

Keycloak Authorization 서버 설정

Keycloak, JWT 기반 OAuth2 책임의 분산 (1/3) : 마이크로서비스와 OAuth2 구성요소인 Authorization Server/ Client/ Resource Server 를 활용해 Single Sign-On 구현 모형을 실습한다. OAuth2 에서 Authorization Server 로 Keycloak 을 설치하고 설정하는 방법을 간단하게 실습한다.

Instruction

Keycloak 기반 OAuth2 - Authorization Svr

OAuth2 Stackholders

- Gateway 를 OAuth2 Client 로, 주문 마이크로서비스를 Resource Server 로 설정한다.
- Keycloak 서버를 설치하고 접속하여 기본설정과 사용할 User 를 등록한다.
- OAuth2 의 Grant type 을 'authorization_code'를 적용한다.
- Platform 에서 작업이 원활하지 않을 경우, Local 에서 수행한다.

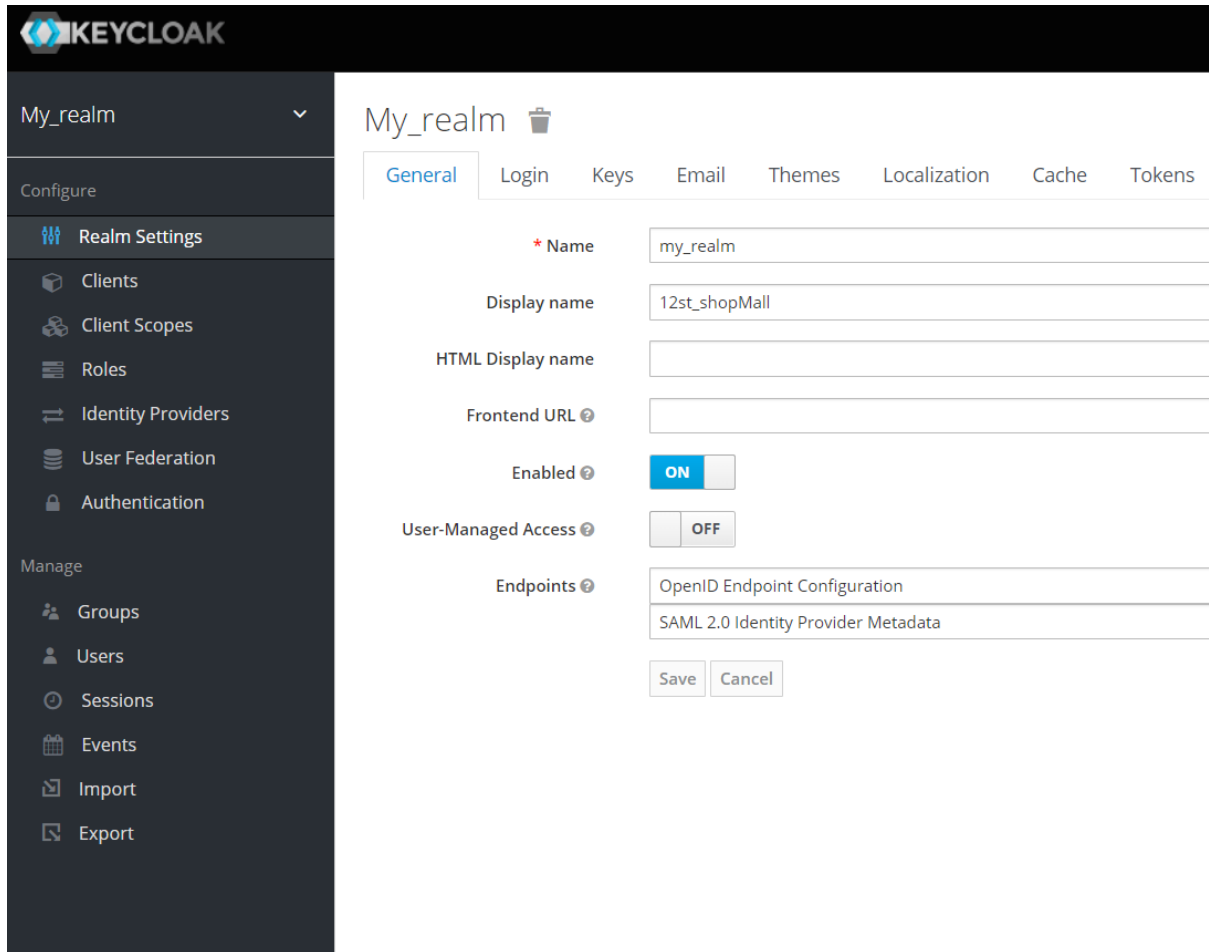
Local 머신에 IDE(IntelliJ, VSCode)와 JDK 11 이상이 설치되어 있어야 한다.

Keycloak 시작

- Redhat 이 만든 Keycloak 서버는 8080 포트를 기본 사용한다.
- bin 폴더 하위에 OS 에 맞는 Script 를 실행한다.

```
cd keycloak/bin
chmod 744 ./kc.sh
./kc.sh start-dev
```

- 웹브라우저에서 Keycloak 관리콘솔(<http://localhost:8080/>)에 접속한다.
- 관리자 계정이 (admin/admin)으로 등록되어 있다.
- 'Administration Console'을 눌러 콘솔로 진입한다.



