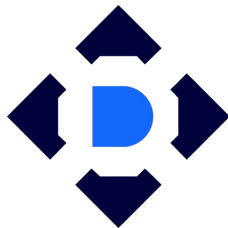


Istio

Мультикластер
Общие принципы



FLANT

Deckhouse
Kubernetes Platform

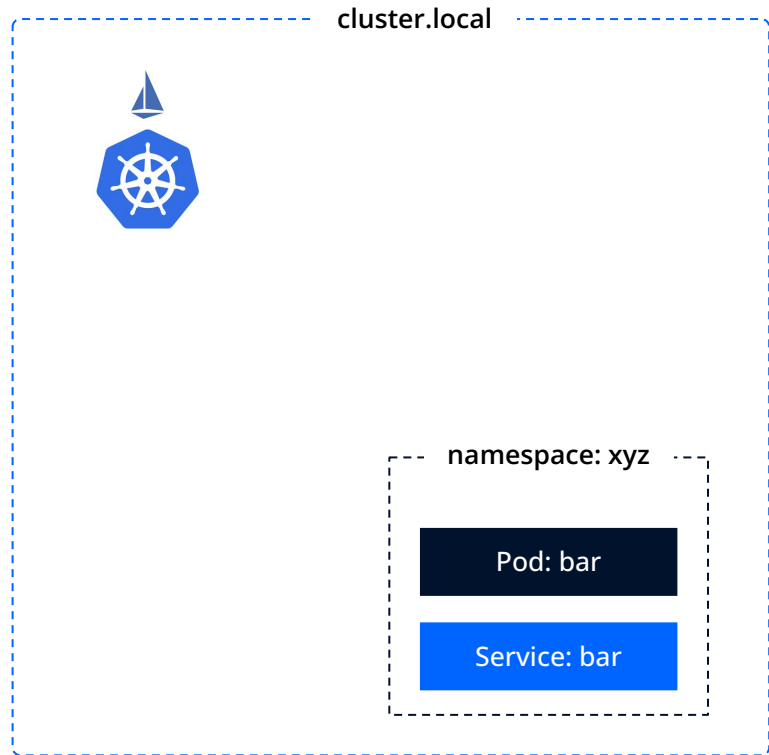
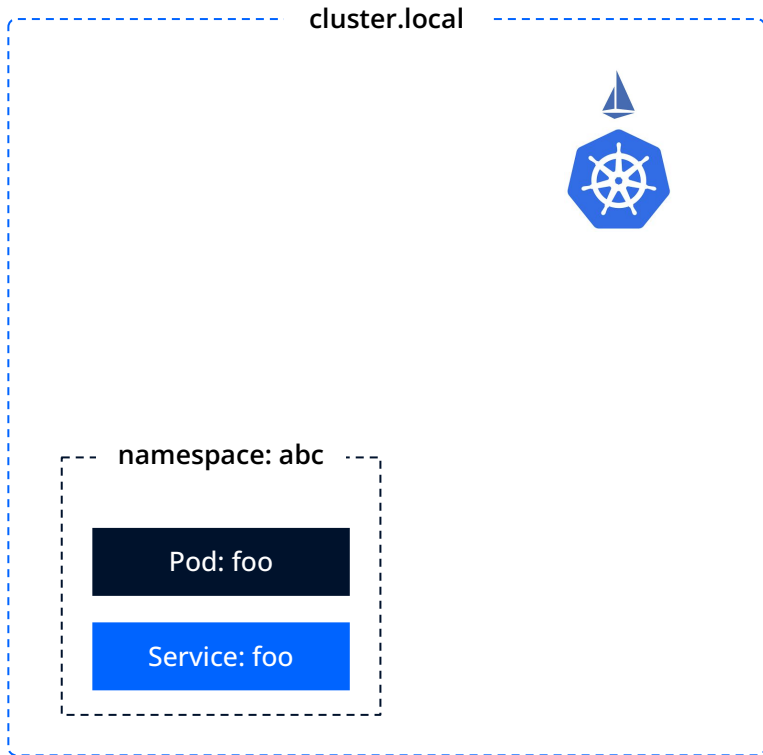
cluster.local



