
KubeCon
CloudNativeCon
North America 2023


KubeCon | CloudNativeCon

North America 2023

The Next Frontier: Exploring the Confidentiality of Kubernetes Control Planes

Jens Freimann, Pradipta Banerjee
Red Hat


KubeCon | CloudNativeCon

North America 2023

1. Setting the scene: The need for control plane protection

Why protect the control-plane?

1. Central Management:
   - Orchestrates cluster activities: deployment, scaling, ..

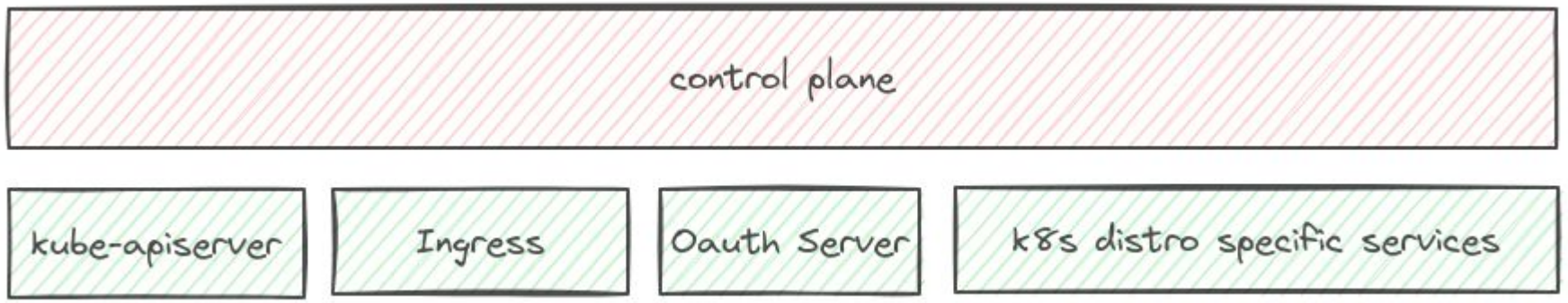
2. Sensitive Data Storage:
   - Houses critical data: configurations, secrets, and state data.

3. Access Control:
   - Manages authentication and authorization.

4. API Exposure:
   - Primary point of interaction for users and systems.

End user facing components

These request serving pods are especially vulnerable as they are directly exposed to end user




KubeCon | CloudNativeCon

North America 2023

2. Learning from the past: Vulnerabilities and their impact

Understanding Vulnerabilities

External exposure: kube-apiserver & others are prime targets

Operational complexity: Handles diverse requests & protocols

Critical change authority: Risks unauthorized system changes

Auth challenges: Vulnerabilities risk unauthorized access

Config cisks: Potential for system exposure

End user facing components

Vulnerabilities:

- High privileges: Attractive targets due to administrative control
- Misconfiguration risks: Can lead to unauthorized access or data leaks
- Auth challenges: OAuth mishaps can result in serious security breaches

e.g. Kube API server:
CVE-2019-11253 “Billion laughs” attack on API servier
CVE-2020-8559 “... escalate privileges from a node compromise to a full cluster compromise.”

3. Current state: Protecting Kubernetes clusters

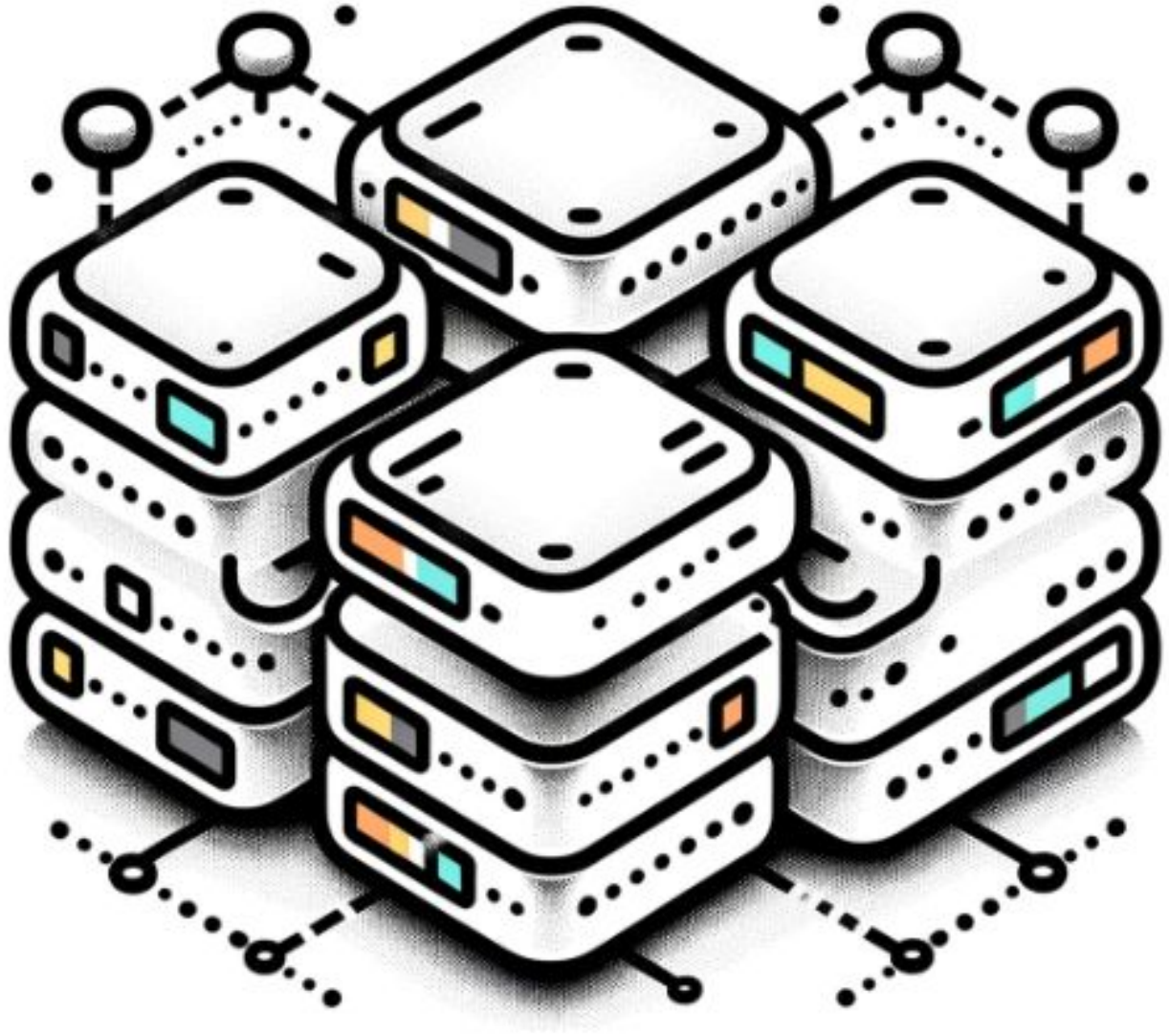
Existing processes and tools

- Access control and RBAC
- Network policies and segmentation
- Encryption at rest and transit
- Regular updates and patch management
- Monitoring, logging and auditing

