LF NETWORKING
Developer & Testing Forum

ONAP: Service Mesh in London

Status of ServiceMesh
in ONAP

https://lfnetworking.org

Andreas Geissler February 14, 2023

Anti-Trust Policy Notice

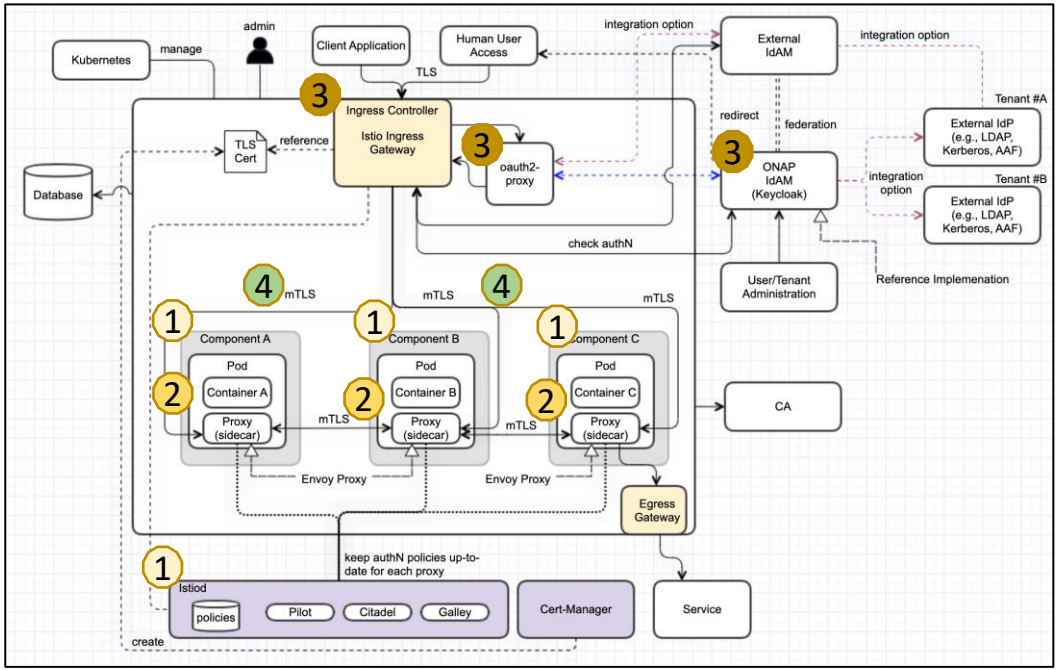
LFN NETWORKING
LFN Developer & Testing Forum

- Linux Foundation meetings involve participation by industry competitors, and it is the intention of the Linux Foundation to conduct all of its activities in accordance with applicable antitrust and competition laws. It is therefore extremely important that attendees adhere to meeting agendas, and be aware of, and not participate in, any activities that are prohibited under applicable US state, federal or foreign antitrust and competition laws.

- Examples of types of actions that are prohibited at Linux Foundation meetings and in connection with Linux Foundation activities are described in the Linux Foundation Antitrust Policy available at http://www.linuxfoundation.org/antitrustpolicy. If you have questions about these matters, please contact your company counsel, or if you are a member of the Linux Foundation, feel free to contact Andrew Updegrove of the firm of Gesmer Updegrove LLP, which provides legal counsel to the Linux Foundation.

