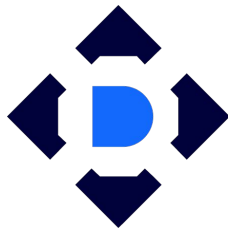


Istio

Federation

Common principles

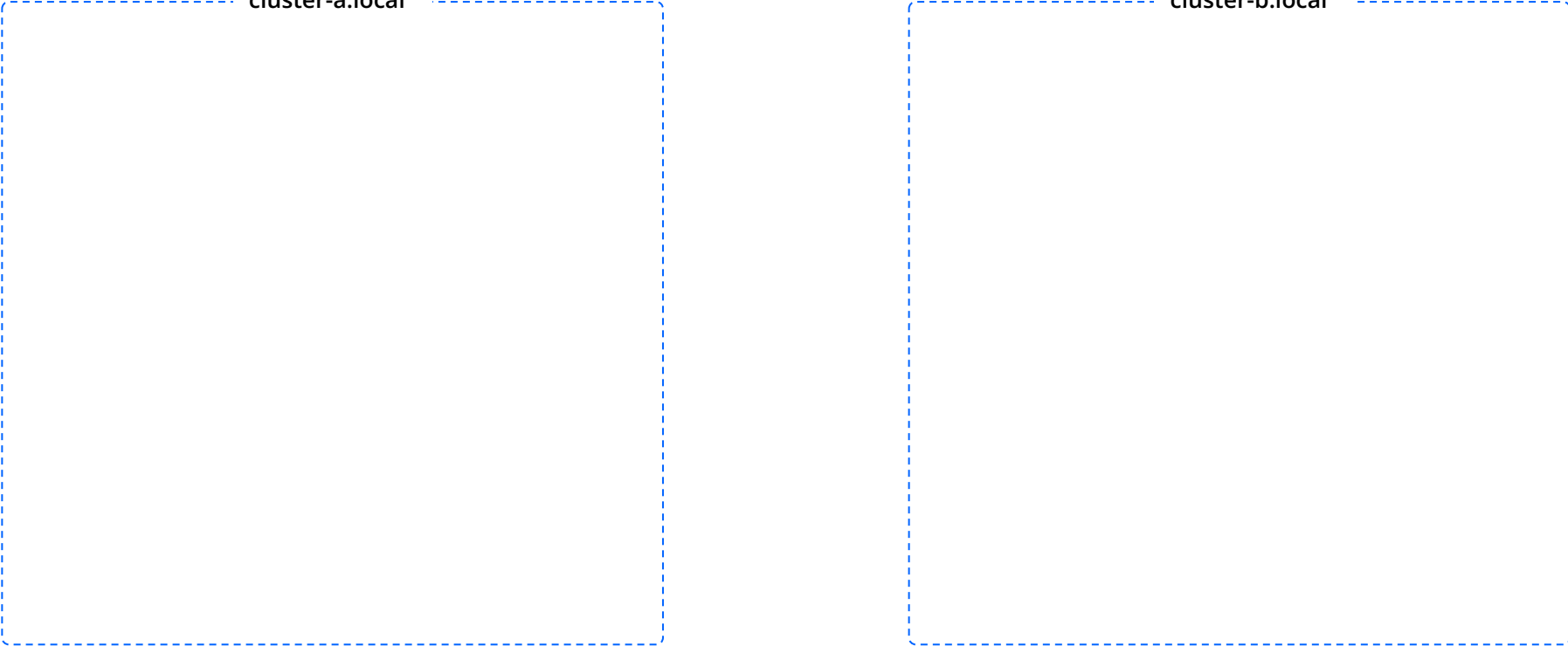


FLANT

