Member-only story

# Istio MTLS configuration: Validate client

Indika Udagedara · Follow

2 min read · Aug 29, 2021

This is mostly a note to self…

Istio supports MTLS to authenticate clients. This is configured using a `Gateway` resource. There's great documentation on the configuration steps here. However, what's not quite clear is how to validate client identity using the `subjectAltName` (SAN) presented in the client certificate. In the example from Istio documentation, any client who presents a certificate using a given CA is accepted which is not desired in certain cases e.g. server exposed to multiple clients in the same network but accepts traffic only from specific clients.

Starting from the example here, MTLS client validation is done by adding `tls.subjectAltNames`

```
apiVersion: networking.istio.io/v1alpha3
kind: Gateway

... <snip> ...

tls:
     mode: MUTUAL
     credentialName: httpbin-credential
     subjectAltNames:
      - client.example.com
```

The caveat is, Istio validates only the SAN and not the Common Name (CN).

To create a CSR with SANs, do

```
openssl req -nodes -newkey rsa:2048 -subj
"/CN=client.example.com/O=client organization" -out
client.example.com.csr -pubkey -new -keyout client.example.com.key -
sha256 -config ssl.cnf
```

where `ssl.cnf` is

```
[ CA_default ]
copy_extensions = copy

[req]
req_extensions = v3_req
distinguished_name = req_distinguished_name

[req_distinguished_name]

[ v3_req ]
# Extensions to add to a certificate request
basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
subjectAltName = client.example.com
```

To sign the client certificate, do

```
openssl x509 -req -in client.example.com.csr -CA example.com.crt -
CAkey example.com.key -CAcreateserial -out client.example.com.crt -
days 3650 -sha256 -extfile ssl-ext.cnf
```

where `ssl-ext.cnf` is

```
basicConstraints = CA:FALSE
subjectAltName = client.example.com
```

and CA certificate/key are generated from

```
openssl req -x509 -sha256 -nodes -days 365 -newkey rsa:2048 -subj
'/O=example Inc./CN=example.com' -keyout example.com.key -out
example.com.crt
```

Server certificates installed installed in `Gateway.tls.credentialName` are generated from

```
openssl req -out httpbin.example.com.csr -newkey rsa:2048 -nodes -
keyout httpbin.example.com.key -subj
"/CN=httpbin.example.com/O=httpbin organization"
openssl x509 -req -days 365 -CA example.com.crt -CAkey
example.com.key -set_serial 0 -in httpbin.example.com.csr -out
httpbin.example.com.crt
```

The credential contains

```
$ kubectl describe secrets/httpbin-credential -n istio-system

... <snip> ...

Data
====
ca.crt:   1046 bytes
tls.crt:  1054 bytes
tls.key:  1708 bytes
```

To test (against the httpbin server in the example)

```
curl -vvv -HHost:httpbin.example.com --resolve
"httpbin.example.com:$SECURE_INGRESS_PORT:$INGRESS_HOST" \
--cacert example.com.crt --cert client.example.com.crt --key
client.example.com.key \
"https://httpbin.example.com:$SECURE_INGRESS_PORT/status/418"
```

