Autonomous Confidential Kubernetes

How to securely manage K8s from within K8s
The different flavors of confidential computing

**Level 1**
Protect keys

**Level 2**
Protect single containers/apps

**Level 3**
Protect entire deployments
Challenges with Level 3

- UX
- Orchestration
- Scalability
- Attestation
- I/O
- Day-2 Ops
- Managed Services
From a Confidential VM...
... to a Confidential Cluster
Keeping the UX simple...

```plaintext
constellation create <cloud> <initial size>
constellation init
kubect1 [scale anything!]
```
... by addressing the challenges below

```
constellation create <cloud> <initial size>
constellation init
kubect1 [scale anything!]
```
What about “managed” and day-2 operations?
MANAGE K8S FROM WITHIN K8S
Cluster management strategies

**On prem**
Manually managed

- Scale
- Join
- Update OS
- Update K8s

Admin in control

**Fully managed**
Automatically managed by CSP

- Scale
- Join
- Update OS
- Update K8s

CSP in control
... meeting in the middle

In cluster
Autonomously managed

Scale
Join
Update OS
Update K8s

Admin & cluster in control

Confidential context
Constellation Node

- k8s
- Pod
- ... Bootstrapper
- State Disk
- rootFS
- Unified Kernel Image
- Bootloader
- Firmware
Constellation Services

- Node Operator
- JoinService
- KeyService
- ...

Diagram showing the services in a Constellation.
Autonomous Join

New node

Join Service

aTLS handshake

Request to Join

JoinToken, ...

New node

Join Service
Updates

Node Operator

Node A

Node B

DevOps engineer
Treat your nodes like cattle, not pets
Updates: Apply declarative configuration

kubernetesVersion: 1.26.1
nodeImageReference: ami-063a9ea2ff5685f7f

OS image measurements

K8s component hashes
Updates: Node operator reconciles

Node A
- Up to date
- OS image
- Kubelet

Node B
- Need replacement
- OS image
- Kubelet

Node C
- Need replacement
- OS image
- Kubelet
Updates: Node operator reconciles

- **Node A**: OS image (🟢), Kubelet (🟢)
- **Node B**: OS image (🟢), Kubelet (🟡)
- **Node C**: OS image (🟡), Kubelet (🟡)
- **Node D**: OS image (🟢), Kubelet (🟢)

- **Up to date**
- **Replace**
- **Need replacement**
Updates: Node operator reconciles

Node A
- OS image
- Kubelet

Node B
- OS image
- Kubelet

Cordon & Drain

Node C
- OS image
- Kubelet

Node D
- OS image
- Kubelet

Up to date
Replace
Need replacement
Updates: Node operator reconciles

Node A
- OS image
- Kubelet

Node D
- OS image
- Kubelet

Node C
- OS image
- Kubelet

Up to date

Need replacement
CONCLUSION
Constellation

DevOps engineer

Container + Container

Cloud storage

Microsoft Azure, AWS, Google Cloud, openstack
Learn more

MARCH 15. ONLINE

Open Confidential Computing Conference 2023

Sponsored by

Microsoft Azure  intel  CONSENSUS COMPUTING CONSORTIUM
Thanks!

- Check it out on GitHub: https://github.com/edgelesssys/constellation
  - Create your first confidential Kubernetes today
  - Leave a 🌟:-)
- Get in touch via @malt3 & @m1ghtymo
  - Or join us @ https://discord.gg/rH8QTH56JN

Learn more

- CLI demo
- Features, benchmarks, etc.
- App demos: