Athenz: The Open-Source Solution to Provide Access Control in Dynamic Infrastructures

Tatsuya Yano / Yahoo Japan Corporation
Athenz: Open Source System
Created by Yahoo Inc.

• Service Authentication
  – Provide secure identity in the form 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 / Okta / etc

- Service Authentication
  - Instances within a service with a unique identity to enable secure communication
    - IP / Networks ACLs / iptable
    - Mutual TLS with x.509 certificates
Why does this matter?

• Many persistent large scale infrastructure problems are rooted in identity and policy
  – Network ACL complexity
  – Federated “Single” Sign On (SSO) systems
  – Headless/Automation users
  – Shared secrets
Certificate Based Authentication

- Every instance / service in your cloud has its own identity
- Stronger security by Mutual TLS Authentication
- 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

1. Launch instance
2. Boot (Instance with Identity Document)
3. Service Identity Agent (Create Private Key Create CSR)
4. Register Instance
5. Verify Provider is Authorized to Launch this instance
6. Request Provider to Validate Instance Document and Metadata
7. Generate X.509 Certificate Based on instance CSR
8. Athenz X.509 Certificate

Authorized Principal (AWS, Openstack, etc)
Authorization
Athenz Data Model
- Most infrastructures in Cloud computing environments (e.g. Kubernetes, OpenStack, AWS, etc) have their own system of access control.
- Athenz provides interface to integrate with each infrastructure to run multi environments with a single access control model.
Authorization - Centralized Access Control

User
John Doe

Set “Max Heap Memory” setting to 8GB

Configuration Service Manager

Does John Doe have access to set “Max Heap Memory” setting value?

Domain Admin

Grant John Doe access to set “Max Heap Memory” setting

Management Service

ATHENZ
Authorization - Decentralized Access Control

1. Get Authorization Token
2. Submit Authorization Token

Retrieve Project “x” Secret

Secret Management System
On Box Enforcement

Grant John Doe access to Project “x” Secret

Policy Data Async Update

Management Service
Token Service
Demo
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.
Future plans

• To support SPIFFE ID in SAN field of x509 certificate
• To integrate with Istio envoy for authorization
Resources

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

http://www.athenz.io
Q & A