4. Evolution of cluster usage: From single to managed control planes

Shared clusters

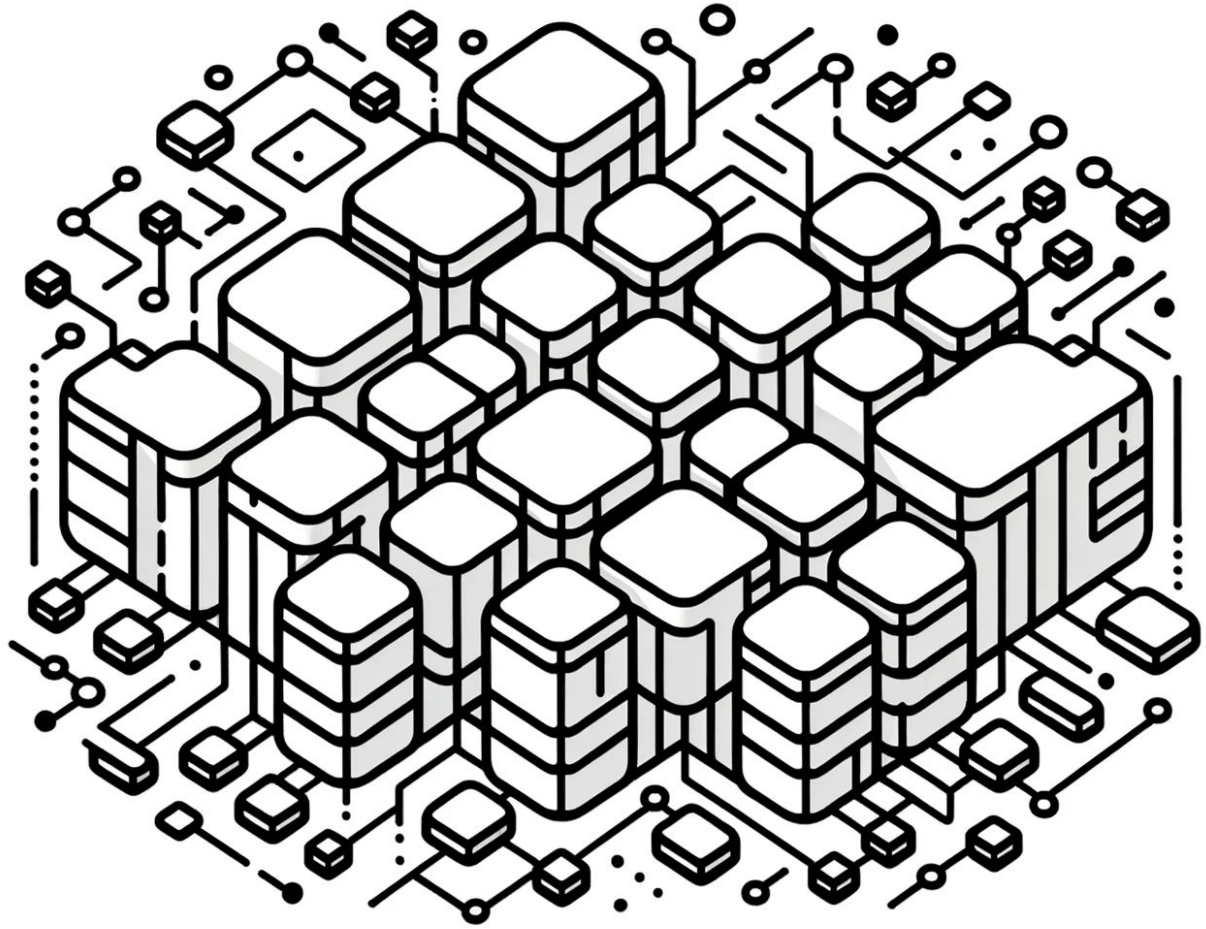
shared control-plane



Many clusters

Every team/tenant/
customer gets their
own cluster

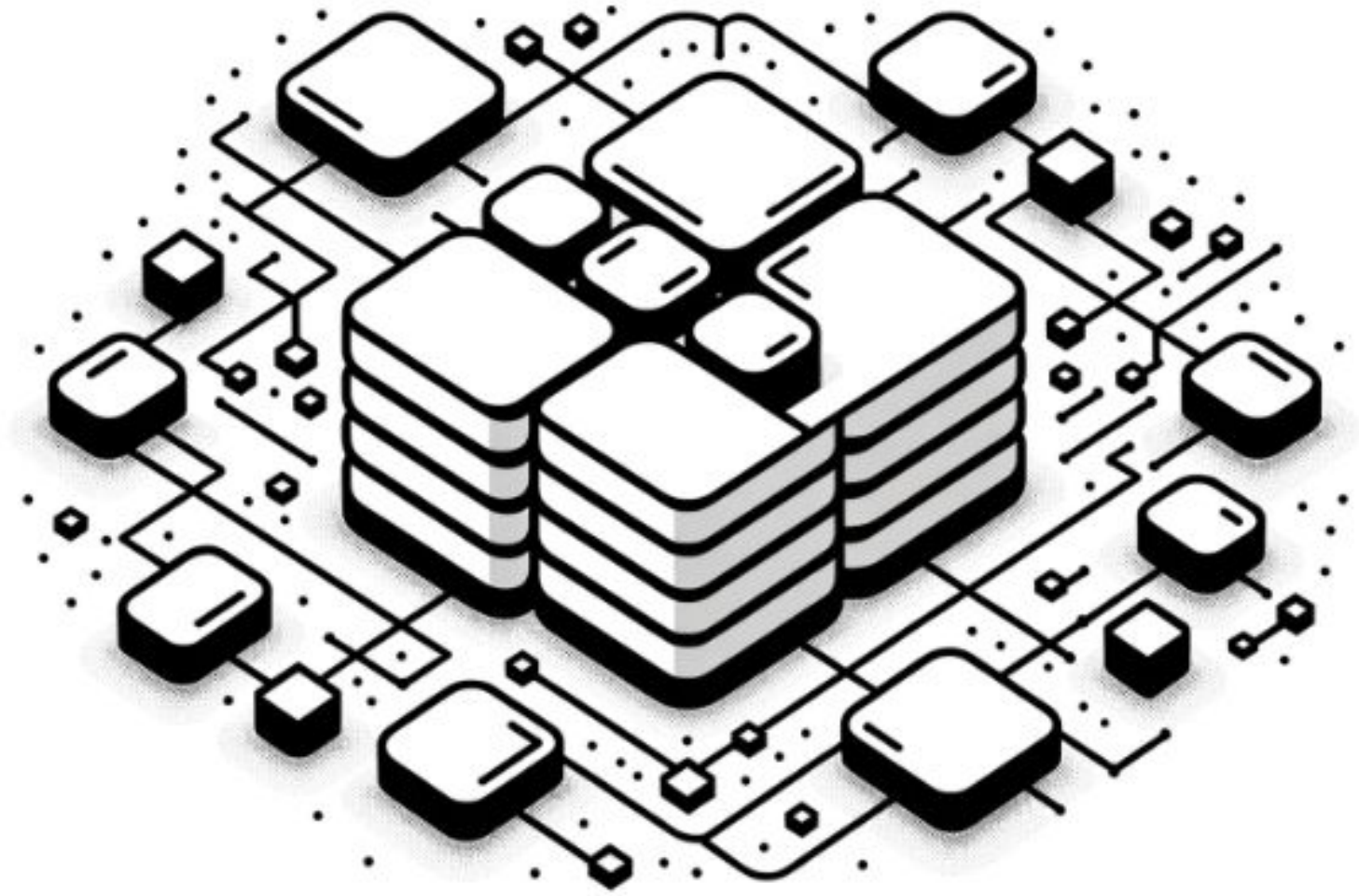
- compliance
- independence, flexibility
- performance
- simpler debugging
- predictable costs
- stronger isolation



Managed control planes

Many control planes on
a management cluster +
separate worker pools

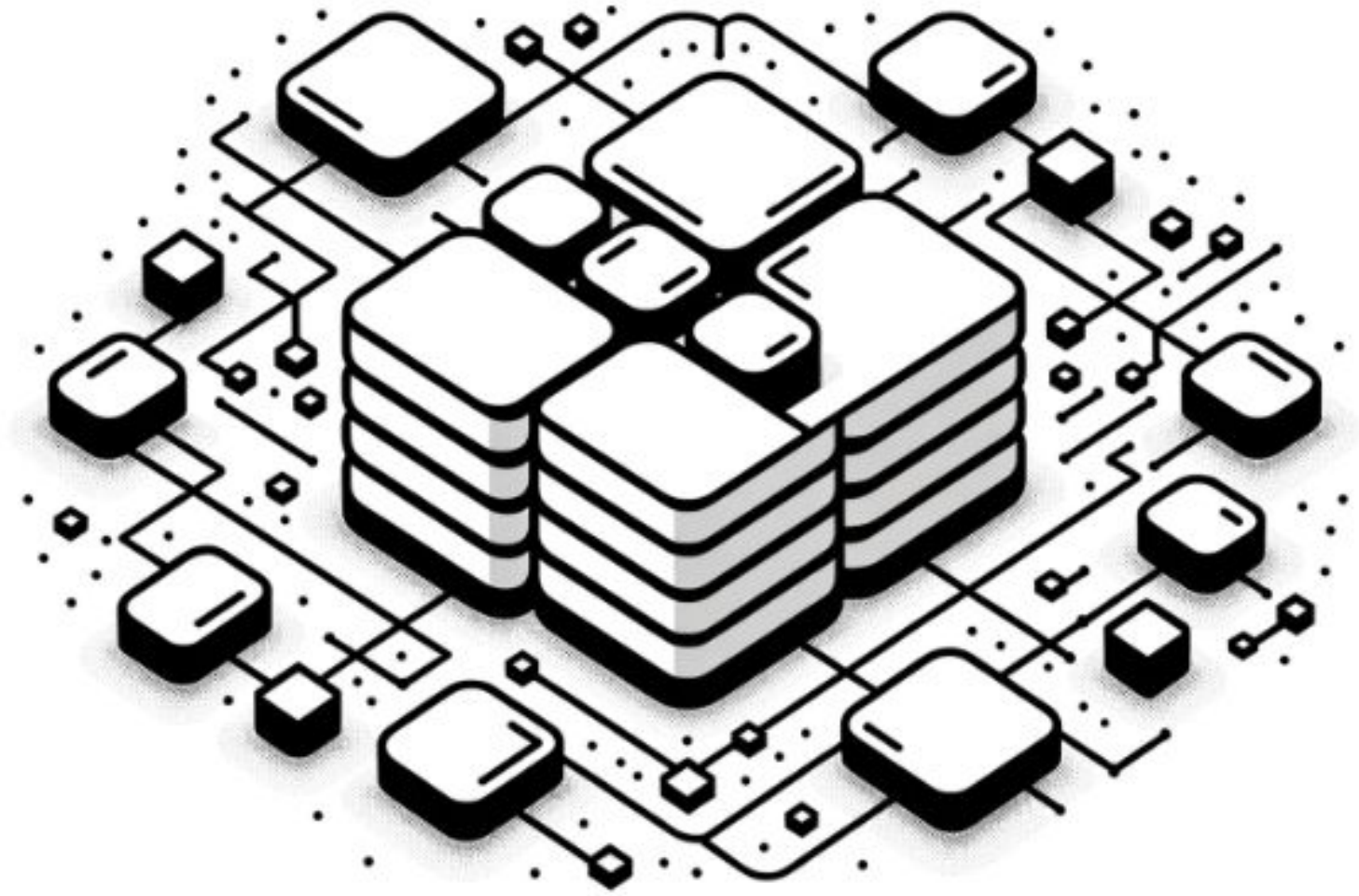
Gardener
(GKE/EKS/AKS)
Kamaji
Hypershift



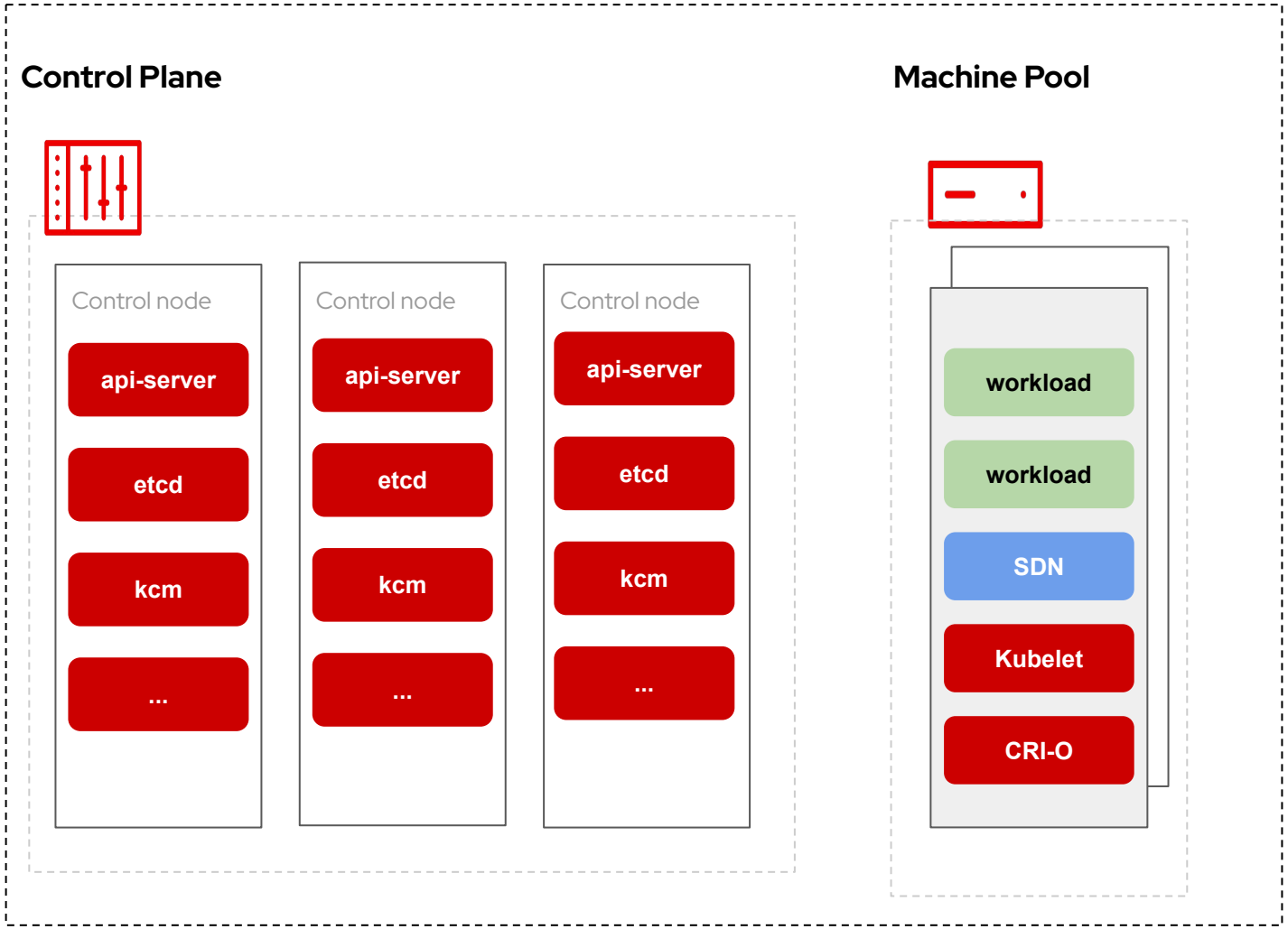
Managed control planes

Many control planes on a management cluster + separate worker pools

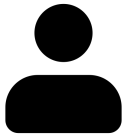
Gardener (GKE/EKS/AKS)
Kamaji
Hypershift



