
KubeCon
CloudNativeCon
North America 2018
Athenz with Istio:
Single Access Control Model in
Cloud Infrastructures

Agenda

- What is Athenz?
  - Service Authentication
  - Authorization
- Multi-cloud in Yahoo Japan
- How do we integrate with Istio?
  - Why Istio?
  - Benefit of using Athenz with Istio

About

- Tatsuya Yano
  - Platform Developer, Yahoo Japan Corporation
  - Contributor to Athenz
  - Open Source Summit Japan (https://sched.co/FDjp)

Athenz: Open Source System
Created by Yahoo Inc.

- Service Authentication
  - Provide secure identity in the form short lived x.509 certificate to every workload / service in modern environments
- Authorization
  - Provides fine-grained Role Based Access Control (RBAC)

Service Authentication

Authentication

- User Authentication
  - AD / LDAP / Kerberos / etc
- Service Authentication
  - Instances within a service with a unique identity to enable secure communication
    - IP / Networks ACLs / iptable
    - Headless/Automation users
    - Shared secrets
    - Mutual TLS with x.509 certificates

Certificate Based Authentication

- Every instance / service in your cloud has its own identity
- Stronger security by Mutual TLS Authentication
- Zero-trust security
- Short Lived Certificates

Copper Argos

- Generalized model for authorized service providers to launch other service identities in an authorized way through a callback-based verification model.

