

Envoy Gateway API

TLS Magic



Agenda



1. Envoy Gateway API
2. Cert-Manager
3. Demo

Envoy Gateway API

Same features as Azure Application Gateway for Containers:

- Gateway
- GatewayClass
- HTTPRoute

No Azure integration, e.g. no Azure WAF

Cert-Manager

Use of Certificate object is optional

Add ClusterIssuer name to Gateway as annotation

```
apiVersion: gateway.networking.k8s.io/v1
kind: Gateway
metadata:
  name: $GatewayName
  namespace: $GatewayNamespace
  annotations:
    cert-manager.io/cluster-issuer: $ClusterIssuerName
spec:
  gatewayClassName: $GatewayClassName
  listeners:
```

```
apiVersion: cert-manager.io/v1
kind: Certificate
metadata:
  name: $TraefikCertificateName
  namespace: $InfrastructureNamespace
spec:
  secretName: $TraefikSecretName
  issuerRef:
    name: $ClusterIssuerName
    kind: ClusterIssuer
  dnsNames:
    - $TraefikUrl
```

Cert-Manager

Use of Certificate object is optional

Add ClusterIssuer name to Gateway as annotation

Cert-Manager will create certificate when TLS secret is configured in Gateway listener

```
- name: traefik-https-listener
  port: 443
  protocol: HTTPS
  hostname: $TraefikUrl
  allowedRoutes:
    namespaces:
      from: All
  tls:
    certificateRefs:
      - group: ""
        kind: Secret
        name: $TraefikSecretName
```

Demo