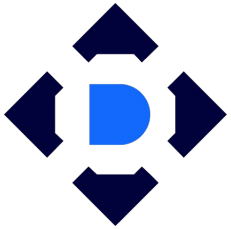
Istio

Multicluster

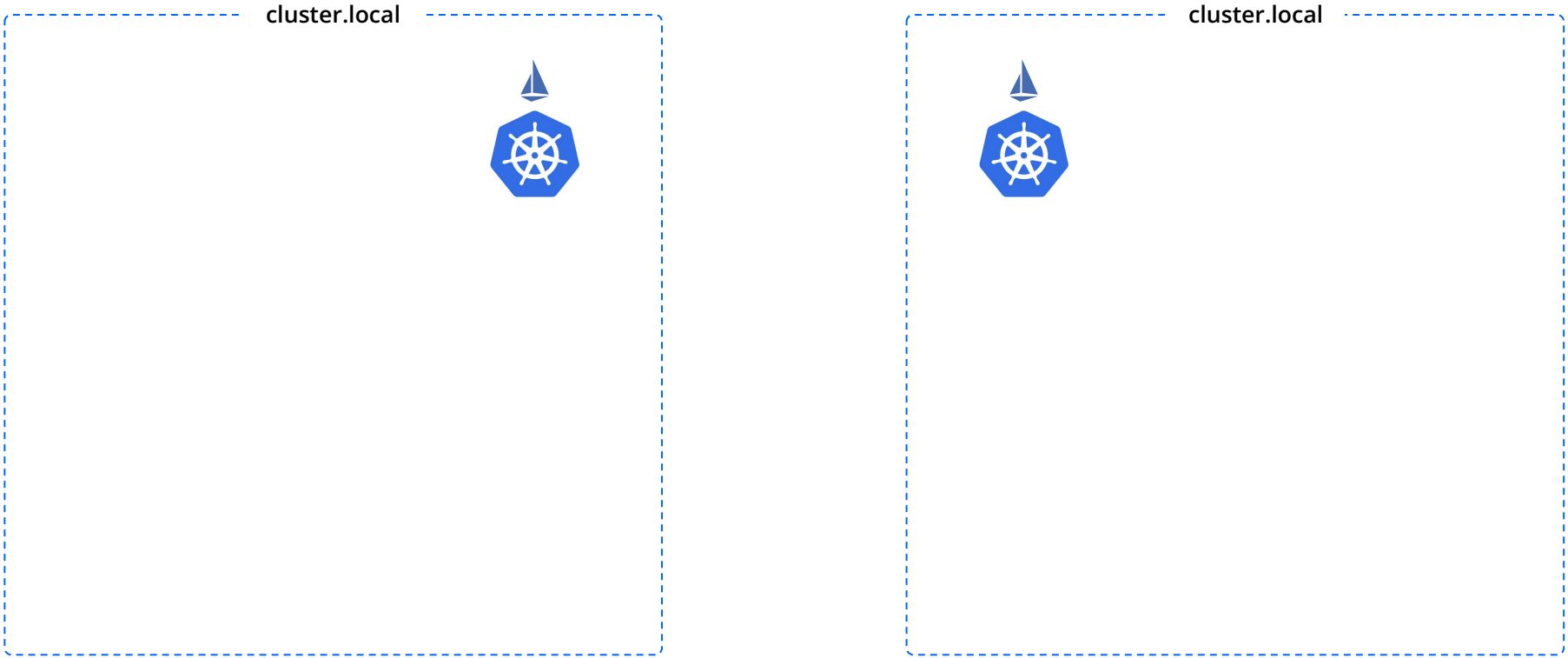
Common principles



