LF NETWORKING
Developer & Testing Forum

ONAP Security Enhancements and Strategy for NF Security

ONAP Streamlining – The Process

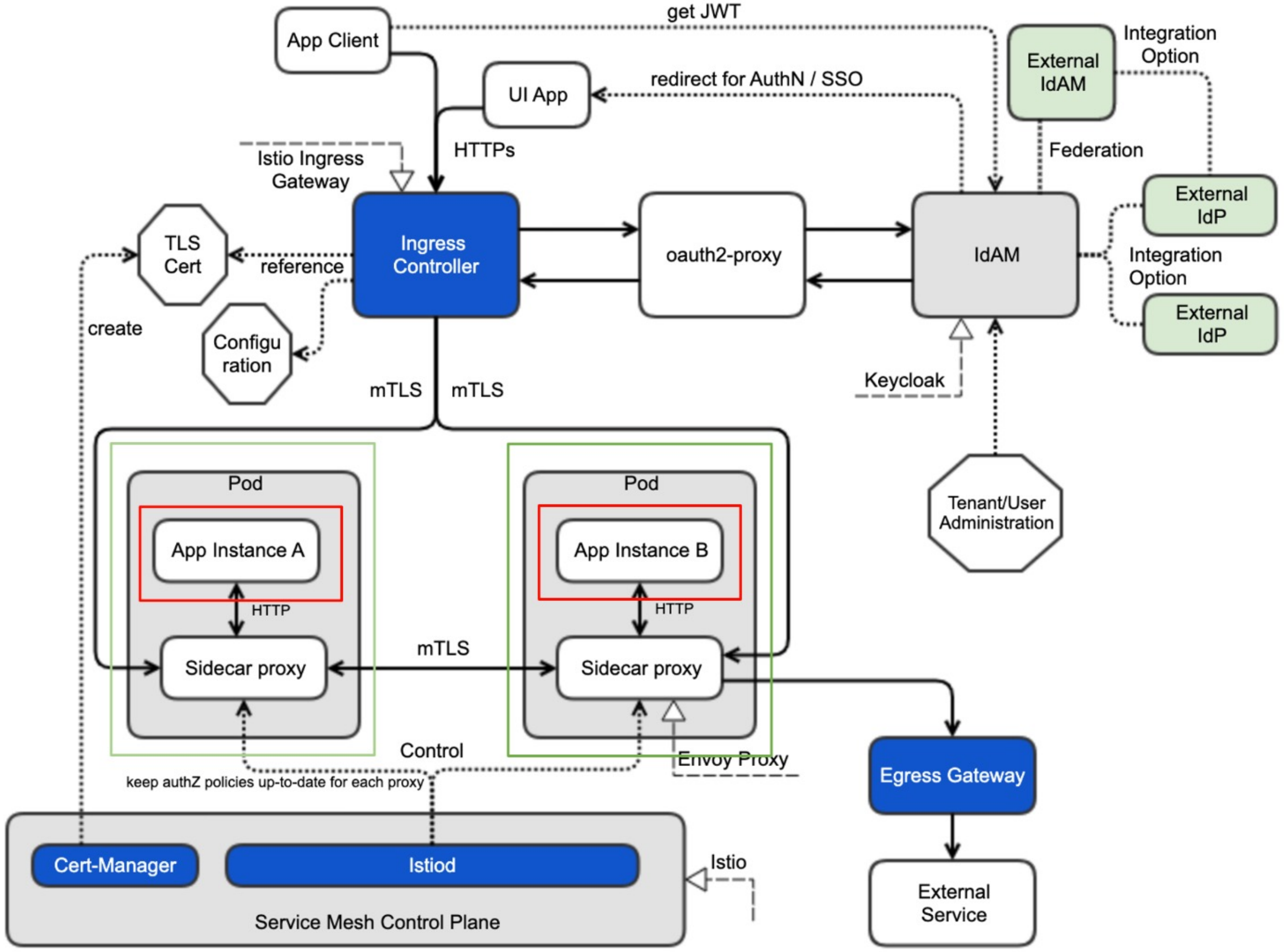
November 2023
Presenter:
Andreas Geissler (DT) – OOM PTL
Byung-Woo Jun (Ericsson) – ARCCOM Chair, TSC