Providers


OpenStack


Kubernetes

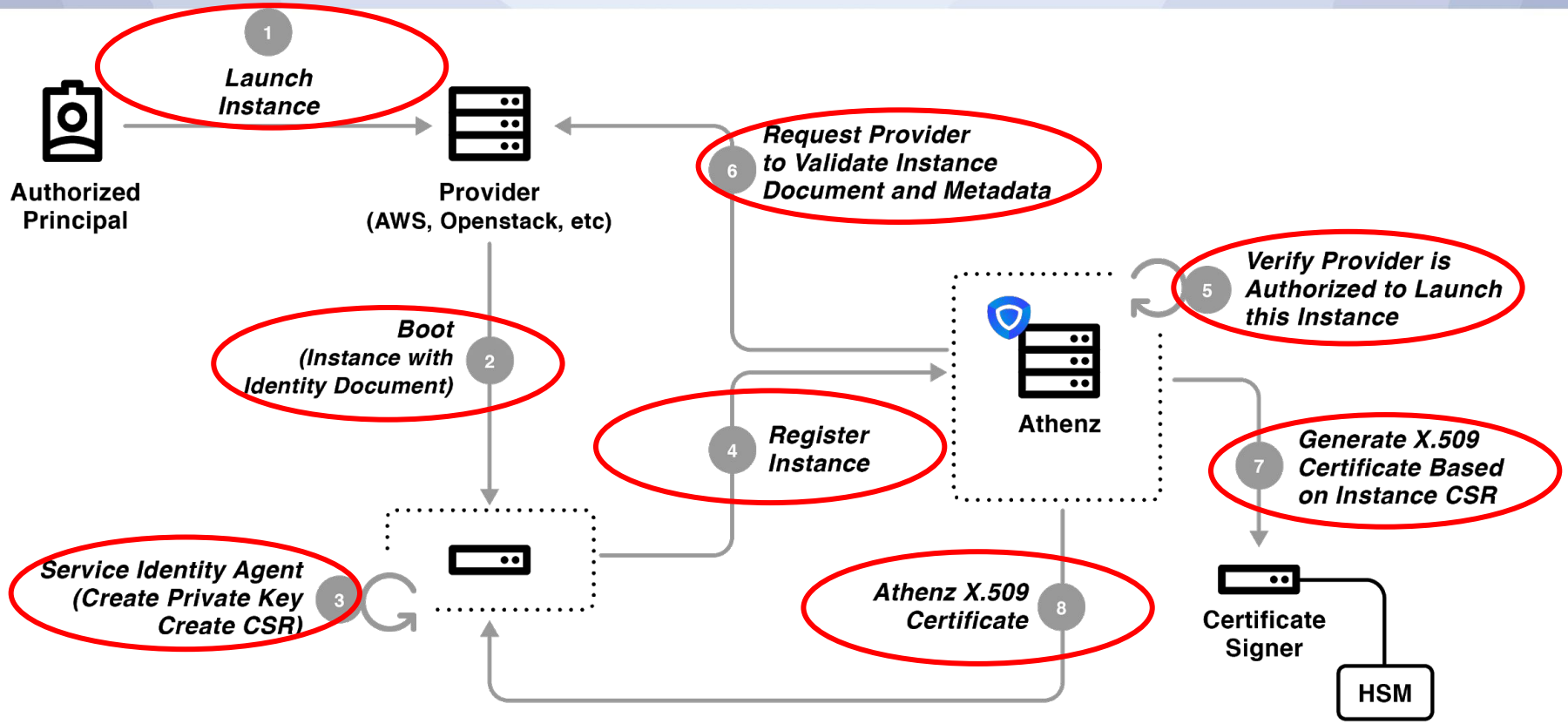

Screwdriver


Amazon EC2


AWS ECS

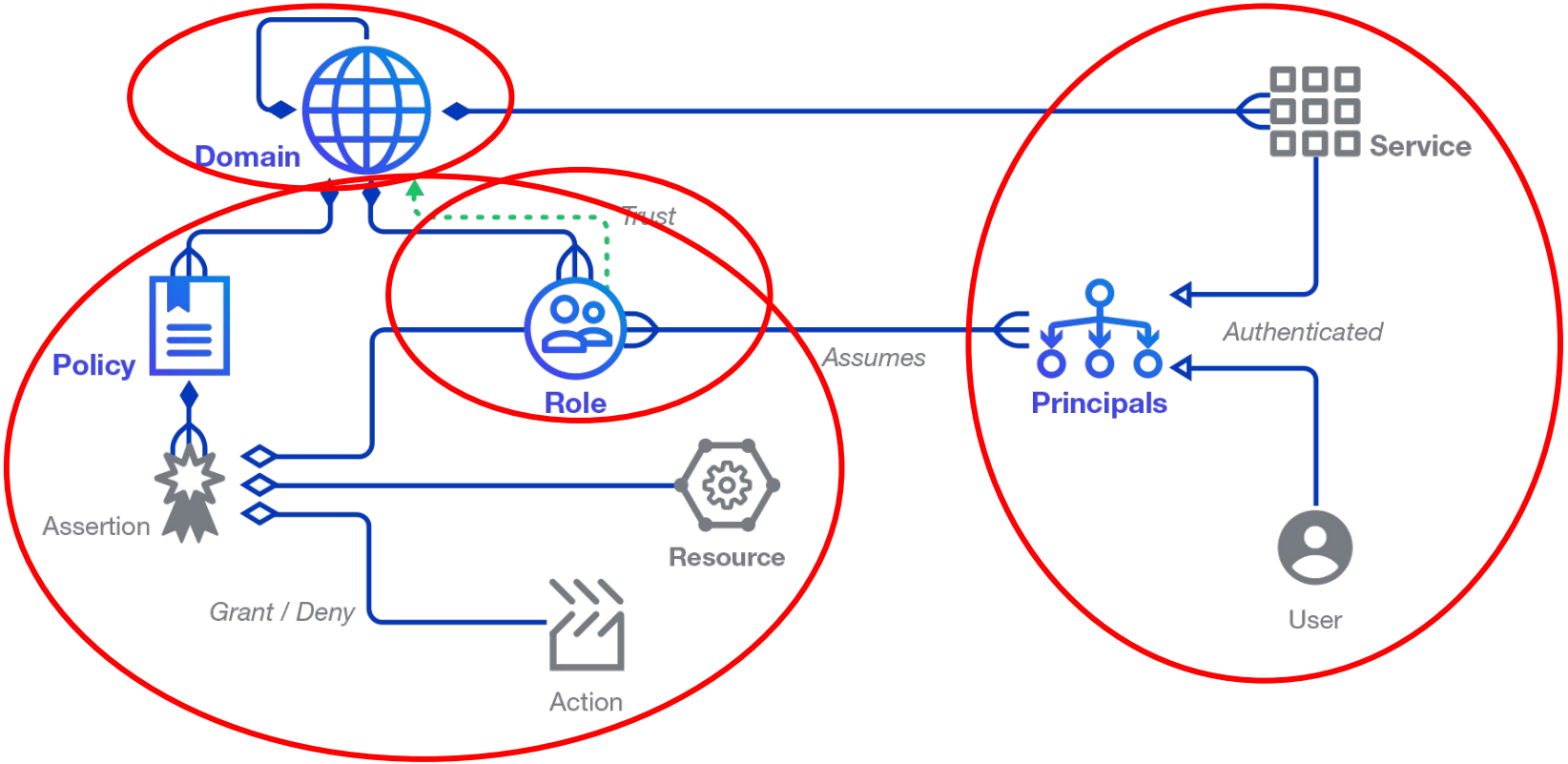

AWS Lambda

Bootstrapping Athenz Identity



