Deckhouse
Kubernetes Platform

Istio

Федерация
IstioFederation

cluster-a.local

Certificates

Root CA

namespace: abc

Pod: foo

Service: foo

Cloud

Ingress-gateway

Ingress-gateway

cluster-b.local

Certificates

Root CA

namespace: xyz

Pod: bar

Service: bar

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

cluster-a.local

Certificates

Root CA

namespace: abc

Pod: foo

Service: foo

Cloud

Ingress-gateway

Ingress-gateway

cluster-b.local

Certificates

Root CA

namespace: xyz

Pod: bar

open

Service: bar

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

cluster-a.local

Certificates

Root CA

namespace: abc

Pod: foo

Service: foo

Cloud

Ingress-gateway

Ingress-gateway

metadata-exporter

cluster-b.local

Certificates

Root CA

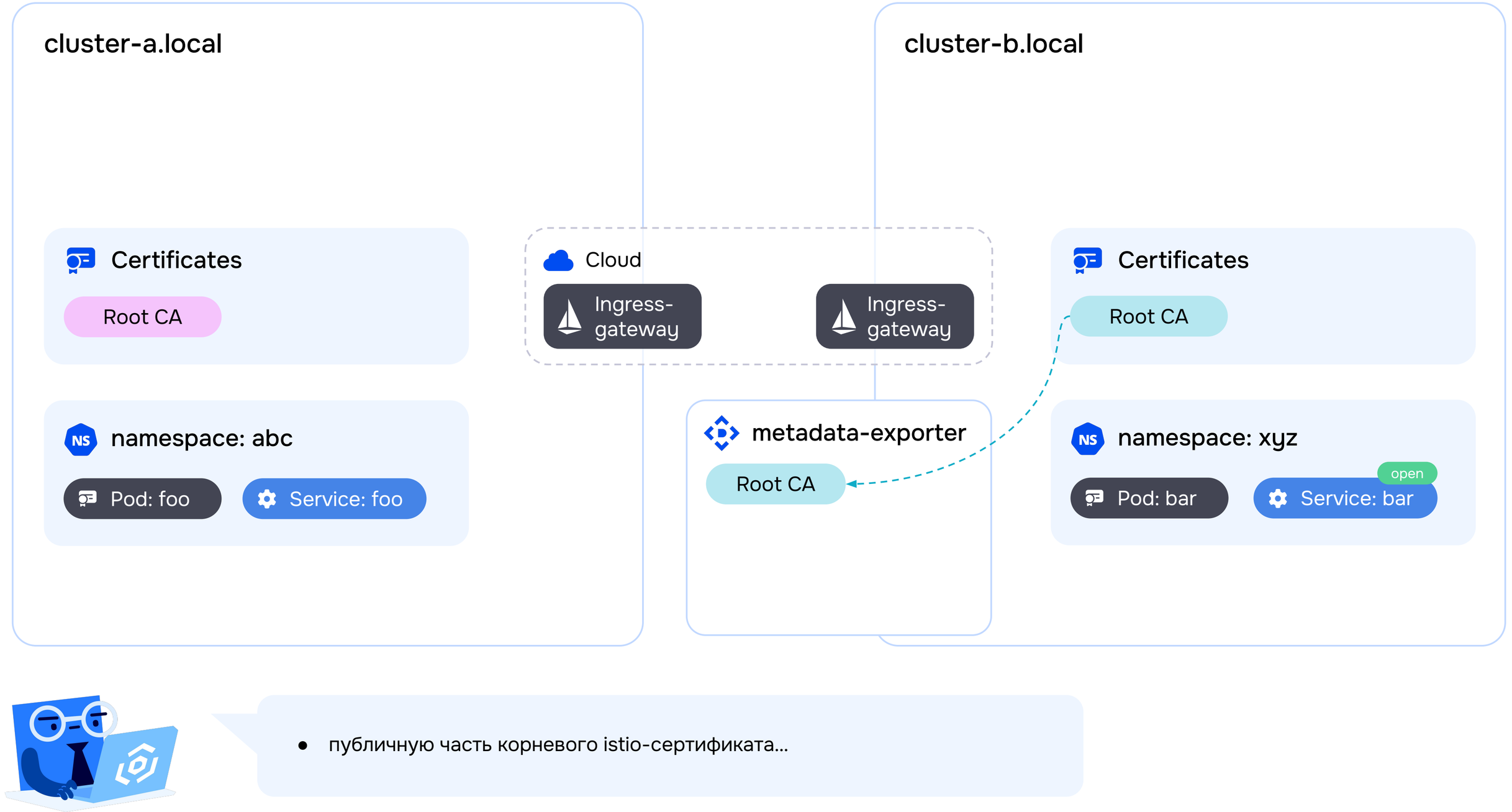
namespace: xyz

Pod: bar

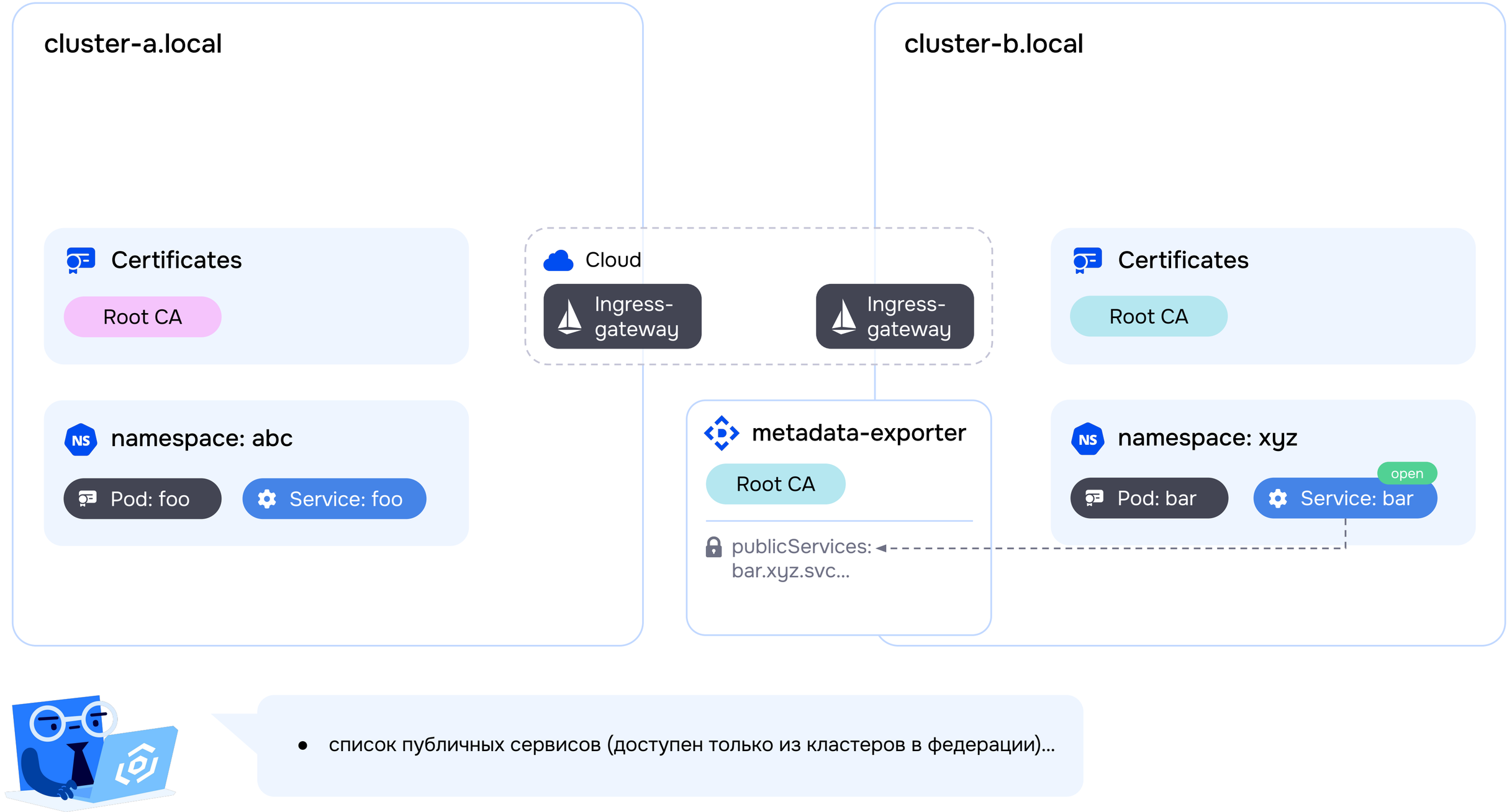
open

Service: bar

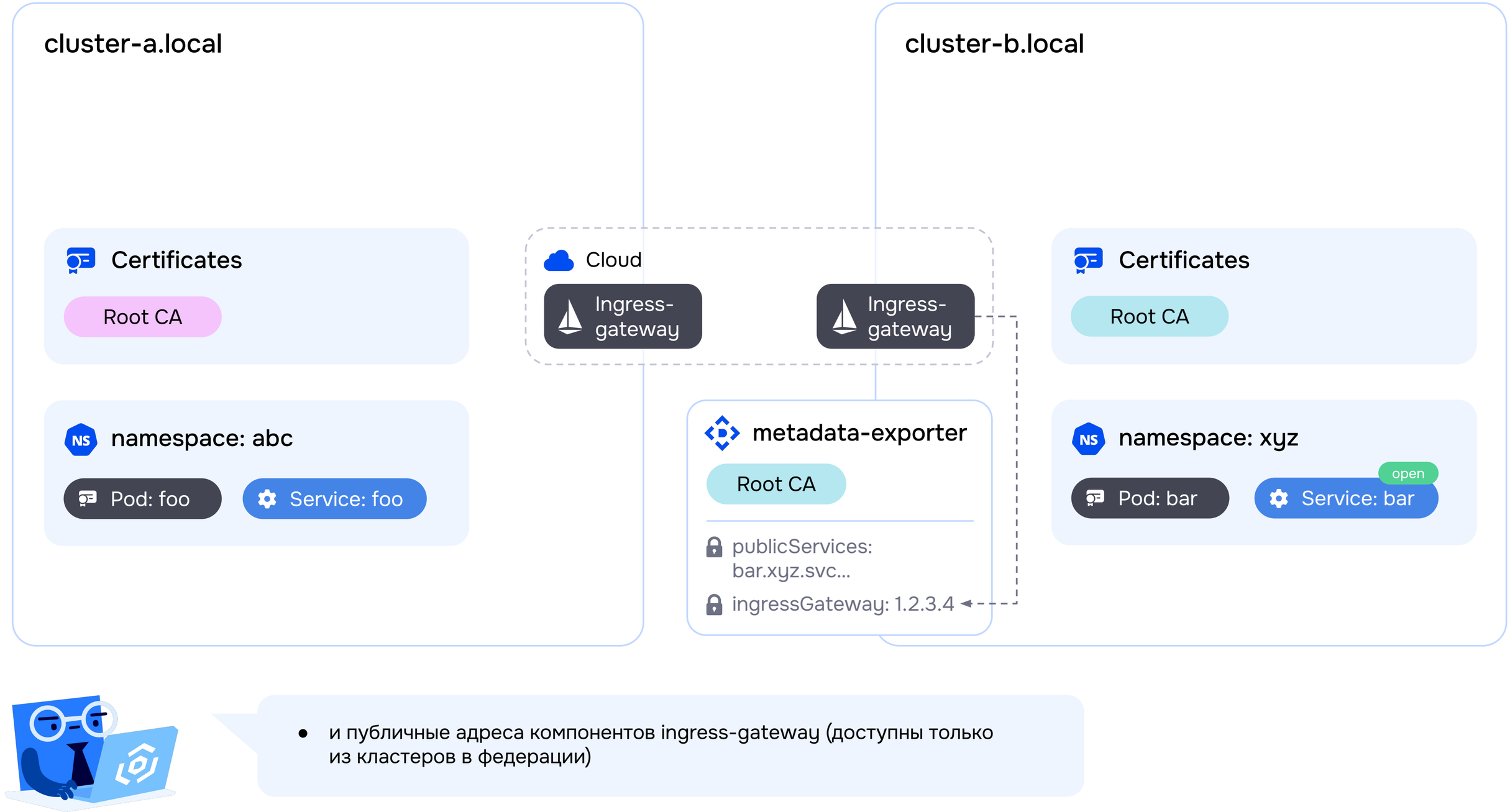
Специальный компонент metadata-exporter собирает и публикует метаинформацию... (для примера проиллюстрируем только на кластере cluster-b.local, действие происходит на обоих кластерах)



