Google

Istio contributor workshop

Taller para contribuidores de Istio

CCOSS

Rodrigo Caballero

Ingeniero de contenidos

Istio Docs WG Maintainer

GitHub: rcaballeromx

Email: grca@google.com

Google

CC SS

Lee Calcote

Founder, Layer5

Twitter: lcalcote

LinkedIn: leecalcote

Talks: calcotestudios.com/talks

GitHub: leecalcote

Email: lee@calcotestudios.com

Visit Layer5.io
the service mesh company

Try Meshery
the multi-mesh manager

Agenda

- Introduciendo Istio
- Usando Istio
- Contribuyendo a Istio

Google

Introduciendo Istio

Conecta, asegura y monitorea tus servicios y sistemas híbridos.

CCOSS

¿Qué es Istio?

01

¿Qué es una malla de servicios?

Una malla de servicio ofrece una manera **transparente** e **independiente del lenguaje** de **automatizar** sencilla- y flexiblemente las funcionalidades de la red para aplicaciones.

¿Qué es Istio?

Una malla de servicios y más: Una **plataforma open source** para administrar **interacciones entre servicios** corriendo en **contenedores** y **máquinas virtuales**.

Visión de Producto

02

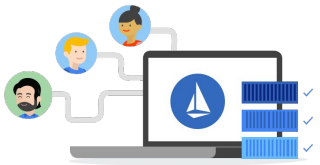
Google

El Valor de Istio

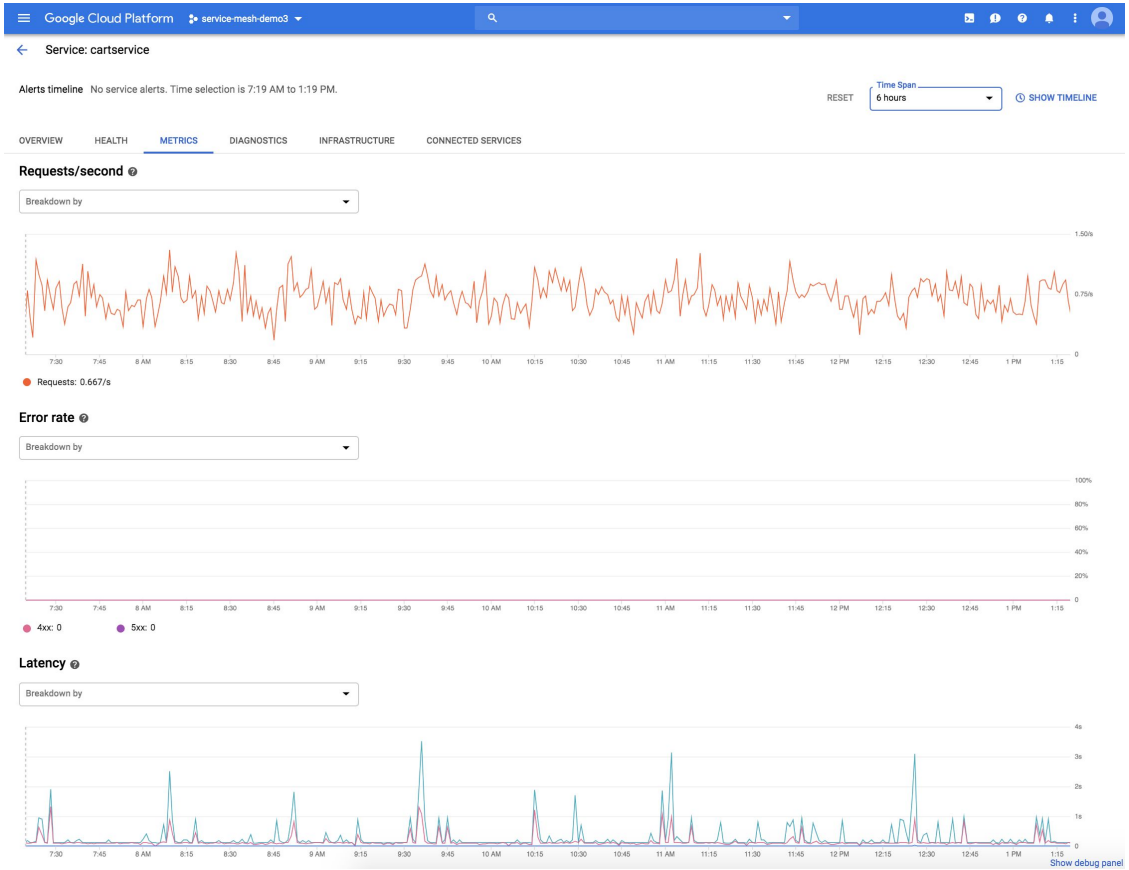
¿Qué ofrece Istio?