Deckhouse

Kubernetes Platform

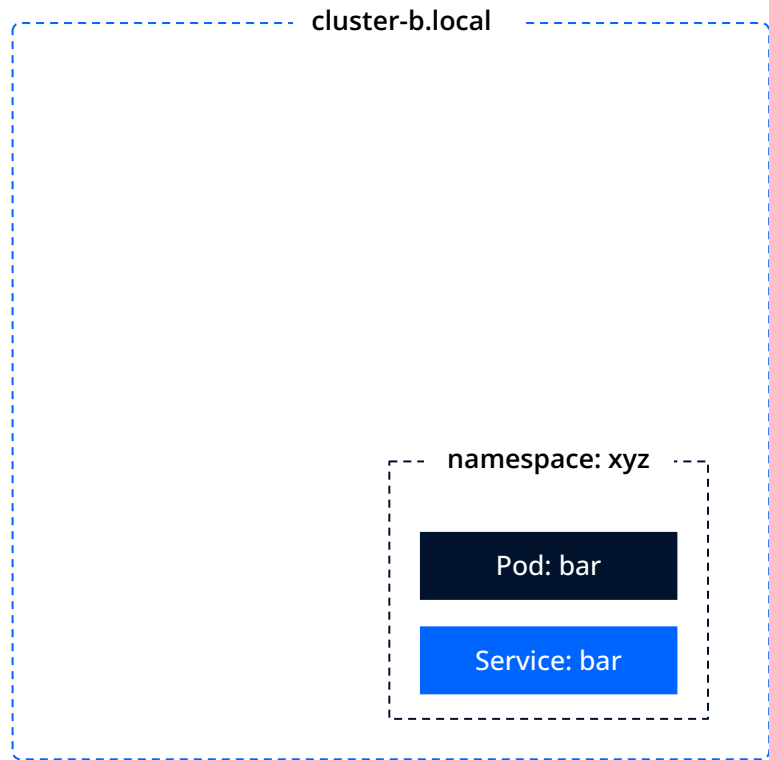
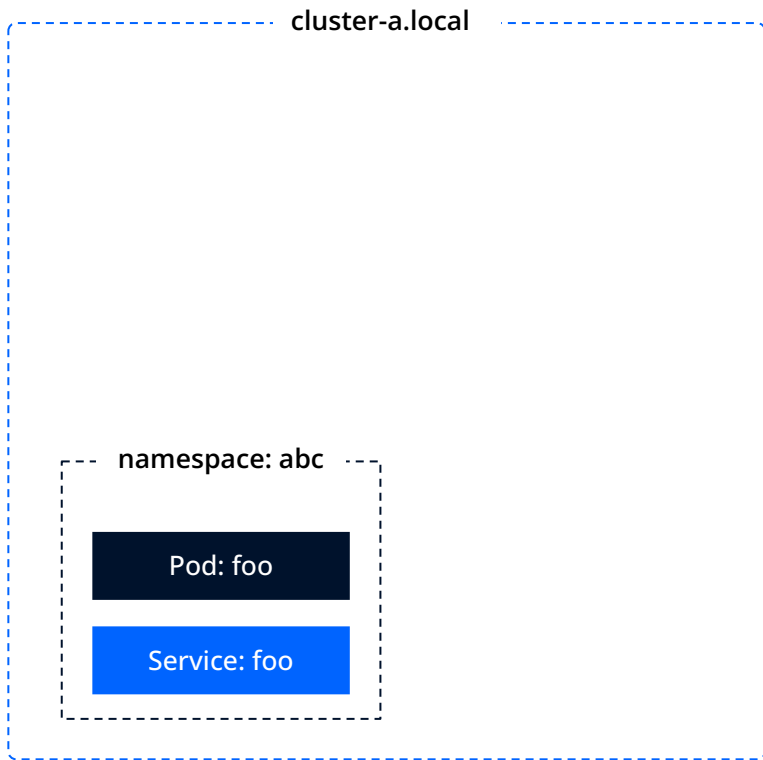
cluster-a.local



