Produit - GitLab

Contient les procédures et documentations liées à GITLAB

- GITLAB - Configuration SSO Oauth avec keycloak

GITLAB - Configuration SSO Oauth avec keycloak

Difficulté : Confirmé

Notions : Authentification, SSO

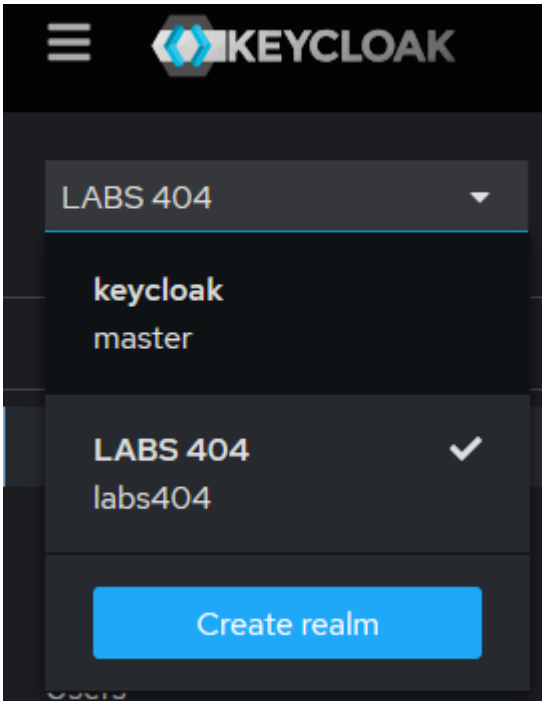
I. Introduction

Cette procédure à pour but d'expliquer le paramétrage de l'authentification SSO de Gitlab avec Keycloak.

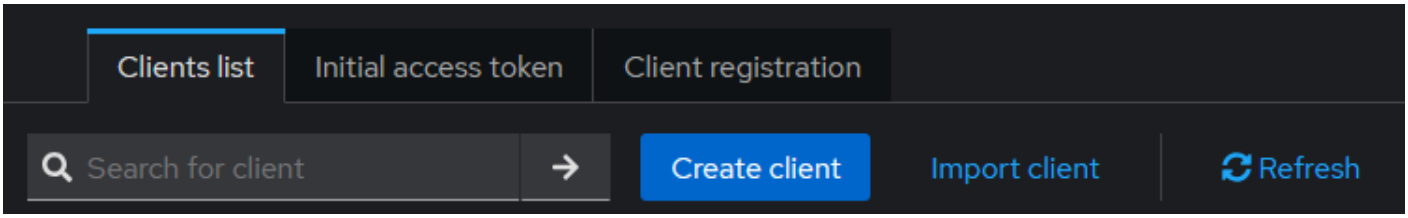
II. Côté Keycloak

2.1 Créer le client

Se connecter au keycloak et choisir le realm sur lequel ajouter le client Gtilab.



Cliquer sur '***Create client***'



Sélectionner le type '***OpenID Connect***'

