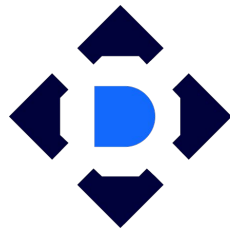
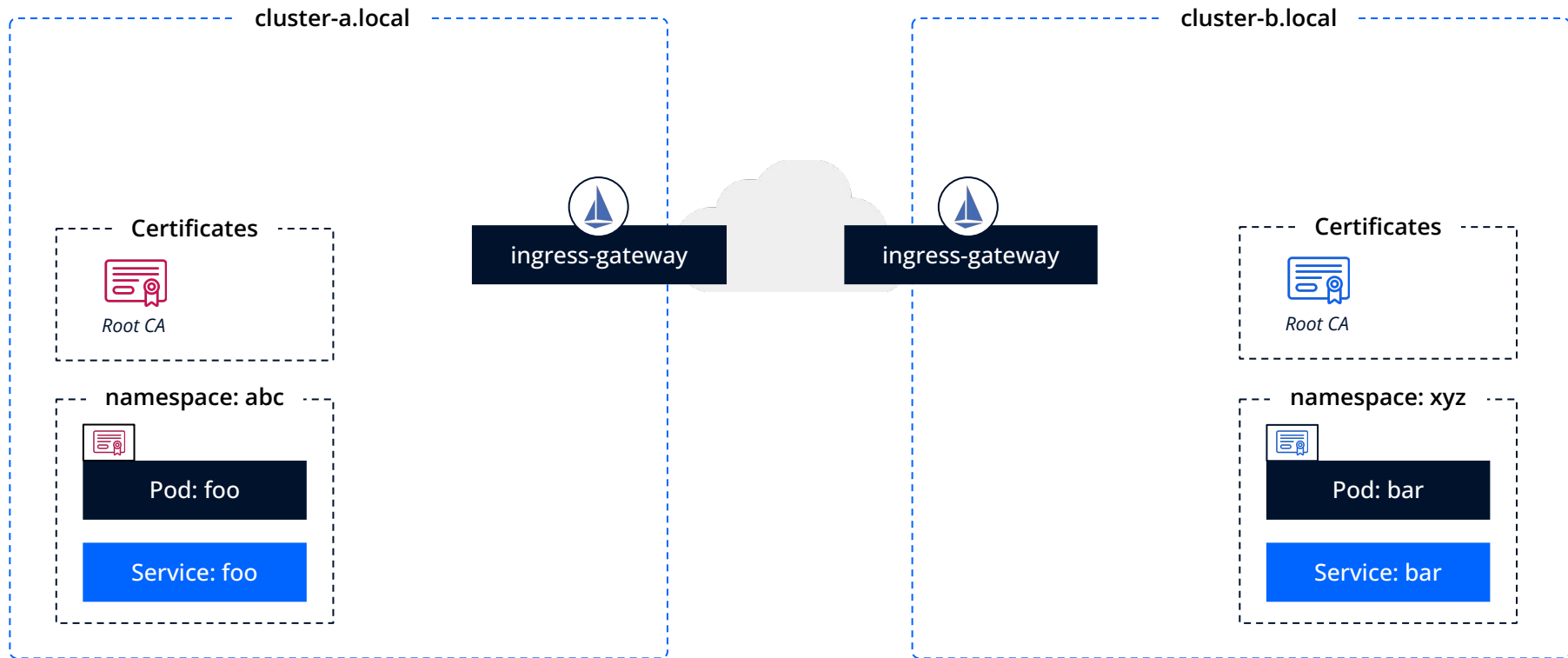