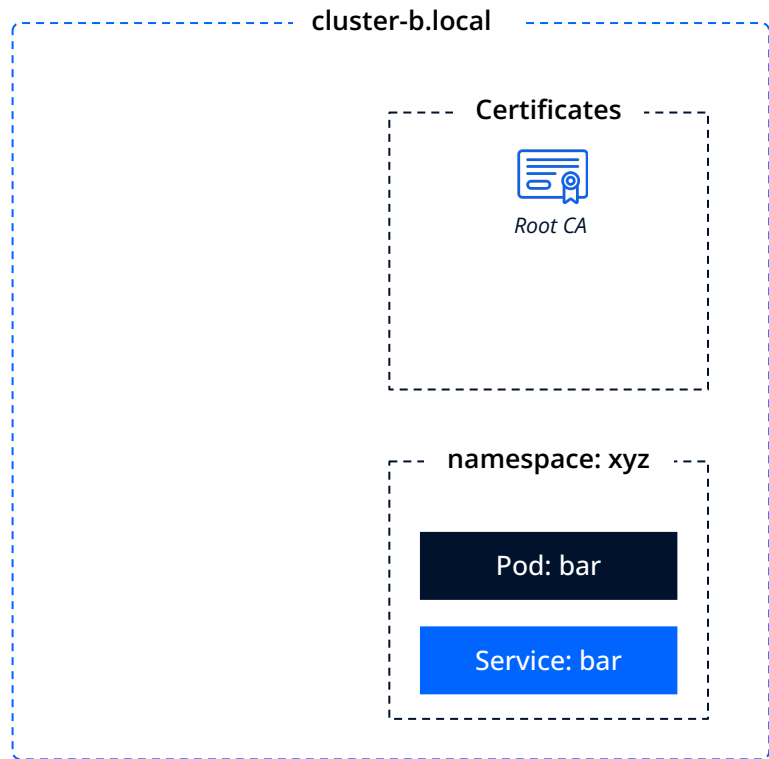
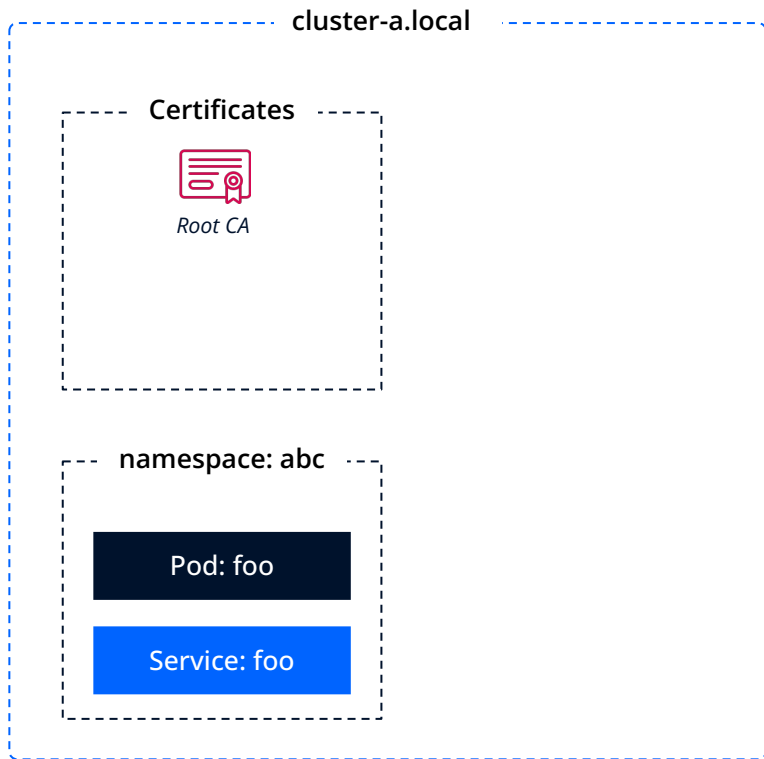
The diagram consists of two identical dashed blue rectangular boxes arranged horizontally. The left box is labeled 'cluster-a.local' at its top-left corner, and the right box is labeled 'cluster-b.local' at its top-left corner. The boxes are empty, representing the internal state or components of each cluster.