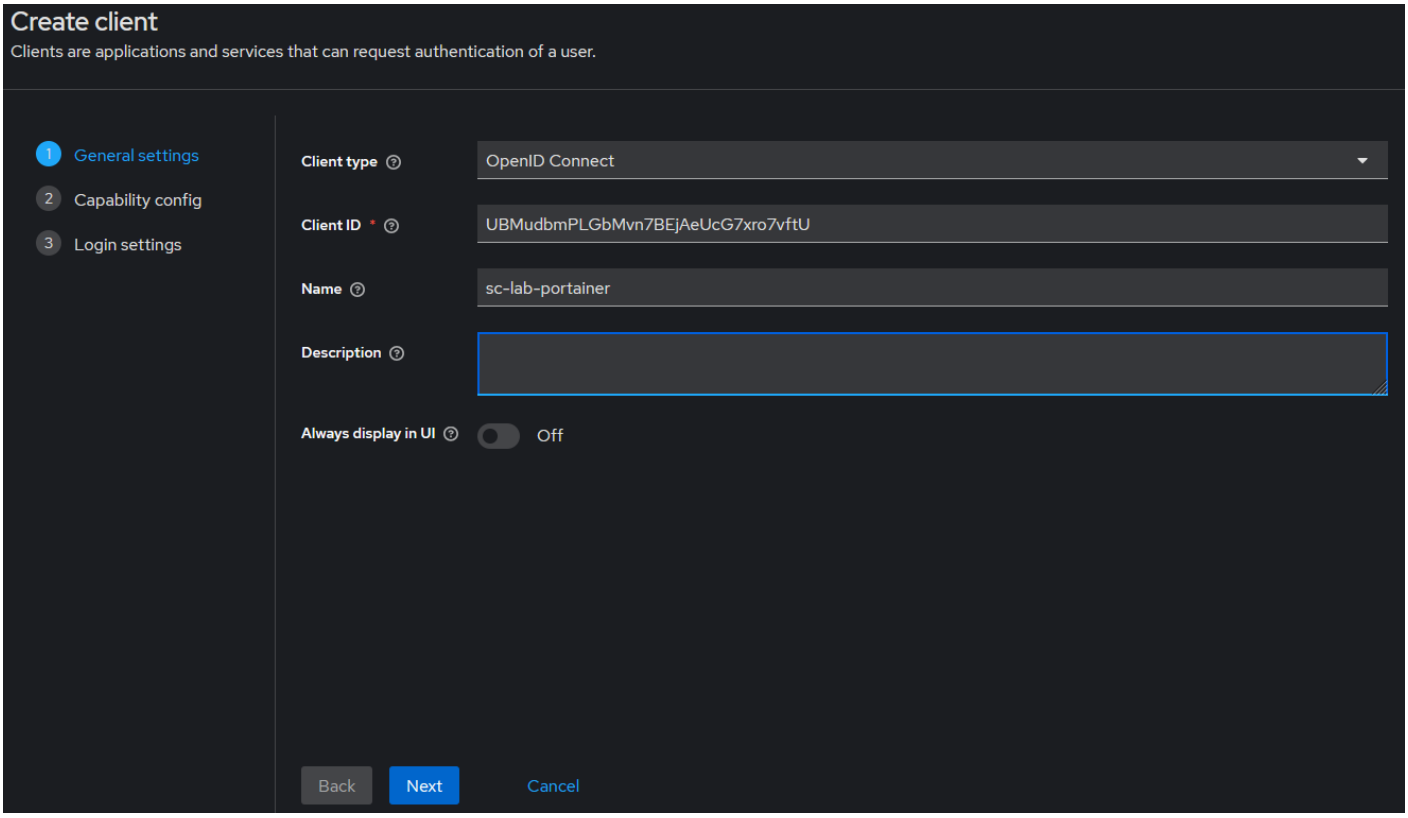
Générer ou définir un '***clientID***'.

> *Il est possible d'utiliser un générateur afin de générer un e chaîne de 32 caractères. Par exemple : ici.*

> **Best Practice** *: 32 caractères avec minuscules, majuscules et chiffres.*

Choisir un nom parlant.