Istio
Федерация
IstioFederation

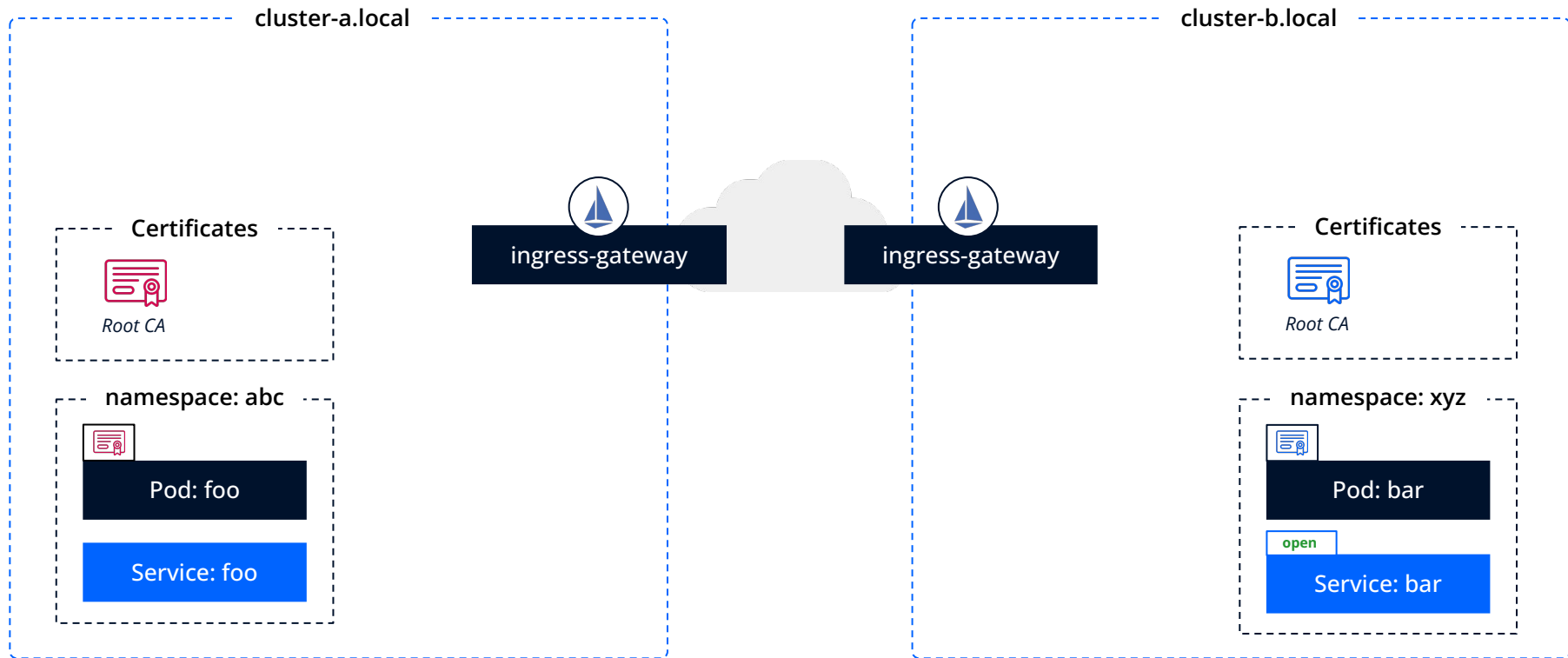


FLANT

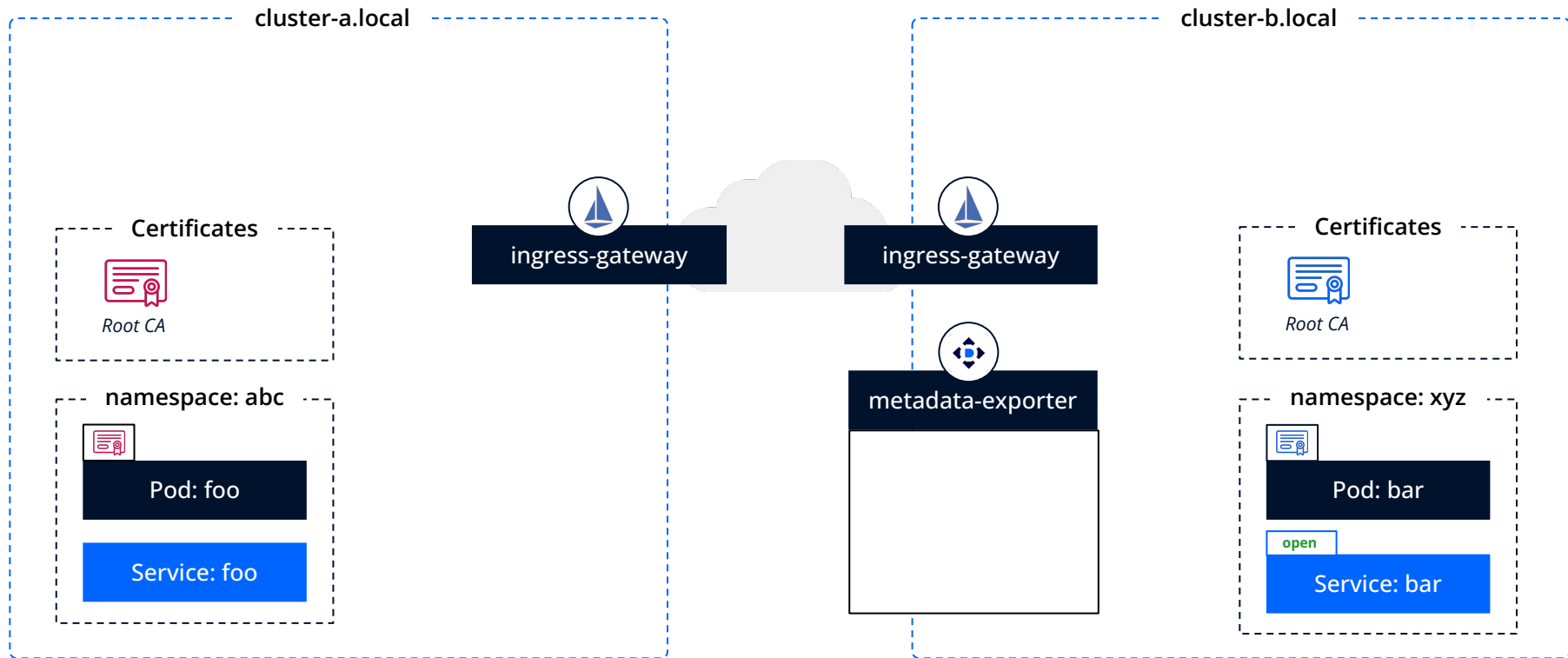
Deckhouse
Kubernetes Platform



Имеем два суверенных кластера, в которых работают приложения. У каждого кластера свой корневой istio-сертификат, которым