**Setup KeyCloak Server in Ubuntu22**

Follow the steps below to install KeyCloak server on Ubuntu22.

* **Create a directory on gateway**

mkdir -p /home/Collab8/keycloak

cd /home/Collab8/keycloak

* **Install java on gateway** (if available then skip this step):

wget <https://download.oracle.com/java/23/latest/jdk-23_linux-x64_bin.tar.gz>tar -xzf jdk-23\_linux-x64\_bin.tar.gz  
sudo mv jdk-23.0.2 /opt/java  
export JAVA\_HOME=/opt/java/jdk-23.0.2  
export PATH=$JAVA\_HOME/bin:$PATH  
java –version

After above commands java will be installed successfully for the next steps

* **Install KeyCloak on gateway:**

wget <https://github.com/keycloak/keycloak/releases/download/26.1.1/keycloak-26.1.1.zip>   
unzip keycloak-26.1.1.zip  
cd keycloak-26.1.1  
sudo chmod +x bin/\*.sh  
cd bin  
export KC\_BOOTSTRAP\_ADMIN\_USERNAME=admin  
export KC\_BOOTSTRAP\_ADMIN\_PASSWORD=admin  
./kc.sh build  
./kc.sh start-dev

After the above command keyCloak server will be start and we can access by http://<gateway\_ip>:8080 URL.

* **Run keyCloak Server on Startup (Optional):**

Create start\_kc.sh file inside /home/Collab8/keycloak/ and paste the below code

#!/bin/bash

export JAVA\_HOME=/opt/java/jdk-23.0.2

export PATH=$JAVA\_HOME/bin:$PATH

export KC\_BOOTSTRAP\_ADMIN\_USERNAME=admin

export KC\_BOOTSTRAP\_ADMIN\_PASSWORD=admin

/home/Collab8/keycloak/keycloak-26.1.1/bin/kc.sh start-dev

Then, edit /home/Collab8/StartVinager.sh file and add below line at bottom

/home/Collab8/keycloak/kstart.sh

* **Login credentials of KeyCloak Server:**

As per the setup the default login and password of KeyCloak server.

**Username:** admin

**Password:** admin

After login you can change the password or create users with different roles.

* **Configure AD server with KeyCloak:**
* Go to the Admin Console:
* Select your realm (e.g., master).
* Navigate to User Federation.
* Click **"Add Provider"** → Select **"LDAP"**.

Fill in the below LDAP Configuration

|  |  |
| --- | --- |
| **Fields** | **Value** |
| Vendor | Active Directory |
| Connection URL | ldap://kramerindia-ad.local |
| Bind type | simple |
| Bind DN | Administrator@kramerindia-ad.local |
| Bind credentials | A!s1d1f1 |
| Edit mode | READ\_ONLY |
| Users DN | dc=kramerindia-ad,dc=local |
| Username LDAP attribute | sAMAccountName |
| RDN LDAP attribute | sAMAccountName |
| UUID LDAP attribute | objectGUID |
| User object classes | person, organizationalPerson, user, top |
| Search scope | subtree |

* After filling in the above info click Test authentication button to verify the AD server credentials.
* If a success message comes then click on the Save button.
* Now, navigate to the **Users** section you can see all the users of AD server are showing.
* **Login AD users using KeyCloak:**

$keycloak\_url = <http://172.30.92.108:8080>;

*// This is the server base URL.*

$realm = "master";

*// realm name*

$client\_id = "account";

*// Client\_id get from Clients section module.*

$redirect\_uri = <https://172.30.92.108/keyclock/test/callback.php>;  
*// After authentication you will be redirected here with authorization code.*  
*This URL should be added in Clients > click on account > navigate to* ***Valid redirect URIs option.***

$auth\_url = "{$keycloak\_url}/realms/{$realm}/protocol/openid-connect/auth?client\_id={$client\_id}&response\_type=code&scope=openid email profile&redirect\_uri=".urlencode($redirect\_uri);

Header(“Location:”. $auth\_url);

This is the complete URL where user will be redirected when trying to login.

Now redirect to the $auth\_url URL for the authentication. Once you authenticate, you will get an authentication code, and by the authentication code, you will get the access token and other info as per the requirement. For more info, see the implemented code <\\172.30.92.34\media\Niraj\test-keycloak-login>