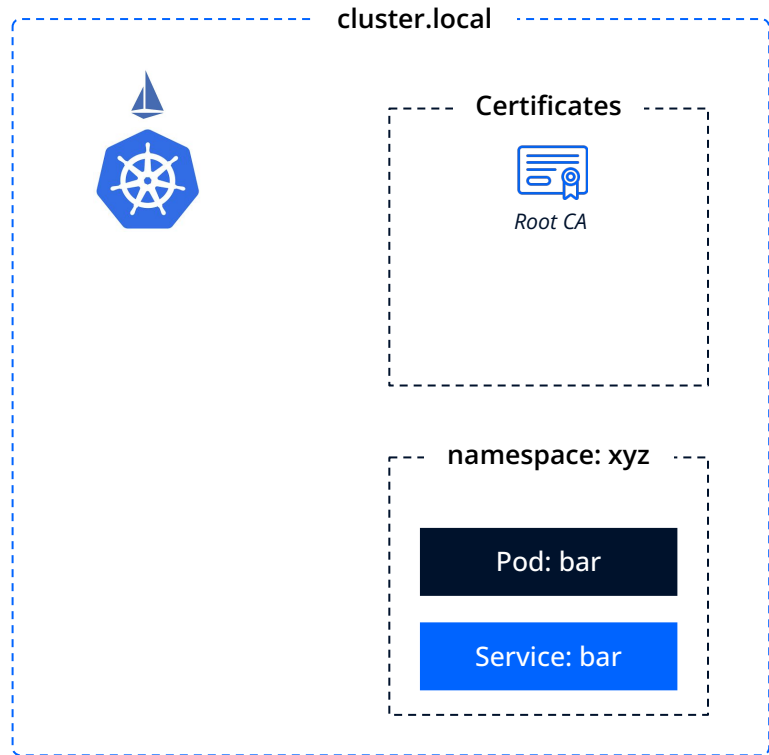
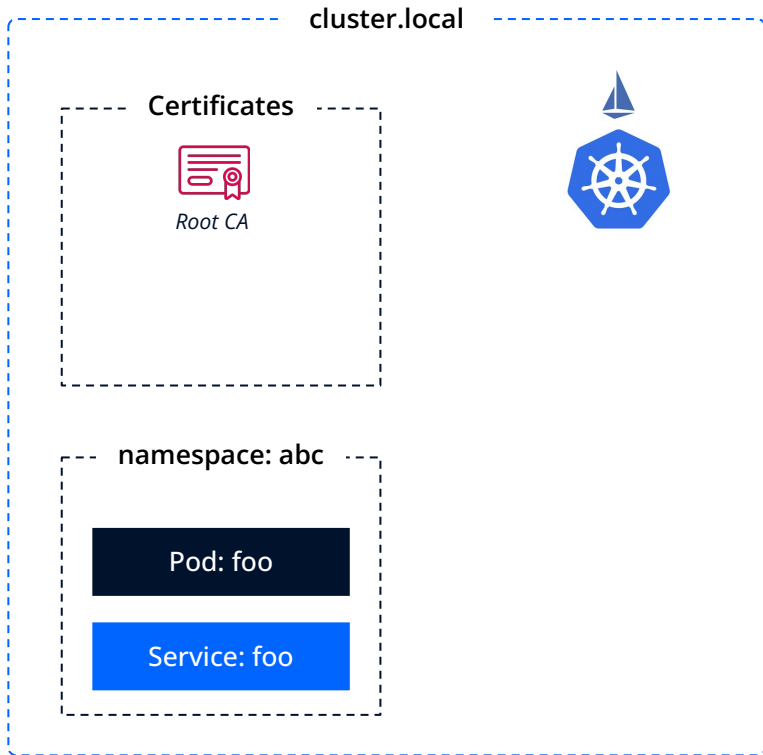
cluster.local



