LF NETWORKING

LFN Developer & Testing Forum

LF NETWORKING

LFN Developer & Testing Forum

Status of ServiceMesh in ONAP

Final status in Kohn and Plans for London

November 18, 2022

Andreas Geissler

Anti-Trust Policy Notice

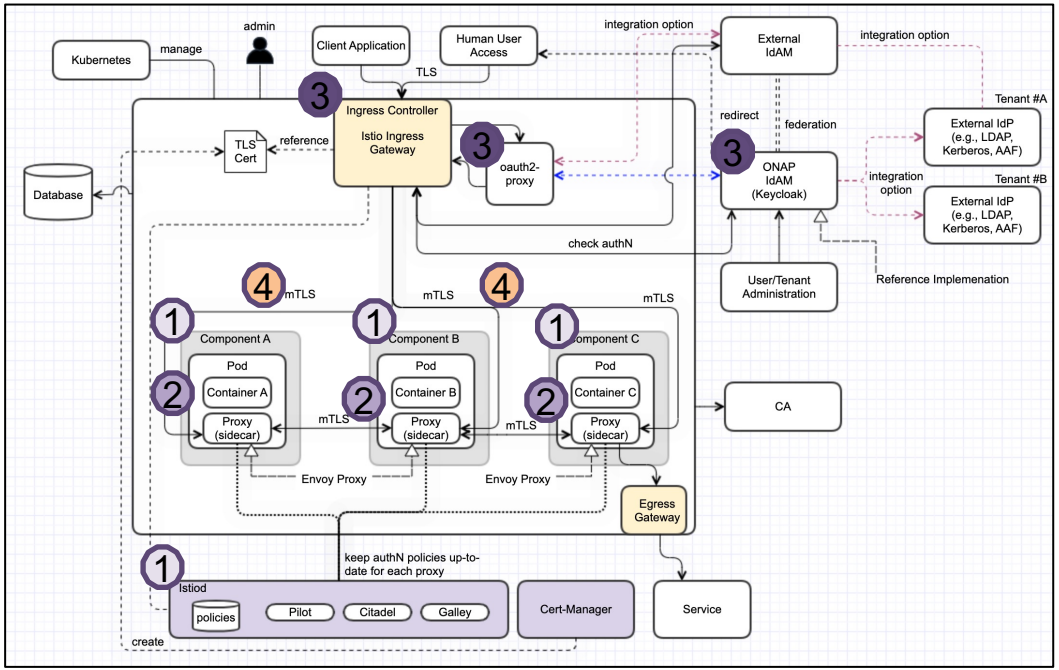
- Linux Foundation meetings involve participation by industry competitors, and it is the intention of the Linux Foundation to conduct all of its activities in accordance with applicable antitrust and competition laws. It is therefore extremely important that attendees adhere to meeting agendas, and be 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 in ONAP

LFN Developer & Testing Forum

- 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 Kohn and plans for London

LFN NETWORKING
LFN Developer & Testing Forum

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

→ (Kohn) In Progress → OOM-2820 Components on Service Mesh (see next slides)
(London) Finalize

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

→ (Kohn) Not started → OOM-2822 Service 2 Service Authorization with Service Mesh
(London) Finalize

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

→ (Kohn) In Progress → OOM-2431 ONAP on Istio with authentication (Ingress, Keycloak, OAuth2)
(London) Finalize

→ (Kohn) Not started → OOM-2823 Customer 2 Service Authorization on Service Mesh
(London) Finalize

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

→ (Kohn) Not started
(London) Not Planned

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

Step 1: Status of components (I)

LFN Developer & Testing Forum

Component	(1a) AAF/MSB independency	(1b) HTTP communication	(2) Ingress	Remarks	CR/Tickets
A1PolicyManagement	NOK	NOK	TBC	Not clear, if Ingress IF is required. Problems in with HTTP	CCSDK-3772
AAI	OK	OK	OK		
CASSANDRA	OK	OK	OK	Still new Cassandra version needed to solve SECCOM requirement	
CDS	OK	OK	OK		
CLI	NOK	NOK	TBD	CLI image has enabled only https communication and does not support HTTP, needs image change	
CONSUL	OK	TBD	OK	Still agent config needs to be updated	
CONTRIB	OK	OK	OK		
CPS	OK	OK	OK		
DCAEGEN2-Services	OK	OK	OK	Some MS have issue with DMAAP (will be fixed)	DCAEGEN2-3277
DCAEMOD	OK	OK	OK		
DMAAP	NOK	OK	OK	Working on the AAF independency	
HOLMES	TBD	TBD	TBD		
MARIADB-GALERA	OK	OK	OK		
MODELLING	OK	OK	OK	Has a strong dependency to MSB	
(MSB)	OK	OK	OK		
MULTICLOUD	OK	NOK	OK	Has a strong dependency to MSB	MULTICLOUD-1495
NBI	OK	OK	OK		
OOF	NOK	OK	OK	OSDF service has an AAF dependency and cannot be started in HTTP mode (patch started, but issues in CSIT)	OPTFRA-1099
PLATFORM	OK	OK	OK		