подписаны индивидуальные сертификаты подов для нужд Mutual TLS.

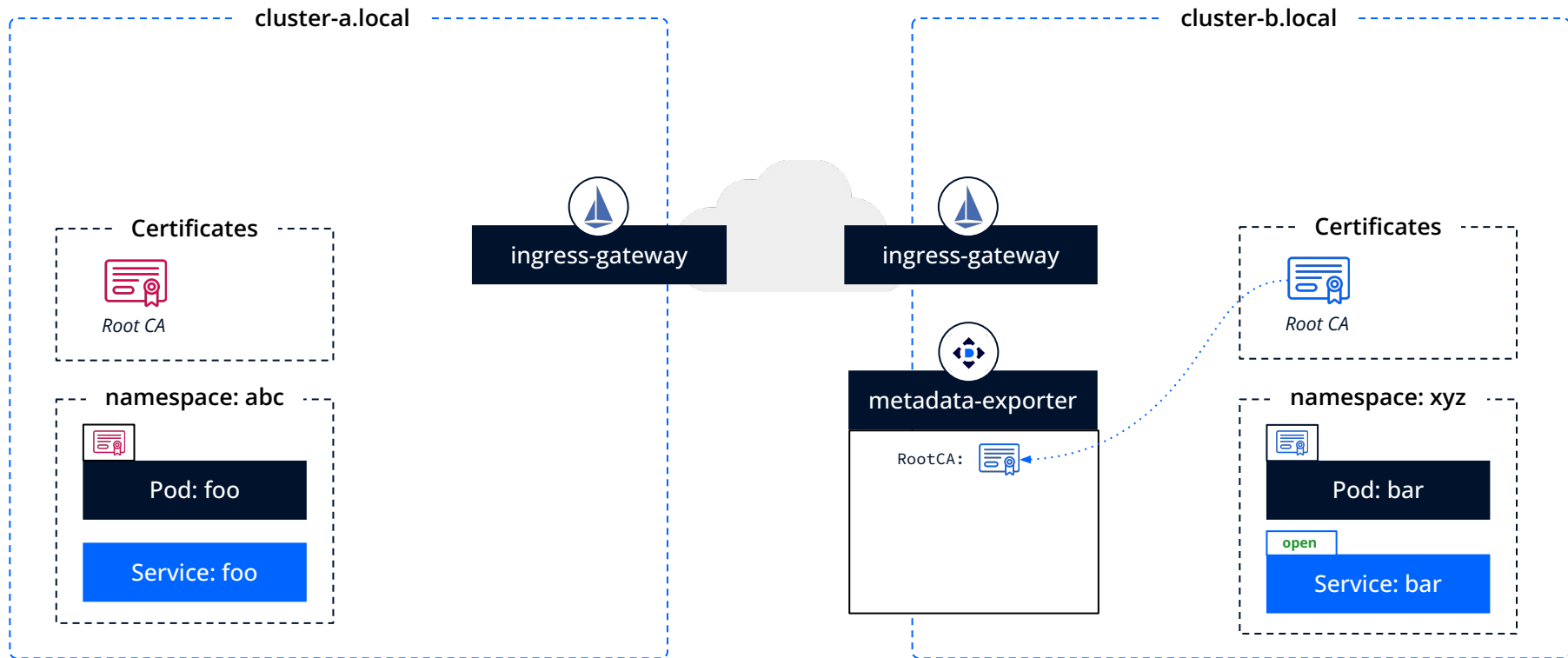


Требуется наладить федерацию и расшарить между кластерами сервис `bar.xyz.svc.cluster-b.local`, для этого включаем параметр модуля `istio.federation.enabled = true`.

