Solutions SSO

Keycloak VS Authentik

Sommaire

- Points en commun des deux solutions
- Les spécificités de Keycloak
  - Des screenshots et exemples de Keycloak
- Les spécificités d’Authentik
  - Des screenshots et exemples d’Authentik
- Les problèmes que j’ai rencontré
- Ma proposition

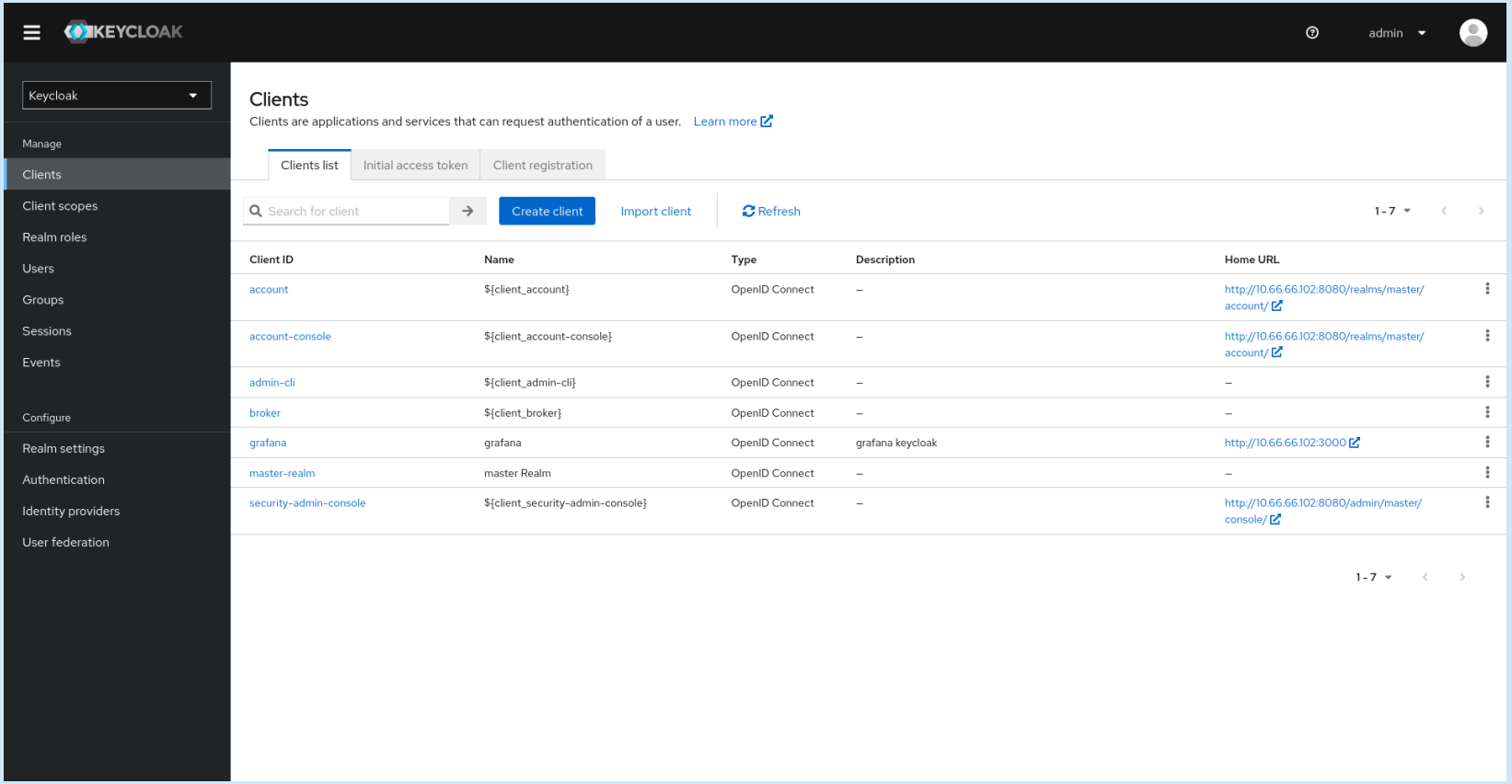
Les points en commun

- Permettent chacun de faire du SSO via OpenID ou SAML
- Gestion des utilisateurs (username, mots de passes, email, nom, prénom etc…)
- Les utilisateurs peuvent se gérer (c’est à dire changer leurs mots de passes par exemple)
- Chacun peuvent agir comme des “Broker” c’est à dire permettre une gestion de plusieurs fournisseurs d’utilisateurs. (ex: OpenLDAP, comptes Google, comptes Microsoft etc)
- Ils peuvent être connecté à un OpenLDAP via un mapping que l’on configure (Keycloak) ou de manière autogéré (Authentik)
- Ils sont assez gourmand en ressources (~1Go de RAM par stack)

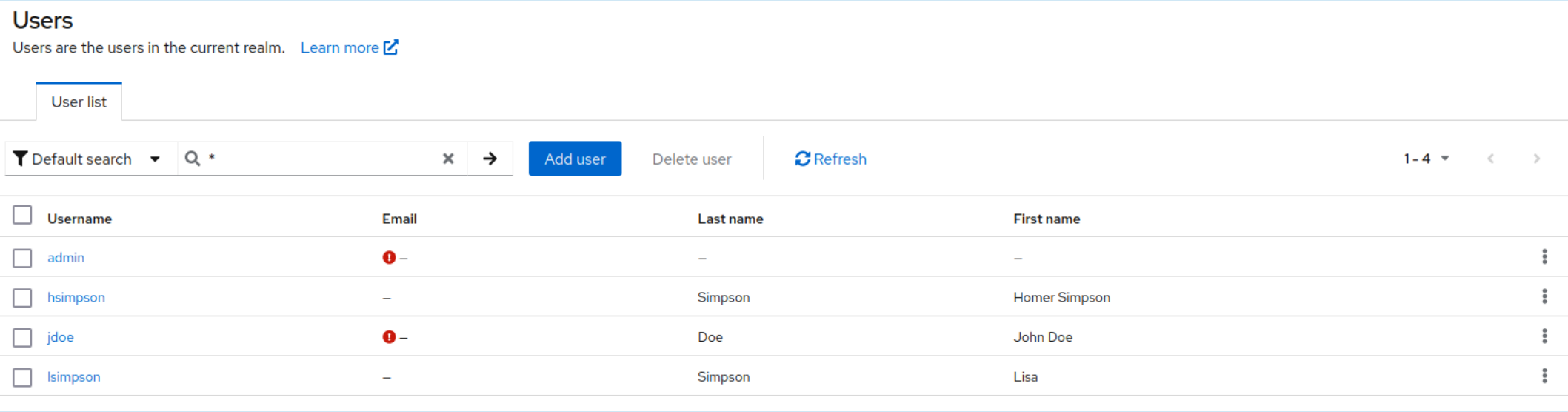
Les spécificités de Keycloak

- Développé en Java
- Le projet est mature (2014)
- Des mises à jour régulières sont présentes
- C’est une application Cloud Native
- Pour utiliser un OpenLDAP, celui-ci doit configuré à l’extérieur de Keycloak, celui-ci doit être ensuite mapper pour la gestion des utilisateurs. De là le Keycloak peut faire ce qu’il veut sur le LDAP du moment que c’est mapper correctement.

