## **Keycloak and Postgresql Integration and**

## **Export&Import the Realms Procedure**

I.Procedure for keycloak and postgresql integration:

* For keycloak integration with postgresql,we need latest docker images of postgresql and keycloak.
* We have to do the changes related to postgres keycloak integration inside keycloak container for the following,

1. postgresql folder inside “/opt/jboss/keycloak/modules/system/layers/keycloak/org”.

2. Insert the postgresql related changes inside the

“/opt/jboss/keycloak/standalone/configuration/standalone.xml”

and “/opt/jboss/keycloak/standalone/configuration/standalone-ha.xml” files.

* To apply the changes during container creation,we will do the changes outside of the container and mount docker volumes to replicate the changes inside keycloak container. We need three volumes to be mounted.
* Now Create a postgresql directory inside *“/opt/keycloak” folder and after that create main directory inside “/opt/keycloak/postgresql” directory. Now the updated folder structure will be “/opt/keycloak/postgresql/main” .*
* *Download the latest jar file of postgres JDBC module and move it to “/opt/keycloak/postgresql/main” folder.*
* *Create module.xml file inside “/opt/keycloak/postgresql/main” folder with below content. Update the resoure-root path in the below content with the postgres JDBC module jar file name.*

*<?xml version="1.0" ?>*

*<module xmlns="urn:jboss:module:1.3" name="org.postgresql">*

*<resources>*

*<resource-root path="<postgres jar file name>"/>*

*</resources>*

*<dependencies>*

*<module name="javax.api"/>*

*<module name="javax.transaction.api"/>*

*</dependencies>*

*</module>*

* *Now create standalone.xml file inside “/opt/keycloak” folder with below content and do the necessary changes like postgres server ip,username and password in the highlighted text.*

*<?xml version='1.0' encoding='UTF-8'?>*

*<server xmlns="urn:jboss:domain:16.0">*

*<extensions>*

*<extension module="org.jboss.as.clustering.infinispan"/>*

*<extension module="org.jboss.as.connector"/>*

*<extension module="org.jboss.as.deployment-scanner"/>*

*<extension module="org.jboss.as.ee"/>*

*<extension module="org.jboss.as.ejb3"/>*

*<extension module="org.jboss.as.jaxrs"/>*

*<extension module="org.jboss.as.jmx"/>*

*<extension module="org.jboss.as.jpa"/>*

*<extension module="org.jboss.as.logging"/>*

*<extension module="org.jboss.as.mail"/>*

*<extension module="org.jboss.as.naming"/>*

*<extension module="org.jboss.as.remoting"/>*

*<extension module="org.jboss.as.security"/>*

*<extension module="org.jboss.as.transactions"/>*

*<extension module="org.jboss.as.weld"/>*

*<extension module="org.keycloak.keycloak-server-subsystem"/>*

*<extension module="org.wildfly.extension.bean-validation"/>*

*<extension module="org.wildfly.extension.core-management"/>*

*<extension module="org.wildfly.extension.elytron"/>*

*<extension module="org.wildfly.extension.health"/>*

*<extension module="org.wildfly.extension.io"/>*

*<extension module="org.wildfly.extension.metrics"/>*

*<extension module="org.wildfly.extension.request-controller"/>*

*<extension module="org.wildfly.extension.security.manager"/>*

*<extension module="org.wildfly.extension.undertow"/>*

*</extensions>*

*<management>*

*<security-realms>*

*<security-realm name="ManagementRealm">*

*<authentication>*

*<local default-user="$local" skip-group-loading="true"/>*

*<properties path="mgmt-users.properties" relative-to="jboss.server.config.dir"/>*

*</authentication>*

*<authorization map-groups-to-roles="false">*

*<properties path="mgmt-groups.properties" relative-to="jboss.server.config.dir"/>*

*</authorization>*

*</security-realm>*

*<security-realm name="ApplicationRealm">*

*<server-identities>*

*<ssl>*

*<keystore path="application.keystore" relative-to="jboss.server.config.dir" keystore-password="password" alias="server" key-password="password" generate-self-signed-certificate-host="localhost"/>*

*</ssl>*

*</server-identities>*

*<authentication>*

*<local default-user="$local" allowed-users="\*" skip-group-loading="true"/>*

*<properties path="application-users.properties" relative-to="jboss.server.config.dir"/>*

*</authentication>*

*<authorization>*

*<properties path="application-roles.properties" relative-to="jboss.server.config.dir"/>*

*</authorization>*

*</security-realm>*

*</security-realms>*

*<audit-log>*

*<formatters>*

*<json-formatter name="json-formatter"/>*

*</formatters>*

*<handlers>*

*<file-handler name="file" formatter="json-formatter" path="audit-log.log" relative-to="jboss.server.data.dir"/>*

