

Sécurité des systèmes distribués Oauth2 OIDC

Keycloak

1. Télécharger Keycloak

Dans ce TP je vais utiliser docker et docker compose

Etape 1 : J'ai créé dans cette étape un fichier docker « dockerfile » afin de créer une image docker pour utiliser keycloak en mode dev :

Dockerfile :

```
FROM quay.io/keycloak/keycloak:latest as builder

# Enable health and metrics support
ENV KC_HEALTH_ENABLED=true
ENV KC_METRICS_ENABLED=true

# Configure a database vendor
ENV KC_DB=postgres

WORKDIR /opt/keycloak
# for demonstration purposes only, please make sure to use proper certificates
in production instead
RUN keytool -genkeypair -storepass password -storetype PKCS12 -keyalg RSA -
keysize 2048 -dname "CN=server" -alias server -ext
"SAN:c=DNS:localhost,IP:127.0.0.1" -keystore conf/server.keystore
RUN /opt/keycloak/bin/kc.sh build

FROM quay.io/keycloak/keycloak:latest
COPY --from=builder /opt/keycloak/ /opt/keycloak/

# change these values to point to a running postgres instance
ENV KC_HOSTNAME=localhost
ENTRYPOINT ["/opt/keycloak/bin/kc.sh", "start-dev"]
```

Etape 2: Dans cette étape j'ai ajouté un fichier docker compose pour démarrer l'instance de keycloak

Docker-compose.yml :

```
version: '3.7'

services:
  keycloak:
    image: keycloak
```

```

container_name: keycloak
environment:
  KC_BOOTSTRAP_ADMIN_USERNAME: # ...admin-username
  KC_BOOTSTRAP_ADMIN_PASSWORD: # ...admin-password
ports:
  - "8080:8080"
networks:
  - keycloak-network
volumes:
  - ./keycloak-data:/opt/keycloak/data
  - ./keycloak-themes:/opt/keycloak/themes

networks:
  keycloak-network:
    driver: bridge

```

2. Démarrer Keycloak

Pour démarrer keycloak en mode dev on utilise la commande « docker-compose up -d »

```

PS C:\Users\pc\Documents\ENSET GLSID\S5\MS\keycloak> docker-compose up -d
time="2024-11-30T18:55:49+01:00" level=warning msg="C:\\Users\\pc\\Documents\\ENSET GLSID\\S5\\MS\\keycloak\\docker-compose.yml: the attribute `version` is obsolete, it will be ignored, please remove it to avoid potential confusion"
[+] Running 1/1
  ✓ Container keycloak Started                                0.9s
PS C:\Users\pc\Documents\ENSET GLSID\S5\MS\keycloak> docker ps
CONTAINER ID   IMAGE      COMMAND                  CREATED        STATUS        PORTS
2aaaca8330ec   keycloak   "/opt/keycloak/bin/k..." 6 seconds ago  Up 5 seconds  8443/tcp, 0.0.0.0:8080->8080/tcp, 9000/tcp   keycloak
PS C:\Users\pc\Documents\ENSET GLSID\S5\MS\keycloak> docker ps
CONTAINER ID   IMAGE      COMMAND                  CREATED        STATUS        PORTS
2aaaca8330ec   keycloak   "/opt/keycloak/bin/k..." 51 seconds ago  Up 51 seconds  8443/tcp, 0.0.0.0:8080->8080/tcp, 9000/tcp   keycloak
PS C:\Users\pc\Documents\ENSET GLSID\S5\MS\keycloak> docker logs keycloak
Updating the configuration and installing your custom providers, if any. Please wait.
2024-11-30 17:56:10,823 INFO [io.qua.dep.QuarkusAugmentor] (main) Quarkus augmentation completed in 16275ms
2024-11-30 17:56:14,706 INFO [org.keycloak.url.HostnameV2ProviderFactory] (main) If hostname is specified, hostname-strict is effectively ignored
2024-11-30 17:56:19,454 INFO [org.keycloak.quarkus.runtime.storage.infinispan.CacheManagerFactory] (main) Starting Infinispan embedded cache manager
2024-11-30 17:56:19,837 INFO [org.keycloak.quarkus.runtime.storage.infinispan.CacheManagerFactory] (main) Persistent user sessions enabled and no memory limit found in configuration. Setting max entries for sessions to 10000 entries.
2024-11-30 17:56:19,838 INFO [org.keycloak.quarkus.runtime.storage.infinispan.CacheManagerFactory] (main) Persistent user sessions enabled and no memory limit found in configuration. Setting max entries for clientSessions to 10000 entries.