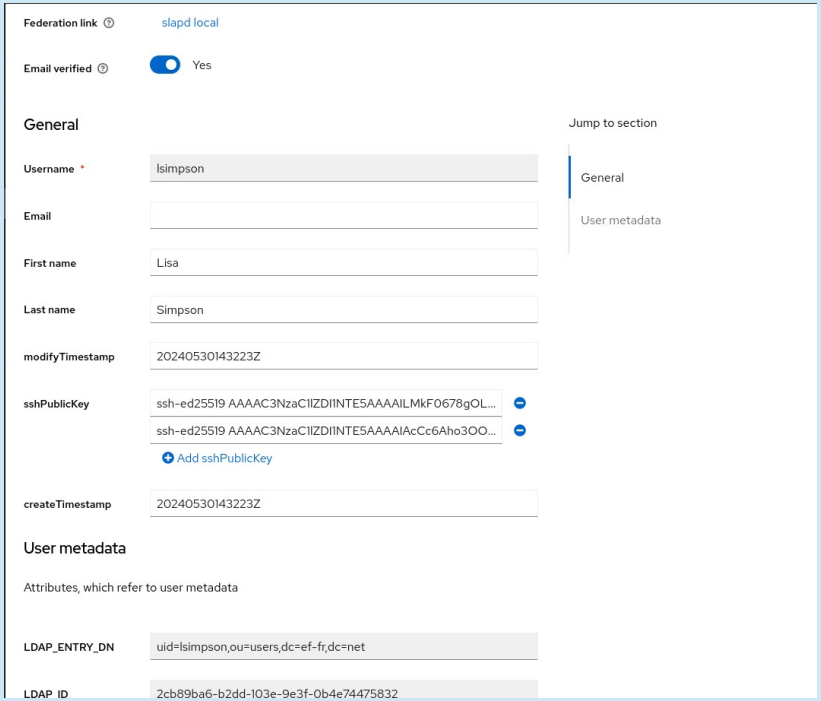
L’interface de Keycloak



L'interface de Keycloak



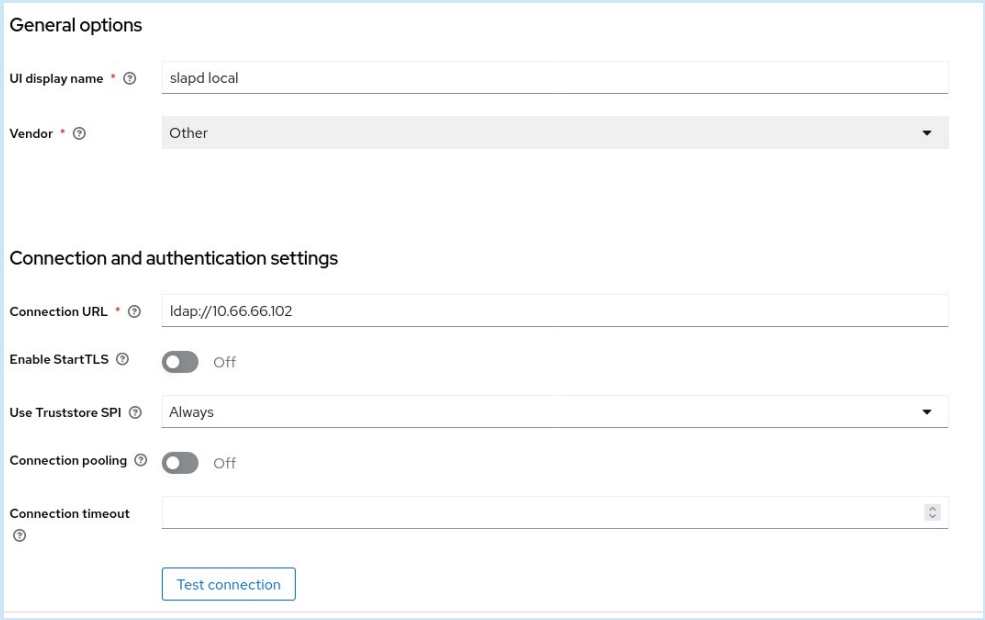
Un exemple d'utilisateur

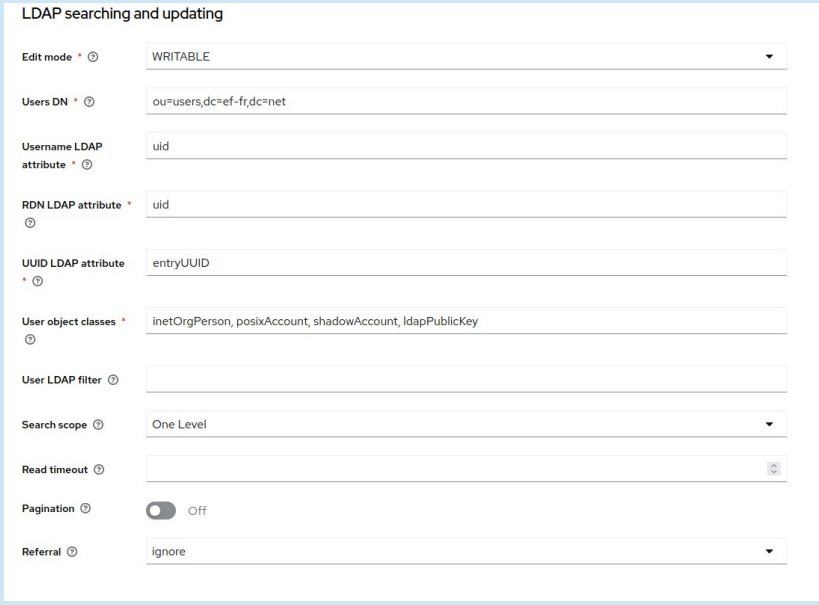


ldapsearch -x -H ldap://10.66.66.102 -D "cn=admin,dc=ef-fr,dc=net" -w 1234 -b "ou=users,dc=ef-fr,dc=net"