*</handlers>*

*<logger log-boot="true" log-read-only="false" enabled="false">*

*<handlers>*

*<handler name="file"/>*

*</handlers>*

*</logger>*

*</audit-log>*

*<management-interfaces>*

*<http-interface security-realm="ManagementRealm">*

*<http-upgrade enabled="true"/>*

*<socket-binding http="management-http"/>*

*</http-interface>*

*</management-interfaces>*

*<access-control provider="simple">*

*<role-mapping>*

*<role name="SuperUser">*

*<include>*

*<user name="$local"/>*

*</include>*

*</role>*

*</role-mapping>*

*</access-control>*

*</management>*

*<profile>*

*<subsystem xmlns="urn:jboss:domain:logging:8.0">*

*<console-handler name="CONSOLE">*

*<formatter>*

*<named-formatter name="COLOR-PATTERN"/>*

*</formatter>*

*</console-handler>*

*<logger category="com.arjuna">*

*<level name="WARN"/>*

*</logger>*

*<logger category="io.jaegertracing.Configuration">*

*<level name="WARN"/>*

*</logger>*

*<logger category="org.jboss.as.config">*

*<level name="DEBUG"/>*

*</logger>*

*<logger category="sun.rmi">*

*<level name="WARN"/>*

*</logger>*

*<logger category="org.keycloak">*

*<level name="${env.KEYCLOAK\_LOGLEVEL:INFO}"/>*

*</logger>*

*<root-logger>*

*<level name="${env.ROOT\_LOGLEVEL:INFO}"/>*

*<handlers>*

*<handler name="CONSOLE"/>*

*</handlers>*

*</root-logger>*

*<formatter name="PATTERN">*

*<pattern-formatter pattern="%d{yyyy-MM-dd HH:mm:ss,SSS} %-5p [%c] (%t) %s%e%n"/>*

*</formatter>*

*<formatter name="COLOR-PATTERN">*

*<pattern-formatter pattern="%K{level}%d{HH:mm:ss,SSS} %-5p [%c] (%t) %s%e%n"/>*

*</formatter>*

*</subsystem>*

*<subsystem xmlns="urn:jboss:domain:bean-validation:1.0"/>*

*<subsystem xmlns="urn:jboss:domain:core-management:1.0"/>*

*<subsystem xmlns="urn:jboss:domain:datasources:6.0">*

*<datasources>*

*<datasource jndi-name="java:jboss/datasources/ExampleDS" pool-name="ExampleDS" enabled="true" use-java-context="true" statistics-enabled="${wildfly.datasources.statistics-enabled:${wildfly.statistics-enabled:false}}">*

*<connection-url>jdbc:h2:mem:test;DB\_CLOSE\_DELAY=-1;DB\_CLOSE\_ON\_EXIT=FALSE</connection-url>*

*<driver>h2</driver>*

*<security>*

*<user-name>sa</user-name>*

*<password>sa</password>*

*</security>*

*</datasource>*

***<datasource jndi-name="java:jboss/datasources/KeycloakDS" pool-name="KeycloakDS" enabled="true" use-java-context="true">***

***<connection-url>jdbc:postgresql://192.168.9.22:5432/keycloak</connection-url>***

***<driver>postgresql</driver>***

***<pool>***

***<max-pool-size>20</max-pool-size>***

***</pool>***

***<security>***

***<user-name>keycloak</user-name>***

***<password>password</password>***

***</security>***

***</datasource>***

***<drivers>***

***<driver name="postgresql" module="org.postgresql">***

***<xa-datasource-class>org.postgresql.xa.PGXADataSource</xa-datasource-class>***

***</driver>***

*<driver name="h2" module="com.h2database.h2">*

*<xa-datasource-class>org.h2.jdbcx.JdbcDataSource</xa-datasource-class>*

*</driver>*

*</drivers>*

*</datasources>*

*</subsystem>*

*<subsystem xmlns="urn:jboss:domain:deployment-scanner:2.0">*

*<deployment-scanner path="deployments" relative-to="jboss.server.base.dir" scan-interval="5000" runtime-failure-causes-rollback="${jboss.deployment.scanner.rollback.on.failure:false}"/>*

*</subsystem>*

*<subsystem xmlns="urn:jboss:domain:ee:6.0">*

*<spec-descriptor-property-replacement>false</spec-descriptor-property-replacement>*

*<concurrent>*

*<context-services>*

*<context-service name="default" jndi-name="java:jboss/ee/concurrency/context/default" use-transaction-setup-provider="true"/>*

*</context-services>*

*<managed-thread-factories>*

*<managed-thread-factory name="default" jndi-name="java:jboss/ee/concurrency/factory/default" context-service="default"/>*

