Customers

Bundesministerium Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie

Bundesministerium Kunst, Kultur, öffentlicher Dienst und Sport

Bundesministerium Justiz

Parlament Österreich

Stadt Wien

universität wien

INTERACT

VF CORPORATION

WIEN ENERGIE

Verbund

APG

FRAUSCHER

PALFINGER

LTW INTRALOGISTICS

esa

cloudflight

Individual digital solutions since 2007

+ 750 employees

+ 1.200 projects

18 Locations in 5 European countries

Long-standing partnerships through strong quality awareness

Various awards for technology, design, and as an employer

Your full-service provider for digital transformation

Expertise

Individual Software Solutions

Legacy System Replacement

Digitalization of Business Processes

Paperless Production

Cloud Migration

Cloud Native

Cloud Operations

Data Platforms & Data Engineering

Data Science & Machine Learning

Computer Vision

NLP / LLMs

Automated Document Processing

TalosOS

The OS Kubernetes Deserves

Who has experience with **Kubernetes**?

Who has experience with **TalosOS**?

Who is mainly here for the
FREE Beer and Food?

Linux

How I became a Talos fan

Pets

Pets VS Herd

VS

Siegfried Stumpfer

What is TalosOS?

- Immutable
- Atomic
- Minimal
- Ephemeral
- API-Driven Kubernetes First
- Hardened (Kernel Self Protection Project)
- Configured via YAML

TalosOS Setup

```
sigi@SigiPC:~$ talosctl gen secrets -o secrets.yaml
```

```
sigi@SigiPC:~$ talosctl gen config --with-secrets secrets.yaml test-cluster https://192.168.0.199:6443

generating PKI and tokens
Created /home/sigi/controlplane.yaml
Created /home/sigi/worker.yaml
```

```
sigi@SigiPC:~$   talosctl apply-config --insecure \
    --nodes 192.168.0.199 \
    --file controlplane.yaml
```

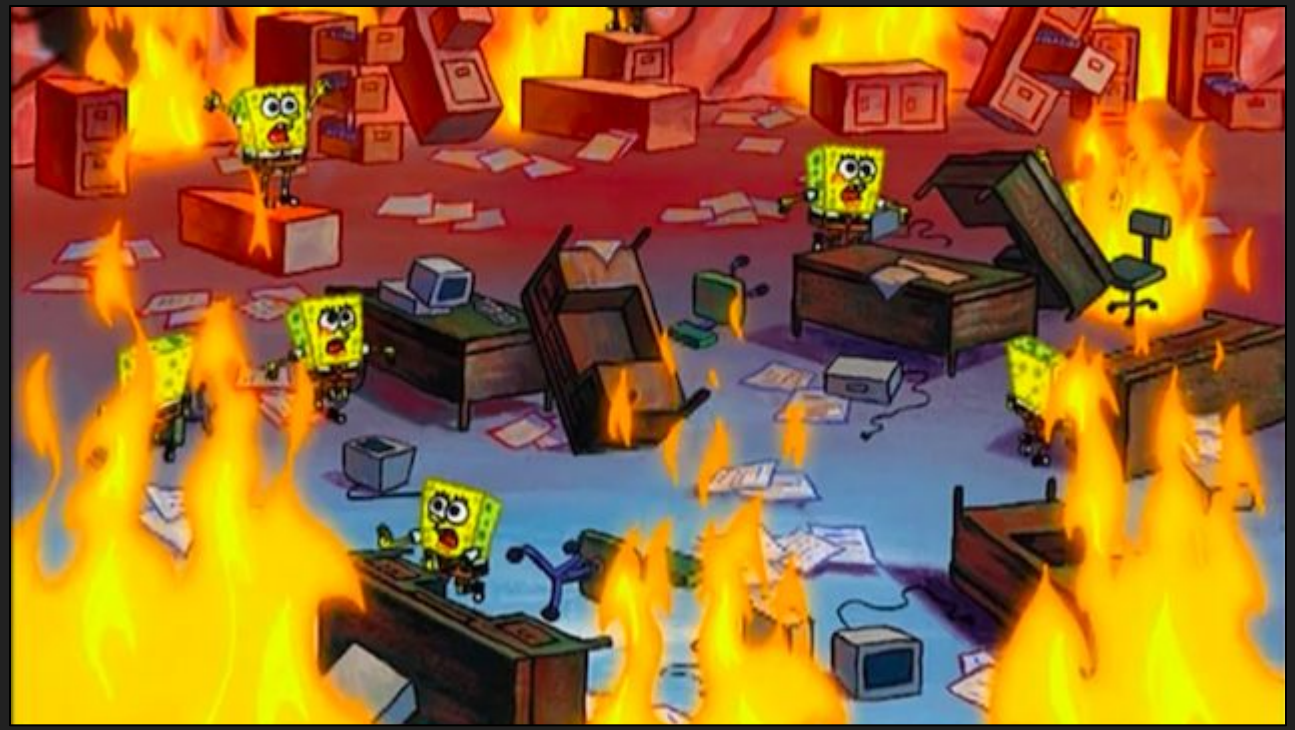
```
sigi@SigiPC:~$ talosctl bootstrap --nodes 192.168.0.199 --endpoints 192.168.0.199 \
  --talosconfig=./talosconfig
```

```
sigi@SigiPC:~$ talosctl kubeconfig --nodes 192.168.0.199 --endpoints 192.168.0.199 \
  --talosconfig=./talosconfig
```