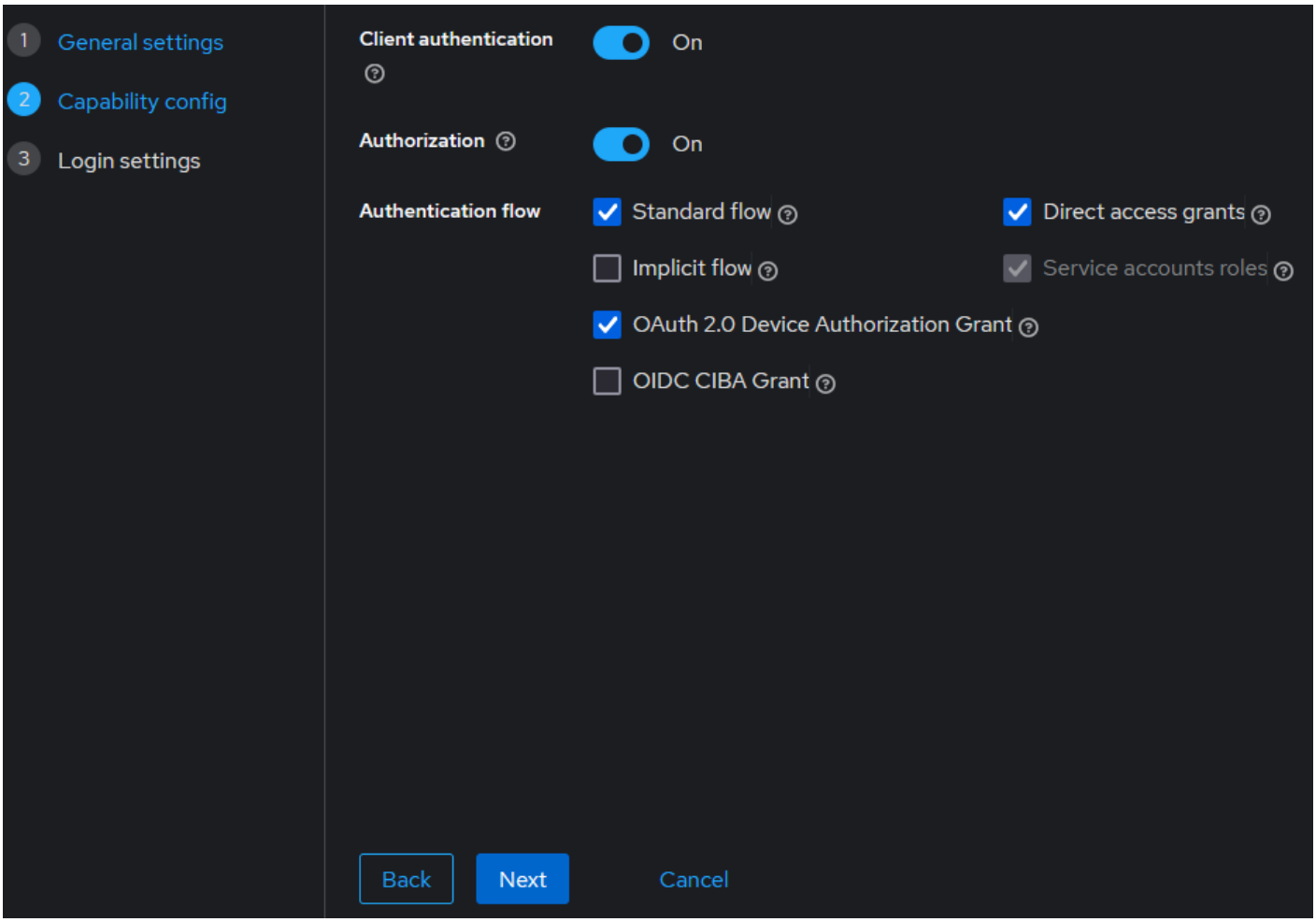
Puis faire '***Next***'.



Sur la page suivante, activer '***Client authentication***' et '***Authorization***'.