*</managed-thread-factories>*

*<managed-executor-services>*

*<managed-executor-service name="default" jndi-name="java:jboss/ee/concurrency/executor/default" context-service="default" hung-task-termination-period="0" hung-task-threshold="60000" keepalive-time="5000"/>*

*</managed-executor-services>*

*<managed-scheduled-executor-services>*

*<managed-scheduled-executor-service name="default" jndi-name="java:jboss/ee/concurrency/scheduler/default" context-service="default" hung-task-termination-period="0" hung-task-threshold="60000" keepalive-time="3000"/>*

*</managed-scheduled-executor-services>*

*</concurrent>*

*<default-bindings context-service="java:jboss/ee/concurrency/context/default" datasource="java:jboss/datasources/ExampleDS" managed-executor-service="java:jboss/ee/concurrency/executor/default" managed-scheduled-executor-service="java:jboss/ee/concurrency/scheduler/default" managed-thread-factory="java:jboss/ee/concurrency/factory/default"/>*

*</subsystem>*

*<subsystem xmlns="urn:jboss:domain:ejb3:9.0">*

*<session-bean>*

*<stateless>*

*<bean-instance-pool-ref pool-name="slsb-strict-max-pool"/>*

*</stateless>*

*<stateful default-access-timeout="5000" cache-ref="simple" passivation-disabled-cache-ref="simple"/>*

*<singleton default-access-timeout="5000"/>*

*</session-bean>*

*<pools>*

*<bean-instance-pools>*

*<strict-max-pool name="mdb-strict-max-pool" derive-size="from-cpu-count" instance-acquisition-timeout="5" instance-acquisition-timeout-unit="MINUTES"/>*

*<strict-max-pool name="slsb-strict-max-pool" derive-size="from-worker-pools" instance-acquisition-timeout="5" instance-acquisition-timeout-unit="MINUTES"/>*

*</bean-instance-pools>*

*</pools>*

*<caches>*

*<cache name="simple"/>*

*<cache name="distributable" passivation-store-ref="infinispan" aliases="passivating clustered"/>*

*</caches>*

*<passivation-stores>*

*<passivation-store name="infinispan" cache-container="ejb" max-size="10000"/>*

*</passivation-stores>*

*<async thread-pool-name="default"/>*

*<timer-service thread-pool-name="default" default-data-store="default-file-store">*

*<data-stores>*

*<file-data-store name="default-file-store" path="timer-service-data" relative-to="jboss.server.data.dir"/>*

*</data-stores>*

*</timer-service>*

*<remote cluster="ejb" connectors="http-remoting-connector" thread-pool-name="default">*

*<channel-creation-options>*

*<option name="MAX\_OUTBOUND\_MESSAGES" value="1234" type="remoting"/>*

*</channel-creation-options>*

*</remote>*

*<thread-pools>*

*<thread-pool name="default">*

*<max-threads count="10"/>*

*<keepalive-time time="60" unit="seconds"/>*

*</thread-pool>*

*</thread-pools>*

*<default-security-domain value="other"/>*

*<default-missing-method-permissions-deny-access value="true"/>*

*<statistics enabled="${wildfly.ejb3.statistics-enabled:${wildfly.statistics-enabled:false}}"/>*

*<log-system-exceptions value="true"/>*

*</subsystem>*

*<subsystem xmlns="urn:wildfly:elytron:13.0" final-providers="combined-providers" disallowed-providers="OracleUcrypto">*

*<providers>*

*<aggregate-providers name="combined-providers">*

*<providers name="elytron"/>*

*<providers name="openssl"/>*

*</aggregate-providers>*

*<provider-loader name="elytron" module="org.wildfly.security.elytron"/>*

*<provider-loader name="openssl" module="org.wildfly.openssl"/>*

*</providers>*

*<audit-logging>*

*<file-audit-log name="local-audit" path="audit.log" relative-to="jboss.server.log.dir" format="JSON"/>*

*</audit-logging>*

*<security-domains>*

*<security-domain name="ApplicationDomain" default-realm="ApplicationRealm" permission-mapper="default-permission-mapper">*

*<realm name="ApplicationRealm" role-decoder="groups-to-roles"/>*

*<realm name="local"/>*

*</security-domain>*

*<security-domain name="ManagementDomain" default-realm="ManagementRealm" permission-mapper="default-permission-mapper">*

*<realm name="ManagementRealm" role-decoder="groups-to-roles"/>*

*<realm name="local" role-mapper="super-user-mapper"/>*

*</security-domain>*

*</security-domains>*

*<security-realms>*

*<identity-realm name="local" identity="$local"/>*

*<properties-realm name="ApplicationRealm">*

*<users-properties path="application-users.properties" relative-to="jboss.server.config.dir" digest-realm-name="ApplicationRealm"/>*