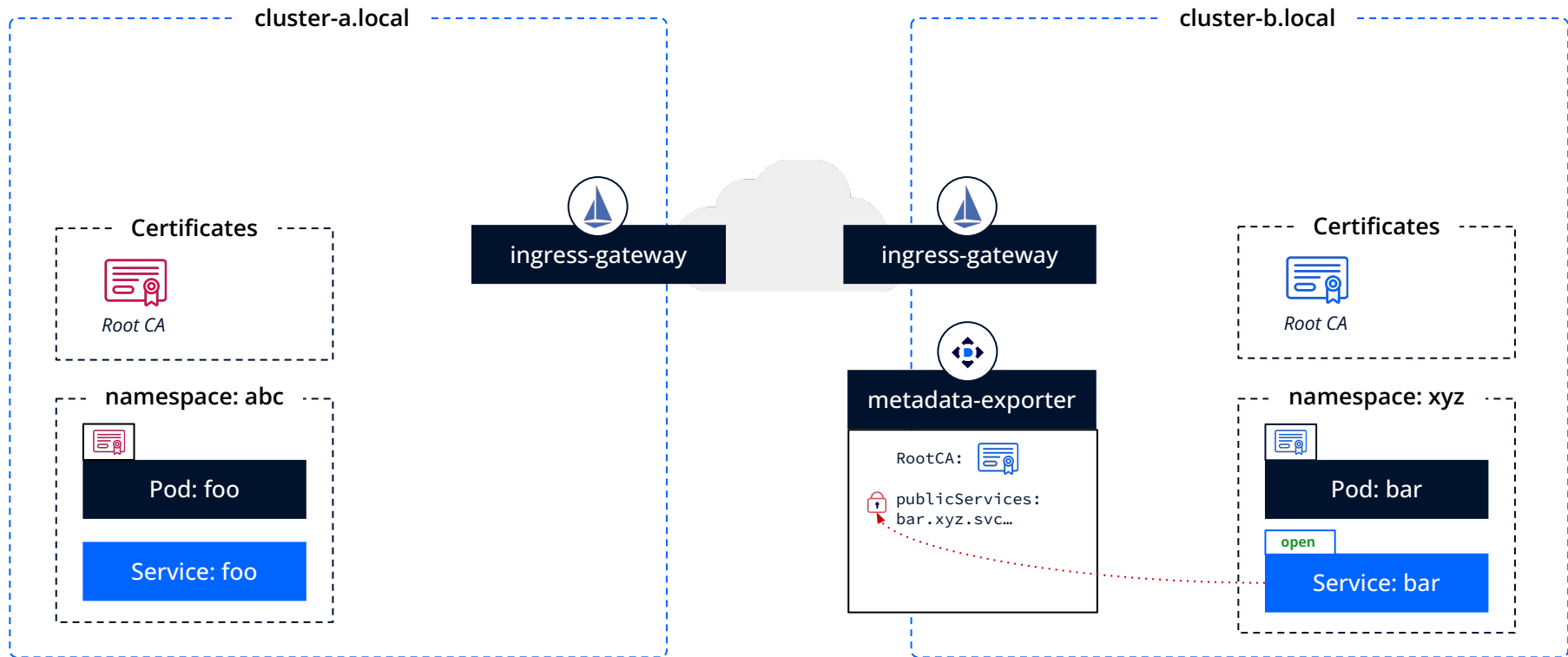


Специальный компонент metadata-exporter собирает и публикует метainформацию...

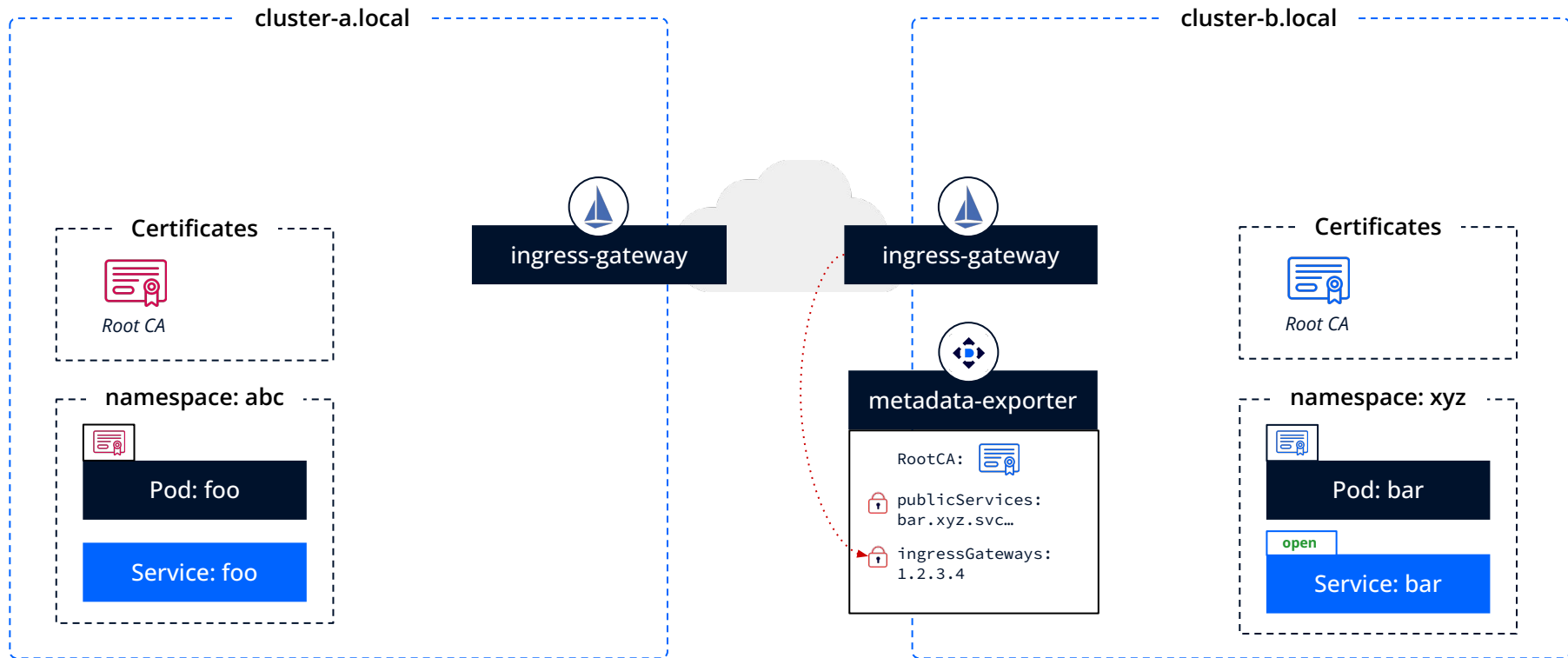
(для примера проиллюстрируем только на кластере cluster-b.local, действие происходит на обоих кластерах)