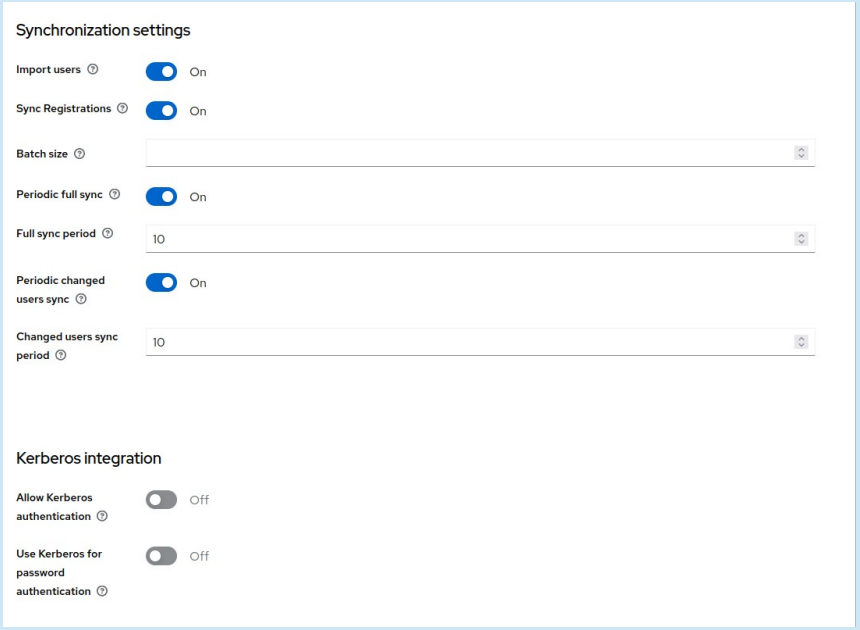
```
# lsimpson, users, ef-fr.net
dn: uid=lsimpson,ou=users,dc=ef-fr,dc=net
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
objectClass: ldapPublicKey
cn:: TGlzYSA=
sn: Simpson
givenName: Lisa
uid: lsimpson
uidNumber: 10002
gidNumber: 10000
homeDirectory: /home/lsimpson
loginShell: /bin/bash
gecos: Lisa Simpson
userPassword:: e1NTSEF9SHVTSmFud0FRTWNjR2RBcERvblJOZ1lKRmQ4K1hBSFQ=
sshPublicKey: ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAILMkF0678gOLwqvtRGGNn9F57EJl
 fCi4iJSsgXK/ZAbQ patch@spaceint.fr
sshPublicKey: ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIAcCc6Aho3OOoa/W/rdy5D+1uHDQ
 8MfaxhwRTALXWLiA patch@blitz
```