Observabilidad uniforme

Agilidad operacional



Políticas de Seguridad



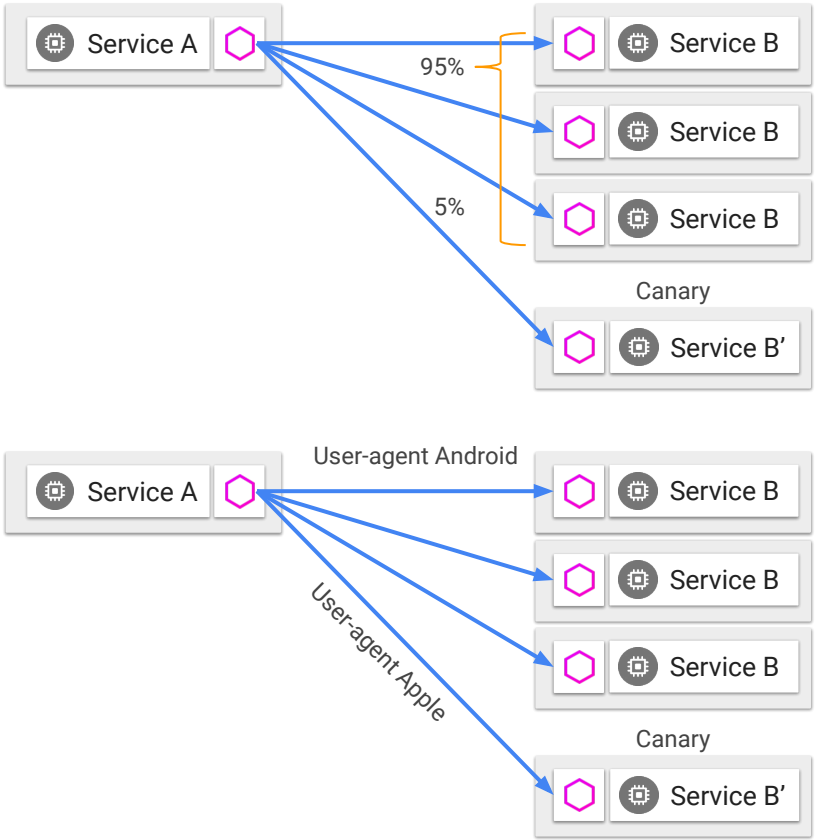
Observabilidad uniforme

- Recolecta las **señales principales** para cada servicio, rastreo y bitácoras para cada llamada
- Entiende los servicios y sus dependencias
- Establece, monitorea y aplica objetivos (SLOs) para los servicios
- Obtén una visión global del comportamiento de los servicios para identificar problemas, reducir el tiempo de detección

Google

Google Cloud

CCOSS



Agilidad operacional

Escala la distribución del tráfico hacia varias versiones

Publica nuevas versiones sin preocuparte de los retos operacionales

Aplica políticas de control de accesos y límite de frecuencia para proteger tus servicios de malos actores

Google

Google Cloud

CCOSS

Políticas de Seguridad

Defensa a fondo: seguridad que continúa incluso pasando el límite de la malla.

Activa TLS mutua para autenticación y encriptación más segura

Autoriza accesos basado en la identidad del servicio o cualquier atributo del canal