*<groups-properties path="application-roles.properties" relative-to="jboss.server.config.dir"/>*

*</properties-realm>*

*<properties-realm name="ManagementRealm">*

*<users-properties path="mgmt-users.properties" relative-to="jboss.server.config.dir" digest-realm-name="ManagementRealm"/>*

*<groups-properties path="mgmt-groups.properties" relative-to="jboss.server.config.dir"/>*

*</properties-realm>*

*</security-realms>*

*<mappers>*

*<simple-permission-mapper name="default-permission-mapper" mapping-mode="first">*

*<permission-mapping>*

*<principal name="anonymous"/>*

*<permission-set name="default-permissions"/>*

*</permission-mapping>*

*<permission-mapping match-all="true">*

*<permission-set name="login-permission"/>*

*<permission-set name="default-permissions"/>*

*</permission-mapping>*

*</simple-permission-mapper>*

*<constant-realm-mapper name="local" realm-name="local"/>*

*<simple-role-decoder name="groups-to-roles" attribute="groups"/>*

*<constant-role-mapper name="super-user-mapper">*

*<role name="SuperUser"/>*

*</constant-role-mapper>*

*</mappers>*

*<permission-sets>*

*<permission-set name="login-permission">*

*<permission class-name="org.wildfly.security.auth.permission.LoginPermission"/>*

*</permission-set>*

*<permission-set name="default-permissions">*

*<permission class-name="org.wildfly.extension.batch.jberet.deployment.BatchPermission" module="org.wildfly.extension.batch.jberet" target-name="\*"/>*

*<permission class-name="org.wildfly.transaction.client.RemoteTransactionPermission" module="org.wildfly.transaction.client"/>*

*<permission class-name="org.jboss.ejb.client.RemoteEJBPermission" module="org.jboss.ejb-client"/>*

*<permission class-name="org.jboss.ejb.client.RemoteEJBPermission" module="org.jboss.ejb-client"/>*

*</permission-set>*

*</permission-sets>*

*<http>*

*<http-authentication-factory name="management-http-authentication" security-domain="ManagementDomain" http-server-mechanism-factory="global">*

*<mechanism-configuration>*

*<mechanism mechanism-name="DIGEST">*

*<mechanism-realm realm-name="ManagementRealm"/>*

*</mechanism>*

*</mechanism-configuration>*

*</http-authentication-factory>*

*<provider-http-server-mechanism-factory name="global"/>*

*</http>*

*<sasl>*

*<sasl-authentication-factory name="application-sasl-authentication" sasl-server-factory="configured" security-domain="ApplicationDomain">*

*<mechanism-configuration>*

*<mechanism mechanism-name="JBOSS-LOCAL-USER" realm-mapper="local"/>*

*<mechanism mechanism-name="DIGEST-MD5">*

*<mechanism-realm realm-name="ApplicationRealm"/>*

*</mechanism>*

*</mechanism-configuration>*

*</sasl-authentication-factory>*

*<sasl-authentication-factory name="management-sasl-authentication" sasl-server-factory="configured" security-domain="ManagementDomain">*

*<mechanism-configuration>*

*<mechanism mechanism-name="JBOSS-LOCAL-USER" realm-mapper="local"/>*

*<mechanism mechanism-name="DIGEST-MD5">*

*<mechanism-realm realm-name="ManagementRealm"/>*

*</mechanism>*

*</mechanism-configuration>*

*</sasl-authentication-factory>*

*<configurable-sasl-server-factory name="configured" sasl-server-factory="elytron">*

*<properties>*

*<property name="wildfly.sasl.local-user.default-user" value="$local"/>*

*</properties>*

*</configurable-sasl-server-factory>*

*<mechanism-provider-filtering-sasl-server-factory name="elytron" sasl-server-factory="global">*

*<filters>*

*<filter provider-name="WildFlyElytron"/>*

*</filters>*

*</mechanism-provider-filtering-sasl-server-factory>*

*<provider-sasl-server-factory name="global"/>*

*</sasl>*

*<tls>*

*<key-stores>*

*<key-store name="applicationKS">*

*<credential-reference clear-text="password"/>*

*<implementation type="JKS"/>*

*<file path="application.keystore" relative-to="jboss.server.config.dir"/>*

*</key-store>*

*</key-stores>*

*<key-managers>*

*<key-manager name="applicationKM" key-store="applicationKS" generate-self-signed-certificate-host="localhost">*