Scenario

(Hypothetical)

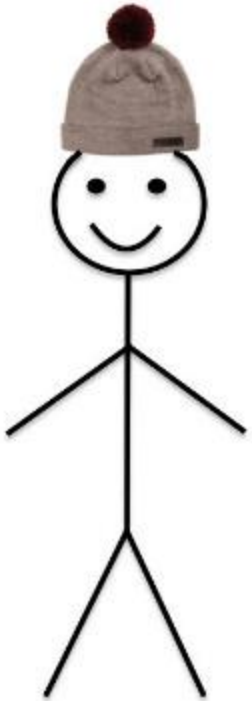
Current Team situation




This is Billy
imgflip.com

This is Billy

He is 19 years old



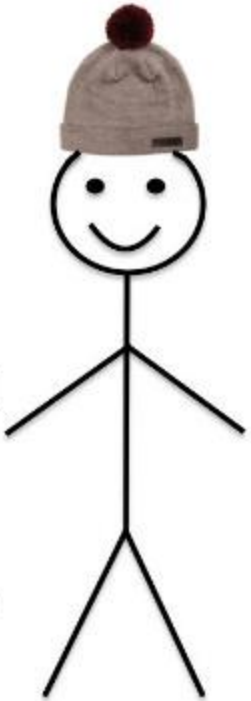

This is Billy
He is 19 years old
He has watched a 1 hour DevOps Tutorial
imgflip.com

This is Billy

He is 19 years old

He has watched a 1 hour DevOps Tutorial

And happens to be the Nephew of your CTO



Team Talos

Manages their Cluster with Talos

2

Team Two

Manages their Cluster with Ubuntu

Billy tries SSH

Billy tries to SSH - Team Two

2

- If password right => gets in
- RBAC

Billy tries to SSH - Team Talos

- There is no SSH installed

Setup Access to Talos - Gen Secrets

```
sigi@SigiPC:~$ talosctl gen secrets -o secrets.yaml
```

secrets.yaml

```yaml
cluster:
    id: GVrv6hR8nkAE1LAuDHqUNIgSumeYH8q2YcqoLoSVCWc=
    secret: rss0XB4vE4PhWNWF8/PBwnAcnHBY3CvYbJ5CIROyNb8=
secrets:
    bootstraptoken: jtno4k.8xoyk0cqo1pegzcu
    secretboxencryptionsecret: xZJJZdq72JLYMSEgJNnfjHZEO8ySXS48EDA6XrR+KOs=
trustdinfo:
    token: 0hz6da.oe0plobziq5nrfgq
certs: ...
```