Configura los accesos al nivel de RPC para REST y gRPC de manera granular

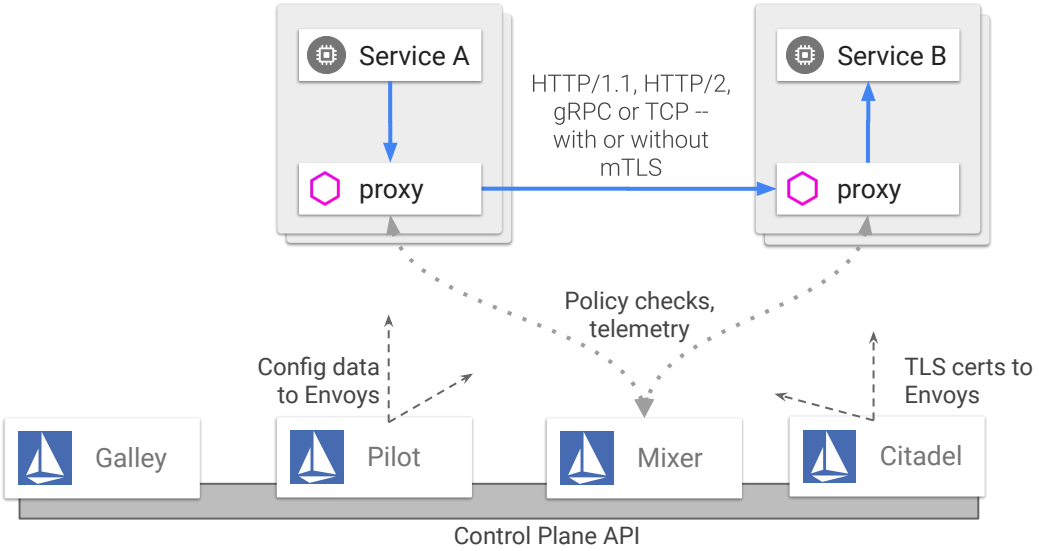
Arquitectura

03

Google

La Arquitectura de Istio

Pilot: Plano de control para configurar y mandar políticas de comunicación de servicios.
Mixer: Aplicación de políticas con un modelo flexible de enchufes para los proveedores de las políticas.
Citadel: Autorización de servicio-a-servicio (auth[n,z]) usando TLS mutua incluyendo administración de identidad y credenciales.
Galley: Valida la configuración del usuario por parte de los otros componentes del plano de control

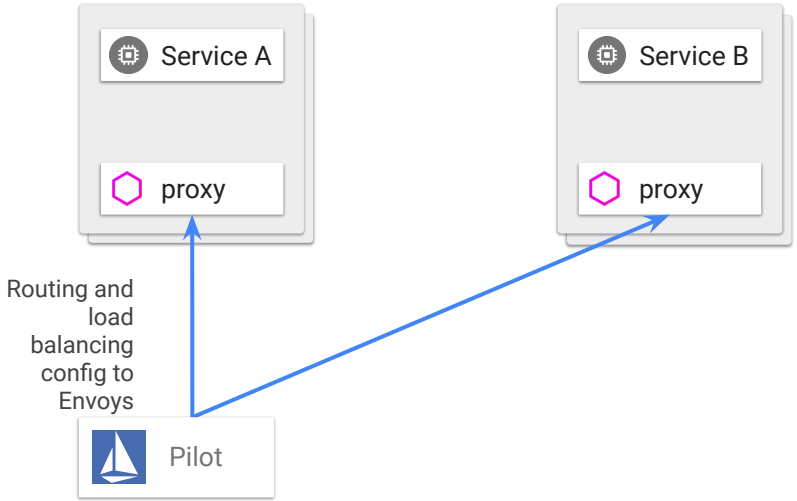


La magia del sidecar!

- Despliega sidecars con cada carga de trabajo
- Sirve de proxy para todo tráfico que entra y sale de un servicio
- Direcciona al tráfico (incluyendo las reglas de ruteo)
- Aplica las políticas
- Reporta telemetría
- Todo sin insertar una biblioteca de cliente

Pilot: configurando el plano de control

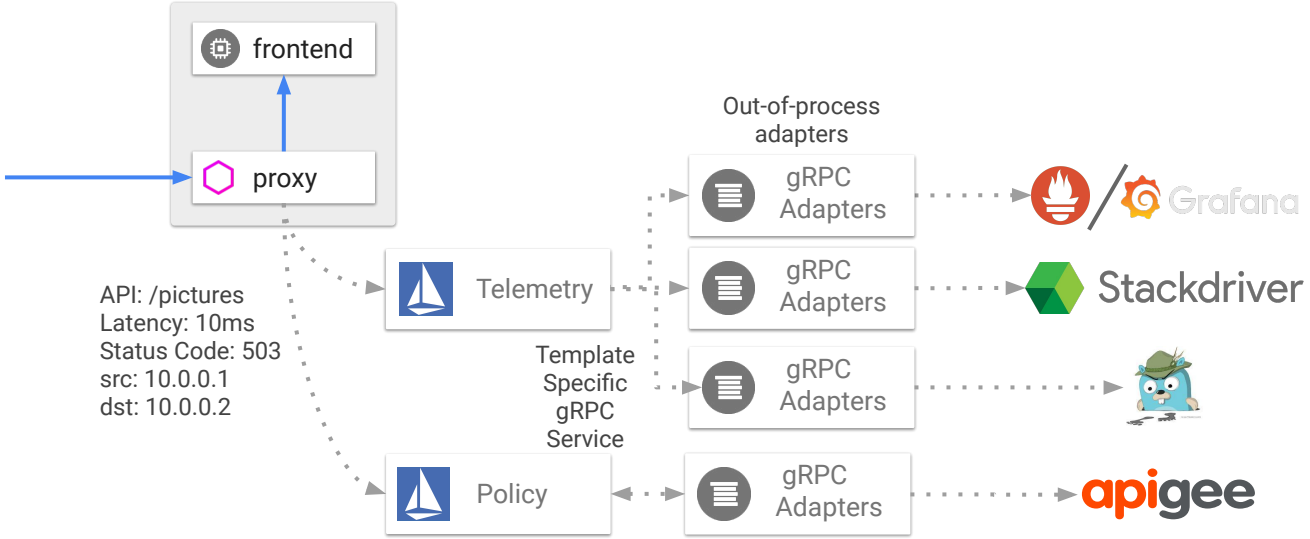
Pilot manda la información del registro de servicios y todas las reglas de ruteo a los Envoy proxys -- tanto en los sidecars como en la puerta de ingreso.



