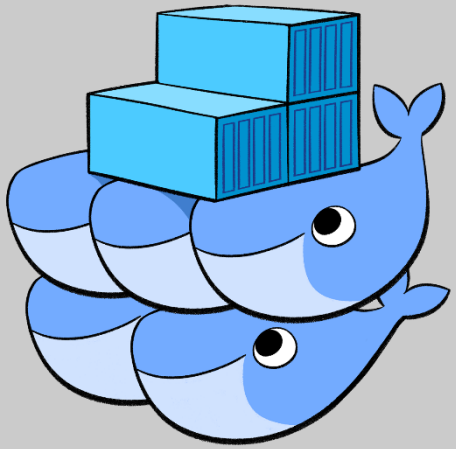
# Building a Secure Swarm


## Nigel Poulton

@nigelpoulton www.nigelpoulton.com

# Module Outline



- Big Picture
- Deeper Dive
- Build a Secure Swarm
- Orchestration
- Recap


Domain 1: Orchestration

- Complete the setup of a swarm mode cluster, with managers and worker nodes
- Demonstrate steps to lock a swarm cluster
- Paraphrase the importance of quorum in a swarm cluster

Domain 5 Security

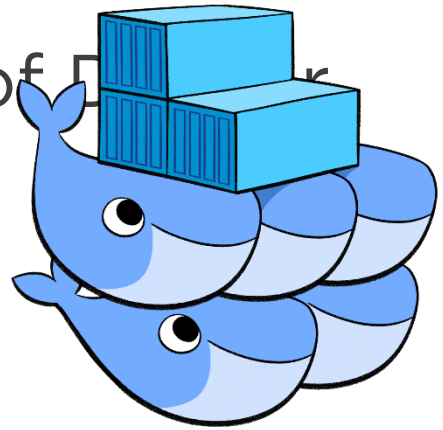
- Describe MTLS

# The Big Picture

Swarm, Swarm, Swarm. And a bit of Kubernetes.

# Swarm

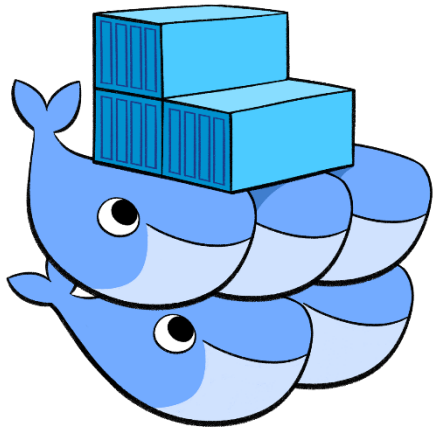
The future of D[illegible]r



VS

# Swarm

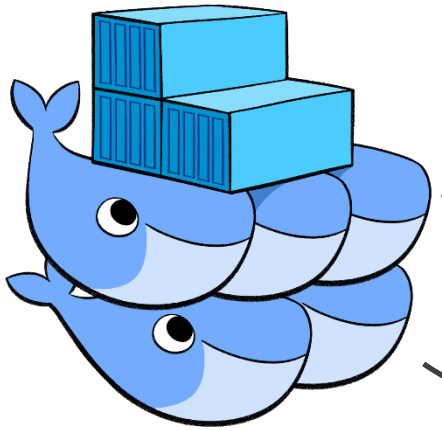
The future of Docker.

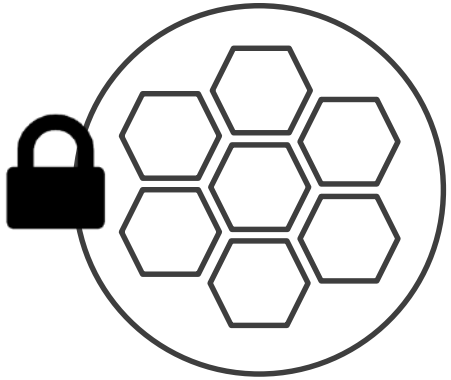


VS

# Swarm

The future of Docker.



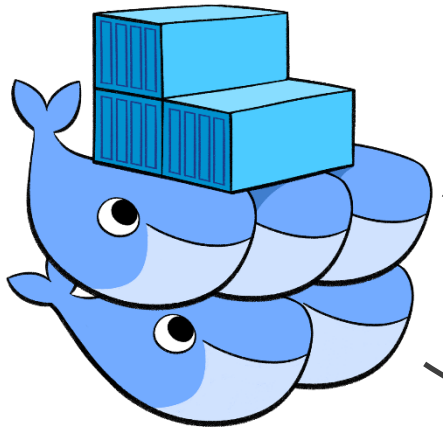


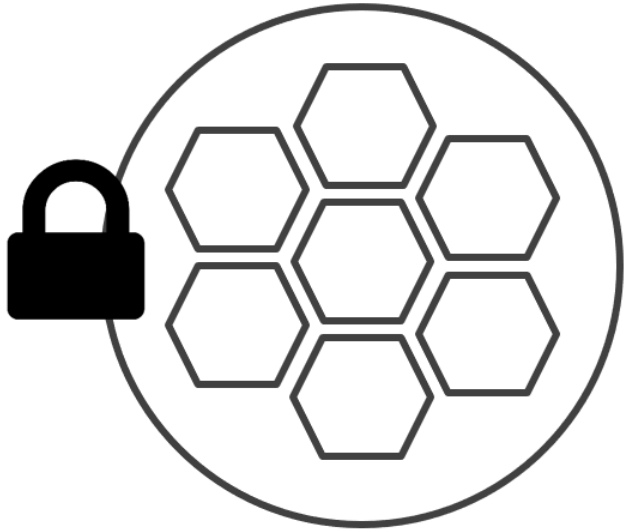
Secure cluster

Orchestrator

# Swarm

The future of Docker.





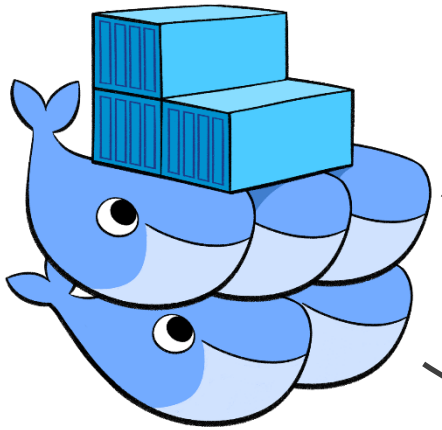
Secure cluster

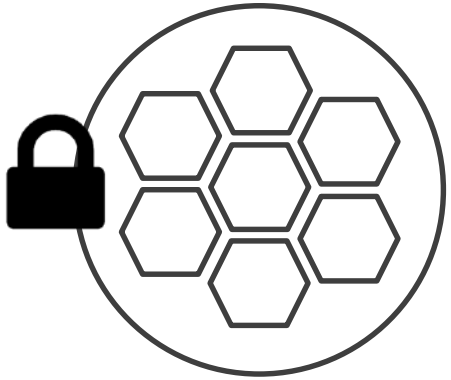
Orchestrator

# Swarm

## Secure Swarm cluster

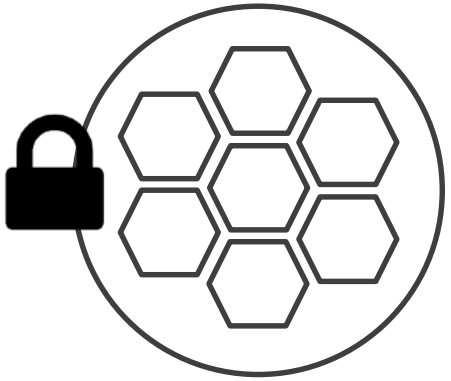
The future of Docker.