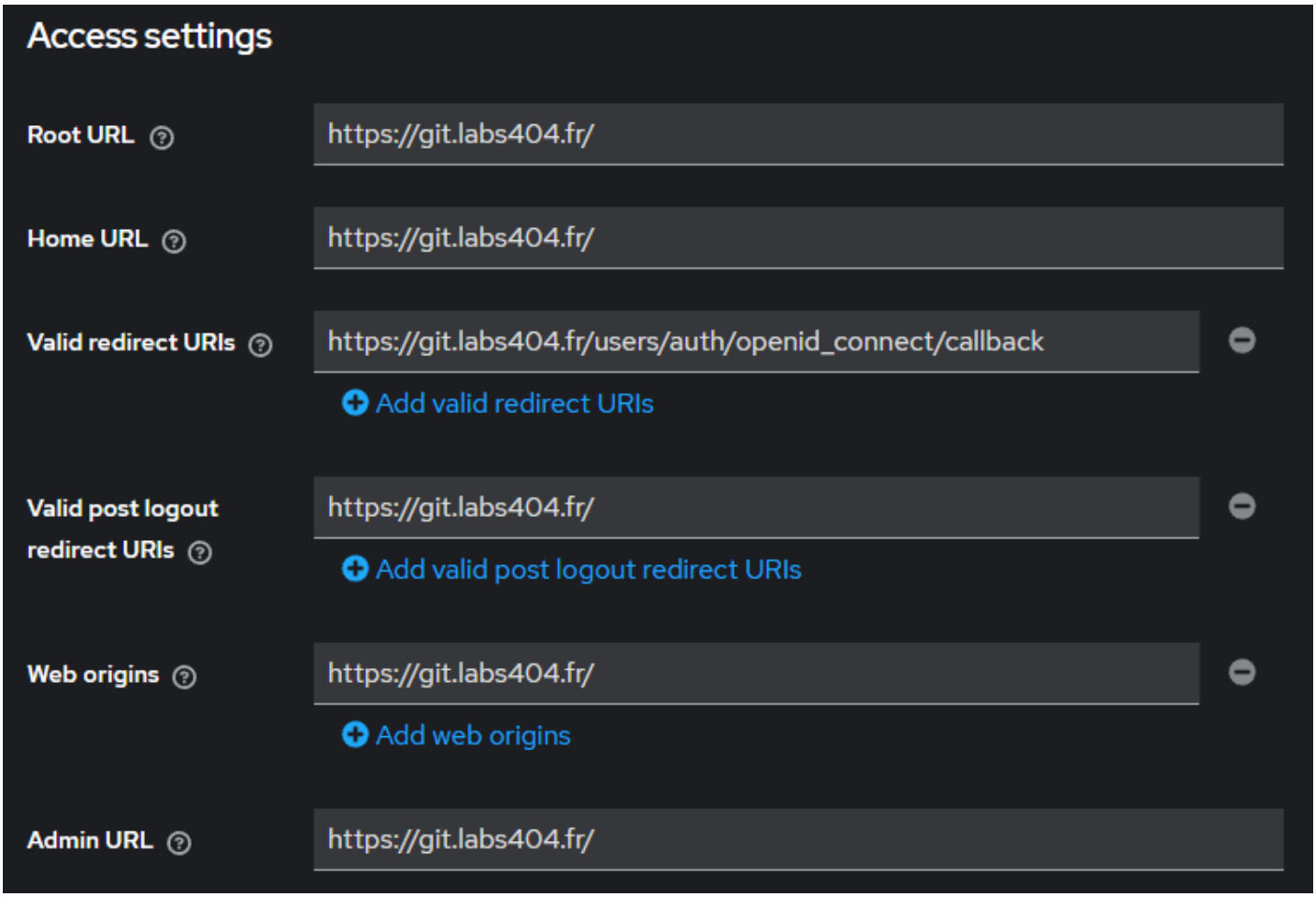
Vérifier que les cases suivantes sont cochées.

Puis faire '***Next***'.



Entrer les URL au format suivant (en modifiant les FQND).

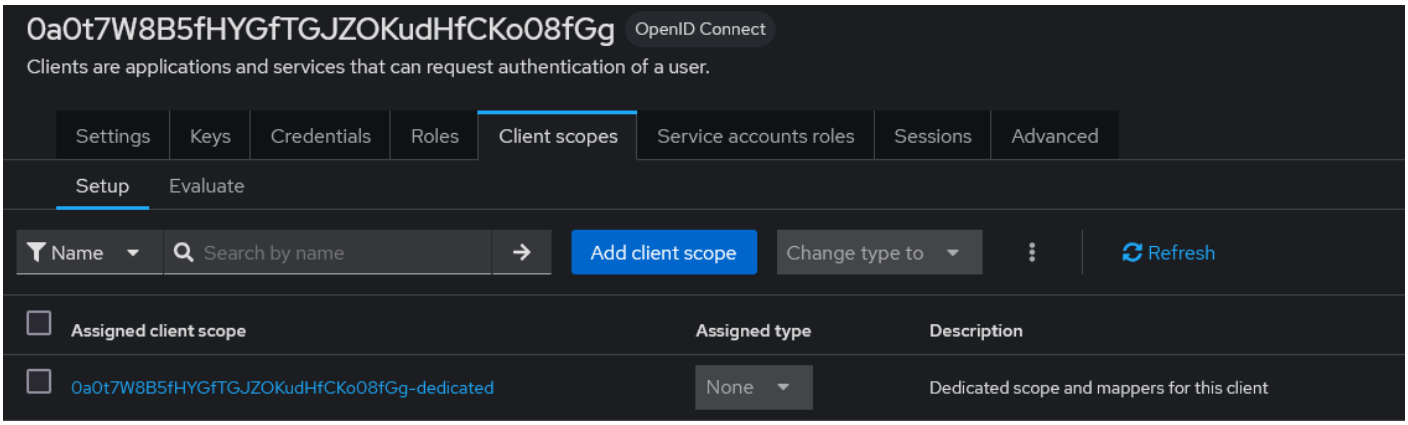
Puis faire '***Save***'.