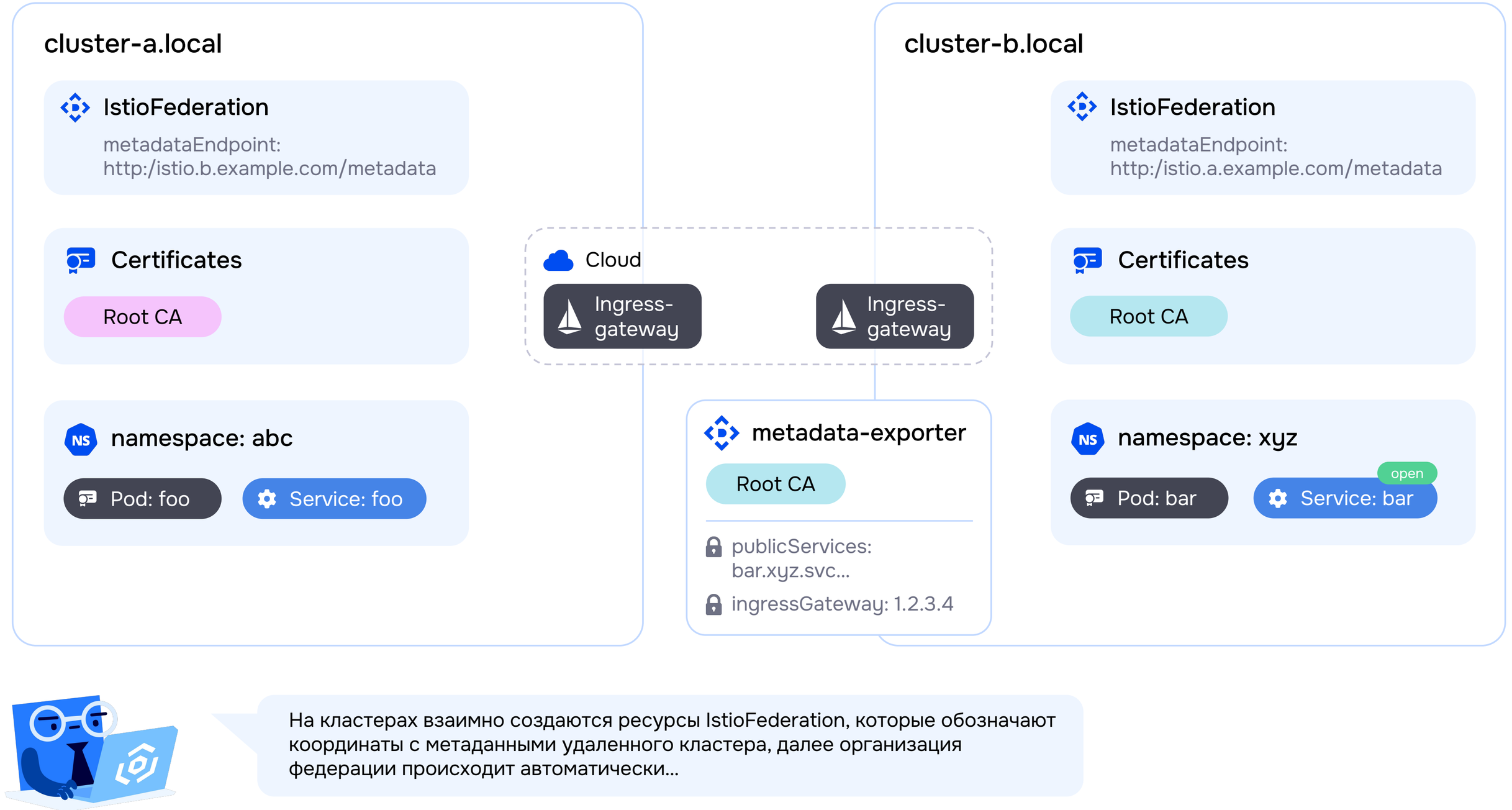
- публичную часть корневого istio-сертификата...



