Produit - Keycloak

Contient les procédures liées à la mise en place de keycloak.

- Keycloak - Personnaliser le realm
- Keycloak - Créer un realm fédéré avec Active directory

Keycloak - Personnaliser le realm

Difficulté : Confirmé

Notions : Keycloak, SSO, realm,

I. Introduction

Cette procédure à pour but de présenter les différents aspect de la personnalisation d'un realm.

Allant des options à la personnalisation de la page de login.

II. Personnaliser la page de login

2.1 Changer le logo

2.2 Changer le fond de la page

Keycloak - Créer un realm fédéré avec Active directory

Difficulté : Confirmé

Notions : SSO, LDAP(s), fédération

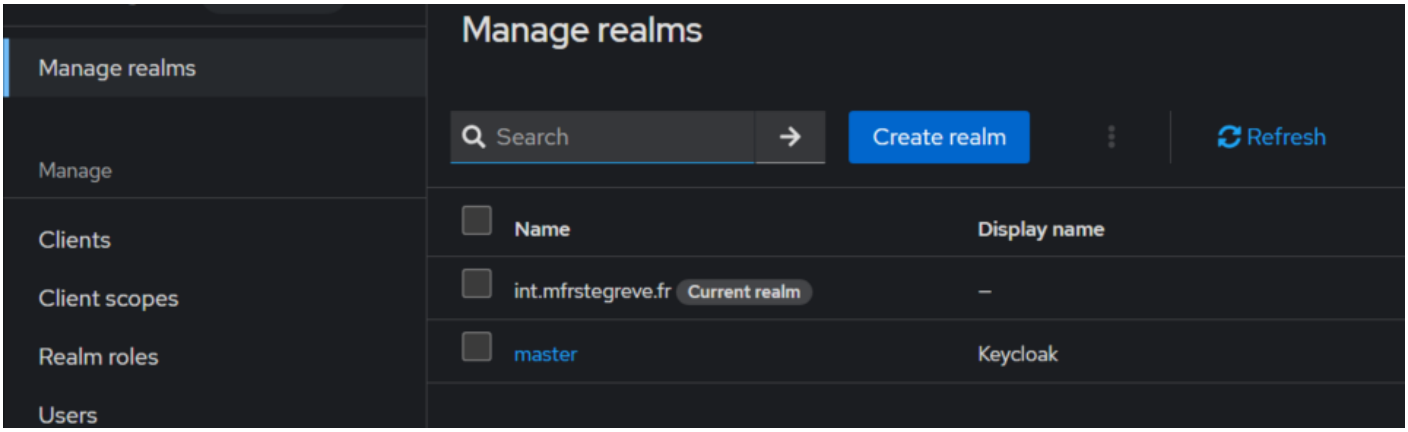
I. Introduction

Cette procédure à pour but de présenter la mise en place d'un realm keycloak pour le SSO avec une fédération active directory pour synchroniser les utilisateurs et les groupes afin de les utiliser après dans les différents environnements pour gérer les autorisations et rôles.