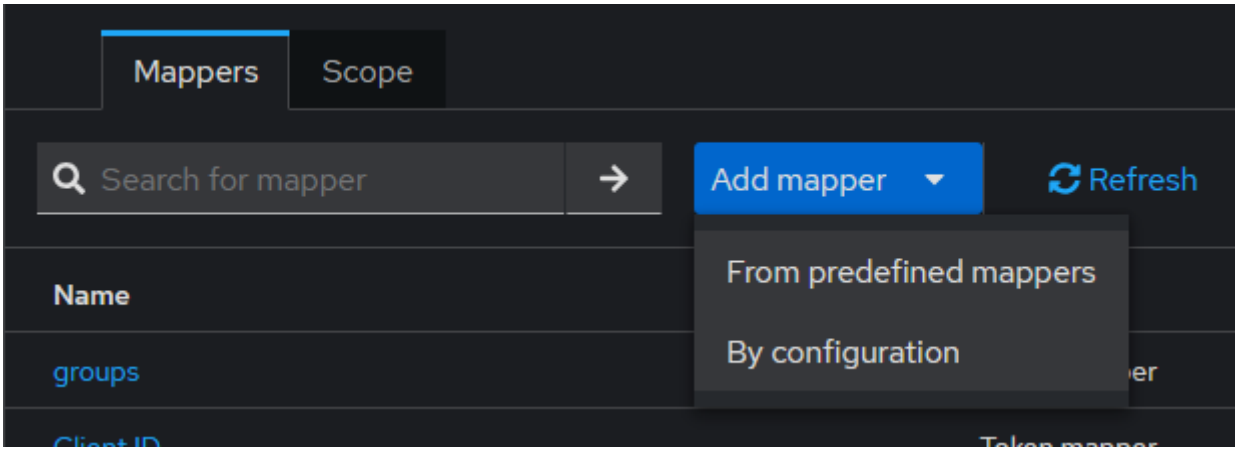
2.2 Préparer la synchro des groupes

Afin de pouvoir gérer les droits depuis le keycloak et synchroniser les groupes, aller dans l'onglet '***Client scope***'.

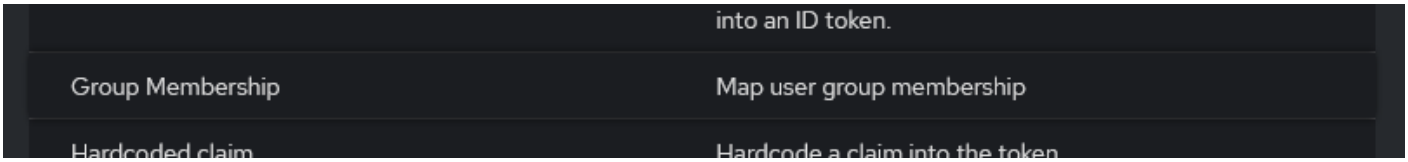
Choisir le client scope au nom du client suivi de '***-dedicated***'.



Faire '***Add Mapper***' puis '***By Configuration***'.



Choisir '***Group Membership***'.

