

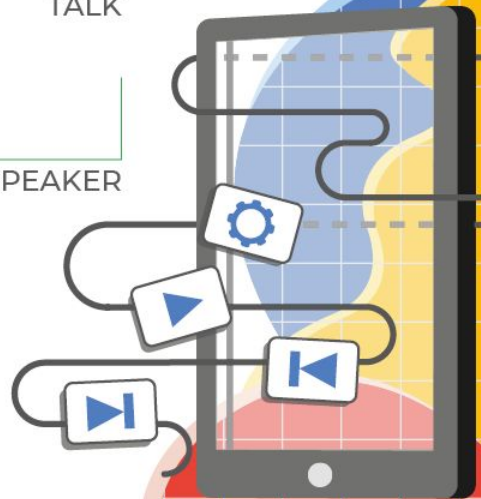


Autenticazione OAuth2 in un cluster Kubernetes tramite Istio ed Envoy

TALK

Ludovico Russo

SPEAKER



GDG Italia

Ludovico Russo

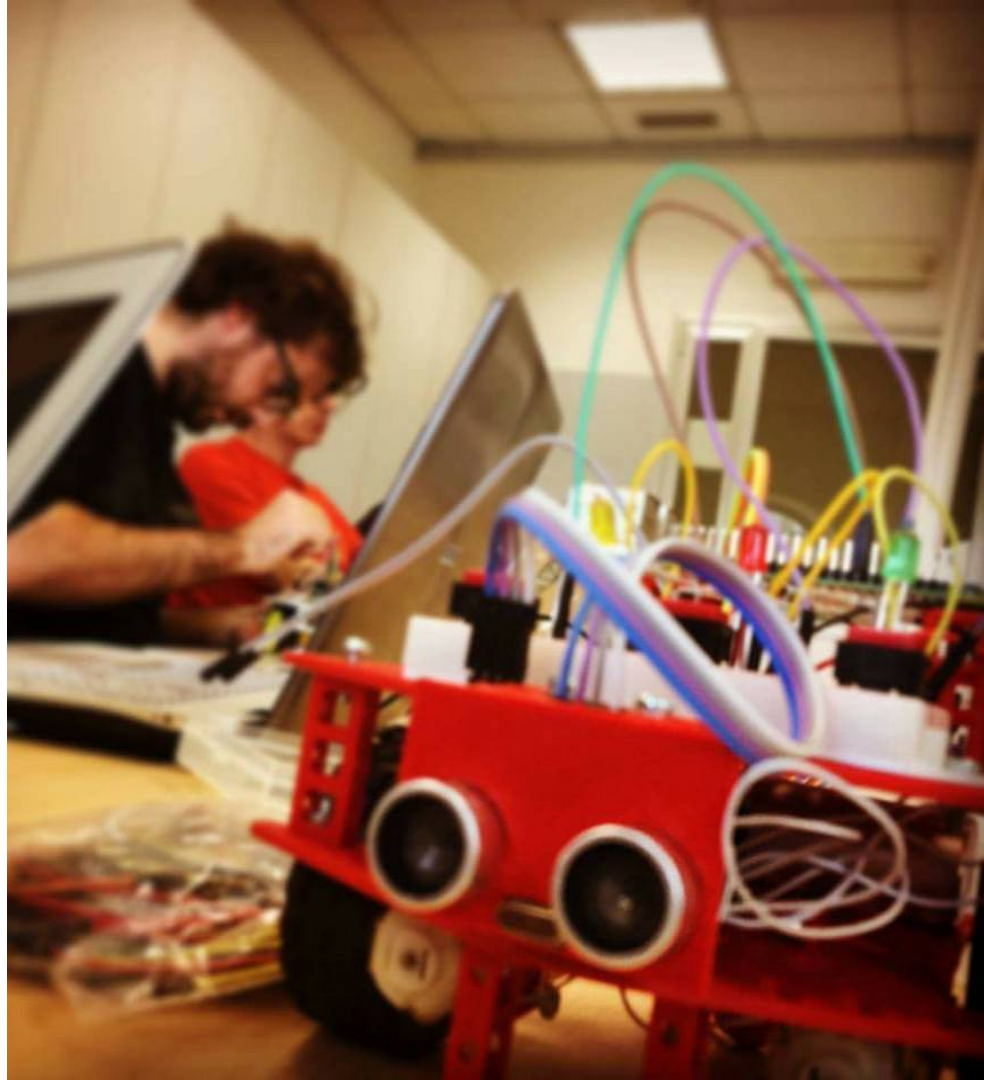
Ph.D. in **Computer and Control Engineering**
@Politecnico di Torino

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

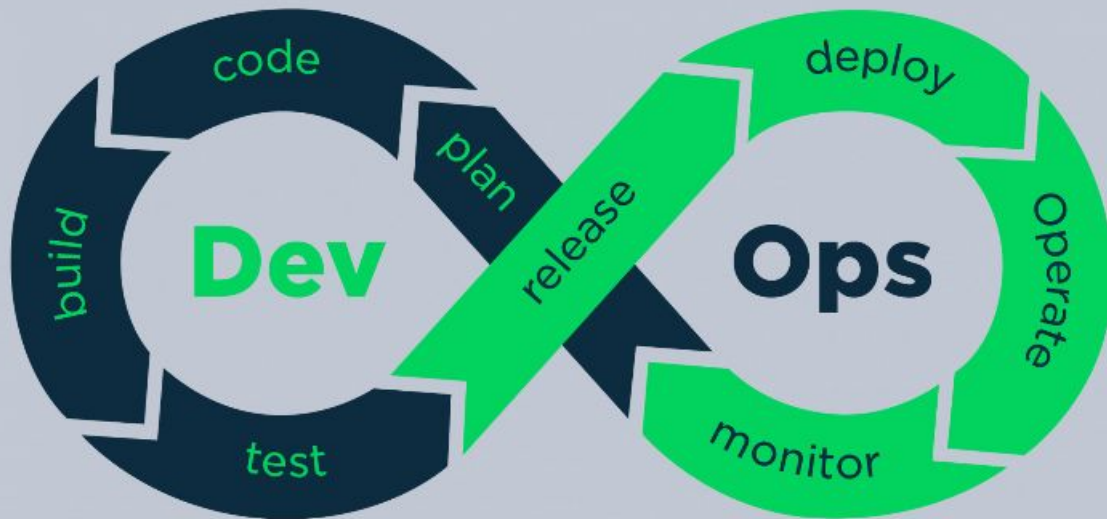


Google Cloud

- DevOps - The Three Ways

- Deployment Pipeline

- Seguiteci Live su YouTube

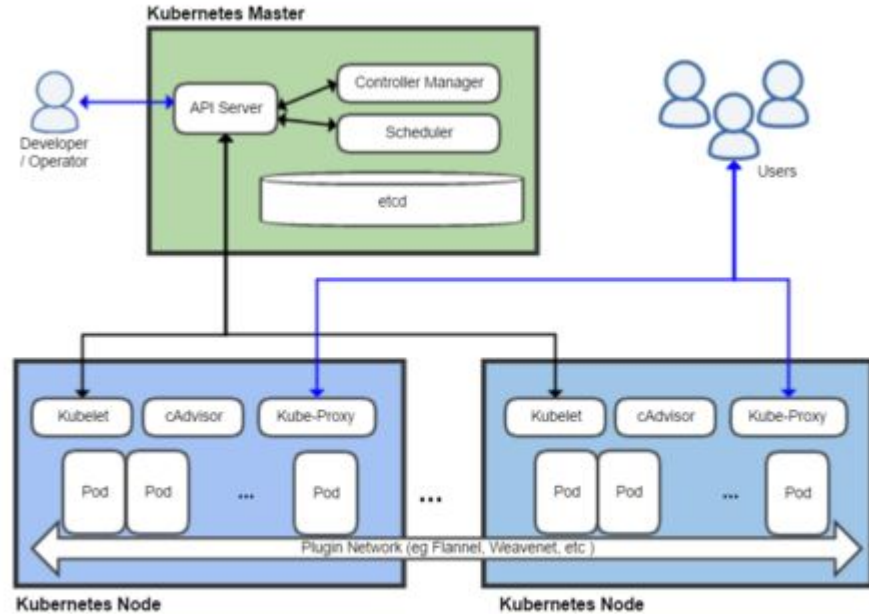
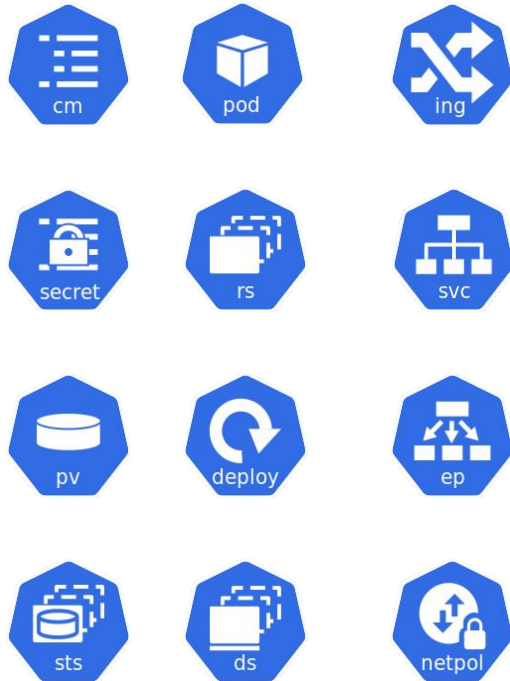