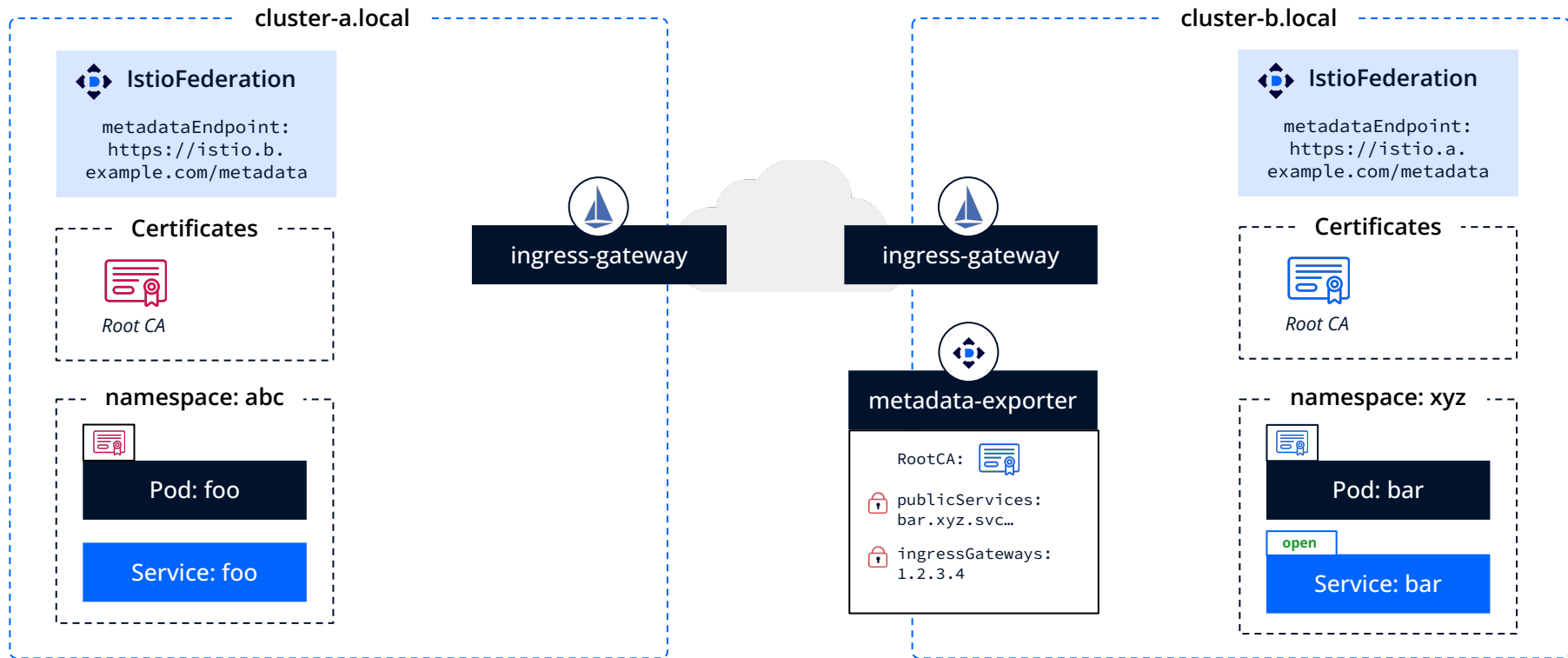
публичную часть корневого istio-сертификата...