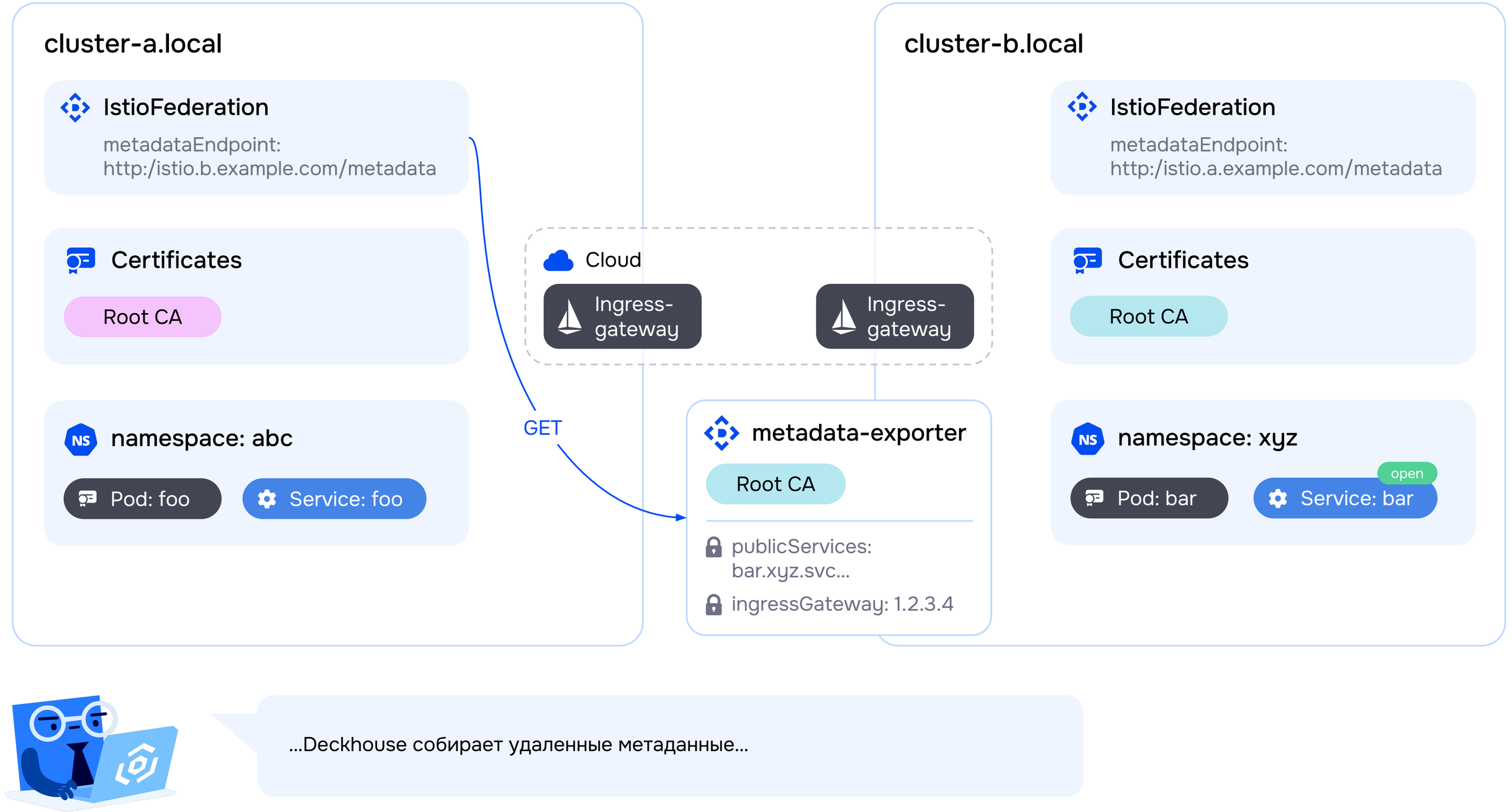
- список публичных сервисов (доступен только из кластеров в федерации)...