Autenticazione OAuth2 in un cluster Kubernetes tramite Istio ed Envoy

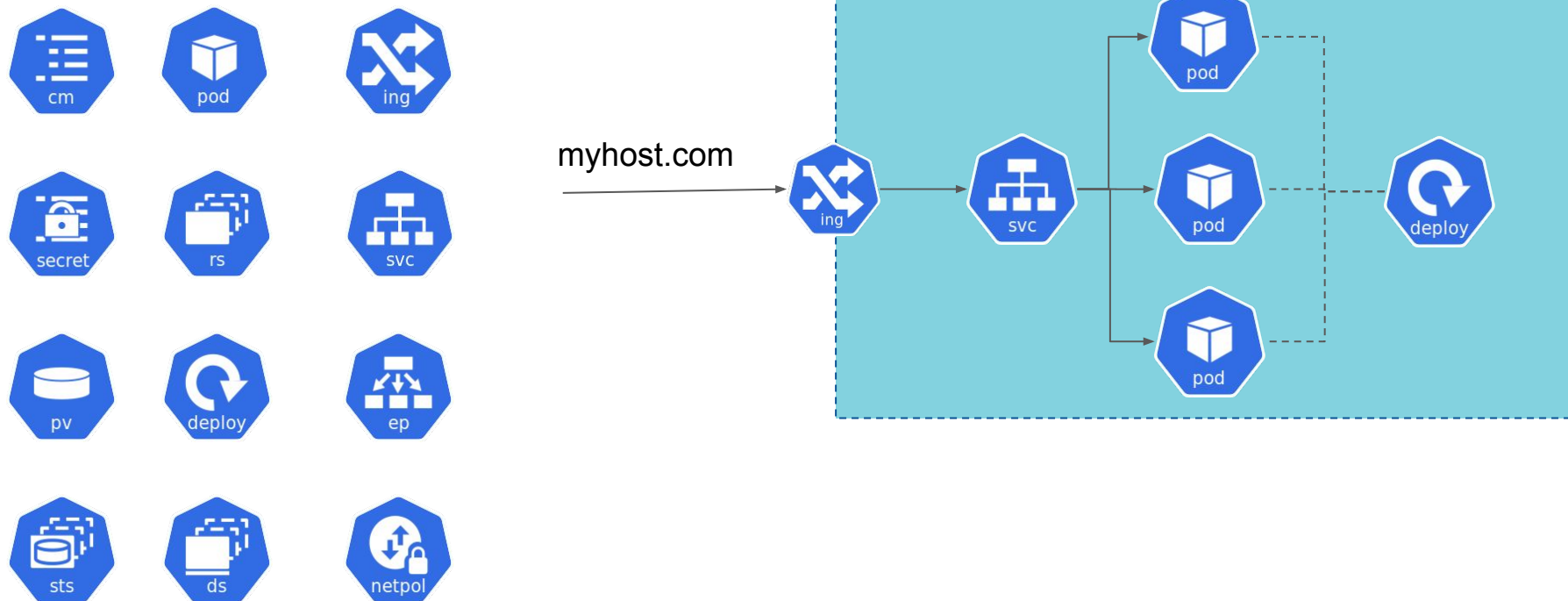
- Introduzione ai microservizi e Kubernetes
- Cos'è e come funziona Istio?
- Autenticazione e Autorizzazione tramite token JWT e OAuth2
- RequestAuthentication e AuthorizationPolicy in Istio
- Demo Time! (se rimane tempo 😊)



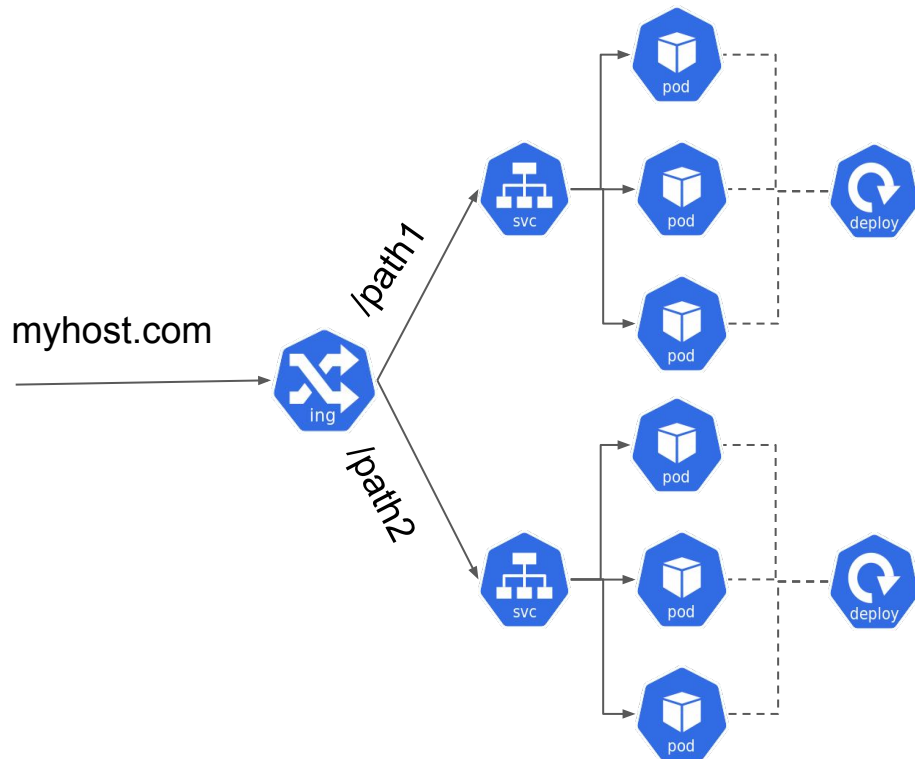
Kubernetes e le architetture a Microservizi