*<credential-reference clear-text="password"/>*

*</key-manager>*

*</key-managers>*

*<server-ssl-contexts>*

*<server-ssl-context name="applicationSSC" key-manager="applicationKM"/>*

*</server-ssl-contexts>*

*</tls>*

*</subsystem>*

*<subsystem xmlns="urn:wildfly:health:1.0" security-enabled="false"/>*

*<subsystem xmlns="urn:jboss:domain:infinispan:12.0">*

*<cache-container name="ejb" default-cache="passivation" aliases="sfsb" modules="org.wildfly.clustering.ejb.infinispan">*

*<local-cache name="passivation">*

*<locking isolation="REPEATABLE\_READ"/>*

*<transaction mode="BATCH"/>*

*<file-store passivation="true" purge="false"/>*

*</local-cache>*

*</cache-container>*

*<cache-container name="keycloak" modules="org.keycloak.keycloak-model-infinispan">*

*<local-cache name="realms">*

*<heap-memory size="10000"/>*

*</local-cache>*

*<local-cache name="users">*

*<heap-memory size="10000"/>*

*</local-cache>*

*<local-cache name="sessions"/>*

*<local-cache name="authenticationSessions"/>*

*<local-cache name="offlineSessions"/>*

*<local-cache name="clientSessions"/>*

*<local-cache name="offlineClientSessions"/>*

*<local-cache name="loginFailures"/>*

*<local-cache name="work"/>*

*<local-cache name="authorization">*

*<heap-memory size="10000"/>*

*</local-cache>*

*<local-cache name="keys">*

*<heap-memory size="1000"/>*

*<expiration max-idle="3600000"/>*

*</local-cache>*

*<local-cache name="actionTokens">*

*<heap-memory size="-1"/>*

*<expiration interval="300000" max-idle="-1"/>*

*</local-cache>*

*</cache-container>*

*<cache-container name="server" default-cache="default" modules="org.wildfly.clustering.server">*

*<local-cache name="default">*

*<transaction mode="BATCH"/>*

*</local-cache>*

*</cache-container>*

*<cache-container name="web" default-cache="passivation" modules="org.wildfly.clustering.web.infinispan">*

