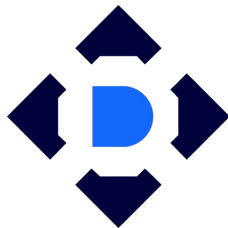


Istio

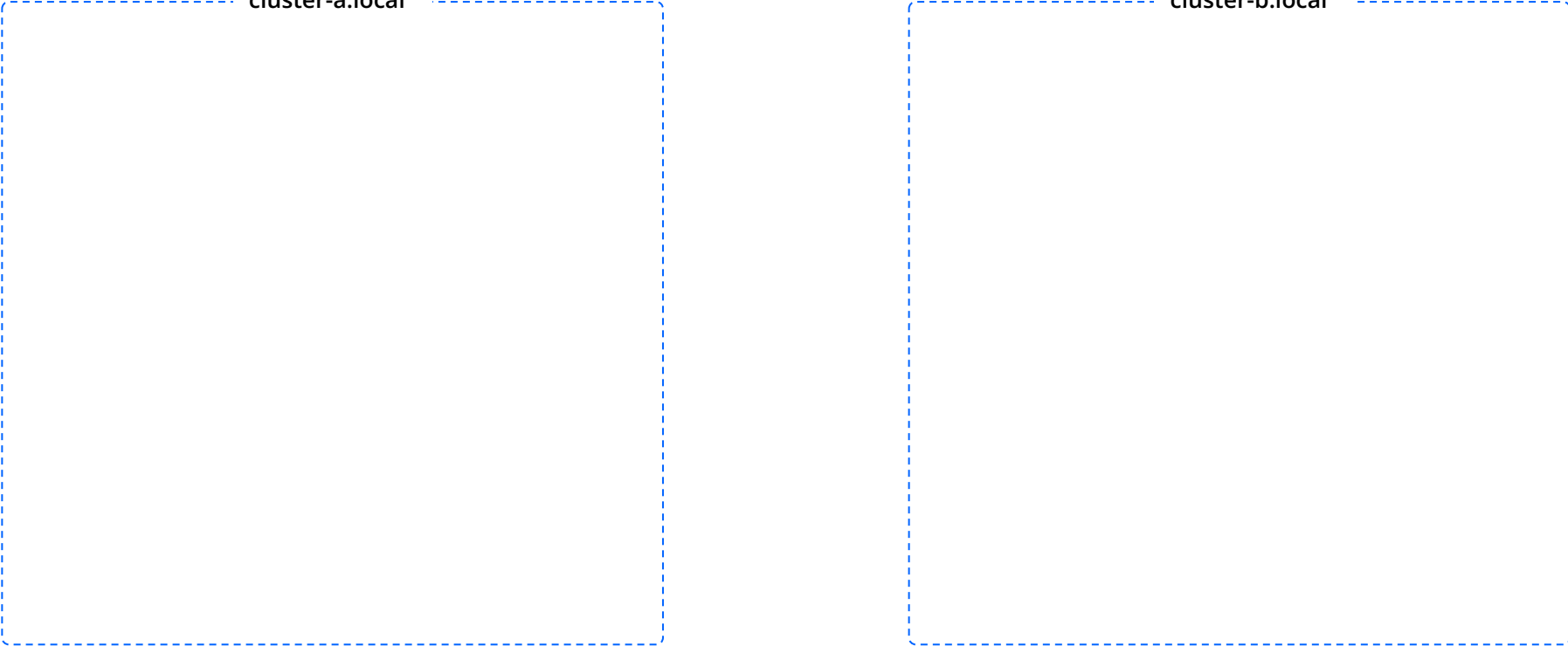
Федерация
Общие принципы