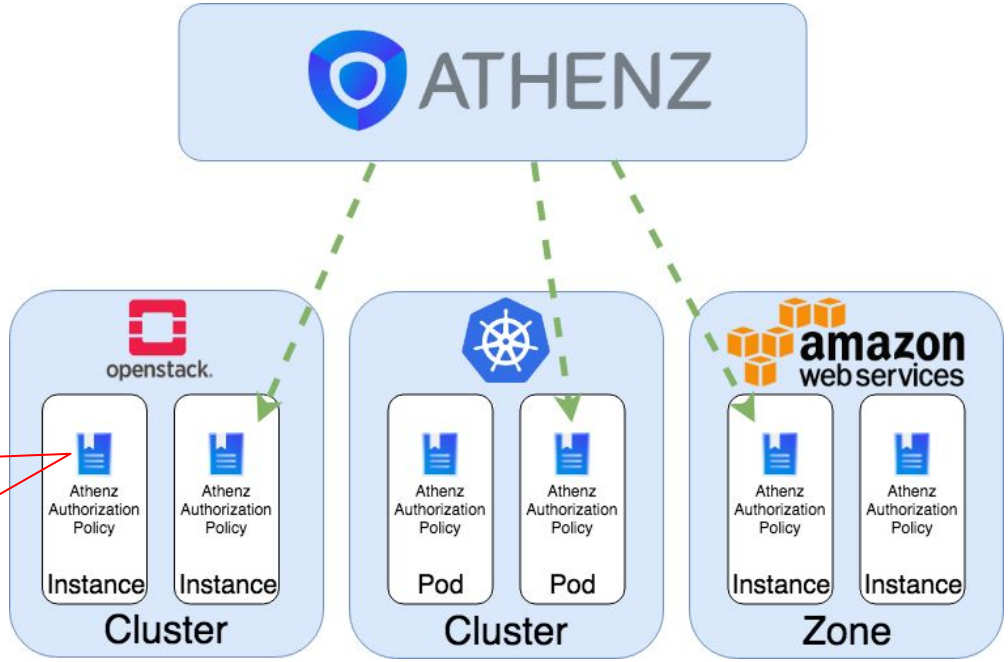

KubeCon
CloudNativeCon
North America 2018
Authorization

Athenz Data Model

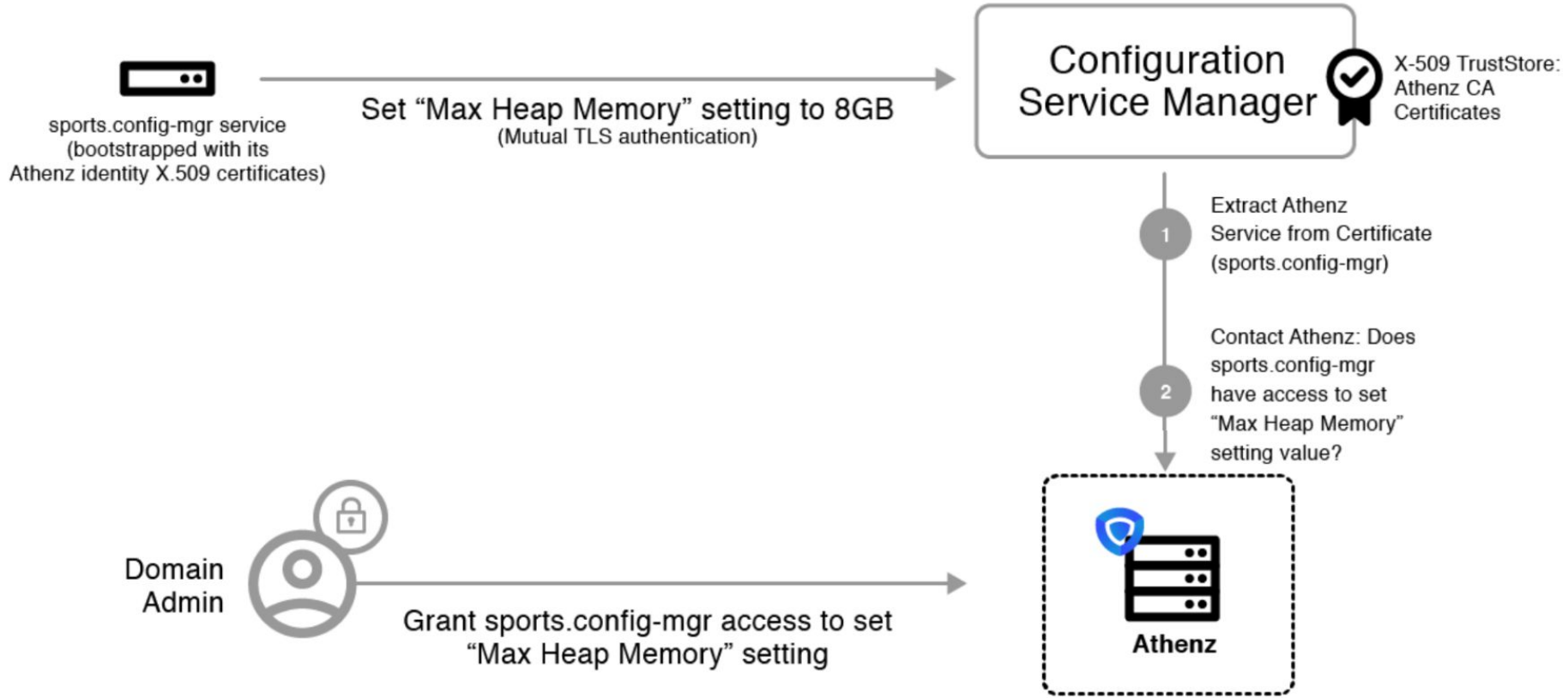


Domain data example (YAML)