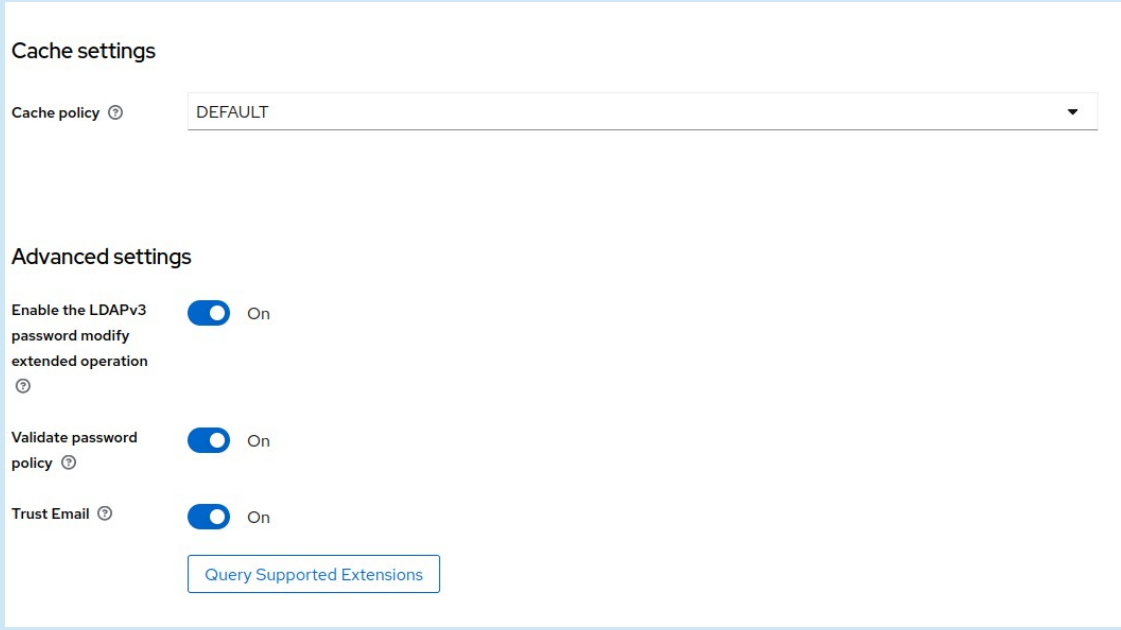
Configuration LDAP



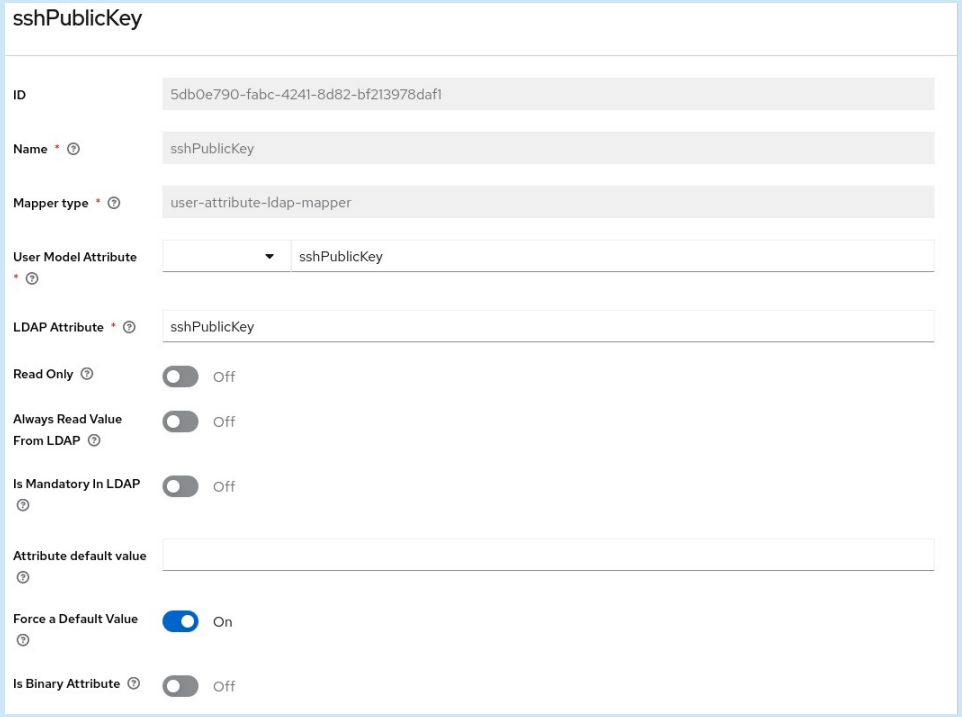


Configuration LDAP

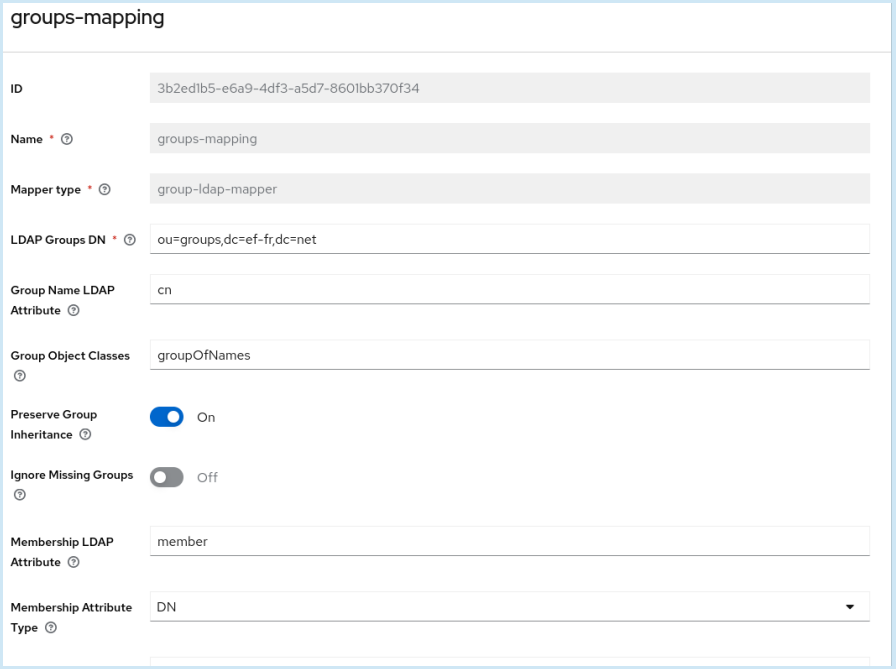


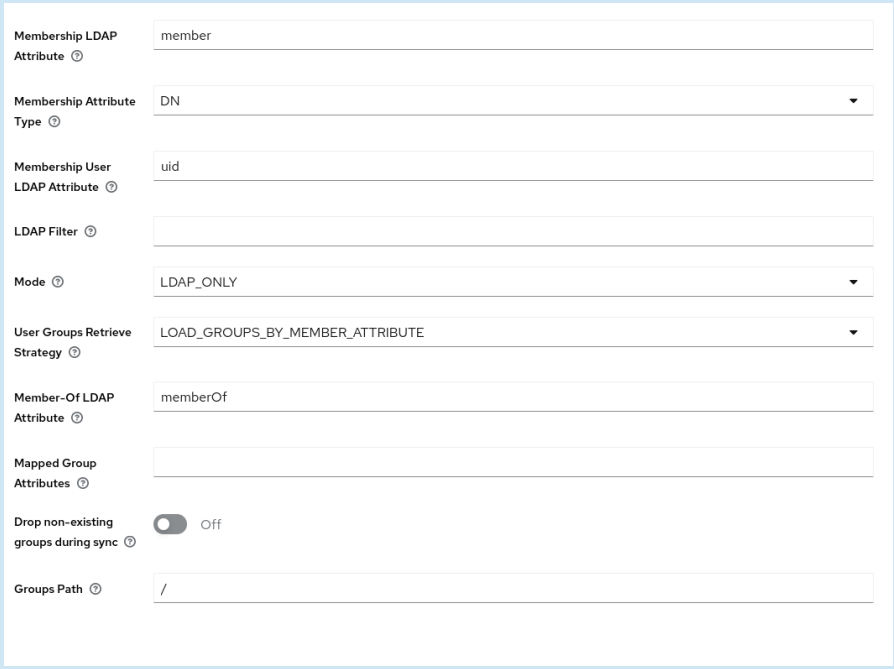


Mapping LDAP

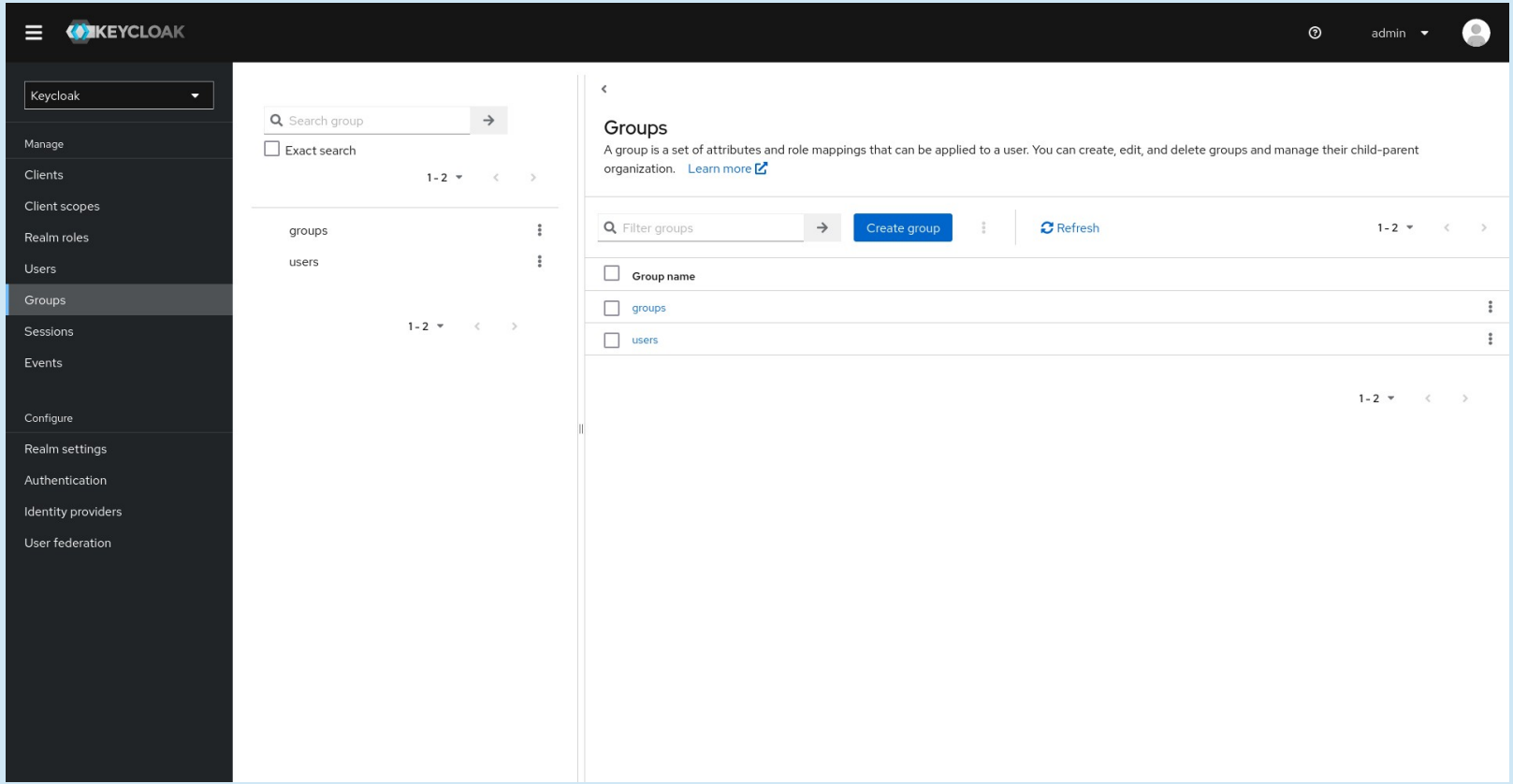


Mapping LDAP

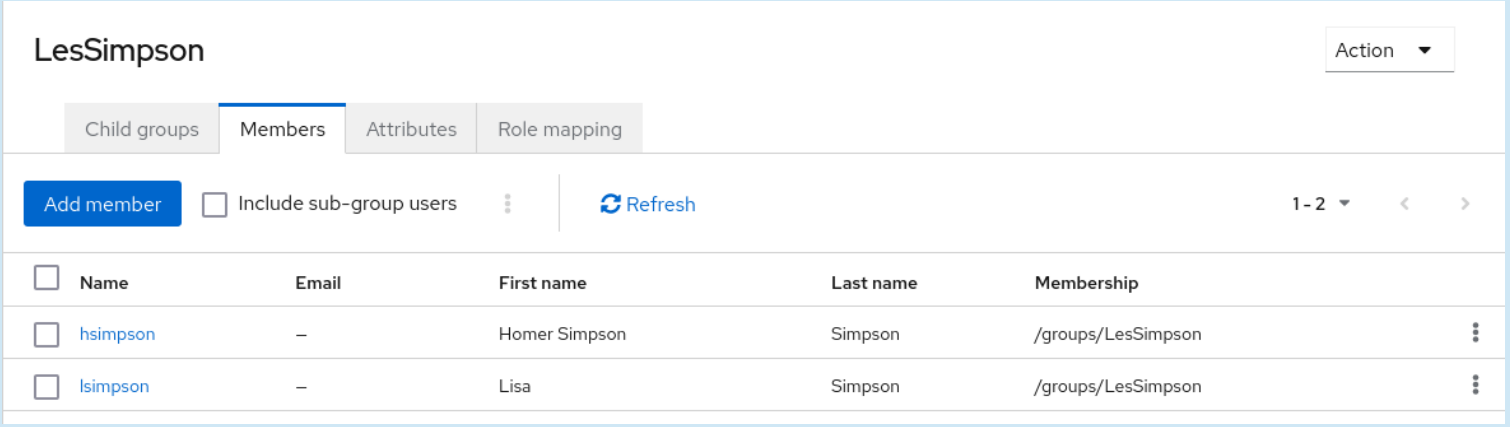




Groupes


KEYCLOAK
admin
Keycloak
Manage
Clients
Client scopes
Realm roles
Users
Groups
Sessions
Events
Configure
Realm settings
Authentication
Identity providers
User federation
Search group
Exact search
1 - 2
groups
users
1 - 2
