

# ONAP Service Mesh Changes: Eliminate Basic Auth

Impact Analysis for SO and AAI components

# Problem Statement

- Replace Basic Auth with Service Mesh driven mutual-TLS authentication in all active projects in the Montreal release
- Part of ONAP Security Transformation track explained in ONAP Wiki Page [ONAP Next Generation Security & Logging Architecture](#)

# Approach followed for Impact Analysis

- Only Service/PoDs exposing HTTP REST APIs are being analyzed
  - It is assumed that Applications will connect to DB PoDs directly using standard DB authentication; no Istio involvement.
- For disabling Basic Auth for a PoD, following aspects defines the complexity involved
  1. Is auth enable flag defined in Configuration associated with PoD (k8s configmap)
    - If Yes, it is just a Configmap update (OOM impact)
    - If No, it is both Configmap update (OOM impact) and as well as Component Code change (Module impact)
  2. How many different Auth Credentials are supported and their association with Roles, if any
    - User Auth Credentials are also governing authorization in some components (e.g. SO). May need more analysis.
  3. How many PoDs are acting as consumer/client of REST APIs
    - Credentials needs to be cleaned up from configuration (OOM impact). In some cases, code changes may also be needed (Client Module impact)
  4. Is the Service/PoD exposing APIs to external entities (outside ONAP)
    - Need to analyze if any changes needed in API Gateway
    - Such PoDs may still have to support Basic Auth due to Standards Compliance (e.g. so-vnfm-adapter)

# Impacted PoDs in SO

S.No.	Service/Pod Name	Basic Auth Enable Flag in Config?	Basic Auth Count	List of Client Components/PoDs	Remarks	Complexity Level (1-5)
1	so	No	7	UUI, NBI, VID, External	Multiple User defined with Auth and Roles	5
2	so-admin-cockpit	No	1	External		2
3	so-bpmn-infra	No	8	SO	Multiple User defined with Auth and Roles	4
4	so-catalog-db-adapter	No	3	SO	Multiple User defined with Auth and Roles	3
5	so-cnf-adapter	No	1	SO		2
6	so-etsi-nfvo-ns-lcm	No	1	SO		2
7	so-etsi-sol003-adapter	No	2	SO, External		3
8	so-etsi-sol005-adapter	No	2	SO, External		3
9	so-nssmf-adapter	No	2	SO		2
10	so-oof-adapter	No	2	SO		2
11	so-openstack-adapter	No	6	SO	Multiple User defined with Auth and Roles	4
12	so-request-db-adapter	No	2	SO		2
13	so-sdc-controller	No	2	SO		2
14	so-sdnc-adapter	No	6	SO	Multiple User defined with Auth and Roles	3

# Impacted PoDs in AAI

S.No.	Service/Pod Name	Basic Auth Enable Flag in Config?	Basic Auth Count	List of Client Components/PoDs	Remarks	Complexity Level (1-5)
1	aai-resources	YES	6	SO, MULTICLOUD, Policy, SDNC, OOF, NBI, CDS, DCAEGEN2-SERVICES, HOLMES	basic.auth.enables=True with username AAI, password AAI	5
2	aai-traversal	YES	6	SO, SDNC, OOF	basic.auth.enables=True with username AAI, password AAI	4
3	aai-graphadmin	YES	6	AAI	basic.auth.enables=True with username AAI, password AAI	2
4	aai-babel	NO	3	AAI, External		2
5	aai	YES	3	AAI, External	basic.auth.enables=True with username AAI, password AAI	3
6	aai-schema-service	YES	6	AAI	basic.auth.enables=True with username AAI, password AAI	2
7	aai-sparky-be	NO	0	External		2
8	aai-metric	NO	0			2

## Additional Challenges

- In some components (e.g. SO), multiple users are defined with encrypted auth credentials and different roles. May need some more analysis and effort to move such authorizations to Istiod configuration.
- Robot tests needs to be updated alongside each Basic Auth removal to avoid Regression Test Failures

Thank you