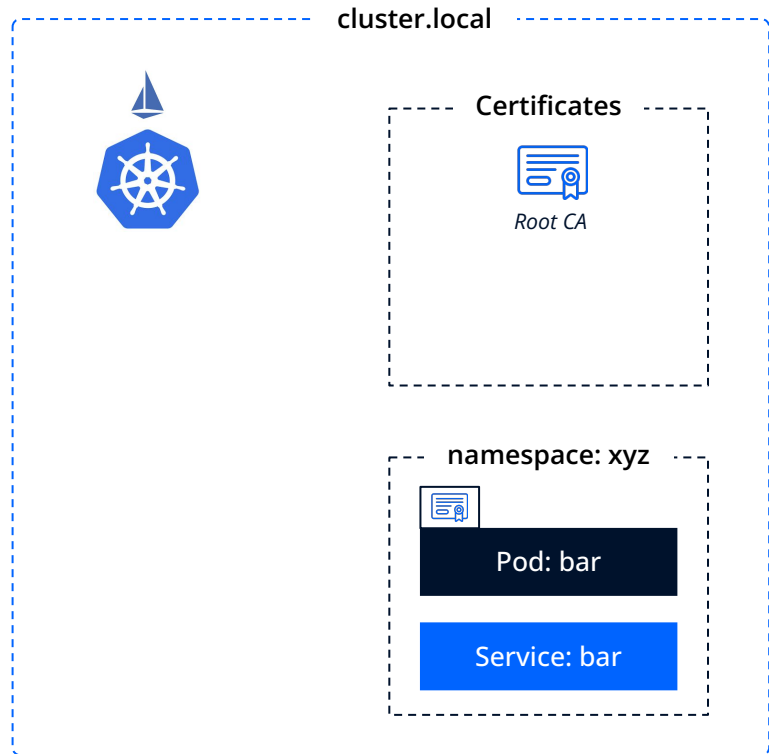
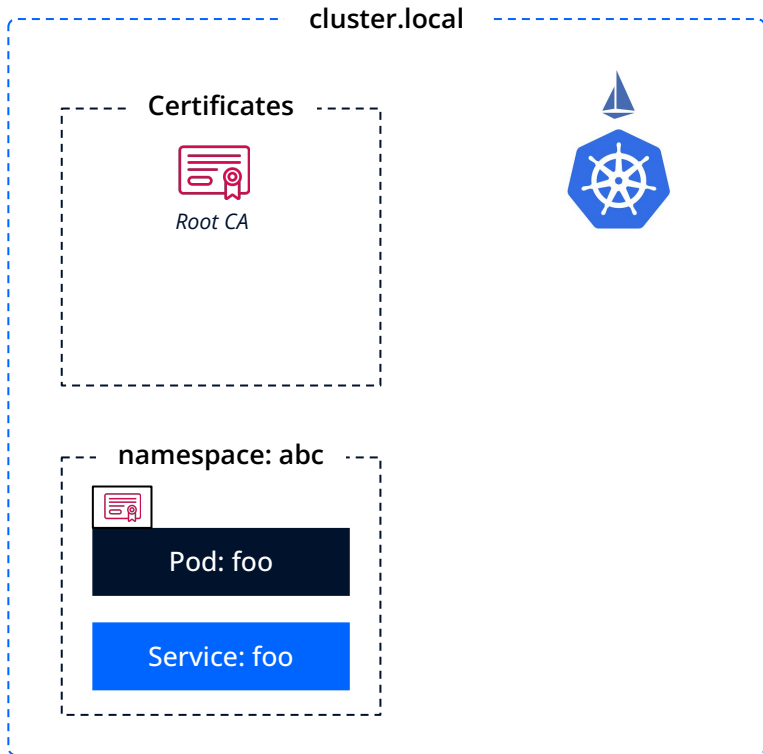
Есть два кластера под управлением Istio с одинаковым Cluster Domain.