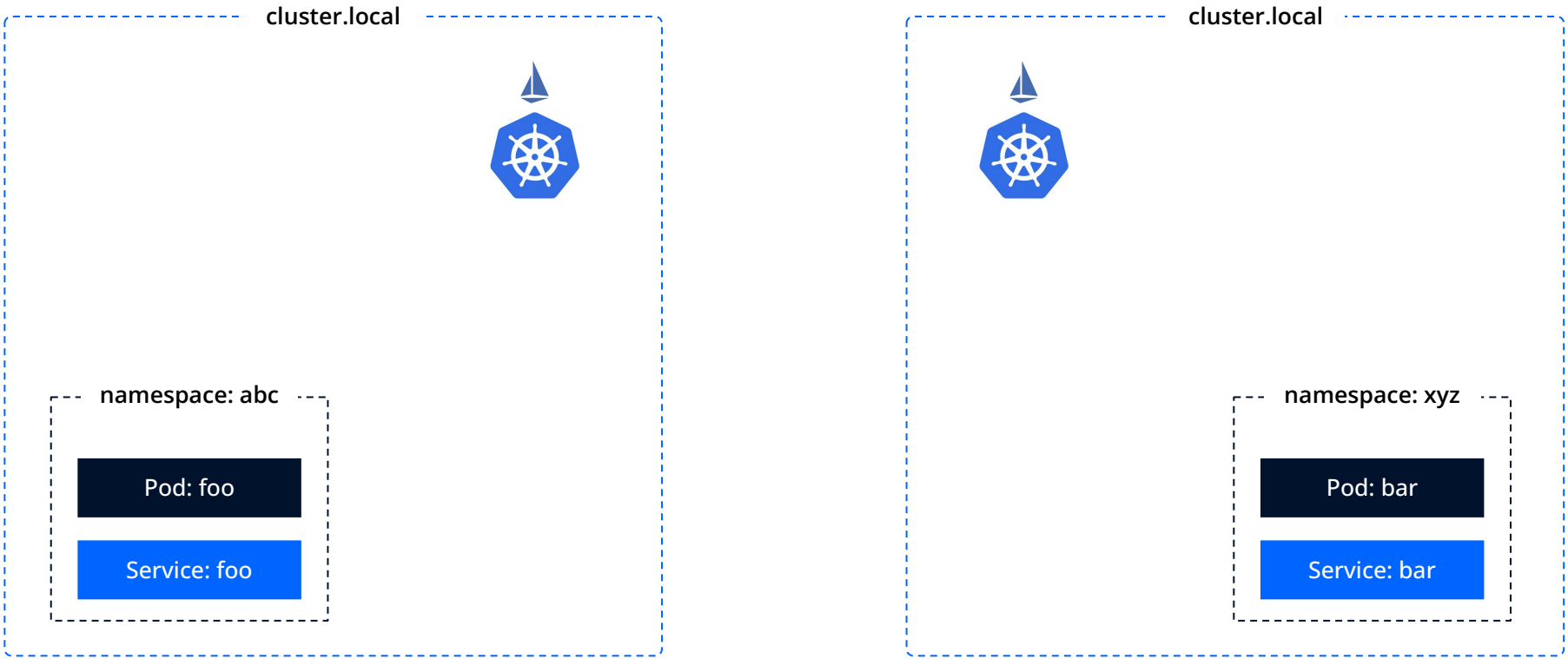
FLANT

Deckhouse

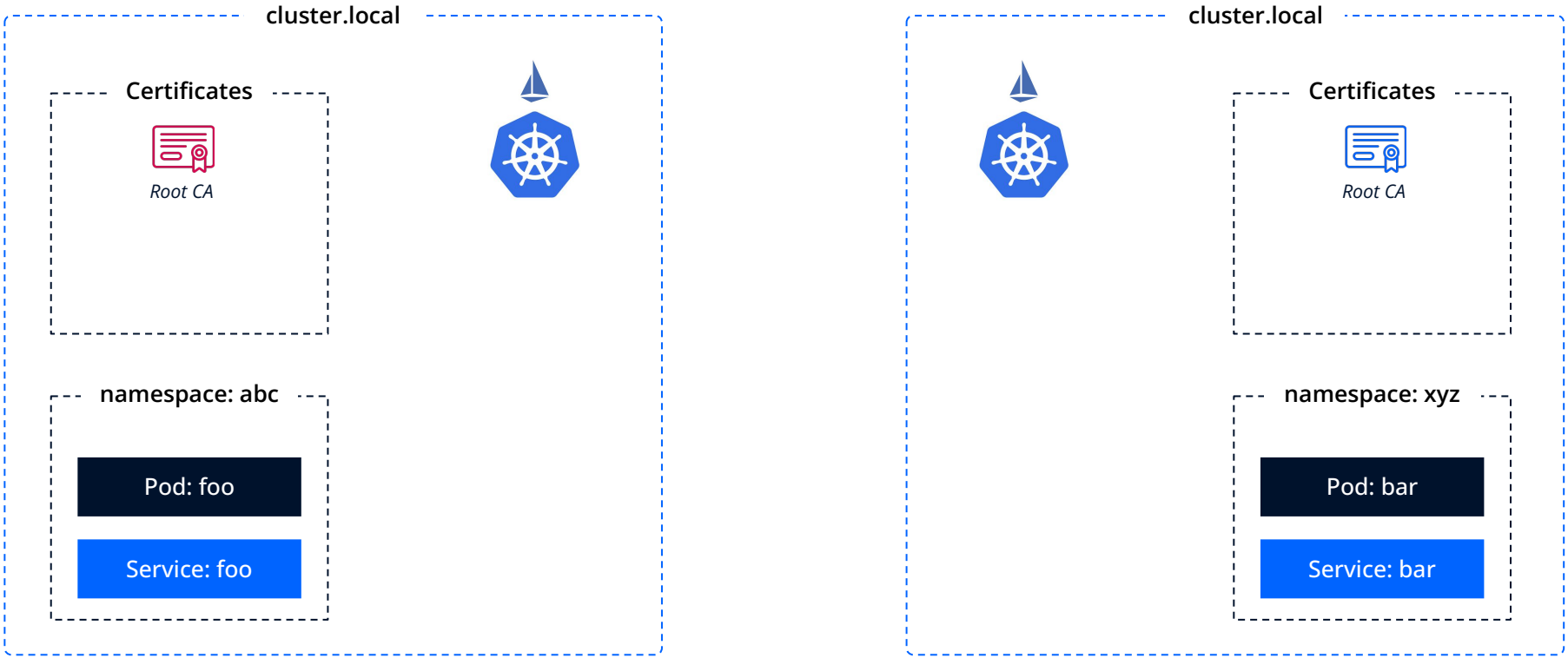
Kubernetes Platform