cluster-b.local

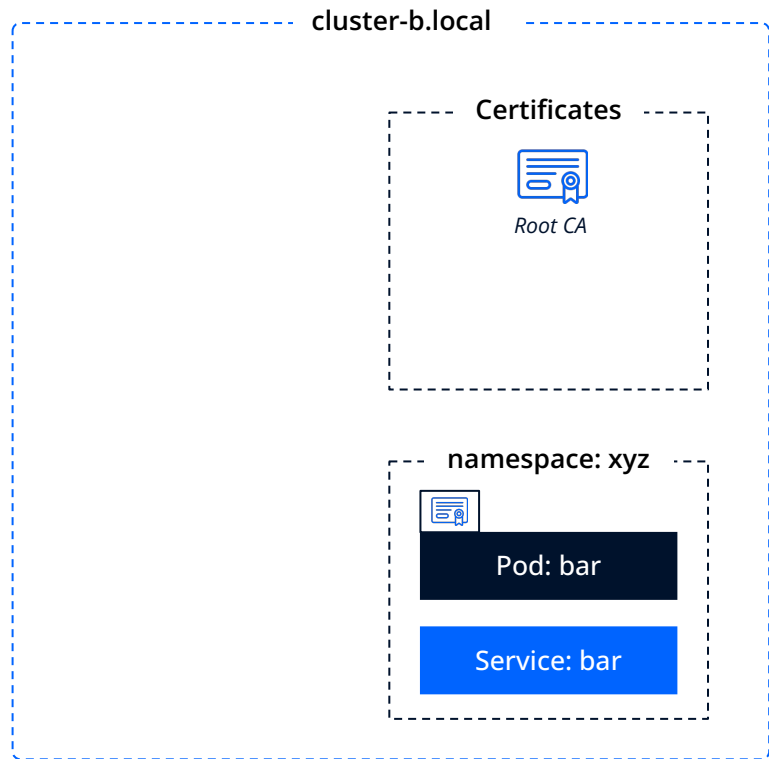
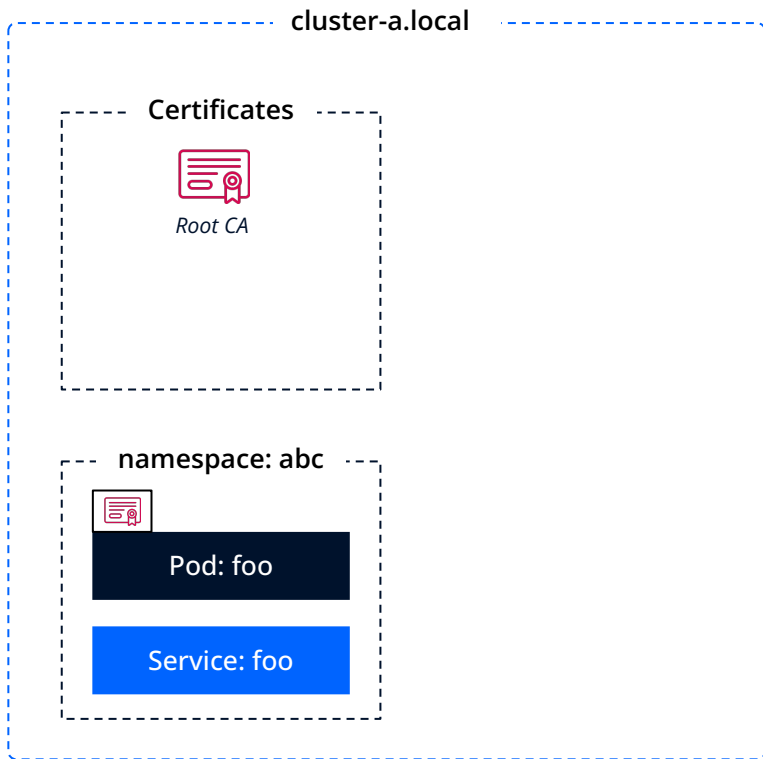
Suppose Istio manages two clusters...



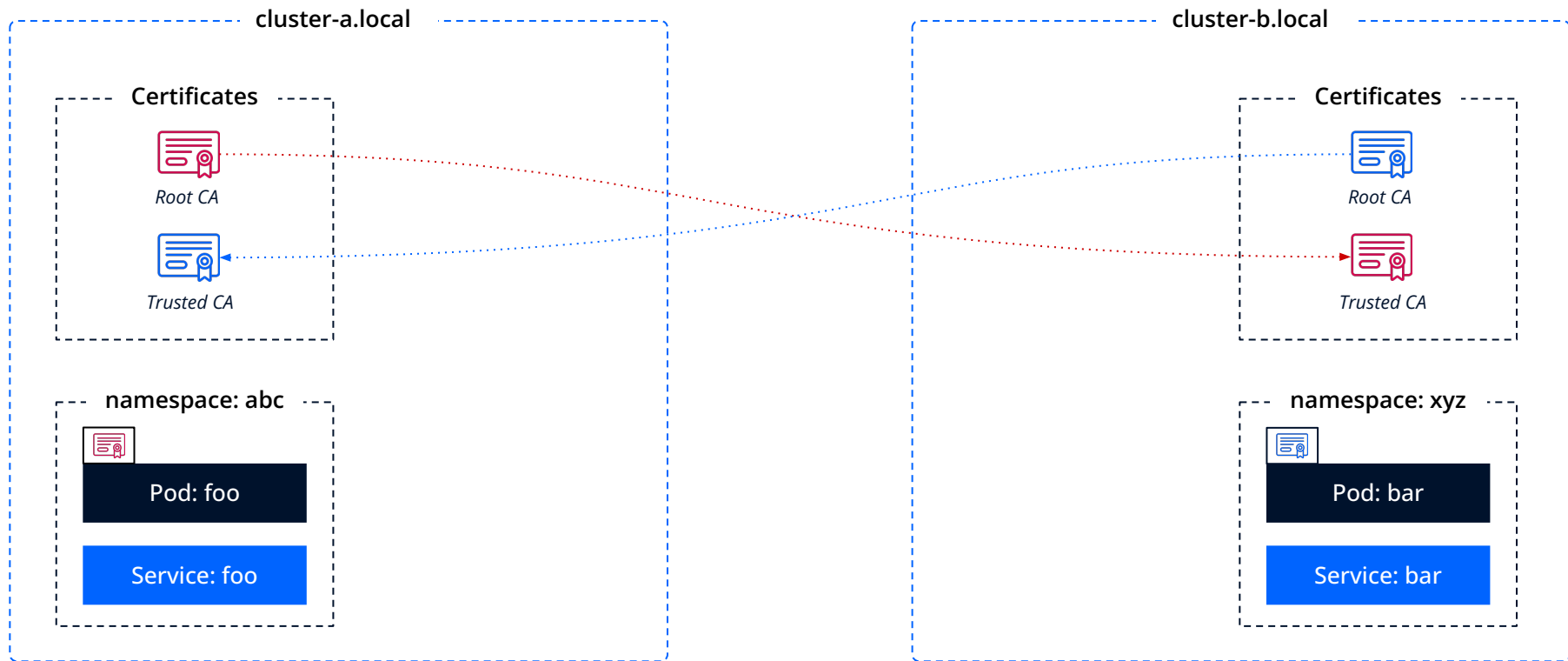
...with applications running in them.



