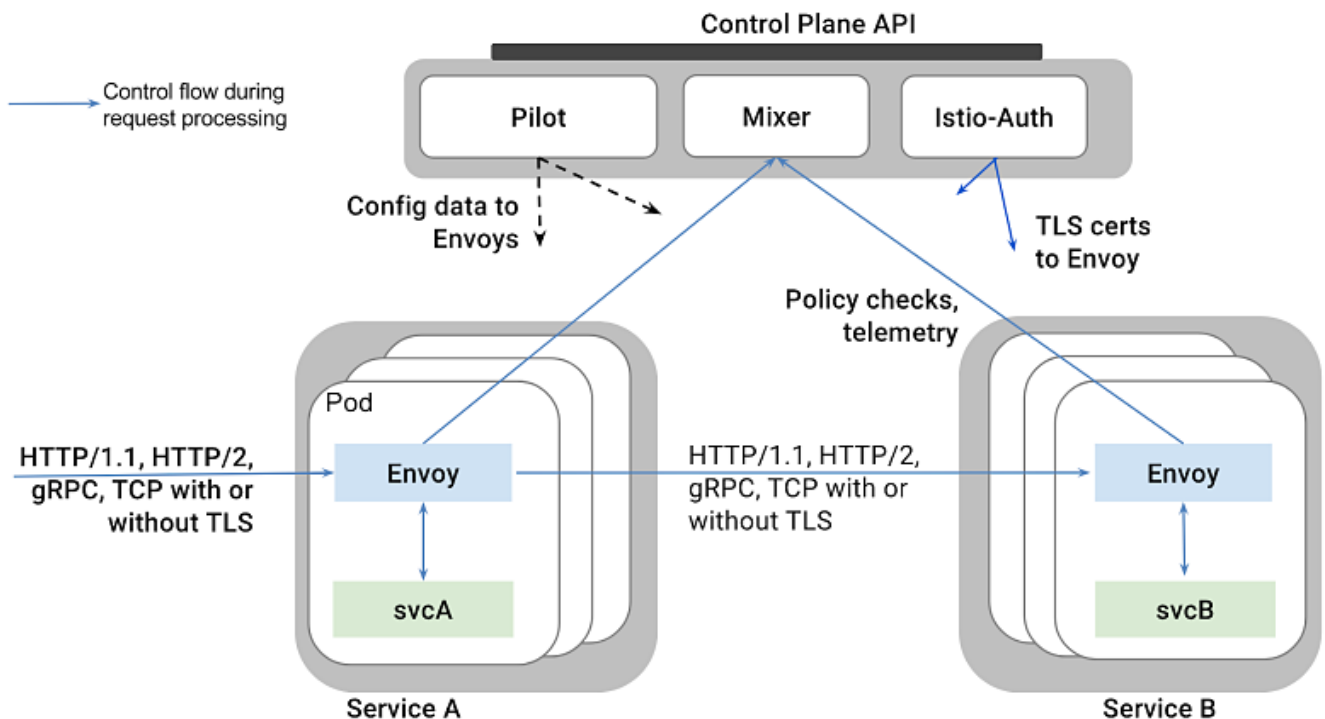


istio

info

- patrón sidecar (aislamiento y encapsulación)
- proxy:
 - (Envoy) que controla todas las comunicaciones del pod
 - notifica a «control»:
 - Mixer: métricas
 - Pilot: información a los proxies de los pods: registro y configuraciones
 - Istio-Auth: certificados para las comunicaciones TLS



