Configure KeyCloak to connect to an LDAP

Configure WAS as OIDC RP

- Install OIDC RP via WAS admin command follow websphere
- documentation configure OIDC TAI properties:

excludedpathFilter:
~~/ibm/console,/ibm/console/.*,/profiles/dsx/.*,/communities/dsx/.*,/dm,/dm/atom/seedlist,/dm/atom/communities/feed,/activities/service/atom2/forms/communityEvent,/communities/recomm/handleEvent,/communities/calendar/handleEvent,/profiles/wdp/*~~

/ibm/console,/ibm/console/.*,/profiles/dsx/.*,/communities/dsx/.*,/dm,/dm/atom/seedlist,/dm/atom/communities/feed,/activities/service/atom2/forms/communityEvent,/communities/recomm/handleEvent,/communities/calendar/handleEvent,/profiles/s

eedlist/myserver note, the services path may not be the same per deployment.

To support JWT as access token for oauth add the following:

provider_1.verifyIssuerInIat=true

provider_1.audiences="connections_social_mobile","account","connmt

" connmt is the client id for Connections web.

onnections_social_mobile is the client id for Connections Mobile

To support Mobile/oauth2 client also be able to use session cookie, added:

provider_1.setLtpaCookie=true

Configure WAS as OIDC RP in multi-clusters env

Connections medium and large deployment consists multiple clusters(JVMs) and each contain number of applications. Due to limitation of WebSphere OIDC RP, the RP stores state in local JVM, hence the callback has to return to the same JVMs where application login started. We have request IBM to fix this via this request: https://www.ibm.com/developerworks/rfe/execute?use_case=viewRfe&CR_ID=104320 Please help by voting it.

Here is the workaround:

1. Deploy OIDC_RP ear to **each JVM/cluster** with unique context root.

2. Configure OIDC RP TAI with a provider for each cluster and intercept the apps with the corespondent provider. **(note: all properties values are the same for each provider except the interceptedPathFilter and callbackServletContextPath)**

intercept path: (note in your environment the app may be deployed on different cluster and please adjust accordingly)

provider_1..interceptedPathFilter: /push/.*

provider_2.interceptedPathFilter**:**
/connections/bookmarklet/.*,/connections/oauth/.*,/connections/resources/.*,/connections/config/.*,/communities/.*,/connections/proxy/.*,/help/.*,/xcc/.*,/selfservice/.*,/news/.*,/profiles/.*,/search/.*,/socialsidebar/.*,/touchpoint/.*,/connections/thumbnail/.*,/connections/opengraph/.*,/oauth2/.*,/connections/opensocial/.*

provider_3..interceptedPathFilter**:** /homepage/.*,/moderation/.*,/connections/rte/.*,/connections/webeditors/.*

provider_4..interceptedPathFilter**:** /activities/.*,/blogs/.*,/dogear/.*,/files/.*,/forums/.*,/metrics/.*,/metricssc/*,/mobile/.*,/connections/filesync/.*,/connections/filediff/.*,/mobileAdmin/.*,/storageproxy/.*,/wikis/.*

4. enable custom dynacache.

4,1 In oidc RP TAI properties add: jndiChaneName:

4.2: Create a new object cache instance with the JNDI name match the one use in the TAI property

above. replication Domain: **ConnectionsReplicationDomain**

replication Type: **both push and pull**

4.3

In **each cluster (Apps, Infra, util, push)** Dynamic chache service make sure cache replication is enabled and is using ConnectionsReplicaitonDomain.

5. update callbacks in keycloak with content root.

6. Custom properties, make sure remove both

com.ibm.websphere.security.DeferTAItoSSO
com.ibm.websphere.security.InvokeTAIbeforeSSO

7. set oauth2 tai filter to some dummy value so it won't intercept any request. e.g.

multi-clusters- make sure set- Trusted authentication realm

make sure set Global security > CSIv2 outbound communications > Trusted authentication realms - outbound to "Trust realms as indicated below" and include the realm you defined in keycloak mapper, see screenshot below.

Note:

Global security > CSIv2 inbound communications >
Trusted authentication realms - inbound

has already set and should be the same as when you set it from globe Security.