

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

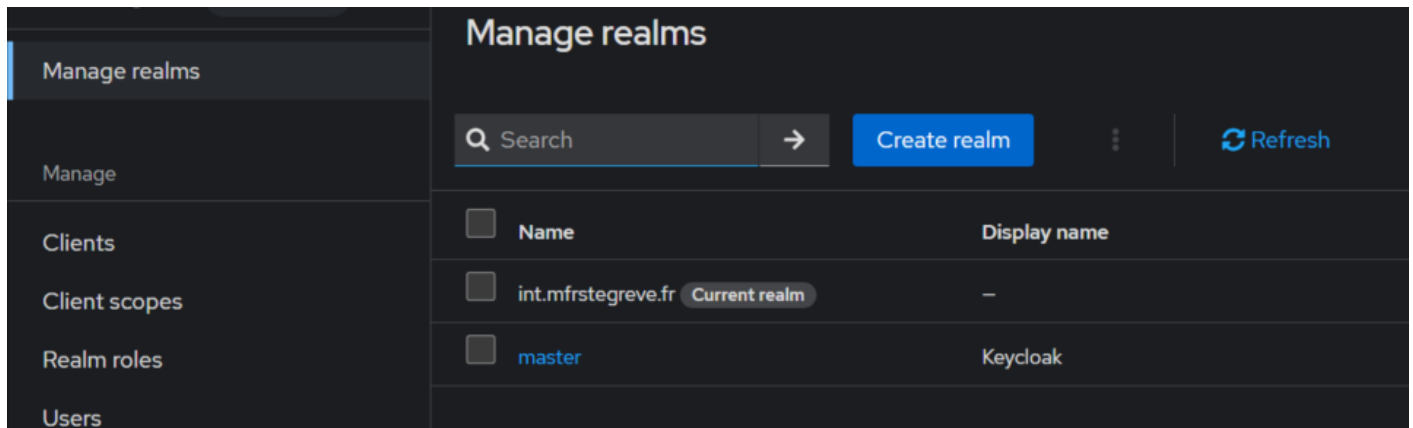
I. Introduction

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.