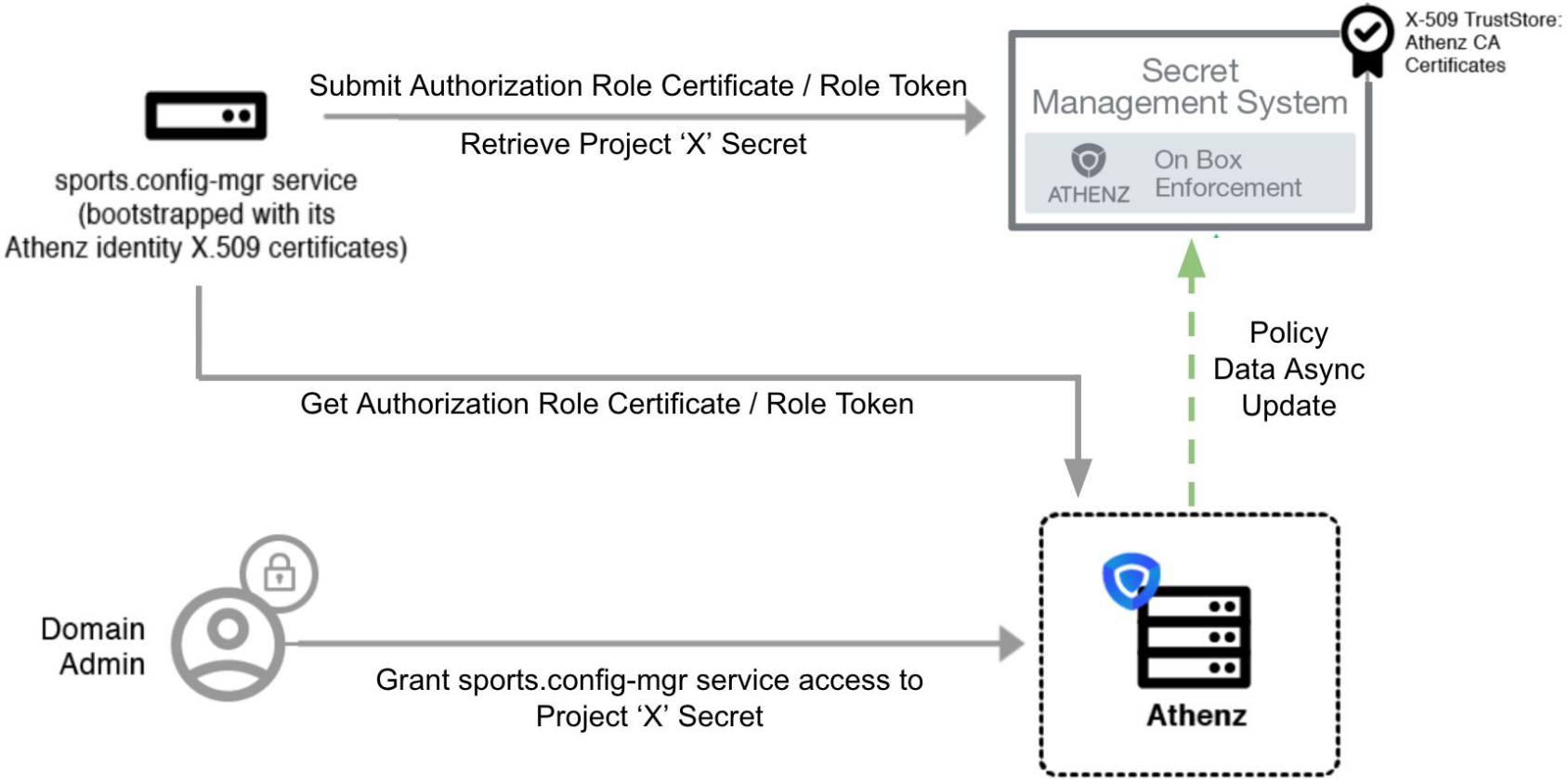

```yaml
domain:
    name: athenz
    audit_enabled: false
    modified: 2018-12-11T08:21:25.896Z
    roles:
        - name: admin
          members:
            - user.admin
        - name: frontend
          members:
            - athenz.instance
    policies:
        - name: admin
          assertions:
            - grant * to admin on *
        - name: blacklist
          assertions:
            - deny post to admin on webapi/secret
        - name: whitelist
          assertions:
            - grant get to frontend on webapi/backend
            - grant post to frontend on webapi/backend
    services:
        - name: athenz.instance
          modified: 2018-12-10T23:45:48.188Z
          publicKeys: []
```