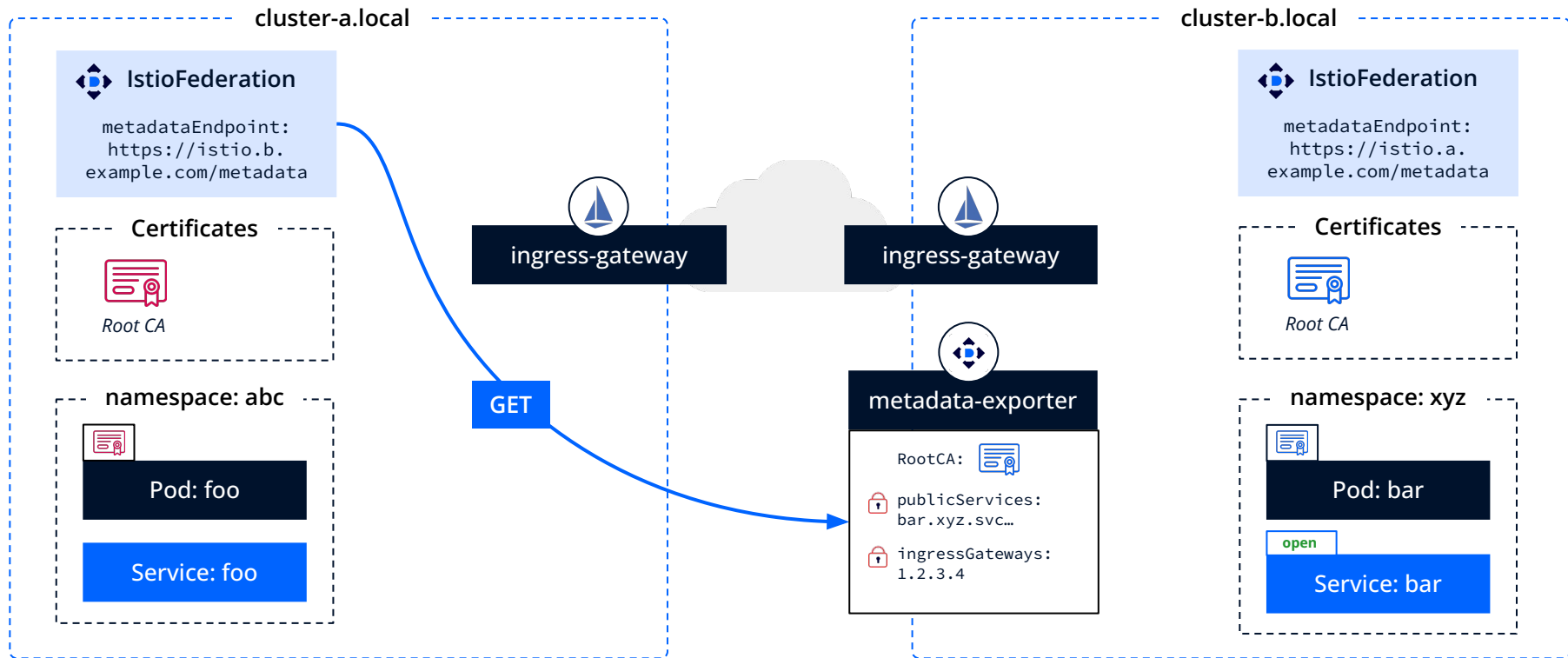
список публичных сервисов (доступен только из кластеров в федерации)...