Mixer: Extensibilidad

El API open source de Mixer y su arquitectura enchufable permiten mandar telemetría, bitácoras y rastreos al sistema que prefieras.

Los adaptadores permiten una escalabilidad independiente para agregar backends sin necesidad de desplegar nuevamente.



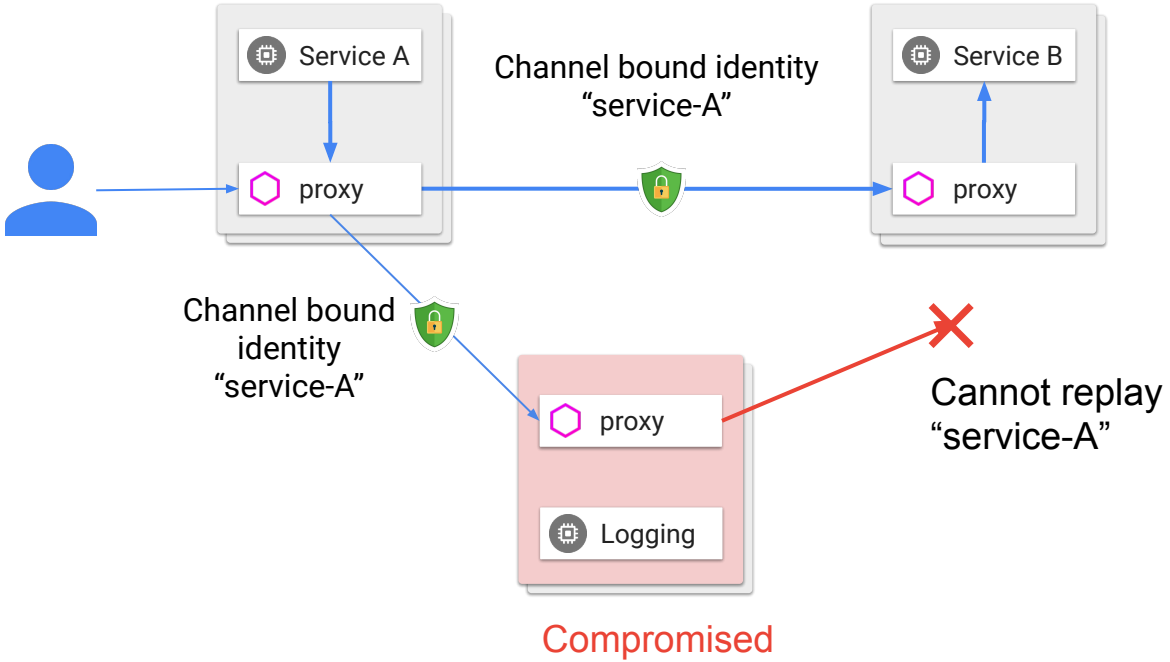
https://github.com/istio/istio/tree/master/mixer/adapter

Citadel: Autenticación reforzada con TLS mutua

Encriptación en tránsito:

Cada igual autentica a los otros usando identidades no-reproducibles dado que están ligadas al canal TLS.

La identidad del usuario final o de la aplicación se propaga como una ficha que va “saltando” por los servicios.



Citadel: Autorización a nivel de servicios

¿Quién realiza qué operación y usando qué cliente?

Visibilidad centralizada de los permisos generales de acceso.

Micro-segmentación basada en identidad, espacio de nombres, IP.