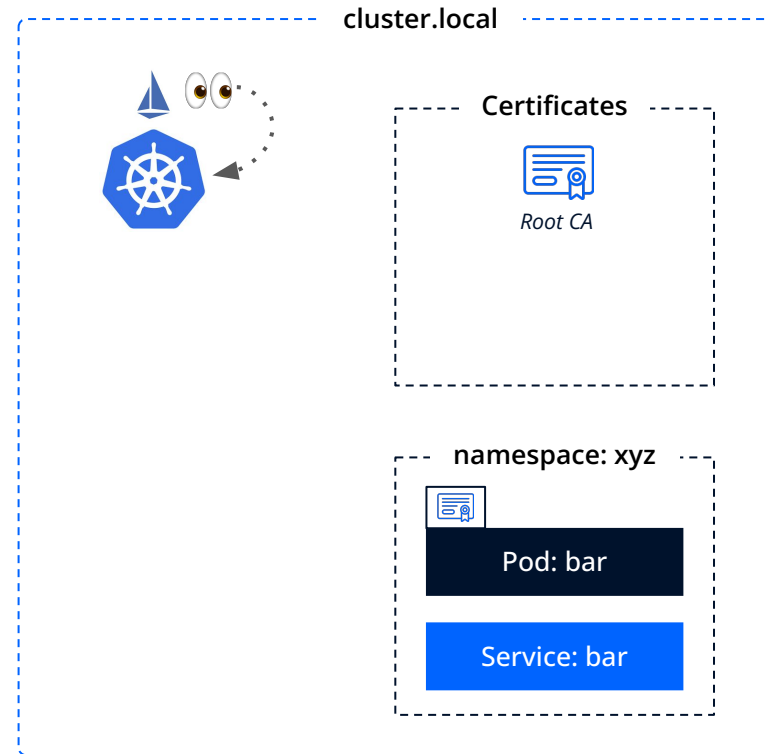
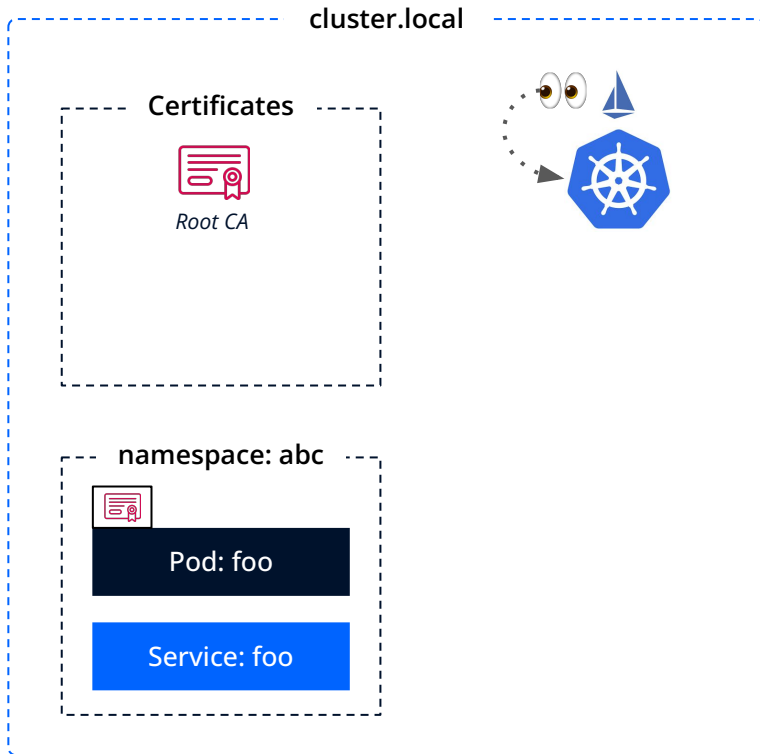
В них работают приложения.



