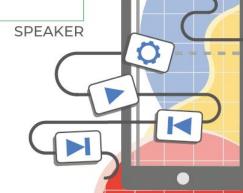


Autenticazione OAuth2 in un cluster Kubernetes tramite Istio ed Envoy

TALK

Ludovico Russo





Ludovico Russo

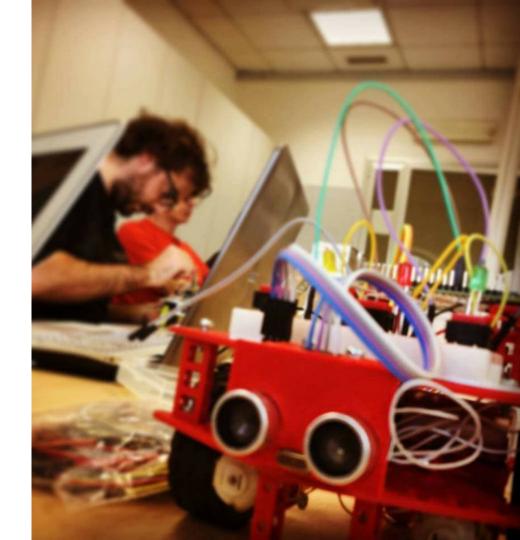
Ph.D. in **Computer and Control** Engineering @Politecnico di Torino

I Worked mainly on Cloud Robotics and Computer Vision for Service Robot Application

Now **cloud architect** and **full stack developer** consultant

Passionate in Computer Vision and Cloud Computing

@ludusrusso



DevOps, Questo Sconosciuto

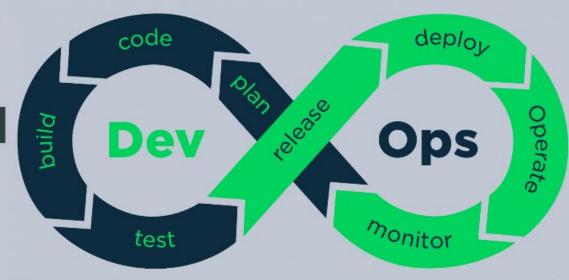
5 Maggio 18:30



WebMeetup #3

- DevOps The Three Ways
- Deployment Pipeline
- Seguiteci Live su YouTube





Autenticazione OAuth2 in un cluster Kubernetes tramite Istio ed Envoy

- Introduzione ai microservizi e Kubernetes
- Cos'è e come funziona Istio?
- Autenticazione e Autorizzazione tramite token
 JWT e OAuth2
- RequestAuthentication e AuthorizationPolicy in Istio
- Demo Time! (se rimane tempo 😀)