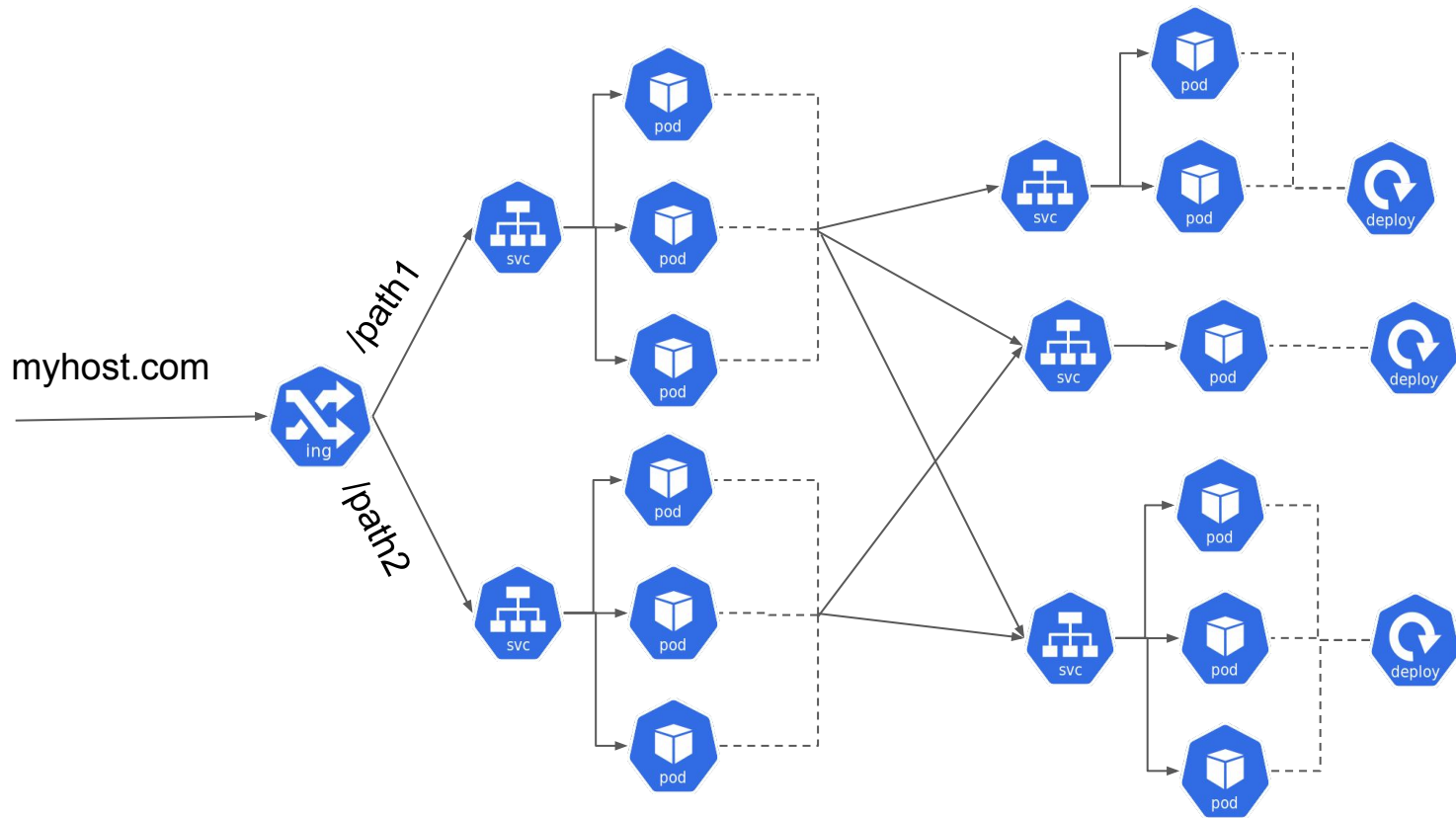
Kubernetes e le architetture a Microservizi



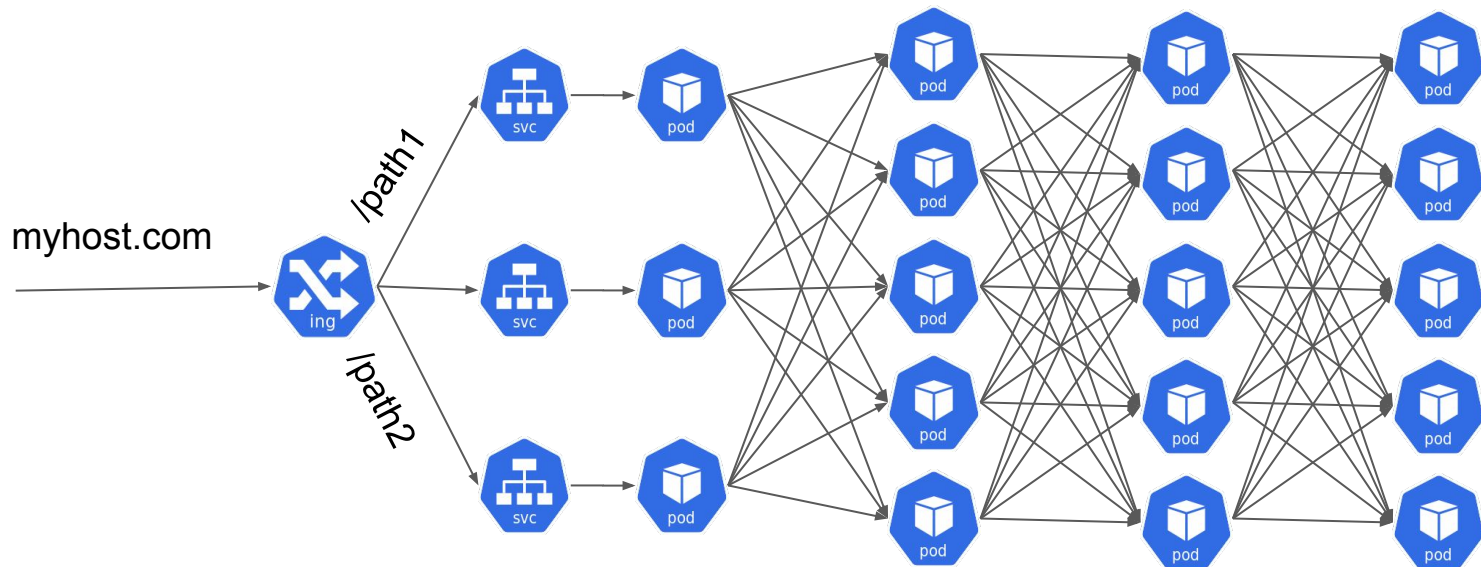
Kubernetes e le architetture a Microservizi



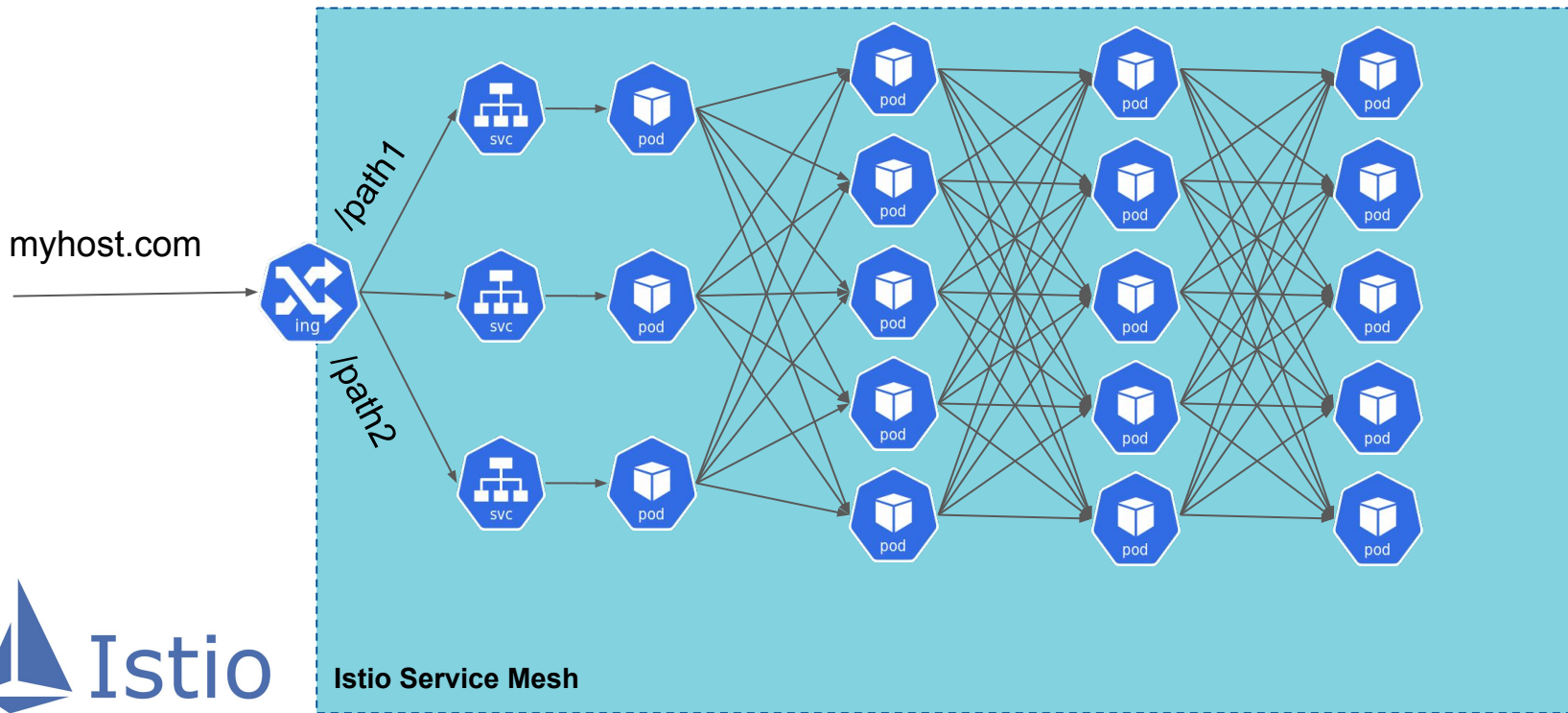
Kubernetes e le architetture a Microservizi