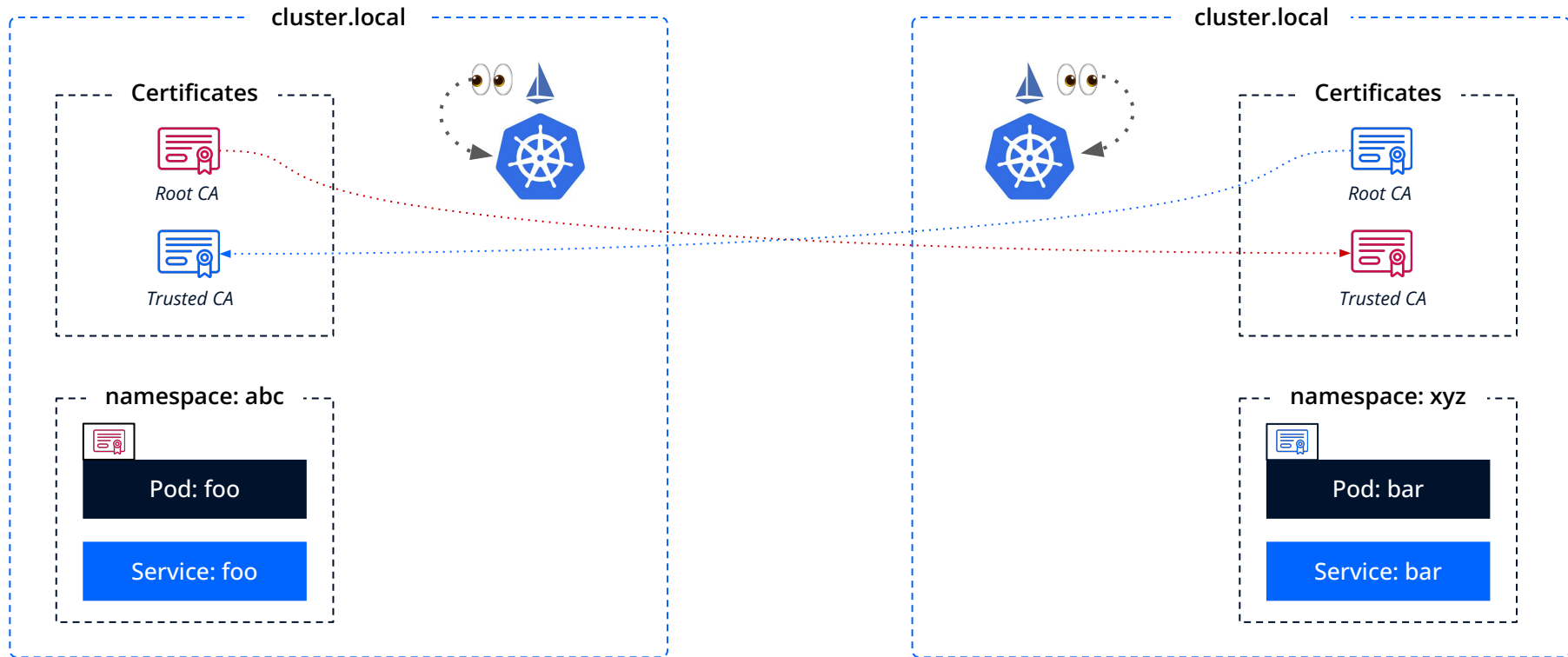
У каждого кластера есть хранилище доверенных сертификатов, которое содержит единственный корневой сертификат кластера.



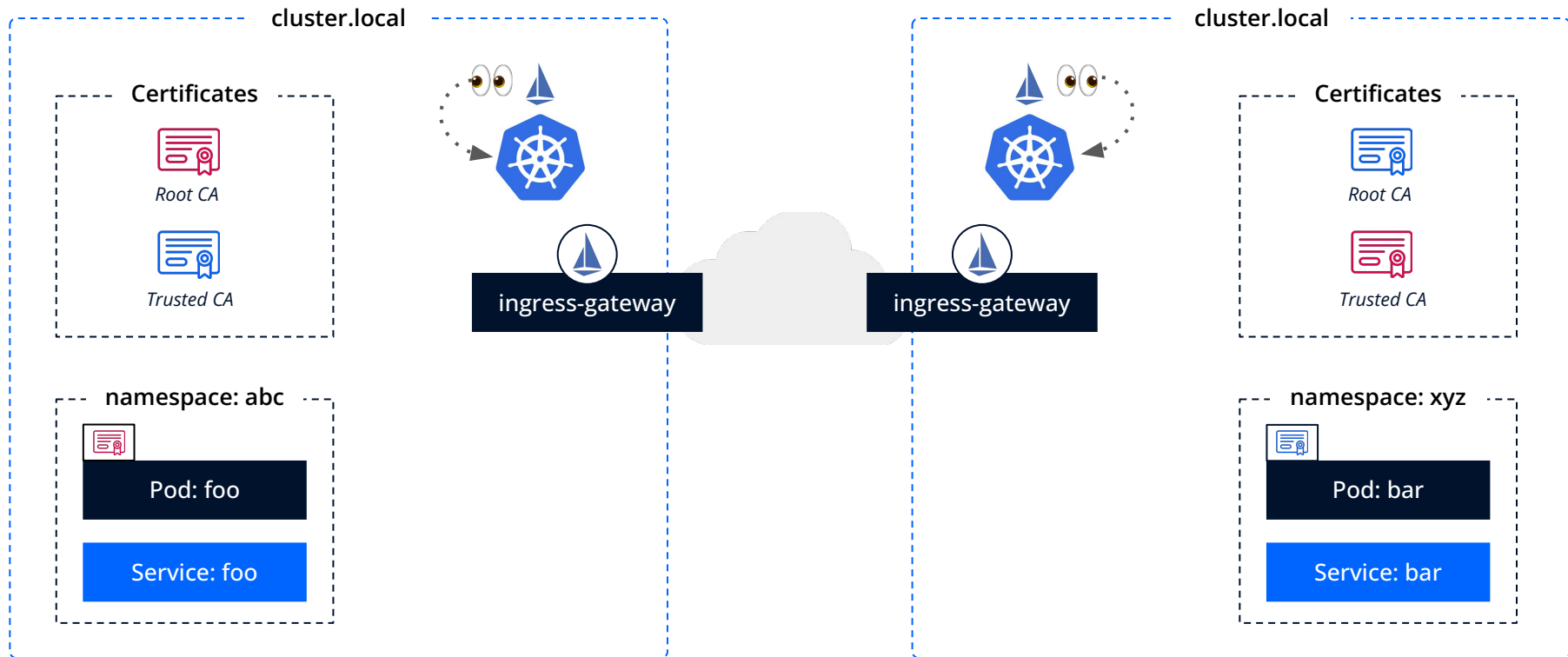
Этими корневыми сертификатами подписаны индивидуальные сертификаты подов для нужд Mutual TLS.