Groups
A group is a set of attributes and role mappings that can be applied to a user. You can create, edit, and delete groups and manage their child-parent organization. Learn more
Filter groups
Create group
Refresh
1 - 2
Group name
groups
users
1 - 2

Groupes

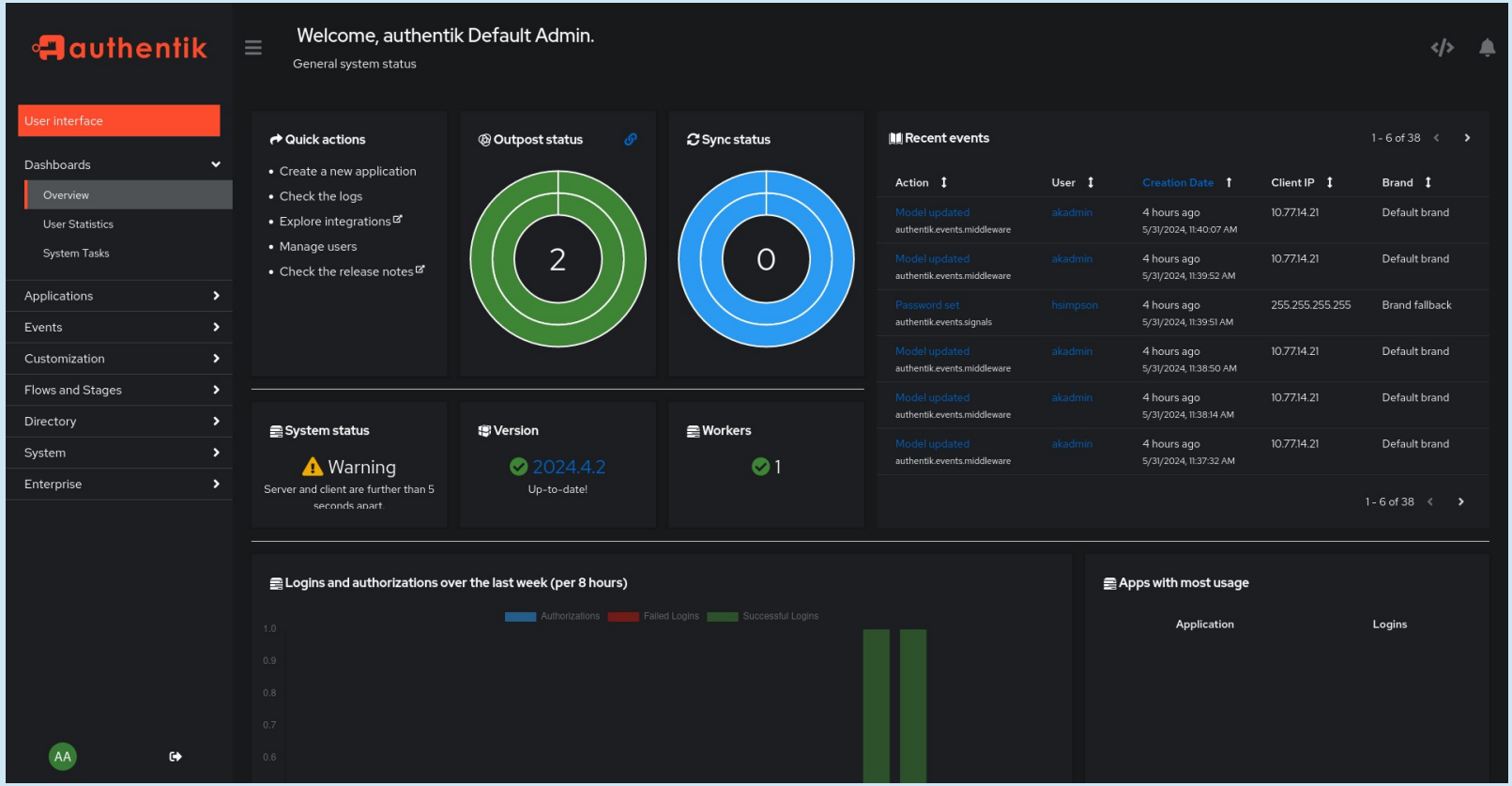



```
# LesSimpson, groups, ef-fr.net
dn: cn=LesSimpson,ou=groups,dc=ef-fr,dc=net
objectClass: groupOfNames
cn: LesSimpson
member: cn=empty-membership-placeholder
member: uid=lsimpson,ou=users,dc=ef-fr,dc=net
member: uid=hsimpson,ou=users,dc=ef-fr,dc=net
```