Setup Access to Talos - Gen config

```
sigi@SigiPC:~$ talosctl gen config --with-secrets secrets.yaml test-cluster https://192.168.0.199:6443

generating PKI and tokens
Created /home/sigi/controlplane.yaml
Created /home/sigi/worker.yaml
```

talosconfig

```yaml
context: talos-prod
contexts:
    talos-prod:
        endpoints:
            - 192.168.0.199
        nodes:
            - 192.168.0.199
        ca: ...
        crt: ...
        key: ...
```

Monitor Output

Billy walks to Machine - Team Talos

```
talos-worker-1 (v1.9.3): uptime 406h49m57s, 2x3GHz, 3.8 GiB RAM, PROCS 22, CPU

UUID        02a26102-          TYPE        worker    HOST          talos-worker-1
cd3d-4540-aa2b-fc16e2c1c065    KUBERNETES  v1.32.1   IP            192.168.0.105/24
CLUSTER     talos-prod (4      KUBELET     √         GW            192.168.0.1
machines)                      Healthy               CONNECTIVITY  √ OK
SIDEROLINK  n/a                                      DNS           192.168.0.1
STAGE       √ Running                                NTP
── Logs ──────────────────────────────────────────────────────────────────────
lookup discovery.talos.dev on 127.0.0.53:53: no such host\"", "endpoint":
"discovery.talos.dev:443"}
user: warning: [2025-02-18T03:58:23.2577146Z]: [talos] hello failed
{"component": "controller-runtime", "controller":
"cluster.DiscoveryServiceController", "error": "rpc error: code = Unavailable
desc = connection error: desc = \"transport: Error while dialing: dial tcp:
lookup discovery.talos.dev on 127.0.0.53:53: no such host\"", "endpoint":
"discovery.talos.dev:443"}
user: warning: [2025-02-18T03:58:25.5510776Z]: [talos] hello failed
{"component": "controller-runtime", "controller":
"cluster.DiscoveryServiceController", "error": "rpc error: code = Unavailable
desc = connection error: desc = \"transport: Error while dialing: dial tcp
```

Billy walks to Machine - Team Two

2

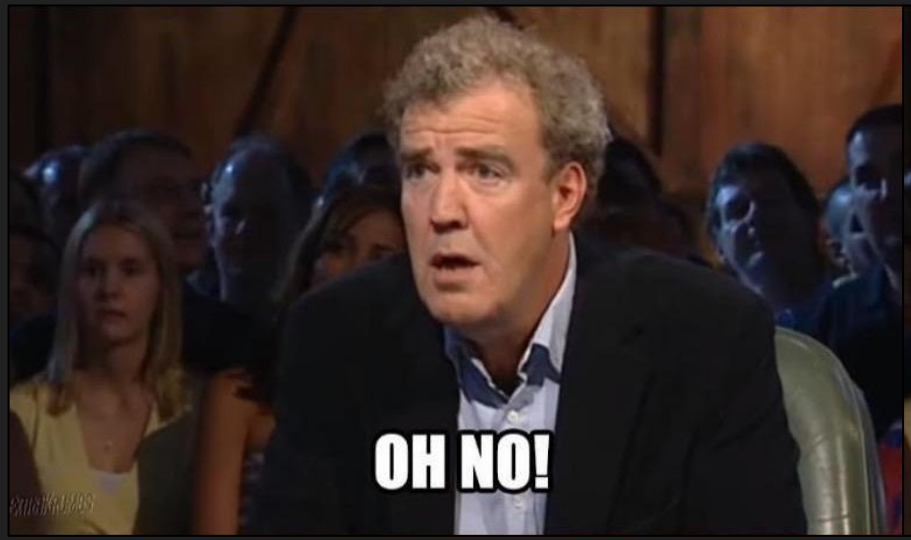
```
9 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

1 additional security update can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm


Last login: Sun Feb 16 13:03:08 2025 from 192.168.0.143
user@dockervm:~$
```