Keycloak 설정

- **Realm** 추가
- 'test-realm' 이름으로 **Root** 관리단위인 **Realm** 을 추가한다.
- 추가된 **Realm** 에서 **Token** 의 **Lifespan** 을 1 시간으로 조정한다.
- **Client** 등록
- 왼쪽 메뉴 **Client** 를 눌러, **Realm** 범주의 **Client** 를 추가한다.
- 'test-client' 이름으로 **OAuth2 CLIENT** 를 등록한다.

Root URL: <http://localhost:8080>

- 'Save'를 눌러 저장한다.
- **Client** 의 **OAuth2** 설정을 추가한다.

Redirect URI: <http://localhost:8088/login/oauth2/code/keycloak>

Access Type: public 에서 confidential 로 설정


OAuth2 의 “Client Credentials” 타입이 활성화된다.

| | |
|------------------------------------------------|---------------------------------------------------------------------------------|
| Access Type ? | <input type="text" value="confidential"/> |
| Standard Flow Enabled ? | <input checked="" type="checkbox"/> ON |
| Implicit Flow Enabled ? | <input type="checkbox"/> OFF |
| Direct Access Grants Enabled ? | <input checked="" type="checkbox"/> ON |
| Service Accounts Enabled ? | <input type="checkbox"/> OFF |
| OAuth 2.0 Device Authorization Grant Enabled ? | <input type="checkbox"/> OFF |
| OIDC CIBA Grant Enabled ? | <input type="checkbox"/> OFF |
| Authorization Enabled ? | <input type="checkbox"/> OFF |
| Front Channel Logout ? | <input type="checkbox"/> OFF |
| Root URL ? | <input type="text" value="http://localhost:8080"/> |
| * Valid Redirect URIs ? | <input type="text" value="http://localhost:8088/login/oauth2/code/keycloak"/> + |


- ‘Save’를 눌러 저장한다.
- ‘Credentials’ 탭을 눌러, Client 의 Secret 정보가 발급됨을 확인한다.

권한(Role) 및 사용자 설정

- ‘Roles’ 탭을 눌러 Client 의 Local Role 을 추가한다.

Test_client 

Settings Credentials Keys **Roles**



No client roles available

- 아래 목록처럼 나타나도록 **Role** 이름을 부여한다.

| Search... | Q | View all roles |
|----------------|-----------|----------------|
| Role Name | Composite | Description |
| DELIVERY_ADMIN | False | DELIVERY_ADMIN |
| ORDER_ADMIN | False | ORDER_ADMIN |
| ORDER_CUSTOMER | False | ORDER_CUSTOMER |
| PRODUCT_ADMIN | False | PRODUCT_ADMIN |

- 왼쪽 메뉴에서 **Users** 를 눌러 사용자를 등록한다.

사용자 정보는 **Custom** 하게 생성해 본다. (**User** 와 **Admin** 계정포함)

Add user

| | |
|-------------------------|------------------------------------------------------------------------------------|
| ID | <input type="text"/> |
| Created At | |
| Username * | <input type="text" value="user@uengine.org"/> |
| Email | <input type="text"/> |
| First Name | <input type="text" value="GilDong"/> |
| Last Name | <input type="text" value="Hong"/> |
| User Enabled ? | <input checked="" type="checkbox"/> ON |
| Email Verified ? | <input type="checkbox"/> OFF |
| Groups ? | <input type="text" value="Select existing group..."/> <div>No group selected</div> |
| Required User Actions ? | <input type="text" value="Select an action..."/> |
| | <input type="button" value="Save"/> <input type="button" value="Cancel"/> |

- 등록 후, **Credentials** 탭에서 비밀번호를 등록하는데 이때, **Temporary** 를 **Off** 로 설정한다.

User@uengine.org 

Details Attributes **Credentials** Role Mappings Groups Consents Sessions

Manage Credentials

| Position | Type | User Label | Data |
|----------|------|------------|------|
|----------|------|------------|------|

Set Password

Password

Password Confirmation

Temporary ☐ OFF

- User 등록이 끝나면, Role 과 사용자를 매핑한다.
- 등록된 사용자 각각에서 'Role Mappings' 탭을 눌러 Client 의 Local Role 을 선택해 준다.

User@uengine.org 

Details Attributes Credentials **Role Mappings** Groups Consents Sessions

| | | | |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| Realm Roles | <div>Available Roles ⓘ offline_access uma_authorization <input type="button" value="Add selected >"/></div> | <div>Assigned Roles ⓘ default-roles-test_realm <input type="button" value="« Remove selected"/></div> | <div>Effective Roles ⓘ default-roles-test_realm offline_access uma_authorization</div> |
| Client Roles | <div>test_client</div> <div>Available Roles ⓘ DELIVERY_ADMIN ORDER_ADMIN PRODCUT_ADMIN <input type="button" value="Add selected »"/></div> | <div><input type="button" value="« Remove selected"/></div> <div>Assigned Roles ⓘ ORDER_CUSTOMER <input type="button" value="« Remove selected"/></div> | <div>Effective Roles ⓘ ORDER_CUSTOMER</div> |

User 계정에는 'ORDER_CUSTOMER' 역할 매핑

Admin 계정에는 'ORDER_ADMIN', 'ORDER_CUSTOMER' 역할 매핑

- 이로써, 간단하게 Keycloak 설정을 마무리한다.

CheckPoints

1. 모든 요구사항을 만족하는가 ☐