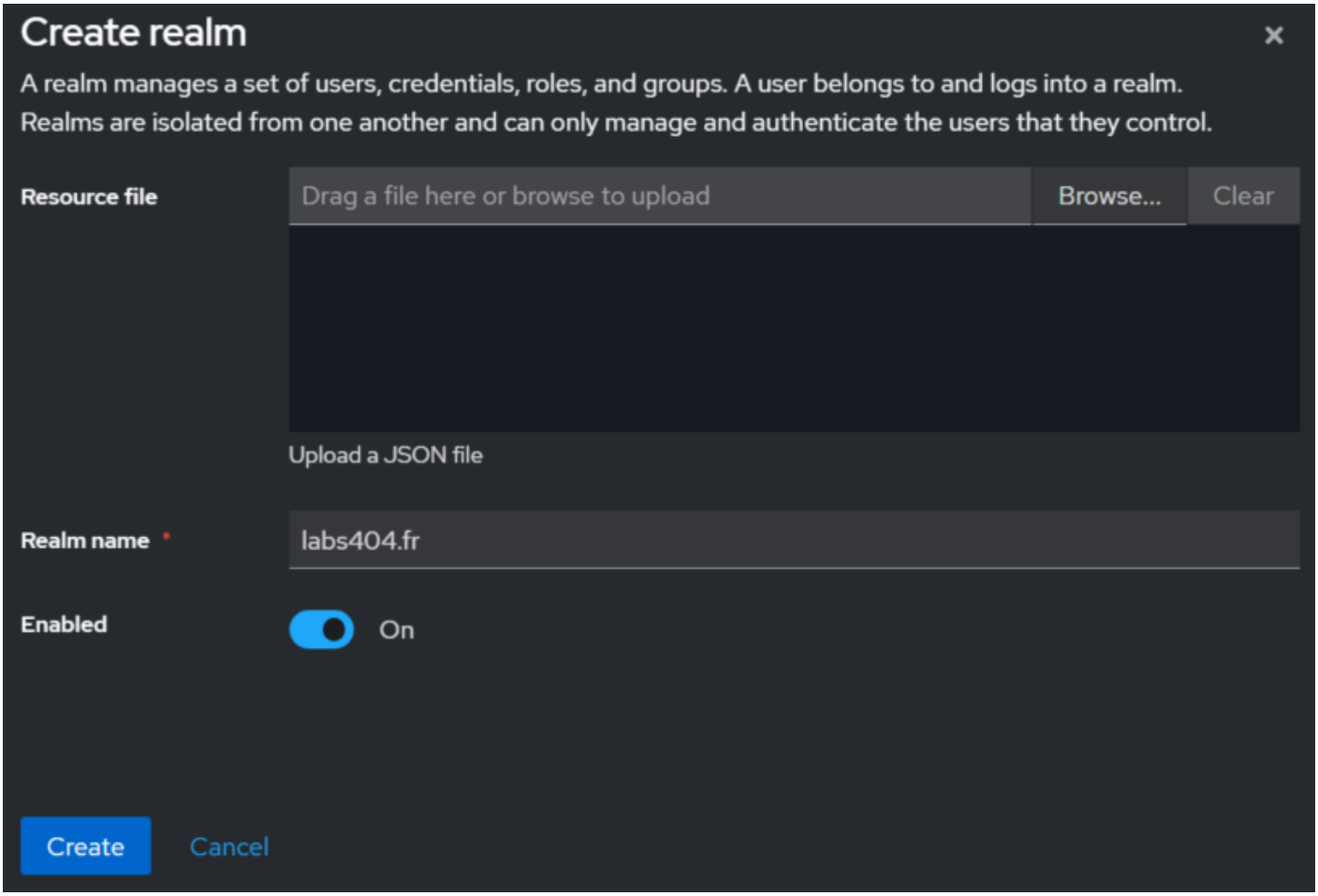
II. Créer le Realm

2.1 Création

Dans l'onglet "***Manage realms***", cliquer sur le bouton "***Create realm***".



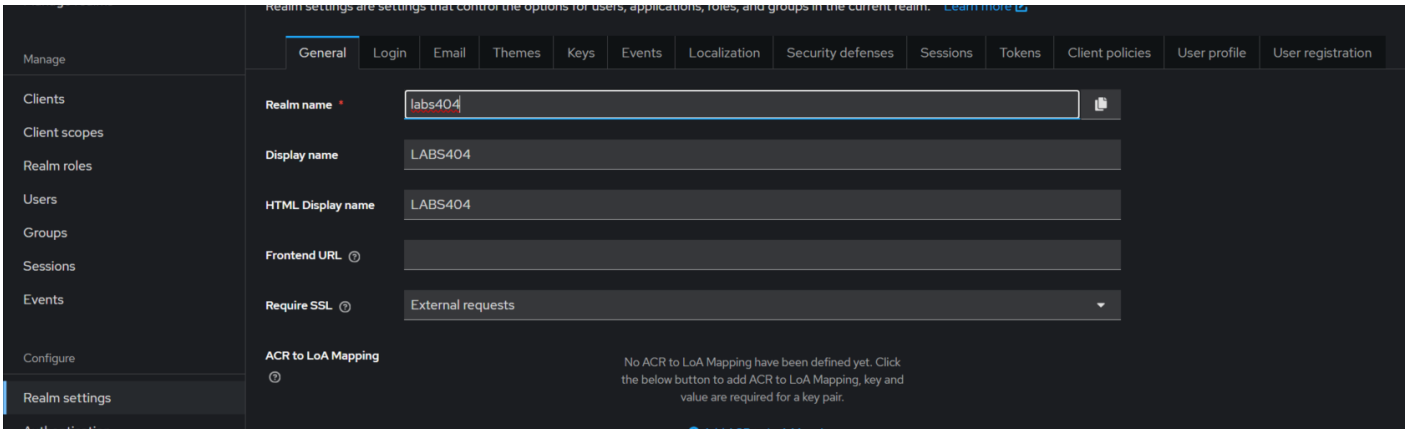
Dans la fenêtre qui s'affiche, entrer le nom du realm puis cliquer sur "***Create***":



2.2 Configuration de base

Dans le menu, aller sur "***Realm settings***".

Modifier le 'Display name' et le 'HTML Display name' Pour pouvoir personnaliser le nom du realm qui apparaîtra à la connexion.