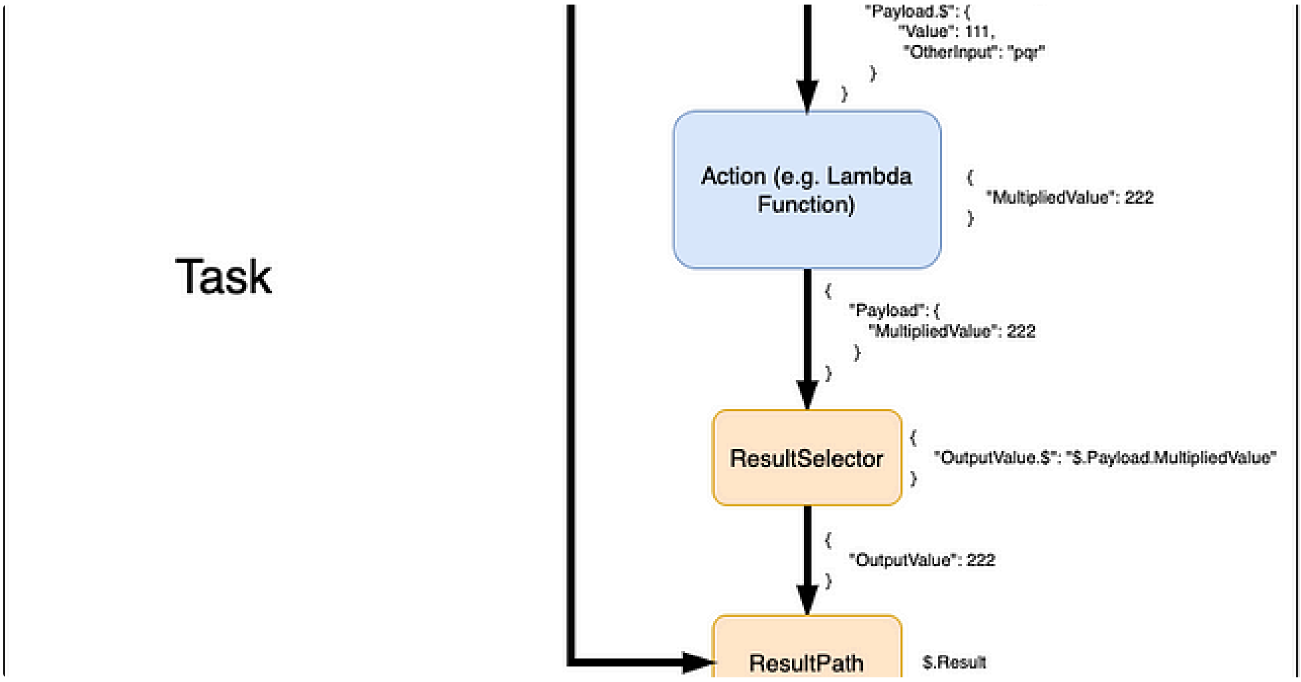
Istio Kubernetes Tls

Follow

## Written by Indika Udagedara

0 Followers

### More from Indika Udagedara



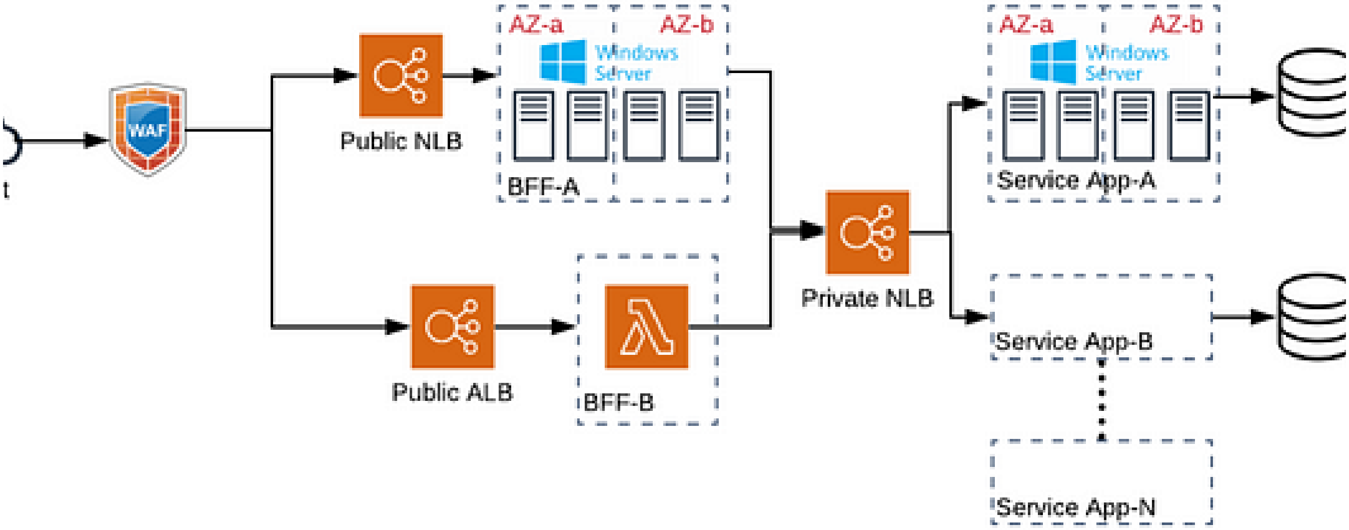
Indika Udagedara

## AWS Step Functions data processing simplified

AWS Step Functions is a powerful workflow engine that offers a lot of customization options. There is a lot of documentation available on...

