YAHOO! JAPAN

Athenz & Spire によるアクセス制御

ヤフー株式会社

矢野 達也

2021/04/20

自己紹介

矢野 達也

Web ServiceやSmartphone Appの開発/運用に従事した後、現在はYahoo! JAPANにおけるアプリケーション間アクセス制御のDevOpsを行うチームでProduct Ownerを担当しています。AthenzのContributorとしても活動しており、KubeCon等のカンファレンスでの発表も行なっています。

今やっていること

Athenz の Yahoo!JAPAN 社内での導入、機能拡充など

好きなもの

自動化、システム連携など

Yahoo! JAPANにおけるクラウド環境

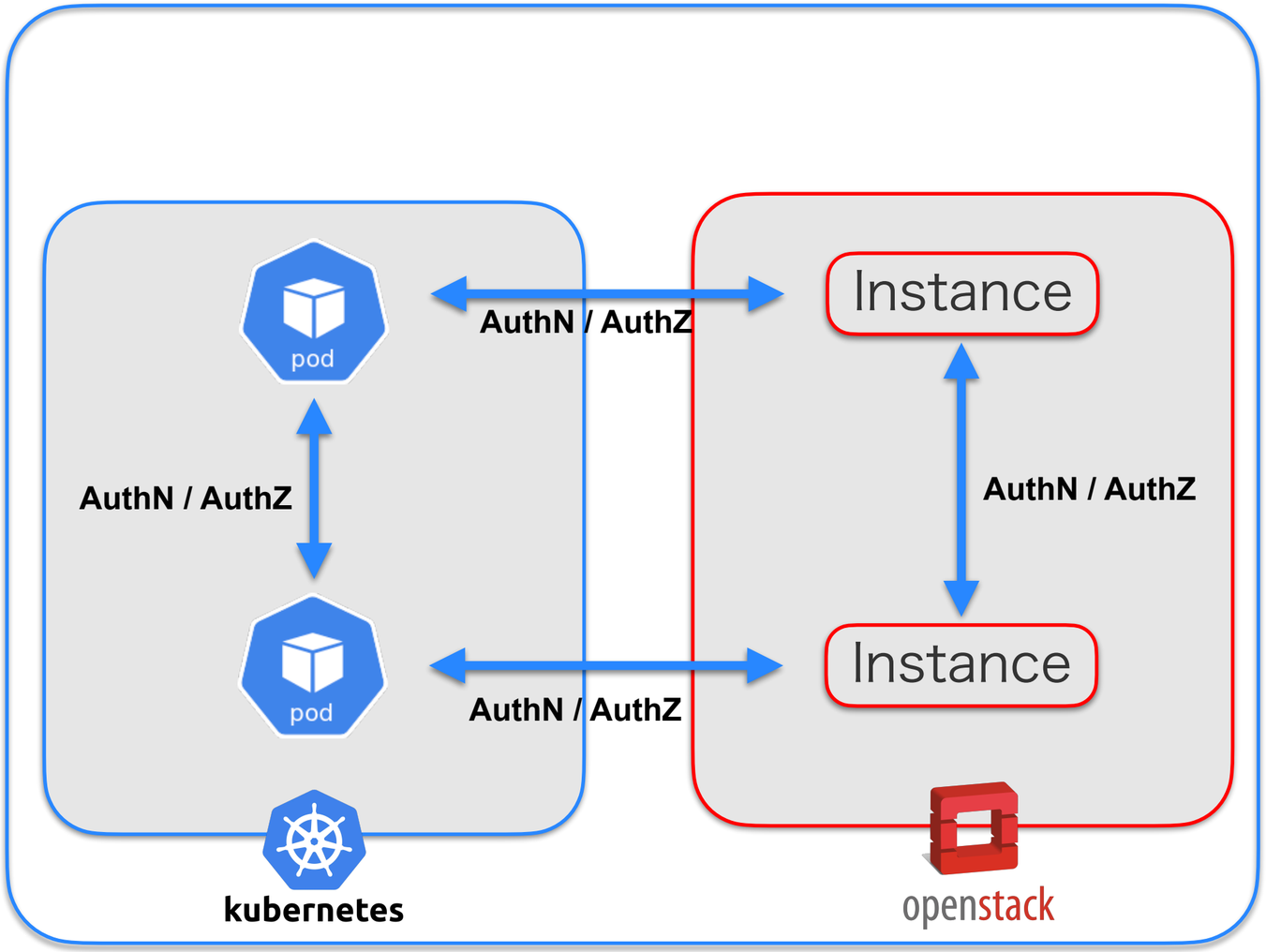
Yahoo! JAPAN
Cloud computing environments