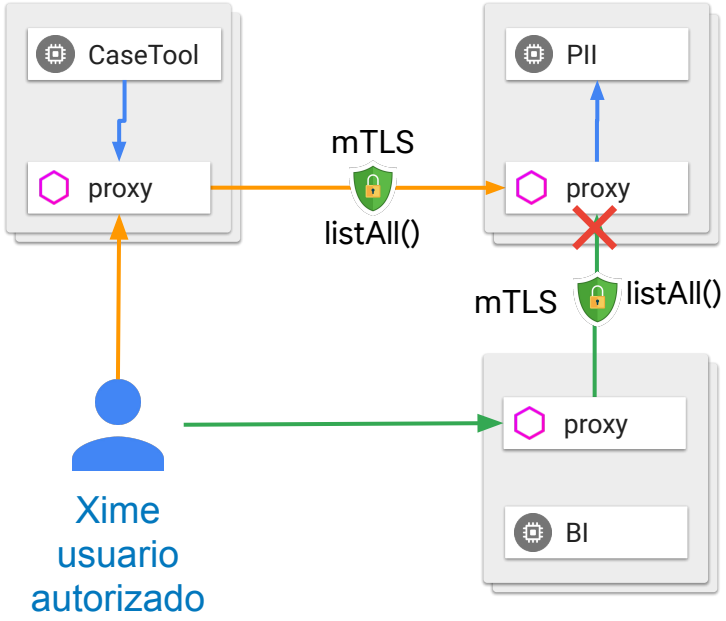
Políticas consistentes en todas las plataformas.

	Capa	Política de Entrada	Aplicabilidad
Aplicación	Aplicación (enchufable)	Modelo de recursos	Aplicaciones personalizables
Aplicación	**API / RPC**	Operaciones: URI, verbs JWT Claims	HTTP / REST gRPC
Red	**Canal**	Servicios de identidad IP K8S Namespace	Protocolos basados en TCP

Citadel: Caminos cerrados salvo con acceso privilegiado

Acceso a operaciones sensibles solo se brinda a usuarios autorizados usando el servicio cliente correcto.

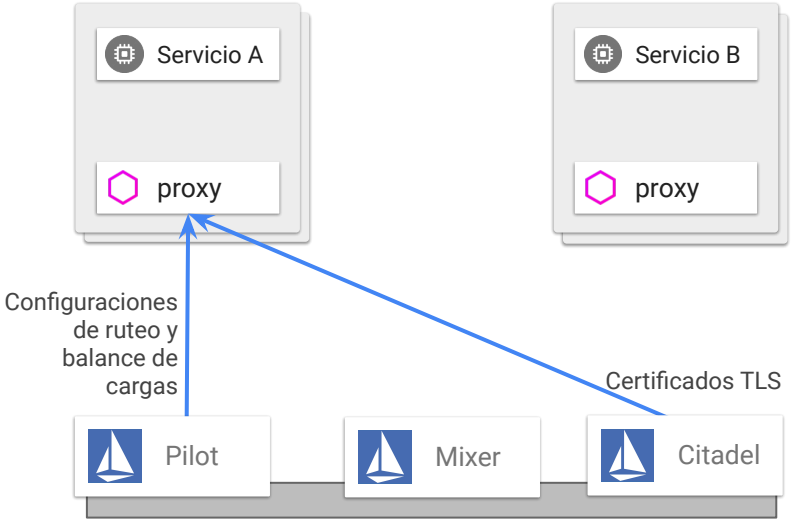
```
spec:
  subjects:
  - user: “spiffe://case-ns/case-tool”
    properties:
      request.auth.claims[role]: “reader”
  roleRef:
    kind: ServiceRole
    name: "book-reader"
```



La vida de una petición

04

La vida de una petición

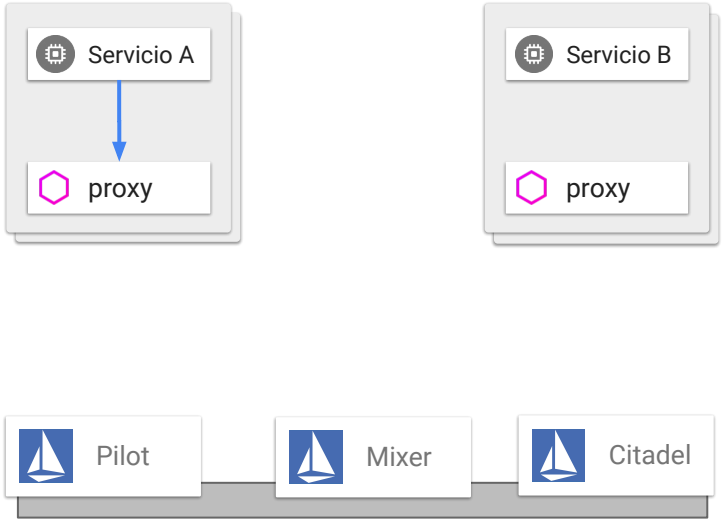


Servicio A se activa. Se despliega Envoy y obtiene lo siguiente de Pilot:

- La información sobre los servicios
- La información de ruteo
- Las políticas de configuración

Si usas Citadel, Envoy también obtiene los certificados de TLS de manera segura.