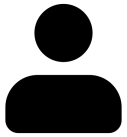
classic cluster



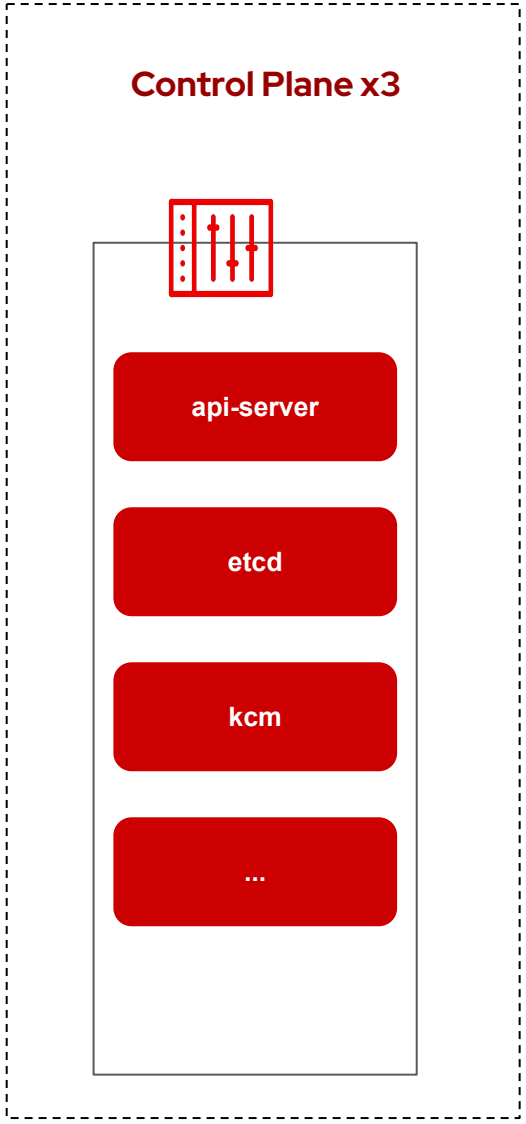
Hypershift

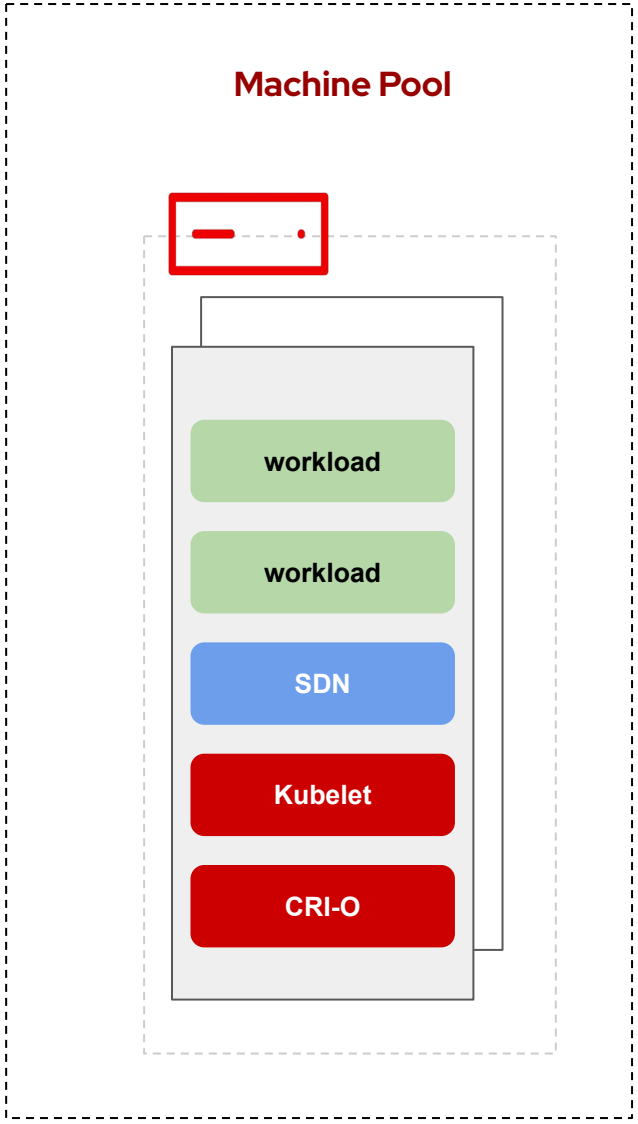


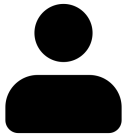
Infrastructure owner



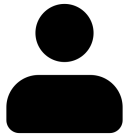
Orchestration owner





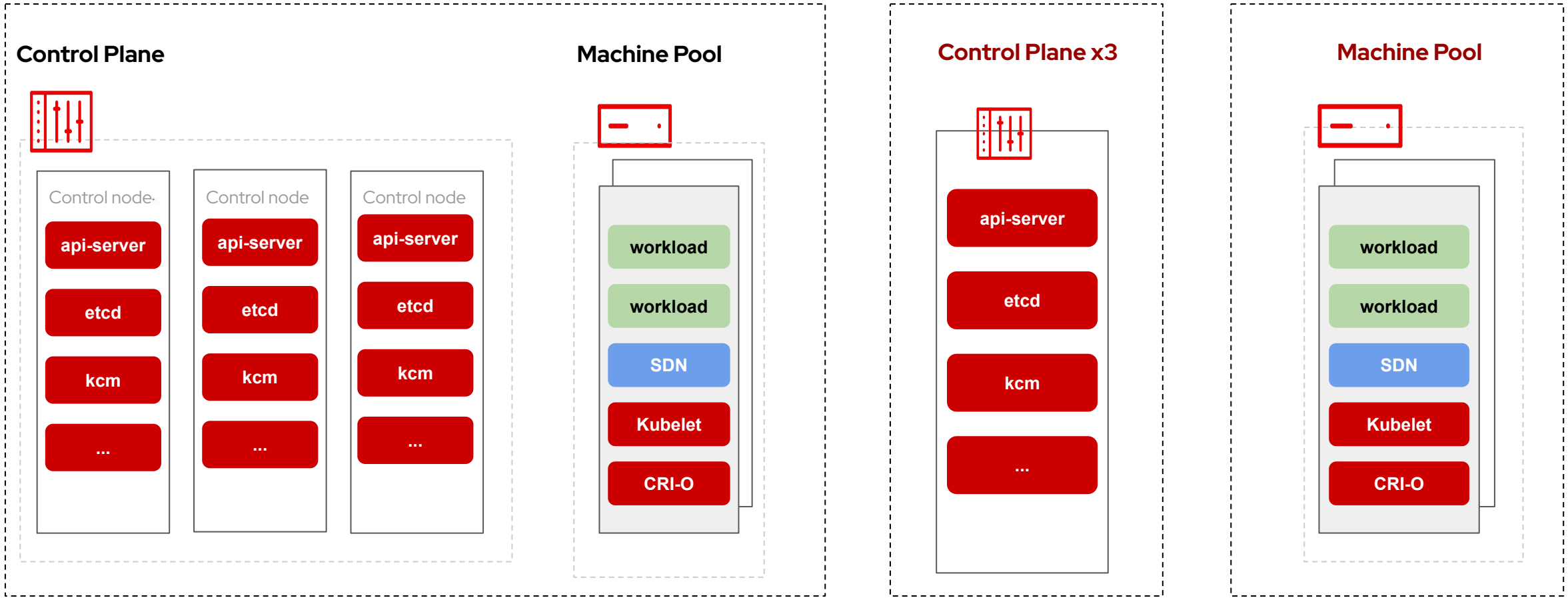


Workload provider

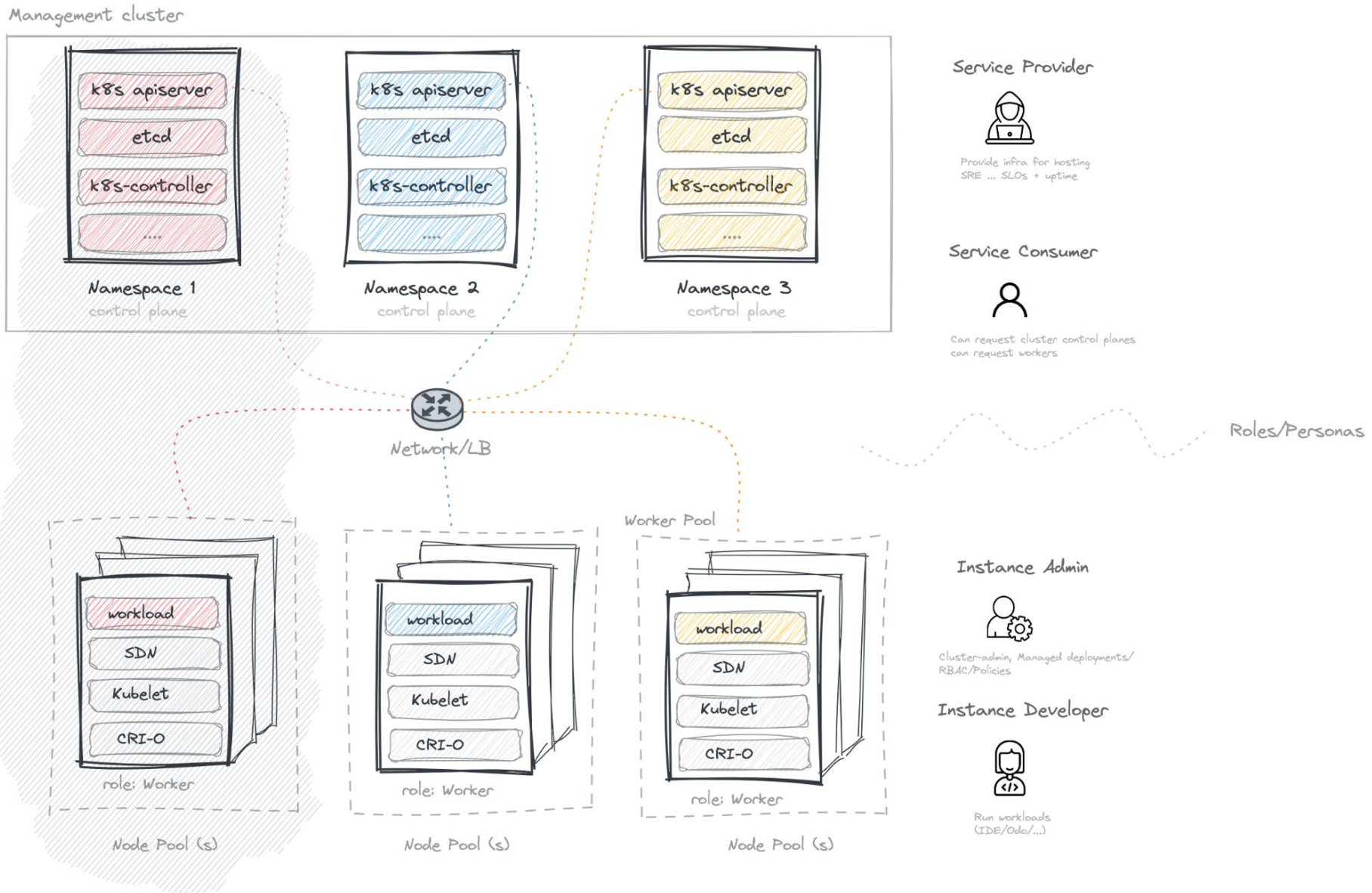


Data owner

Hypershift


Control Plane
Machine Pool
Control node
Control node
Control node
api-server
api-server
api-server
etcd
etcd
etcd
kcm
kcm
kcm
...
...
...
workload
workload
SDN
Kubelet
CRI-O
Control Plane x3
Machine Pool
api-server
etcd
kcm
...
workload
workload
SDN
Kubelet
CRI-O

Hypershift


Management cluster
k8s apiserver
etcd
k8s-controller
....
Namespace 1
control plane
k8s apiserver
etcd
k8s-controller
....
Namespace 2
control plane
k8s apiserver
etcd
k8s-controller
....
Namespace 3
control plane
Service Provider
Provide infra for hosting
SRE ... SLOs + uptime
Service Consumer
Can request cluster control planes
can request workers
Network/LB
Roles/Personas
Worker Pool
workload
SDN
Kubelet
CRI-O
role: Worker
Node Pool (s)
workload
SDN
Kubelet
CRI-O
role: Worker
Node Pool (s)
workload
SDN
Kubelet
CRI-O
role: Worker
Node Pool (s)
Instance Admin
Cluster-admin, Managed deployments/
RBAC/Policies
Instance Developer
Run workloads
(IDE/Odo/...)


KubeCon | CloudNativeCon

North America 2023

5. Trust and roles in managed control plane setups

Groups that we trust

In-house:
Kubernetes administrator
Application developer
Application administrator

Cloud Provider SREs,