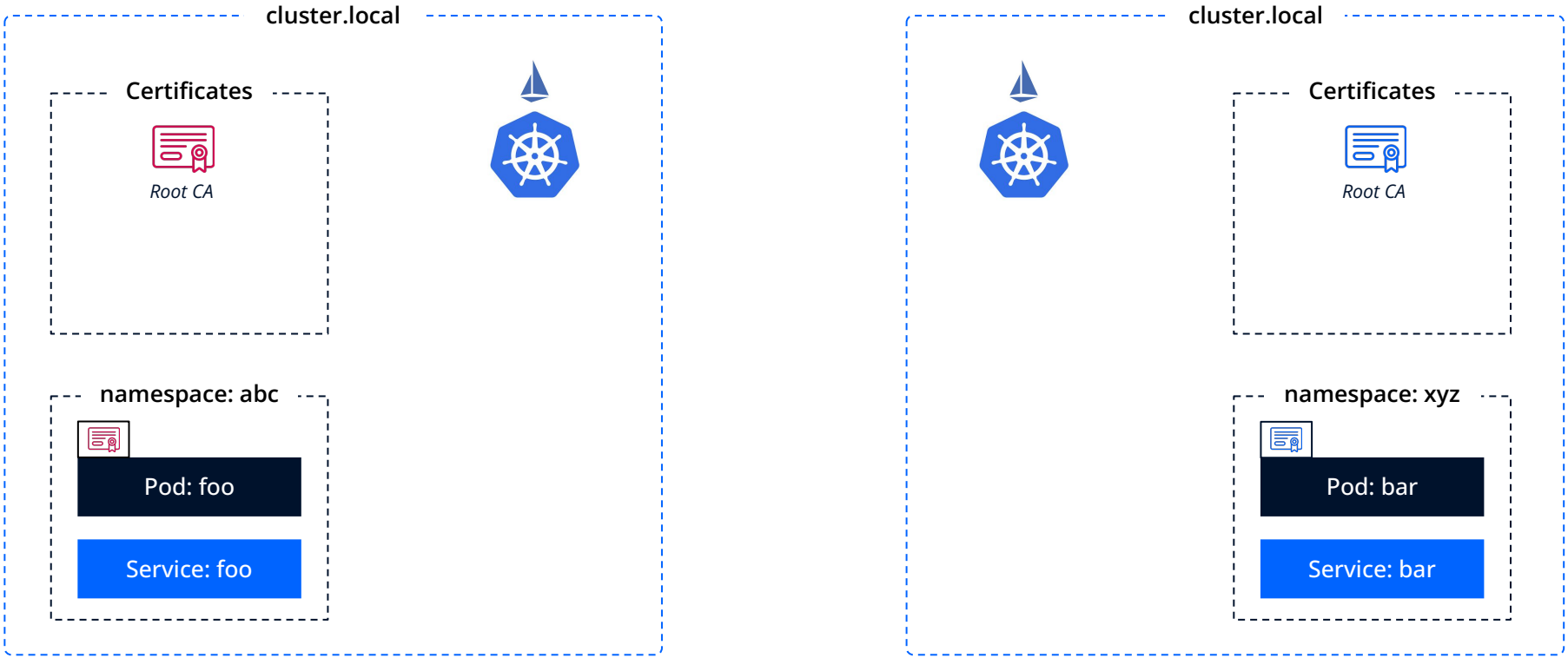
Suppose there are two clusters with the identical Cluster Domain assigned...