La vida de una petición

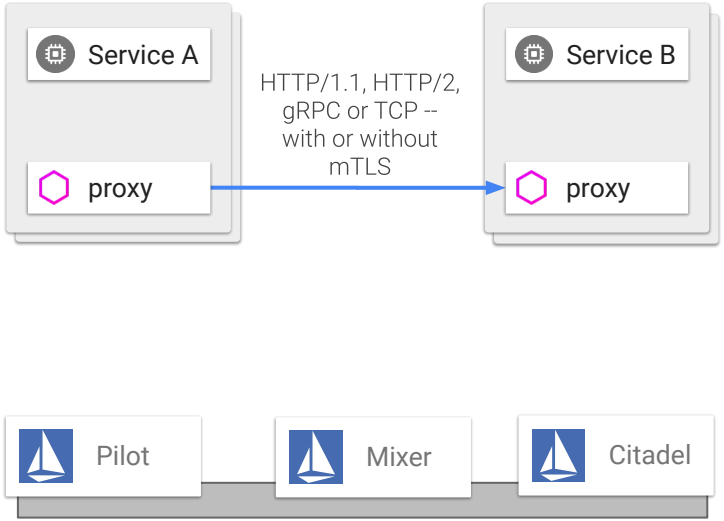


Servicio A llama al Servicio B.

El Envoy proxy del cliente intercepta la llamada.

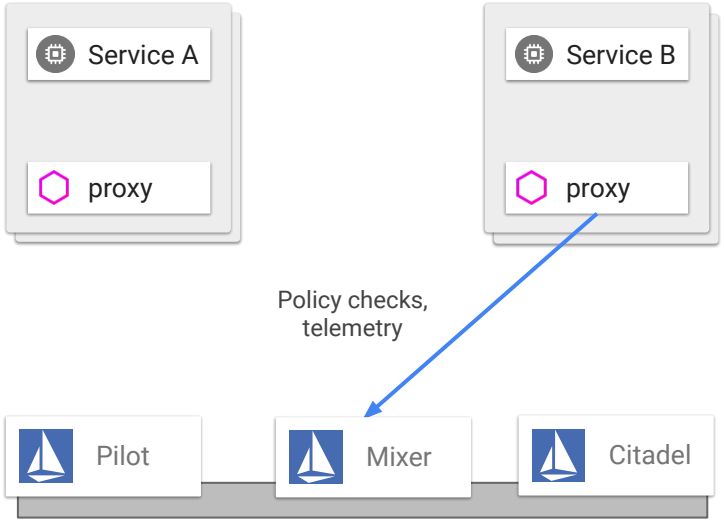
El Envoy proxy consulta la configuración para saber cómo y a dónde mandar la llamada para que llegue al servicio B.

La vida de una petición en la malla



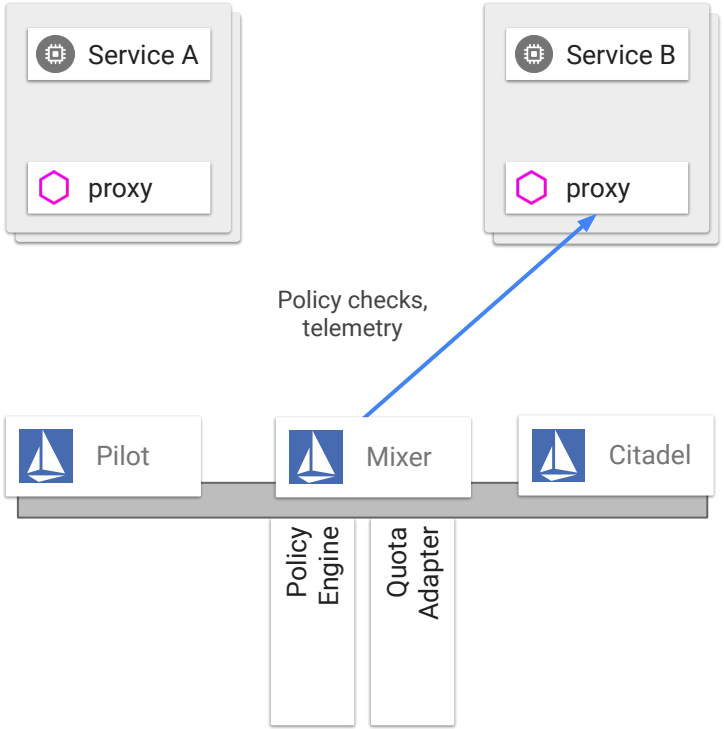
El Envoy proxy manda la petición a la instancia correcta del Servicio B. Allí, el Envoy proxy desplegado con el Servicio B intercepta la petición.

