name: Paulo Araújo
Role: SRE/DevOps Engineer
Email: paulo.silvaaraujo@promptlyhealth.com