FLANT

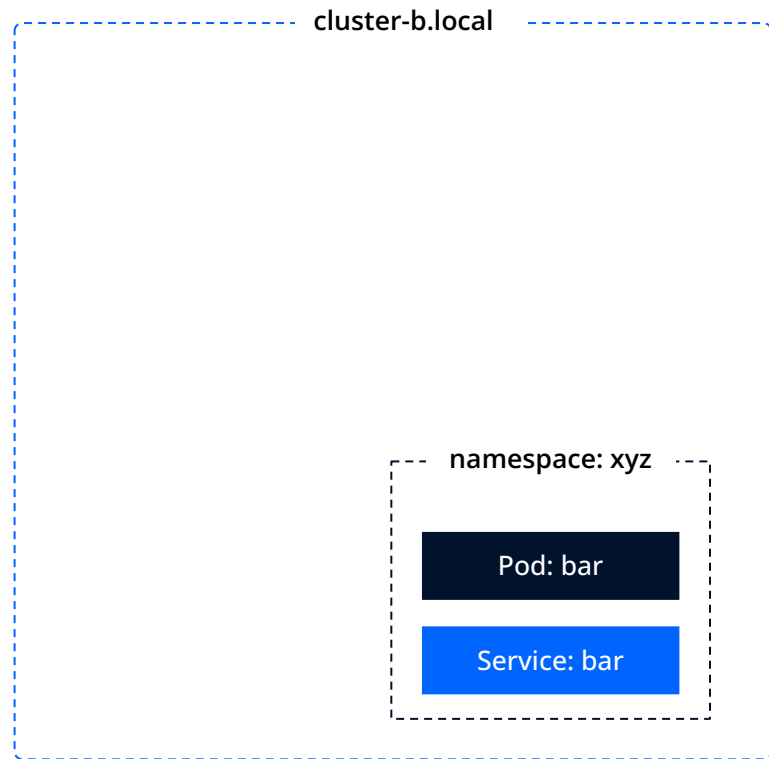
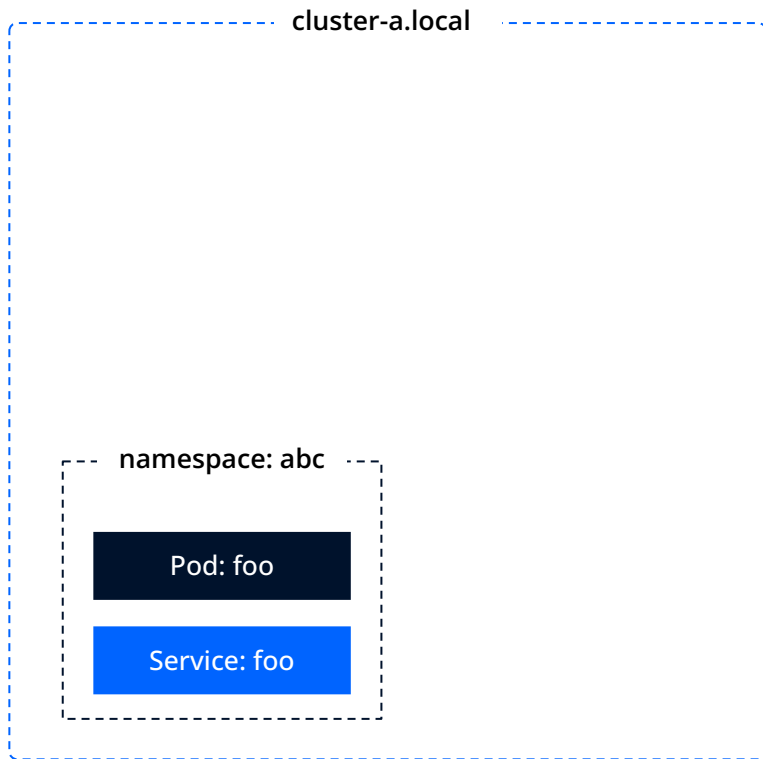
Deckhouse
Kubernetes Platform