proxy envoy

- intercepta todo el tráfico
- se comunica con control

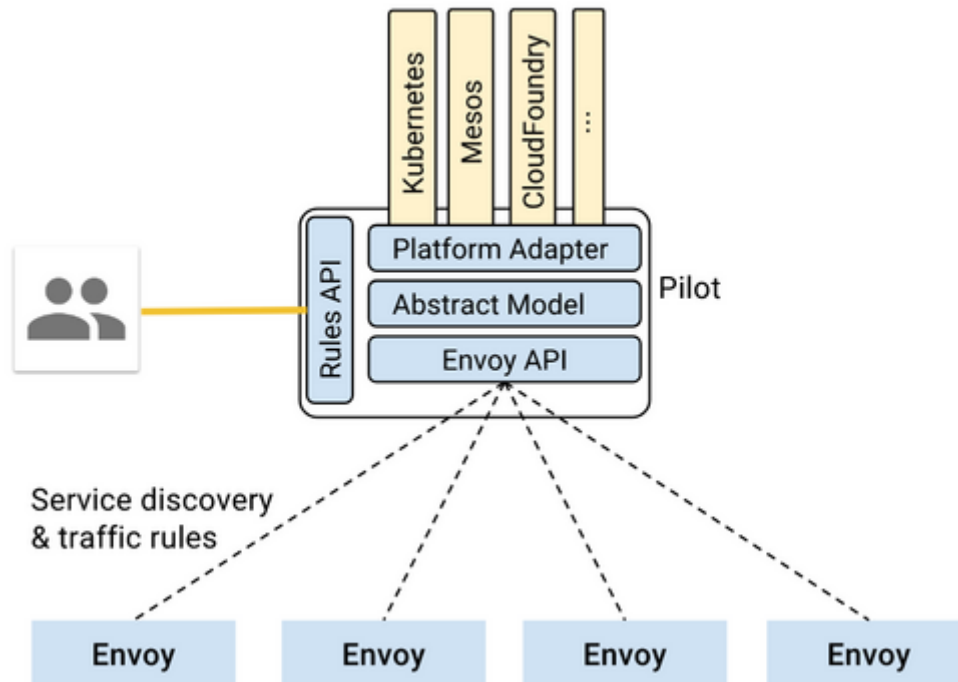
mixer

- control de acceso y recepción de métricas
- no se acopla a la aplicación (servicio)
- adaptadores o plugins para interactuar con diferentes sistemas: Prometheus, AWS, GCP
- proporciona API unificada sea cual sea la herramienta que haya debajo
- funcionalidades:
 - verificación de precondiciones:
 - comprobación de poder realizar llamadas a los servicios
 - restricciones: autenticación, lista negras, ...
 - gestión de cuota:
 - si un servicio destino dispone de recursos limitados, garantiza una distribución justa entre los llamantes

- informe de telemetría:
 - logs y monitorización

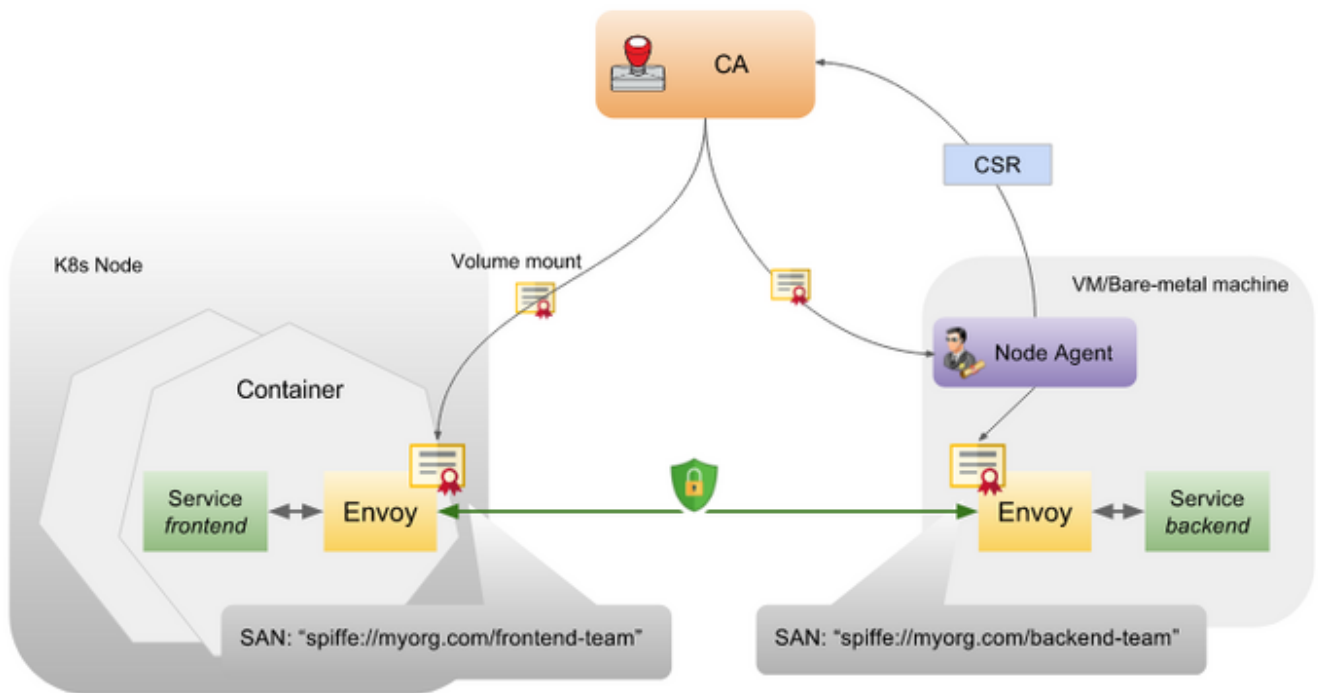
pilot

- gestiona registros de servicios, enrutado y resiliencia¹⁾
- desde aquí se gestionan esas configuraciones que serán transmitidas a los proxies Envoy
- abstracción de la plataforma (Kubernetes, CloudFoundry, Mesos)



istio-auth

- securiza la comunicación entre servicios y usuario final via TLS
- se identifica quien a invocado a quien, pudiendo establecer políticas de acceso en base a integridad en lugar de control de red
- genera, distribuye, rota y revoca claves y certificados



- características:
 - identidad: usando las **service accounts** de Kubernetes, identifica quien ejecuta un servicio. El identificador de una **service account** es **spiffe:///<namespace>/<service_account>/******, correspondiendo en **namespace** al proyecto/namespace en el que se ejecutan los servicios. Nos da potencia por su flexibilidad para identificar máquinas, usuarios, procesamientos, etc
 - comunicación segura, securizando los proxies Envoy:
 - los servicios se comunican solo a través de conexiones locales TCP
 - los proxies se comunican usando TLS (ambos)
 - durante el handshake, se comprueba que la **service account** identificada en el certificado del servidor tiene permisos
 - gestión de claves: lleva toda la gestión de claves y certificados

docs

- <https://www.paradigmadigital.com/dev/jugando-con-istio-the-next-big-thing-en-microservicios-1-2/>

¹⁾
Capacidad de un material, mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que había estado sometido.

From:
<https://matebcn.eu/> - miguel angel torres egea

Permanent link:
<https://matebcn.eu/tech:istio:start>

Last update: 07/04/2020 15:18