OpenStack

Kubernetes

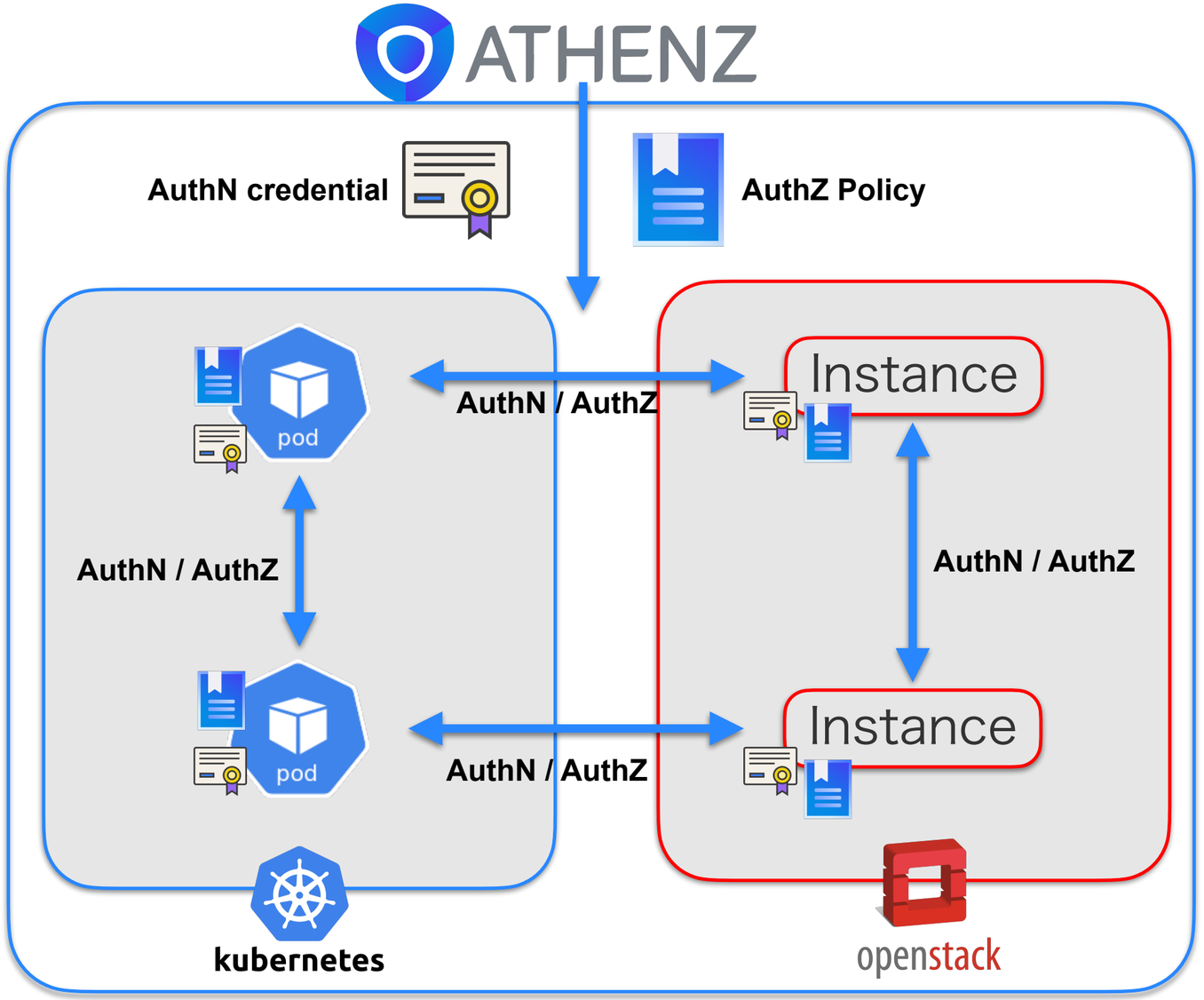
Pivotal Application Service

Screwdriver



クラウド環境におけるアクセス制御の課題

- 認証情報の確実さや設定の作業コスト
  - IPアドレスでは同一Nodeのアプリケーションを識別できない
  - 認証情報を手動で設定するコスト
- アクセス制御設定の複雑さ
  - スケールアウトに応じた反映コスト