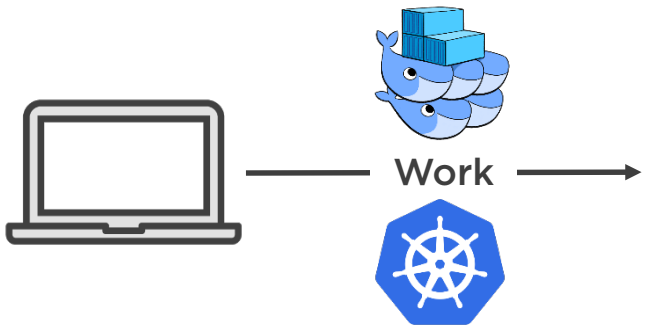


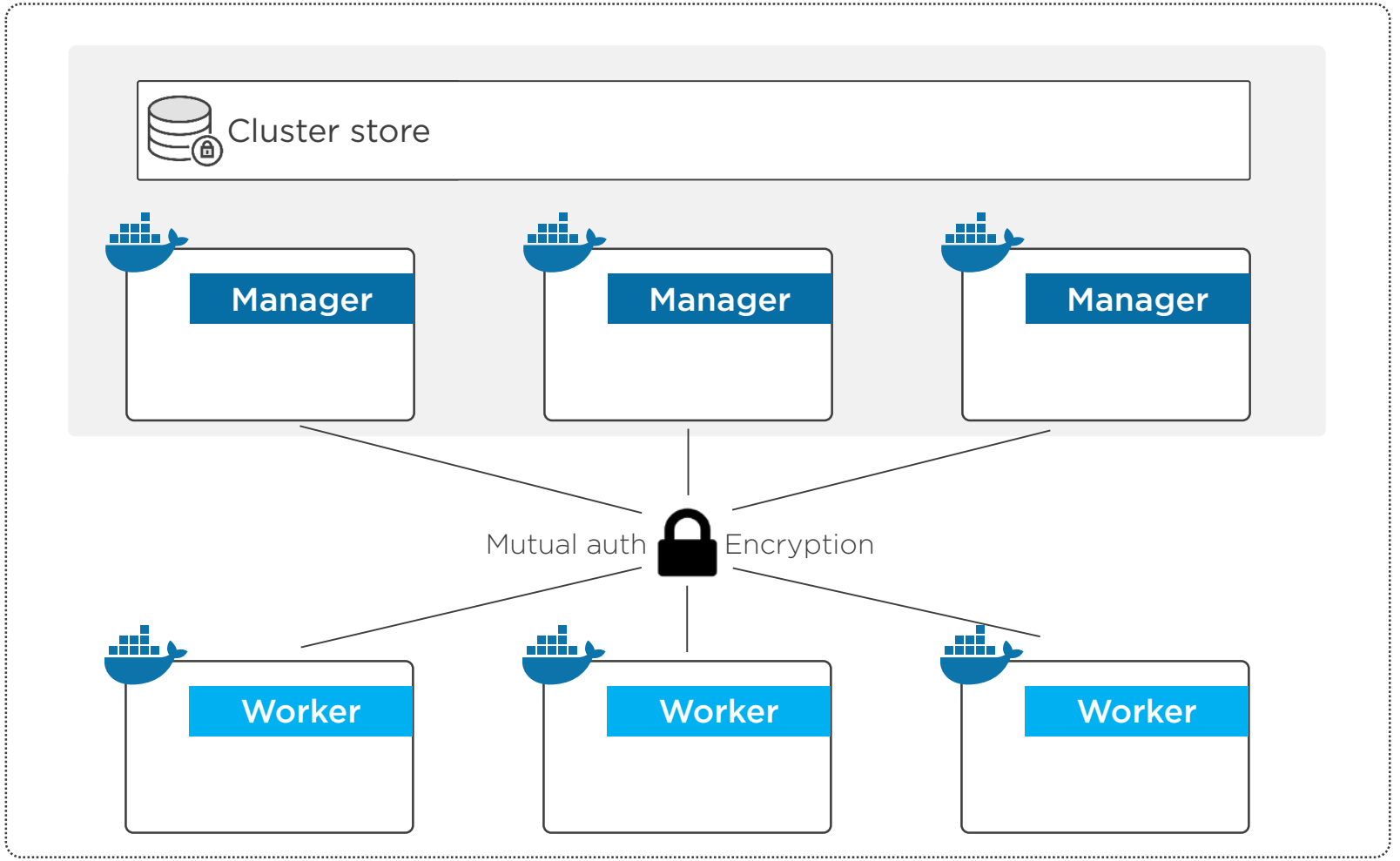
Secure cluster

Orchestrator



# Secure Swarm cluster



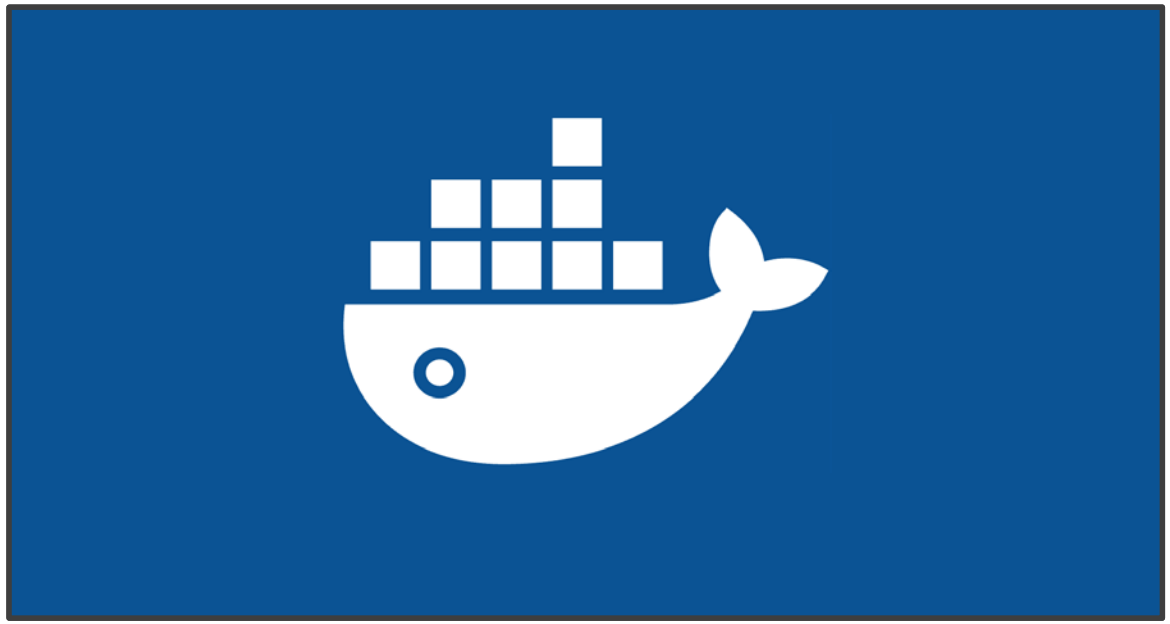



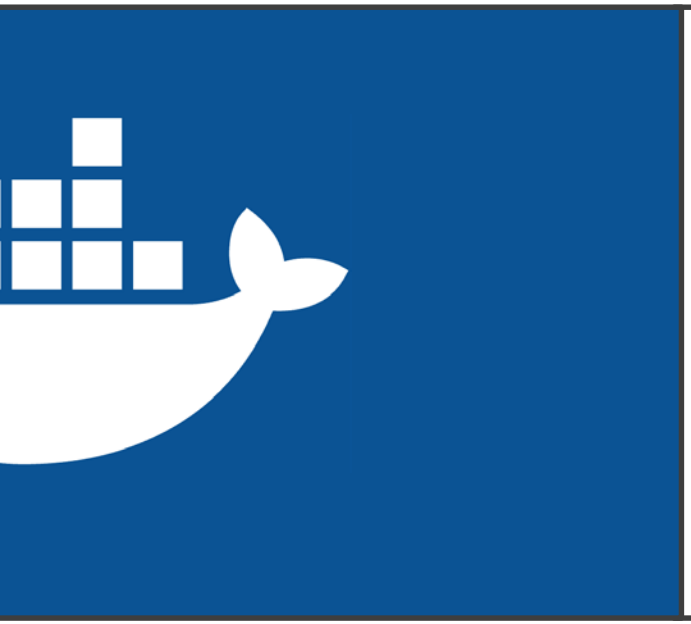
## Coming up

# Swarm Deep Dive

# Swarm Deep Dive

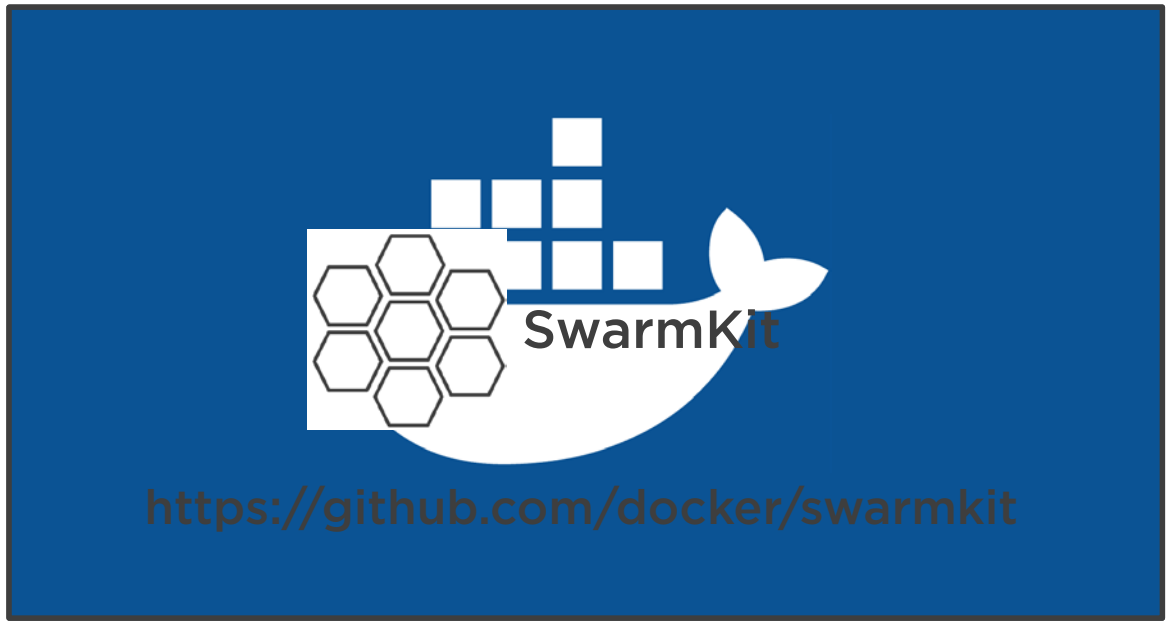
Secure out-of-the-box



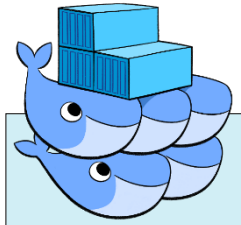