https://lfnetworking.org

ONAP Runtime Security Architecture

LF NETWORKING
LFN Developer & Testing Forum

- ONAP components are protected by Ingress Controller, Keycloak (IdAM) and Istio (Service Mesh), with AuthN/Authz, intra-secure communications, external-secure communications.
- ONAP components themselves do not have their own/ proprietary protection any longer (e.g., removal of HTTP Basic Authentication and HTTPs).
- Current OOM-provided security support as described above will be provided as ONAP reference security mechanism.
- It is assumed that vendors/operators support industry de facto security mechanism like ONAP security and imported ONAP components are protected by the security mechanism.
- ONAP will provide documentation of security architecture, global requirements and best practices, informing how to protect/secure selected ONAP components.
  - For secure external communications, Ingress Controller, aouth2-proxy and IdAM are used
  - For intra-secure communications, Istio is be used with Cert-Manager and policies
  - For user authentication and authorization, KeyCloak is used, with SSO support and OAuth2-based token generation and validation
- ONAP (OOM) provides security reference implementation and configuration by leveraging service mesh (Istio), ingress (Istio GA) and IdAM (Keycloak). The reference implementation and configuration can be replaced by the vendor/operator-provided security mechanism.

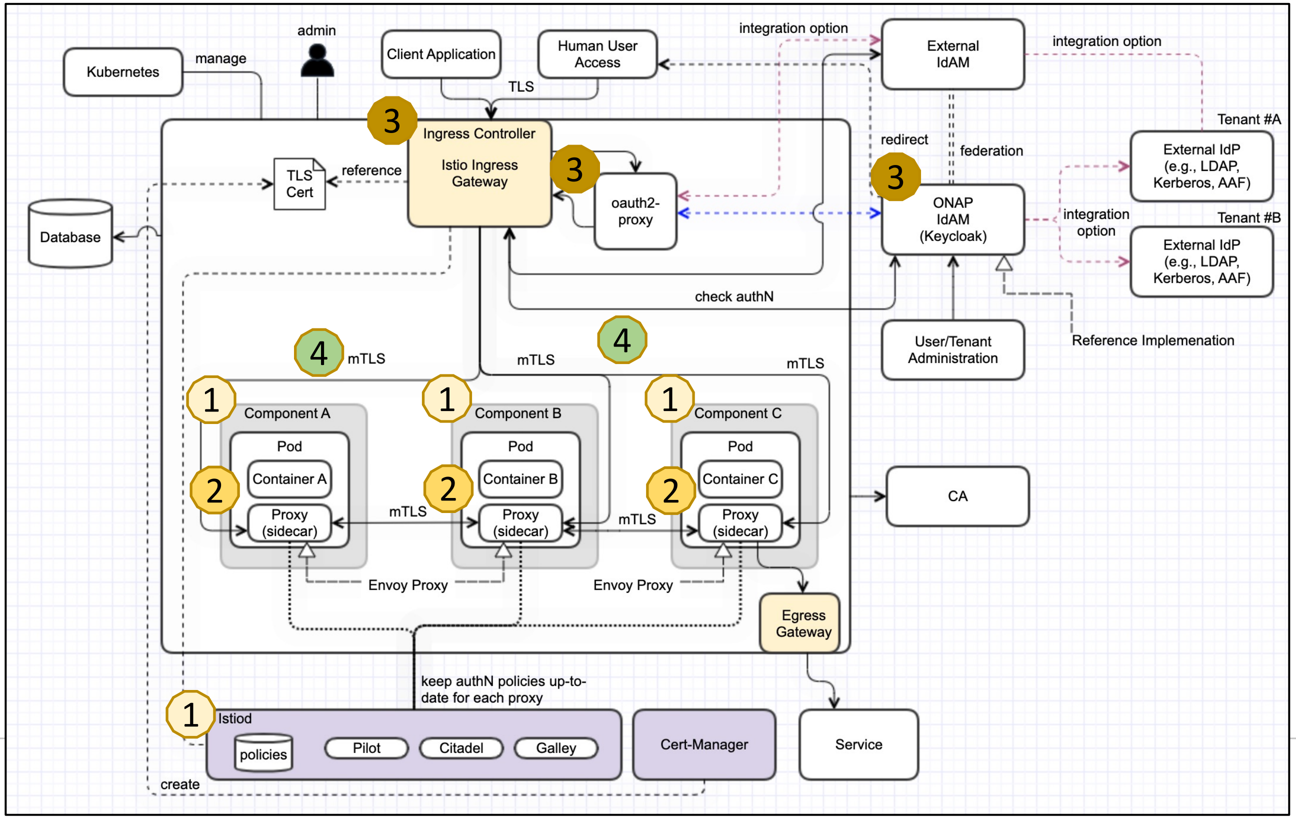


- ONAP provides security reference implementation. Vendors / operators can realize and configure with their own security system.
- Since vendor/operator component can be deployed with ONAP components, Secure Software Supply Chain is important.

ONAP Service Mesh Target Version

LF NETWORKING
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



1

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

2

- **Step 2 (Authorization)**
  - Service Account per subcomponent
  - "AuthorizationPolicy" for inter-component communication

3

- **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…)

Done

4

- **Step 4 (full RBAC)**
  - User access authorization is performed by each component via JWT token
  - Components pass the header to the connected components