La vida de una petición en la malla



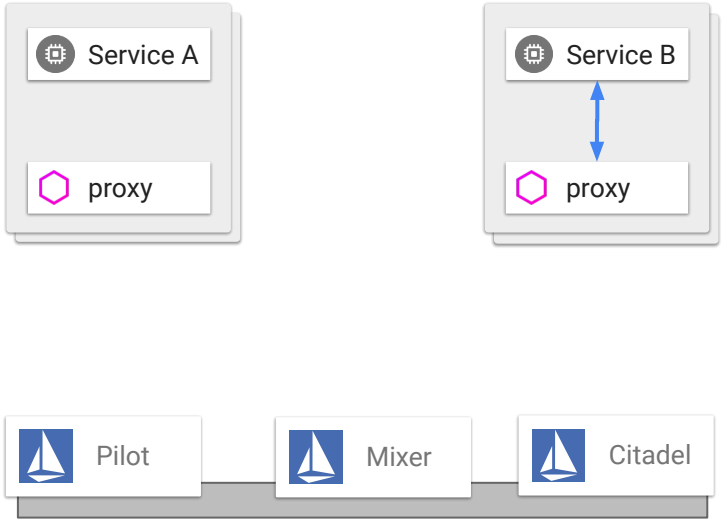
El Envoy proxy del Servicio B verifica con Mixer y valida que la llamada está permitida (verificación ACL, verificación de cupos, etc).

La vida de una petición en la malla



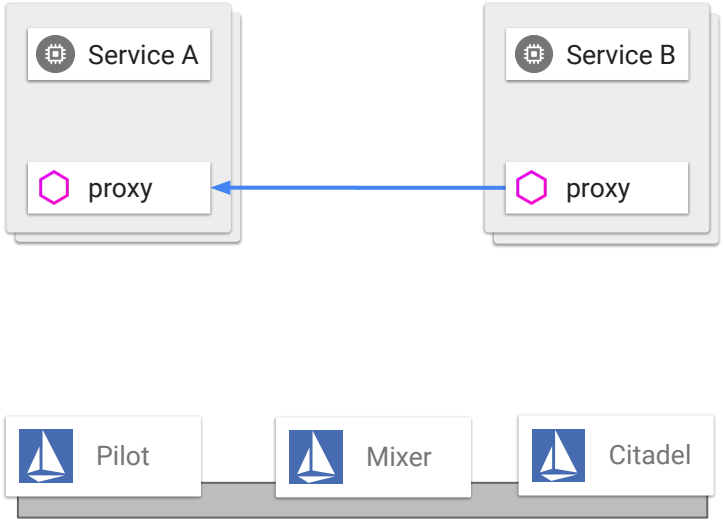
Mixer verifica con los adaptadores correspondientes (el motor de políticas, el adaptador de cupos) y comprueba que la llamada puede proseguir y responde con verdadero o falso al Envoy proxy.

La vida de una petición en la malla



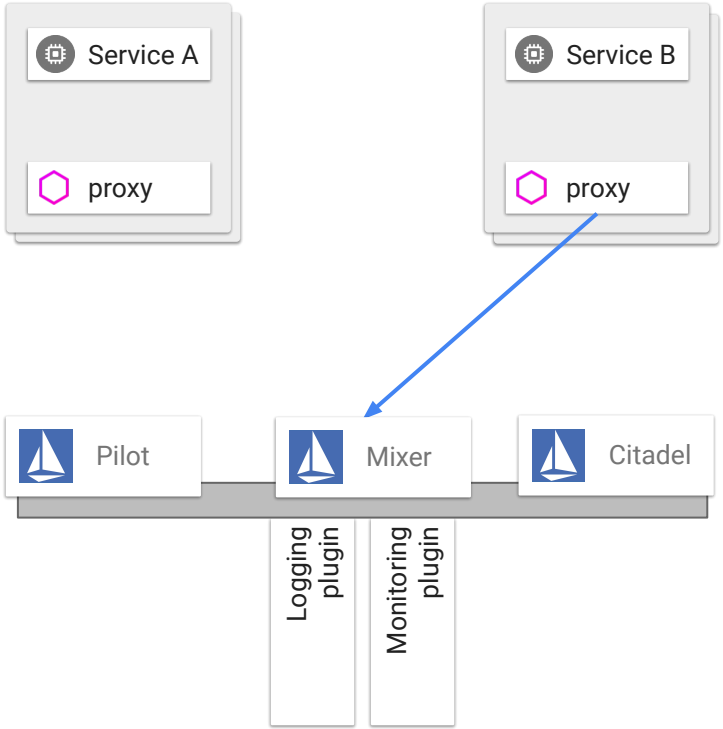
El Envoy proxy del lado del servidor reenvía la petición al Servicio B; el servicio procesa la petición y responde.