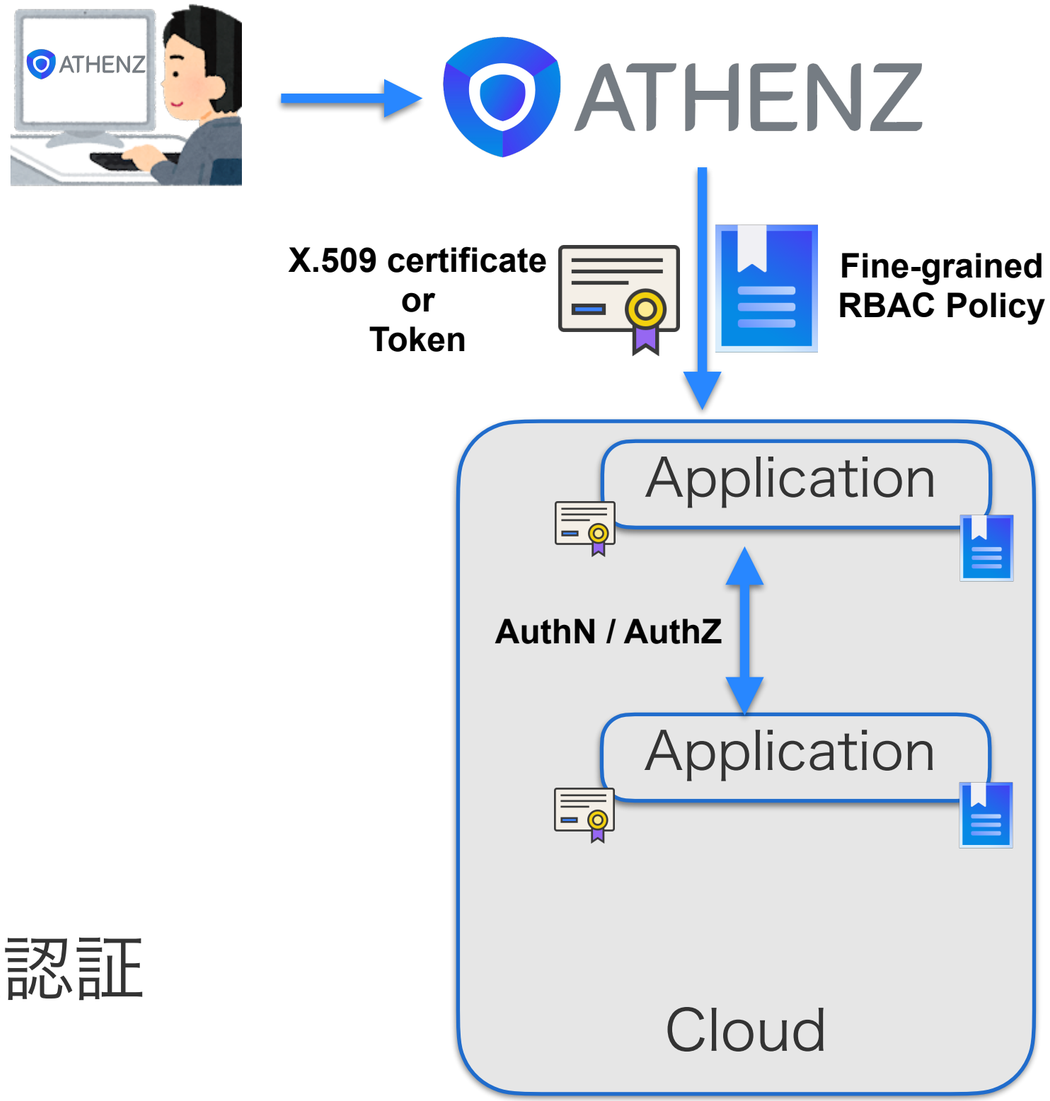


ATHENZ とは

- クラウド環境でのアプリケーション間アクセス制御（SSoT）
- ロールベースのアクセス制御（RBAC）
- Yahoo Inc.（現 Verizon Media）が開発しオープンソース化
- Yahoo! JAPANにてコントリビュート
- CNCF Sandbox project