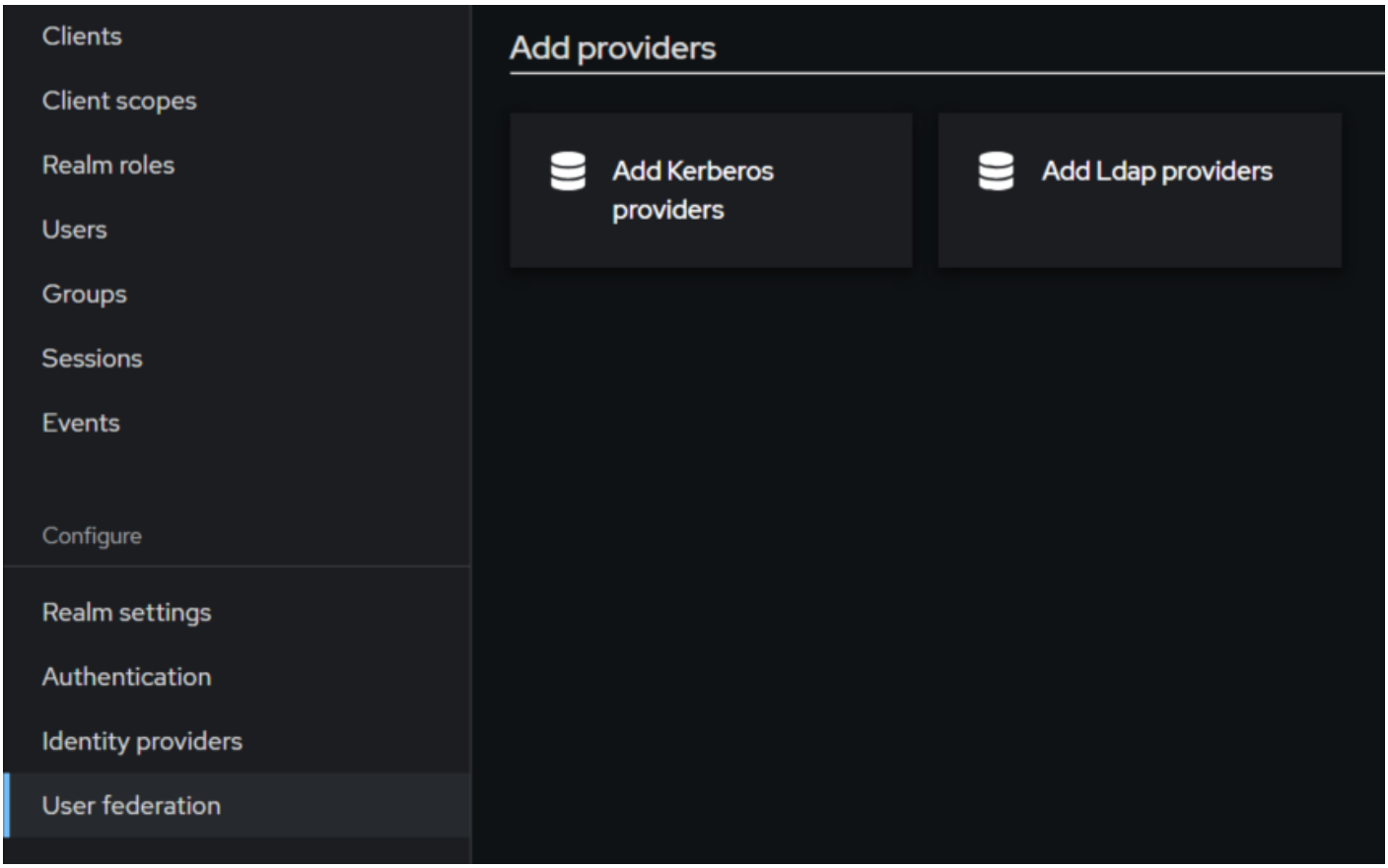


III. Créer la fédération

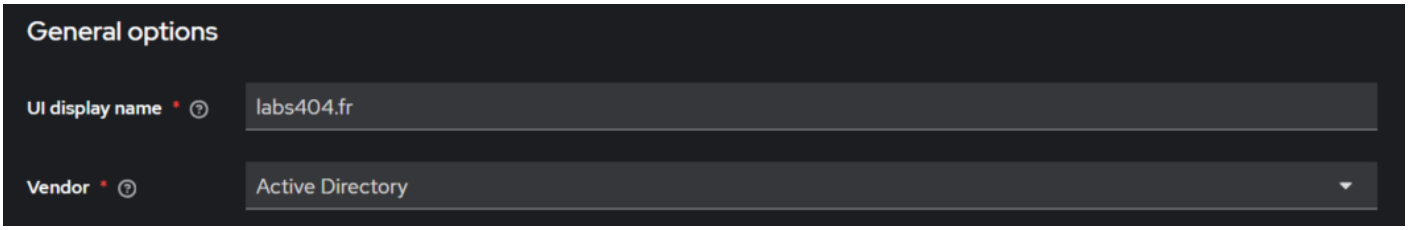
> **Prérequis** : un compte active directory pour le Bind LDAP doit avoir été créé. Les DC doivent être joignables.

> **Attention** : Windows Active Directory 2025 peut poser des problèmes pour les liasions LDAP. En cas de problème, Voir ici : KB-Active directory - windows 2025 bind ldap(s)

Dans le menu, aller sur "***User federation***" puis faire "***Add Ldap providers***".

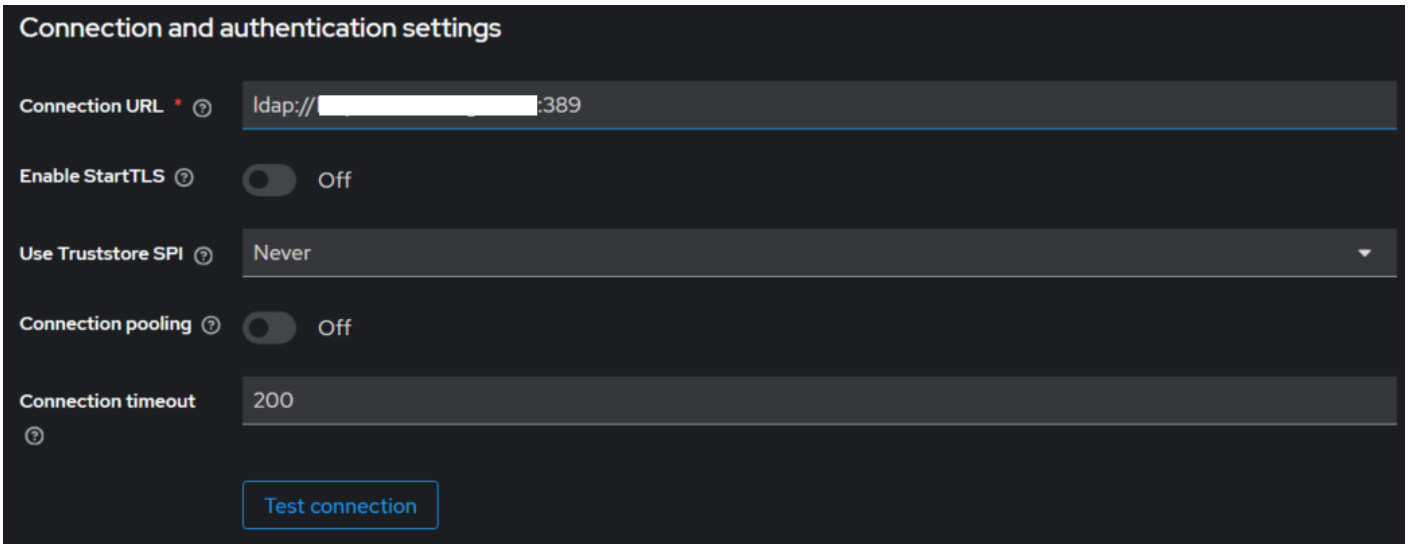


Dans les General options, définir le nom du realm et choisir le Vendor '***Active Directory***'.