containerd

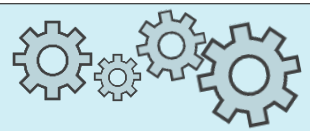
SwarmKit

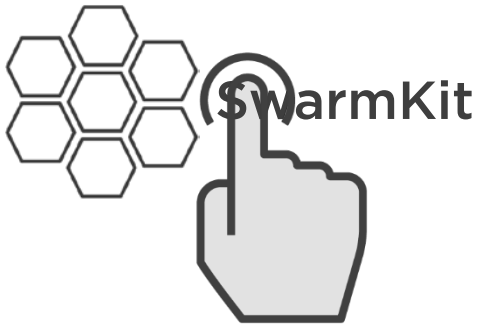

SwarmKit
https://github.com/docker/swarmkit





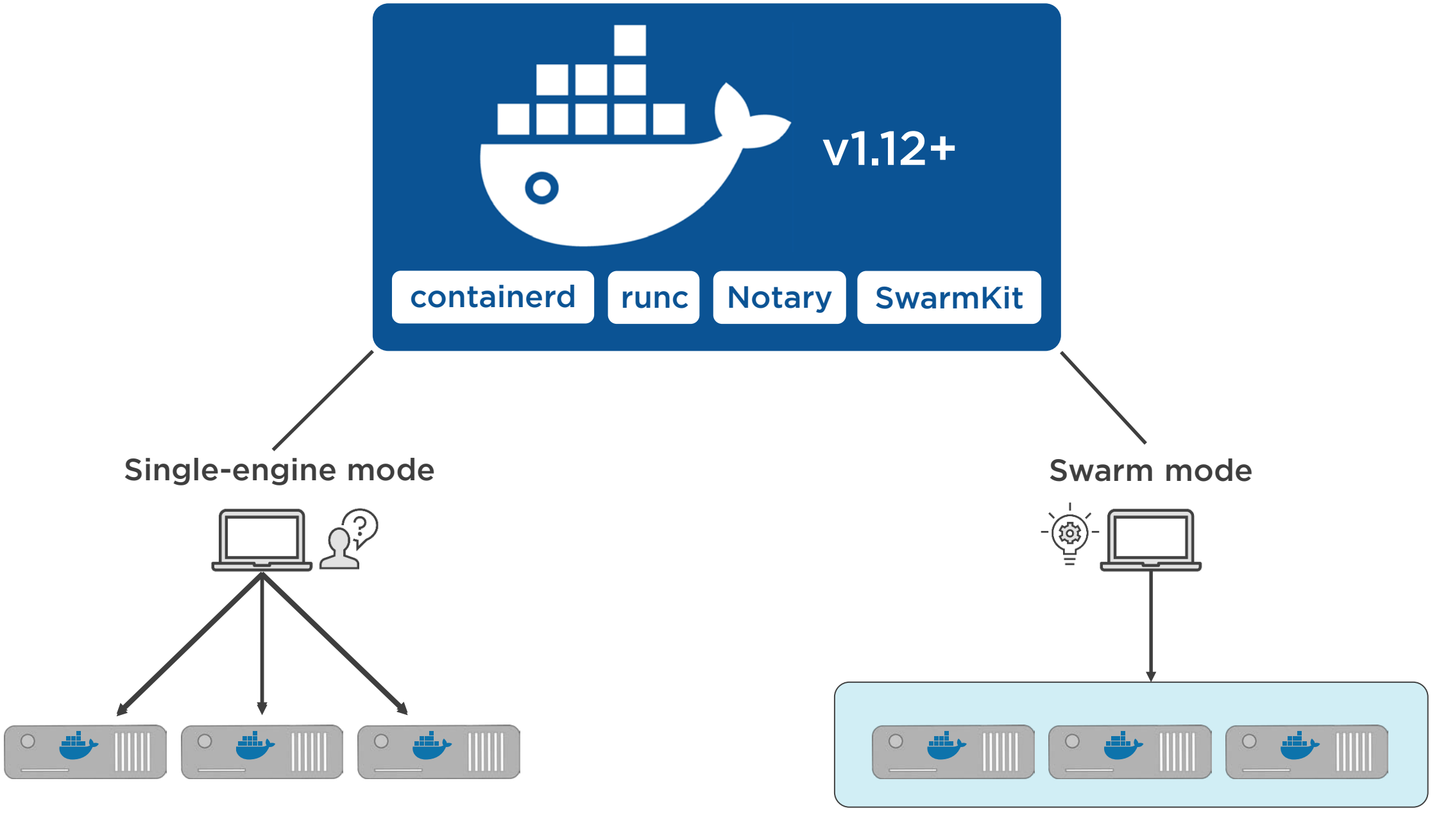
Classic Swarm

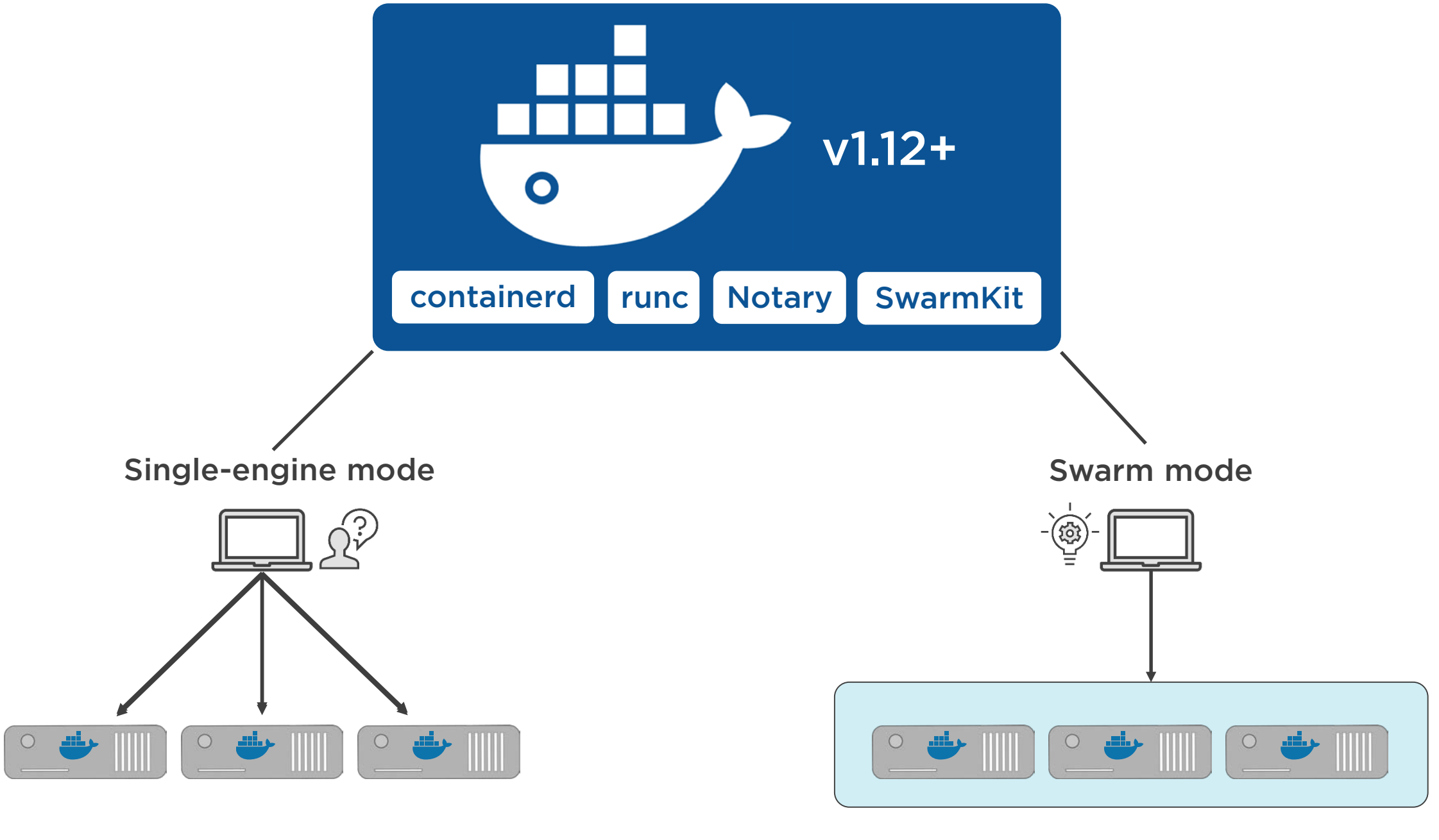


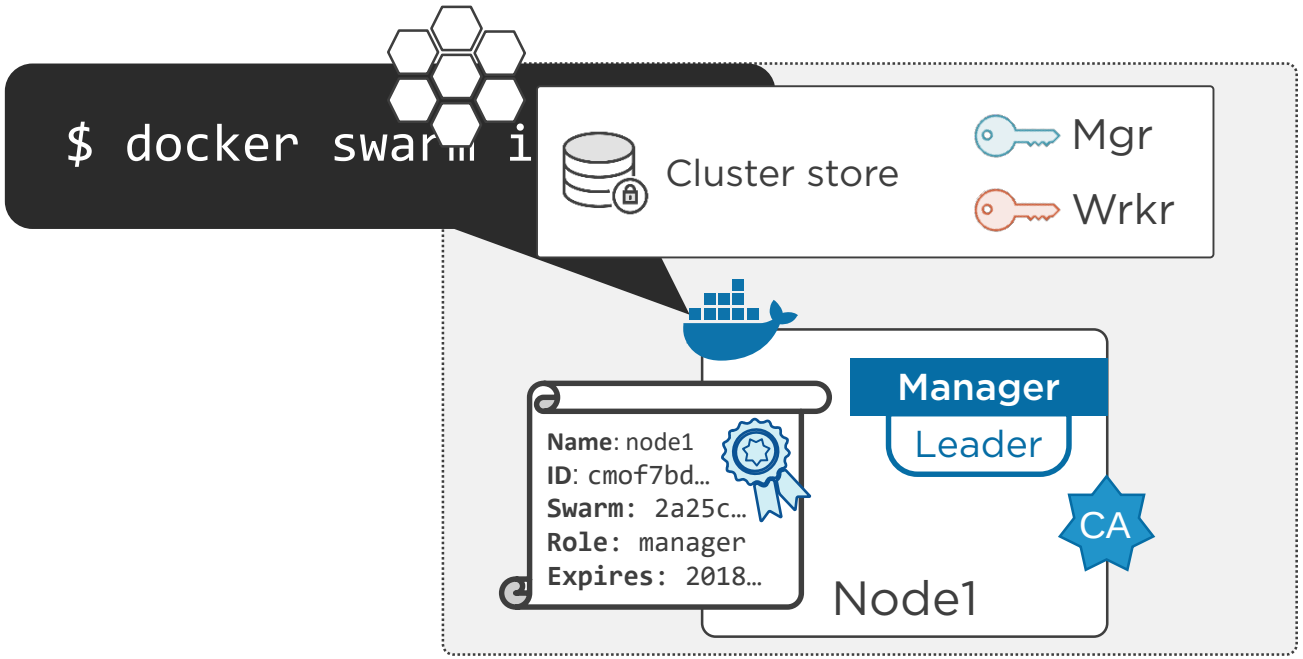

SwarmKit

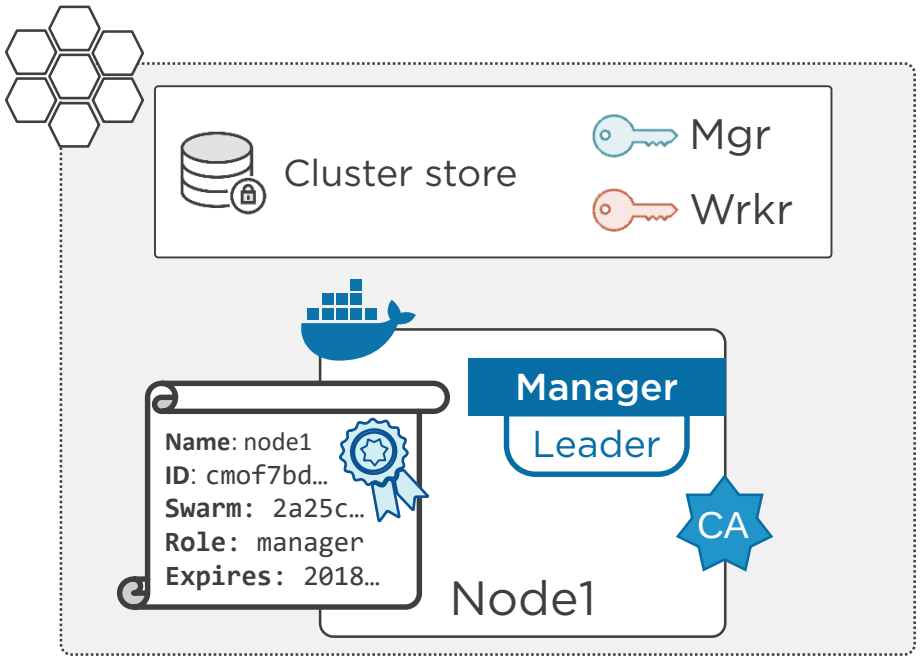

containerd

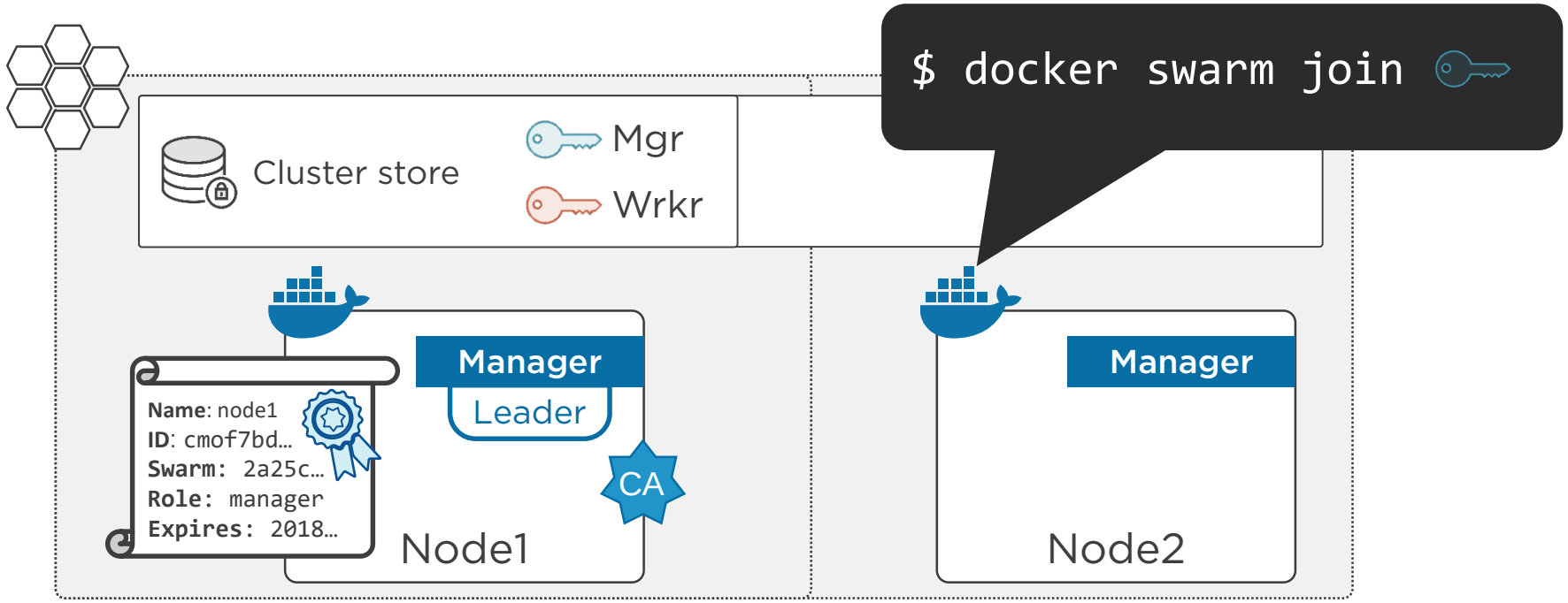