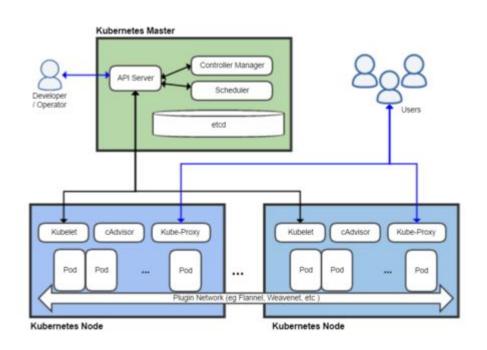


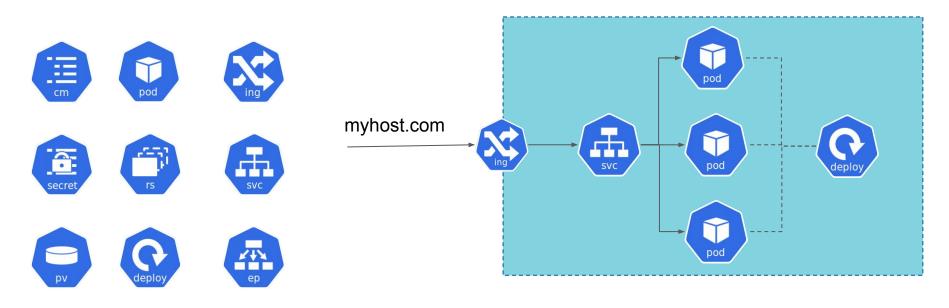


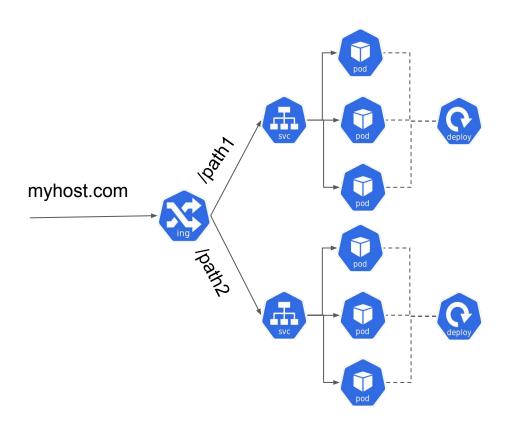


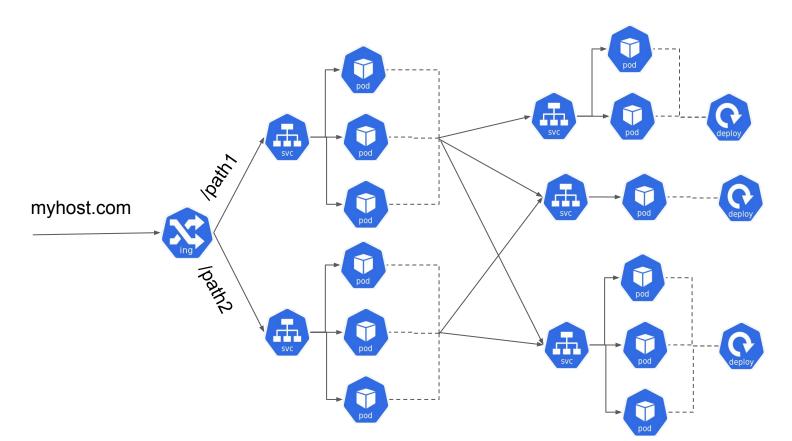


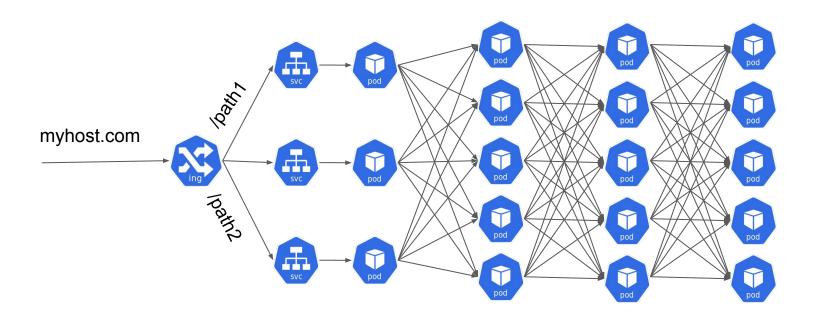




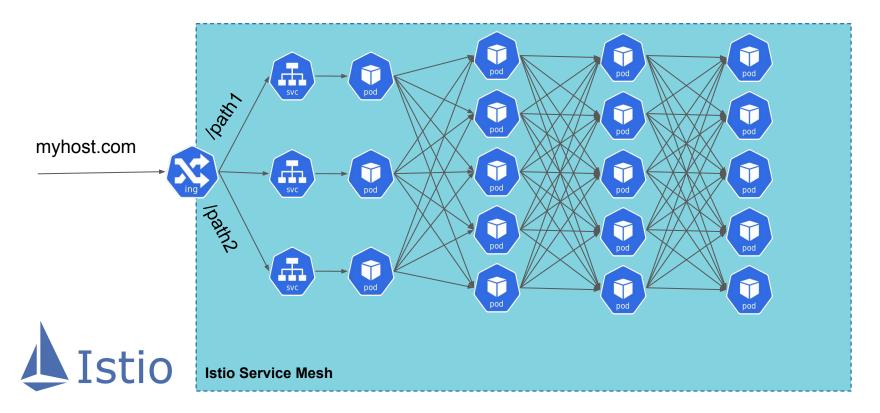




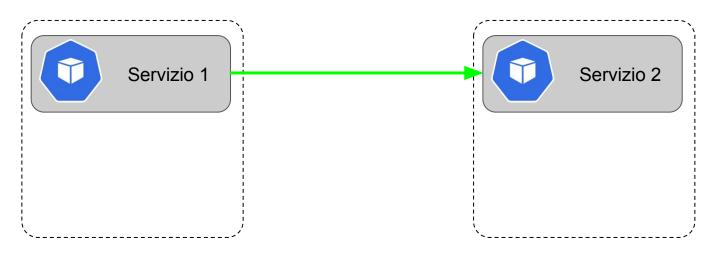