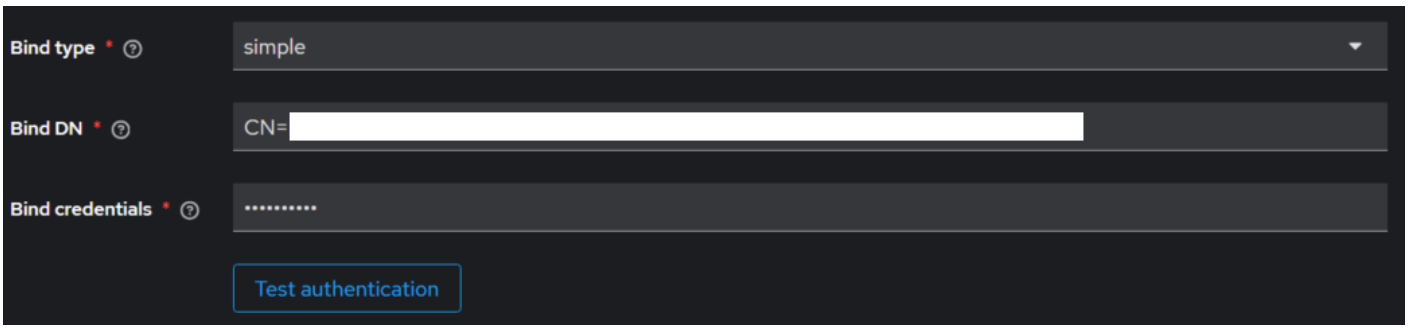
Enter l'URL du domaine LDAP au format : '***ldap://<FQDN du domaine:<port>***'

En fonction de si le lien se fait en LDAP ou LDAPS, il faudra activer '***EnableStartTLS***' choisir d'utiliser ou non '***Use Truststore SPI***'.



Puis cliquer sur le bouton "***Test Connection***". Le résultat devrait être :

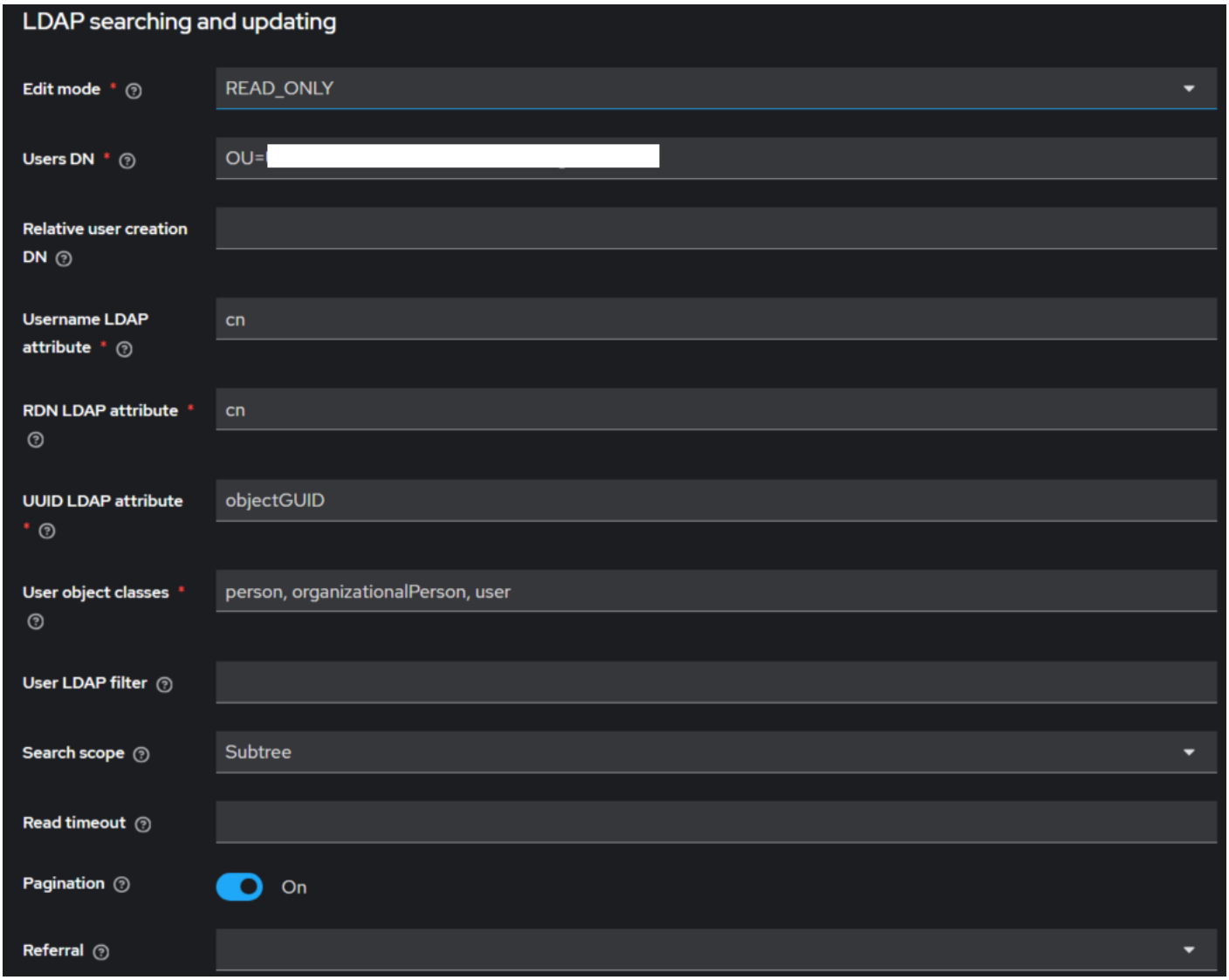
Choisir ensuite le type de bind '***simple***'. Puis entrer le User DN pour la connexion et le mot de passe du compte.



