Run time Security using ISTIO - as a POC

Executive Summary - Improve security posture of ONAP without complicating each application container logic.

Business Impact - Lesser operational issues, centralized monitoring of ONAP

Business Markets - *Applicable across compute continuum : On-prem edges, network edges, edge clouds and public clouds.*

Funding/Financial Impacts - *Reduces OPEX as the security, traffic management & observability is centralized.*

Organization Mgmt, Sales Strategies - *There is no additional organizational management or sales strategies for this use case outside of a service providers "normal" ONAP deployment and its attendant organizational resources from a service provider.*

Goal:

- Avoid node ports (use ingress gateways)
- Load balancer as it is done in public clouds (such as MetalLB)
- Secure communication to outside entities
- Secure communication among the micro services
- User authentication via tokens

Prove that ISTIO can achieve above goals with the help OAUTH2.

Start with Multi-Cloud project and show that there is no change in applications to achieve run time security.

Once proven come back to ONAP wider community on the need for separating the security from the applications.

Current challenges with ONAP

We feel that user management, creating roles, RBAC of resources with roles is basic for any project. ONAP is not very well secured on this aspect.

Proposal:

Since the intention is to start slow, current proposal is providing ISTIO security to ONAP4K8S profile (Multi Cluster Orchestration (ONAP4K8s))

Proposal items:

- ISTIO-ingress and MetalLB for ingress connections (connections to Multi-Cloud project from other projects) – Secure at least with one project (SO) and non-secure with others.
- User Management with OAUTH2 server with local userDB of OAUTH2 server.
- RBAC as per ISTIO RBAC
- ISTIO (with envoy)for inter-service communication of containers within the Multi-Cloud project.
- ISTIO CA (Citadel) for certificate enrollment of internal services.
- Manual certificates for external communication
- Certificate credential storage using TPM
- Use ORY (OAUTH2) server
- Improve performance of Envoy with hardware crypto accelerators