ServiceMesh Target Vision

- It is based on Jakarta plans (https://wiki.lfnetworking.org/display/LN/2022-01-13+-+ONAP%3A+ONAP+on+Service+Mesh+status+update)
- Service Mesh intent is to use Istio for encrypting inter pod traffic and to use JWT in conjunction with Istio for authN and authZ. Details see ArcCom/SecCom page: ONAP Next Generation Security & Logging Architecture



- **Step 1 (Certificates)**
  - Deployment of ONAP in "Istio" enabled system
  - Enable HTTP communication + AAF disabling
- **Step 2 (Authorization)**
  - Service Account per subcomponent
  - "AuthorizationPolicy" for inter-component communication
- **Step 3 (simple RBAC)**
  - Deploy and configure Ingress, Keycloak, OAuth2-Proxy
  - JWT configuration on "AuthorizationPolicy" for external user access
  - User access authorization is only performed on the first component (NBI, UUI, Portal, APIs…)
- **Step 4 (full RBAC)**
  - User access authorization is performed by each component via JWT token
  - Components pass the header to the connected components

Status in London

LFN Developer & Testing Forum

Step 1 (Certificates)
- Deployment of ONAP in “Istio” enabled system
- Enable HTTP communication + AAF disabling

→ (London) → OOM-2820 Components on Service Mesh
Open component fixes:
UUI, CLI, VNFSDK, HOLMES, A1PolicyManagement, CDS-UI, OOF, DCAE-OpenAPI-Manager

Step 2 (Authorization)
- Service Account per subcomponent
- “AuthorizationPolicy” for inter-component authorization

→ (London) → OOM-2822 Service 2 Service Authorization with Service Mesh

Step 3 (Simple RBAC)
- Deploy and configure Ingress, Keycloak, OAuth2-Proxy
- JWT configuration on “AuthorizationPolicy” for external user access
- User access authorization is only performed on the first component (NBI, UUI, Portal, APIs…)

→ (London) → OOM-2431 ONAP on Istio with authentication
(Ingress, Keycloak, OAuth2 deployment and configuration)

→ (London) → OOM-2823 Customer 2 Service Authorization on Service Mesh
(done for portal-ng, planned for other services…)

Step 4 (Full RBAC)
- User access authorization (e.g., fine-grained one) is only performed by each component via JWT token
- Components pass the header to the connected components

→ (London) Not Planned

- OOM SM Tests
  - OOM-3004 Test ONAP on SM
- OOM CRs
  - https://gerrit.onap.org/r/q/topic:%2522service_mesh%2522

Requirement for London

REQ-1349 Removal of AAF

- Component offers only unencrypted http interface
- “AAF enabled” option will be removed from charts
- Code handling of AAF certificate/SMS can be removed

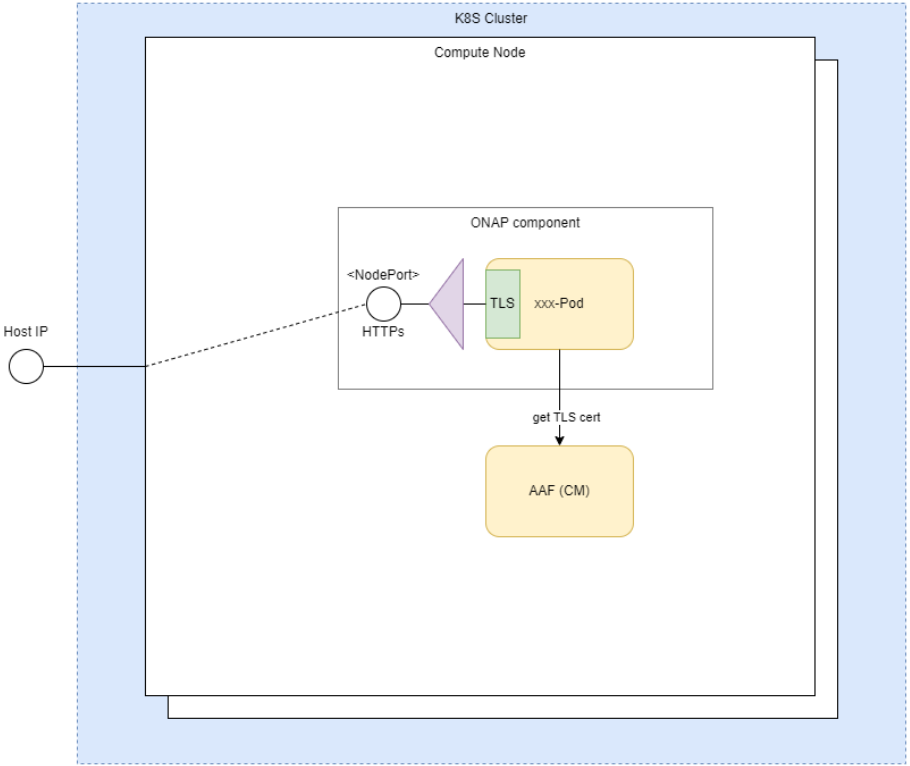
REQ-1351 External secure communication only via Ingress