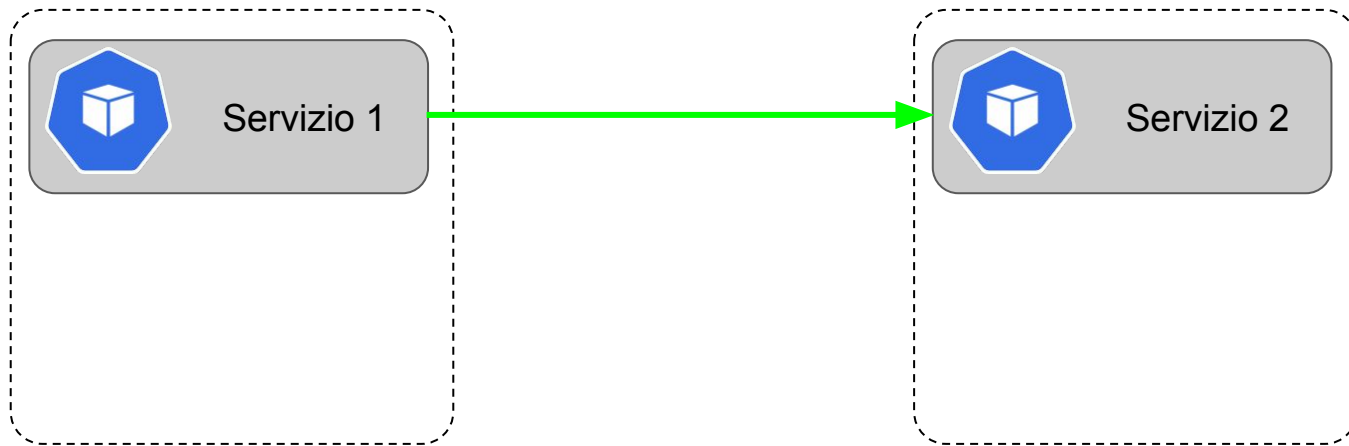
Kubernetes e le architetture a Microservizi



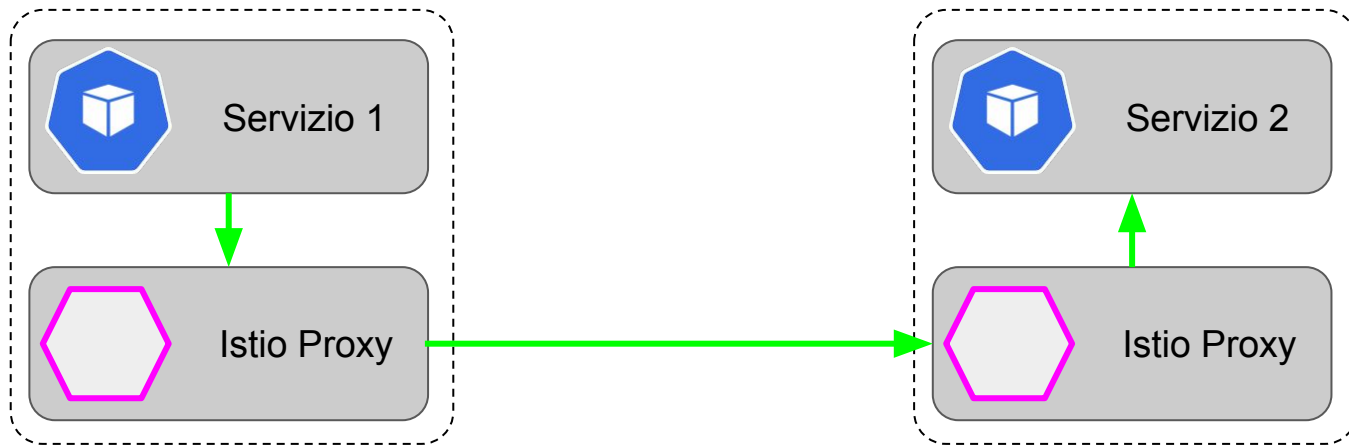
Istio: Connect, secure, control and observe services



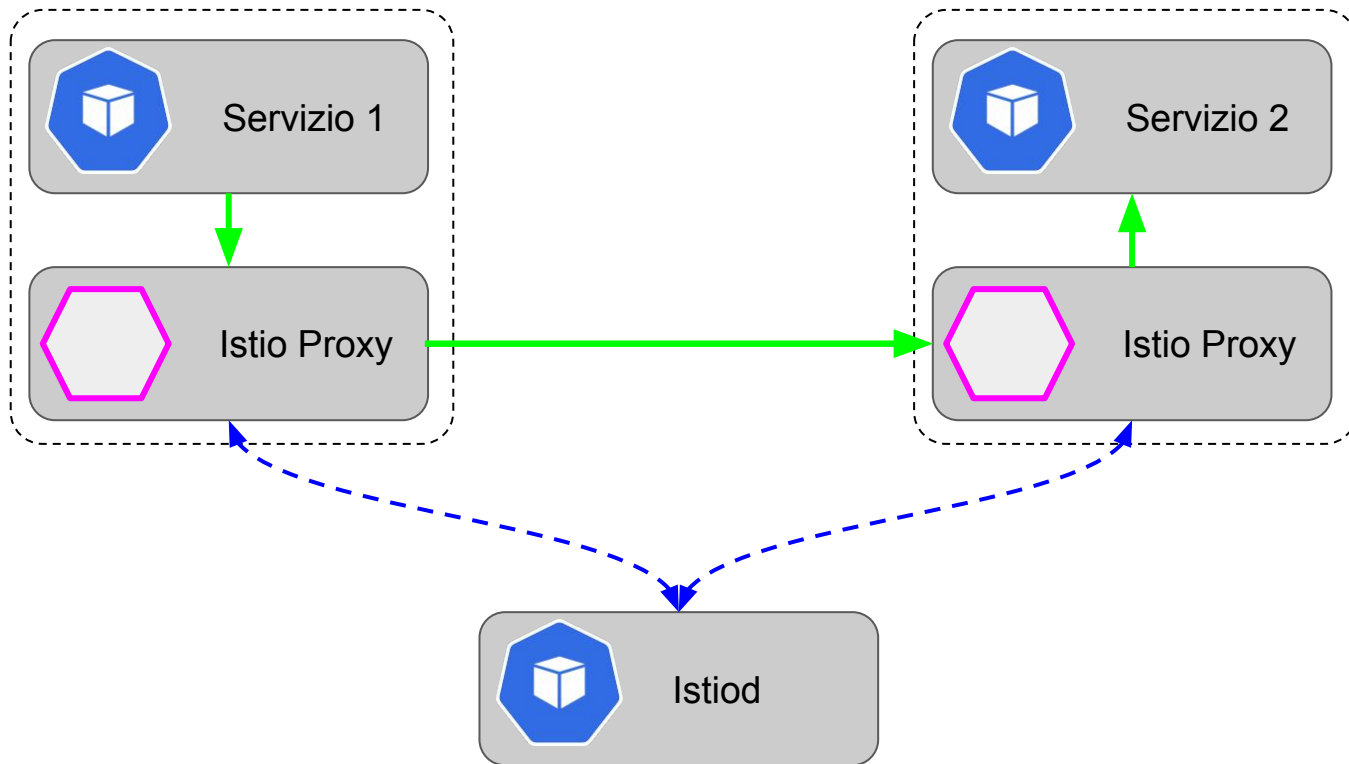
Istio: come funziona?