infrastructure,
proesses

3rd Party:
Tenants
Container provider

Trust

Cloud Provider SREs,
infrastructure, proesses

Trust

In your cloud provider:

- Infrastructure owner
- Hardware, Infrastructure and Managed Service (SREs)

Trust

But should you?

Do they **need** to be able to access your secrets, business data, code in order to do their job?

Trust

In-house:

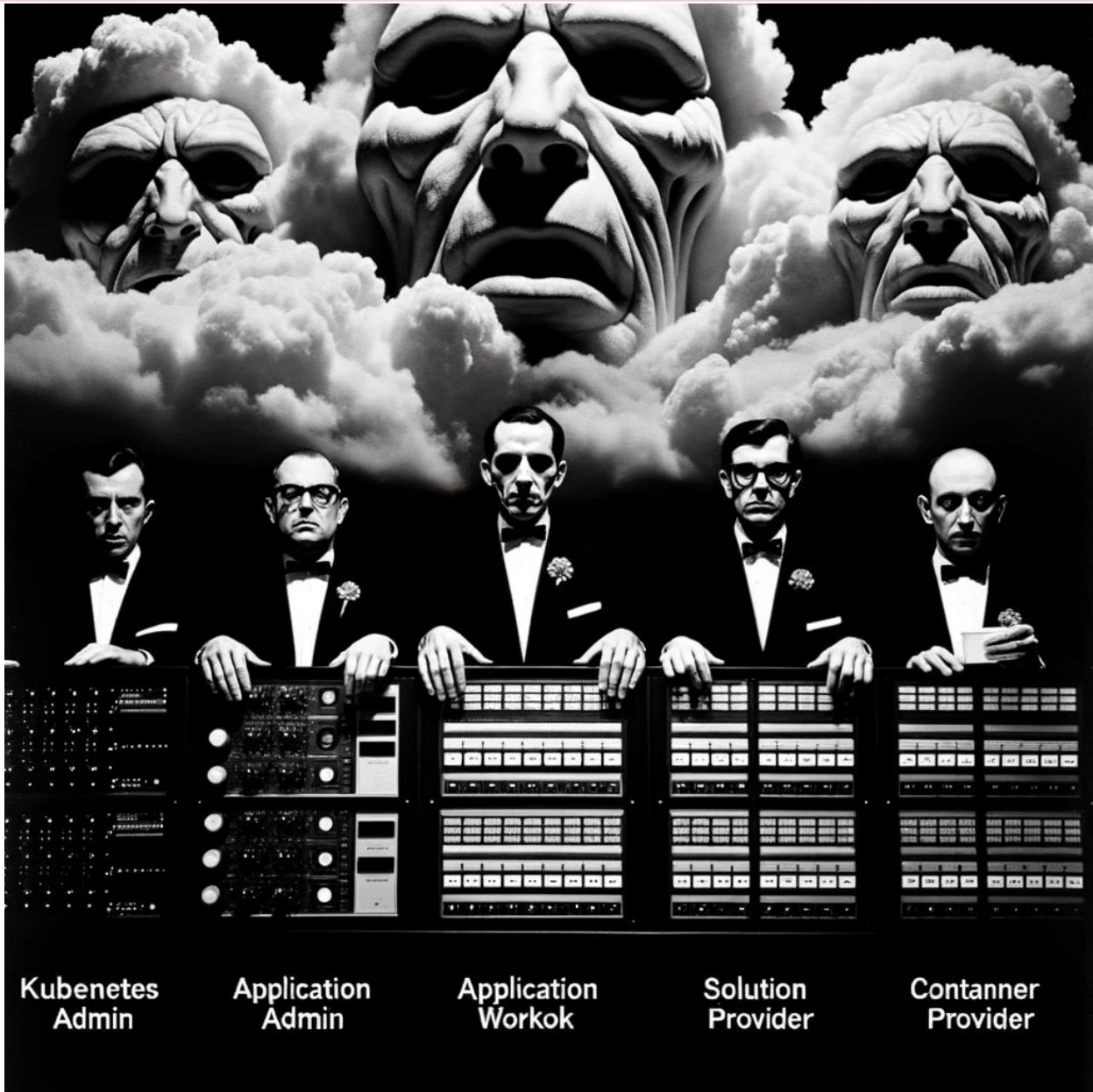
- Orchestration provider Kubernetes and application administrator
- Container providers
- Developer

I

Trust

But should you?

Do they **need** to be able to access your secrets, business data, code in order to do their job?



Trust

3rd parties

- Application user / tenant
- Container provider

Trust

But should you?

Do they **need** to be able to access your secrets, business data, code in order to do their job?

Trust

in Computer criminals?

No, but at least you know what they are up to

Threats and mitigations

Threat Vectors:

Pod Images: Risk of tampering/access.

Pod Memory: Infrastructure provider access.

Pod Data: Provider tampering/access.

Trust boundaries

Technical assurance by

using Confidential

Computing technology

Assurance strategies

Trust-based/procedural assurance		Systemic/cryptographic assurance
-	vs.	-
we promise not to		we cannot

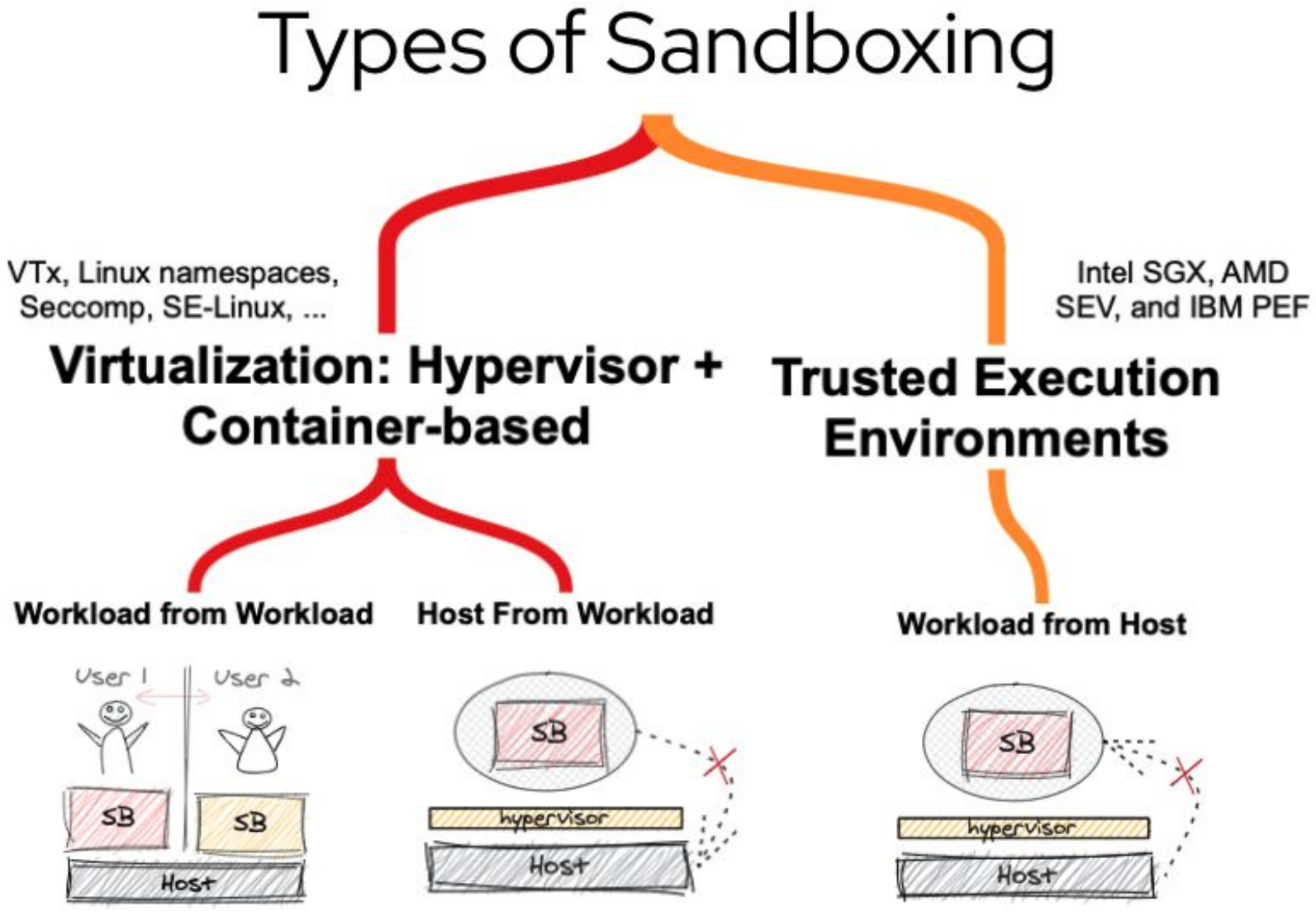
CONFIDENTIAL CONTAINERS


KubeCon | CloudNativeCon

North America 2023

6. Making the case for Confidential Containers

Build on virtualization technology



Confidential Containers threats and mitigations

Threat Vectors:

Pod Images: Risk of tampering/access.

