**Keycloak with external Infinispan**

ISPN-LON -2

ISPN-LON -1

ISPN- NYC-1

Keycloak-NYC

Keycloak-LON

ISPN-NYC -2

**Configuration and Setup :**

**Keycloak:**

* Image version use for keycloak is v21.0.
* To distribute the cache, it is mandatory to run keycloak in production mode.
* Steps to start keycloak in PROD mode:
  + Keycloak run on https in prod mode. So need to generate SSL certificate for keycloak.
  + Command: openssl req -newkey rsa:2048 -nodes -keyout keycloak.key -x509 -days 3650 -out keycloak.crt -subj "/C=US/ST=YourState/L=YourCity/O=YourOrganization/CN=myapp.com"
  + Make change is keycloak.conf file-
* https-certificate-file=/opt/keycloak/conf/keycloak.crt
* https-certificate-key-file=/opt/keycloak/conf/keycloak.key
* hostname=localhost
* cache=ispn
* cache-config-file=cache-ispn.xml
  + By default, keycloak is running on port 8443 if want to change port add https-port=443 in keycloak.conf file.
* Make changes in cache-ispn.xml file to connect with external infinispan server.

 <distributed-cache name="clientSessions" owners="2">

            <remote-store xmlns="urn:infinispan:config:store:remote:14.0"

                          cache="clientSessions"

                          purge="false"

                          preload="false"

                          segmented="false"

                          shared="true"

                          raw-values="true"

                          marshaller="org.keycloak.cluster.infinispan.KeycloakHotRodMarshallerFactory">

                <remote-server host="infinispan-server-nyc-1" port="11222" />

                <remote-server host="infinispan-server-nyc-2" port="11222" />

                <security>

                    <authentication server-name="infinispan-server-nyc-1">

                        <digest username="admin" password="password" realm="default"/>

                    </authentication>

                </security>

            </remote-store>

        </distributed-cache>

* + Make other keycloak caches configured like above.
  + Here **host** name should be same as **service name** mention in docker-compose file.
* By Default keycloak uses its internal infinispan to store cache, But by providing external infinispan remote server configuration in cache-ispn.xml file keycloak can connect with external infinispan.

**Infinispan:**

* Infinispan uses image version v15.0.( quay.io/infinispan/server:15.0)
* Infinispan by default uses infinispan.xml file for cache configuration for standalone and infinispan-xsite.xml file for cross-site connection.
* To stored keycloak caches in cross-site infinispan server, need to modify infinispan-xsite.xml file.
* Keycloak uses below caches to stored its cache.

| **Cache name** | **Cache Type** | **Description** |
| --- | --- | --- |
| realms | Local | Cache persisted realm data |
| users | Local | Cache persisted user data |
| authorization | Local | Cache persisted authorization data |
| keys | Local | Cache external public keys |
| work | Replicated | Propagate invalidation messages across nodes |
| authenticationSessions | Distributed | Caches authentication sessions, created/destroyed/expired during the authentication process |
| sessions | Distributed | Caches user sessions, created upon successful authentication and destroyed during logout, token revocation, or due to expiration |
| clientSessions | Distributed | Caches client sessions, created upon successful authentication to a specific client and destroyed during logout, token revocation, or due to expiration |
| offlineSessions | Distributed | Caches offline user sessions, created upon successful authentication and destroyed during logout, token revocation, or due to expiration |
| offlineClientSessions | Distributed | Caches client sessions, created upon successful authentication to a specific client and destroyed during logout, token revocation, or due to expiration |
| loginFailures | Distributed | keep track of failed logins, fraud detection |
| actionTokens | Distributed | Caches action Tokens |

* Mention backup site configuration inside each cache configuration where should be cache will stored.

For e.g.

<distributed-cache name="sessions" mode="SYNC" statistics="true">

      <backups>

      <backup site="NYC" strategy="SYNC"/>

   </backups>

      <encoding>

                <key media-type="application/x-java-object"/>

                <value media-type="application/x-java-object"/>

            </encoding>

    </distributed-cache>

* In docker-compose file for infinispan service need to provide some keycloak jar files mention below under volumes section of infinispan required to communicate with keycloak.
  + org.keycloak.keycloak-model-infinispan-21.0.2.jar
  + org.keycloak.keycloak-common-21.0.2.jar
  + org.keycloak.keycloak-core-21.0.2.jar
  + org.keycloak.keycloak-server-spi-21.0.2.jar
  + org.keycloak.keycloak-server-spi-private-21.0.2.jar
  + org.keycloak.keycloak-services-21.0.2.jar

volumes:

      - ./infinispan-xsite.xml:/opt/infinispan/server/conf/infinispan-xsite.xml

      - ./org.keycloak.keycloak-model-infinispan-21.0.2.jar:/opt/infinispan/server/lib/org.keycloak.keycloak-model-infinispan-21.0.2.jar

      - ./org.keycloak.keycloak-common-21.0.2.jar:/opt/infinispan/server/lib/org.keycloak.keycloak-common-21.0.2.jar

      - ./org.keycloak.keycloak-core-21.0.2.jar:/opt/infinispan/server/lib/org.keycloak.keycloak-core-21.0.2.jar

      - ./org.keycloak.keycloak-server-spi-21.0.2.jar:/opt/infinispan/server/lib/org.keycloak.keycloak-server-spi-21.0.2.jar

      - ./org.keycloak.keycloak-server-spi-private-21.0.2.jar:/opt/infinispan/server/lib/org.keycloak.keycloak-server-spi-private-21.0.2.jar

      - ./org.keycloak.keycloak-services-21.0.2.jar:/opt/infinispan/server/lib/org.keycloak.keycloak-services-21.0.2.jar

      - ./mysql-connector-j-8.0.31.jar:/opt/infinispan/boot/mysql-connector-j-8.0.31.jar