notary

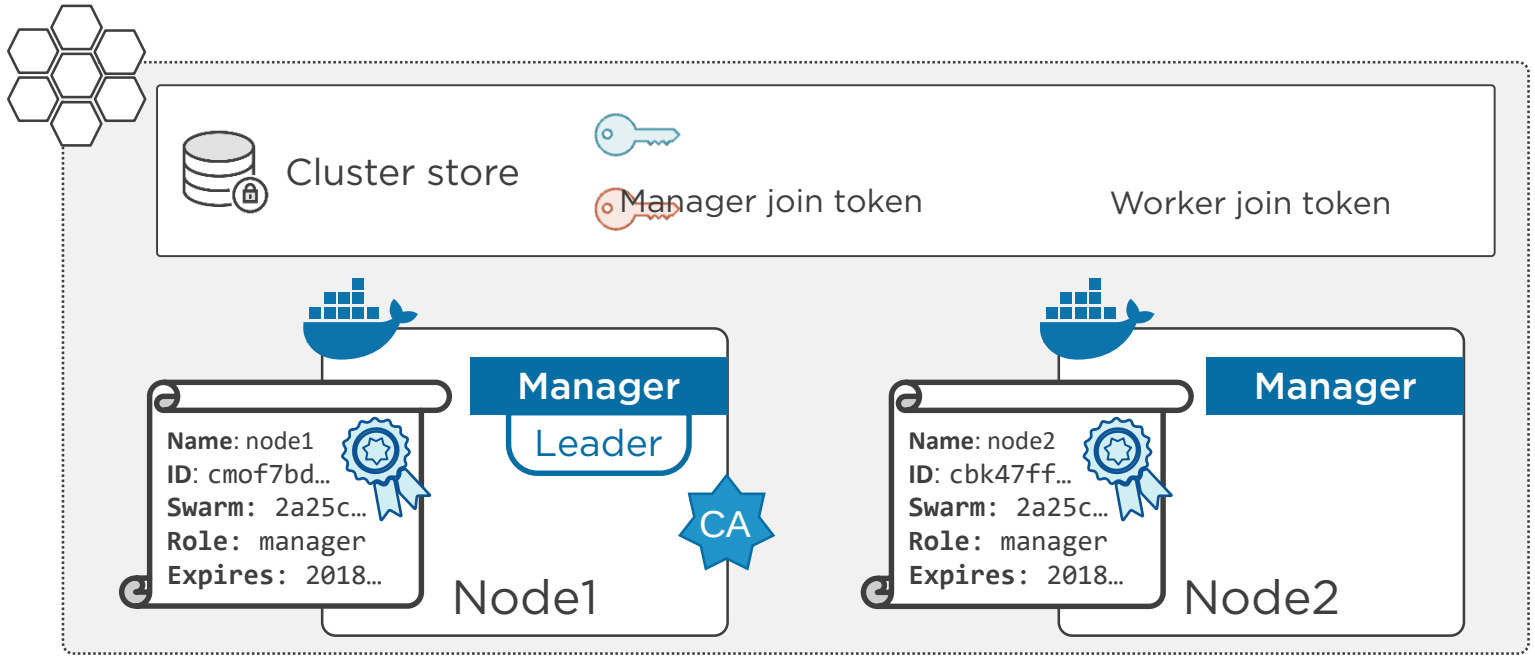

v1.12+
containerd
runc
Notary
SwarmKit
Single-engine mode
Swarm mode

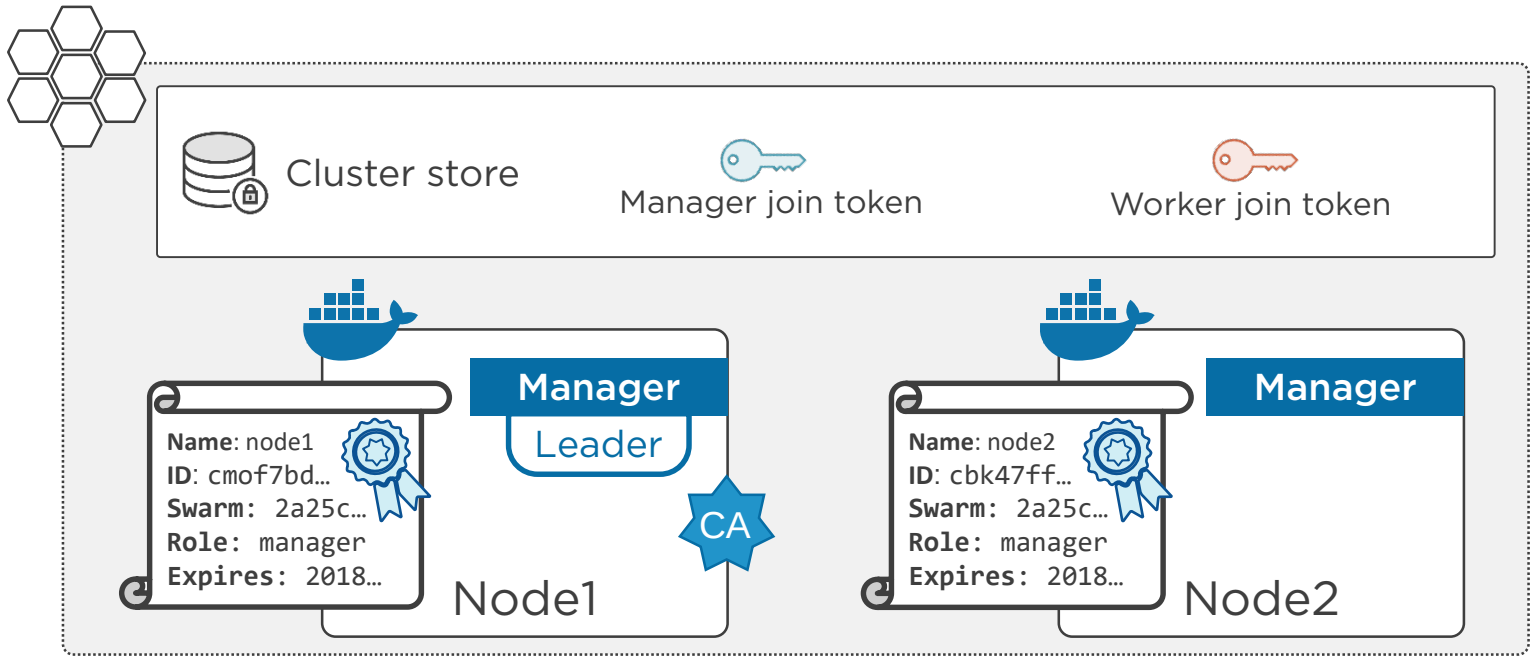

v1.12+
containerd
runc
Notary
SwarmKit
Single-engine mode
Swarm mode

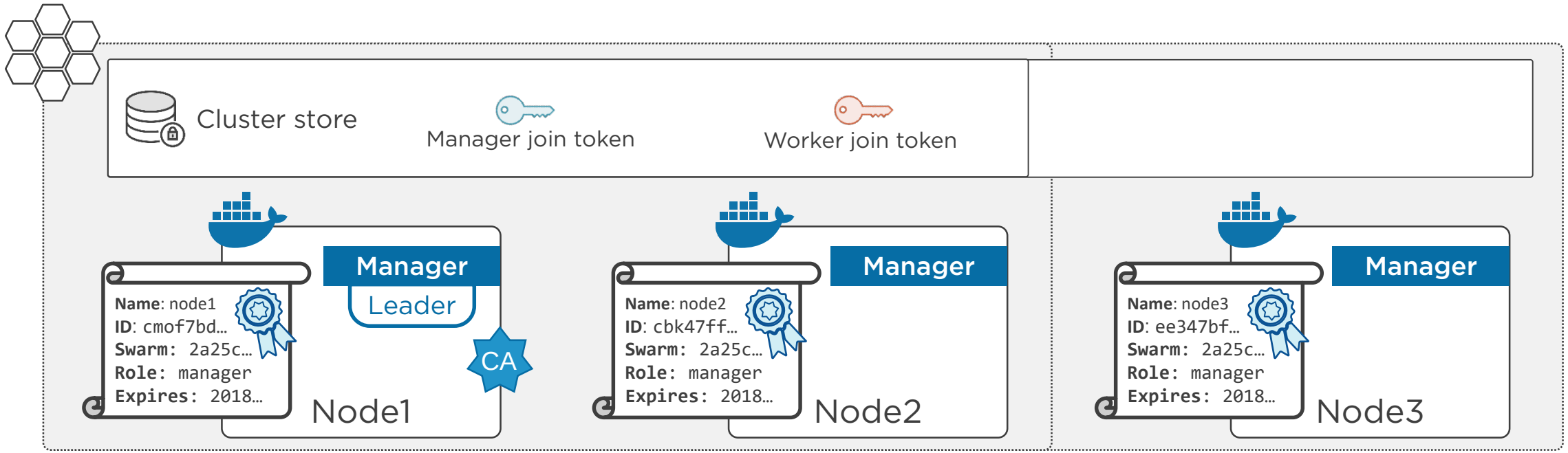

$ docker swarm i
Cluster store
Mgr
Wrkr
Manager
Leader
Name: node1
ID: cmof7bd…
Swarm: 2a25c…