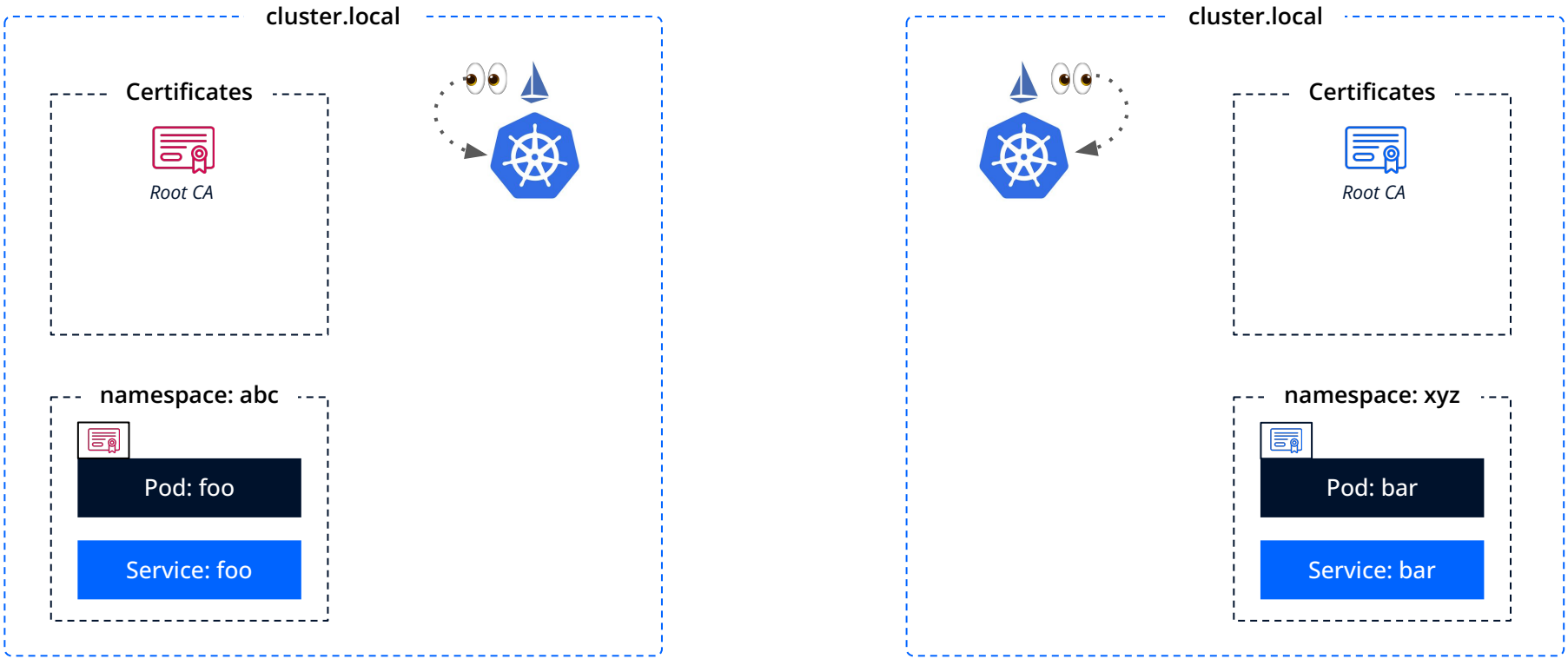
...and applications running in them.



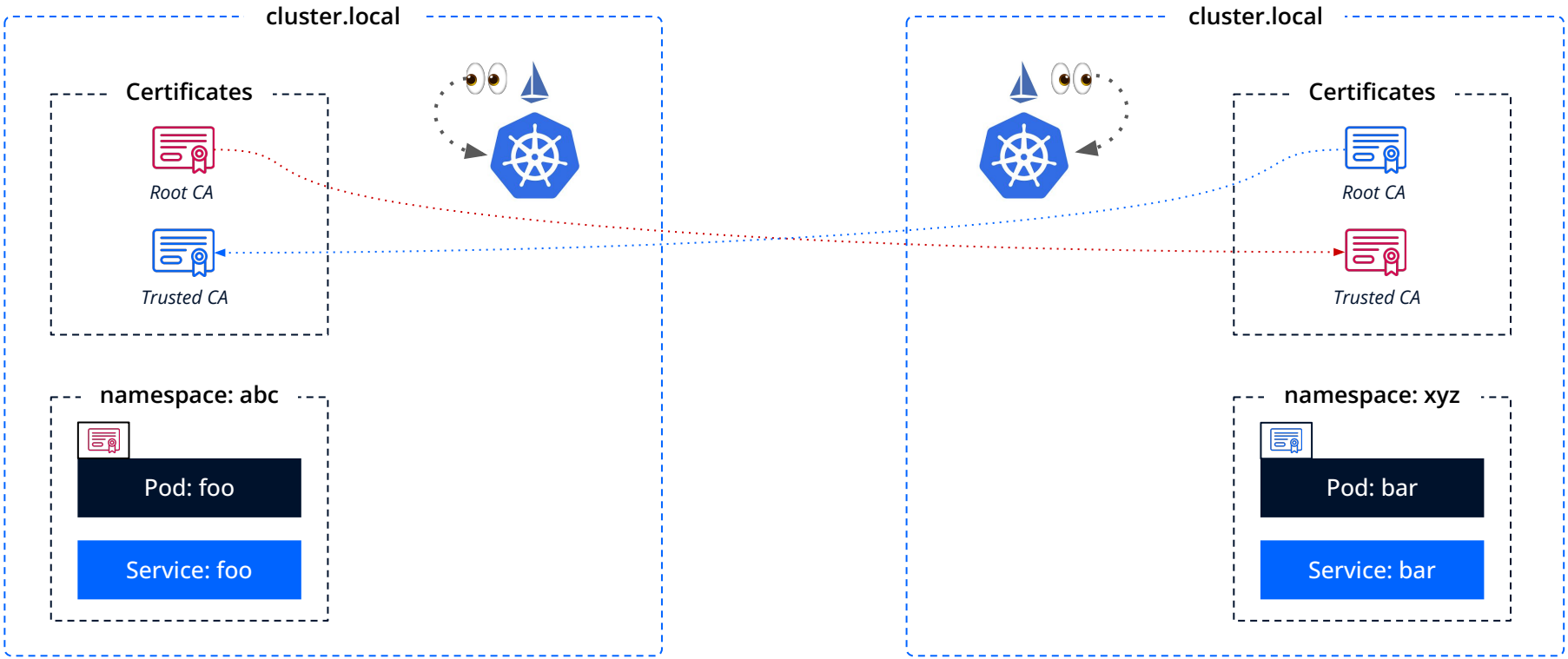
Each cluster has a trusted certificate repository that contains a single root certificate of the cluster.