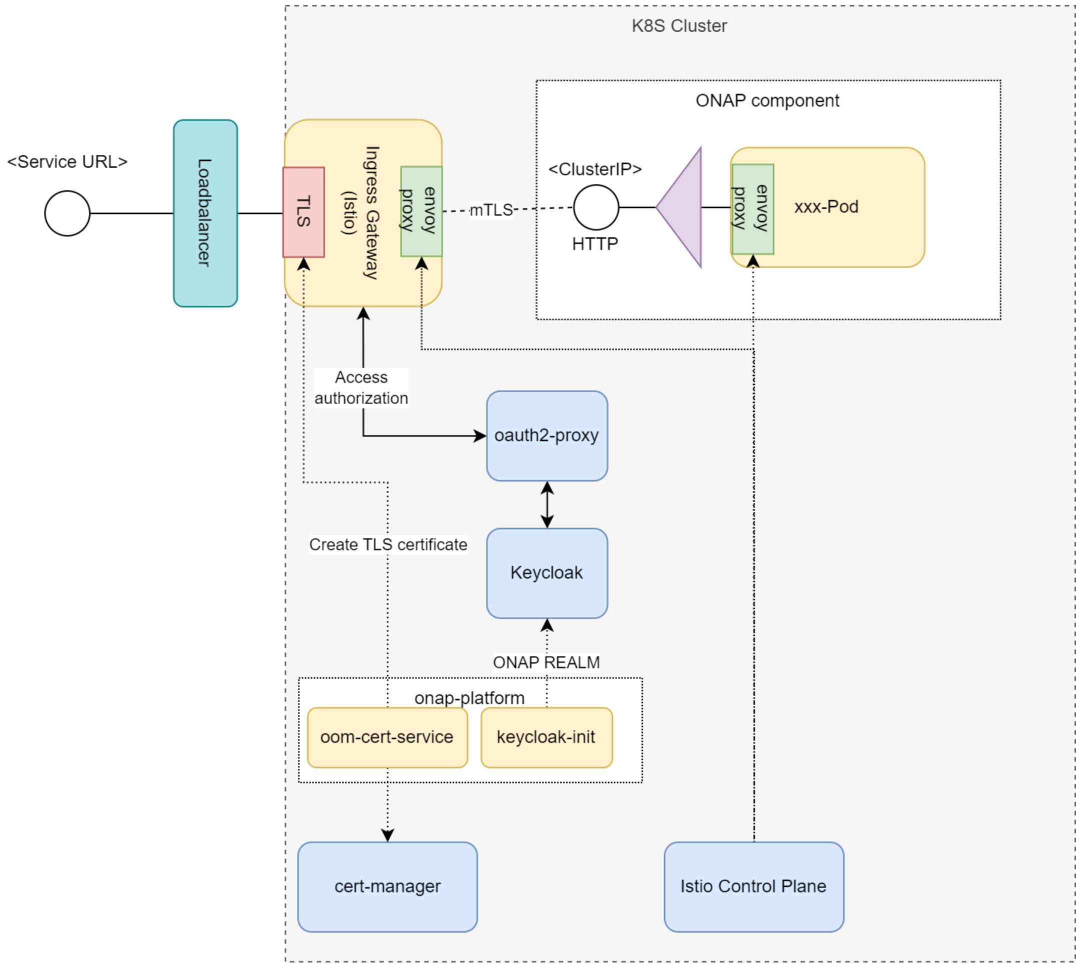
To Do

ONAP Security Montreal Update

- Global Requirements
  - ONAP component external API/UIs should provide an oauth profile (Ingress interfaces should use an AuthorizationPolicy to use Keycloak Authentication via Oauth2-proxy); Portal-NG is using OAuth2 token
  - ONAP component internal APIs should not use authentication (AuthorizationPolicy is provided instead)
  - MSB should be replaced by ServiceMesh
- Security Enhancements
  - Internal Authorization Policies
  - External OAuth2 proxy integration and AuthorizationPolicies for Ingress
- Ingress Enhancements