Authorization - Centralized Access Control



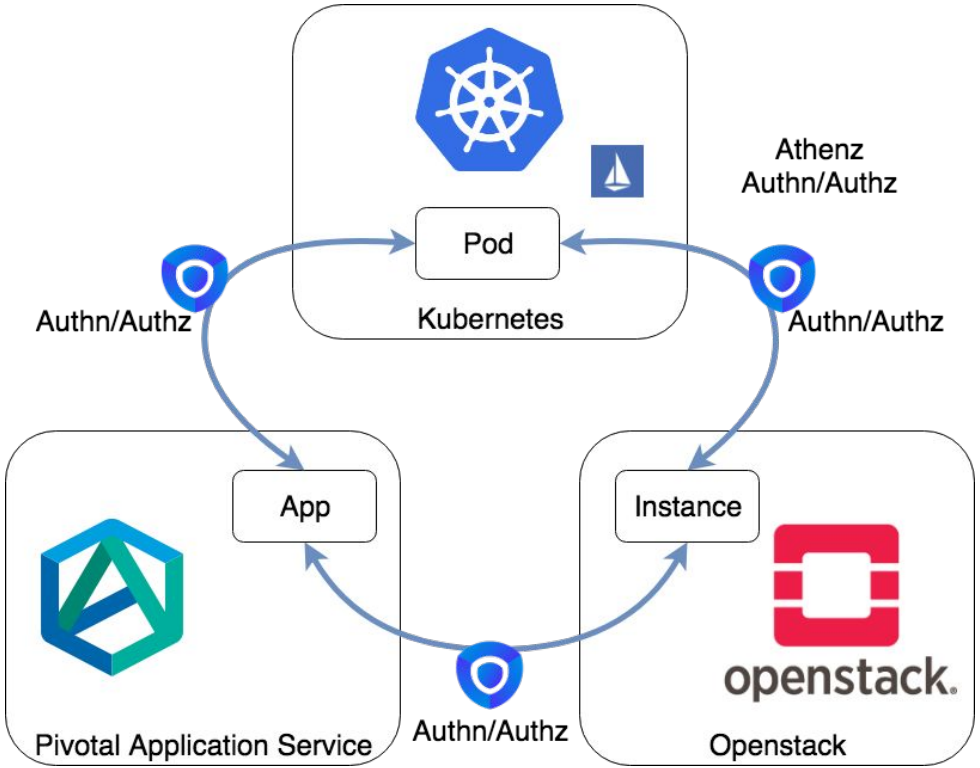
Authorization - Decentralized Access Control



Advantages of Athenz

- To provide service identity X.509 certificates for services running in common providers like Kubernetes, OpenStack or AWS that can be used for mutual TLS authentication.
- To have precise and frequently configurable access controls with single source of truth.

Athenz in Yahoo Japan




KubeCon
CloudNativeCon
North America 2018
How do we integrate with Istio?

Why use Istio?

- Automatic load balancing.
- Fine-grained control of traffic behavior.
- A pluggable policy layer and configuration API.
- Automatic metrics, logs, and traces for all traffic.
- Secure service-to-service communication.