Pod Memory: Infrastructure provider access.

Pod Data: Provider tampering/access.

Confidential Containers threats and mitigations

Mitigations:

- *Images*:
  - Controlled by workload
  - Encrypted/signed

Memory: Runs in confidential memory

Storage: Encrypted & integrity-maintained volumes


KubeCon | CloudNativeCon

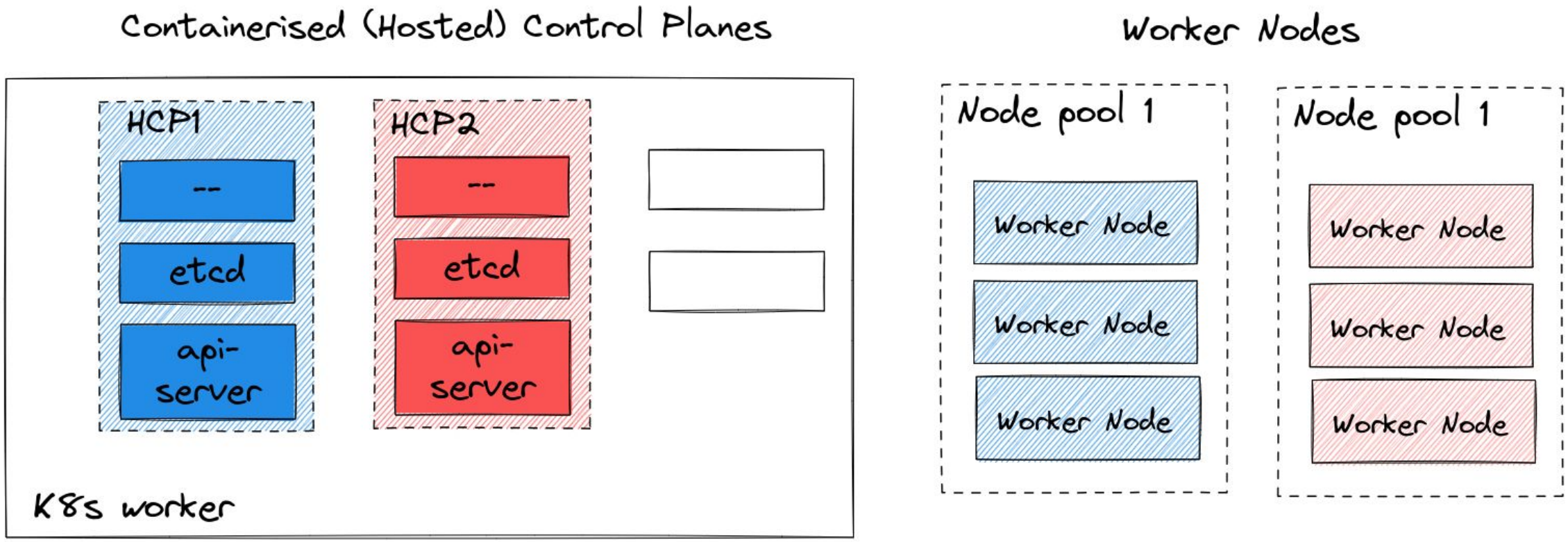
North America 2023

7. Bringing it all together: Hypershift and demo

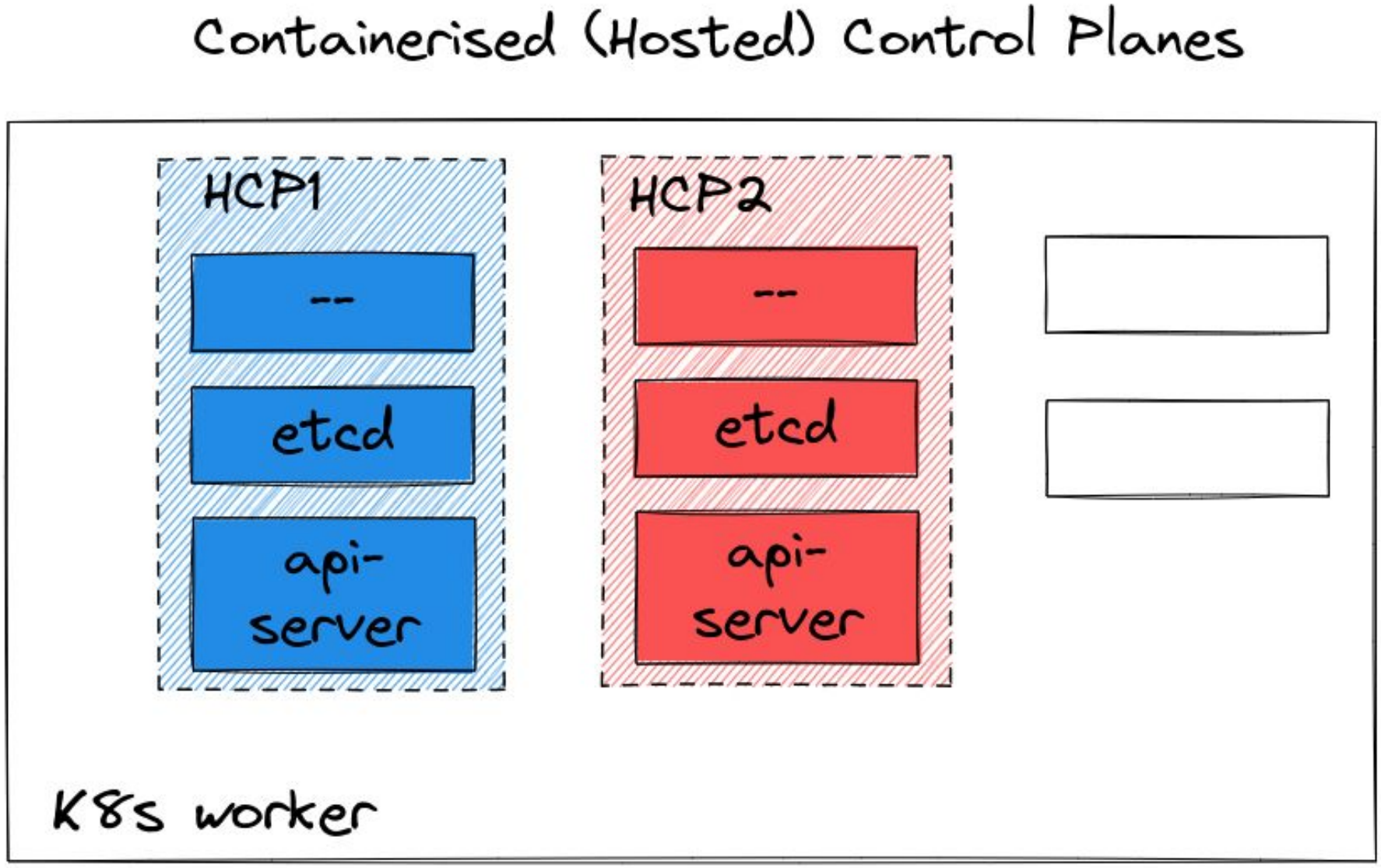
Ensuring integrity and confidentiality

- **Situation**
  - multiple tenants control-plane's on one system, separated in namespaces
- Why is this a risk?
- **Achieve Full Control**: Retain full authority over your control-plane, even in a shared environment
- **Guaranteed Integrity**: Ensure the control-plane only initializes after thorough integrity and security verification.