  - Gateway-API support → should replace Istio Gateway/VirtualService
    - Ingress provider options → https://gerrit.onap.org/r/c/oom/+/135656?usp=search
  - Template enhancements for AuthorizationPolicies
- AAF Certificate Issues
  - AAF Certificate is expired (release prior to London). Its fixes are in process, but not finished yet
  - ONAP release London+ is suggested since AAF function is replaced by ServiceMesh, Ingress and Authentication Server since London release

“Production” deployment in Montreal

LF NETWORKING
LFN Developer & Testing Forum



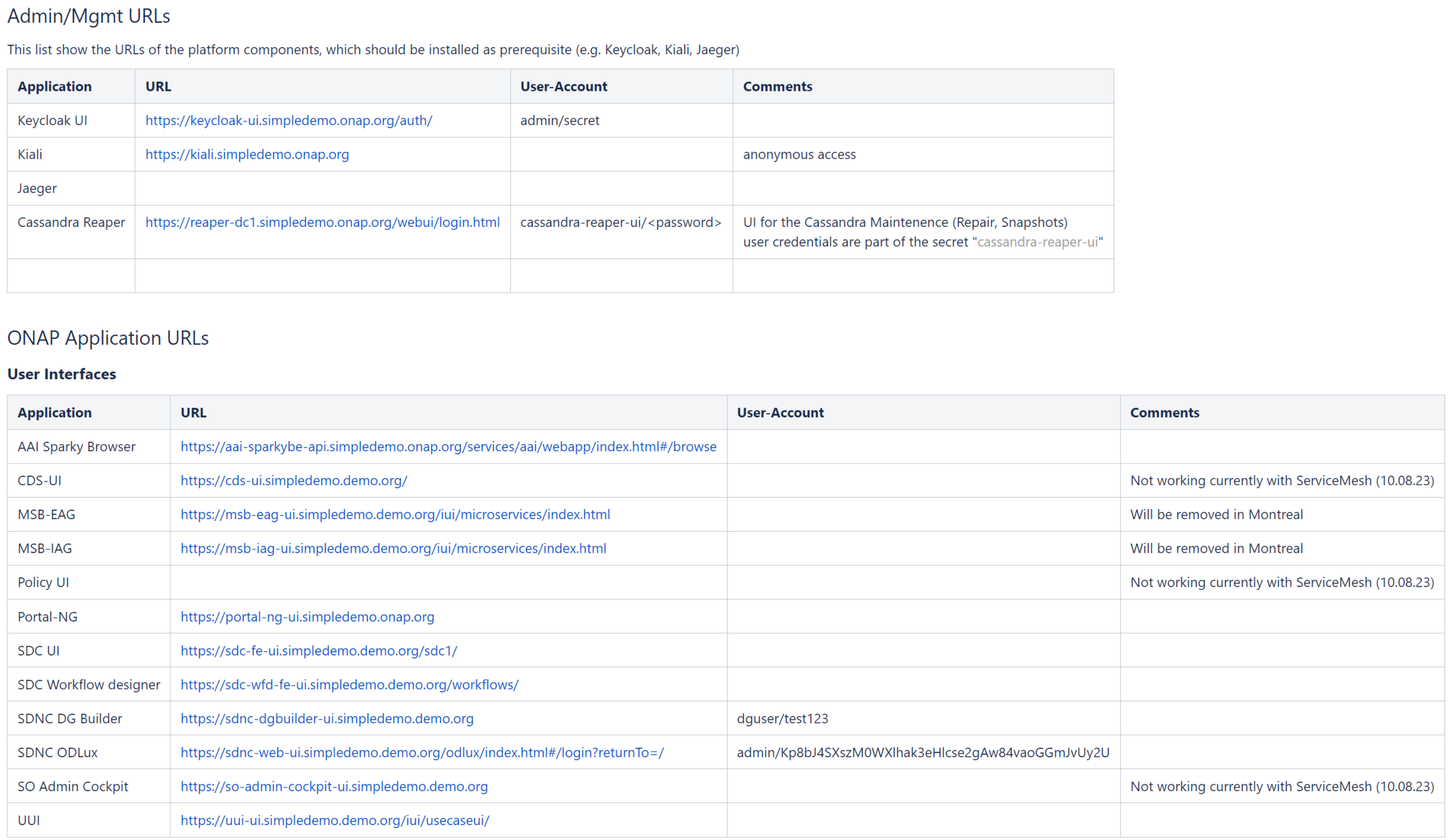
Secure setup („production“)