cluster-a.local

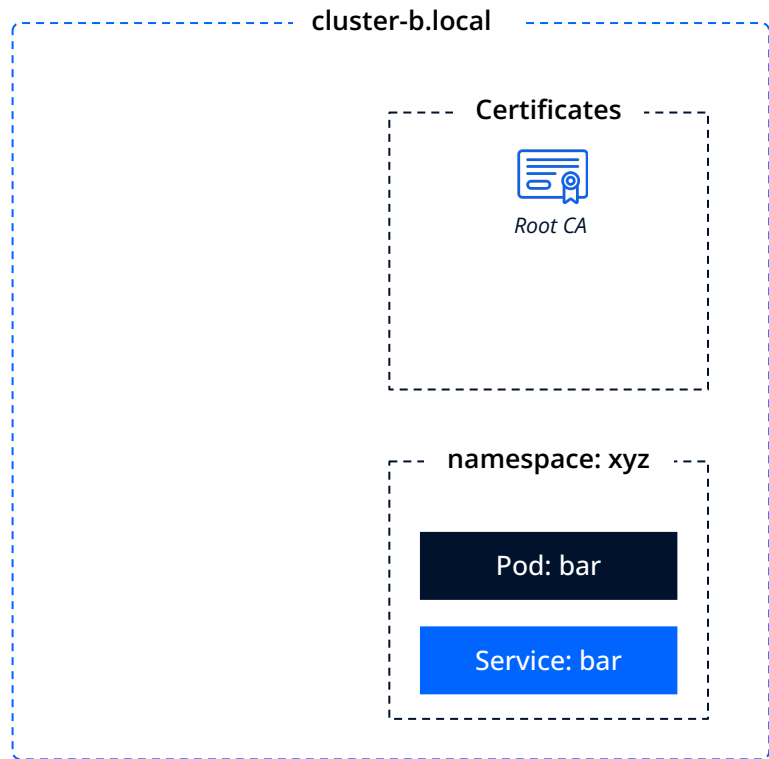
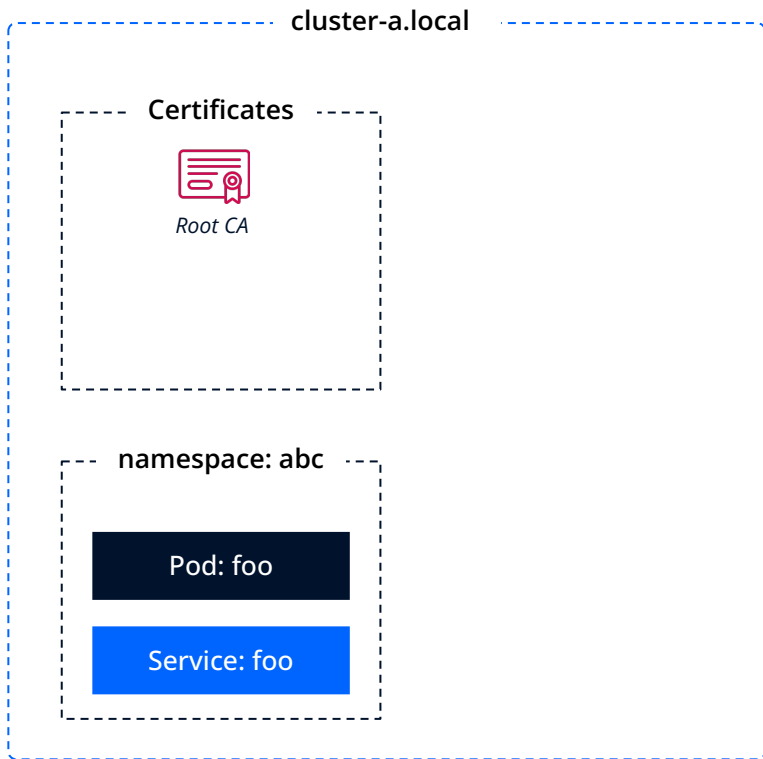
The diagram consists of two identical dashed blue rectangular boxes arranged horizontally. The left box is labeled 'cluster-a.local' at its top-left corner, and the right box is labeled 'cluster-b.local' at its top-left corner. The boxes are empty, representing the internal structure of each cluster.

cluster-b.local

Есть два кластера под управлением Istio...



...в них работают приложения.