Hosted control planes

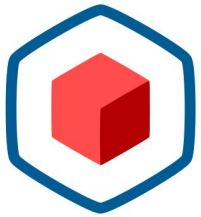


Hosted control planes



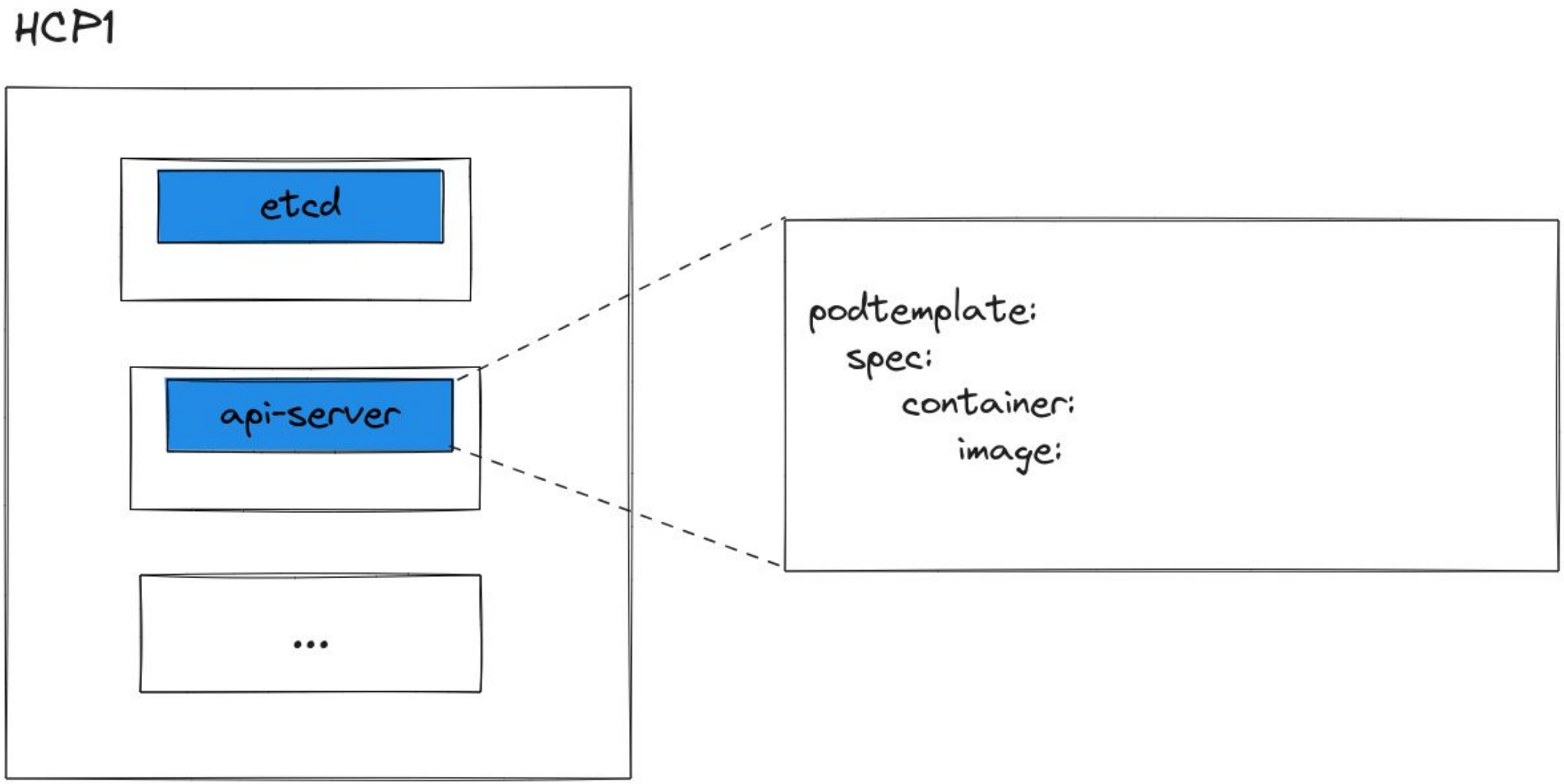
Setup

Hypershift Operator +

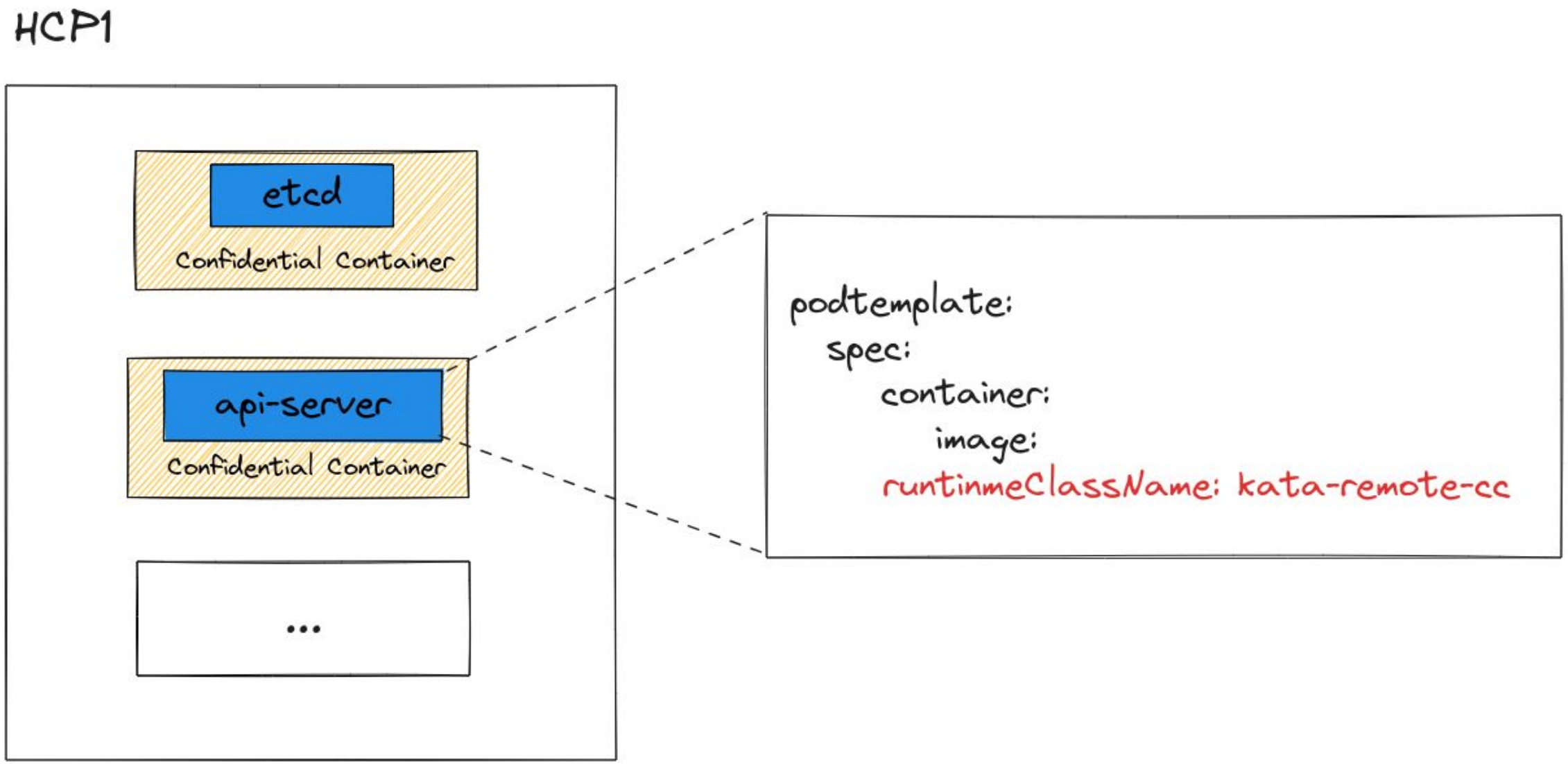


CONFIDENTIAL CONTAINERS

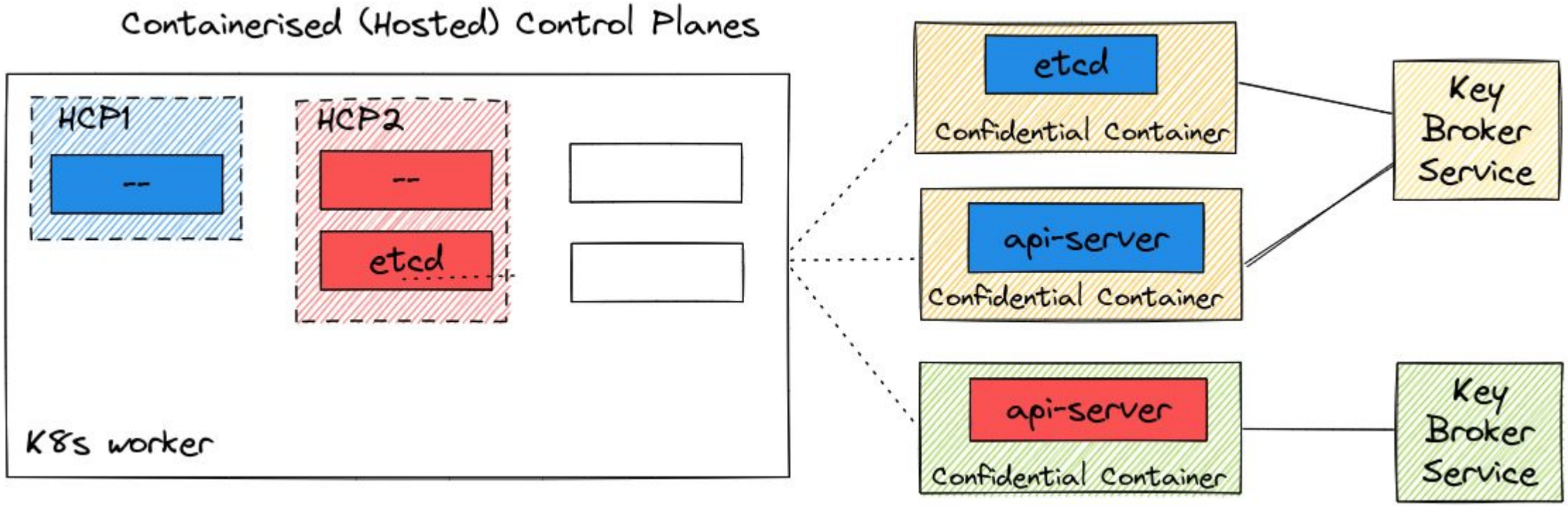
Hosted control planes

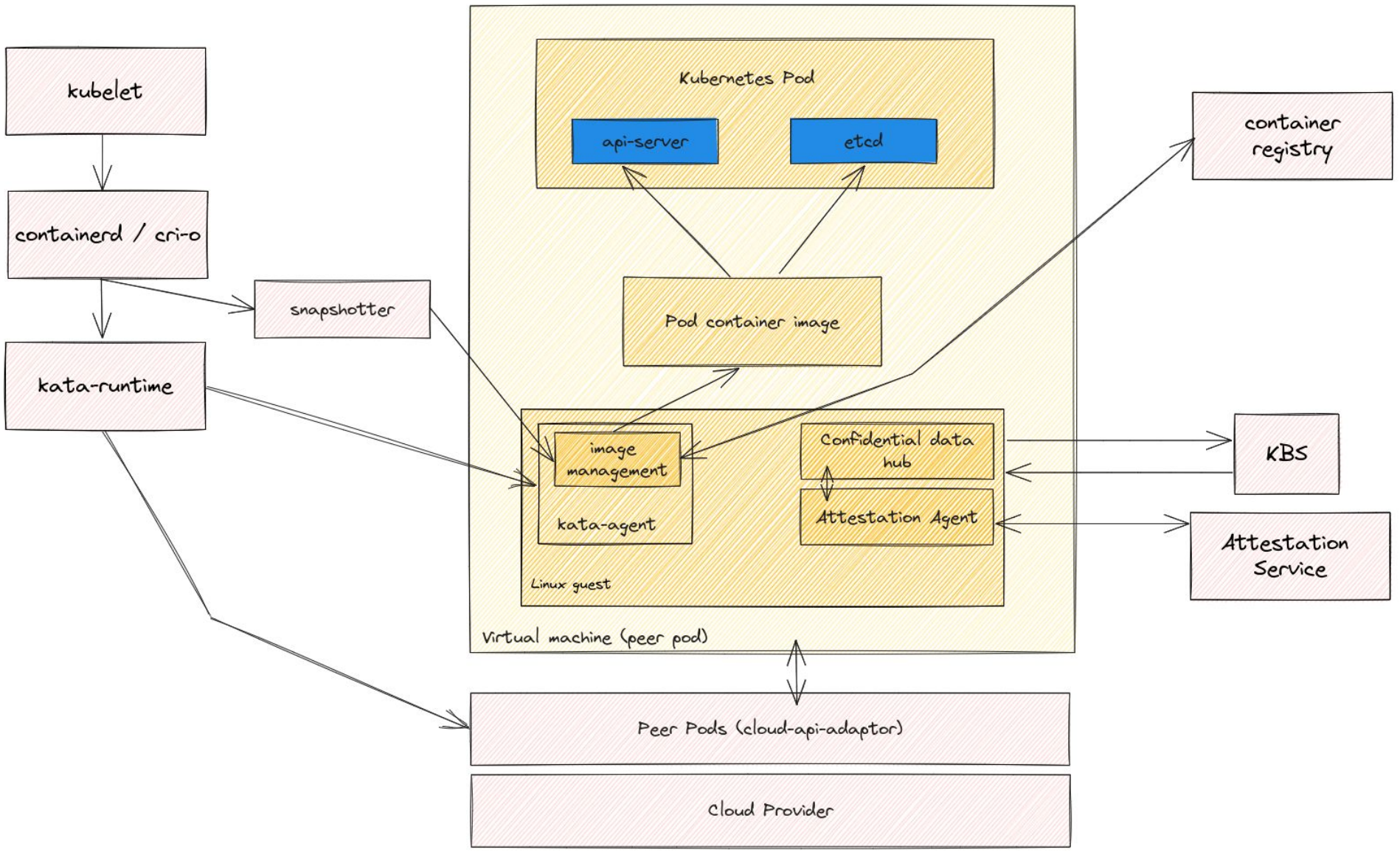


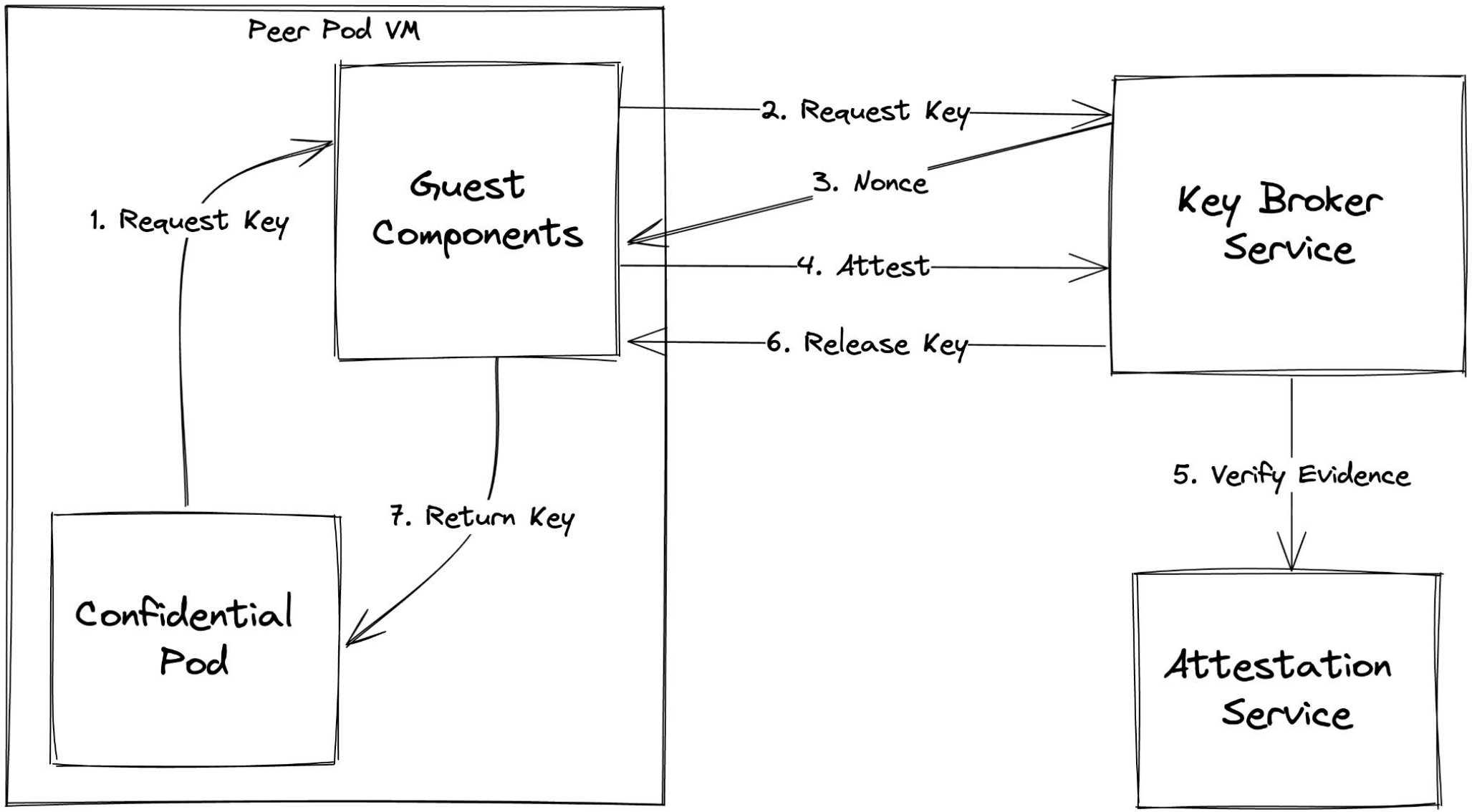