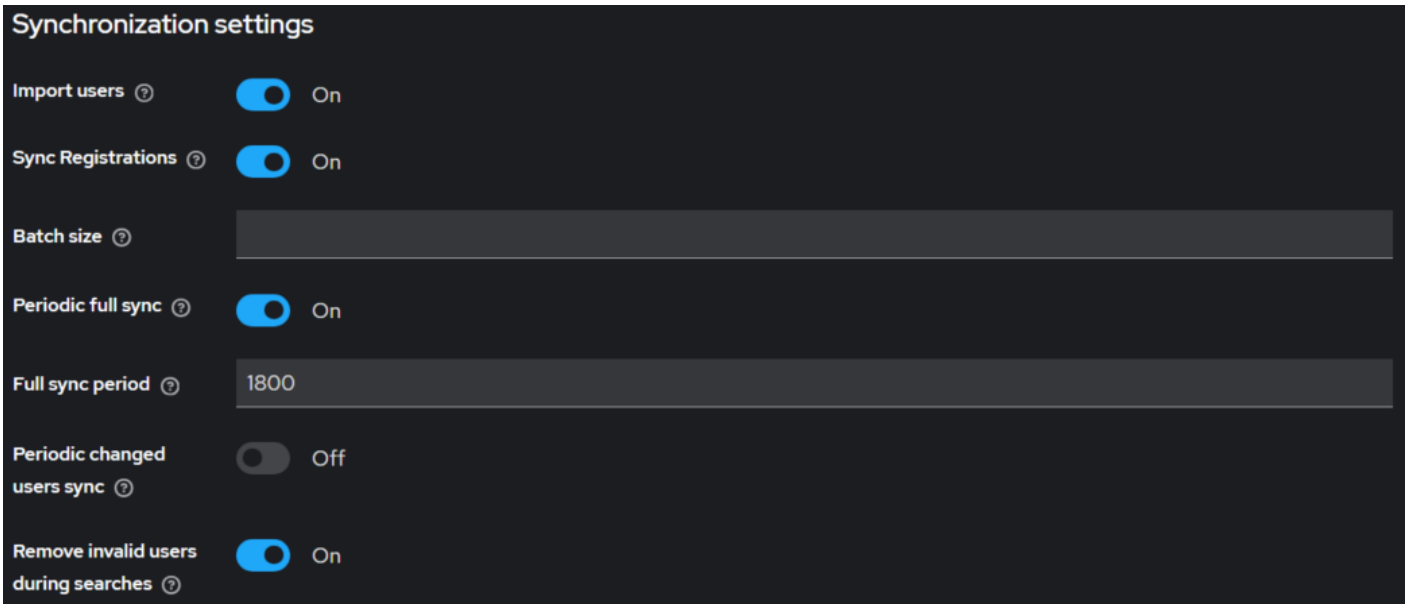
Cliquer sur "***Test authentication***". Le résultat devrait être :

Pour les paramètres supplémentaires, changer :

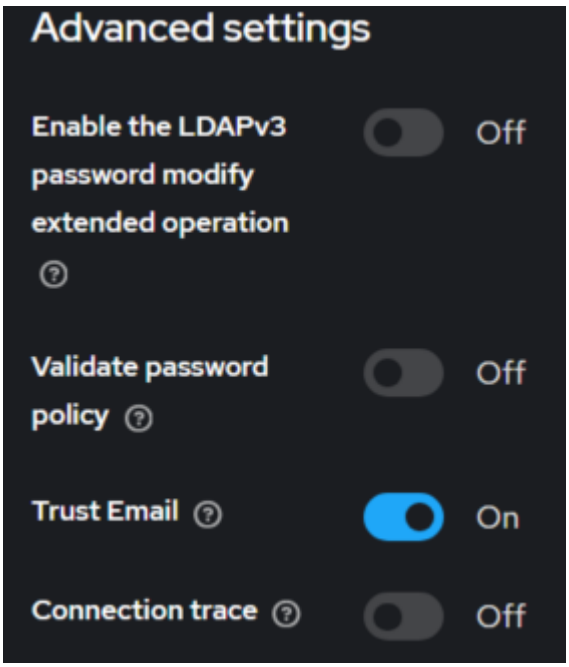
- Edit mode : ***READ_ONLY***
- Users DN : ***<dn de l'ou contenant les users>***
- Search scope : ***Subtree***



Pour les Synchronisation Settings :

