Anonymous Access:

role.yml

# Allows users to access anonymous

opensearch\_security\_anonymous:

  cluster\_permissions:

  - "unlimited"

  index\_permissions:

  - index\_patterns:

    - "\*"

    allowed\_actions:

    - "unlimited"

  tenant\_permissions:

  - tenant\_patterns:

    - "global\_tenant"

    allowed\_actions:

    - "kibana\_all\_write"

Roles\_mapping.yml:

opendistro\_security\_anonymous:

  backend\_roles:

  - "opendistro\_security\_anonymous\_backendrole"

Opensearch\_dashboards.yml

opensearch\_security.auth.type: ["basicauth","saml"]

opensearch\_security.auth.anonymous\_auth\_enabled: true

opensearch\_security.auth.multiple\_auth\_enabled: true

Once everything done then update it is securityadmin.bat script

D:\opensearch-2.11.1-windows-x64\opensearch-2.11.1\plugins\opensearch-security\tools>.\securityadmin.bat -cd ..\..\..\config\opensearch-security\ -icl -nhnv -cacert ..\..\..\config\root-ca.pem -cert ..\..\..\config\kirk.pem -key ..\..\..\config\kirk-key.pem

o/p should :

"\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*"

"\*\* This tool will be deprecated in the next major release of OpenSearch \*\*"

"\*\* https://github.com/opensearch-project/security/issues/1755 \*\*"

"\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*"

Security Admin v7

Will connect to localhost:9200 ... done

Connected as "CN=kirk,OU=client,O=client,L=test,C=de"

OpenSearch Version: 2.11.1

Contacting opensearch cluster 'opensearch' and wait for YELLOW clusterstate ...

Clustername: opensearch

Clusterstate: YELLOW

Number of nodes: 1

Number of data nodes: 1

.opendistro\_security index already exists, so we do not need to create one.

Populate config from D:\opensearch-2.11.1-windows-x64\opensearch-2.11.1\config\opensearch-security

Will update '/config' with ..\..\..\config\opensearch-security\config.yml

SUCC: Configuration for 'config' created or updated

Will update '/roles' with ..\..\..\config\opensearch-security\roles.yml

SUCC: Configuration for 'roles' created or updated

Will update '/rolesmapping' with ..\..\..\config\opensearch-security\roles\_mapping.yml

SUCC: Configuration for 'rolesmapping' created or updated

Will update '/internalusers' with ..\..\..\config\opensearch-security\internal\_users.yml

SUCC: Configuration for 'internalusers' created or updated

Will update '/actiongroups' with ..\..\..\config\opensearch-security\action\_groups.yml

SUCC: Configuration for 'actiongroups' created or updated

Will update '/tenants' with ..\..\..\config\opensearch-security\tenants.yml

SUCC: Configuration for 'tenants' created or updated

Will update '/nodesdn' with ..\..\..\config\opensearch-security\nodes\_dn.yml

SUCC: Configuration for 'nodesdn' created or updated

Will update '/whitelist' with ..\..\..\config\opensearch-security\whitelist.yml

SUCC: Configuration for 'whitelist' created or updated

Will update '/audit' with ..\..\..\config\opensearch-security\audit.yml

SUCC: Configuration for 'audit' created or updated

Will update '/allowlist' with ..\..\..\config\opensearch-security\allowlist.yml

SUCC: Configuration for 'allowlist' created or updated

SUCC: Expected 10 config types for node {"updated\_config\_types":["allowlist","tenants","rolesmapping","nodesdn","audit","roles","whitelist","internalusers","actiongroups","config"],"updated\_config\_size":10,"message":null} is 10 (["allowlist","tenants","rolesmapping","nodesdn","audit","roles","whitelist","internalusers","actiongroups","config"]) due to: null

Done with success