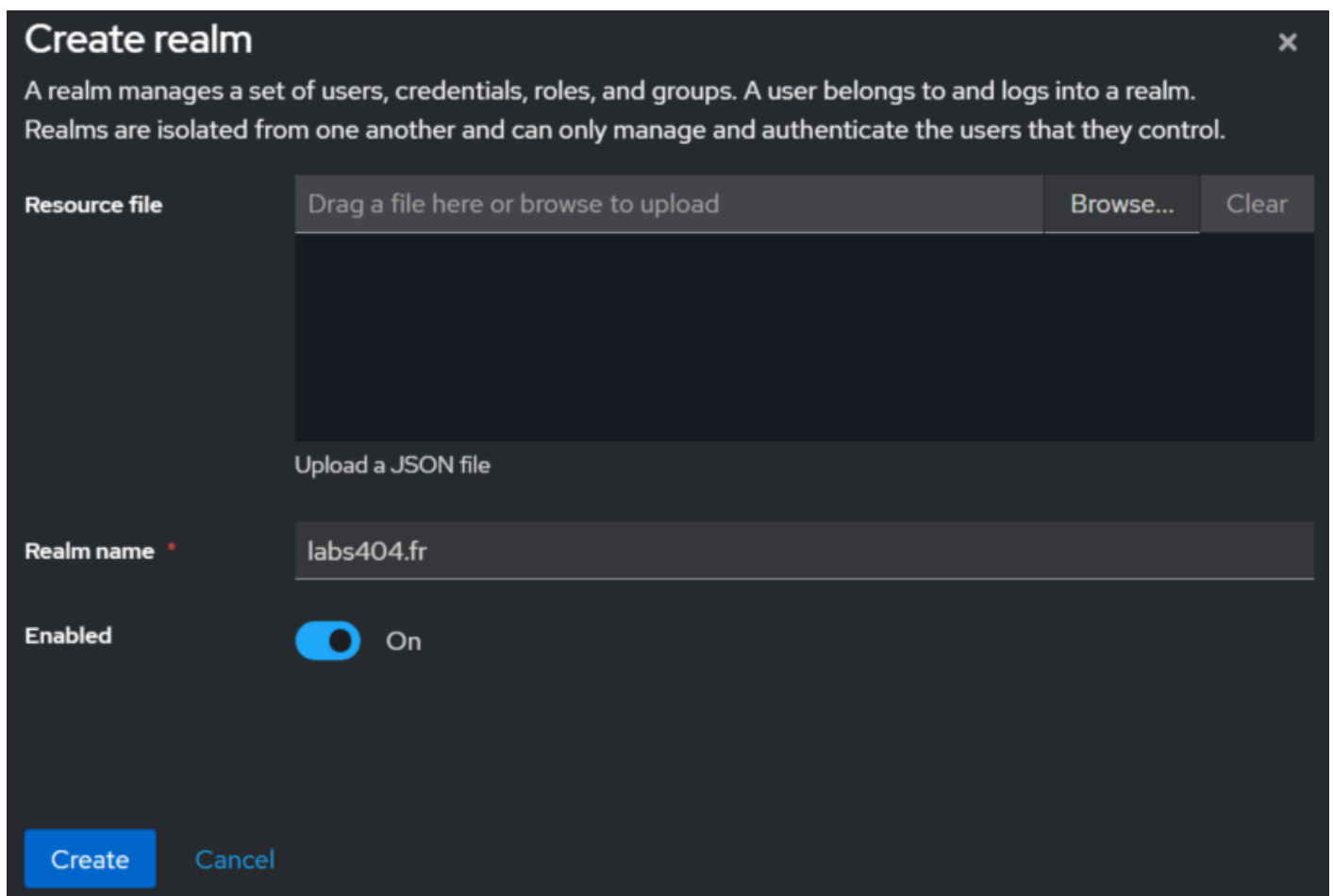
II. Créer le Realm

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**".

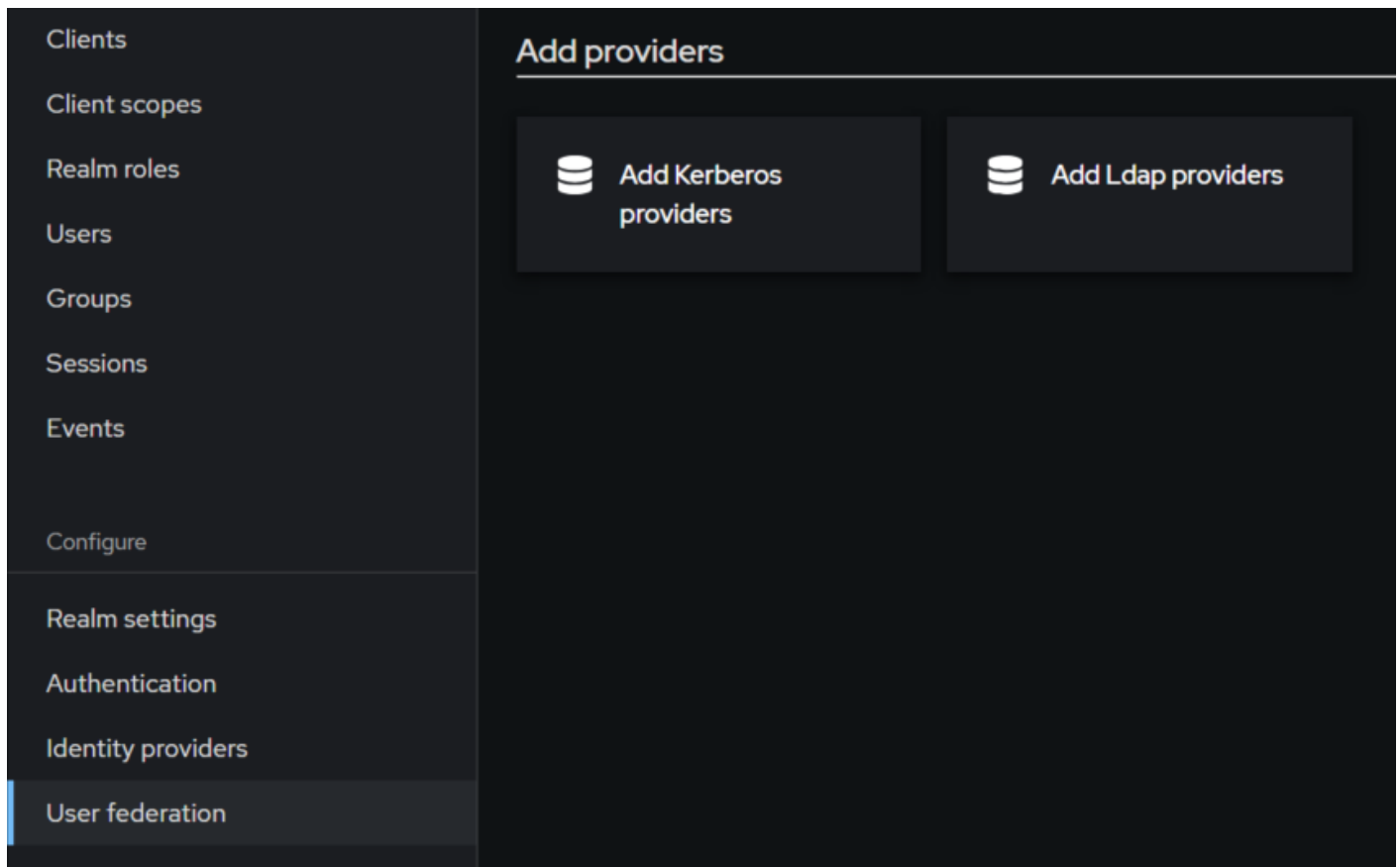
Modifier le 'Display name' et le 'HTML Display name' Pour pouvoir personnaliser le nom du realm qui apparaîtra à la connexion.