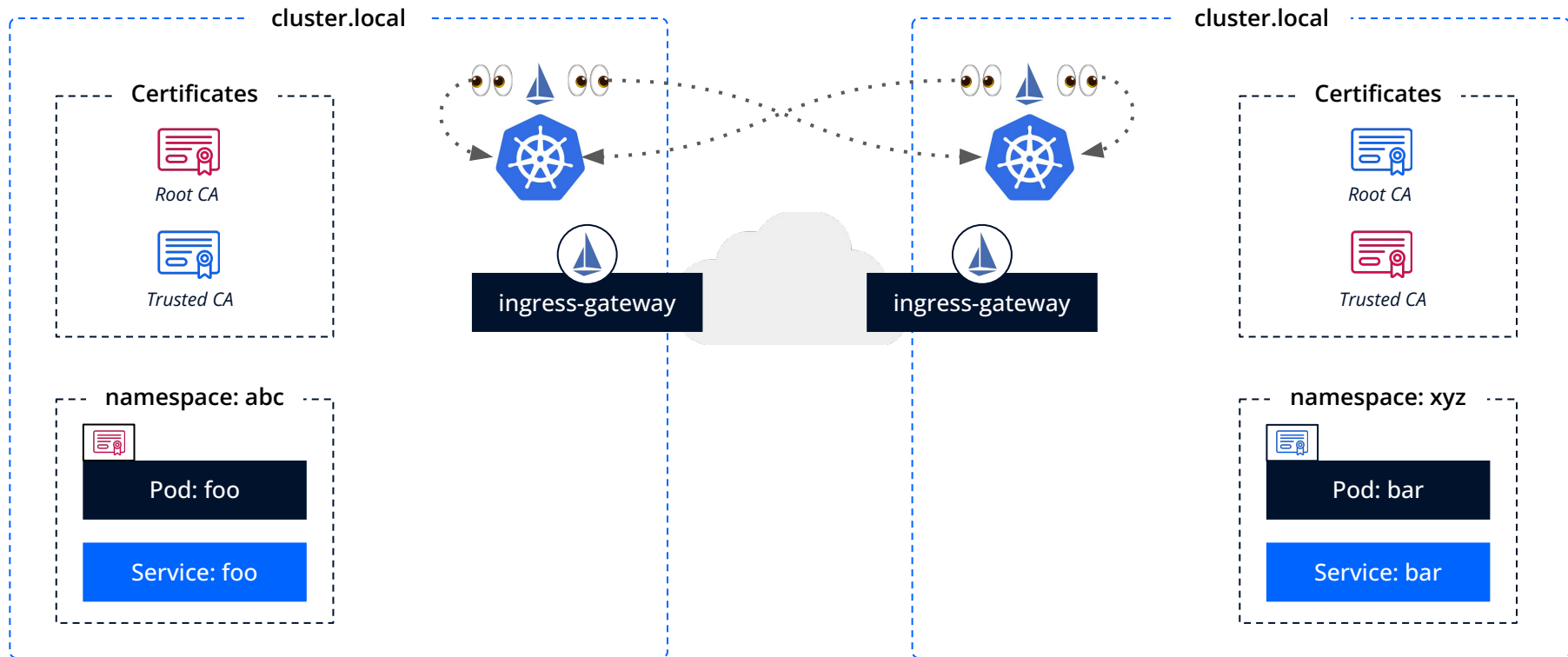
Control plane Istio взаимодействует с локальным kube-apiserver для сбора информации о сервисах, их адресах и состоянии, собранная информация консолидируется и рассылается по сайдкартам приложений.