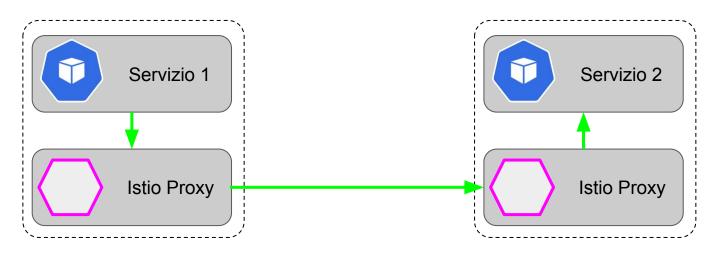
Istio: Connect, secure, control and observe services



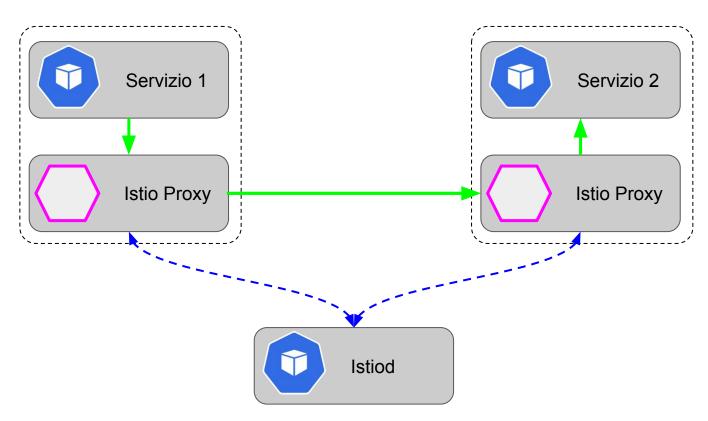
Istio: come funziona?



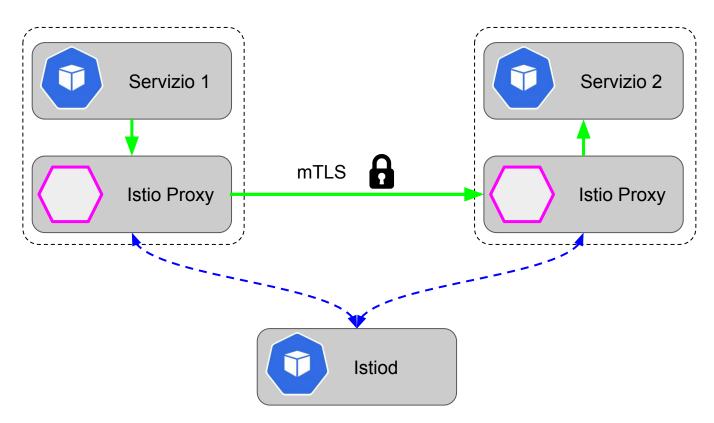
Istio: come funziona?



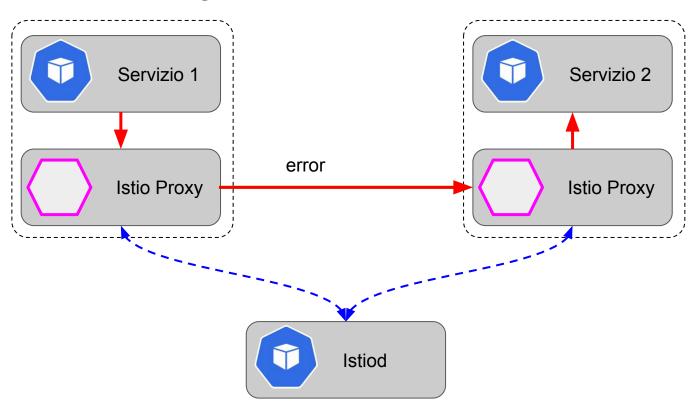
Istio: come funziona?