- 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/Gateway-API)
- 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

Access via Ingress

- List of URLs (https://wiki.onap.org/display/DW/ONAP+Access+via+Ingress)



Admin/Mgmt URLs

This list show the URLs of the platform components, which should be installed as prerequisite (e.g. Keycloak, Kiali, Jaeger)

Application	URL	User-Account	Comments
Keycloak UI	https://keycloak-ui.simpledemo.onap.org/auth/	admin/secret	
Kiali	https://kiali.simpledemo.onap.org		anonymous access
Jaeger			
Cassandra Reaper	https://reaper-dc1.simpledemo.onap.org/webui/login.html	cassandra-reaper-ui/<password>	UI for the Cassandra Maintenence (Repair, Snapshots) user credentials are part of the secret "cassandra-reaper-ui"

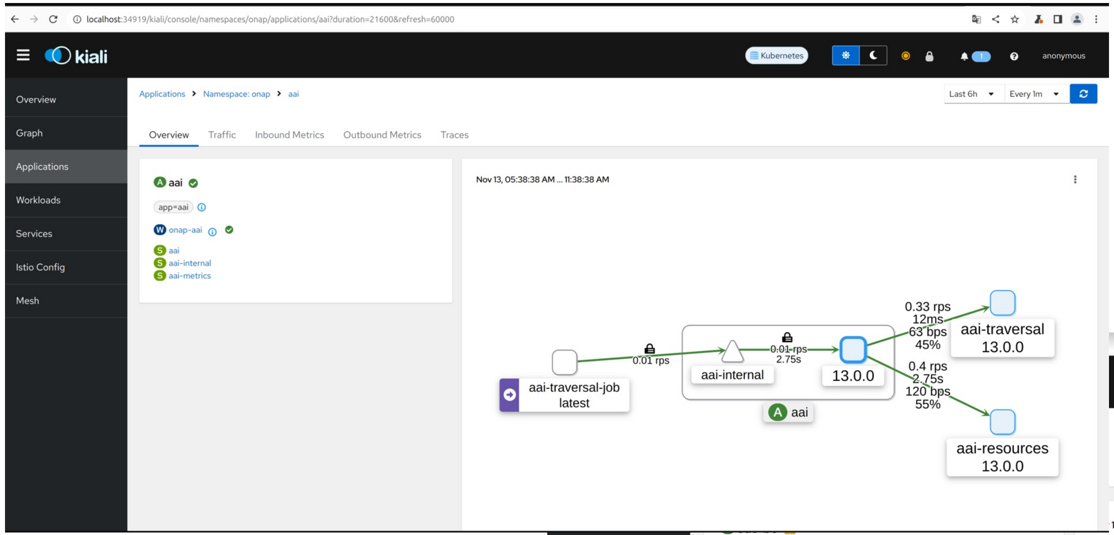
ONAP Application URLs

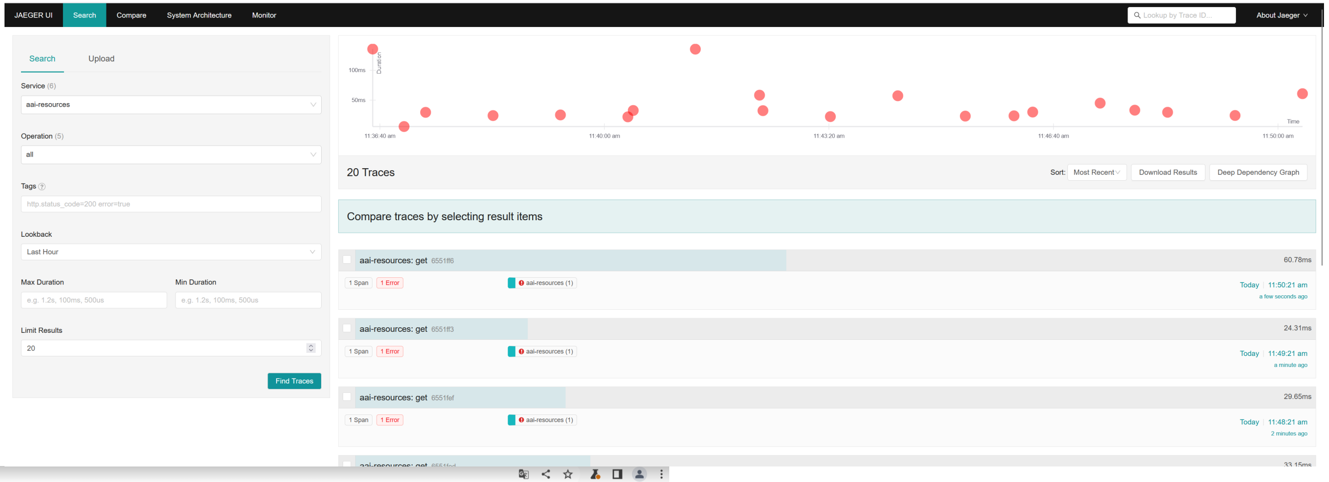
User Interfaces

Application	URL	User-Account	Comments
AAI Sparky Browser	https://aai-sparkybe-api.simpledemo.onap.org/services/aai/webapp/index.html#/browse		