```

3. Créer un compte Admin

Le compte admin est déjà précisé à travers les variables d'environnement dans le fichier docker compose mais c'est un compte temporaire. Donc en crée un compte admin permanent :

Users > Create user

Create user

Required user actions

Select action



Email verified



Off

General

Jump to section

Username *

ahmed

Email

Email

General

Create

Cancel

Users > User details

ahmed



Enabled

Action



De

Set password for ahmed



Password *

.....



Password confirmation *

.....



Temporary



On

Save

Cancel

Set password

Users > User details

ahmed



Enabled

Action



Details

Credentials

Role mapping

Groups

Consents

Identity provider links

Sessions

Search by name



Hide inherited roles

Assign role

Unassign

Refresh

1-2



Name

Inherited

Description



default-roles-master

False

role_default-roles



admin

False

role_admin



4. Créer une Realm

Create realm

A realm manages a set of users, credentials, roles, and groups. A user belongs to and logs into a realm. Realms are isolated from one another and can only manage and authenticate the users that they control.

Resource file

Drag a file here or browse to upload

Browse...Clear

1

Upload a JSON file

Realm name *

wallet-realm

Enabled

☒ On

5. Créer un client à sécuriser

Clients > Create client

Create client

Clients are applications and services that can request authentication of a user.

1 General settings

2 Capability config

3 Login settings

Client type ?

OpenID Connect

Client ID * ?

wallet-client

Name ?

Description ?

Always display in UI ?

☐ Off

Home URL ?

http://localhost:4200/

Valid redirect URIs ?

http://localhost:4200/*

+ Add valid redirect URIs

Valid post logout redirect URIs ?

http://localhost:4200/

+ Add valid post logout redirect URIs

Web origins ?

*

+ Add web origins

6. Créer des utilisateurs

Create user

Required user actions ?

Select action

Email verified ?

Off

General

Username *

ahmed.mrabet

Email

ahmed.mrabet@gmail.com

Jump to section

General

Create **Cancel**

Users

Users are the users in the current realm. [Learn more](#)

User list

Default search Search user Add user Delete user Refresh

1-2

<input type="checkbox"/>	Username	Email	Last name	First name	
<input type="checkbox"/>	ahmed.mrabet	ahmed.mrabet@gmail.com	—	—	⋮
<input type="checkbox"/>	elalami	elalami@gmail.com	—	—	⋮

1-2

7. Créer des rôles

Realm roles

Realm roles are the roles that you define for use in the current realm. [Learn more](#)