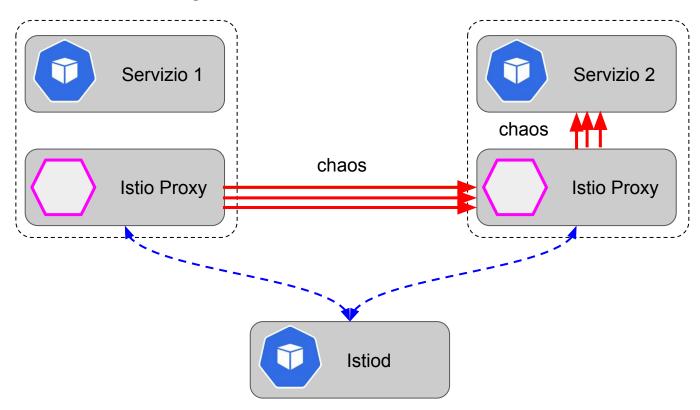
Istio: Auto mTLS



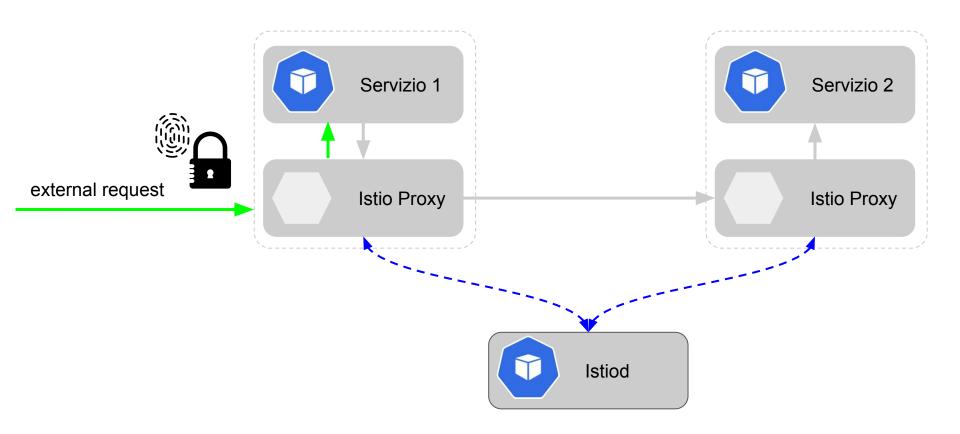
Istio: Monitoring



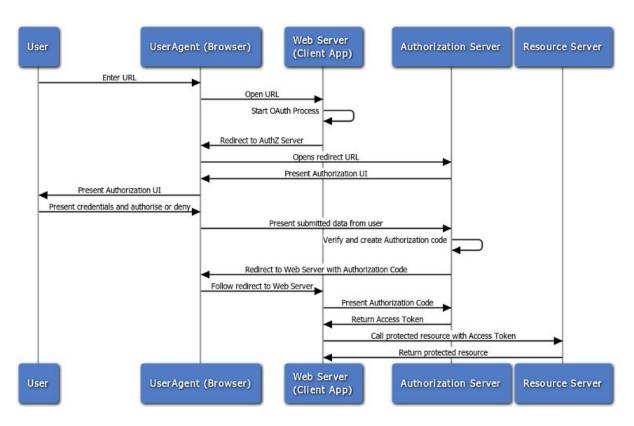
Istio: Chaos Injection



Istio: Autenticazione e Autorizzazione



Autenticazione tramite OAuth2



Token JWT

eyJhbGciOiJSUzI1NiIsImtpZCI6Ijg4ODQ4YjVh ZmYyZDUyMDEzMzFhNTQ3ZDE5MDZ1NWFhZGY2NTEz YzgiLCJ0eXAiOiJKV1QifQ.eyJuYW1lIjoiTHVkb 3ZpY28gUnVzc28iLCJwaWN0dXJlIjoiaHR0cHM6L y9saDUuZ29vZ2xldXNlcmNvbnRlbnQuY29tLy01R 1VWaTZBYTV2TS9BQUFBQUFBQUFBSS9BQUFBQUFBQ UFBQS9BQUtXSkpPdjU4clhESkdrU0hwZzBNd251Z 1RaWmF2VE1BL3Bob3RvLmpwZyIsImlzcyI6Imh0d HBz0i8vc2VjdXJldG9rZW4uZ29vZ2x1LmNvbS9nZ GctZGV2ZmVzdC1kZW1vLTI00WQ0IiwiYXVkIjoiZ 2RnLWRldmZlc3QtZGVtby0yNDlkNCIsImF1dGhfd GltZSI6MTU4ODQxMTIxMSwidXNlcl9pZCI6Im9QZ nZoNFI0bGlWY113bEdpWDNoSDU1M2dvcDEiLCJzd WIiOiJvUGZ2aDRSNGxpVmNZd2xHaVgzaEg1NTNnb 3AxIiwiaWF0IjoxNTg4NDExMjExLCJleHAi0jE10 Dg0MTQ4MTEsImVtYWlsIjoibHVkb3ZpY29AbHVkd XNydXNzby5zcGFjZSIsImVtYWlsX3ZlcmlmaWVkI jp0cnV1LCJmaXJ1YmFzZSI6eyJpZGVudG10aWVzI jp7Imdvb2dsZS5jb20i0lsiMTA30DI5NTE5MjQ4M zMzMDQ5MjM5Il0sImVtYWlsIjpbImx1ZG92aWNvQ Gx1ZHVzcnVzc28uc3BhY2UiXX0sInNpZ25faW5fc HJvdmlkZXIiOiJnb29nbGUuY29tIn19.AAIP1IlR 