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.



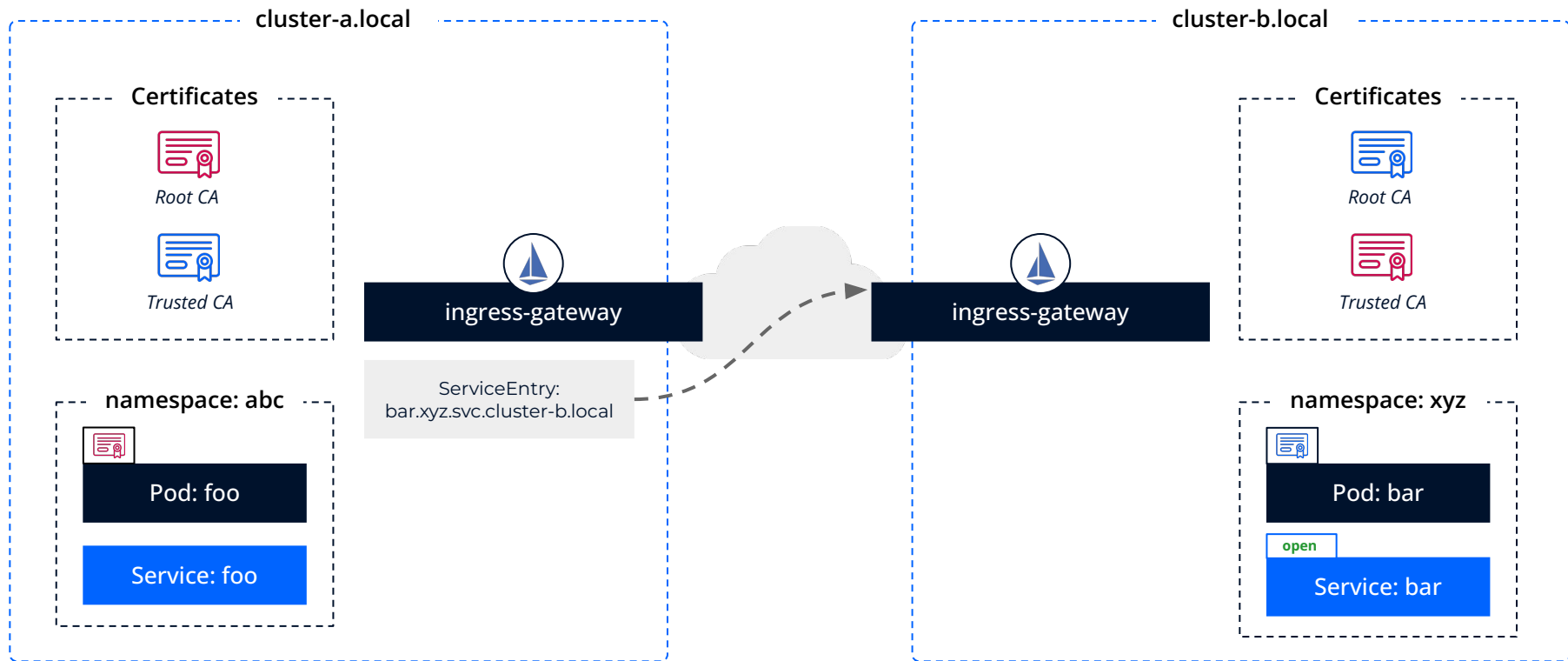
These two clusters must mutually exchange root certificates and put them in the trusted certificate repository to establish mutual trust.