Role: manager
Expires: 2018…
CA
Node1

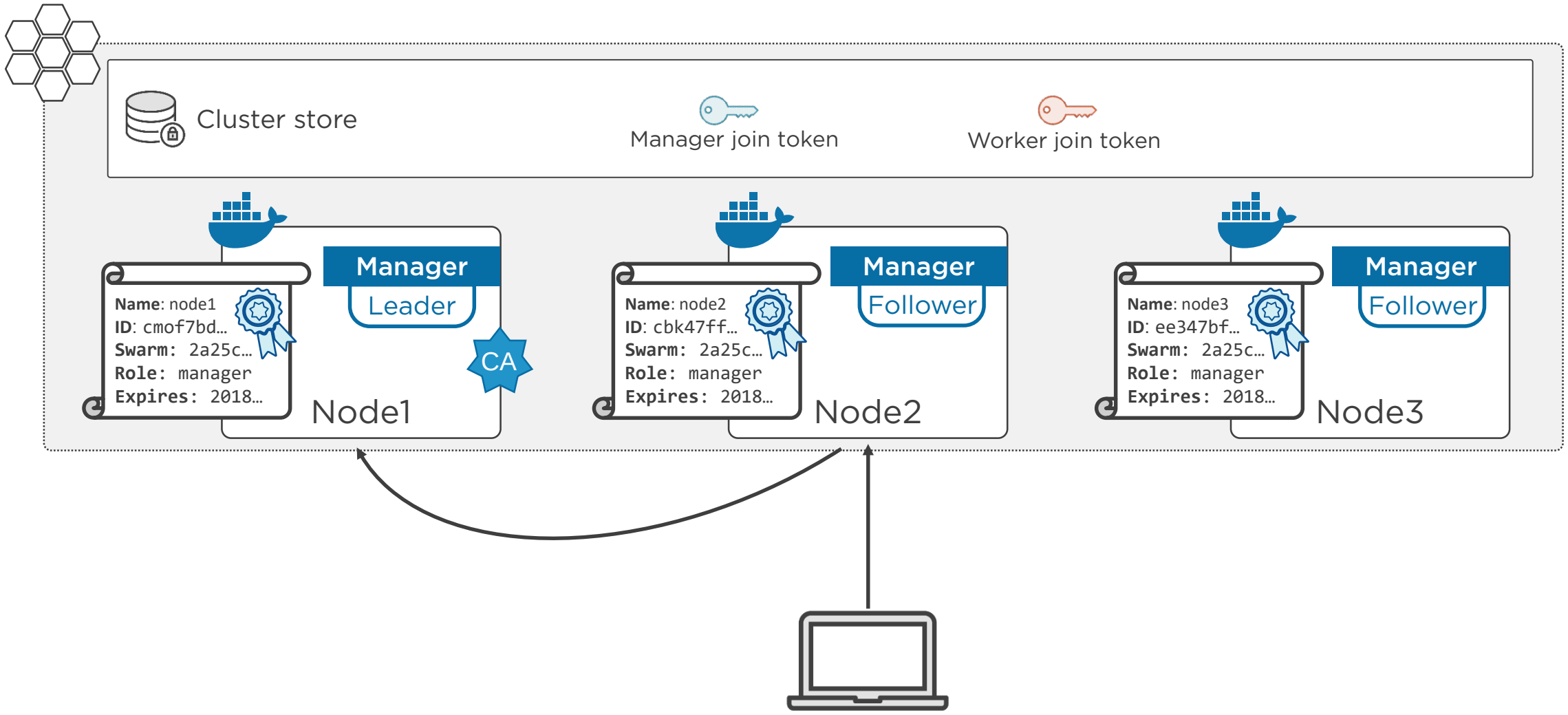

Cluster store
Mgr
Wrkr
Name: node1
ID: cmof7bd…
Swarm: 2a25c…
Role: manager
Expires: 2018…
Manager
Leader
CA
Node1

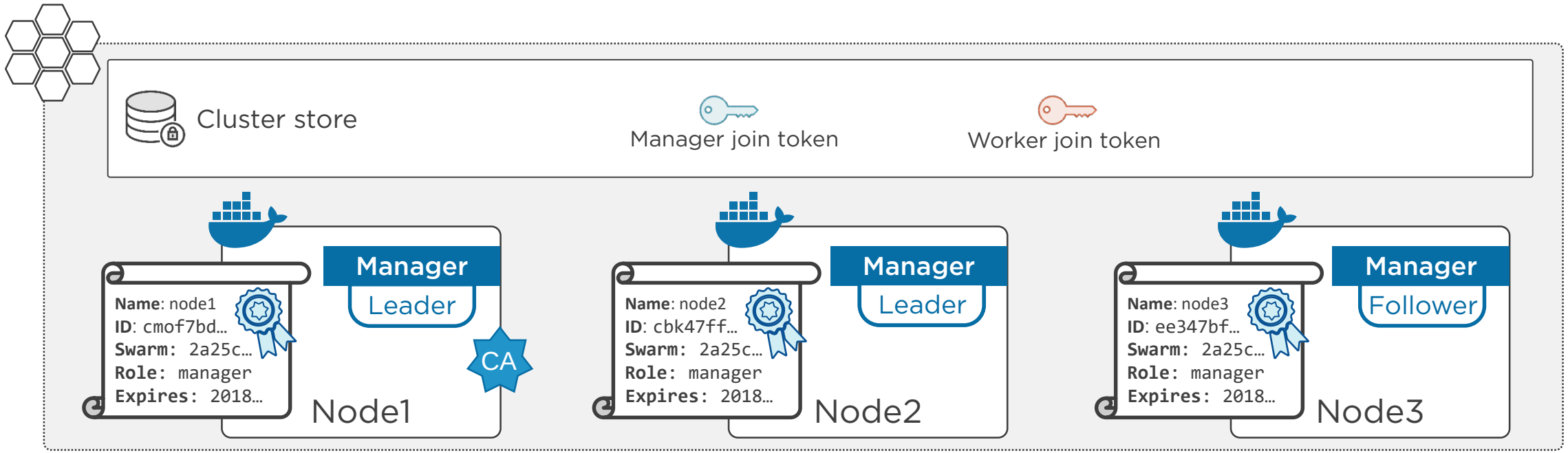

$ docker swarm join
Cluster store
Mgr
Wrkr
Name: node1
ID: cmof7bd...
Swarm: 2a25c...
Role: manager
Expires: 2018...
Manager
Leader
CA
Node1
Manager
Node2