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 liaisons 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**'.

A screenshot of a 'General options' form. It contains two fields. The first field is labeled 'UI display name' with a red asterisk and a help icon; its value is 'labs404.fr'. The second field is labeled 'Vendor' with a red asterisk and a help icon; it is a dropdown menu currently showing '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**'.

Connection and authentication settings

Connection URL * ⓘ ldap://[redacted]:389

Enable StartTLS ⓘ ☐ Off

Use Truststore SPI ⓘ Never

Connection pooling ⓘ ☐ Off

Connection timeout ⓘ 200

[Test connection](#)

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.

Bind type * ⓘ simple

Bind DN * ⓘ CN=[redacted]

Bind credentials * ⓘ

[Test authentication](#)

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**

LDAP searching and updating

Edit mode * ?

READ_ONLY ▼

Users DN * ?

OU=

Relative user creation DN ?

Username LDAP attribute * ?

cn

RDN LDAP attribute * ?

cn

UUID LDAP attribute * ?

objectGUID

User object classes * ?

person, organizationalPerson, user

User LDAP filter ?

Search scope ?

Subtree ▼

Read timeout ?

Pagination ?

☒ On

Referral ?

▼

Pour les Synchronisation Settings :

Synchronization settings

Import users ⓘ ☒ On

Sync Registrations ⓘ ☒ On

Batch size ⓘ

Periodic full sync ⓘ ☒ On

Full sync period ⓘ

Periodic changed users sync ⓘ ☐ Off

Remove invalid users during searches ⓘ ☒ On

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

Advanced settings

Enable the LDAPv3 password modify extended operation ⓘ ☐ Off

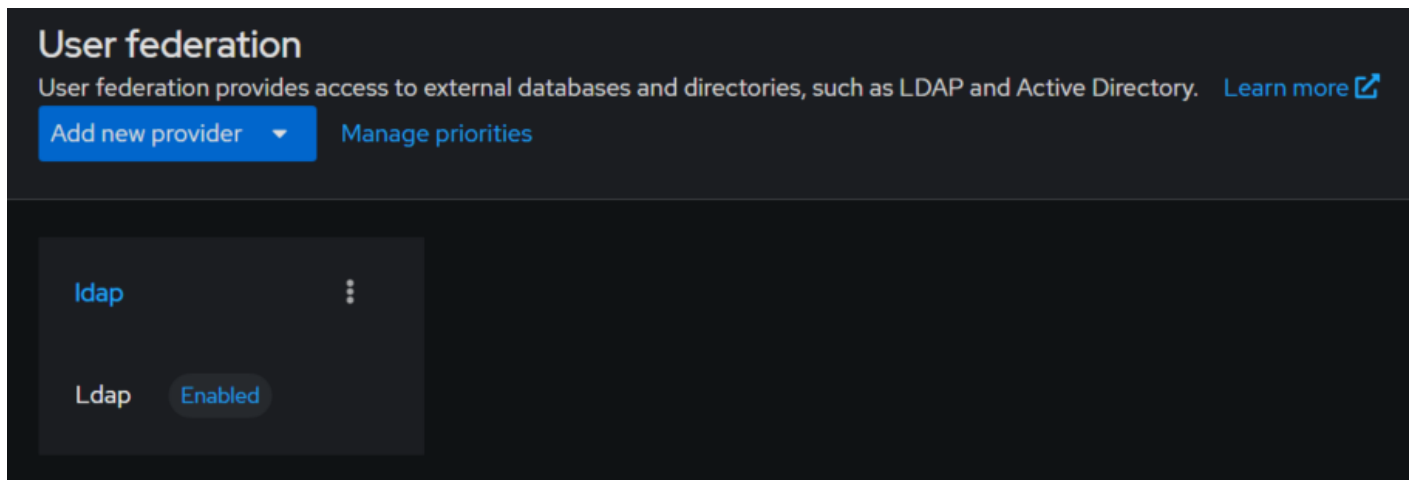
Validate password policy ⓘ ☐ Off

Trust Email ⓘ ☒ On

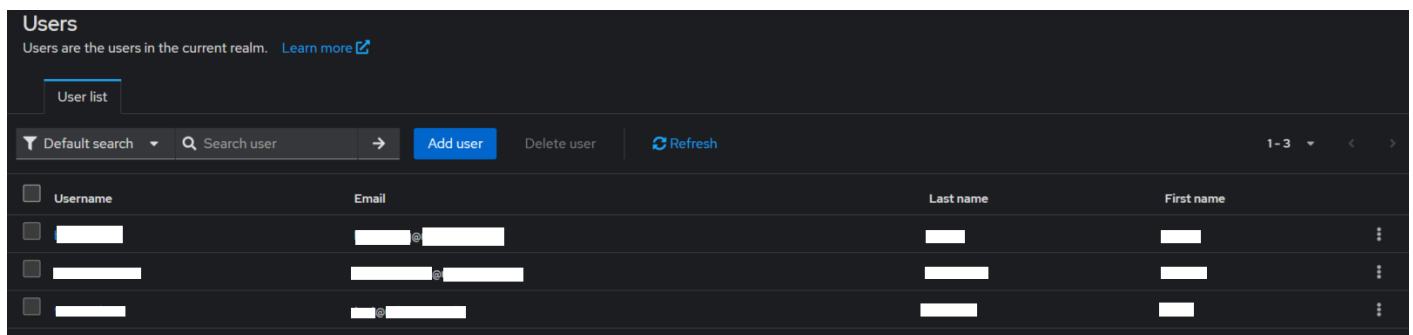
Connection trace ⓘ ☐ Off

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

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

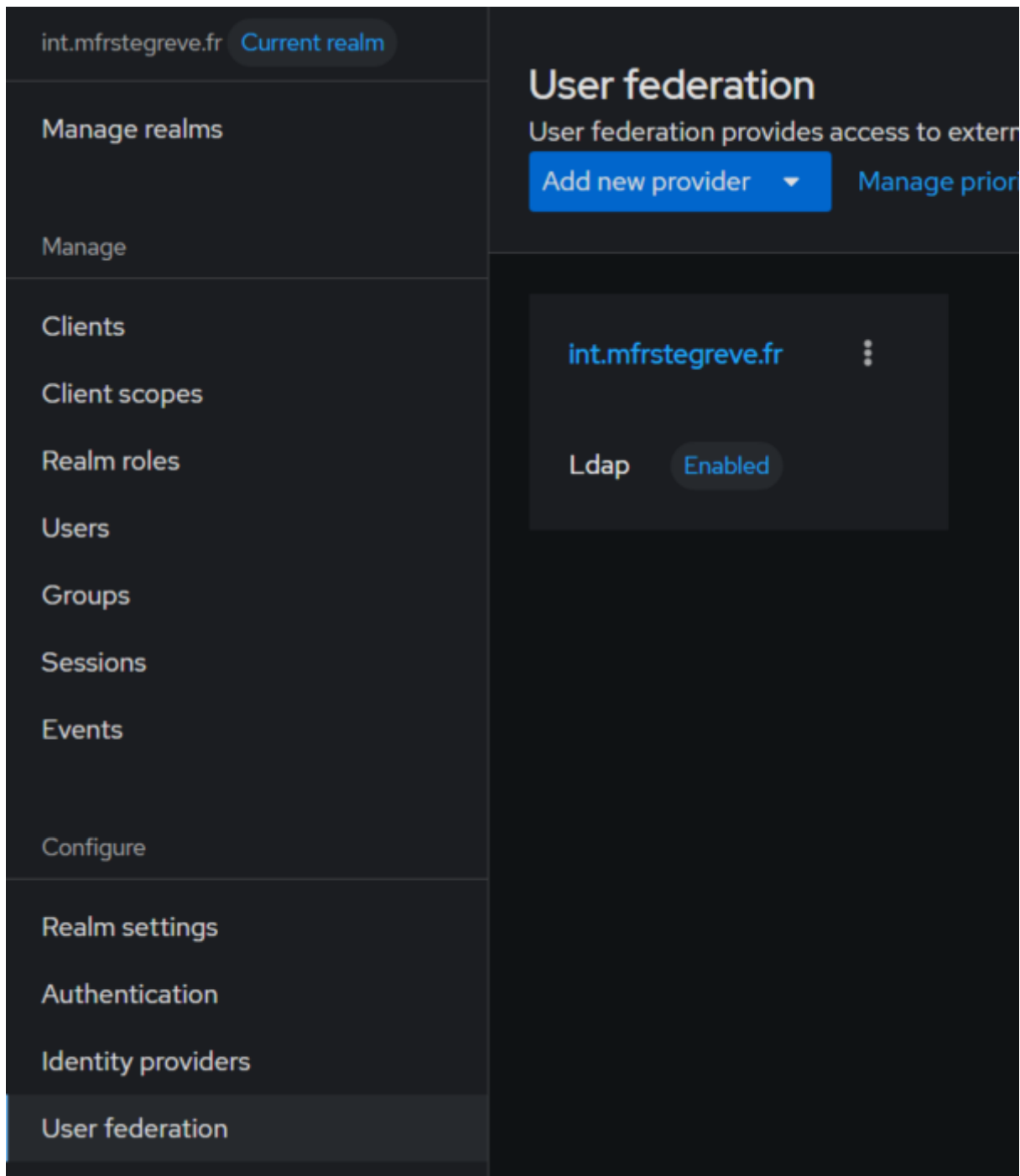


Et les utilisateurs devraient commencer à se synchroniser.

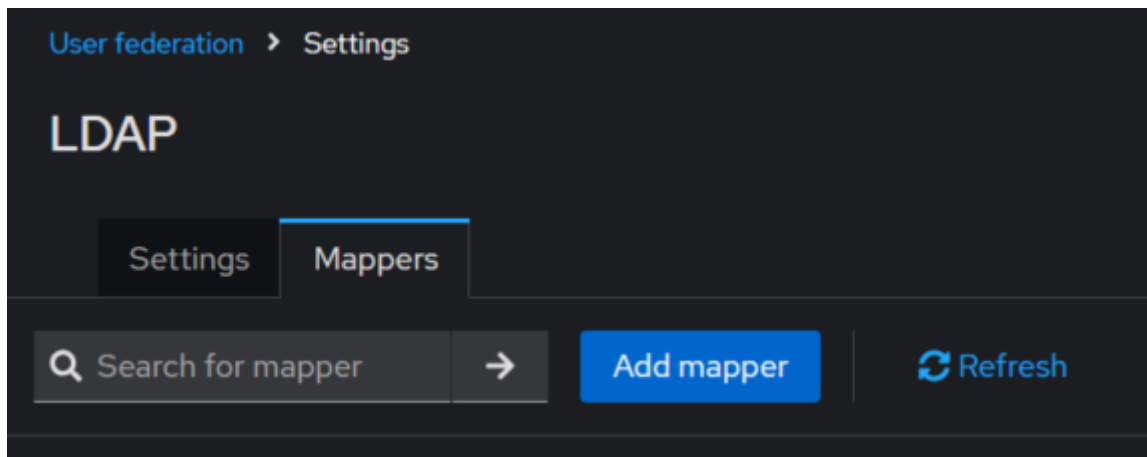


IV. Gérer la synchronisation des groupes

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**".

The screenshot shows the 'Create new mapper' form. The breadcrumb navigation is 'User federation > Settings > Mapper details'. The form has two fields: 'Name' with a red asterisk and a help icon, containing the text 'MFR-int Group Mapper'; and 'Mapper type' with a red asterisk and a help icon, containing a dropdown menu with 'group-ldap-mapper' selected.