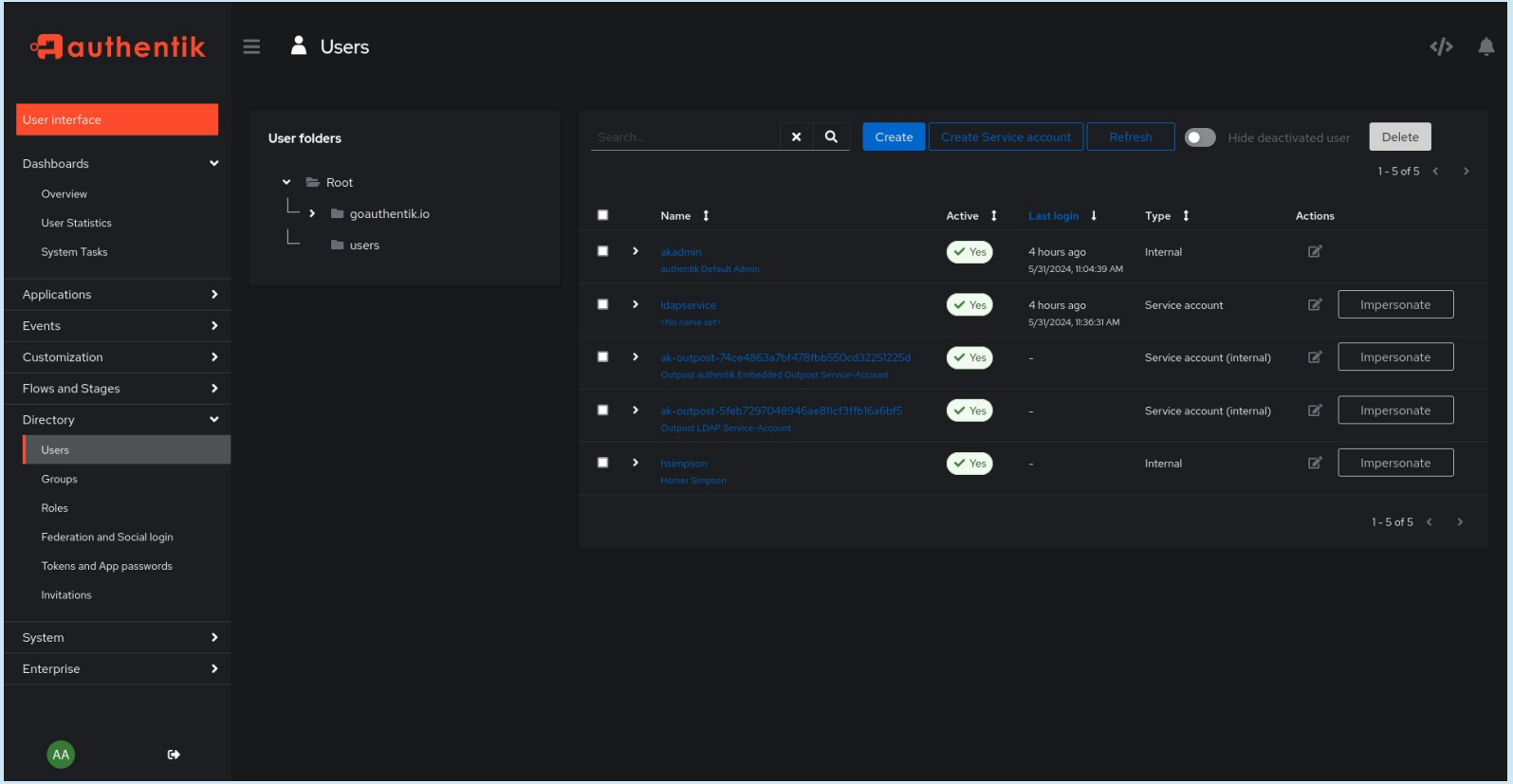
Les spécificités d'Authentik

- Développé en Python et Typescript
- Le projet est encore jeune (2020)
- Des mises à jour régulières sont présentes
- Ce n'est pas une application Cloud Native
- Pour utiliser un OpenLDAP, on doit le configurer depuis Authentik, et celui-ci se charger de déployer tout seul un conteneur OpenLDAP.
- Authentik possède une offre payante pour avoir plus de 50 utilisateurs