Referred from: https://istio.io/docs/concepts/what-is-istio/

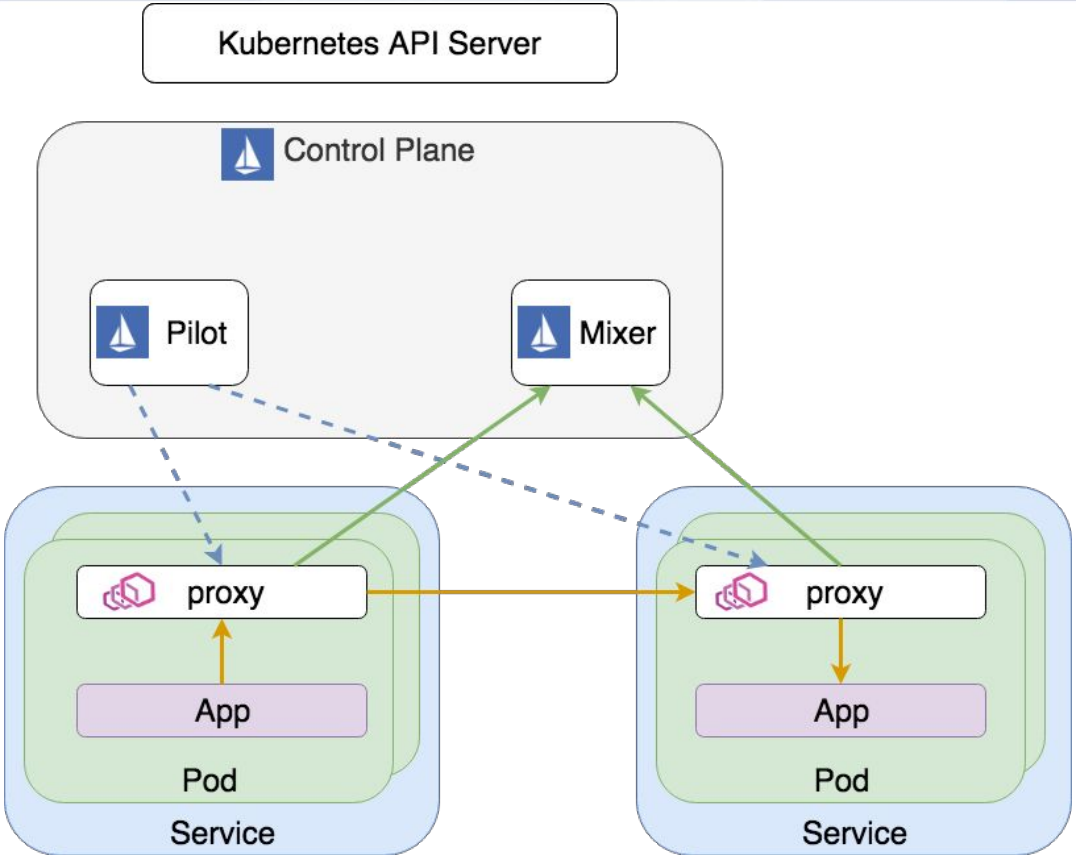
Benefits of using Athenz with Istio

- Istio is in CNCF landscape.
- Service mesh strongly supports microservices architecture.

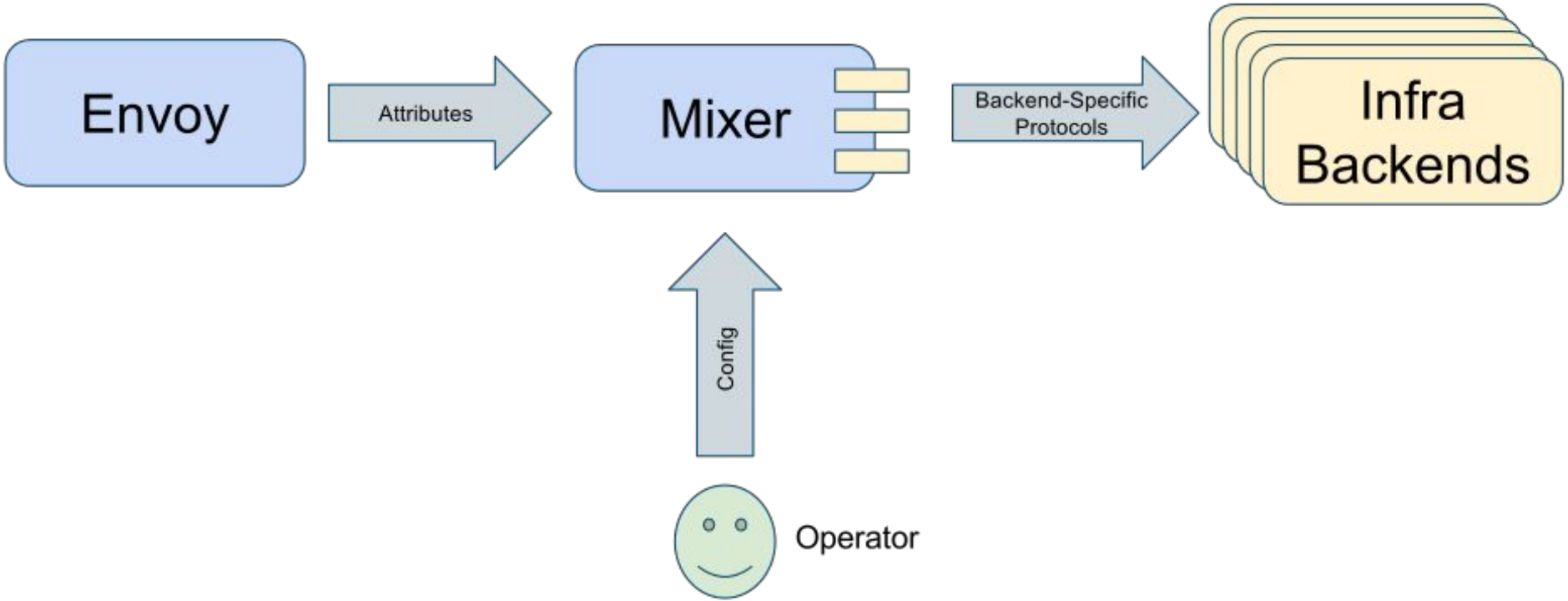
+

- Athenz enables single access control model in multi cloud.