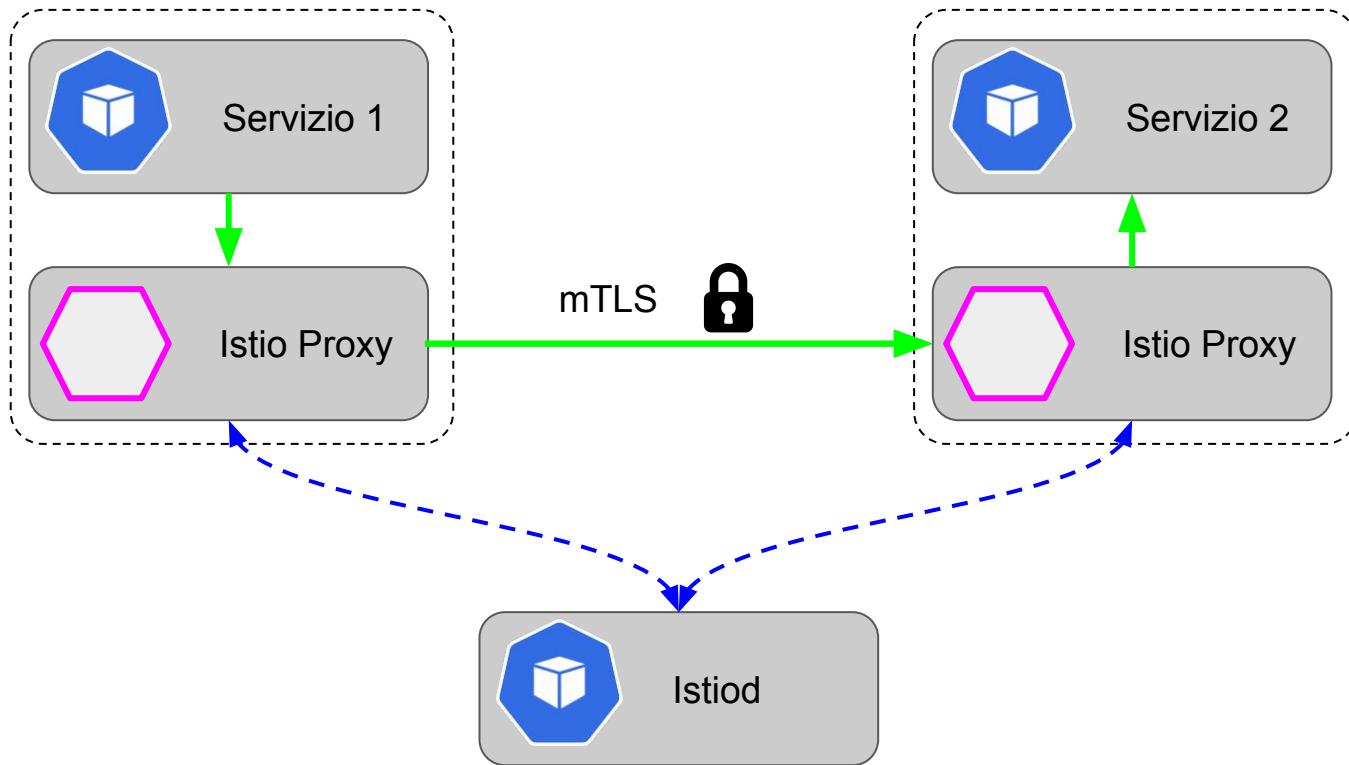
Istio: come funziona?



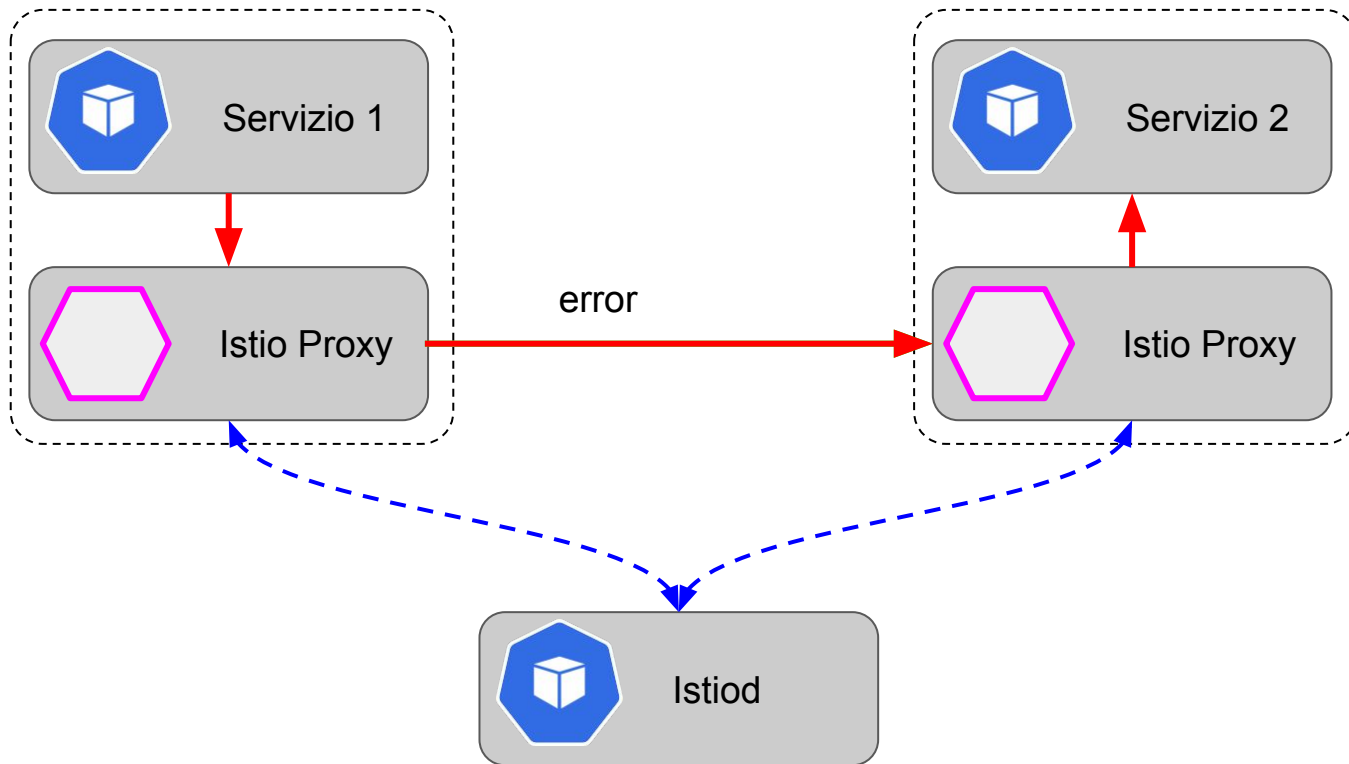
Istio: come funziona?