✦ · 4 min read · Jan 20, 2023

1



Indika Udagedara

## AWS NLB random timeouts with Windows Server/IIS

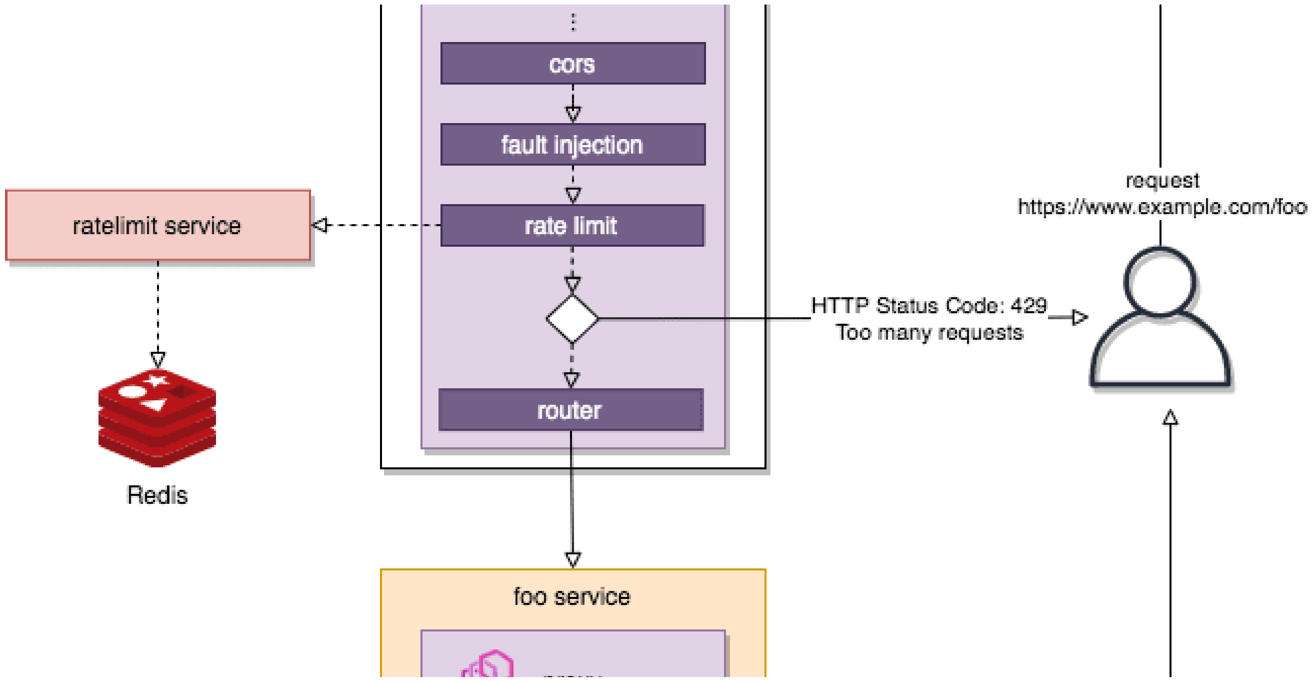
This post is about an issue I faced with one of our customers who have their Microservices running on Windows Server and IIS. The servers...

✦ · 7 min read · Sep 1, 2021

3

See all from Indika Udagedara

## Recommended from Medium



ishujeet panjeta

## Mastering Istio Rate Limiting for Efficient Traffic Management

Istio, the powerful open-source service mesh, offers a plethora of features to enhance microservices architecture. One crucial capability...

