Istio Certificate Management Through Vault

Lei Tang, Yonggang Liu, Google LLC.
Lei Tang
Software Engineer
Istio
leitang@google.com
wechat: LTANG2015

Oliver (Yonggang) Liu
Software Engineer
Istio
yonggangl@google.com
http://oliverliu.org
Istio manages your microservices

Relieve burden of service owners.
Bring order to chaos.
Istio 30,000-foot view

Control Plane
- Pilot
- Citadel
- Mixer

Data Plane
- Envoy
  - Service A
- Envoy
  - Service B

Internet request

policies

Security
Traffic management
Telemetry
Quota
Security risks for service meshes

Is the user authorized to call the service?

Is the traffic secure?

Service mesh

Is a service authorized to call another service?

Service A

Service B
Solution: Istio security

- BeyondCorp
- ALTS
- Zero-trust network
- Context-aware access control
- Secure by default
- Authentication
- Authorization
- Encryption

- Perimeter
  - Istio Ingress/Egress
- Mesh
  - Control Plane
  - Authentication
  - Authorization
  - Encryption
  - Istio sidecar
Istio context-aware access control

Identity and other context

JWT (Json Web Token)

{ "typ": "JWT" }

{ "iss": "issuer@example.com", "groups": ["dev", "admin"] }

{RSA-SHA256(header+payload)}

Role

Certificate

Certificate:

Subject Alternative Name:

spiffe://cluster.local/ns/{name-space}/sa/{service-account-name}

Resource
Example flow of context-aware access

1: deploy policies

2: push authn and authz config

3: request+ context (e.g., JWT, cert.)

4: authenticated context claims
Demo: Istio context-aware access control

- A user must be in a specific group to access a sensitive service.
- The access must be protected by mTLS.
- May also control the calling path.
Demo: authorization policies

apiVersion: "rbac.istio.io/v1alpha1"
kind: ServiceRole
metadata:
  name: httpbin-viewer
spec:
  rules:
  - services:
      - "httpbin.rbac-groups-test-ns.svc.cluster.local"
    methods: ["GET"]
...

apiVersion: "rbac.istio.io/v1alpha1"
kind: ServiceRoleBinding
metadata:
  name: bind-httpbin-viewer
spec:
  subjects:
  - properties:
      request.auth.claims[groups]: "group1"
    roleRef:
      kind: ServiceRole
      name: "httpbin-viewer"
...

apiVersion: "authentication.istio.io/v1alpha1"
kind: "Policy"
metadata:
  name: "require-mtls-jwt"
spec:
  targets:
    - name: httpbin
  peers:
    - mtls: {}
  origins:
    - jwt:
        issuer: "testing@secure.istio.io"
Demo of Istio context-aware access control
Certificate Provision Flow

- Citadel
- Node Agent
- K8s Node
- Workload
- Envoy
- Pod
- CSR
- K8s JWT
- SDS API
- Certificate
## Integration with external CAs

<table>
<thead>
<tr>
<th></th>
<th>Signing-key -injection</th>
<th>Citadel -integration</th>
<th>Nodeagent -integration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Automatic key and cert provision</strong></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Citadel involvement</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
Approach 1: Signing-key-injection

- Operator involved for signing key and cert rotation
Approach 2: Citadel-integration

- Citadel authenticates and authorizes the CSRs
- Citadel is delegated to request certificates for workloads
Approach 3: Nodeagent-integration

- The external CA handles the authentication and authorization of the workload CSRs
- The node agent forwards workload K8s JWT
Prototype: Istio CA Vault integration

- Citadel
  - CA key
  - CSR → Certificate
  - Node Agent
  - SDS (JWT) → Certificate
  - Pod

- Vault
  - CA key
  - CSR → Certificate
  - Node Agent
  - SDS (JWT) → Certificate
  - Pod
Istio CA Vault integration

1. SDS+JWT (SA1)
Istio CA Vault integration

1. SDS+JWT (SA1)
2. CSR, k8s SA1
3. JWT(SA1)

Authn, authz based on SA1

Does the identity in SA1 match that in the SPIFFE SAN of CSR?
Istio CA Vault integration

1. SDS+JWT (SA1)
2. CSR, k8s SA1
3. JWT(SA1)
4. CSR, k8s SA of Citadel
5. SA of Citadel

Does the identity in SA1 match that in the SPIFFE SAN of CSR?
Demo of Istio CA Vault integration
Istio survey

We would love to hear your feedbacks on Istio. Please fill the survey on the survey website; we have rewards waiting for you :)