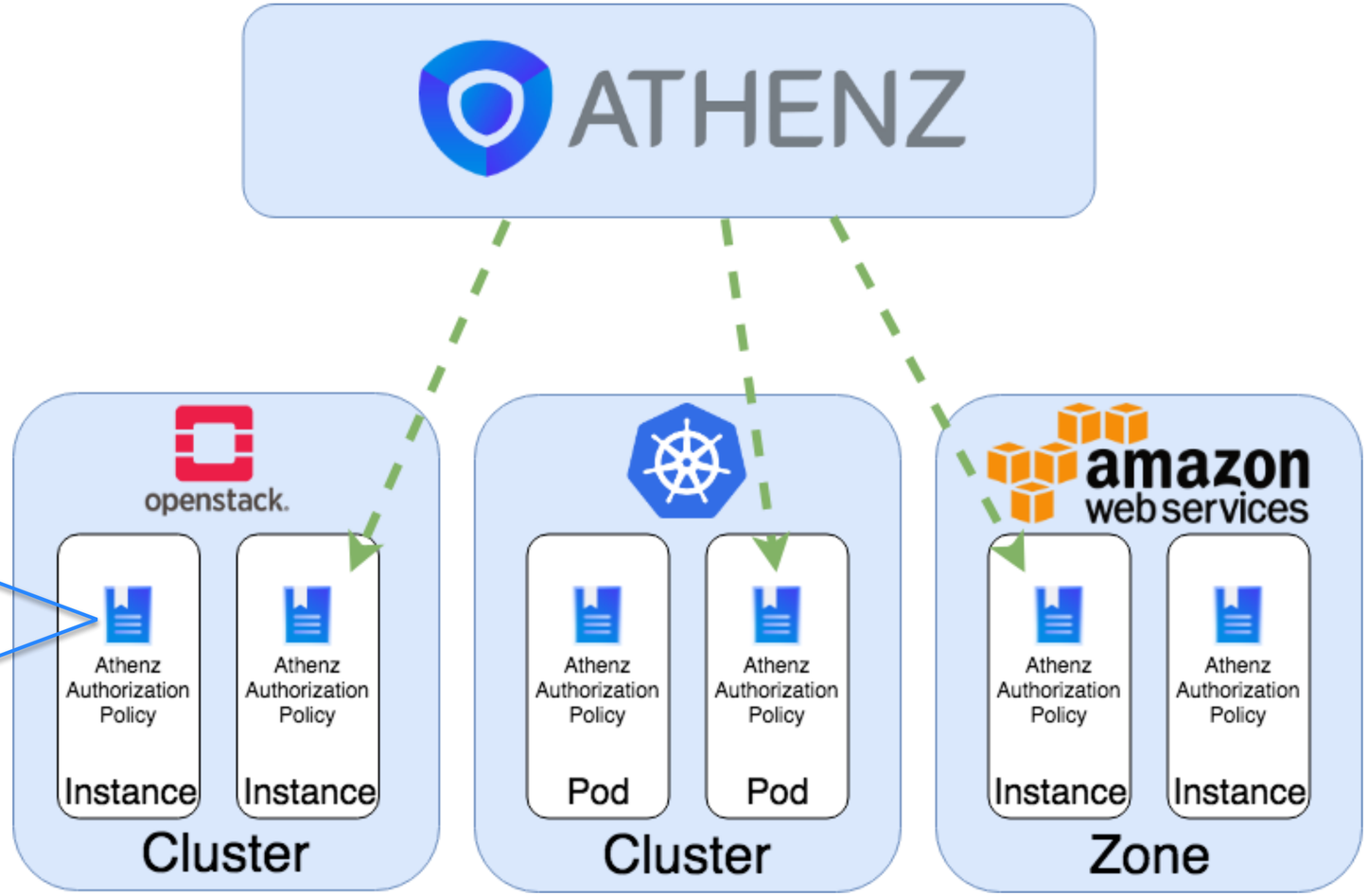
ATHENZ の機能

- 認可 - Authorization (AuthZ)
  - Role ベースのアクセス制御 (RBAC)
  - Policy による細かなアクセス制御
- 認証 - Service Authentication (AuthN)
  - 接続元IPアドレスに依存しない公開鍵認証
  - 各 Application に Token 又は X.509証明書 を自動配布



Athenz による Policy を用いた RBAC

```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: []
```



なぜ SPIRE を導入するのか

- AthenzによるTokenやX.509証明書の自動配布 (Copper Argos)
- Copper Argos では OpenStack 向けのオープンソース実装がない
  - Spire で各 Workload に X.509証明書 を自動配布する仕組みを実現