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**

LDAP Groups DN ⓘ

OU=Services,OU=Groups,OU=MFR,DC=int,DC=mfrstegreve,DC=fr

Relative creation DN ⓘ

Group Name LDAP Attribute ⓘ

cn

Group Object Classes ⓘ

group

Preserve Group Inheritance ⓘ

On

Ignore Missing Groups ⓘ

Off

Membership LDAP Attribute ⓘ

member

Membership Attribute Type ⓘ

DN

Membership User LDAP Attribute ⓘ

cn

LDAP Filter ⓘ

Mode ⓘ

READ_ONLY

User Groups Retrieve Strategy ⓘ

LOAD_GROUPS_BY_MEMBER_ATTRIBUTE

Member-Of LDAP Attribute ⓘ

memberOf

Mapped Group Attributes ⓘ

Drop non-existing groups during sync ⓘ

On

Groups Path ⓘ

/

Save

Cancel

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.

Users > User details

olivier chabran Enabled Action

Details Credentials Role mapping **Groups** Consents Identity provider links Sessions Events

Search group → Join Group ☒ Direct membership Leave Who will appear in this group list? Refresh 1-3 < >

☐ Group membership	Path	
☐ [redacted]	/[redacted]	Leave
☐ [redacted]	/[redacted]	Leave
☐ [redacted]	/[redacted]	Leave

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