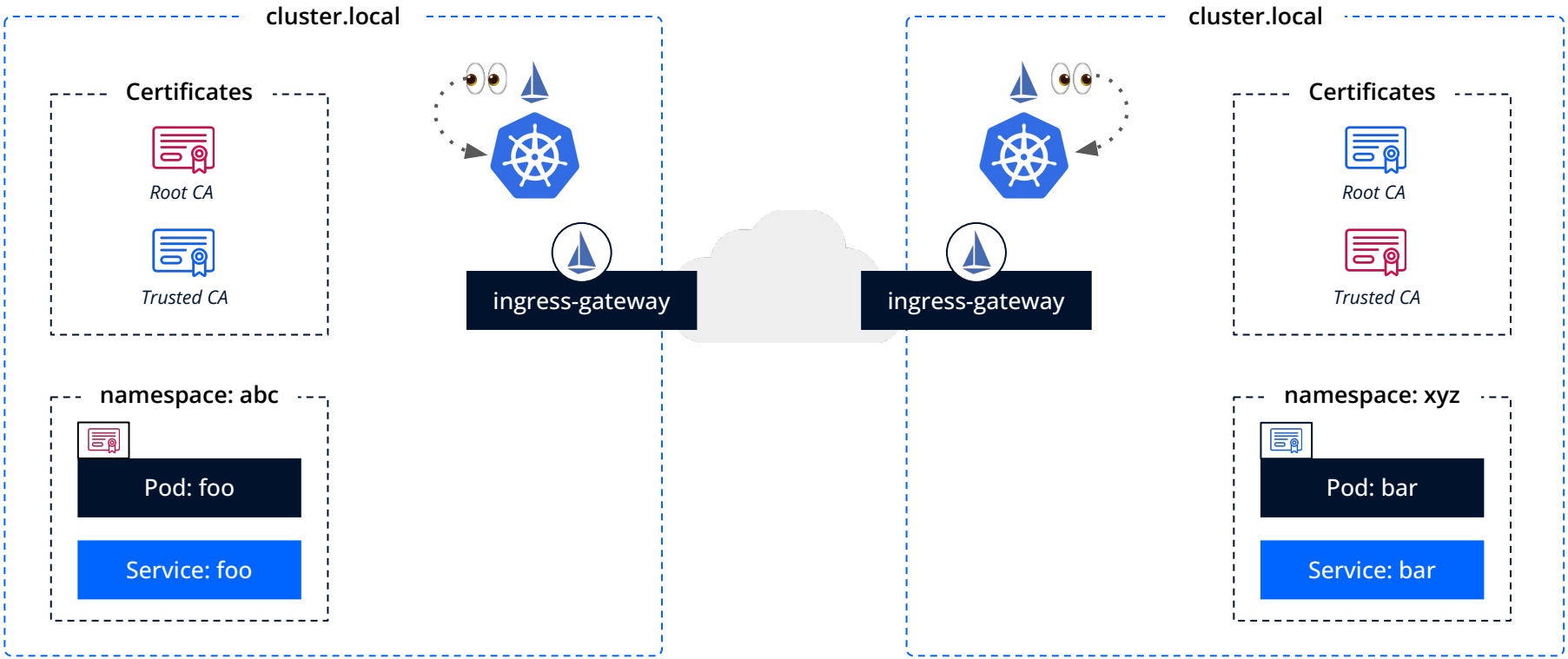
These root certificates are used to sign individual Pod certificates for Mutual TLS.