La vida de una petición en la malla



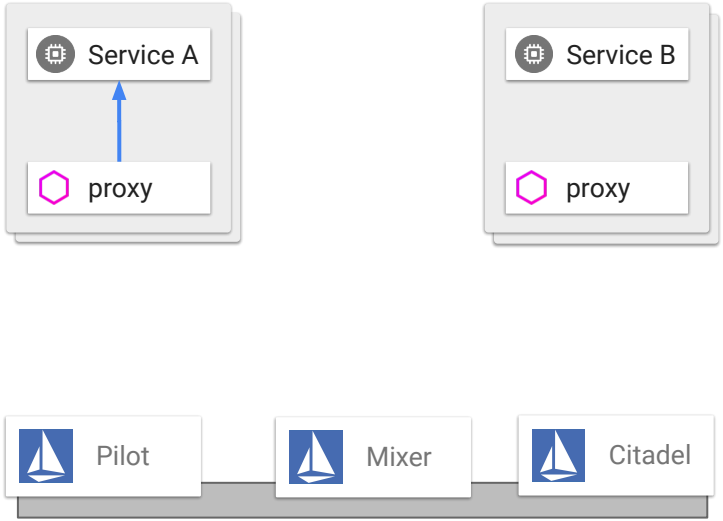
El Envoy proxy reenvía la respuesta al servicio que llamó originalmente. La respuesta es interceptada por el Envoy del lado del servicio que llamó.

La vida de una petición en la malla



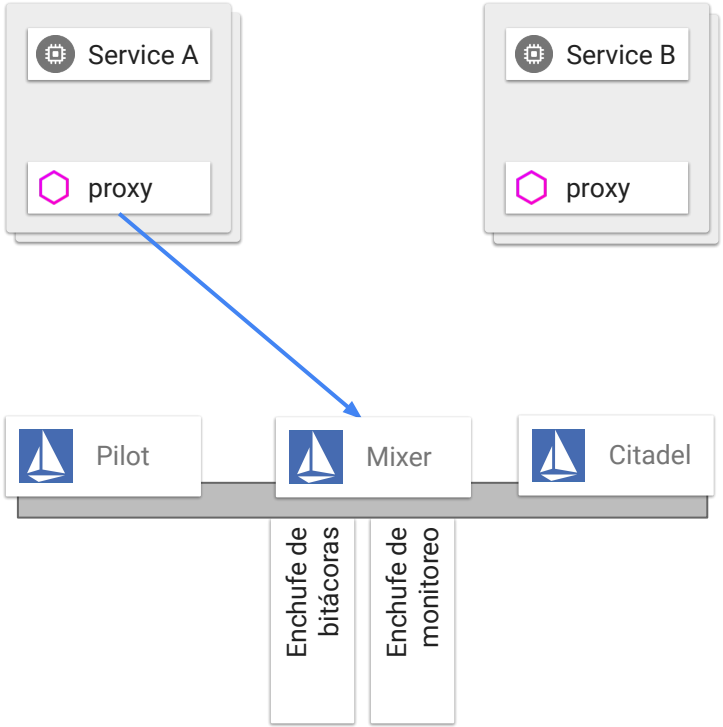
El Envoy proxy reporta la telemetría a Mixer, quien a su vez notifica a los enchufes apropiados.

La vida de una petición en la malla



El Envoy proxy del lado del cliente reenvía la respuesta al Servicio A que originó la llamada.

La vida de una petición en la malla



El Envoy del cliente reporta telemetría a Mixer, incluida la latencia percibida por el cliente. Mixer notifica a los enchufes apropiados.

Despliega una malla de servicios

Usando Istio

1

Prepara tu plataforma

Google Cloud

Google

CCOSS

2

Instala Istio

3

Despliega una aplicación

Google Cloud

Gracias, eso es todo.

Google Cloud

istio.io
github.com/istio
cloud.google.com/istio
istio-users@googlegroups.com
Twitter: @IstioMesh