Basics of Istio Mixer

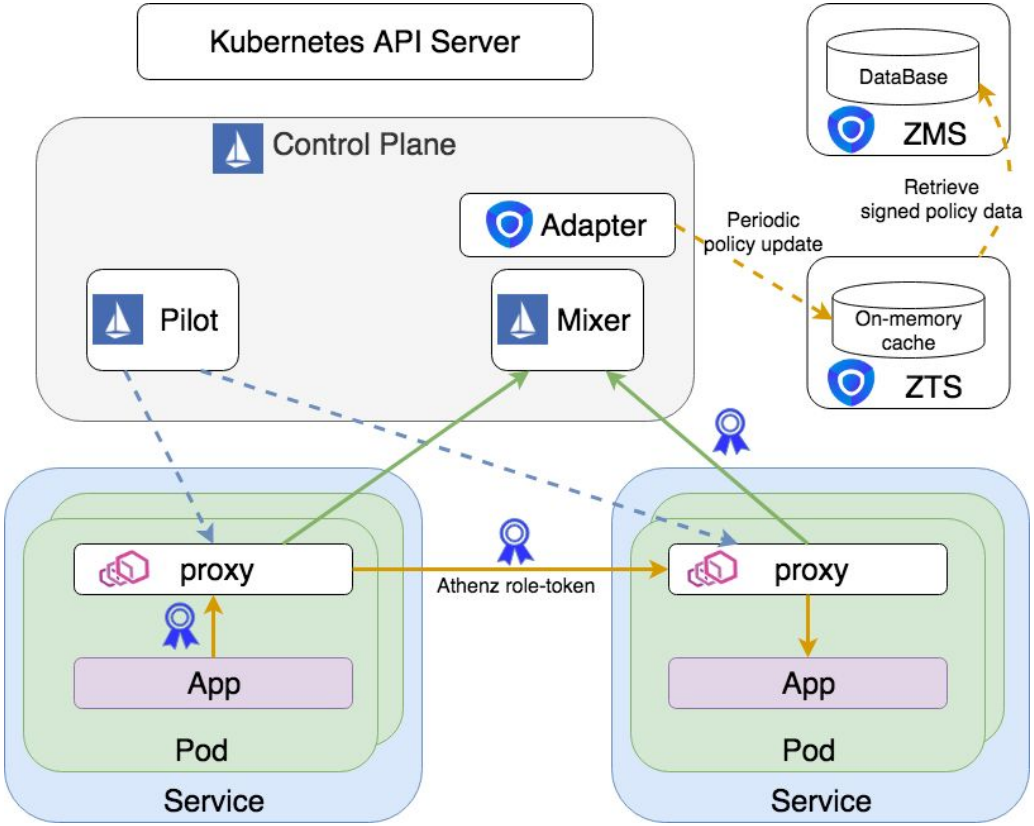


Example integration: Athenz Istio Mixer adapter

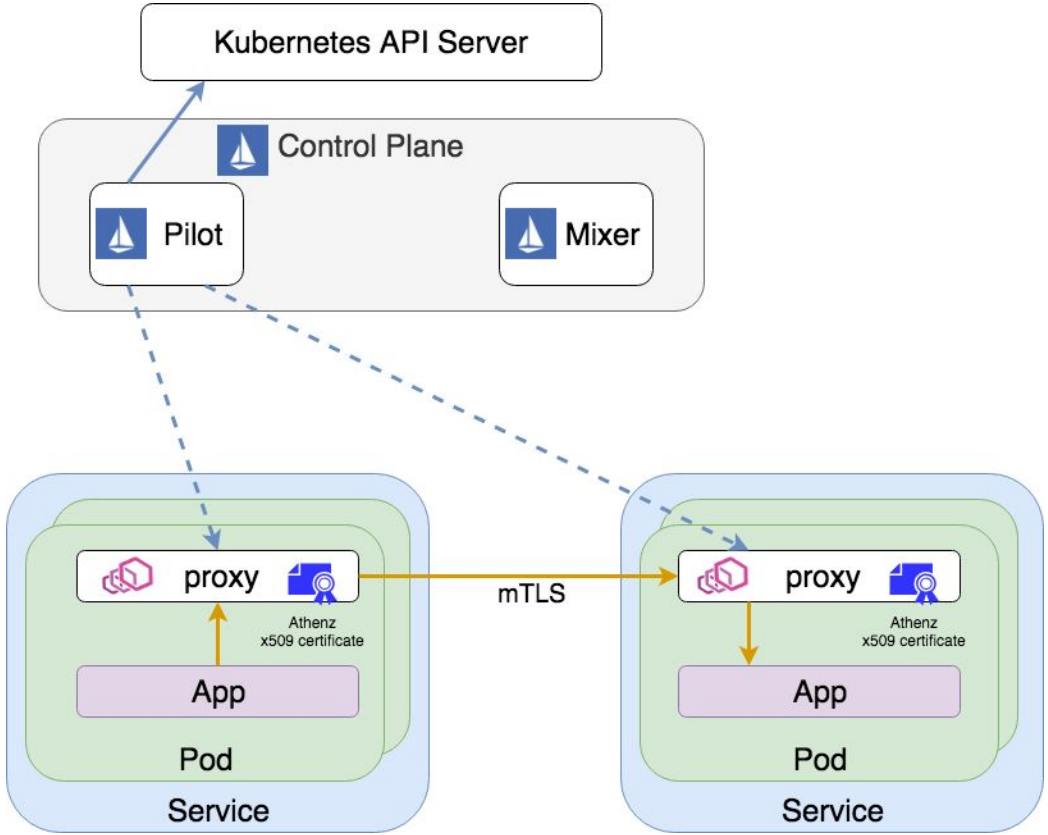


Referred from: https://istio.io/blog/2017/adapter-model/

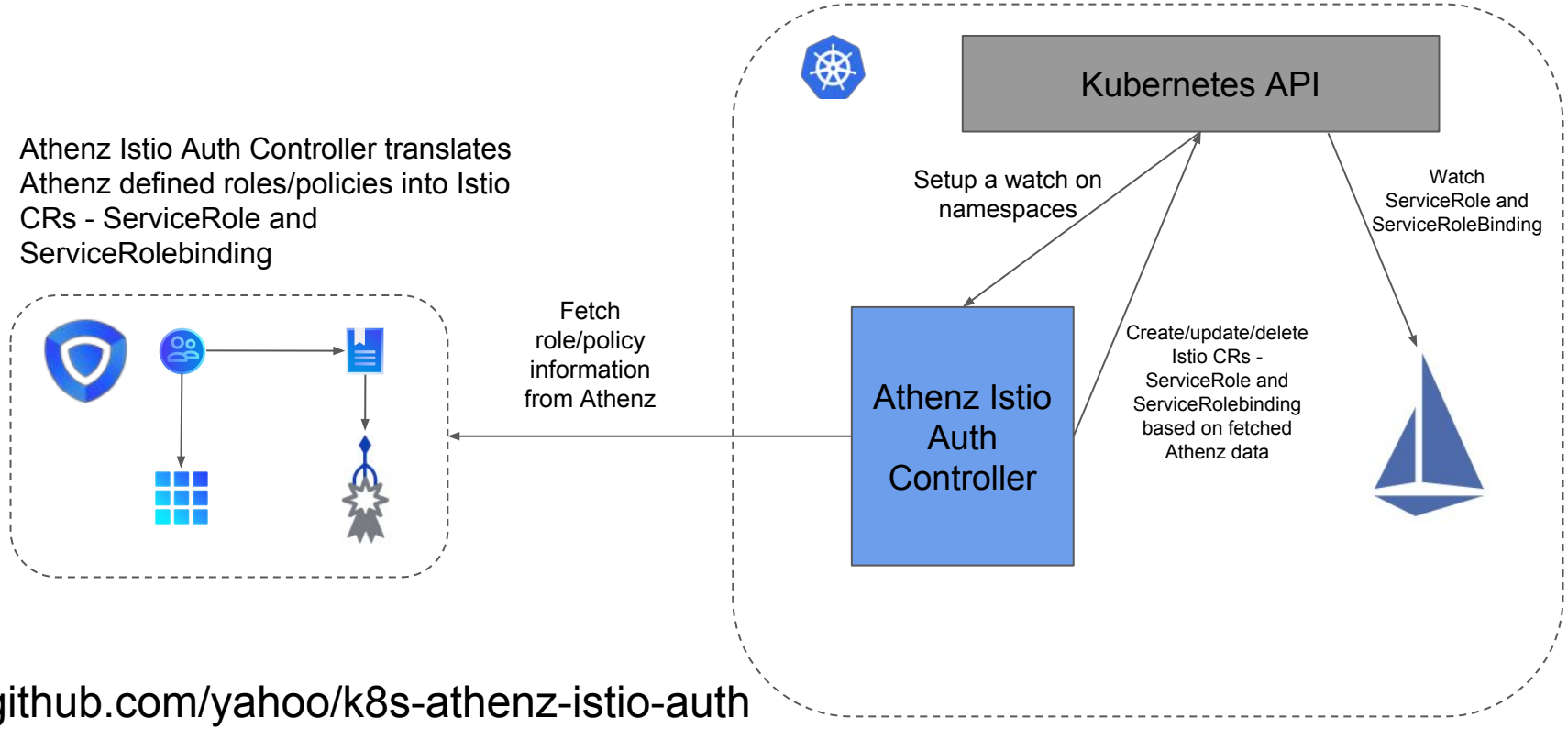
Example integration: Athenz Istio Mixer adapter



Other use-case:
Simplified mTLS authN/Z using Istio/Athenz



Simplified mTLS authN/Z using Istio/Athenz



https://github.com/yahoo/k8s-athenz-istio-auth


KubeCon
CloudNativeCon
North America 2018
Prototype Demo

Future plans

- Currently
  - On Premises and AWS Provisioning

- Planned
  - Provide Athenz servers with Docker images
    - Helm charts
  - Productionize Athenz x509 certificate provisioning
  - Productionize the authorization flow using Istio Envoy

Resources

- Website : http://www.athenz.io
- Github: https://github.com/yahoo/athenz
- Slack Channel: https://athenz.slack.com/
- Discussion Group:
  - Google Group: Athenz-Users
- Questions or Comments:
  - Tatsuya Yano: tatyano@yahoo-corp.jp

Join Us

http://www.athenz.io


KubeCon
CloudNativeCon
North America 2018
Thank you


KubeCon
CloudNativeCon
North America 2018
Q & A


KubeCon
CloudNativeCon
North America 2018