Hosted control planes



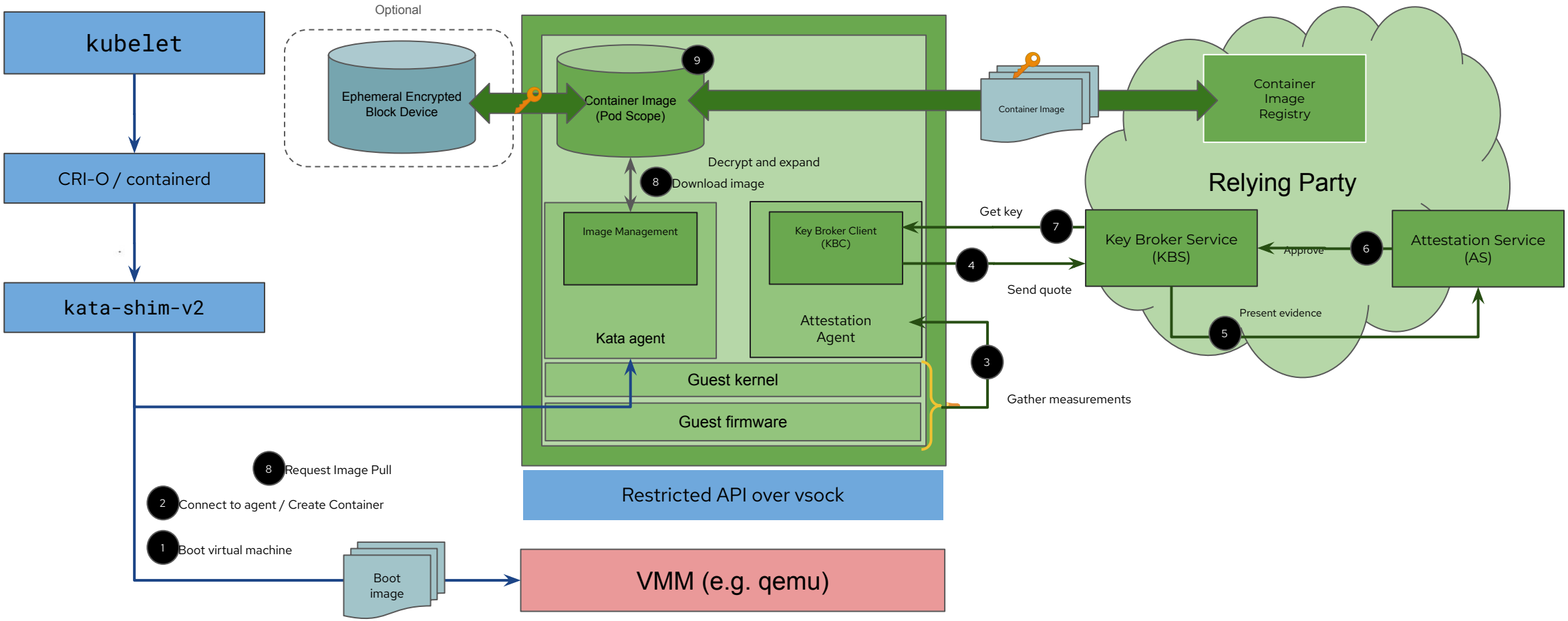
Attestation




kubelet
containerd / cri-o
snapshotter
kata-runtime
Kubernetes Pod
api-server
etcd
Pod container image
image management
kata-agent
Confidential data hub
Attestation Agent
Linux guest
Virtual machine (peer pod)
container registry
KBS
Attestation Service
Peer Pods (cloud-api-adaptor)
Cloud Provider