6 min read · Nov 24, 2023

7 1

Deciphering Istio Multi-Cluster Authentication
Unveiling the Initial mTLS Connection Process
for Remote Gateways

Jimmy Song

## Deciphering Istio Multi-Cluster Authentication & mTLS Connection

Introduction

3 min read · Jan 16, 2024

3

## Lists

Natural Language Processing

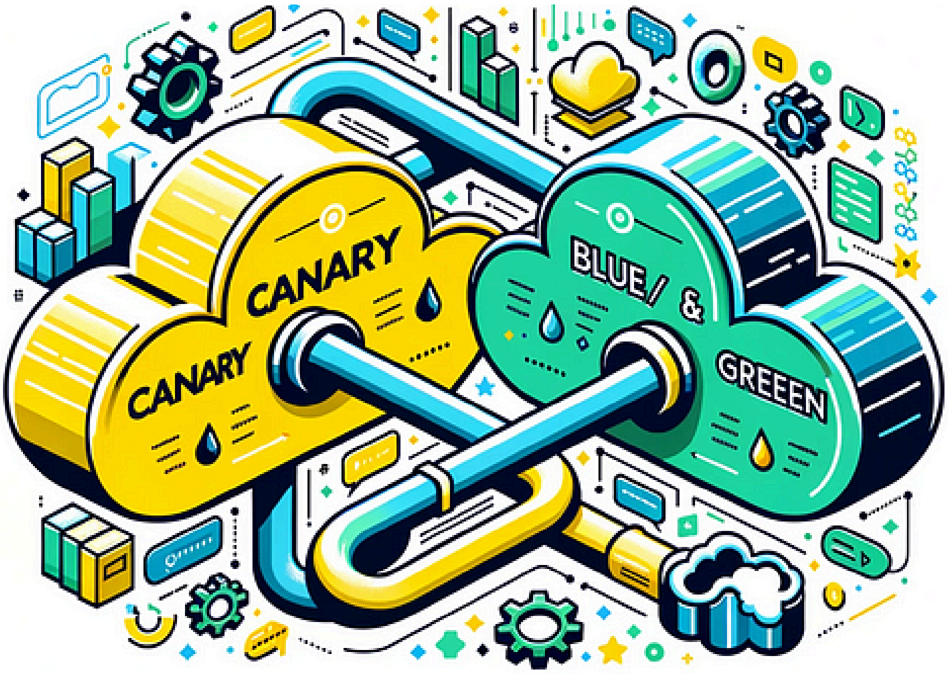
1377 stories · 871 saves

Ric Hincapie

### Istio global rate limit based on path

This article is for those who are starting with Istio rate limit feature aiming to understand how rate limit based on request path works...