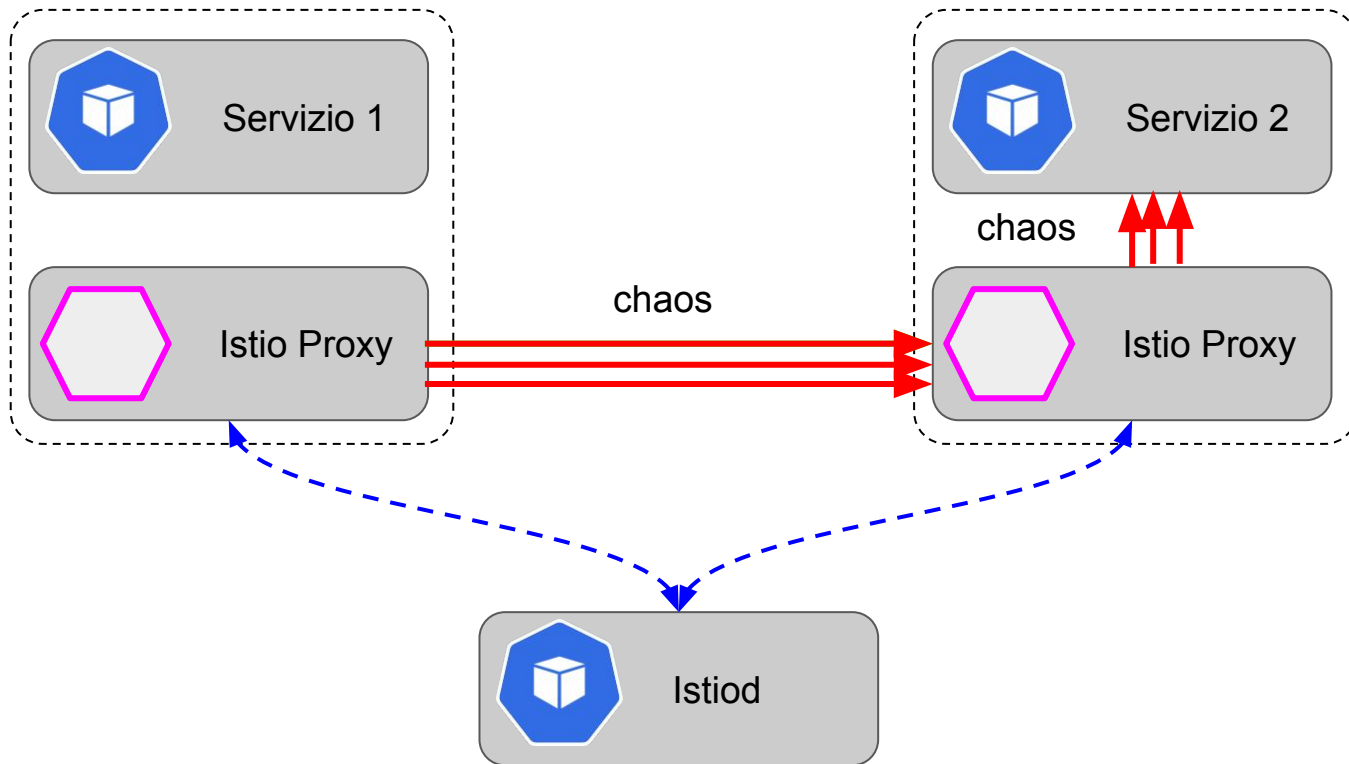
Istio: Auto mTLS



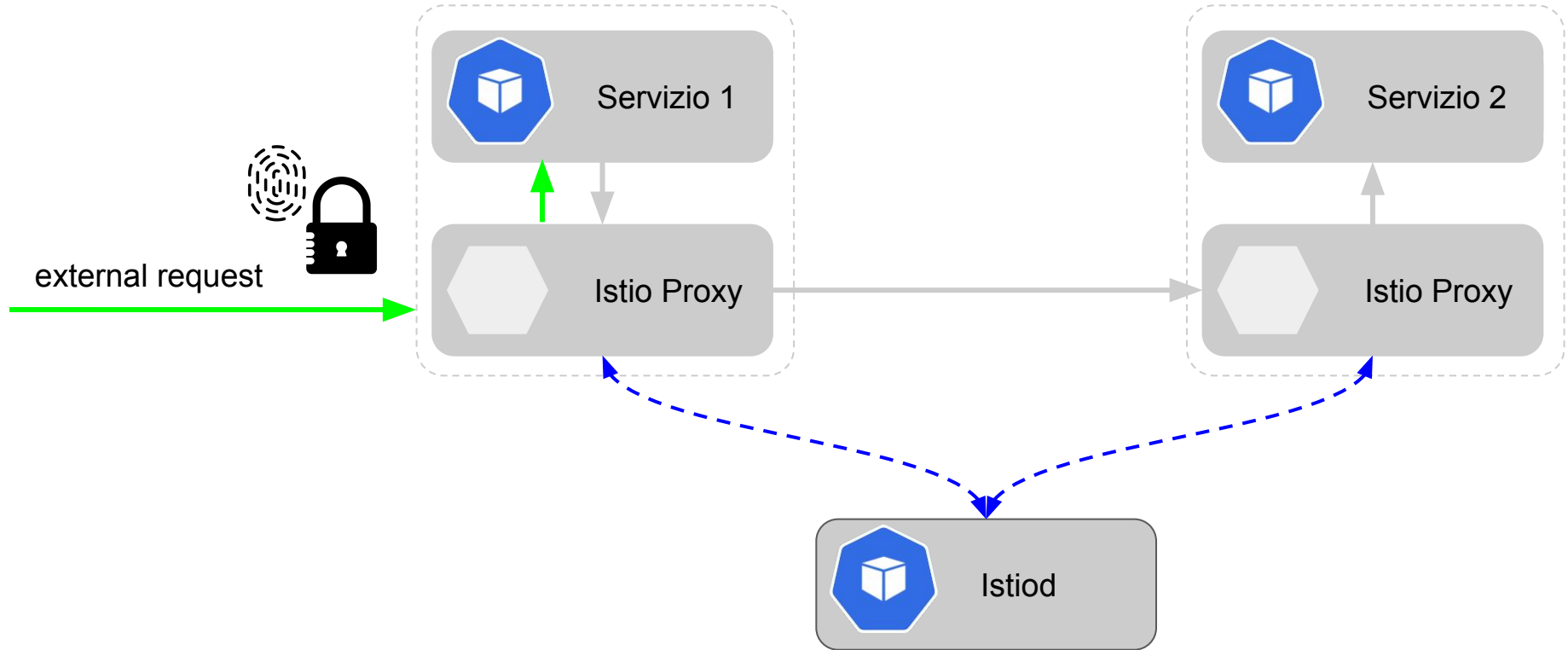
Istio: Monitoring



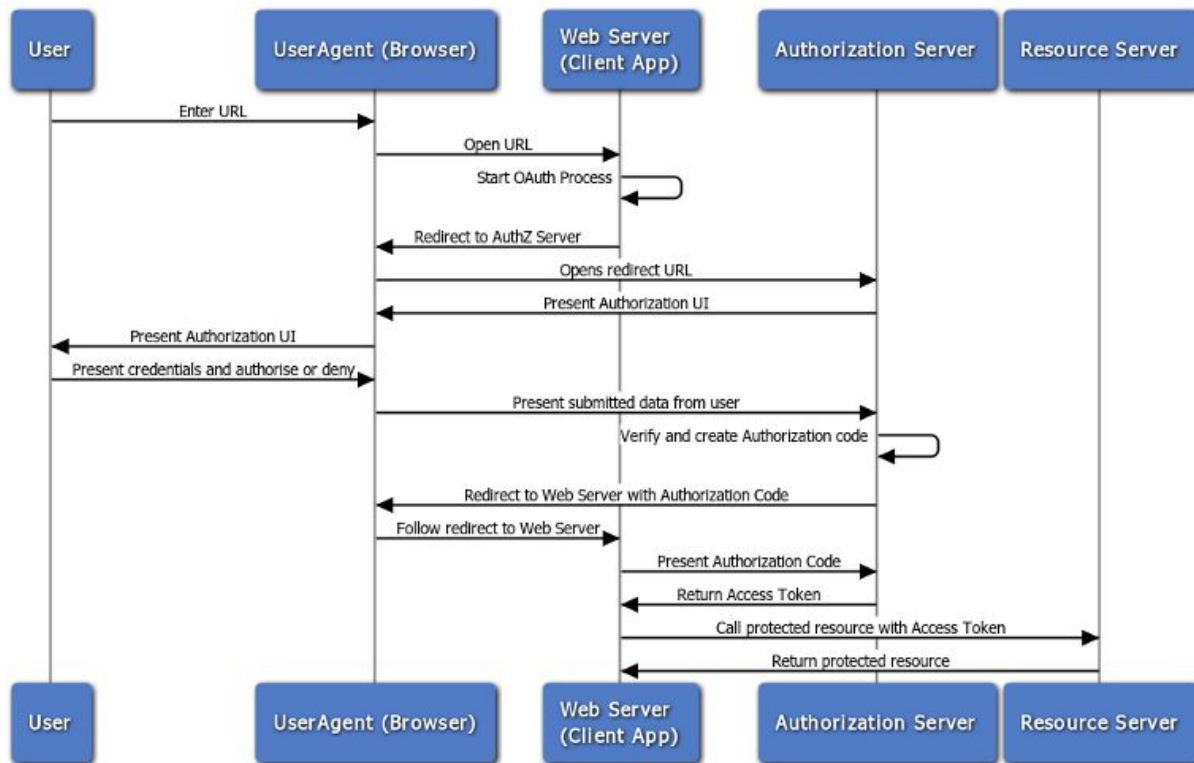
Istio: Chaos Injection



Istio: Autenticazione e Autorizzazione



Autenticazione tramite OAuth2



Token JWT

[illegible]