- No Nodeports, when Ingress option is used

REQ-1350 All component must be able to run without MSB

- In the default ONAP deployment case using ServiceMesh, an Ingress Gateway is used for external access to the services.
- Therefor the MSB component would not be needed and must be disabled.
- If the internal API gateway is required, it can be implemented in the Ingress gateway

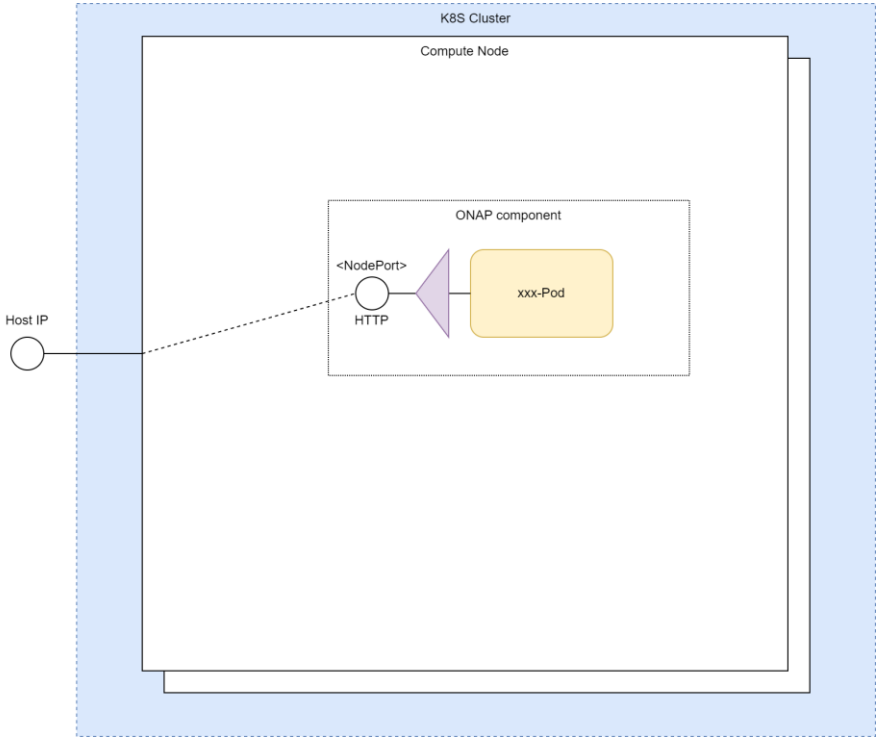
ONAP Deployment up to Kohn



- ONAP pods providing TLS (HTTPs) interfaces
- Retrieve certificates during startup from AAF Certificate Manager
- ONAP pod interface is exposed via service using "NodePort" (if cluster external access is required)
- Hosts expose the "NodePort" via its Host Ips (or hostname)