1215xKfidxBDRheQ8bzjQp0EC8n4FdQYxtdwUNEq Z5HiBve-zJgRi8atB3PKg3rjPSa1lTgwjUWZi2DRAmEdnC2yQEbns6Rpg3TizB gyOc5y4ybeX0KtTC-g1dzjNbtgzlcaTTLmsZEwRzeIyMh9nrJELbArhTv80ExJxZqfodd wwGeUeMbzoQSm8Nw3KG4Uc2dAeGNEjQvCQ0AsdDj ryjd1ej2vEW5YRBEF9Ftbr_FiALHhxNdDovxH95y trnx5piHEIvHaovlo-pMH3qdzAVeLoln5jF60EuUCmhPBdfhU-

```
HEADER: ALGORITHM & TOKEN TYPE
    "alg": "RS256",
    "kid": "88848b5aff2d5201331a547d1906e5aadf6513c8".
PAYLOAD: DATA
    "name": "Ludovico Russo".
    "picture":
  "https://lh5.googleusercontent.com/-5FUVi6Aa5vM/AAAAAAAAAA
 I/AAAAAAAAAAAA/AAKWJJOv58rXDJGkSHpg@MwnugTZZavTIA/photo.jpg
    "iss": "https://securetoken.google.com/gdg-devfest-demo-
 249d4",
    "aud": "gdg-devfest-demo-249d4",
   "auth_time": 1588411211,
    "user_id": "oPfvh4R4liVcYwlGiX3hH553gop1".
    "sub": "oPfvh4R4liVcYwlGiX3hH553gop1",
    "iat": 1588411211.
    "exp": 1588414811,
    "email": "ludovico@ludusrusso.space",
    "email verified": true.
    "firebase": {
      "identities": {
        "google.com": [
          "107829519248333049239"
        "email": [
          "ludovico@ludusrusso.space"
      "sign_in_provider": "google.com"
VERIFY SIGNATURE
```