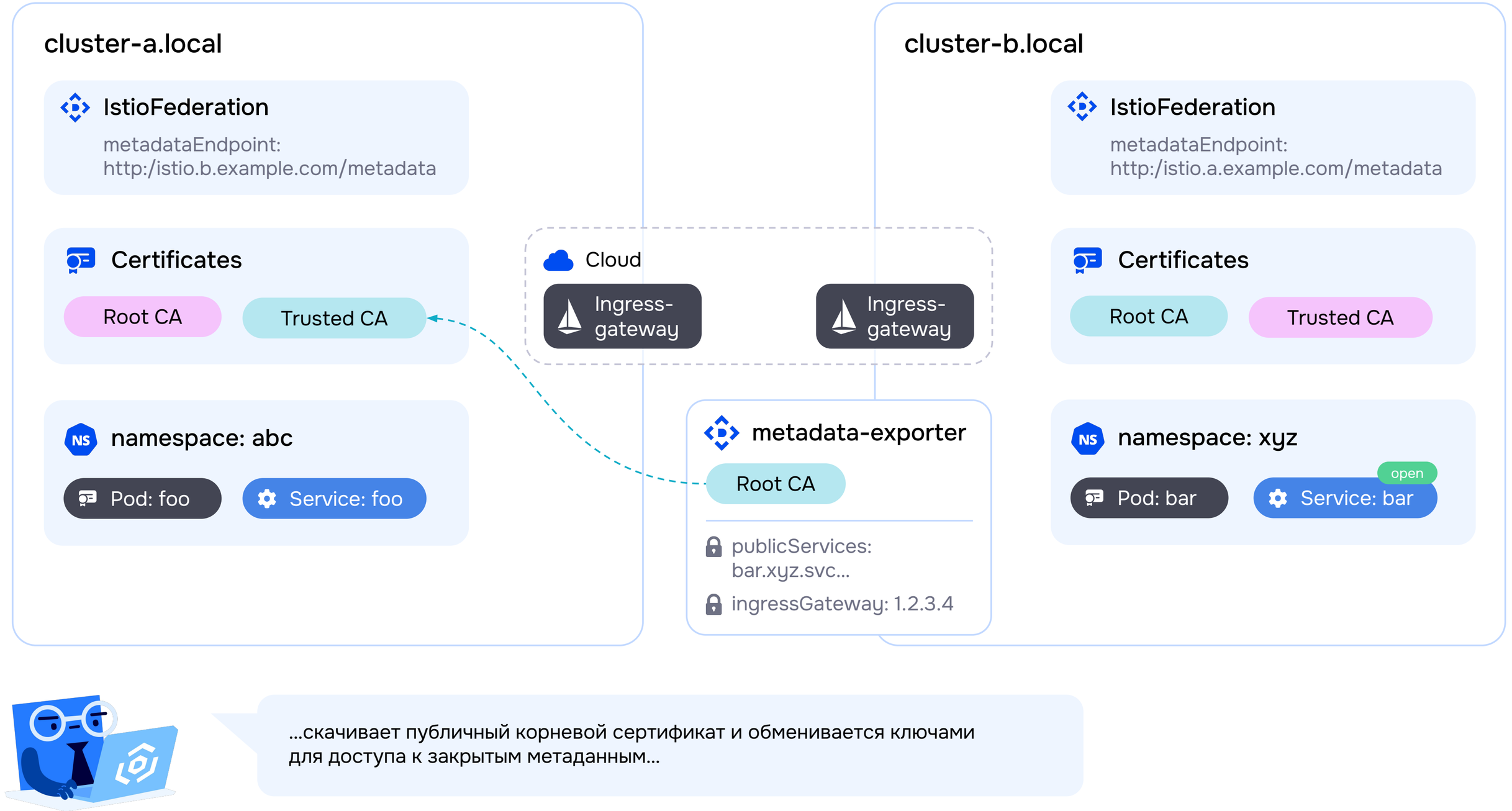
- и публичные адреса компонентов ingress-gateway (доступны только из кластеров в федерации)



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...

cluster-a.local

IstioFederation

metadataEndpoint:
http:/istio.b.example.com/metadata

Certificates

Root CA

Trusted CA

namespace: abc

Pod: foo

Service: foo

ServiceEntry: Bar.xyz.svc.cluster-b.local

Cloud

Ingress-gateway

Ingress-gateway

metadata-exporter

Root CA

publicServices:
bar.xyz.svc...