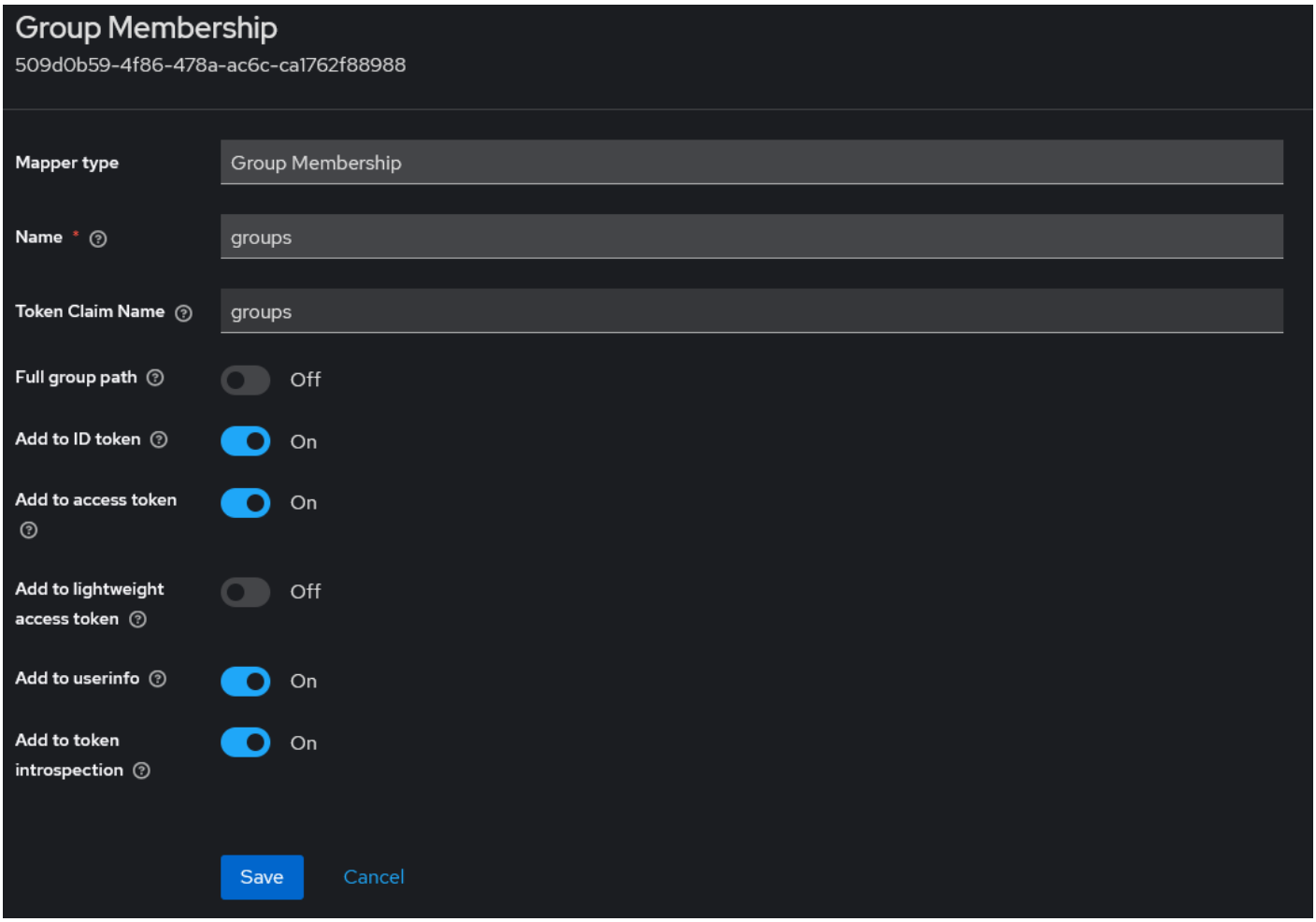


Définir le nom du ***mapper*** en '***groups***'.

Définir le Token ***claim name*** en '***groups***'.