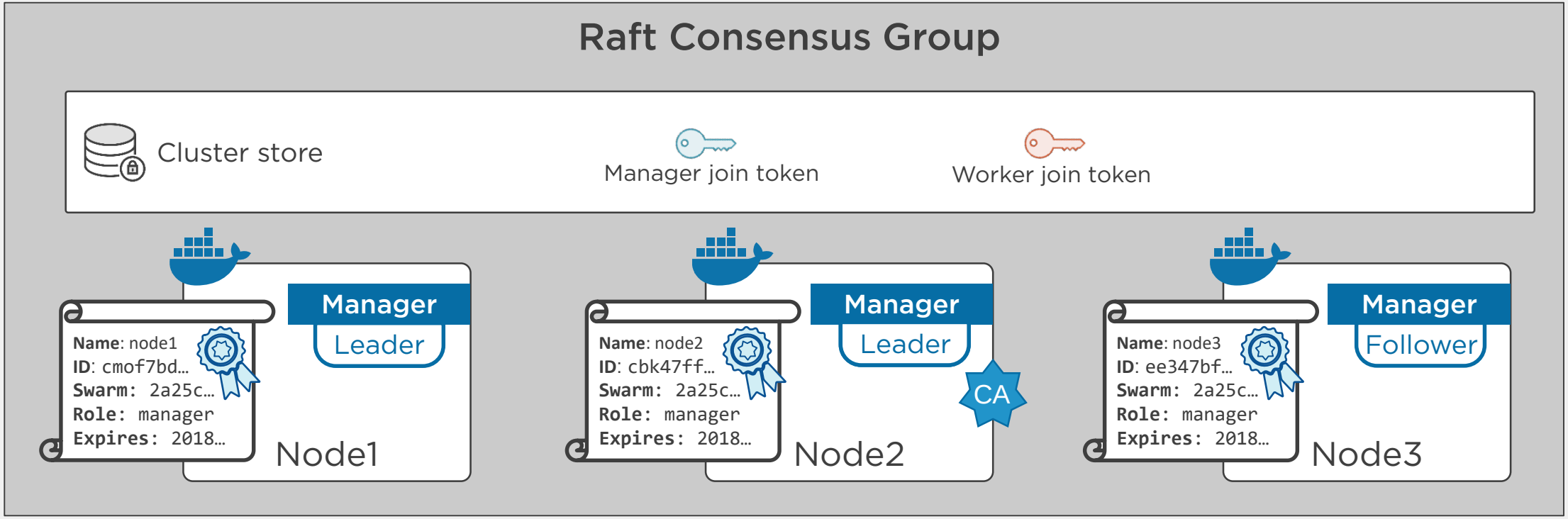

Cluster store
Manager join token
Worker join token
Manager
Leader
Name: node1
ID: cmof7bd...
Swarm: 2a25c...
Role: manager
Expires: 2018...
CA
Node1
Manager
Name: node2
ID: cbk47ff...
Swarm: 2a25c...
Role: manager
Expires: 2018...
Node2

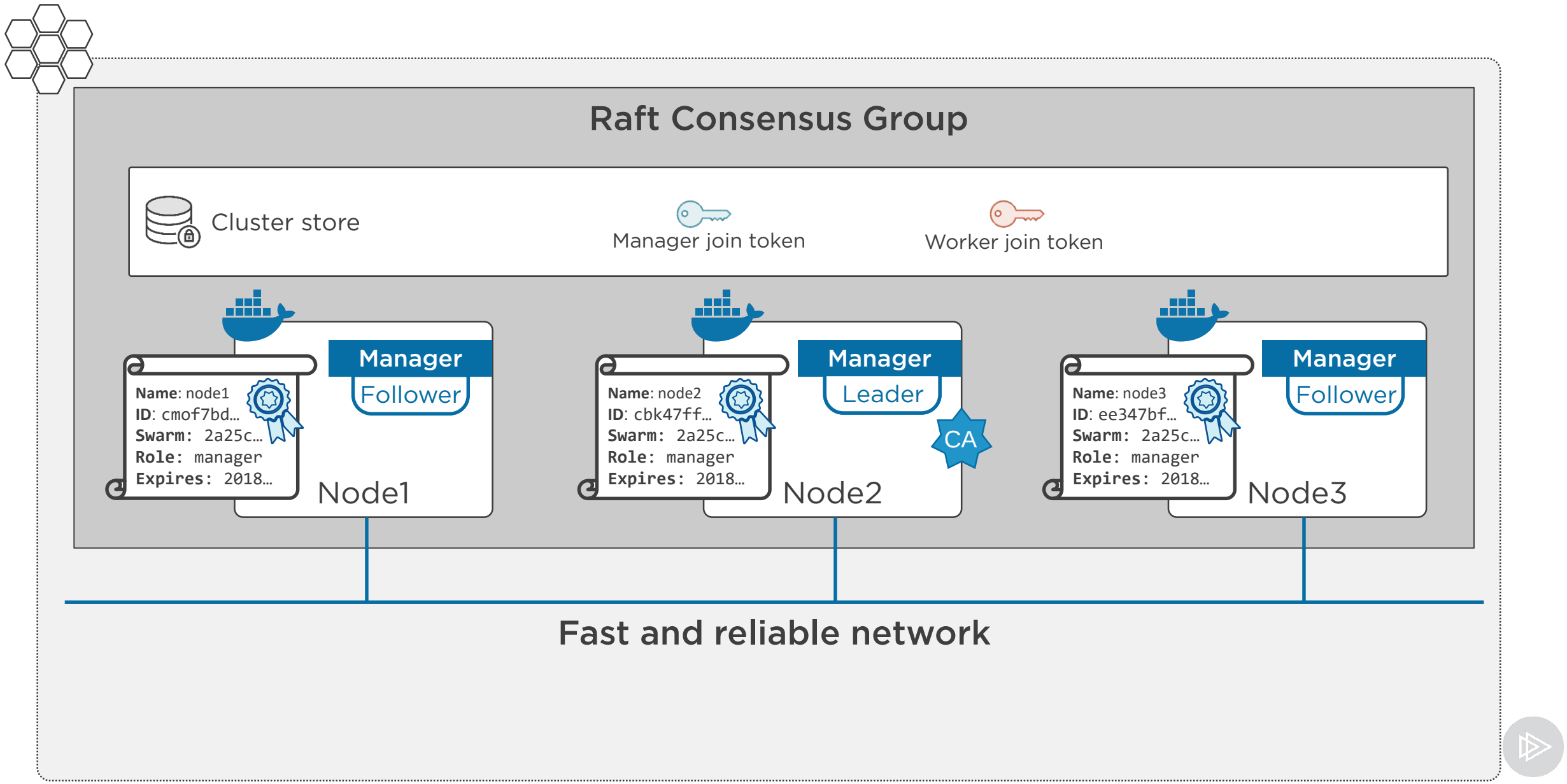

Cluster store
Manager join token
Worker join token
Manager
Leader
Name: node1
ID: cmof7bd…
Swarm: 2a25c…
Role: manager
Expires: 2018…
CA
Node1
Manager
Name: node2
ID: cbk47ff…
Swarm: 2a25c…
Role: manager
Expires: 2018…
Node2

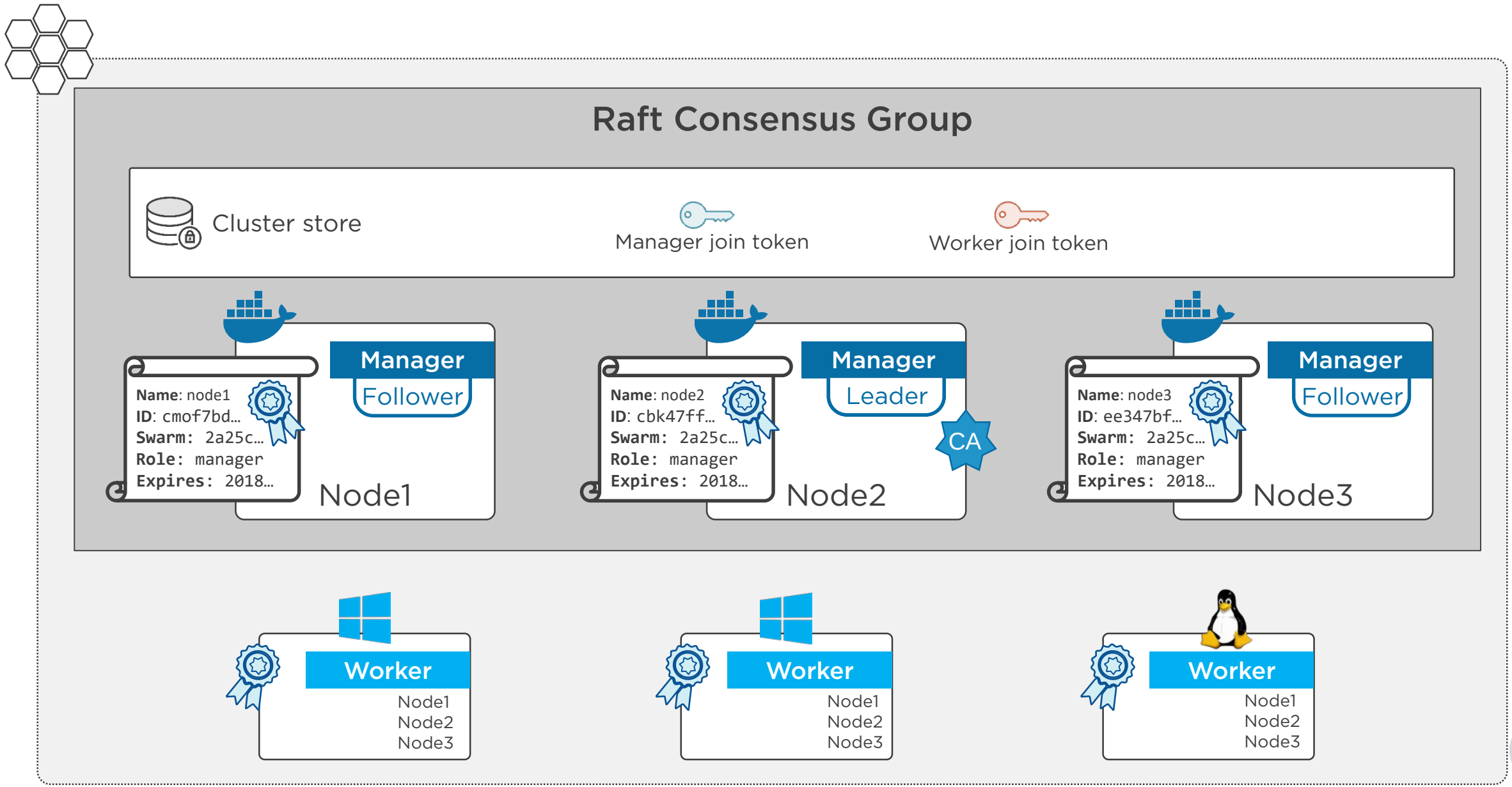

Cluster store
Manager join token
Worker join token
Manager
Leader
Name: node1
ID: cmof7bd...
Swarm: 2a25c...
Role: manager
Expires: 2018...
CA
Node1
Manager
Name: node2
ID: cbk47ff...
Swarm: 2a25c...
Role: manager
Expires: 2018...
Node2
Manager
Name: node3
ID: ee347bf...
Swarm: 2a25c...
Role: manager
Expires: 2018...
Node3