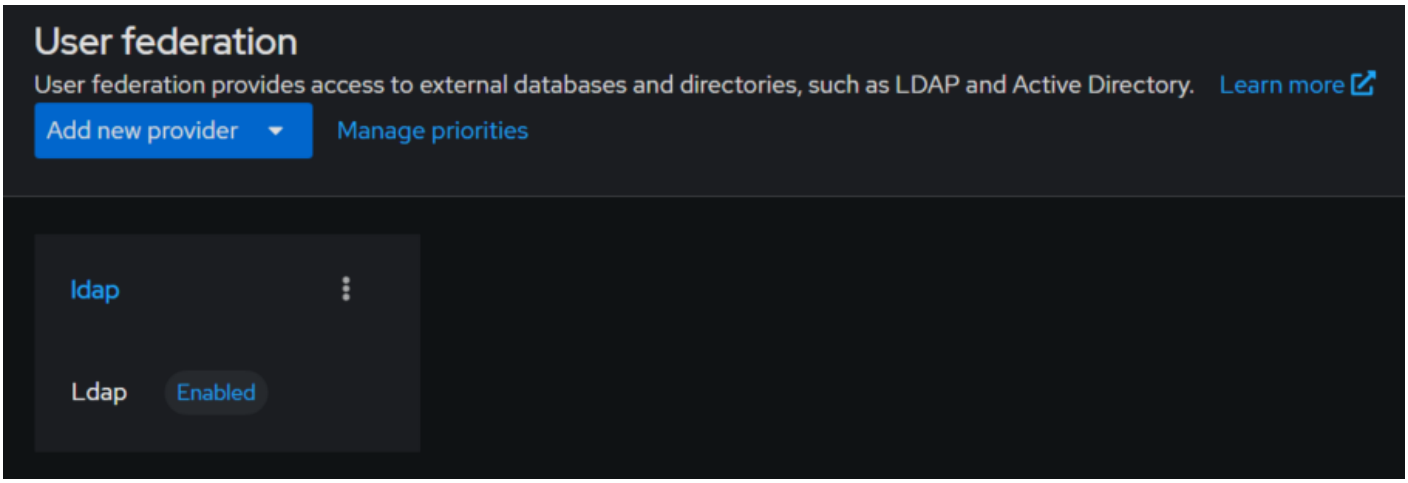


Dans les Advanced settings, activer '***Trust Email***'.

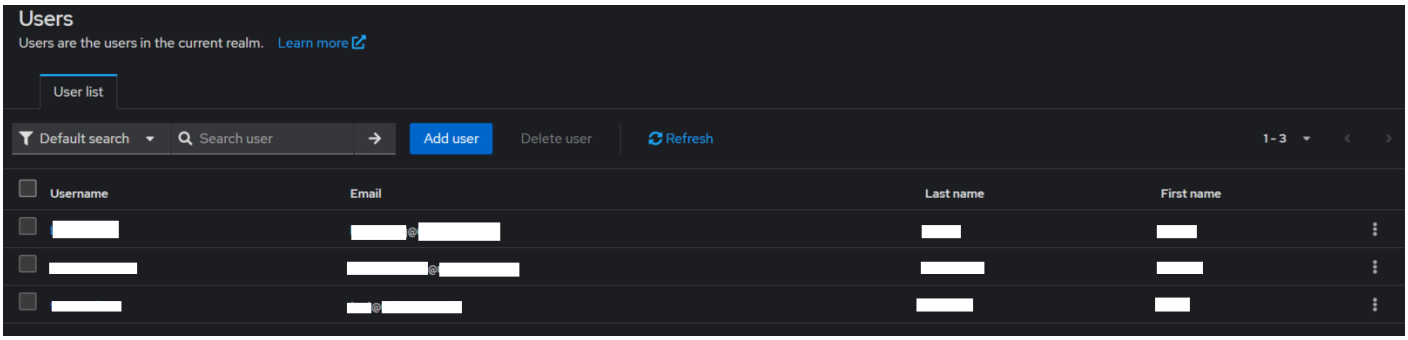


Puis cliquer sur '***Save***' pour terminer la création.

Dans le menu, sous '***User federation***', il devrait y avoir :