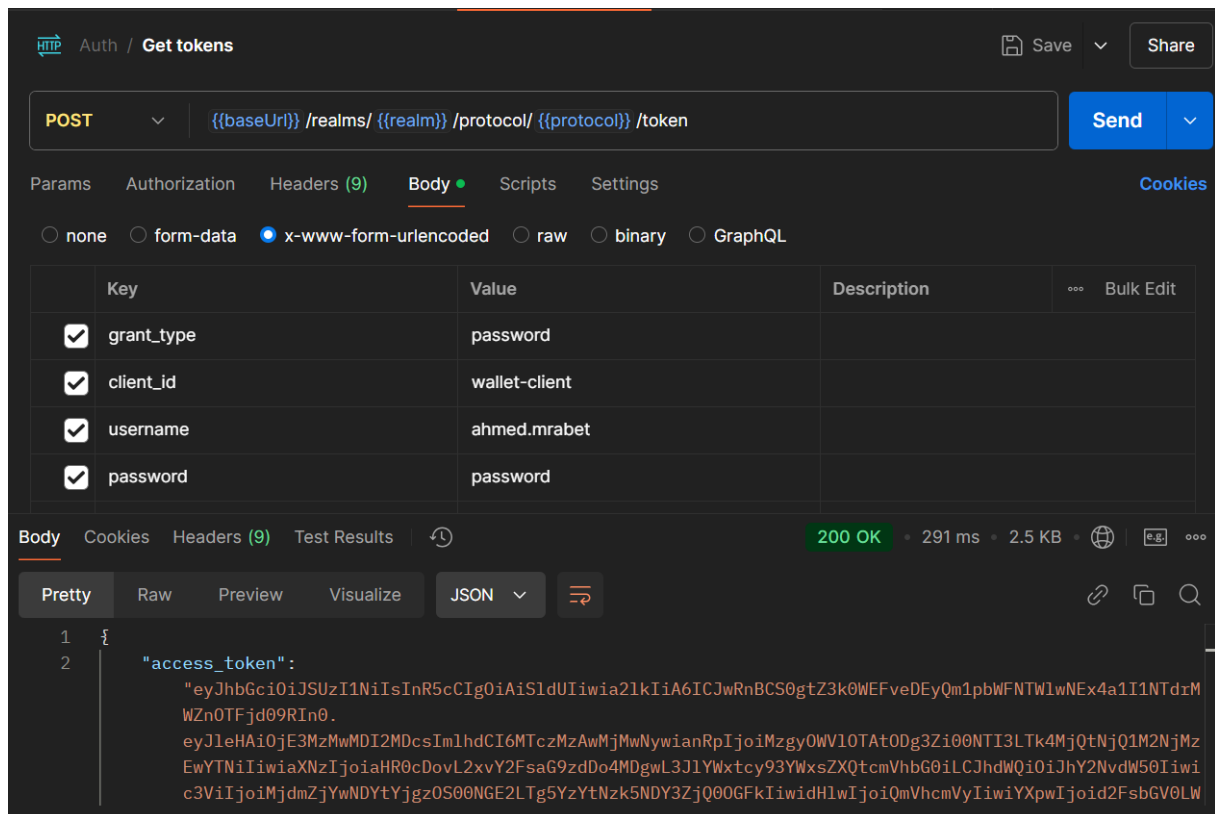
Search role by name Create role Refresh

1-5

Role name	Composite	Description	
ADMIN	False	—	⋮
USER	False	—	⋮
default-roles-wallet-realm	True	role_default-roles	⋮
offline_access	False	role_offline-access	⋮
uma_authorization	False	role_uma_authorization	⋮

1-5

8. Affecter les rôles aux utilisateurs



- Analyser les contenus des deux JWT Access Token et Refresh Token

Access Token :

L'algorithme utiliser c'est : RS256

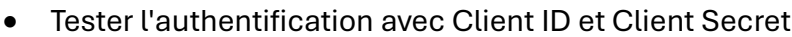
Le payload contient les informations sur le token (ex. temps d'expirations, date de création...) en plus des informations sur l'utilisateur tel que les rôles, nom, prénom, email...

Refresh Token :

L'algorithme utiliser c'est : HS512

Elle ne contient pas les informations sur l'utilisateur.

- Tester l'authentification avec le Refresh Token



Capability config

Client authentication

On

?

Authorization

Off

?

Authentication flow

Standard flow

Direct access grants

Implicit flow

OAuth 2.0 Device Authorization Grant

?

Capability config

Login settings

Logout settings

[illegible]