Cluster store
Manager join token
Worker join token
Manager
Leader
Name: node1
ID: cmof7bd...
Swarm: 2a25c...
Role: manager
Expires: 2018...
CA
Node1
Manager
Follower
Name: node2
ID: cbk47ff...
Swarm: 2a25c...
Role: manager
Expires: 2018...
Node2
Manager
Follower
Name: node3
ID: ee347bf...
Swarm: 2a25c...
Role: manager
Expires: 2018...
Node3


Cluster store
Manager join token
Worker join token
Manager
Leader
Name: node1
ID: cmof7bd…
Swarm: 2a25c…
Role: manager
Expires: 2018…
CA
Node1
Manager
Leader
Name: node2
ID: cbk47ff…
Swarm: 2a25c…
Role: manager
Expires: 2018…
Node2
Manager
Follower
Name: node3
ID: ee347bf…
Swarm: 2a25c…
Role: manager
Expires: 2018…
Node3


Raft Consensus Group
Cluster store
Manager join token
Worker join token
Manager
Leader
Name: node1
ID: cmof7bd...
Swarm: 2a25c...
Role: manager
Expires: 2018...
Node1
Manager
Leader
CA
Name: node2
ID: cbk47ff...
Swarm: 2a25c...
Role: manager
Expires: 2018...
Node2
Manager
Follower
Name: node3
ID: ee347bf...
Swarm: 2a25c...
Role: manager
Expires: 2018...
Node3


Raft Consensus Group
Cluster store
Manager join token
Worker join token
Manager
Follower
Name: node1
ID: cmof7bd...
Swarm: 2a25c...
Role: manager
Expires: 2018...
Node1
Manager
Leader
CA
Name: node2
ID: cbk47ff...
Swarm: 2a25c...
Role: manager
Expires: 2018...
Node2
Manager
Follower
Name: node3
ID: ee347bf...
Swarm: 2a25c...
Role: manager
Expires: 2018...
Node3
Fast and reliable network


Raft Consensus Group
Cluster store
Manager join token
Worker join token
Manager
Follower
Name: node1
ID: cmof7bd…
Swarm: 2a25c…
Role: manager
Expires: 2018…
Node1
Manager
Leader
CA
Name: node2
ID: cbk47ff…
Swarm: 2a25c…
Role: manager
Expires: 2018…
Node2
Manager
Follower
Name: node3
ID: ee347bf…
Swarm: 2a25c…
Role: manager
Expires: 2018…
Node3
Worker
Node1
Node2
Node3
Worker
Node1
Node2
Node3
Worker
Node1
Node2
Node3

## Coming up

# Building a Secure Swarm

# Building a Secure Swarm

Certificates, join-tokens, rotation policies, more....

# Create a Swarm (anywhere)

- Create a Swarm manager
  - Assign it a crypto ID
  - Elect it as the Swarm leader
- Create an Swarm config DB
  - Encrypt it
  - Configure it to automatically replicate with all Swarm managers
- Create a Swarm join token for new workers
- Create a Swarm join token for new manager
- Configure a new Root CA on the leader
  - Configure a 90 day certificate rotation period

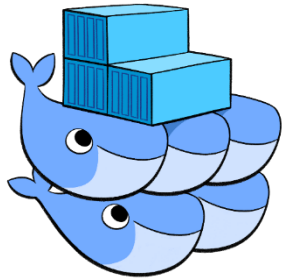
## Coming up

# Orchestration

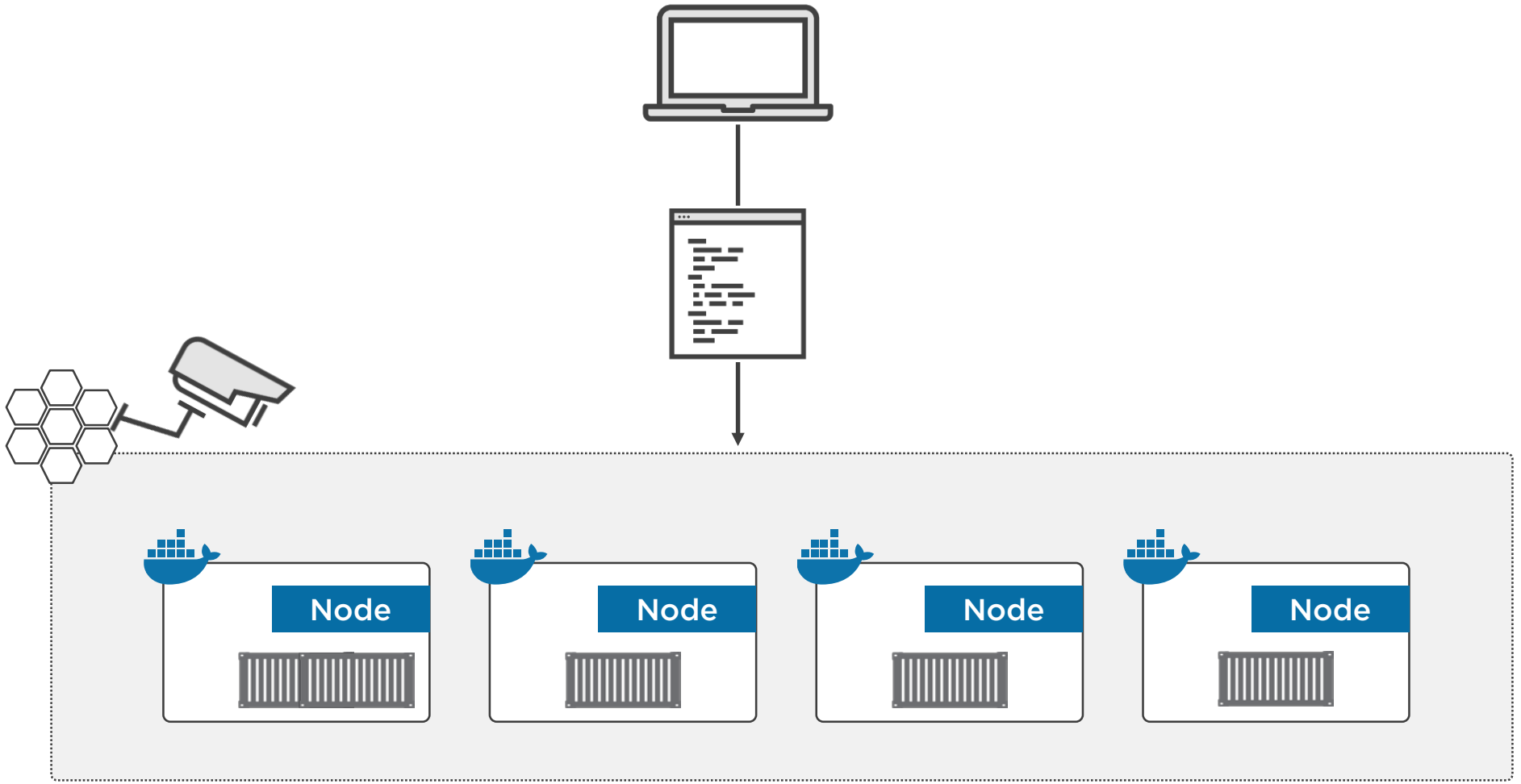
# Orchestration

Pulling the strings

# Operating at scale is hard!



Here to help!