Destroy a Node

Billy destroys node - Team Talos



Reset Talos Nodes

```
sigi@SigiPC:~$ talosctl gen config --with-secrets secrets.yaml test-cluster https://192.168.0.199:6443

generating PKI and tokens
Created /home/sigi/controlplane.yaml
Created /home/sigi/worker.yaml
```

```
sigi@SigiPC:~$ talosctl reset -n 192.168.0.199
```

```
sigi@SigiPC:~$ talosctl -n 192.168.0.199 apply-config -f worker.yaml
```

worker.yaml

```yaml
version: v1alpha1
debug: false
persist: true
machine:
    type: worker
    token: 0hz6da.oe0plobziq5nrfgq
    ca:
        crt: ...
        key: ""
    certSANs: []
    kubelet:
        image: ghcr.io/siderolabs/kubelet:v1.32.1
        defaultRuntimeSeccompProfileEnabled: true
        disableManifestsDirectory: true
    network: {}
    install:
        disk: /dev/sda
        image: ghcr.io/siderolabs/installer:v1.9.3
        wipe: false
    registries: {}
    features:
        rbac: true
        stableHostname: true
        apidCheckExtKeyUsage: true
        diskQuotaSupport: true
        kubePrism:
            enabled: true
            port: 7445
        hostDNS:
            enabled: true
            forwardKubeDNSToHost: true
...
```

worker.yaml

```yaml
...

cluster:
    id: GVrv6hR8nkAE1LAuDHqUNIgSumeYH8q2YcqoLoSVCWc=
    secret: rss0XB4vE4PhWNWF8/PBwnAcnHBY3CvYbJ5CIROyNb8=
    controlPlane:
        endpoint: https://192.168.0.199:6443
    clusterName: test-cluster
    network:
        dnsDomain: cluster.local
        podSubnets:
            - 10.244.0.0/16
        serviceSubnets:
            - 10.96.0.0/12
    token: jtno4k.8xoyk0cqo1pegzcu
    ca:
        crt: ...
        key: ""
    discovery:
        enabled: true
        registries:
            kubernetes:
                disabled: true
            service: {}
```

Billy destroys node - Team Two

2

Upgrades an OS

(and corrupts it)

Billy upgrades System - Team Talos

- A/B Rollout
- Atomic Failure
- Logs of what failures occurred

Billy upgrades System - Team Two

2

- Partially Applied updates
- Pray to god you have backup Snapshots
- Manual Intervention or complex systems needed

This is Dimitry

Dimitry attempts Hack - Team Talos

1. /sbin/init => custom Init instead of Systemd
2. /bin/containerd => Container Runtime (also CRI-O support)
3. /bin/runc => What runs Containerd
4. /sbin/modprobe => configuring Kernel Modules
5. /sbin/lvm => Linux logical Volumes
6. /sbin/dmsetup => more complex Disk situations
7. /sbin/udevd => manage kernel Messages
8. /sbin/mkfs.xfs => create xfs file system
9. /sbin/xfs_repair => repair xfs file systems
10. /sbin/xtables-legacy-multi => System linked to iptables and ip6tables

Dimitry attempts Hack - Team Two

2

- What ever you have installed is attackable
- No limits to attack surface

But you could….

Downsides

- Only and only kubernetes
- Most benefits gone in hybrid clusters
- No shell or SSH => different philosophy
- Able to be used insecure (non-default)
- Only recent ISCSI support

Demo

Talos Cluster

- Siegfried Stumpfer
- **Work:** Software Engineer / SRE @Cloudflight
- **Interests:** All things Tech, Gardening, Reading
- Municipal council member

Thank you! Questions?