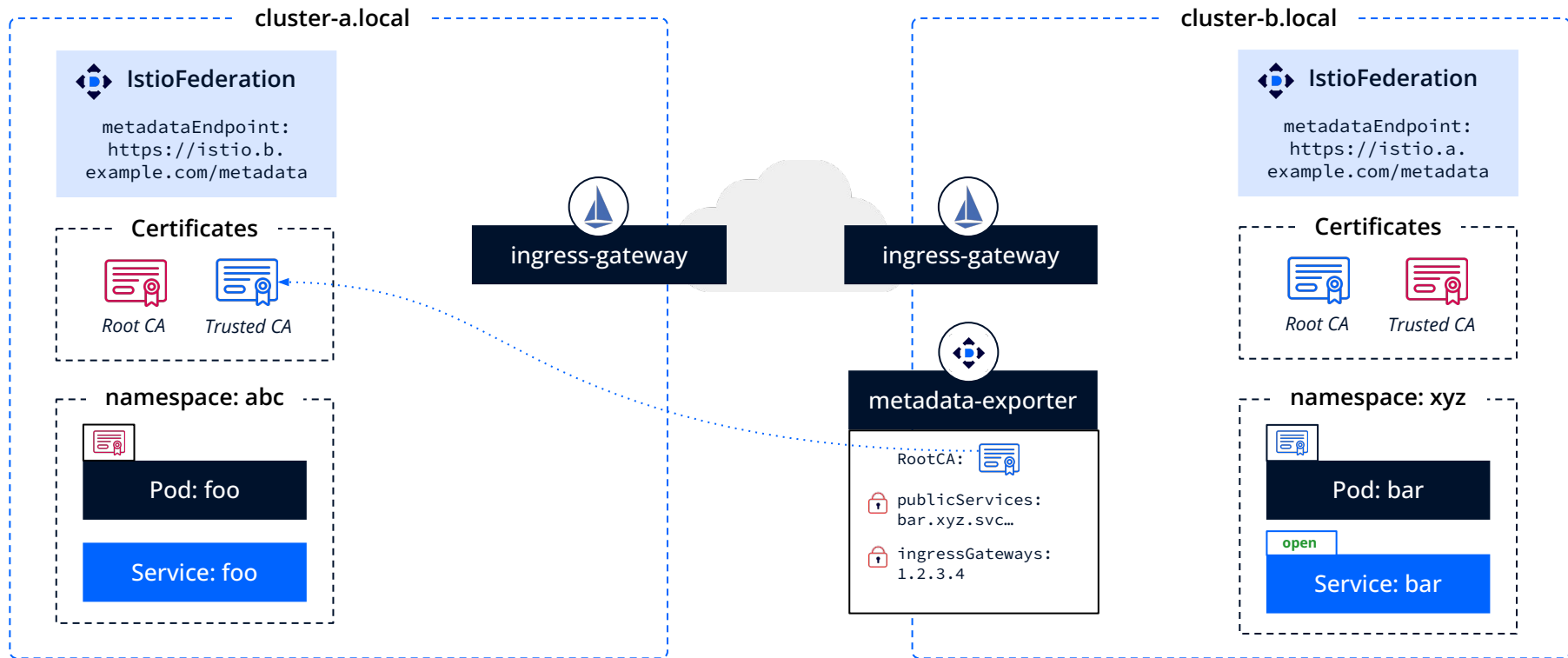
и публичные адреса компонентов ingress-gateway (доступны только из кластеров в федерации).



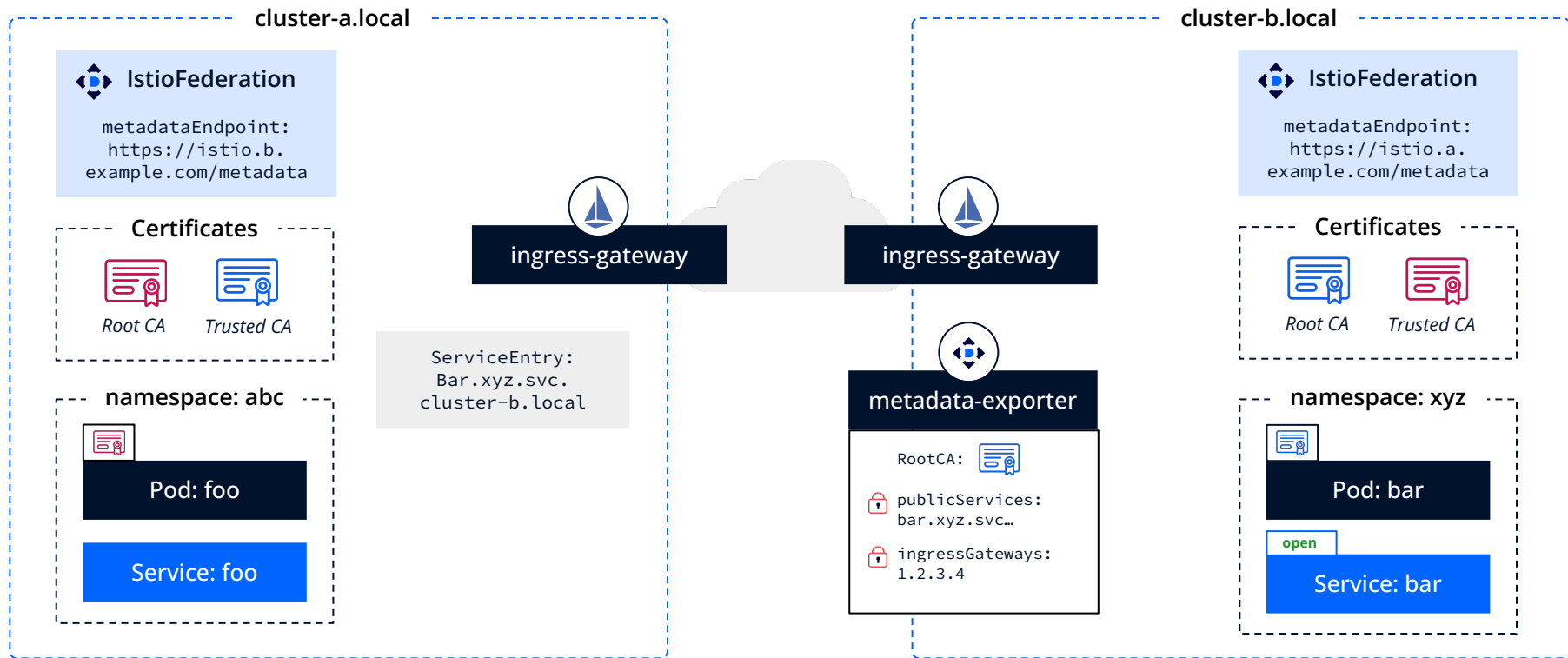
На кластерах взаимно создаются ресурсы IstioFederation, которые обозначают координаты с метаданными удаленного кластера, далее организация федерации происходит автоматически...