ingressGateway: 1.2.3.4

cluster-b.local

IstioFederation

metadataEndpoint:
http:/istio.a.example.com/metadata

Certificates

Root CA

Trusted CA

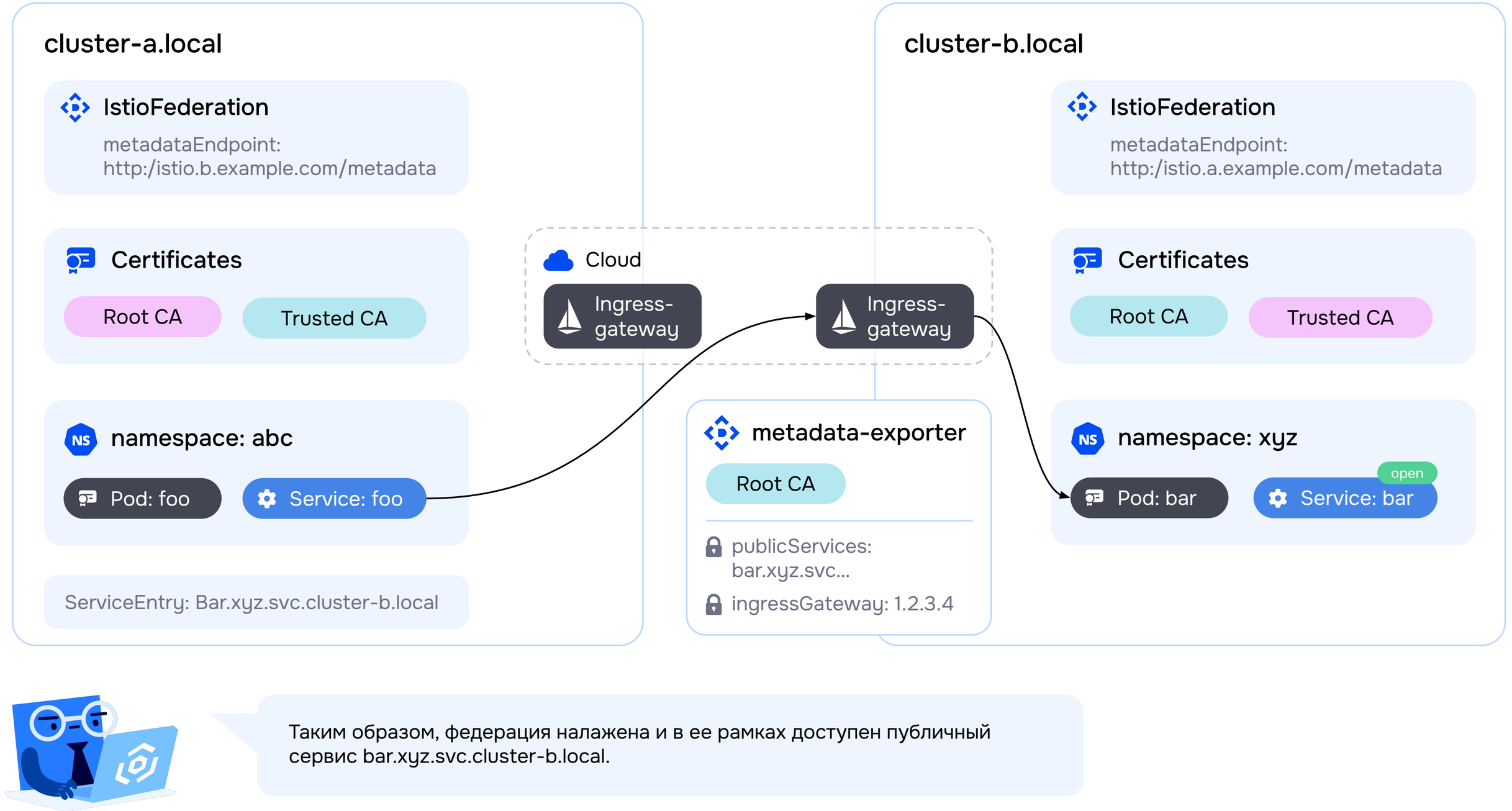
namespace: xyz

Pod: bar

open

Service: bar

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.