- Example (SDC-UI):
https://<HostIP>:30207/sdc1/portal

“Development” deployment in London

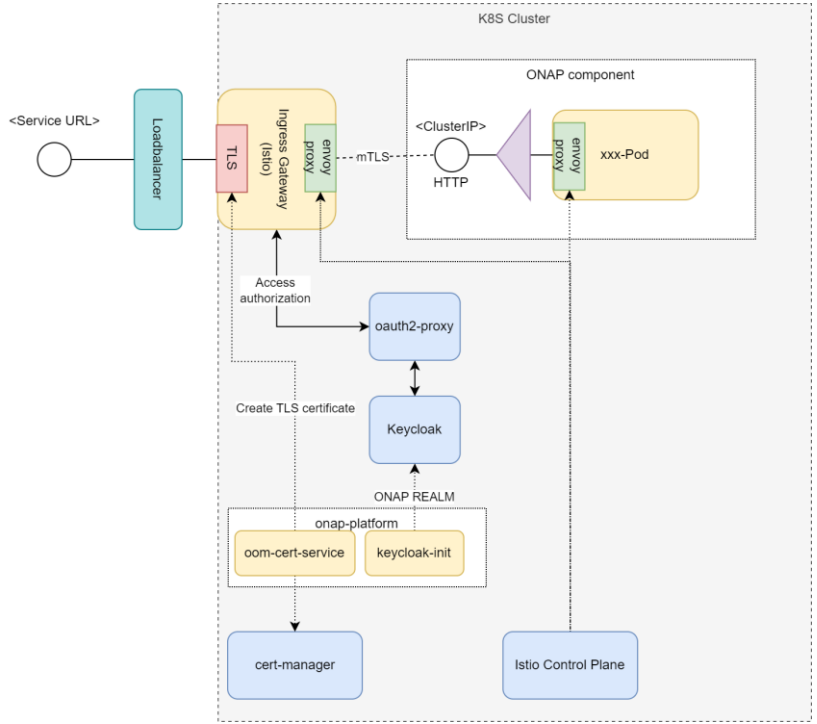


For testing purpose only („development“)

- AAF is not deployed anymore !
- ONAP pods non-TLS (HTTP) interfaces
- ONAP pod interface is exposed via service using "NodePort" (if cluster external access is required)
- Hosts expose the "NodePort" via its Host Ips (or hostname)

- Example (SDC-UI):
http://<HostIP>:30207/sdc1/portal

“Production” deployment in London



Secure setup („production“)

- ONAP pods provide non-TLS (HTTP) interfaces
- Encrypted communication via Envoy Proxies (nTLS) provided by ServiceMesh (Istio)
- ONAP pod interface is exposed through Ingress (Istio-Gateway)
- Service access via hostname (configured by Gateway/VirtualService in Ingress GW)
- External TLS interface on Ingress Gateway
- Authentication/Authorisation via oauth2-proxy and Keycloak

- Example (SDC-UI):
https://sdc-fe-ui.simpledemo.onap.org

Integration/E2E tests of SM

LFN NETWORKING
LFN Developer & Testing Forum

“Production” deployment tests:
- https://logs.onap.org/onap-integration/daily/onap-daily-dt-oom-sm-master/

“Development” deployment tests:
- https://logs.onap.org/onap-integration/daily/onap-daily-dt-oom-master/

Gating Tests:
- https://logs.onap.org/onap-integration/gating/
- Currently using “Development” setup
- Will be soon updated to “Production”

Open testcase fixes:
- 5GBulkPM https://jira.onap.org/browse/OOM-3100

Open component fixes:
- UUI https://jira.onap.org/browse/OOM-2998 -> Fix ongoing
- A1Policy Management https://jira.onap.org/browse/OOM-3008 https://jira.onap.org/browse/CCSDK-3772
- VNFSDK https://jira.onap.org/browse/OOM-3095
- CLI https://jira.onap.org/browse/OOM-3096
- CDS-UI https://jira.onap.org/browse/CCSDK-3814
- HOLMES https://jira.onap.org/browse/OOM-3101
- SO https://jira.onap.org/browse/SO-4027
- DCAE (VES-OpenAPI-Manager) https://jira.onap.org/browse/DCAEGEN2-3335