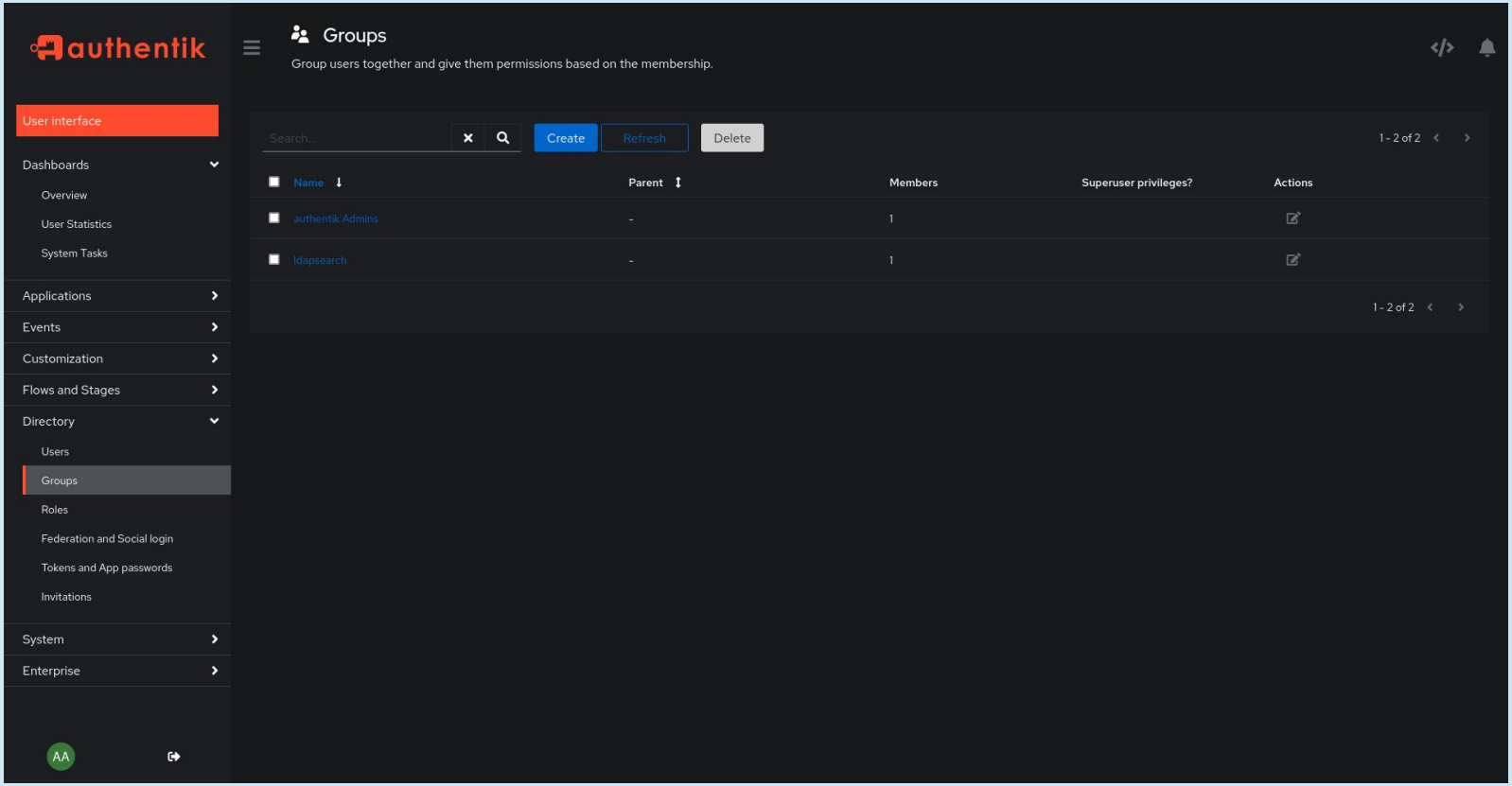
L’interface d’Authentik



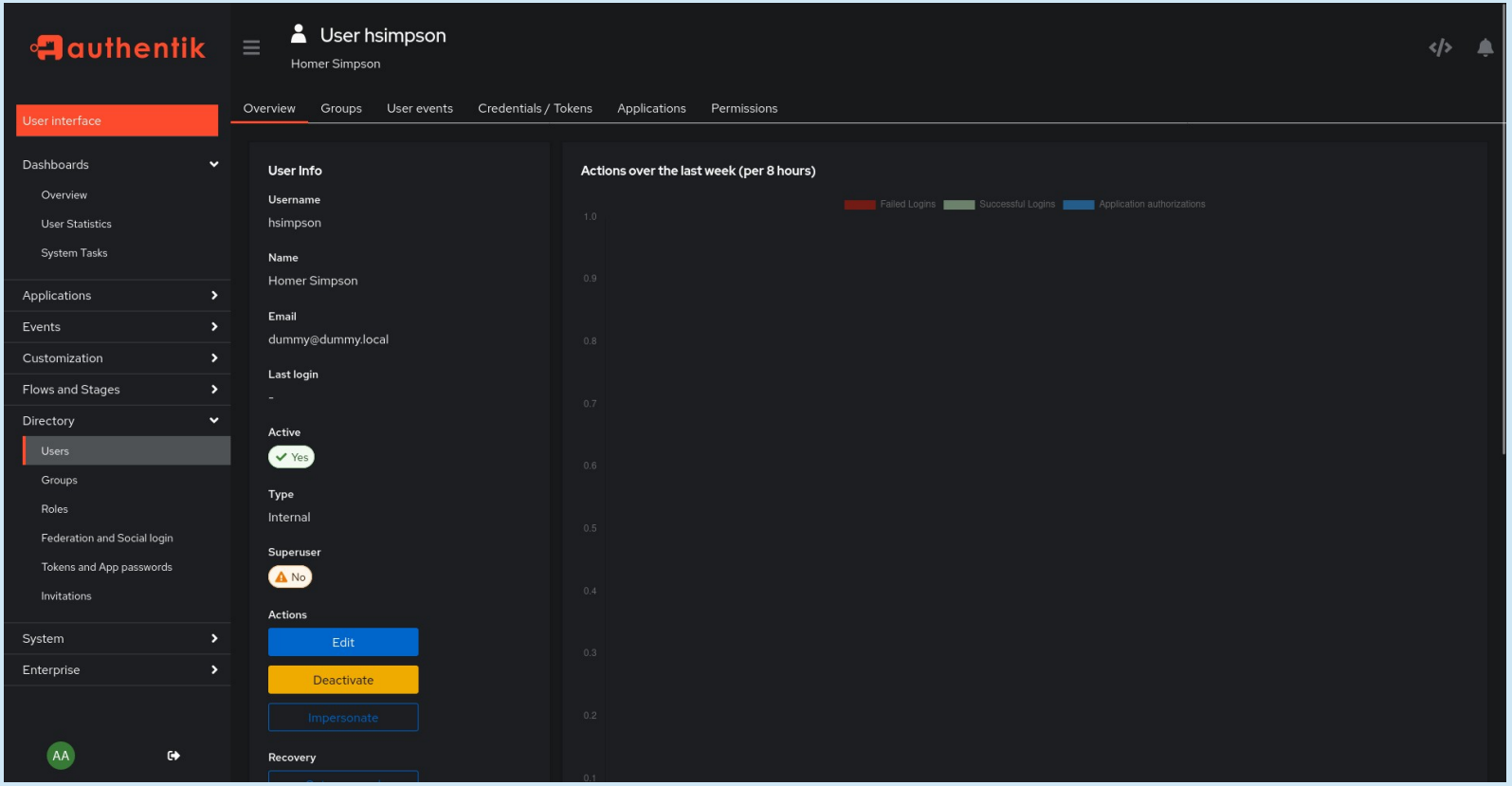
L’interface d’Authentik



L’interface d’Authentik

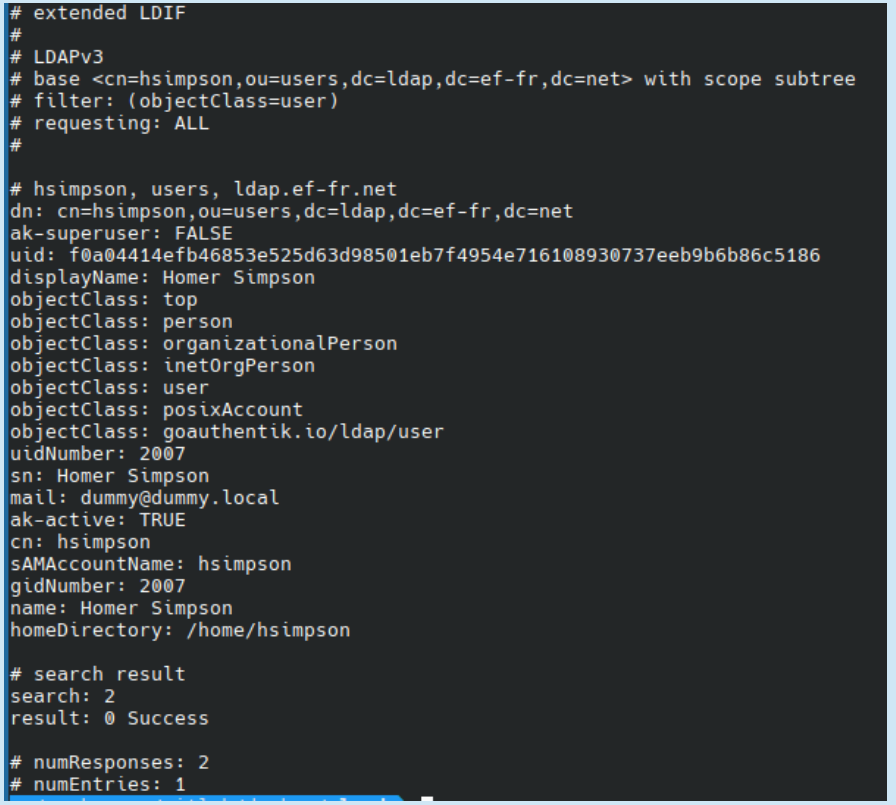


Exemple d’utilisateur



Exemple d’utilisateur

En requête LDAP : ldapsearch -x -H ldap://10.66.66.219:389 -D "cn=ldapservice,ou=users,dc=ldap,dc=ef-fr,dc=net" -w abcd1234 -b "cn=hsimpson,ou=users,dc=ldap,dc=ef-fr,dc=net" '(objectClass=user)'