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "RS256",
  "kid": "88848b5aff2d5201331a547d1906e5aadf6513c8",
  "typ": "JWT"
}
```

PAYLOAD: DATA

```
{
  "name": "Ludovico Russo",
  "picture": "https://lh5.googleusercontent.com/-5FUVi6Aa5vM/AAAAAAAAAAAI/AAAAAAAAAA/AAKWJJOv58rXDjGkSHpg0MwnugTZzVtIA/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
```

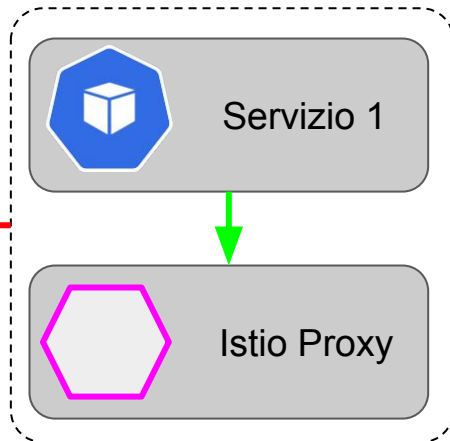
Istio: Risorsa RequestAuthentication



```
1 apiVersion: security.istio.io/v1beta1
2 kind: RequestAuthentication
3 metadata:
4   name: server
5 spec:
6   selector:
7     matchLabels:
8       name: server
9   jwtRules:
10     - issuer: https://securetoken.google.com/gdg-devfest-demo-249d4
11       jwksUri:
12         https://www.googleapis.com/service_accounts/v1/metadata/x509/secureto
13         ken@system.gserviceaccount.com
14       outputPayloadToHeader: "auth"
15       forwardOriginalToken: true
```

Istio: Risorsa RequestAuthentication

```
1 apiVersion: security.istio.io/v1beta1
2 kind: RequestAuthentication
3 metadata:
4   name: server
5 spec:
6   selector:
7     matchLabels:
8       name: server
9   jwtRules:
10     - issuer: https://securetoken.google.com/gdg-devfest-demo-249d4
11       jwksUri:
12         https://www.googleapis.com/service_accounts/v1/metadata/x509/secureto
13         ken@system.gserviceaccount.com
14     outputPayloadToHeader: "auth"
15     forwardOriginalToken: true
```

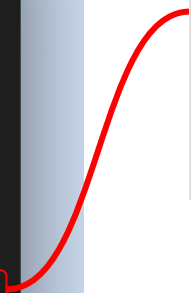


Istio: Risorsa RequestAuthentication

```
1 apiVersion: security.istio.io/v1beta1
2 kind: RequestAuthentication
3 metadata:
4   name: server
5 spec:
6   selector:
7     matchLabels:
8       name: server
9   jwtRules:
10    - issuer: https://securetoken.google.com/gdg-devfest-demo-249d4
11      jwksUri:
12        https://www.googleapis.com/service_accounts/v1/metadata/x509/secureto
13        ken@system.gserviceaccount.com
14
15    outputPayloadToHeader: "auth"
16    forwardOriginalToken: true
```

PAYLOAD: DATA

```
{
  "name": "Ludovico Russo",
  "picture":
    "https://lh5.googleusercontent.com/~5FUvi6Aa5vM/AAAAAAAAA
    I/AAAAAAAAA/AAKWJJ0v58rXDJGkSHpg@MwnugTZZavTIA/photo.jpg"
  "iss": "https://securetoken.google.com/gdg-devfest-demo-
    249d4",
  "aud": "gdg-devfest-demo-249d4",
  "auth_time": 1588411211,
  "user_id": "oPfVh4R4liVcYw1GiX3hH553gop1",
  "sub": "oPfVh4R4liVcYw1GiX3hH553gop1",
  "iat": 1588411211,
  "exp": 1588414811,
  "email": "ludovico@ludusrusso.space",
```



Istio: Risorsa RequestAuthentication

```
1 apiVersion: security.istio.io/v1beta1
2 kind: RequestAuthentication
3 metadata:
4   name: server
5 spec:
6   selector:
7     matchLabels:
8       name: server
9   jwtRules:
10    - issuer: https://securetoken.google.com/gdg-devfest-demo-249d4
11      jwksUri:
12        https://www.googleapis.com/service_accounts/v1/metadata/x509/secureto
13        ken@system.gserviceaccount.com
14      outputPayloadToHeader: "auth"
15      forwardOriginalToken: true
```

```
{
  "88848b5aff2d5201331a547d1906e5aadf6513c8": "-----BEGIN CERTIFIC
\nMIIDHCCAgSgAwIBAgIIA/oH1w0GNmMwDQYJKoZIhvcNAQEFBQAwMTEvMC0GA1UE
xMS8wLQYDVQQDEYzZWN1cmV0b2t1\nbi5zeXN0ZW0uZ3N1cnZpY2VhY2NvdW50LmN
H3SeUIR0KH8K1bjBYcF8DVZLF0xWSA1hVCbcp1t+53ICri4uWrh6VI0vv1\nnsj0u5z:
pHORHnprzDxd13jIansoj\nHO4fphkxBJiiXBaCuWreXrLdPJZiYtyuimuMtVBTfN:
8BAf8EBAMCB4AwFgYDVR0LAQH/BAwwCgYIKwYBBQUHAWIwDQYJ\nnKoZIhvcNAQEFBQ.
XHm7KNvY+c8FA\nnI7lBbf9azJcrtZGQsSbTuowTQZX1R1jBqlFWZ/bxwn6vnIU75L
8dAgNk97aQWVULrxZm/LjFh4A+FLK6FpGgITLpbp+I\nnzlhFewXrAFp8Up6U3Sch6S
"5e9ee97c840f97e0253688a3b7e94473e528a7b5": "-----BEGIN CERTIFIC
\nMIIDHCCAgSgAwIBAgIIZC7uPq+FdkiwDQYJKoZIhvcNAQEFBQAwMTEvMC0GA1UE
xMS8wLQYDVQQDEYzZWN1cmV0b2t1\nbi5zeXN0ZW0uZ3N1cnZpY2VhY2NvdW50LmN
yDssopXt6jiUGeBKMvm65fi108EfGZXCYPZVBX1dgkddRkgNA2afhvrqdf\nn7BG9U1:
65ogW/4uQCaD8V54Ncf6D\nnn0qX3qW3ze2ko1W4NdMhLhpef8nBORs1Mt7dvKxK3Q:
8BAf8EBAMCB4AwFgYDVR0LAQH/BAwwCgYIKwYBBQUHAWIwDQYJ\nnKoZIhvcNAQEFBQ.
t0ZHGAD1/d2U8\nny0wPZJWjCWHrkufPOMr2EFhw1A5PjlmBTKn9PZAQf9rWiJuYhkb
JnRbds4WbLmpzS8Fq6APa0ukHRV9cimjqmQBEJ5v6y\nnTBtNG1gPxsUJQldCKMYWmX:
}
```

Istio: Risorsa RequestAuthentication

