The bridge to possible

Apache Kafka with Istio on K8s

Sebastian Toader & Zsolt Varga

2021-Feb-26

Production grade Apache Kafka on Kubernetes

- Scalability
- Resiliency
- Security
- Observability
- Disaster recovery

Security goals

- Secure communication using mTLS between all services
- Configurable short-lived certificates
- On the fly certificate renewals with no service downtime
- Unified simplified configuration to enable mTLS for all services
- Kubernetes service account based authn/authz
- Secure cross-cluster interaction between client apps and Kafka

Challenges – Kafka broker SSL with client auth

- Kafka brokers require private-key and certificate pairs
- Private keys and certificates are stored in keystore and truststore files in JKS or PKCS12 or PEM format

Challenges – Certificate renewal

- Certificate renewal requires keystore and truststore regeneration
- Broker pods need restarting to pick up the modified keystore and truststore files
- May cause service degradation

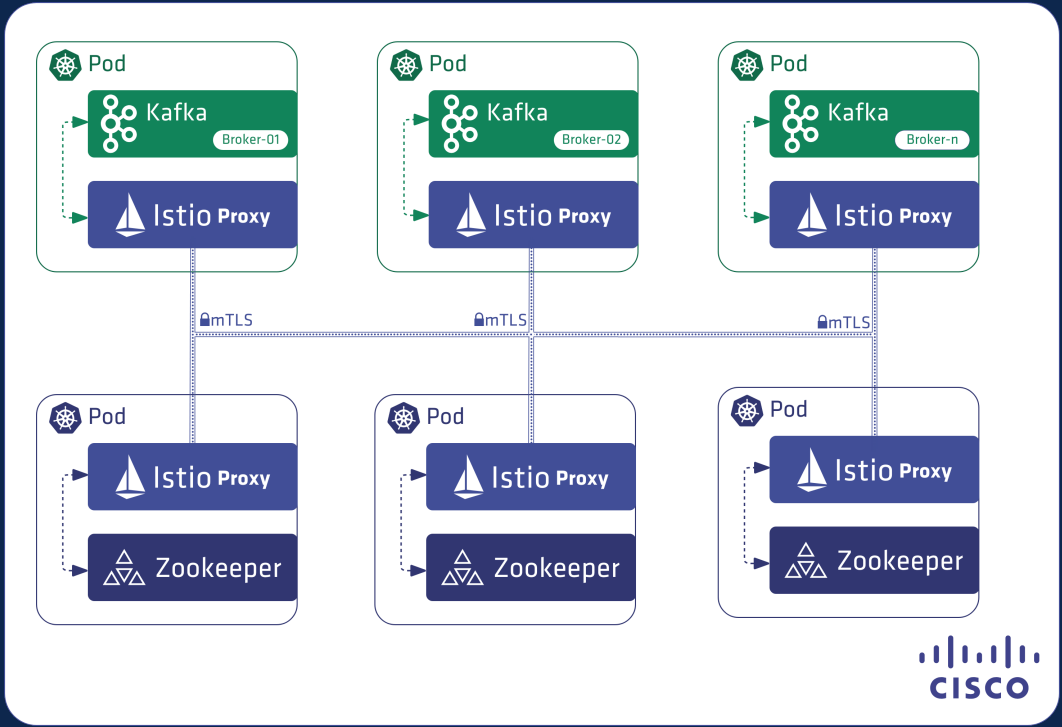
Challenges – Client certificates

- Client certificates has be created for each separate client identity
- Client certificates may take different formats (JKS, PEM, etc)
- Client certificate renewal may require client application restarts

Security layer provided by Istio

- mTLS provided by Istio
- Server certificate provided by Istio Proxy sidecar container
- Each Kafka client request gets a client certificate attached automatically by Istio Proxy sidecar container
- Client certificate includes the K8s service account of the Kafka client application
  - *SPIFE://<trust domain>/ns/<namespace>/sa/<service account name>*
- Configurable certificate expiration
- On the fly certificate renewal
- Kafka listeners configured in PLAINTEXT mode