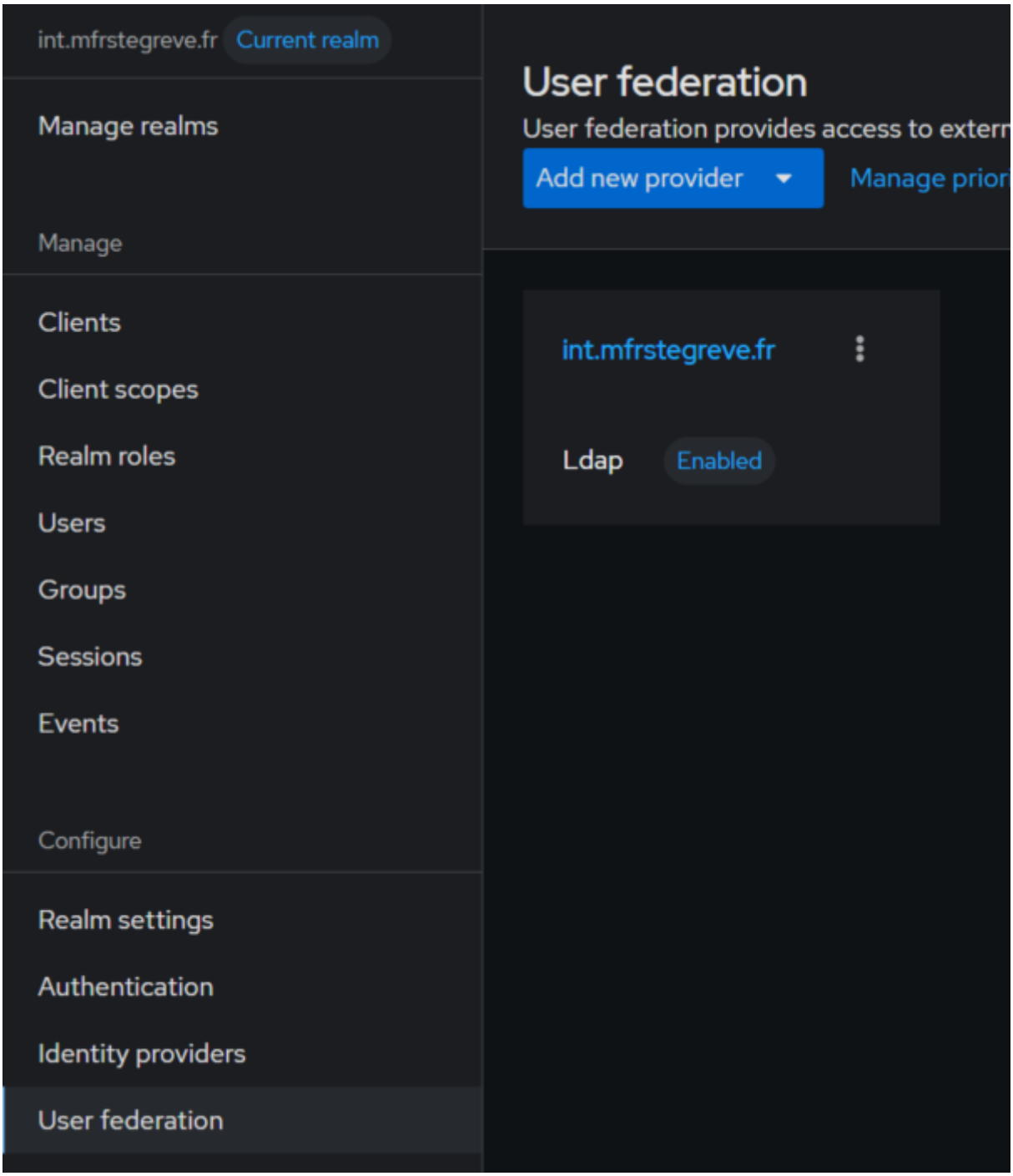


Et les utilisateurs devraient commencer à se synchroniser.

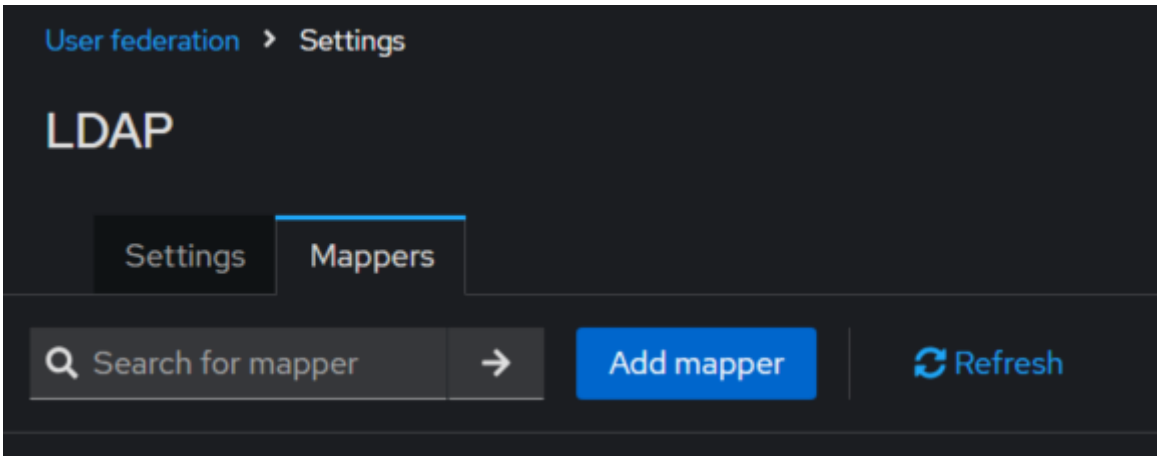


IV. Gérer la synchronisation des groupes

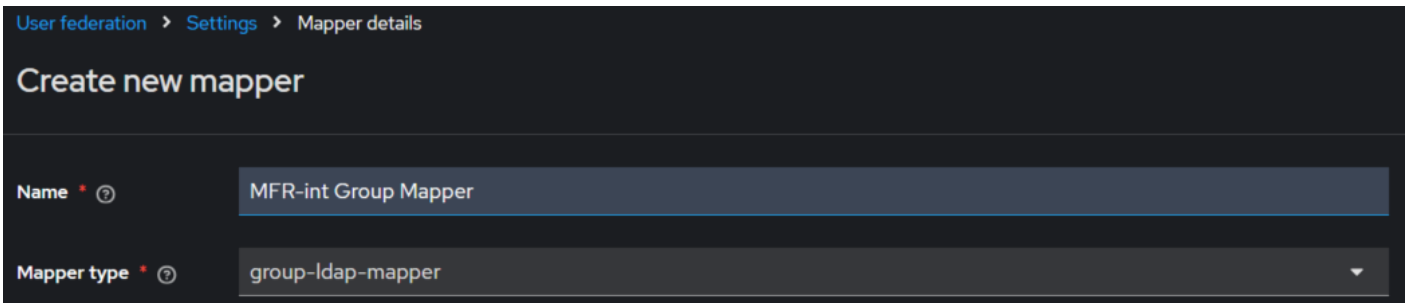
Pour synchroniser les groupes, aller dans le menu '***User federation***', sélectionner le provider précédemment créé.



Aller dans l'onglet '***Mappers***' et cliquer sur "***Add mapper***".