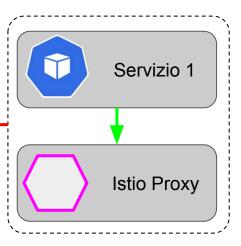
RSASHA256 (

base64UrlEncode(header) + "." +
base64UrlEncode(payload),

Public Key or Certificate Ent

```
1 apiVersion: security.istio.io/v1beta1
   kind: RequestAuthentication
3 metadata:
     name: server
     selector:
       matchLabels:
        name: server
     iwtRules:
       - issuer: https://securetoken.google.com/gdg-devfest-demo-249d4
         jwksUri:
   https://www.googleapis.com/service_accounts/v1/metadata/x509/secureto
   ken@system.gserviceaccount.com
         outputPayloadToHeader: "auth"
         forwardOriginalToken: true
```

```
1 apiVersion: security.istio.io/v1beta1
   kind: RequestAuthentication
  metadata:
     name: server
   spec:
     selector:
       matchLabels:
         name: server
     iwtRules:
       - issuer: https://securetoken.google.com/gdg-devfest-demo-249d4
         jwksUri:
   https://www.googleapis.com/service_accounts/v1/metadata/x509/secureto
   ken@system.gserviceaccount.com
         outputPayloadToHeader: "auth"
         forwardOriginalToken: true
```



```
1 apiVersion: security.istio.io/v1beta1
   kind: RequestAuthentication
  metadata:
     name: server
   spec:
     selector:
       matchLabels:
         name: server
     iwtRules:
       - issuer: https://securetoken.google.com/gdg-devfest-demo-249d4
         jwksUri:
   https://www.googleapis.com/service_accounts/v1/metadata/x509/secureto
   ken@system.gserviceaccount.com
         outputPayloadToHeader: "auth"
         forwardOriginalToken: true
```

```
PAYLOAD: DATA

{
    "name": "Ludovico Russo",
    "picture":
    "https://lh5.googleusercontent.com/-5FUVi6Aa5vM/AAAAAAAAA
I/AAAAAAAAAAAAAAAKWJJOv58rXDJGkSHpg@MwnugTZZavTIA/photo.jpg
    "iss": "https://securetoken.google.com/gdg-devfest-demo-
49d4",
    aud': "gdg-devfest-demo-249d4",
    audth_time": 1588411211,
    "user_id": "oPfvh4R4livCvwlGiX3hH553gop1",
    "iat": 1588411211,
    "exp": 1588414811,
    "email": "ludovico@ludusrusso.space",
```

```
1 apiVersion: security.istio.io/v1beta1
   kind: RequestAuthentication
   metadata:
     name: server
   spec:
     selector:
       matchLabels:
         name: server
     iwtRules:
       - issuer: https://securetoken.google.com/gdg-devfest-demo-249d4
         jwksUri:
   https://www.googleapis.com/service_accounts/v1/metadata/x509/secureto
   ken@system.gserviceaccount.com
         outputPayloadToHeader: "auth"
         forwardOriginalToken: true
```

"88848b5aff2d5201331a547d1906e5aadf6513c8": "----BEGIN CERTIFIC. \nMIIDHDCCAgSgAwIBAgIIA/oH1w0GNmMwDQYJKoZIhvcNAQEFBQAwMTEvMC0GA1UE xMS8wLQYDVQQDEyZzZWN1cmV0b2t1\nbi5zeXN0ZW0uZ3N1cnZpY2VhY2NvdW50LmN H3SeUIR0KH8KIbjBYcF8DVZLF0xWSAIhVCbcplt+53ICri4uWrh6VI0vvl\nsj0u5z pHOrHnprzDxdl3jIansoj\nHO4fphkxBJiiXBaCuWrexrLdPJZiYtyuimuMtVBTPnI 8BAf8EBAMCB4AwFqYDVR01AQH/BAwwCqYIKwYBBQUHAwIwDQYJ\nKoZIhvcNAQEFBQ. XHm7KNvY+c8FA\ni7lBbfq9azJcrtZGQsSbTuowTQZX1R1jBq1FWZ/bxwn6vnIU75L 8dAqNk97aQWVULrxZm/LjFh4A+FLK6FpGgITLpbp+I\nz1hFewXrAFp8Up6U3Sch6S "5e9ee97c840f97e0253688a3b7e94473e528a7b5": "----BEGIN CERTIFIC. \nMIIDHDCCAqSqAwIBAqIIZC7uPq+FdkIwDOYJKoZIhvcNAOEFBOAwMTEvMC0GA1UE xMS8wLOYDVOODEvzzzWN1cmV0b2tl\nbi5zeXN0zW0uz3N1cnzpY2VhY2NvdW50LmN vDssopXt6jiUGeBKMvm65fil08EfGZXCYPZVBXldgkddRkgNA2afhvrgdF\n7BG9Ul-65ogW/4uOCaD8V54Ncf6D\nn0gX3gW3ze2kO1W4NDmOhLhpef8nBORs1Mt7dvKxK3O 8BAf8EBAMCB4AwFqYDVR01AQH/BAwwCqYIKwYBBQUHAwIwDQYJ\nKoZIhvcNAQEFBQ. t0ZHGAD1/d2U8\ny0wPZJWjCWHRkufPOMr2EFhw1A5Pj1mBTKn9PZAQf9rWiJuYhkb JnRDbs4WbLMpzS8Fq6APa0ukHRV9cimjqmQbEJ5v6y\nTBtNGlqPXsUJQldCKMYWMX

```
1 apiVersion: security.istio.io/v1beta1
  kind: RequestAuthentication
  metadata:
     name: server
     selector:
       matchLabels:
        name: server
     iwtRules:
       - issuer: https://securetoken.google.com/gdg-devfest-demo-249d4
         jwksUri:
   https://www.googleapis.com/service_accounts/v1/metadata/x509/secureto
   ken@system.gserviceaccount.com
        outputPayloadToHeader: "auth"
        forwardOriginalToken: true
```