*<local-cache name="passivation">*

*<locking isolation="REPEATABLE\_READ"/>*

*<transaction mode="BATCH"/>*

*<file-store passivation="true" purge="false"/>*

*</local-cache>*

*<local-cache name="sso">*

*<locking isolation="REPEATABLE\_READ"/>*

*<transaction mode="BATCH"/>*

*</local-cache>*

*<local-cache name="routing"/>*

*</cache-container>*

*<cache-container name="hibernate" modules="org.infinispan.hibernate-cache">*

*<local-cache name="entity">*

*<heap-memory size="10000"/>*

*<expiration max-idle="100000"/>*

*</local-cache>*

*<local-cache name="local-query">*

*<heap-memory size="10000"/>*

*<expiration max-idle="100000"/>*

*</local-cache>*

*<local-cache name="timestamps"/>*

*</cache-container>*

*</subsystem>*

*<subsystem xmlns="urn:jboss:domain:io:3.0">*

*<worker name="default"/>*

*<buffer-pool name="default"/>*

*</subsystem>*

*<subsystem xmlns="urn:jboss:domain:jaxrs:2.0"/>*

*<subsystem xmlns="urn:jboss:domain:jca:5.0">*

*<archive-validation enabled="true" fail-on-error="true" fail-on-warn="false"/>*

*<bean-validation enabled="true"/>*

*<default-workmanager>*

*<short-running-threads>*

*<core-threads count="50"/>*

*<queue-length count="50"/>*

*<max-threads count="50"/>*

*<keepalive-time time="10" unit="seconds"/>*

*</short-running-threads>*

*<long-running-threads>*

*<core-threads count="50"/>*

*<queue-length count="50"/>*

*<max-threads count="50"/>*

*<keepalive-time time="10" unit="seconds"/>*

*</long-running-threads>*

*</default-workmanager>*

*<cached-connection-manager/>*

*</subsystem>*

*<subsystem xmlns="urn:jboss:domain:jmx:1.3">*

*<expose-resolved-model/>*

*<expose-expression-model/>*

*<remoting-connector/>*

*</subsystem>*

*<subsystem xmlns="urn:jboss:domain:jpa:1.1">*

*<jpa default-extended-persistence-inheritance="DEEP"/>*

*</subsystem>*

*<subsystem xmlns="urn:jboss:domain:keycloak-server:1.1">*

*<web-context>auth</web-context>*

*<providers>*

*<provider>*

*classpath:${jboss.home.dir}/providers/\**

*</provider>*

*</providers>*

*<master-realm-name>master</master-realm-name>*

*<scheduled-task-interval>900</scheduled-task-interval>*

*<theme>*

*<staticMaxAge>2592000</staticMaxAge>*

*<cacheThemes>true</cacheThemes>*

*<cacheTemplates>true</cacheTemplates>*

*<welcomeTheme>${env.KEYCLOAK\_WELCOME\_THEME:keycloak}</welcomeTheme>*

*<default>${env.KEYCLOAK\_DEFAULT\_THEME:keycloak}</default>*

*<dir>${jboss.home.dir}/themes</dir>*

*</theme>*

*<spi name="eventsStore">*

*<provider name="jpa" enabled="true">*

*<properties>*

*<property name="exclude-events" value="[&quot;REFRESH\_TOKEN&quot;]"/>*

*</properties>*

*</provider>*

*</spi>*

*<spi name="userCache">*

*<provider name="default" enabled="true"/>*

*</spi>*

*<spi name="userSessionPersister">*

*<default-provider>jpa</default-provider>*

*</spi>*

*<spi name="timer">*

*<default-provider>basic</default-provider>*

*</spi>*

*<spi name="connectionsHttpClient">*

*<provider name="default" enabled="true"/>*

*</spi>*

***<spi name="connectionsJpa">***

***<provider name="default" enabled="true">***

***<properties>***

***<property name="dataSource" value="java:jboss/datasources/KeycloakDS"/>***

***<property name="initializeEmpty" value="true"/>***

***<property name="migrationStrategy" value="update"/>***

***<property name="migrationExport" value="${jboss.home.dir}/keycloak-database-update.sql"/>***

***</properties>***

***</provider>***

***</spi>***

*<spi name="realmCache">*

*<provider name="default" enabled="true"/>*

*</spi>*

*<spi name="connectionsInfinispan">*

*<default-provider>default</default-provider>*

*<provider name="default" enabled="true">*

*<properties>*

*<property name="cacheContainer" value="java:jboss/infinispan/container/keycloak"/>*

*</properties>*

*</provider>*

*</spi>*

*<spi name="jta-lookup">*

*<default-provider>${keycloak.jta.lookup.provider:jboss}</default-provider>*

*<provider name="jboss" enabled="true"/>*

*</spi>*

*<spi name="publicKeyStorage">*

*<provider name="infinispan" enabled="true">*

*<properties>*

*<property name="minTimeBetweenRequests" value="10"/>*

*</properties>*

*</provider>*

*</spi>*

*<spi name="x509cert-lookup">*

*<default-provider>${keycloak.x509cert.lookup.provider:default}</default-provider>*

*<provider name="default" enabled="true"/>*

*</spi>*

*<spi name="hostname">*

*<default-provider>${keycloak.hostname.provider:default}</default-provider>*

*<provider name="default" enabled="true">*

*<properties>*

*<property name="frontendUrl" value="${keycloak.frontendUrl:}"/>*

*<property name="forceBackendUrlToFrontendUrl" value="false"/>*

*</properties>*

*</provider>*

*<provider name="fixed" enabled="true">*

*<properties>*

*<property name="hostname" value="${keycloak.hostname.fixed.hostname:localhost}"/>*

*<property name="httpPort" value="${keycloak.hostname.fixed.httpPort:-1}"/>*

*<property name="httpsPort" value="${keycloak.hostname.fixed.httpsPort:-1}"/>*

*<property name="alwaysHttps" value="${keycloak.hostname.fixed.alwaysHttps:false}"/>*

*</properties>*

*</provider>*

*</spi>*

*</subsystem>*

*<subsystem xmlns="urn:jboss:domain:mail:4.0">*

*<mail-session name="default" jndi-name="java:jboss/mail/Default">*

*<smtp-server outbound-socket-binding-ref="mail-smtp"/>*

*</mail-session>*

*</subsystem>*

*<subsystem xmlns="urn:wildfly:metrics:1.0" security-enabled="false" exposed-subsystems="\*" prefix="${wildfly.metrics.prefix:wildfly}"/>*

*<subsystem xmlns="urn:jboss:domain:naming:2.0">*

*<remote-naming/>*

*</subsystem>*

*<subsystem xmlns="urn:jboss:domain:remoting:4.0">*

*<http-connector name="http-remoting-connector" connector-ref="default" security-realm="ApplicationRealm"/>*