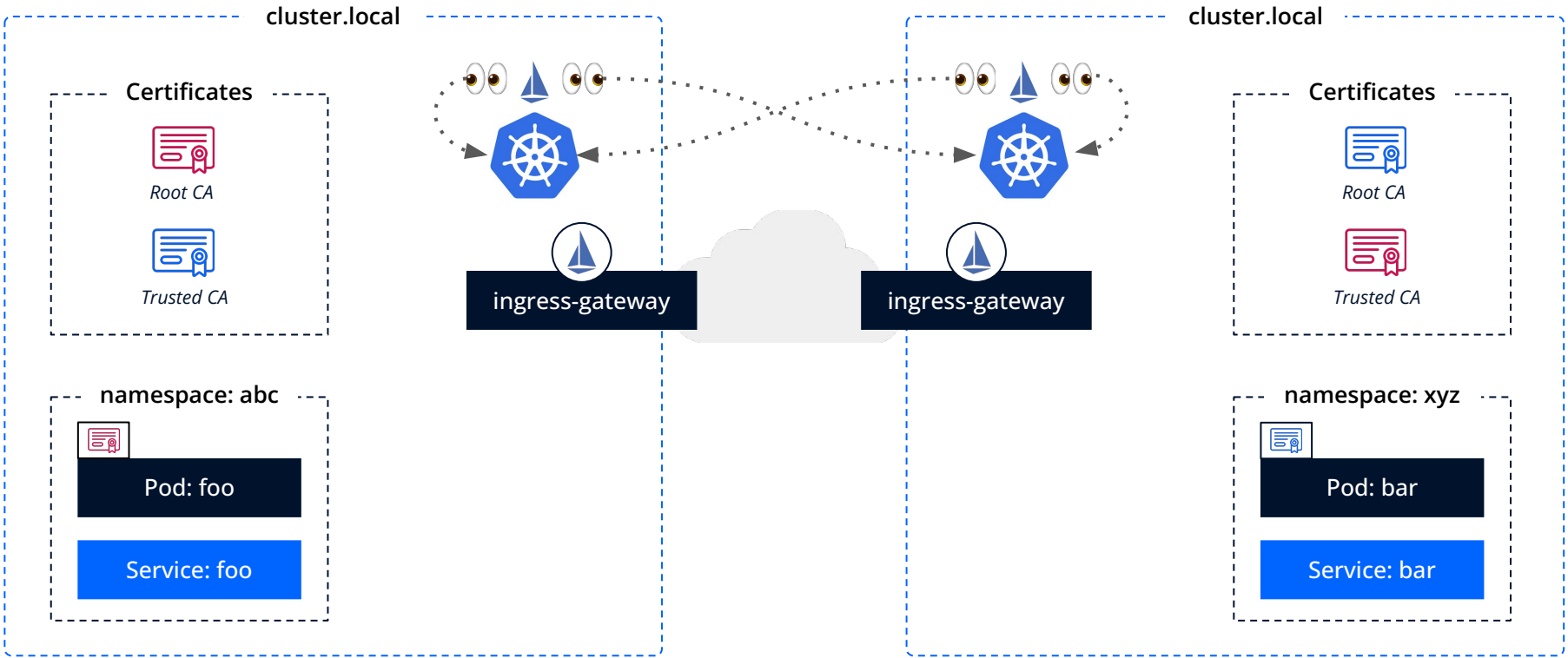
The Istio control plane communicates with the local kube-apiserver to collect information about the services, their addresses and status; the collected information is then aggregated and sent to the application sidecars.



