Google Cloud

Istio: Além do Básico

TDC TRANSFORMATION
COMPETÊNCIAS PARA EVOLUÇÃO
DAS PESSOAS E NEGÓCIOS

Daniel Amadei
Customer Engineer, Google Cloud
https://www.linkedin.com/in/danielamadei

Um pouco sobre mim...

20 anos de experiência em TI

Atuei como desenvolvedor, analista, arquiteto, pré-vendas, etc...

Há 2.5 anos no Google como Customer Engineer

Foco em Modernização de Aplicações, apoiando clientes a extrair o máximo do Google Cloud Platform

Motivação desta Apresentação

Istio: Além do Básico

- Discutir o que um Service Mesh como o Istio pode fazer por você e pelas suas aplicações
- Geralmente a maioria do uso de Istio se restringe à observabilidade e alguns poucos casos de gestão de tráfego
- Temos uma gama de outras opções que o Istio nos oferece e que geralmente não são tão exploradas

Service Mesh

*Um service mesh (ou malha de serviço) é uma **camada de infraestrutura** dedicada que você pode adicionar aos seus aplicativos.*

*Ele permite que você **adicione recursos de forma transparente**, como capacidade de observação, gerenciamento de tráfego e segurança, **sem adicioná-los ao seu próprio código**.*

O que é o Istio?

- Service Mesh open source que se associa às diversas camadas de aplicações distribuídas, de forma transparente
- Os recursos do Istio fornecem uma maneira uniforme e mais eficiente de proteger, conectar e monitorar serviços
- Provê balanceamento de carga, autenticação serviço a serviço e monitoramento - **com poucas ou nenhuma alteração no código da aplicação**

Principais Conceitos

- **Observabilidade**
- **Gestão de Tráfego**
- **Segurança**
- **Extensibilidade**

Observabilidade

- **Métricas**
  - Coletadas nativamente pelo Envoy
  - Métricas dos PODs, serviços, tráfego, etc
  - Suporte aos "4 golden signals"
    - Latência, tráfego, erros e seturação
- **Trace Distribuído**
  - Geralmente é o que buscamos com a observabilidade
  - Gerado automaticamente pelo Istio, compatível com várias ferramentas de mercado
  - Pode ser propagado para várias camadas
- **Access Log**

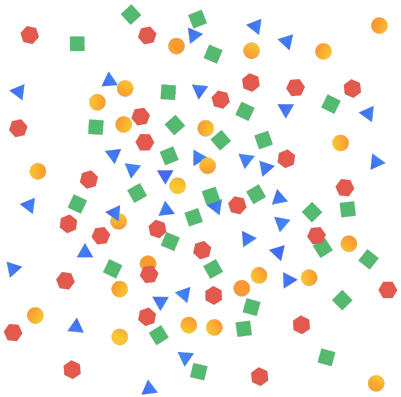
Demo:

Observabilidade com Istio

Gestão do Tráfego

Abstração e Controle

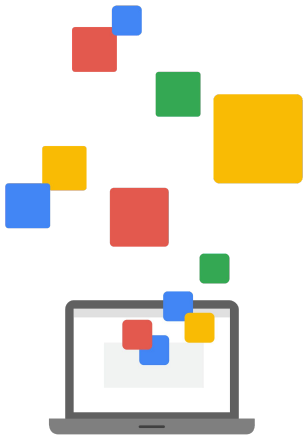
- **Abstração e Roteamento (Virtual Services)**
  - Canary
  - Roteamento
  - Desacoplamento do serviço "real"
- **Adequação do Tráfego para o Destino (Destination Rules)**
  - **Load Balancing**
    - Baseado na localidade ou
    - Aleatório, Round-Robin, Qtd. Conexões



Gestão do Tráfego

Conectividade e Circuite Break

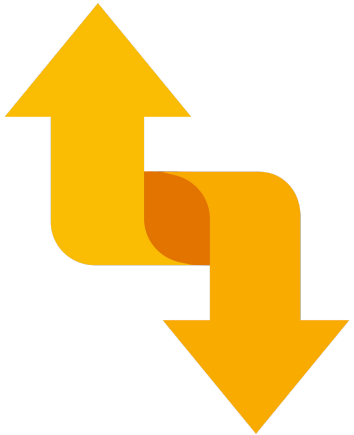
- **Pool de Conexão**
  - Grupo de conexões abertas com os servidores de upstream
  - Acelera a conectividade e diminui o uso de recursos em caso de "burst"
  - Apoia no suporte do Istio ao padrão de circuit break
- **Detecção de Outlier**
  - Remove endpoints com falha do pool
  - Configuração granular sobre como lidar com os outliers
- **Circuit Break**
  - Configurações dos limites suportados pelo serviço
  - Configs concorrência e proteção HTTP, TCP
- **TLS**
  - Certificados, CAs, Mutual TLS, etc.



Gestão do Tráfego

Controle da Entrada e Saída

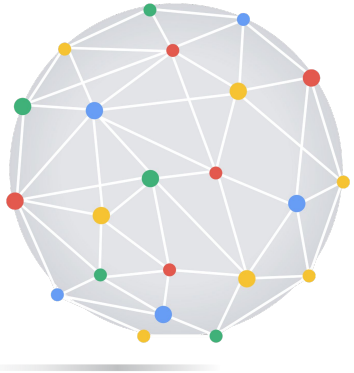
- **Gateways**
  - Permitem controlar a entrada e saída
  - Camada de Rede 4 a 6 (7 configurada no virtual service)
  - Exemplo Ingress: exposição externa TLS ou mTLS
  - Exemplo Egress: controle de quais URLs podem ser acessadas
- **Service Entries**
  - Adiciona serviços que são externos ao mesh
  - Permite aplicar a maioria dos recursos do Istio a chamadas externas: load balancing, retentativas, TLS/mTLS, etc...
  - Dica: use sempre que possível DNS: NONE nos SEs



Gestão do Tráfego

Confiabilidade & Chaos Engineering

- **Confiabilidade**
  - Retentativas a partir de falhas
  - Timeouts
- **Chaos Engineering**
  - Injeção de falhas e timeouts



Demos:

Canary
Virtual Service para Abstração
Confiabilidade

Segurança

- Criptografia para impedir ataques man-in-the-middle
- Autenticação e controle de acesso via mTLS
- Políticas de autorização
- Auditoria

Segurança

Autenticação e Autorização

- **Autenticação**
  - Peer Authentication: segurança na chamada serviço a serviço
  - Request Authentication: autenticação da requisição/usuário
- **Autorização**
  - Quais serviços são públicos
  - Quais serviços necessitam de um usuário
  - Quem pode invocar determinado serviço
    - Usuário, claims ou outros serviços

Demo:

Autenticação e Autorização

Resumindo

Istio: Além do Básico

- Um Service Mesh pode fazer muito mais do que Observabilidade
- Gestão de Tráfego, Confiabilidade, Segurança, etc.
- Lembre-se: o Service Mesh irá permitir que você extraia pontos complexos da sua aplicação e delegue isso para a infra.
- **Não perca amanhã na sala Google Cloud onde falaremos sobre Istio Gerenciado no GCP com o Anthos Service Mesh**

Dúvidas?