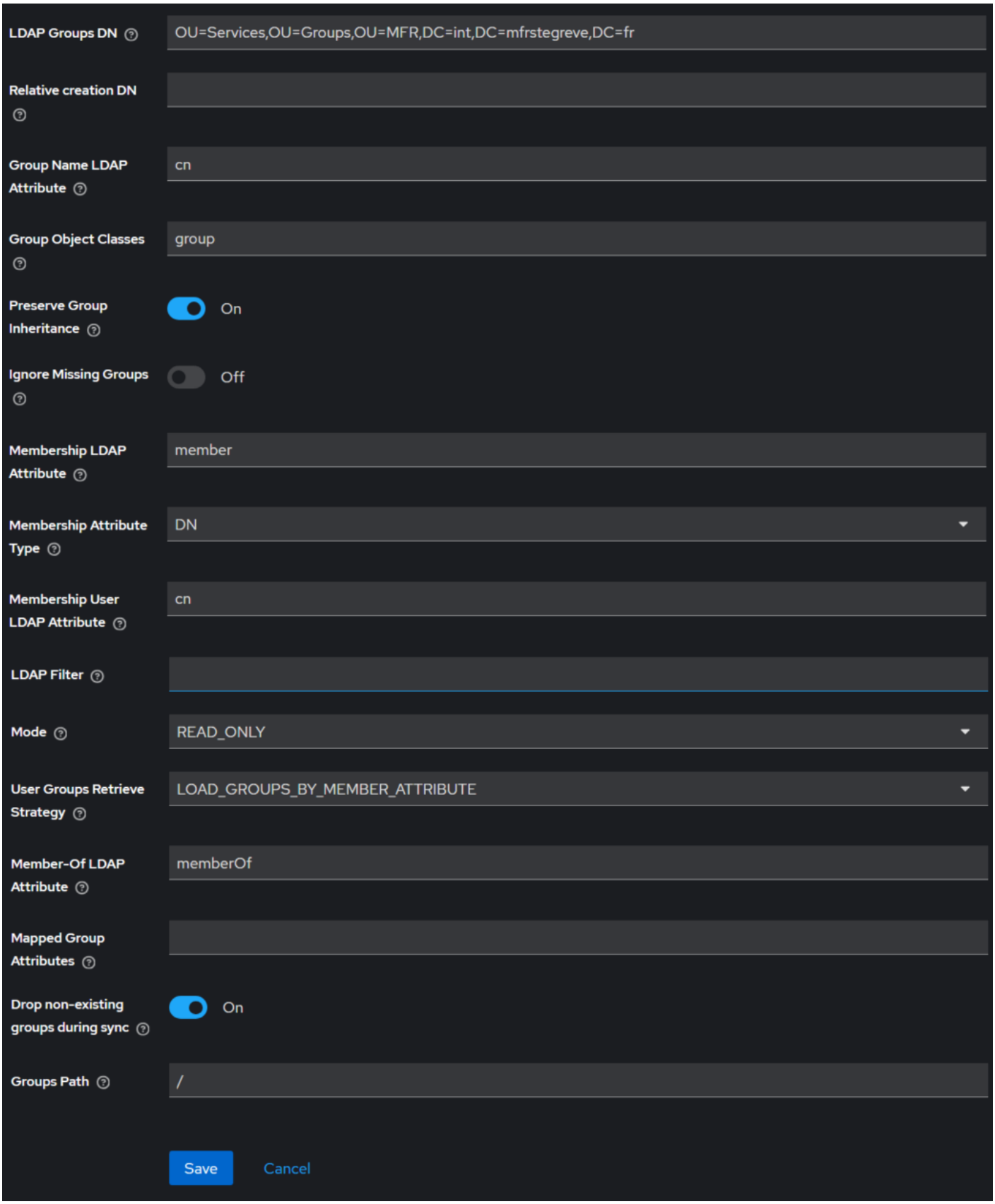


Donner un nom de mapper et choisir en Mapper type : "***group-ldap-mapper***".



Définir les propriété suivantes :

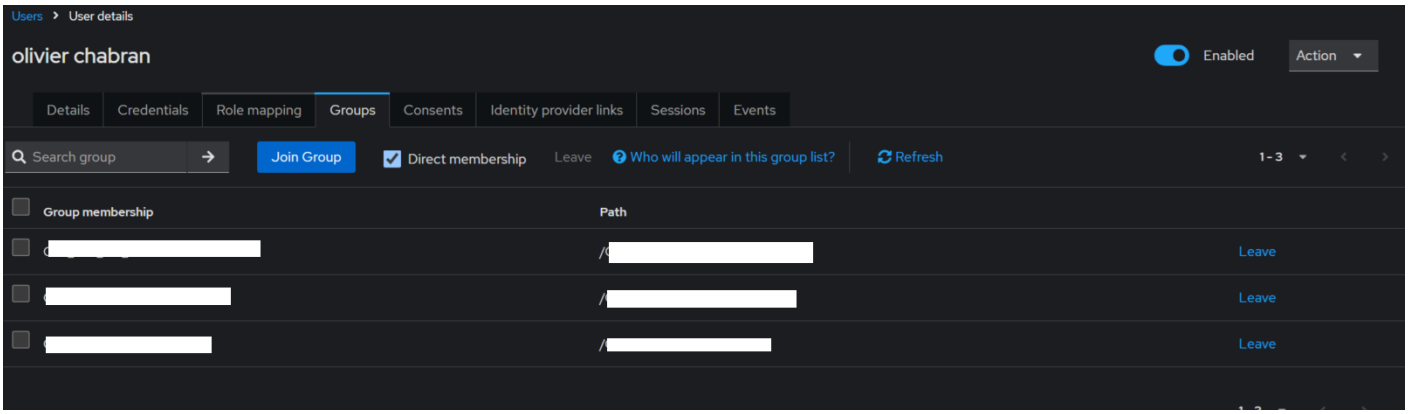
- LDAP Groups DN : ***<DN de l'ou où se situent les groupes>***
- Activer : ***Preserve Group inheritance***
- Mode : ***READ_ONLY***
- User Groups Retrieve strategy : ***LOAD_GROUPS_BY_MEMBER_ATTRIBUTE***
- Activer : ***Drop non-existing groups during sync***



Cliquer sur '***Save***' pour terminer.

> **Astuce** : Pour éviter d'attendre la prochaine synchronisation, il est possible de supprimer un utilisateur pour forcer un refresh.

Sur les utilisateurs, dans l'onglet "***Groups***", les groupes auquel l'utilisateur appartient devrait maintenant apparaître.



Dans le menu "***Groups***", les groupes devraient maintenant apparaître.