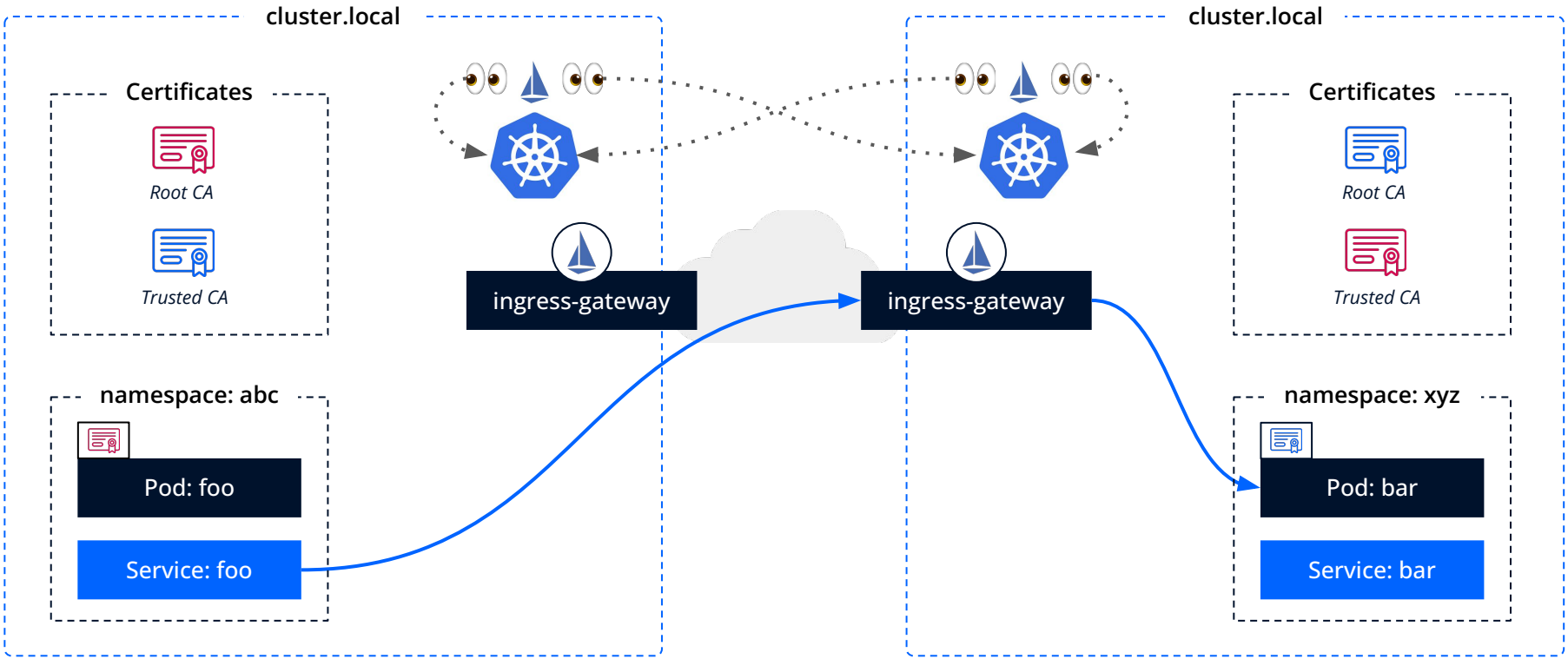
These two clusters must mutually exchange root certificates and put them in the trusted certificate repository to establish mutual trust.



An ingress gateway is used to exchange traffic between Pods from different clusters. It enables receiving Mutual TLS requests from neighboring trusted clusters.



The Istio control plane connects to the remote kube-apiserver to collect information about the services running on the remote cluster.



The collected data is enough to integrate into a single Service Mesh.