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

cluster-a.local

Certificates



Root CA

namespace: abc



Pod: foo

Service: foo

cluster-b.local

Certificates



Root CA

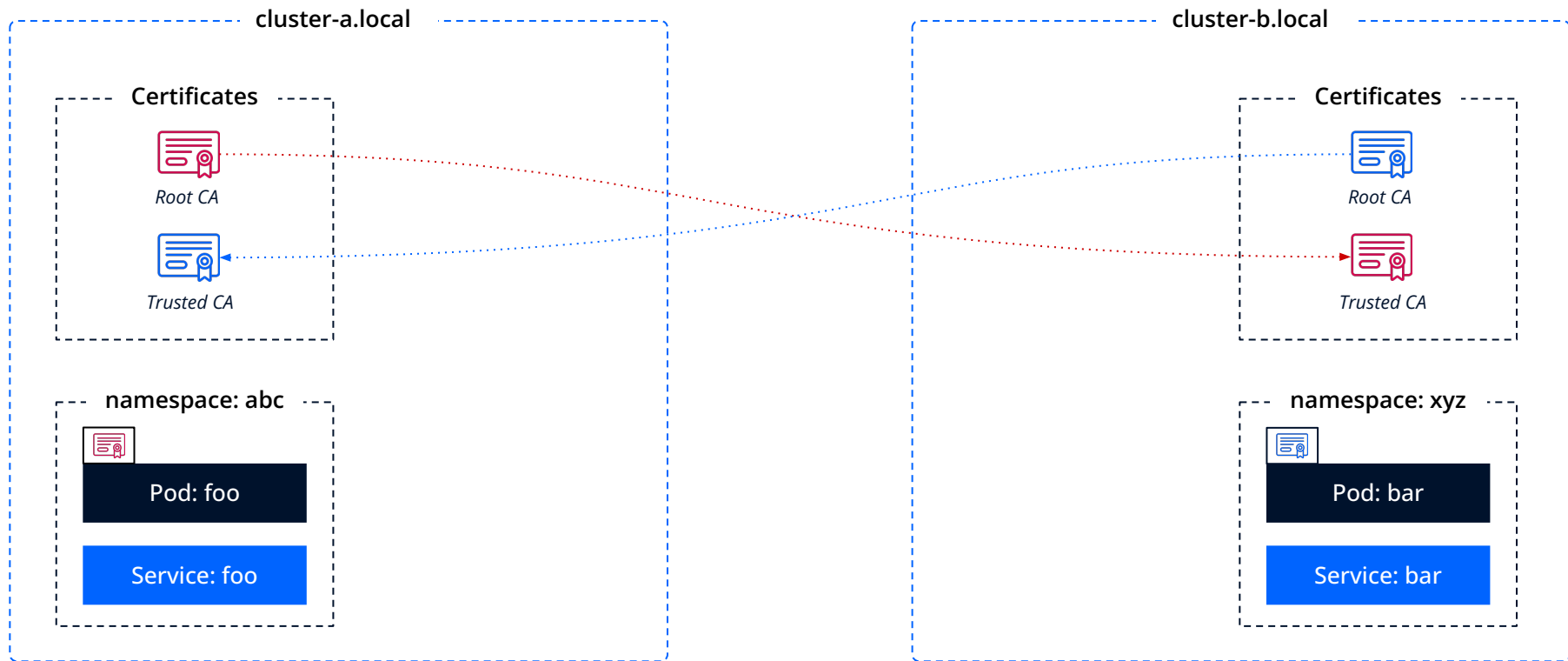
namespace: xyz



Pod: bar

Service: bar

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



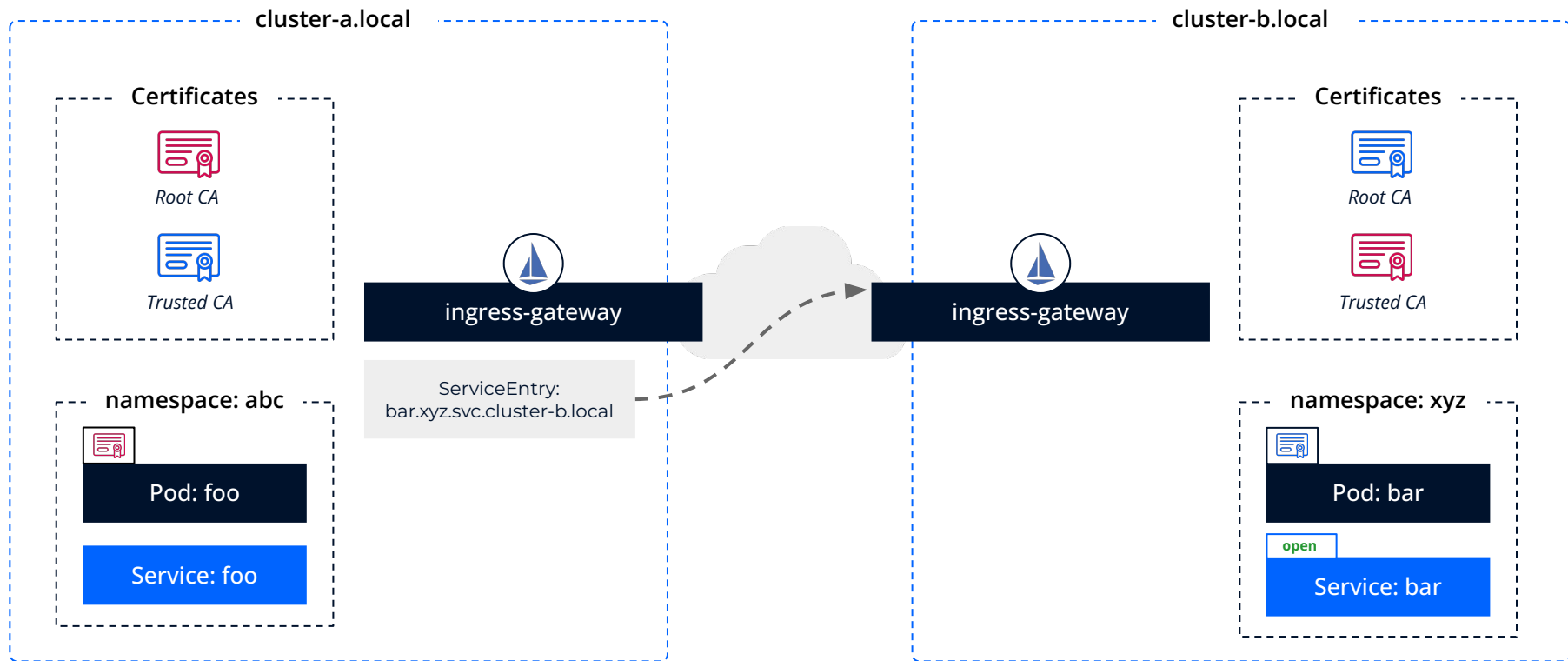
Для обеспечения взаимного доверия необходимо взаимно обменяться корневыми сертификатами и поместить их в хранилище доверенных сертификатов.