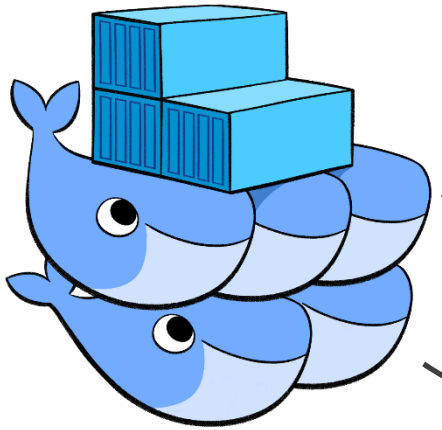

Node
Node
Node
Node

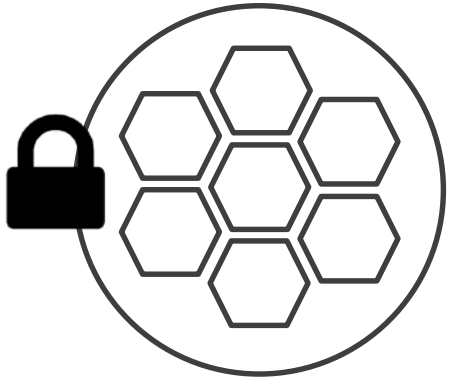
Coming up

Recap

# Recap

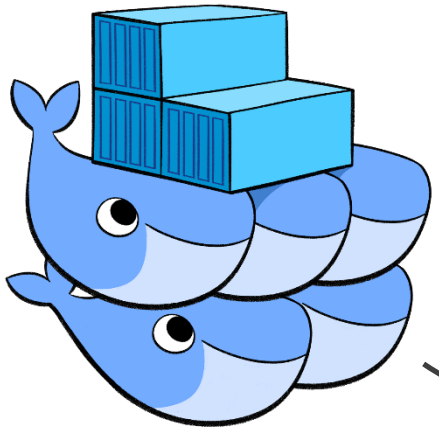
Time for a bit of déjà vu

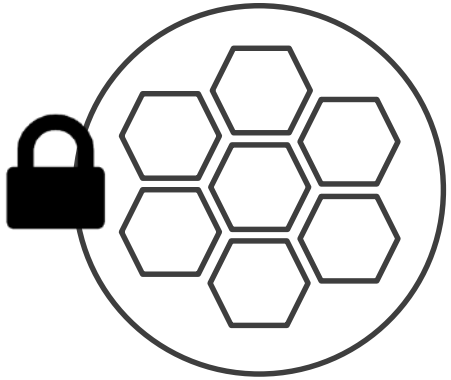




Secure cluster

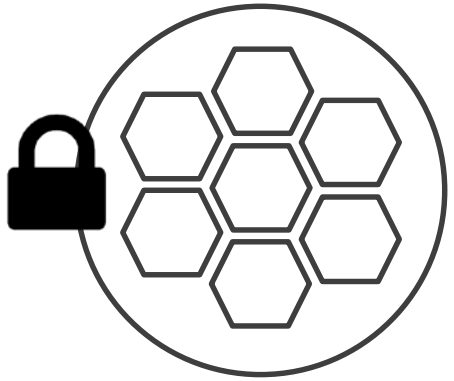
Orchestrator





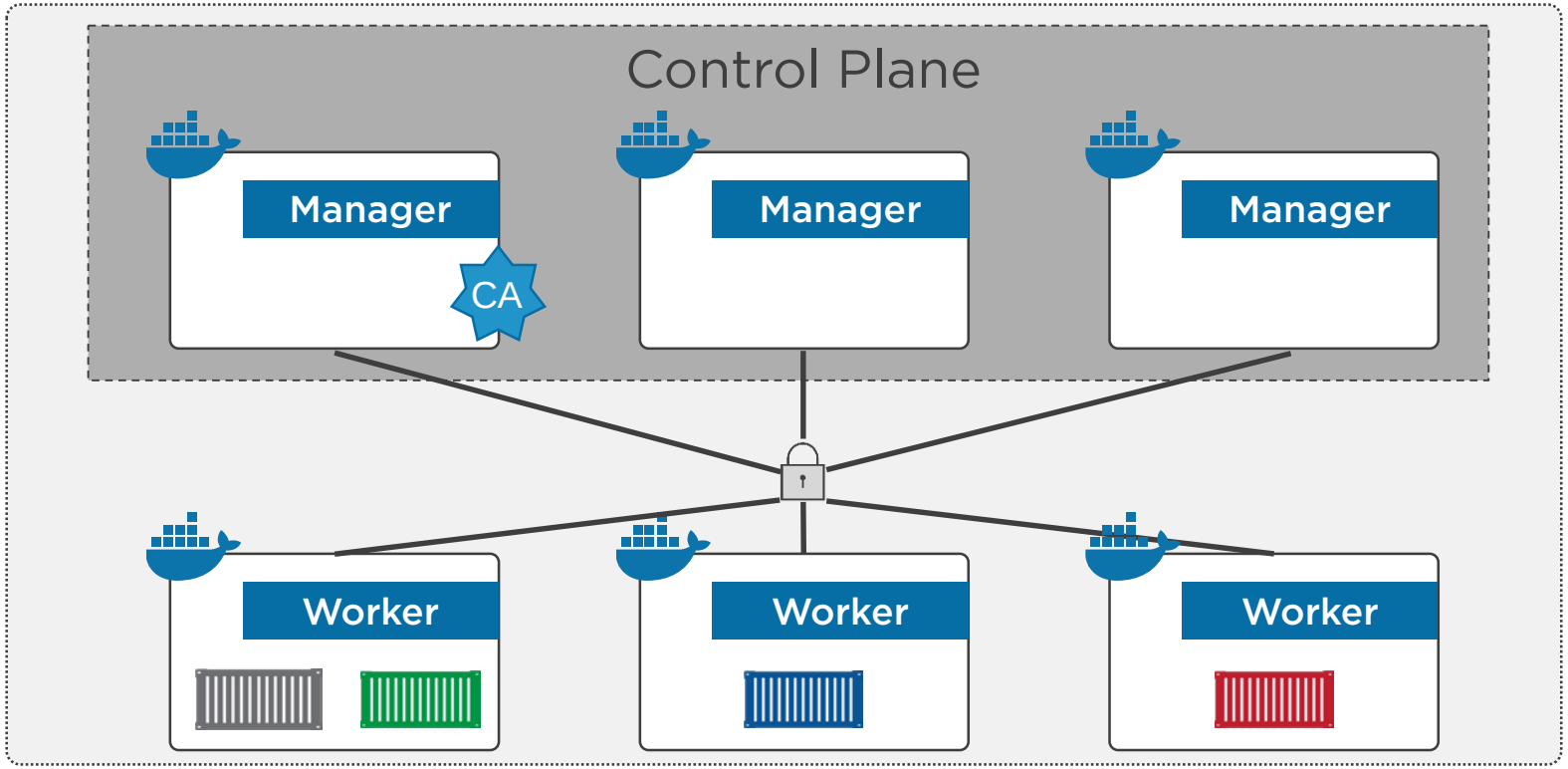
Secure Swarm cluster

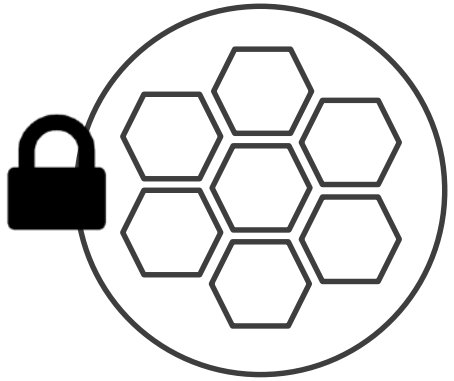
Orchestrator



# Secure Swarm cluster

```
$ docker swarm init
```

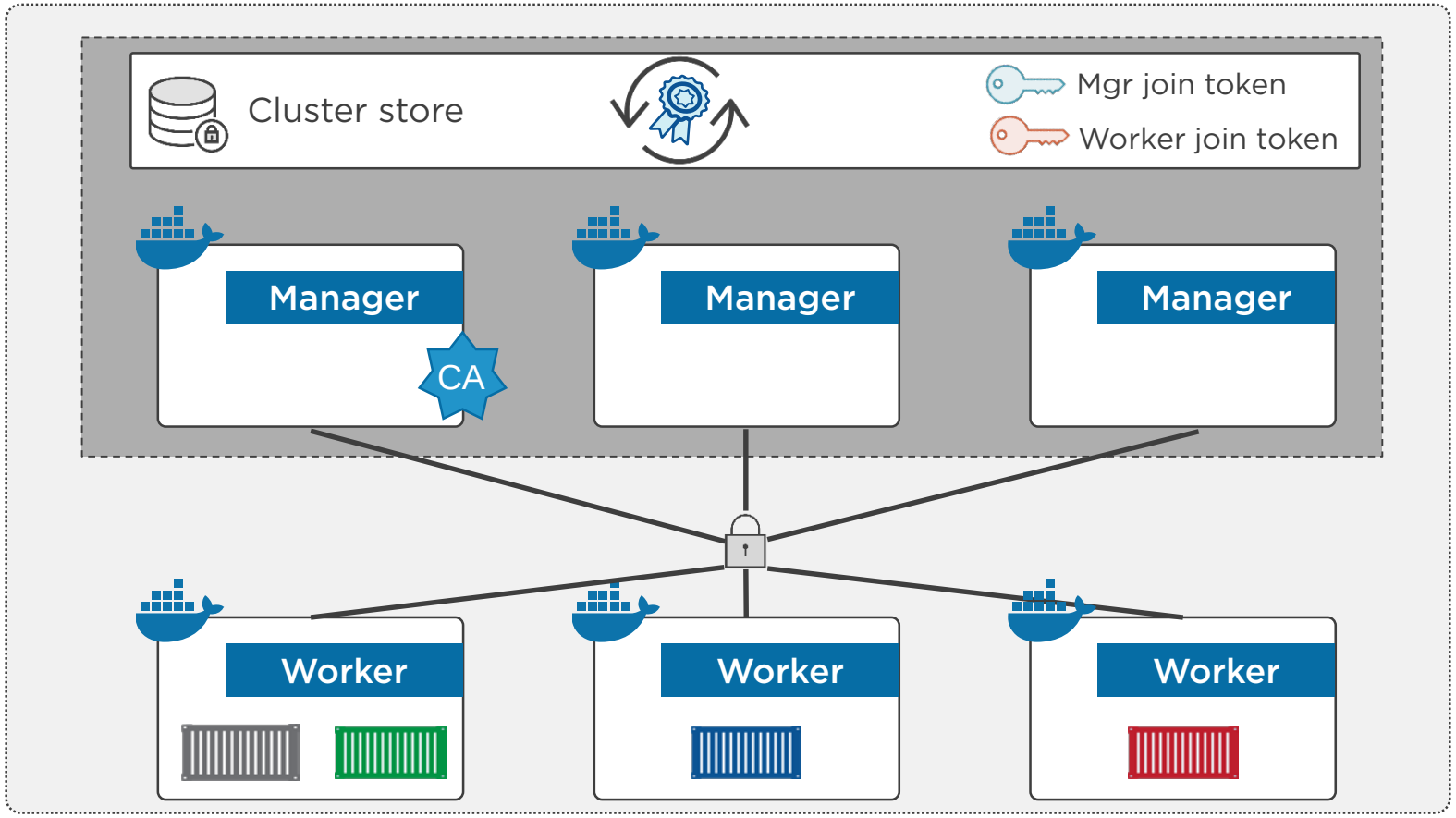




# Secure Swarm cluster

```
$ docker swarm init

$ docker swarm join
```



# Coming up

NEXT MODULE

# Container Networking