6 min read · Nov 29, 2023



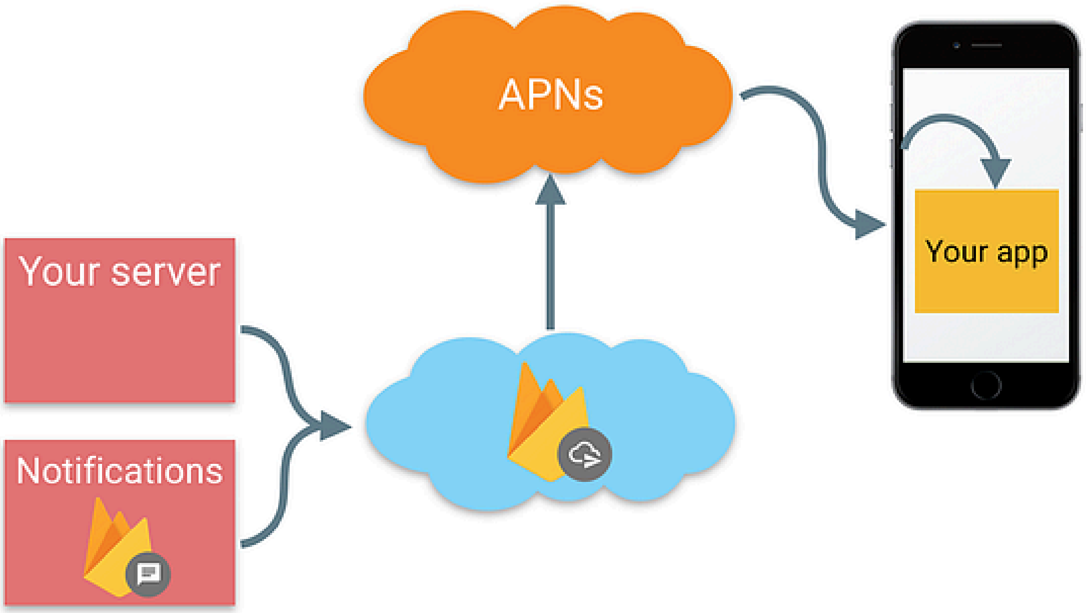
Your cloud Your way

## Canary deployment with Istio and Microk8s

Introduction

5 min read · Oct 23, 2023

1



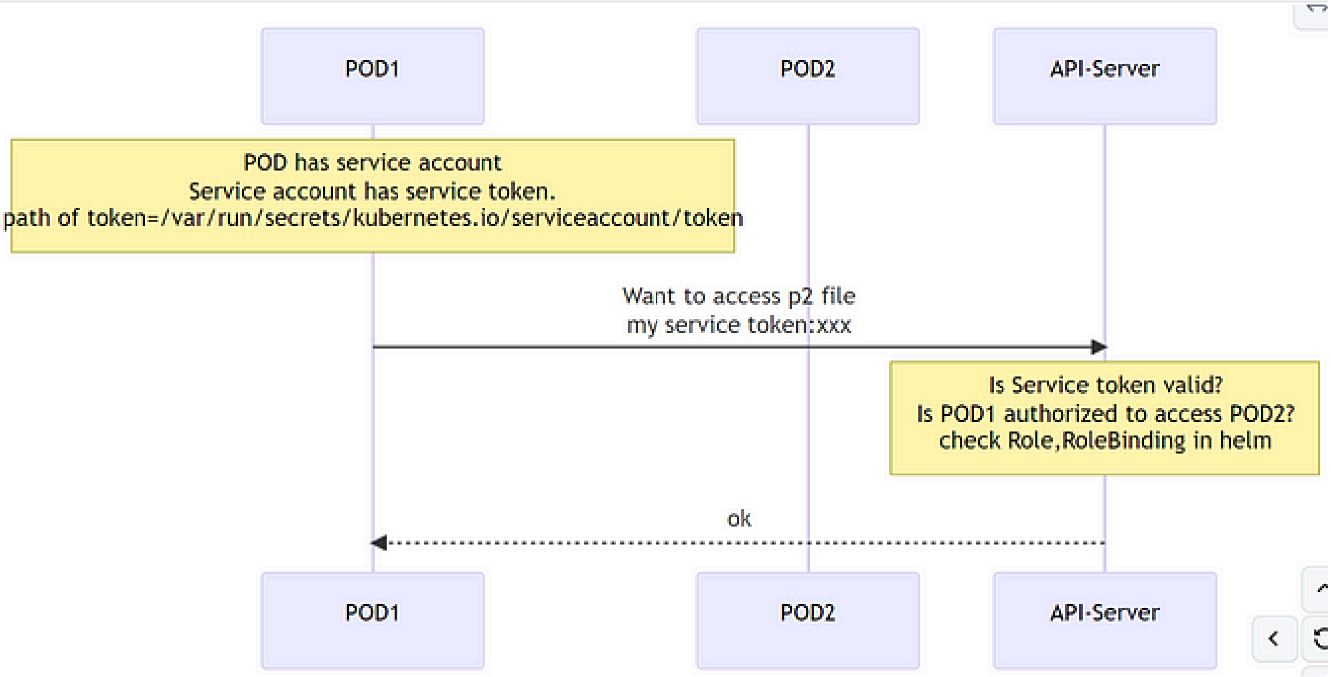
Dmitrijs Beloborodovs in Citadele Bank Developers

## iOS Push Notifications: Part 5—Firebase

There are many third party services helping to integrate push notification sending across different platform (Android & iOS) with your...

5 min read · Mar 21, 2024

49


POD1
POD2
API-Server
POD has service account
Service account has service token.
path of token=/var/run/secrets/kubernetes.io/serviceaccount/token
Want to access p2 file
my service token:xxx
Is Service token valid?
Is POD1 authorized to access POD2?
check Role,RoleBinding in helm
ok
POD1
POD2
API-Server

Everything is MindGame

## Kubernetes Authorization (Service Token, Istio AuthorizationPolicy)

Authorization in kubernetes means, how microservice-1, identifies itself to API server to use end points/resources exposed by...

3 min read · Nov 14, 2023

See more recommendations