Step 1: Status of components (II)

LFN NETWORKING
LFN Developer & Testing Forum

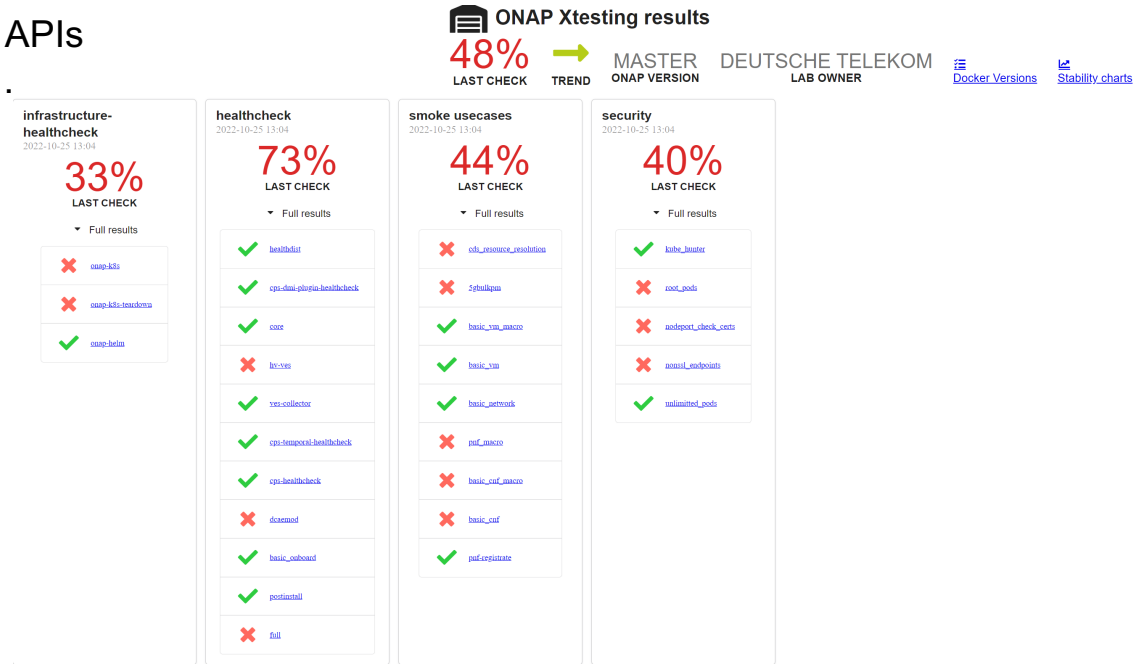
Component	(a) AAF/MSB independency	(b/c) HTTP communication	(d) Ingress	Remarks	CR/Tickets
POLICY	OK	OK	OK		
ROBOT	OK	OK	OK		
SDC	OK	OK	OK	Still new Cassandra version needed to solve SECCOM requirement	
SDNC	OK	OK	OK		
SO	OK	OK	OK	Dependency on MSB (e.g. Openstack Adapter)	
STRIMZI	OK	OK	TBD	External Access to Kafka required (plan for London ?)	
UUI	TBD	TBD	TBD	Strong dependency on MSB	
VFC	OK	OK	OK	Strong dependency on MSB	
VNFSDK	TBD	TBD	TBD		
VID	NOK	NOK	NOK	Would need Code change, but component is deprecated -> not continue	
PORTAL-NG				New component (PoC in Kohn/London)	

Integration/E2E tests of SM

LFN Developer & Testing Forum

Daily Tests are set up:

- https://logs.onap.org/onap-integration/daily/onap-daily-dt-oom-sm-master/
- Robot health-checks are working
- Smoke tests are setup and use Ingress APIs
- Some test-setup needs to be changed…



Requirement Proposals for London

LFN NETWORKING
LFN Developer & Testing Forum

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

LF NETWORKING

LFN Developer & Testing Forum