- Estrai il body del token ed inseriscilo in un header chiamato "auth"
- Inoltra il token originale al service

```
• • •
1 apiVersion: security.istio.io/v1beta1
  kind: AuthorizationPolicy
  metadata:
     name: server
   spec:
     action: ALLOW
     selector:
       matchLabels:
         name: server
     rules:
11
       - from:
12
           - source:
13
               requestPrincipals: ["*"]
```

```
• • •
1 apiVersion: security.istio.io/v1beta1
  kind: AuthorizationPolicy
  metadata:
     name: server
   spec:
     action: ALLOW
     selector:
       matchLabels:
         name: server
10
     rules:
11
       - from:
12
           - source:
13
               requestPrincipals: ["*"]
```

- ALLOW
- DENY

```
Servizio 1
• • •
  apiVersion: security.istio.io/v1beta1
   kind: AuthorizationPolicy
   metadata:
     name: server
                                                                                                     Istio Proxy
   spec:
     action: ALLOW
     selector:
       matchLabels:
         name: server
     rules:
10
11
       - from:
12
           - source:
13
               requestPrincipals: ["*"]
```

```
1 apiVersion: security.istio.io/v1beta1
  kind: AuthorizationPolicy
  metadata:
    name: server
   spec:
    action: ALLOW
    selector:
       matchLabels:
         name: server
10
     rules:
11
       - from:
12
          - source:
13
               requestPrincipals: ["*"]
```

Chi è autorizzato a chiamare questo servizio?

Tutti gli utenti autenticati tramite token JWT

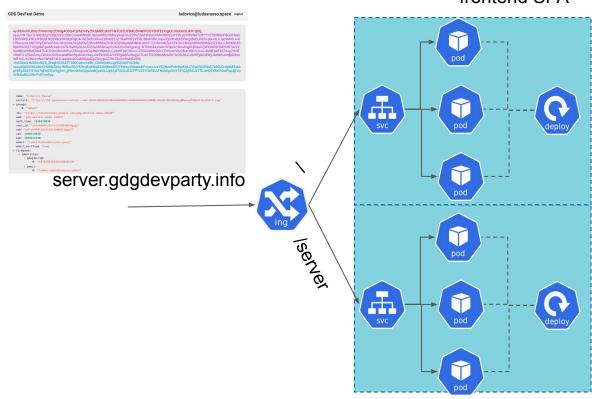
```
action: ALLOW
     selector:
       matchLabels:
         name: server
     rules:
11
       - from:
12
           - source:
13
               requestPrincipals: ['*']
         when:
           - key: request.auth.claims[groups]
             values:
17
               - 'admin'
```

Chi è autorizzato a chiamare questo servizio?

Tutti gli utenti autenticati tramite token JWT che appartengono al gruppo "admin"

Demo TIME

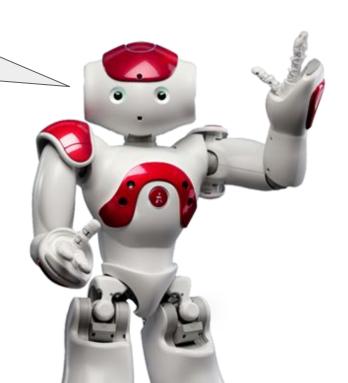
frontend SPA



backend

Grazie per l'attenzione

Domande?



Slide e Codice