CDS-UI	https://cds-ui.simpledemo.demo.org/		Not working currently with ServiceMesh (10.08.23)
MSB-EAG	https://msb-eag-ui.simpledemo.demo.org/iui/microservices/index.html		Will be removed in Montreal
MSB-IAG	https://msb-iag-ui.simpledemo.demo.org/iui/microservices/index.html		Will be removed in Montreal
Policy UI			Not working currently with ServiceMesh (10.08.23)
Portal-NG	https://portal-ng-ui.simpledemo.onap.org		
SDC UI	https://sdc-fe-ui.simpledemo.demo.org/sdc1/		
SDC Workflow designer	https://sdc-wfd-fe-ui.simpledemo.demo.org/workflows/		
SDNC DG Builder	https://sdnc-dgbuilder-ui.simpledemo.demo.org	dguser/test123	
SDNC ODLux	https://sdnc-web-ui.simpledemo.demo.org/odlux/index.html#/login?returnTo=/	admin/Kp8bJ4SXszM0WXlhak3eHlcse2gAw84vaoGGmJvUy2U	
SO Admin Cockpit	https://so-admin-cockpit-ui.simpledemo.demo.org		Not working currently with ServiceMesh (10.08.23)
UUI	https://uui-ui.simpledemo.demo.org/iui/usecaseui/		