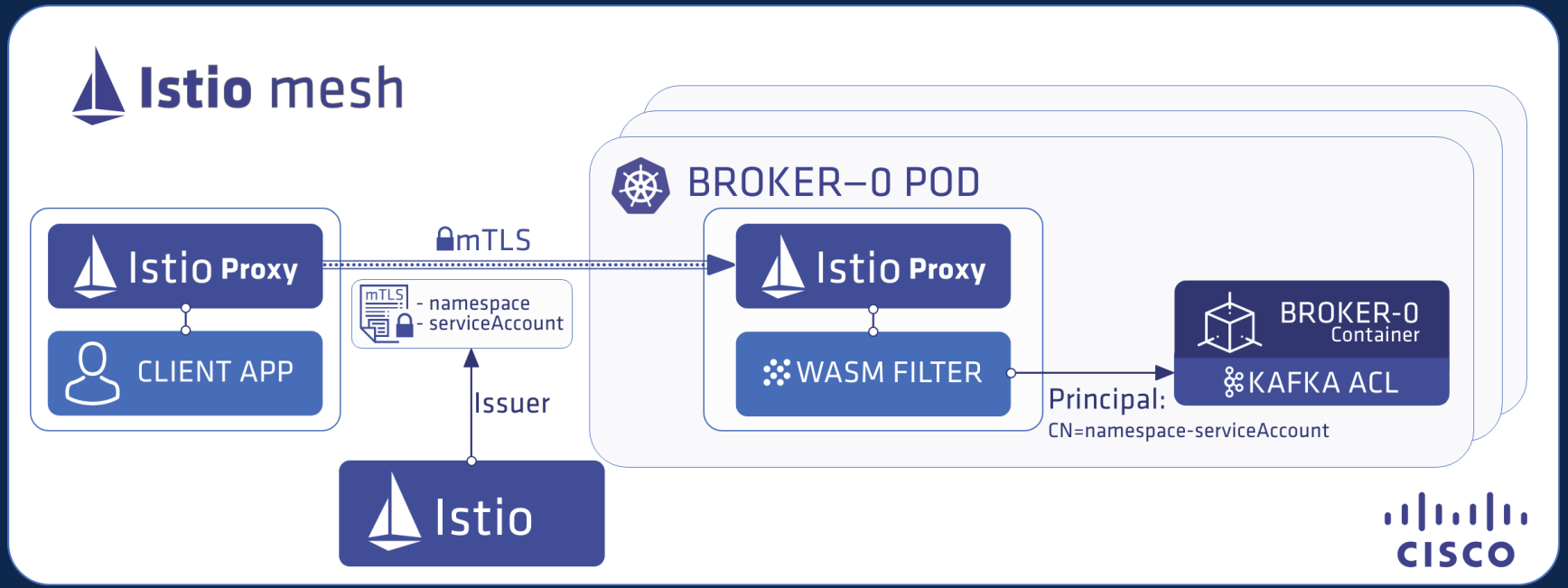
Security layer provided by Istio



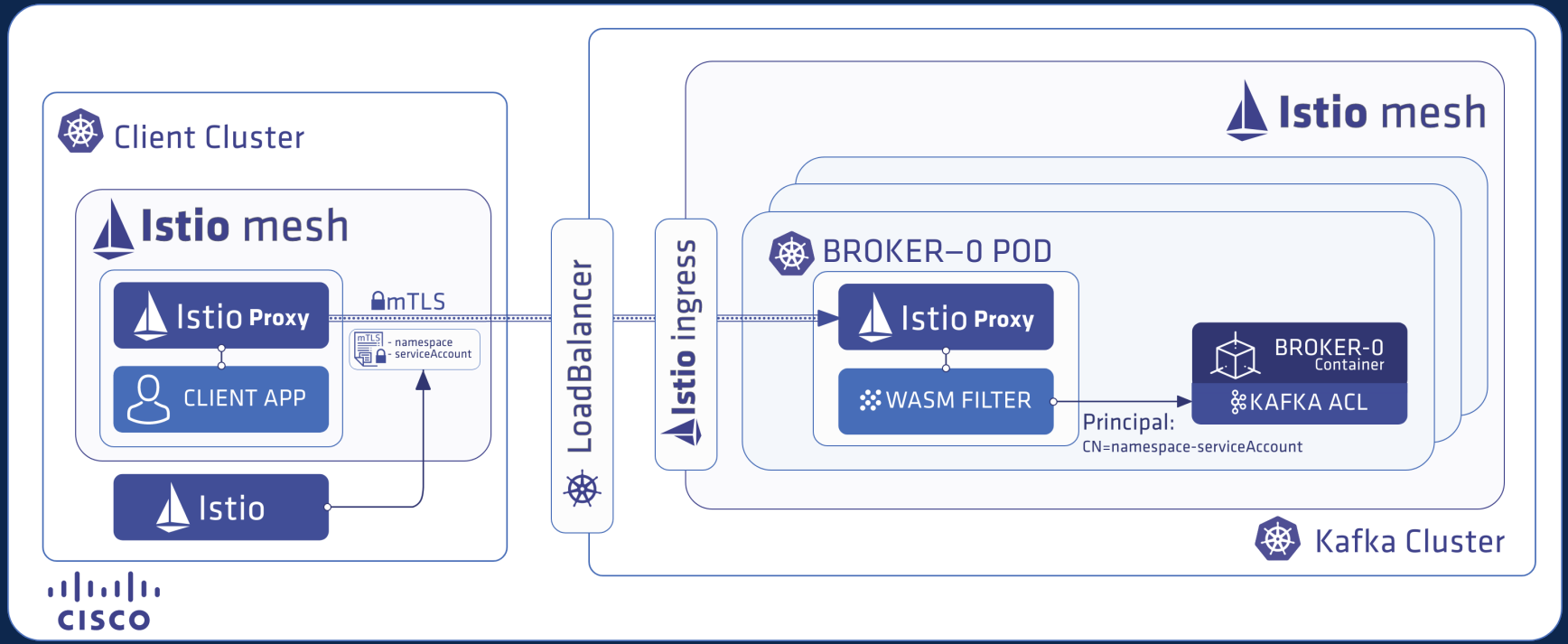
Kafka client authentication with Istio

- Kafka does not process client certificate in PLAINTEXT mode
- Envoy WASM filter extracts client identity from client certificate and passes it to Kafka

Kafka client authentication with Istio



Kafka client authentication with Istio



Takeaway

- Istio provides a security layer for workloads in a uniform way
- Envoy WASM filters opens the gates for a whole array of useful features such as Kafka protocol level metrics, extended client throttling, audit logs to name a few

Q&A

The bridge to possible

Thank you