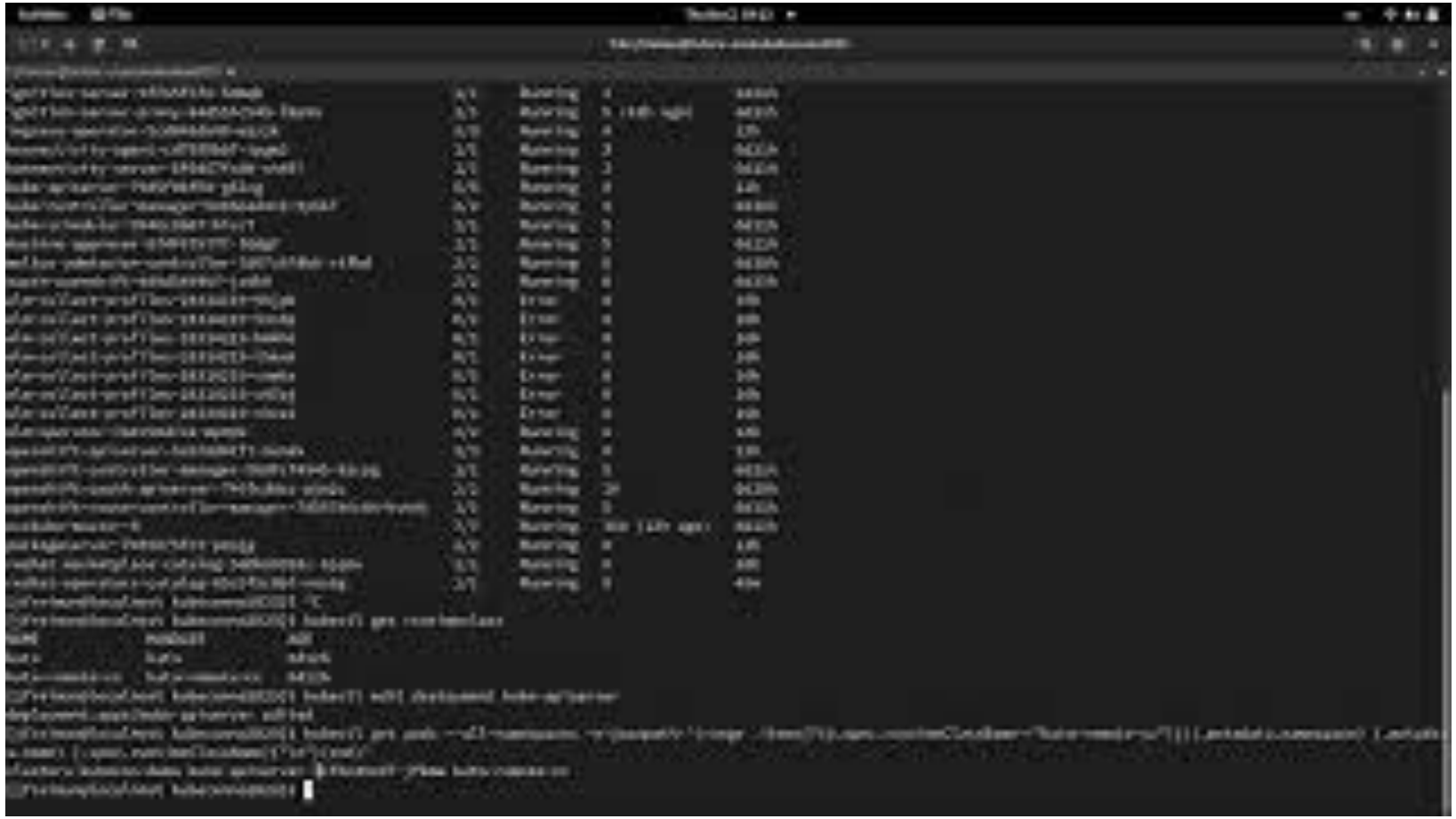

Peer Pod VM
Guest Components
Confidential Pod
1. Request Key
2. Request Key
3. Nonce
4. Attest
5. Verify Evidence
6. Release Key
7. Return Key
Key Broker Service
Attestation Service

Confidential Containers attestation workflow




Demo

Demo



Future work

- integrate into Hypershift, like let user decide which components to run in CoCo, configuration,...
- on CoCo in general, lots of interesting open problems to work on!

Blogs, community meeting, …

Confidential Containers: www.github.com/confidential-containers
Slack: #confidential-containers in CNCF Slack

Release v0.8.0 coming out soon

weekly CoCo Community meeting

Blog: https://red.ht/ccontainers

Relevant talks:

Jeremi Piotrowski, Kubecon EU 2023: The next episode in workload isolation
Fabiano Fidencio, Jens Freimann, Kubecon EU 2023: Confidential Containers made easy
James Magowan, Samuel Ortiz: Confidential Containers Explained
Christophe de Dinechin: The Five Big Problems with Confidential Containers

Q & A

Jens Freimann <jfreiman@redhat.com>
Pradipta Banerjee <bpradipt@redhat.com>

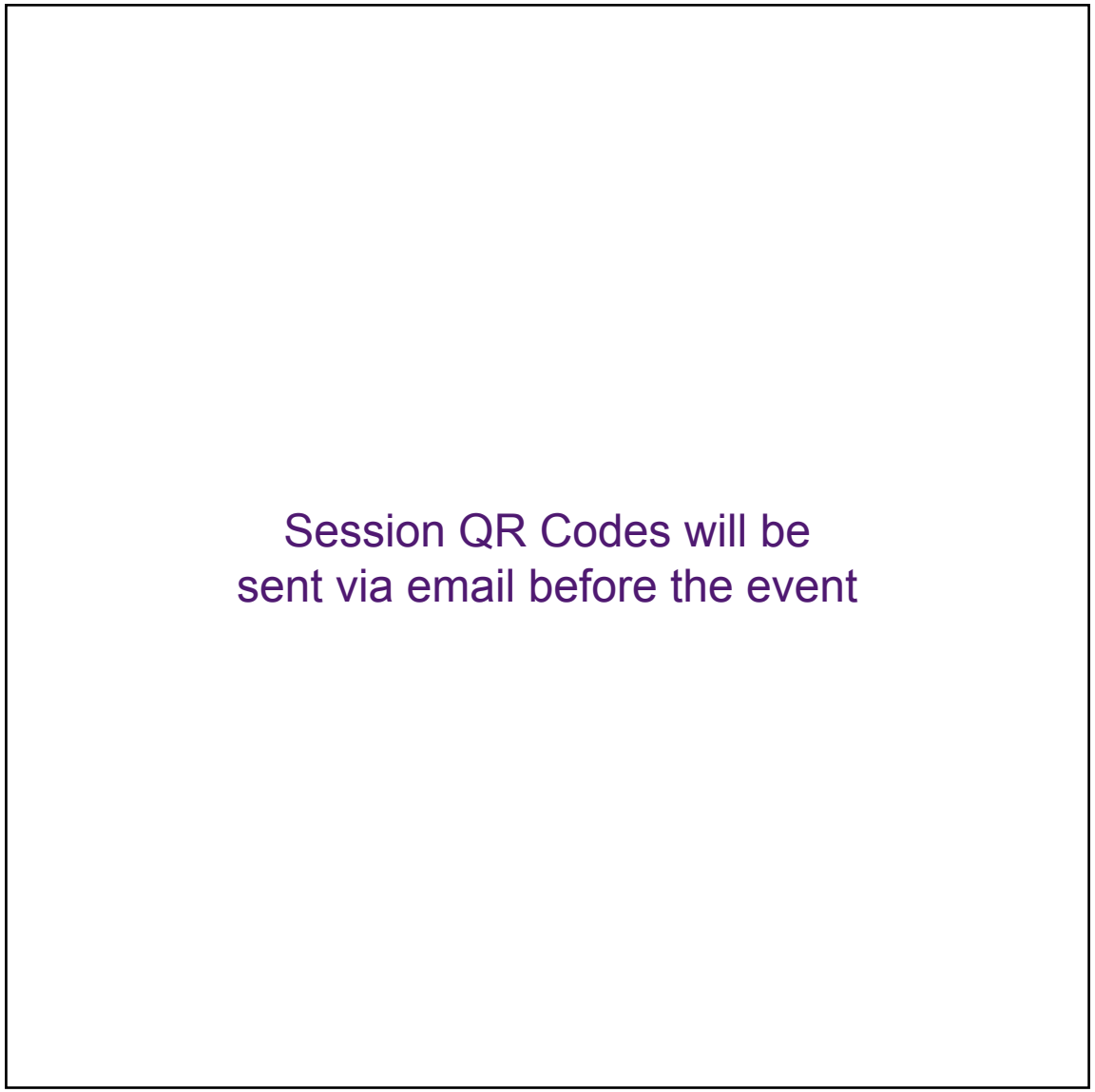

Backup

Sealed secrets

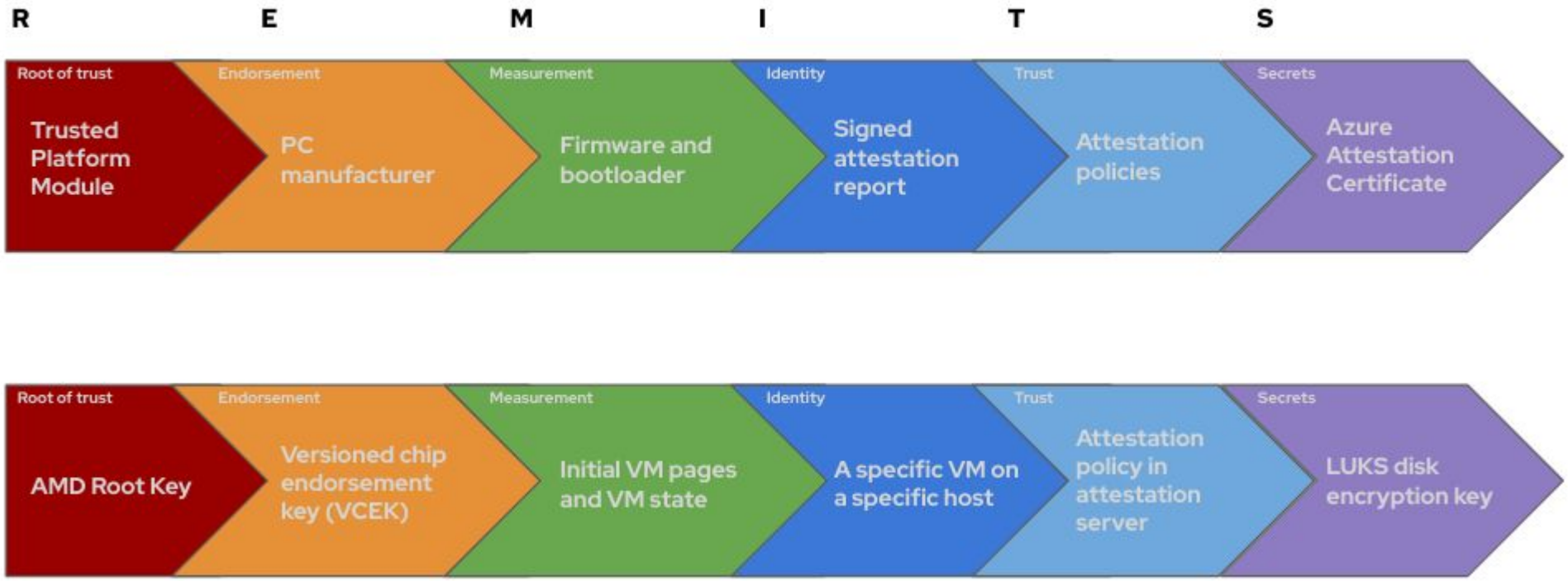
Interesting open issues

Guest identity: https://github.com/confidential-containers/guest-components/issues/340
Document threat vector profiles:
https://github.com/confidential-containers/confidential-containers/issues/118
Document trust model concepts:
https://github.com/confidential-containers/confidential-containers/issues/117
Securing the Kata Control Plane:
https://github.com/confidential-containers/confidential-containers/issues/53
[RFC] Proposal for Container Metadata Validation
https://github.com/confidential-containers/confidential-containers/issues/126

Presentation:
Kata agent policy status: https://github.com/confidential-containers/confidential-containers/issues/53
policy white paper: https://www.ibm.com/downloads/cas/GPVMWPM3



**Please scan the QR Code above
to leave feedback on this session**


R
E
M
I
T
S
Root of trust
Trusted Platform Module
Endorsement
PC manufacturer
Measurement
Firmware and bootloader
Identity
Signed attestation report
Trust
Attestation policies
Secrets
Azure Attestation Certificate
Root of trust
AMD Root Key
Endorsement
Versioned chip endorsement key (VCEK)
Measurement
Initial VM pages and VM state
Identity
A specific VM on a specific host
Trust
Attestation policy in attestation server
Secrets
LUKS disk encryption key