Copper Argos open-source specification

OpenStack

Kubernetes

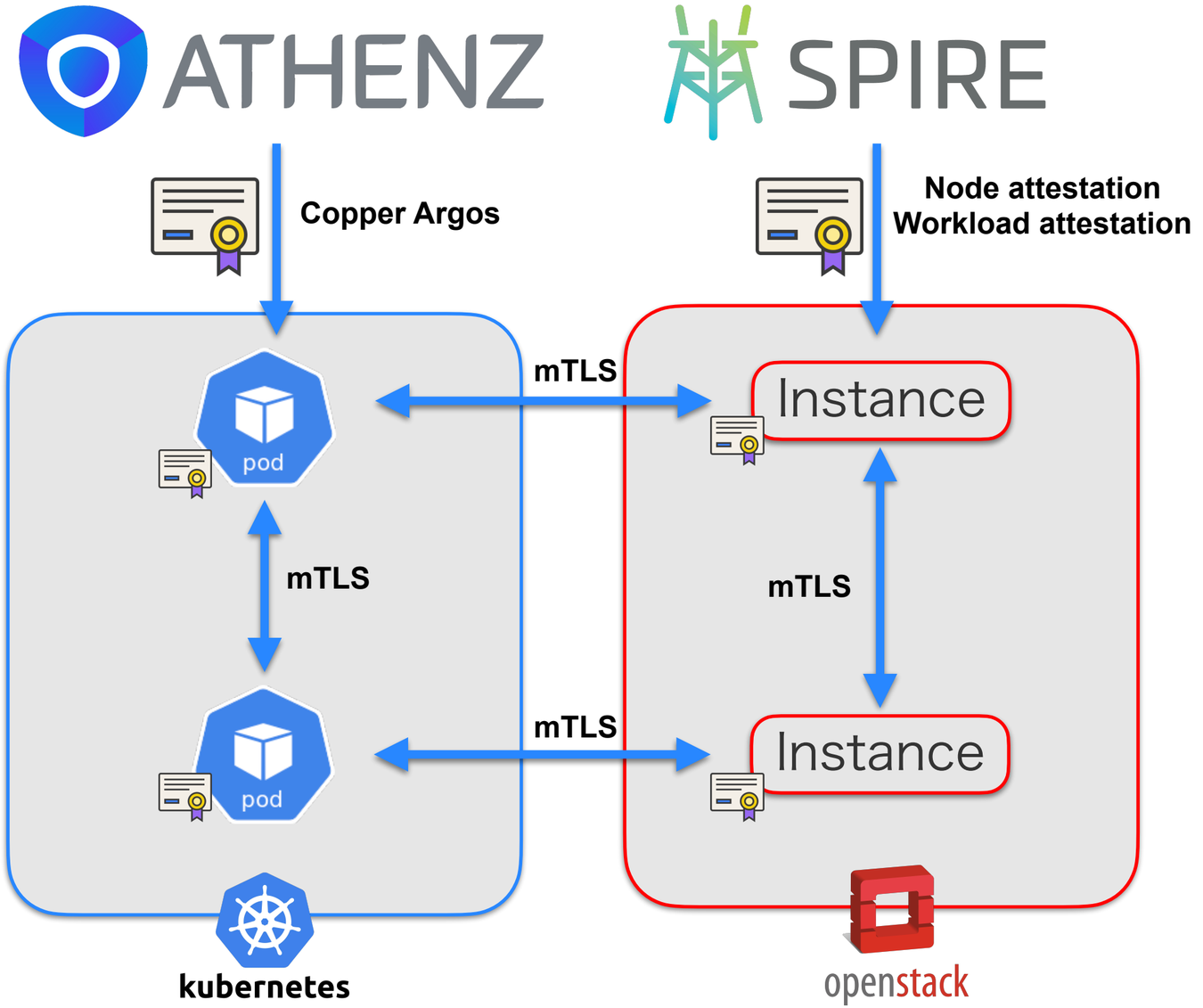
Screwdriver

Amazon EC2

AWS ECS

AWS Lambda

X.509証明書の自動配布 (Identity Provisioning)



Athenz と Spire で共有される SPIFFE ID

- Athenz Copper Argos で発行される X.509証明書

  spiffe://<athenz-domain>/sa/<athenz-service>

  spiffe://<athenz-domain>/ra/<athenz-service>

- Spire で発行される X.509証明書 (SVID)

  spiffe://<spire-trust-domain>/ns/<athenz-domain>/sa/<athenz-service>

  spiffe://<spire-trust-domain>/ns/<athenz-domain>/ra/<athenz-service>

Athenz

- Website: http://www.athenz.io
- CNCF Sandbox: https://www.cncf.io/sandbox-projects/
- Github: https://github.com/yahoo/athenz
- Slack Channel: https://athenz.slack.com/
- Athenz Case Studies:
  - Kubernetes: https://www.athenz.io/casestudies.html#kubernetes
- Google Group: Athenz-Users
- Questions or Comments: https://github.com/tatyano


YAHOO!
JAPAN