```
1 apiVersion: security.istio.io/v1beta1
2 kind: RequestAuthentication
3 metadata:
4   name: server
5 spec:
6   selector:
7     matchLabels:
8       name: server
9   jwtRules:
10     - issuer: https://securetoken.google.com/gdg-devfest-demo-249d4
11       jwksUri: https://www.googleapis.com/service_accounts/v1/metadata/x509/secureto
12         ken@system.gserviceaccount.com
13       outputPayloadToHeader: "auth"
14       forwardOriginalToken: true
15
```

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

Istio: Risorsa AuthorizationPolicy

```
1 apiVersion: security.istio.io/v1beta1
2 kind: AuthorizationPolicy
3 metadata:
4   name: server
5 spec:
6   action: ALLOW
7   selector:
8     matchLabels:
9       name: server
10  rules:
11    - from:
12      - source:
13        requestPrincipals: ["*"]
14
```

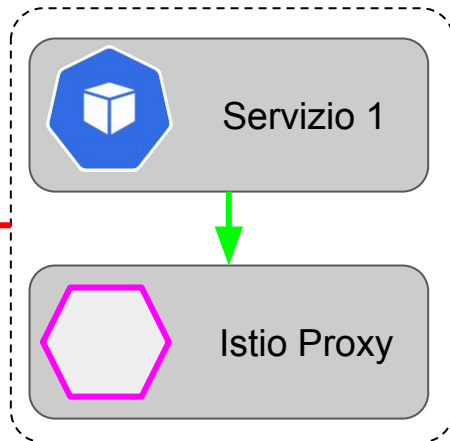
Istio: Risorsa AuthorizationPolicy

```
1 apiVersion: security.istio.io/v1beta1
2 kind: AuthorizationPolicy
3 metadata:
4   name: server
5 spec:
6   action: ALLOW
7   selector:
8     matchLabels:
9       name: server
10  rules:
11    - from:
12      - source:
13        requestPrincipals: ["*"]
14
```

- ALLOW
- DENY

Istio: Risorsa AuthorizationPolicy

```
1 apiVersion: security.istio.io/v1beta1
2 kind: AuthorizationPolicy
3 metadata:
4   name: server
5 spec:
6   action: ALLOW
7   selector:
8     matchLabels:
9       name: server
10  rules:
11    - from:
12      - source:
13        requestPrincipals: ["*"]
14
```



Istio: Risorsa AuthorizationPolicy

```
1 apiVersion: security.istio.io/v1beta1
2 kind: AuthorizationPolicy
3 metadata:
4   name: server
5 spec:
6   action: ALLOW
7   selector:
8     matchLabels:
9       name: server
10  rules:
11    - from:
12      - source:
13        requestPrincipals: ["*"]
14
```

Chi è autorizzato a chiamare questo servizio?

Tutti gli utenti autenticati tramite token JWT

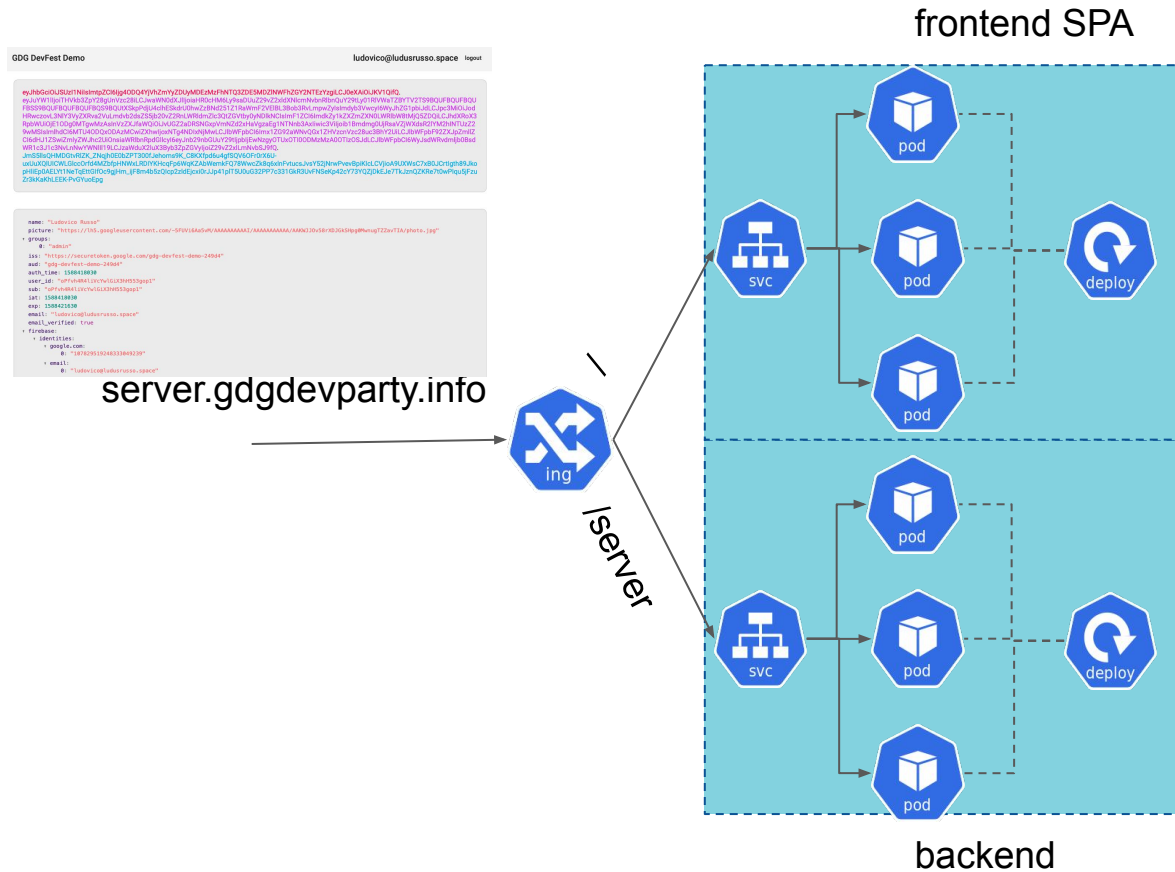
Istio: Risorsa AuthorizationPolicy

```
6  action: ALLOW
7  selector:
8    matchLabels:
9      name: server
10 rules:
11   - from:
12     - source:
13       requestPrincipals: ['*']
14     when:
15       - key: request.auth.claims[groups]
16         values:
17           - 'admin'
```

Chi è autorizzato a chiamare questo servizio?

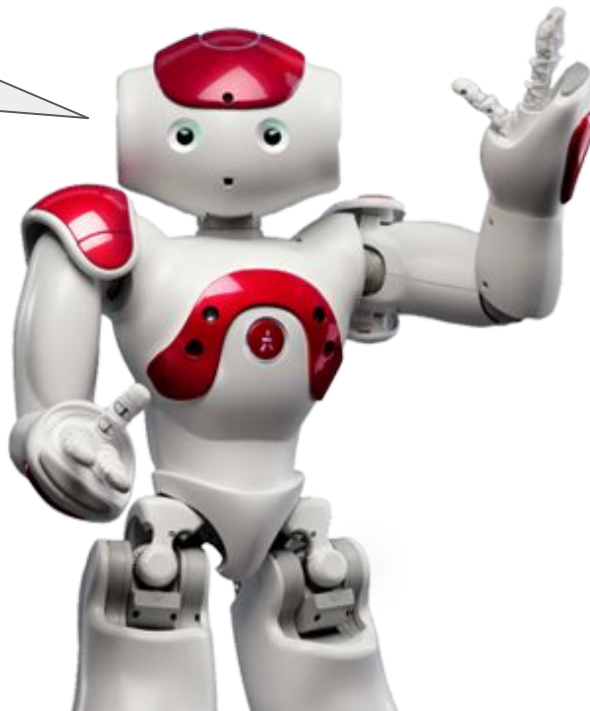
Tutti gli utenti autenticati tramite token JWT che appartengono al gruppo “admin”

Demo TIME



Grazie per l'attenzione

Domande?



Slide e Codice