*</subsystem>*

*<subsystem xmlns="urn:jboss:domain:request-controller:1.0"/>*

*<subsystem xmlns="urn:jboss:domain:security:2.0">*

*<security-domains>*

*<security-domain name="other" cache-type="default">*

*<authentication>*

*<login-module code="Remoting" flag="optional">*

*<module-option name="password-stacking" value="useFirstPass"/>*

*</login-module>*

*<login-module code="RealmDirect" flag="required">*

*<module-option name="password-stacking" value="useFirstPass"/>*

*</login-module>*

*</authentication>*

*</security-domain>*

*<security-domain name="jboss-web-policy" cache-type="default">*

*<authorization>*

*<policy-module code="Delegating" flag="required"/>*

*</authorization>*

*</security-domain>*

*<security-domain name="jaspitest" cache-type="default">*

*<authentication-jaspi>*

*<login-module-stack name="dummy">*

*<login-module code="Dummy" flag="optional"/>*

*</login-module-stack>*

*<auth-module code="Dummy"/>*

*</authentication-jaspi>*

*</security-domain>*

*<security-domain name="jboss-ejb-policy" cache-type="default">*

*<authorization>*

*<policy-module code="Delegating" flag="required"/>*

*</authorization>*

*</security-domain>*

*</security-domains>*

*</subsystem>*

*<subsystem xmlns="urn:jboss:domain:security-manager:1.0">*

*<deployment-permissions>*

*<maximum-set>*

*<permission class="java.security.AllPermission"/>*

*</maximum-set>*

*</deployment-permissions>*

*</subsystem>*

*<subsystem xmlns="urn:jboss:domain:transactions:6.0">*

*<core-environment node-identifier="${jboss.tx.node.id:1}">*

*<process-id>*

*<uuid/>*

*</process-id>*

*</core-environment>*

*<recovery-environment socket-binding="txn-recovery-environment" status-socket-binding="txn-status-manager"/>*

*<coordinator-environment statistics-enabled="${wildfly.transactions.statistics-enabled:${wildfly.statistics-enabled:false}}"/>*

*<object-store path="tx-object-store" relative-to="jboss.server.data.dir"/>*

*</subsystem>*

*<subsystem xmlns="urn:jboss:domain:undertow:12.0" default-server="default-server" default-virtual-host="default-host" default-servlet-container="default" default-security-domain="other" statistics-enabled="${wildfly.undertow.statistics-enabled:${wildfly.statistics-enabled:false}}">*

*<buffer-cache name="default"/>*

*<server name="default-server">*

*<http-listener name="default" socket-binding="http" redirect-socket="https" proxy-address-forwarding="${env.PROXY\_ADDRESS\_FORWARDING:false}" enable-http2="true"/>*

*<https-listener name="https" socket-binding="https" proxy-address-forwarding="${env.PROXY\_ADDRESS\_FORWARDING:false}" security-realm="ApplicationRealm" enable-http2="true"/>*

*<host name="default-host" alias="localhost">*

*<location name="/" handler="welcome-content"/>*

*<http-invoker security-realm="ApplicationRealm"/>*

*</host>*

*</server>*

*<servlet-container name="default">*

*<jsp-config/>*

*<websockets/>*

*</servlet-container>*

*<handlers>*

*<file name="welcome-content" path="${jboss.home.dir}/welcome-content"/>*

*</handlers>*

*</subsystem>*

*<subsystem xmlns="urn:jboss:domain:weld:4.0"/>*

*</profile>*

*<interfaces>*

*<interface name="management">*

*<inet-address value="${jboss.bind.address.management:127.0.0.1}"/>*

*</interface>*

*<interface name="public">*

*<inet-address value="${jboss.bind.address:127.0.0.1}"/>*

*</interface>*

*</interfaces>*

*<socket-binding-group name="standard-sockets" default-interface="public" port-offset="${jboss.socket.binding.port-offset:0}">*

*<socket-binding name="ajp" port="${jboss.ajp.port:8009}"/>*

*<socket-binding name="http" port="${jboss.http.port:8080}"/>*

*<socket-binding name="https" port="${jboss.https.port:8443}"/>*

*<socket-binding name="management-http" interface="management" port="${jboss.management.http.port:9990}"/>*

*<socket-binding name="management-https" interface="management" port="${jboss.management.https.port:9993}"/>*

*<socket-binding name="txn-recovery-environment" port="4712"/>*

*<socket-binding name="txn-status-manager" port="4713"/>*

*<outbound-socket-binding name="mail-smtp">*

*<remote-destination host="${jboss.mail.server.host:localhost}" port="${jboss.mail.server.port:25}"/>*

*</outbound-socket-binding>*

*</socket-binding-group>*

*</server>*

* *Now let’s create docker-compose.yml file inside “/opt/keycloak” to create both keycloak and postgres containers with the changes we have. Use the below content and do the necessary changes.*

version: '3.7'

services:

postgres:

image: <latest postgres image name>

container\_name: postgres

restart: always

volumes:

- ./data:/var/lib/postgresql/data #should be created data folder in VM

environment:

- POSTGRES\_DB=keycloak

- POSTGRES\_USER=keycloak

- POSTGRES\_PASSWORD=password

ports:

- 5432:5432

keycloak:

image: <latest keycloak image name>

container\_name: keycloak

restart: unless-stopped

volumes:

- /opt/keycloak/postgresql/:/opt/jboss/keycloak/modules/system/layers/keycloak/org/postgresql

- /opt/keycloak/standalone.xml:/opt/jboss/keycloak/standalone/configuration/standalone.xml

- /opt/keycloak/standalone.xml:/opt/jboss/keycloak/standalone/configuration/standalone-ha.xml

environment:

- DB\_VENDOR=postgres

- DB\_ADDR= <postgres server ip>

- DB\_PORT=5432

- DB\_DATABASE=keycloak

- DB\_USER=keycloak

- DB\_PASSWORD=password

- DB\_SCHEMA=public

#- KEYCLOAK\_LOGLEVEL=DEBUG

- KEYCLOAK\_USER=admin

- KEYCLOAK\_PASSWORD=admin

- PROXY\_ADDRESS\_FORWARDING=true

- KEYCLOAK\_EXTRA\_ARGS="-Dkeycloak.profile.feature.scripts=enabled"

ports:

- 6060:8080

- 8443:8443

- 443:443 # change port if any

depends\_on:

- postgres

* *Now execute “docker-compose up -d” command to create both postgresql and keycloak containers with the latest changes. Now we will have the entire data of keycloak inside “/opt/keycloak/data” folder.*

***Note:***

*1. After creating both containers check logs of keycloak container to verify the changes.*

***II. Procedure for exporting and importing the realms:***

* *Create “keycloak-export.sh” file in the server where keycloak container is running with below content by replacing realm name and JSON\_EXPORT\_FILE name.*

# docker-exec-cmd.sh

set -o errexit

set -o errtrace

set -o nounset

set -o pipefail

# If something goes wrong, this script does not run forever, but times out

TIMEOUT\_SECONDS=300

# Logfile for the keycloak export instance

LOGFILE=/tmp/standalone.sh.log

# destionation export file

JSON\_EXPORT\_FILE=/tmp/realms-export-single-file.json

# Remove files from old backups inside the container

# You could also move the files or change the name with timestamp prefix

rm -f ${LOGFILE} ${JSON\_EXPORT\_FILE}

# Start a new keycloak instance with exporting options enabled.

# Use the port offset argument to prevent port conflicts

# with the "real" keycloak instance.

timeout ${TIMEOUT\_SECONDS}s \

/opt/jboss/keycloak/bin/standalone.sh \

-Dkeycloak.migration.action=export \

-Dkeycloak.migration.provider=singleFile \

-Dkeycloak.migration.file=${JSON\_EXPORT\_FILE} \

-Djboss.socket.binding.port-offset=99 \

-Dkeycloak.migration.realmName=<realm name> \

> ${LOGFILE} &

# Grab the keycloak export instance process id

PID="${!}"

# Wait for the export to finish

# It will wait till it sees the string, which indicates

# a successful finished backup.

# If it will take too long (>TIMEOUT\_SECONDS), it will be stopped.

timeout ${TIMEOUT\_SECONDS}s \

grep -m 1 "Export finished successfully" <(tail -f ${LOGFILE})

# Stop the keycloak export instance

kill ${PID}

* *Copy this keycloak-export.sh file inside the container under /tmp folder using below command.*

***“*docker cp *keycloak-export.sh* keycloak:/tmp/*keycloak-export.sh”***

* *Now run shell script inside the container using below command.*

***“*docker exec -it keycloak /tmp/*keycloak-export.sh”***

* *The above command will create json file inside /tmp folder of the container with the name you given for JSON\_EXPORT\_FILE in shell script file.*
* *Copy that file to outside of the container using below command.*

**“docker cp keycloak:/tmp/<json file name> <destination folder>”**

* *If you are able to execute the above steps without any errors,the realm export will be successful.*
* *Now to import this realm to another container which is already created,we will follow the below steps.*
* *At first,Copy the json file to inside the container under /tmp folder using below command.*

**“docker cp <json file path> keycloak:/tmp”**

* *Now,execute the below command inside the running container to import the realm.*

*“***/opt/jboss/keycloak/bin/standalone.sh -Dkeycloak.migration.action=import -Dkeycloak.migration.provider=singleFile -Dkeycloak.migration.file=<realm name> -Dkeycloak.migration.strategy=IGNORE\_EXISTING -Djboss.socket.binding.port-offset=100 -Dkeycloak.migration.realmName=<realm name> -Dkeycloak.profile.feature.upload\_scripts=enabled”**

* At last,restart the container to apply the changes you made using below command.

**“docker restart keycloak”**

**------------------------ THE END -------------------------**