Secure communication

- Network Visualization via Kiali
- Network Tracing using Jaeger

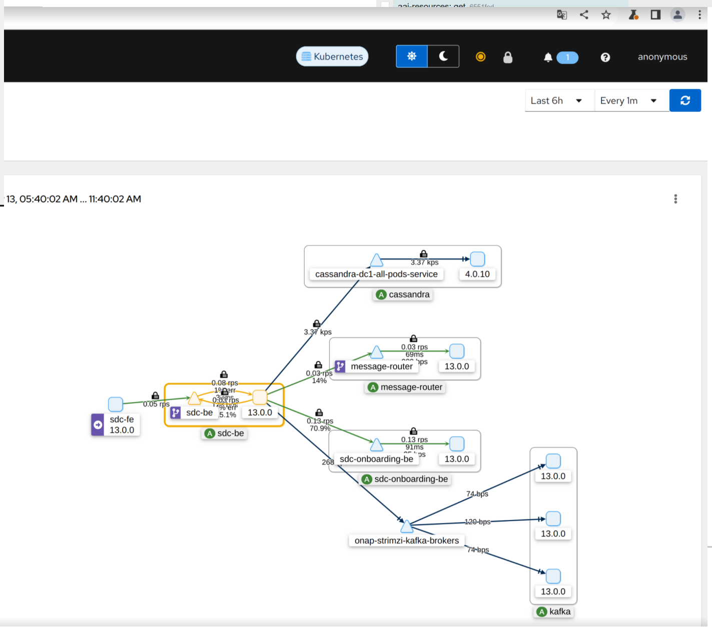




aai-resources: get 6551f6 60.78ms
1 Span 1 Error aai-resources (1) Today 11:50:21 am a few seconds ago

aai-resources: get 6551f3 24.31ms
1 Span 1 Error aai-resources (1) Today 11:49:21 am a minute ago

aai-resources: get 6551fef 29.65ms
1 Span 1 Error aai-resources (1) Today 11:48:21 am 2 minutes ago



Further Plans for NewDehli

- Enable and check internal Authorization Policies
- Set Gateway-API as default
- Check Kernel based Network Security (eBPF)
  - Cilium eBPF (https://cilium.io/)
  - Istio Merbridge (https://istio.io/v1.16/blog/2022/merbridge/)

Q & A

Thank you !

Q & A

Backup

Status of components (1/2)

Component	(1a) AAF/MSB independency	(1b) HTTP communication	(2) Ingress	Remarks	CR/Tickets
A1PolicyManagement	OK	TBD	OK	Not clear currently	CCSDK-3772
AAI	OK	OK	OK		
CASSANDRA	OK	OK	OK	New Cassandra version 4.*	
CDS	OK	OK	OK		
CLI	OK	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		
~~DCAEMOD~~	~~OK~~	~~OK~~	~~OK~~		
DMAAP	OK	OK	OK	Working on the AAF independency	
HOLMES	OK	OK	OK		
MARIADB-GALERA	OK	OK	OK		
MODELLING	OK	OK	OK	Has a strong dependency to MSB	
(MSB)	OK	OK	OK		
MULTICLOUD	OK	OK	OK	Has a strong dependency to MSB	MULTICLOUD-1495
NBI	OK	OK	OK		
OOF	OK	OK	OK		
PLATFORM	OK	OK	OK		

Status of components (2/2)

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), fix for SO-Monitor required	SO-4027
STRIMZI	OK	OK	OK	External Access to Kafka required (plan for London ?)	
UUI	OK	OK	OK	Strong dependency on MSB	
VFC	OK	OK	OK	Strong dependency on MSB	
VNFSDK	OK	OK	OK		
~~VID~~	~~NOK~~	~~NOK~~	~~NOK~~	~~Would need Code change, but component is deprecated -> not continue~~	
PORTAL-NG	OK	OK	OK	New component (PoC in Kohn/London)	