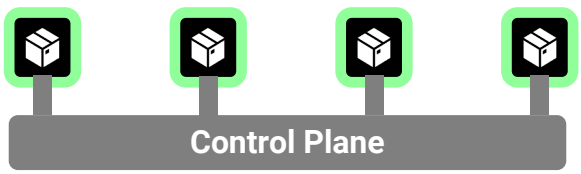
Confidential Kubernetes
Security Analysis

AKS / GKE + Confidential VMs

Concept

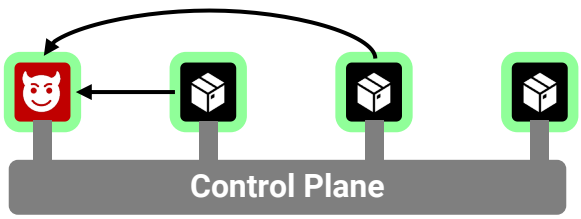


Only worker nodes run in Confidential VMs. The nodes are not verified. This only protects against direct access to node memory and cold boot attacks.

Attack #1: Compromised Control Plane

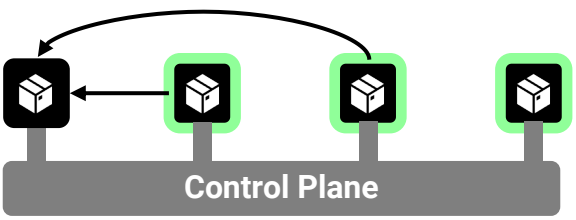
A compromised control plane has full control over worker nodes via *kubelet*.

Attack #2: Manipulated Node



A node running manipulated software receives data from other nodes. Node software can be manipulated at startup or through updates.

Attack #3: No Confidential VM



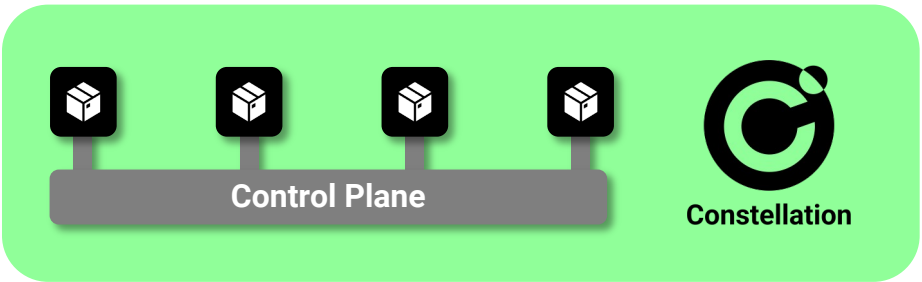
An unprotected node is added to the cluster. Data can be directly accessed through that node.

Many other possible attacks exist

- Manipulation of node parameters
- Interception of K8s admin connections
- Access to external key management
- ...

Constellation

Concept



The control plane and all worker nodes are protected with Confidential VMs. Constellation ensures the integrity of the entire deployment using remote attestation. Constellation ensures that all data is always encrypted – at rest, in transit, and during processing. Constellation transparently manages the corresponding cryptographic keys.

All attacks above are prevented by Constellation.