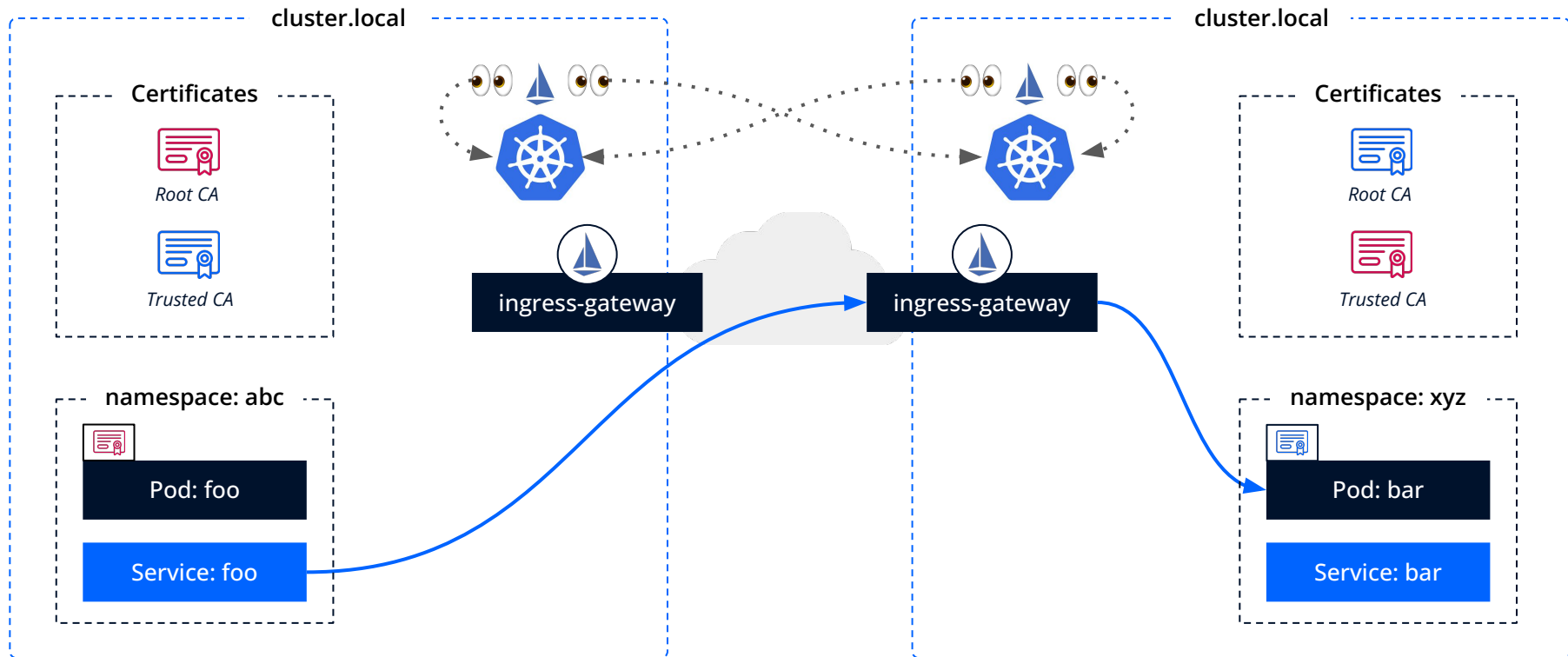
Для обеспечения взаимного доверия необходимо взаимно обменяться корневыми сертификатами и поместить их в хранилище доверенных сертификатов.



Для обмена трафиком между подами из разных кластеров используются ingress-gateway, которые позволяют принимать Mutual TLS запросы из соседних доверенных кластеров.



Для сбора информации о работающих сервисах на удаленном кластере control plane Istio подключается к удаленному kube-apiserver.



Полученных данных достаточно для объединения в единый Service Mesh.