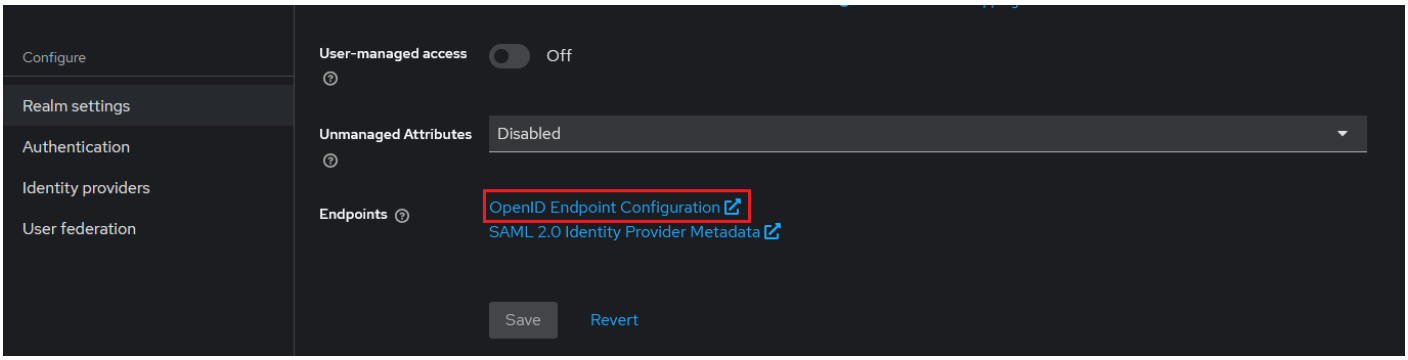
Vérifier que les fonctions suivantes soit activées / désactivées.

Puis faire '***Save***'.

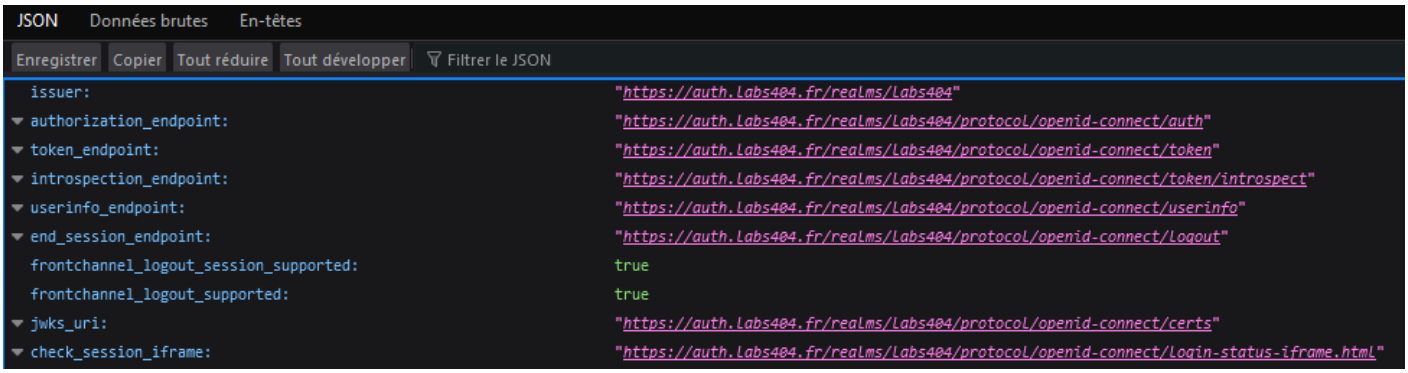


2.3 Récupérer les URL

Pour récupérer les URL, sélectionner le realm et faire '***Realm settings***' puis cliquer sur '***OpenID Endpoint Configuration***'.



Une page s'affiche et permet de récupérer les URL.



II. Côté Gitlab

Se connecter en ***SSH*** dans le container ou serveur / instance booksack.

Modifier le fichier '***/etc/gitlab/gitlab.rb***'

Ajouter le code suivant en modifiant les données nécessaires :

```
gitlab_rails['omniauth_enabled'] =
true
gitlab_rails['omniauth_allow_single_sign_on'] = ['openid_connect']

gitlab_rails['omniauth_providers'] = [
  {
    name: "openid_connect",
    label: "Login with OAuth",
    args: {
      name: "openid_connect",
      scope: ["openid","profile","email"],
      response_type: "code",
      issuer: "https://auth.labs404.fr/realms/LABS404",
      discovery: true,
      client_auth_method: "query",
      uid_field: "preferred_username",
      pkce: true,
      client_options: {
```

```
        identifier: "<Client ID>",
        secret: "<Client Secret>",
        redirect_uri: "https://git.labs404.fr/users/auth/openid_connect/callback",
        gitlab: {
          groups_attribute: "groups",
          admin_groups: ["Admin"]
        }
      }
    }
  }
]
```

Recharger ensuite la configuration avec la commande :

```
gitlab-ctl reconfigure
```