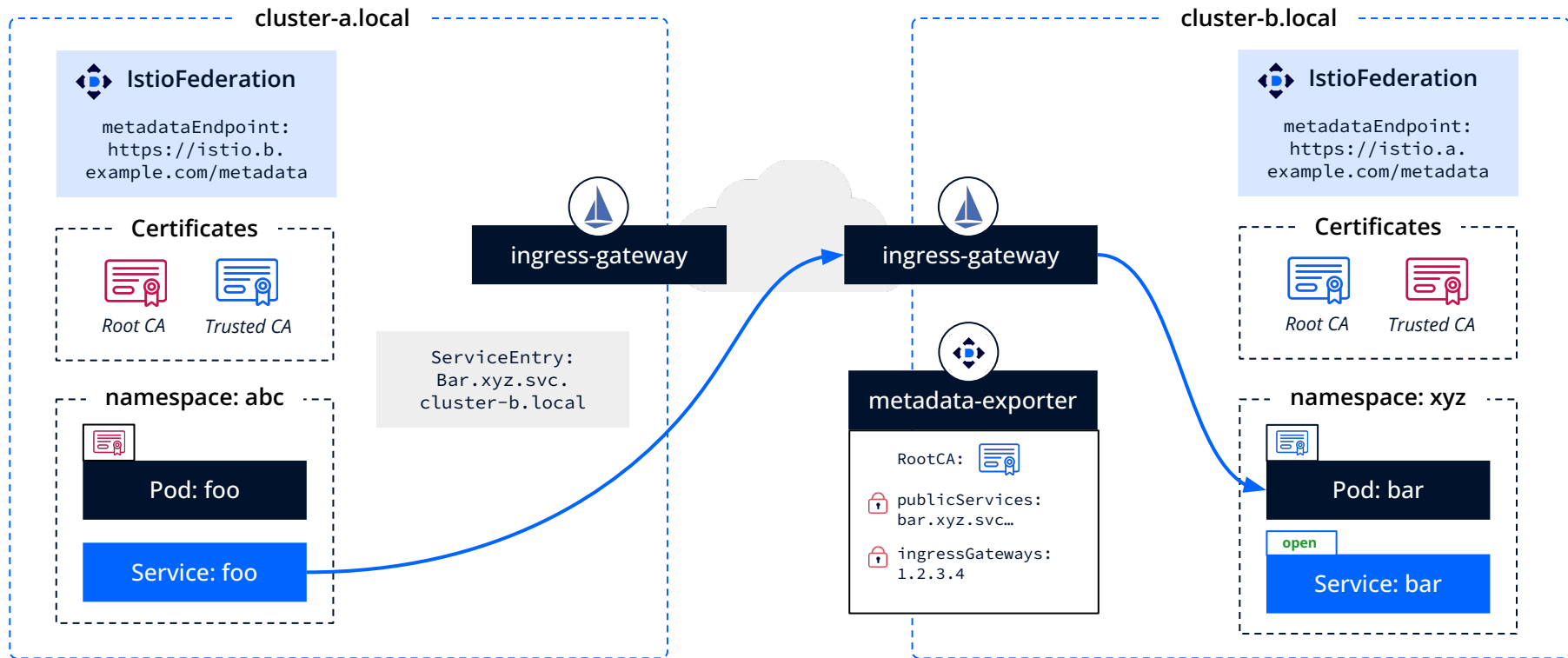
Deckhouse собирает удаленные метаданные...



скачивает публичный корневой сертификат и обменивается ключами
для доступа к закрытым метаданным...



скачивает информацию о публичных сервисах удаленного кластера и об адресах ingress-gateway, через которые эти сервисы доступны. На основе этих данных для каждого публичного сервиса он создает ресурсы ServiceEntry для регистрации удаленных сервисов на локальном кластере



Таким образом, федерация налажена и в ее рамках доступен публичный сервис `bar.xyz.svc.cluster-b.local`.