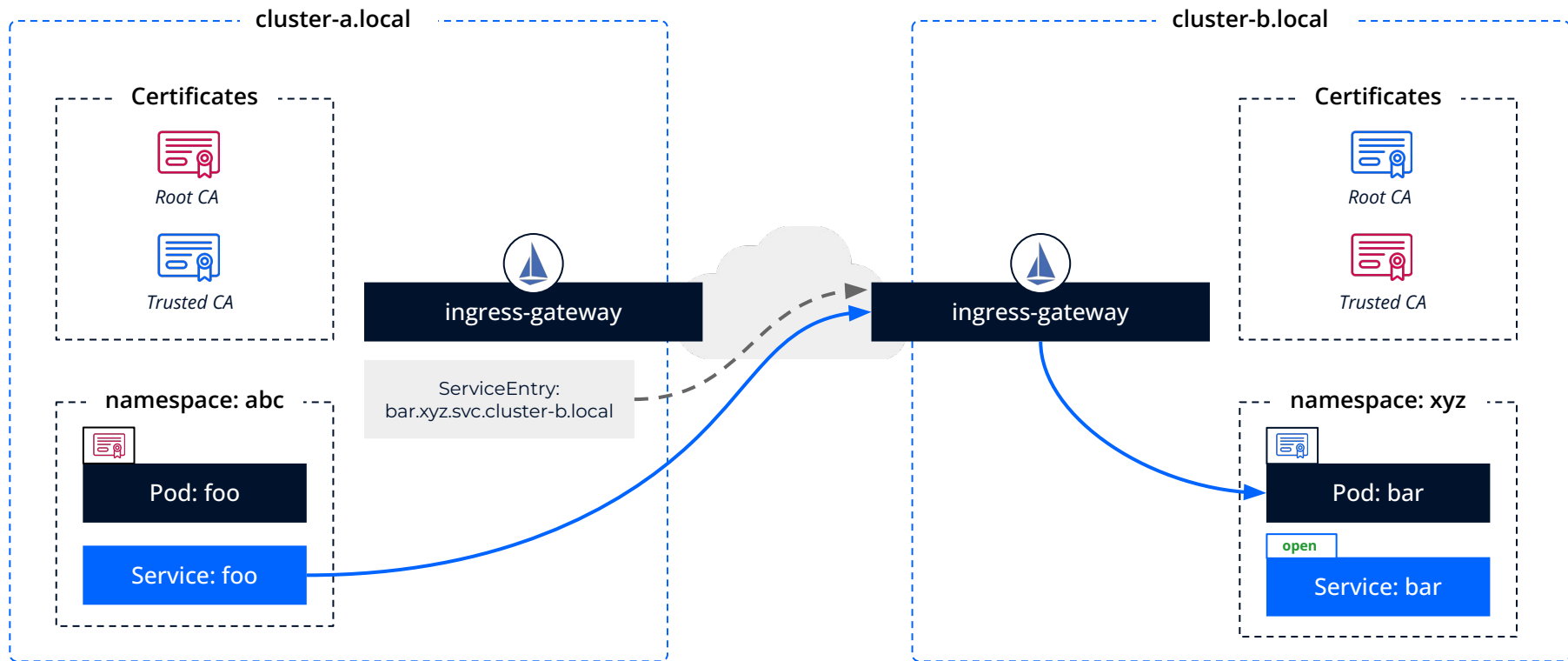
У каждого кластера есть ingress-gateway, который позволяет принимать Mutual TLS запросы извне кластера.



Мы используем эти ingress-gateway чтобы предоставить доступ к сервису
внешним кластерам в рамках федерации.



Теперь достаточно создать ресурс **ServiceEntry**, который зарегистрирует в кластере **cluster-a** удалённый сервис **bar.xyz.svc.cluster-b.local** и опишет координаты **ingress-gateway** кластера, через который можно обратиться к сервису.



Таким образом, федерация налажена и сервисы в разных кластерах доступны друг другу со всеми преимуществами общего Service Mesh.