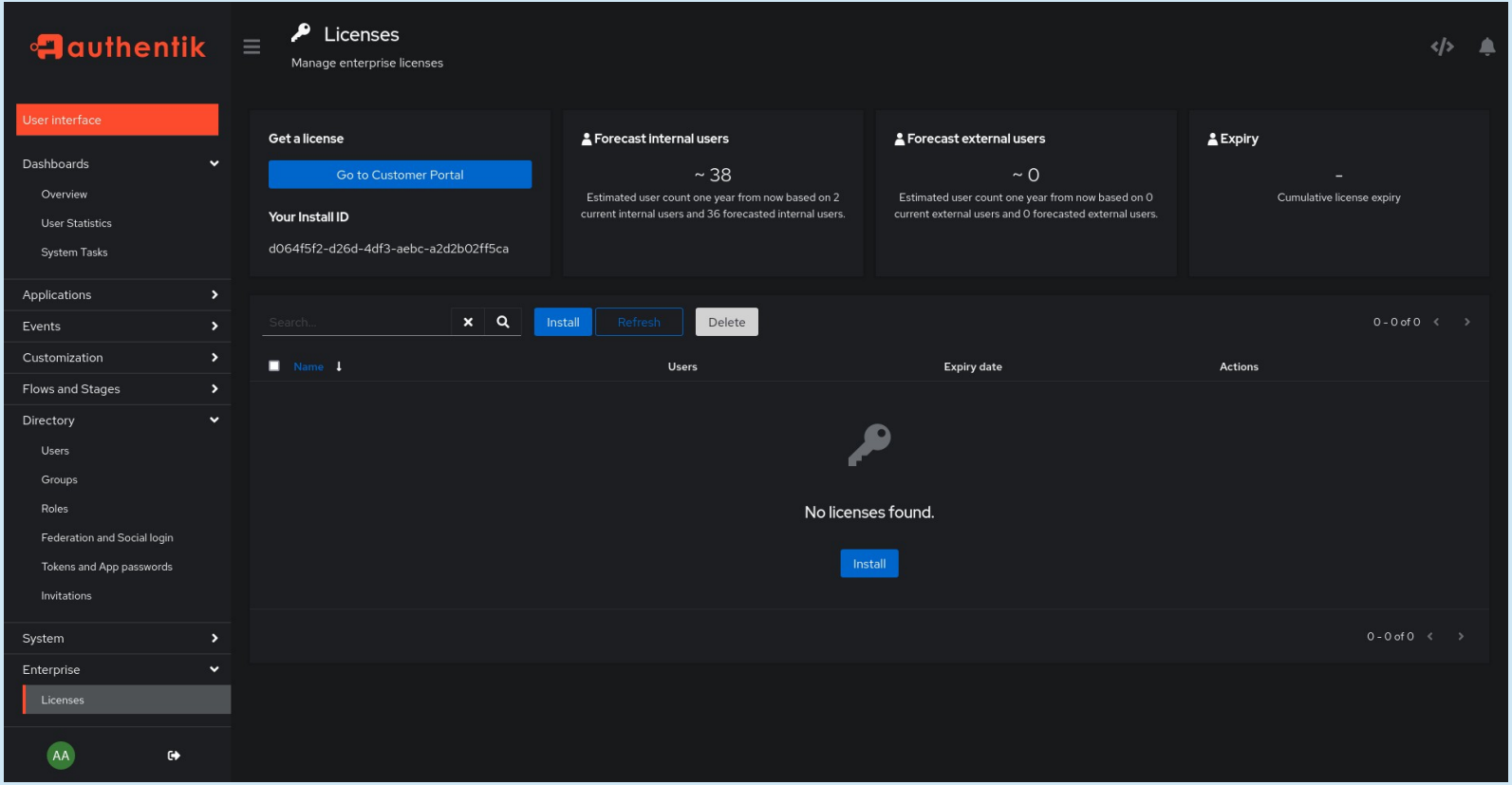


```
# extended LDIF
#
# LDAPv3
# base <cn=hsimpson,ou=users,dc=ldap,dc=ef-fr,dc=net> with scope subtree
# filter: (objectClass=user)
# requesting: ALL
#

# hsimpson, users, ldap.ef-fr.net
dn: cn=hsimpson,ou=users,dc=ldap,dc=ef-fr,dc=net
ak-superuser: FALSE
uid: f0a04414efb46853e525d63d98501eb7f4954e716108930737eeb9b6b86c5186
displayName: Homer Simpson
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: user
objectClass: posixAccount
objectClass: goauthentik.io/ldap/user
uidNumber: 2007
sn: Homer Simpson
mail: dummy@dummy.local
ak-active: TRUE
cn: hsimpson
sAMAccountName: hsimpson
gidNumber: 2007
name: Homer Simpson
homeDirectory: /home/hsimpson

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

L’offre payante d’Authentik

- Deux offres payantes d’Authentik sont disponibles, selon leur page “Pricing” :
  - Enterprise (5€ par utilisateurs par mois, paiement annuel pour 10 utilisateurs internes):
    - Un accès complet au code
    - Du support
    - Permet d’agir comme un bastion SSH/RDP (via la configuration de providers)
    - Une possibilité d’audit d’Authentik (je n’ai pas bien compris ce qu’ils voulaient faire là dessus)
    - Permet d’intégrer des sources externes d’OAuth/SAML
  - Enterprise Plus:
    - Support dédié
    - Tout ce qui est dans Enterprise
    - Des réductions si on prends énormément d’utilisateurs

L’offre payante d’Authentik



Les problèmes que j’ai rencontré

- Le déploiement de Keycloak est assez long, la configuration peut être assez fastidieuse
- Des soucis lié à de la configuration sur différents services de tests (cela ne vient pas de Keycloak ou d’Authentik)
- Keycloak a besoin d’avoir les utilisateurs et un OpenLDAP de créer proprement en amont avoir de pouvoir modifier des attributs d’utilisateurs, pouvoir créer des nouveaux groupes etc.

Ma proposition

- Keycloak :
  - Création d’une image Docker d’OpenLDAP avec des configurations propres à nous
  - Création de playbook Ansible pour créer, supprimer et gérer les utilisateurs du OpenLDAP et le tout manière automatique
  - J’ai déjà un peu commencé l’image Docker et le playbook Ansible
- Authentik :
  - Si on ne veut pas perdre de temps sur la configuration, mais on doit sortir le portefeuille

Merci :)