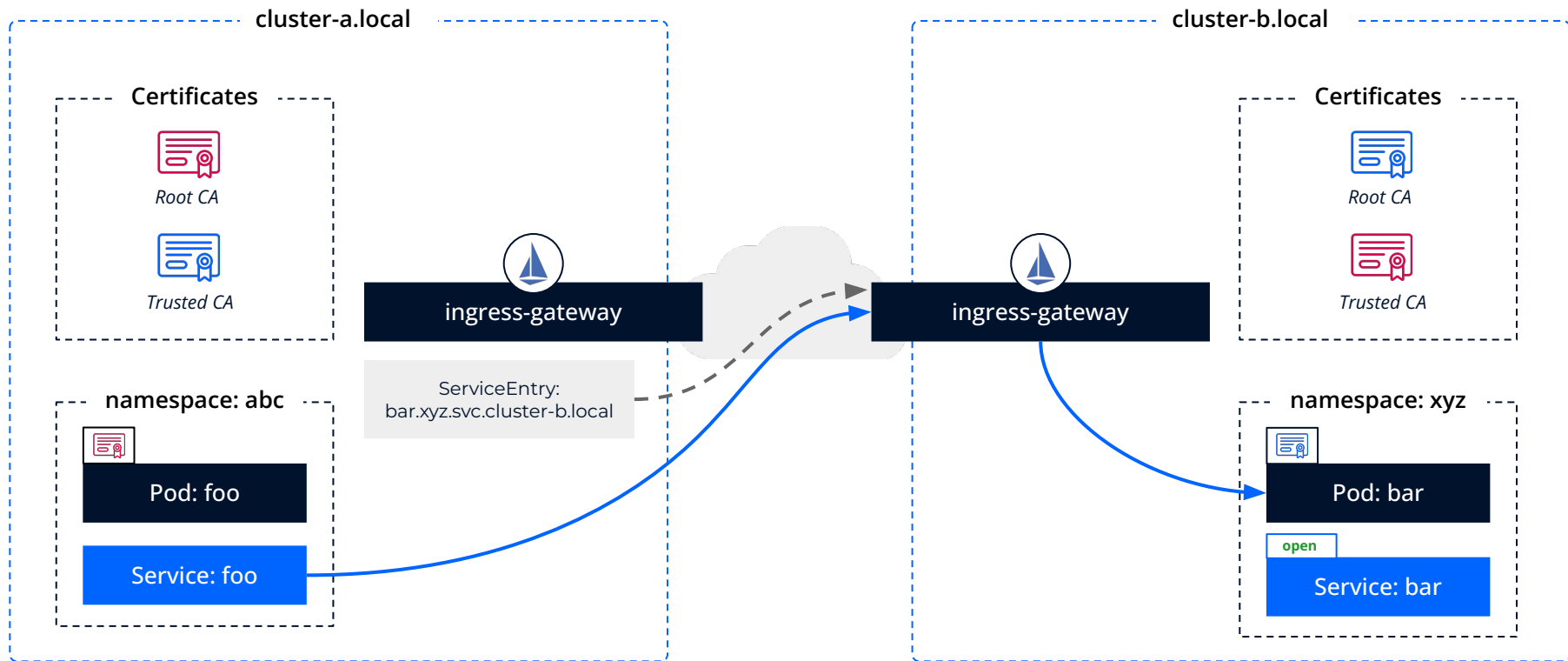
Each cluster has an ingress gateway to receive Mutual TLS requests outside the cluster.



We use these ingress gateways to provide external clusters with access to the service under the federation.



All that is left to do now is to create a ServiceEntry resource. It will register the remote `bar.xyz.svc.cluster-b.local` service in cluster-a and specify the parameters of the cluster ingress-gateway to use for accessing the service.



As a result, the federation is configured, and services in different clusters can access each other with all the benefits of a shared Service Mesh.