

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 être configuré à l'extérieur de Keycloak, celui-ci doit 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 mappé correctement.

L'interface de Keycloak

The screenshot displays the Keycloak Admin Console interface. On the left is a dark sidebar with navigation options: Manage, Clients (selected), Client scopes, Realm roles, Users, Groups, Sessions, Events, Configure, Realm settings, Authentication, Identity providers, and User federation. The main content area is titled 'Clients' and includes a subtitle: 'Clients are applications and services that can request authentication of a user. [Learn more](#)'. Below the title are three tabs: 'Clients list' (active), 'Initial access token', and 'Client registration'. A search bar with the placeholder 'Search for client' and a right arrow is present, followed by buttons for 'Create client', 'Import client', and 'Refresh'. A pagination indicator shows '1 - 7' with navigation arrows. The main table lists the following clients:

Client ID	Name	Type	Description	Home URL
account	<code>\$_client_account</code>	OpenID Connect	–	http://10.66.66.102:8080/realms/master/account/
account-console	<code>\$_client_account-console</code>	OpenID Connect	–	http://10.66.66.102:8080/realms/master/account/
admin-cli	<code>\$_client_admin-cli</code>	OpenID Connect	–	–
broker	<code>\$_client_broker</code>	OpenID Connect	–	–
grafana	grafana	OpenID Connect	grafana keycloak	http://10.66.66.102:3000/
master-realm	master Realm	OpenID Connect	–	–
security-admin-console	<code>\$_client_security-admin-console</code>	OpenID Connect	–	http://10.66.66.102:8080/admin/master/console/

At the bottom right of the table area, there is another pagination indicator showing '1 - 7' with navigation arrows.

L'interface de Keycloak

Users

Users are the users in the current realm. [Learn more](#)

User list

Default search * x → Add user Delete user Refresh 1 - 4 < >				
☐	Username	Email	Last name	First name
☐	admin		–	–
☐	hsimpson	–	Simpson	Homer Simpson
☐	jdoe		Doe	John Doe
☐	lsimpson	–	Simpson	Lisa

Un exemple d'utilisateur

Federation link ⓘ slapd local

Email verified ⓘ ☒ Yes

General

Username * lsimpson

Email

First name Lisa

Last name Simpson

modifyTimestamp 20240530143223Z

sshPublicKey ssh-ed25519 AAAAC3NzaC1lZDIINTE5AAAAIIMkF0678gOL...
ssh-ed25519 AAAAC3NzaC1lZDIINTE5AAAAIACc6Aho3OO...
[Add sshPublicKey](#)

createTimestamp 20240530143223Z

User metadata

Attributes, which refer to user metadata

LDAP_ENTRY_DN uid=lsimpson,ou=users,dc=ef-fr,dc=net

LDAP ID 2cb89ba6-b2dd-103e-9e3f-0b4e74475832

Jump to section

- General
- User metadata

```
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:: e1NTSEF9SHVTSmFud0FRTWNjR2RBcERvblJ0Z1lKRmQ4K1hBSFQ=
sshPublicKey: ssh-ed25519 AAAAC3NzaC1lZDIINTE5AAAAIIMkF0678gOLwqvtrGGNn9F57EJl
fCi4iJSsgXK/ZABQ patch@spaceint.fr
sshPublicKey: ssh-ed25519 AAAAC3NzaC1lZDIINTE5AAAAIACc6Aho300oa/W/rdy5D+1uHDQ
8MfaxhwRTALXWLiA patch@blitz
```

Configuration LDAP

General options

UI display name * ⓘ slapd local

Vendor * ⓘ Other

Connection and authentication settings

Connection URL * ⓘ ldap://10.66.66.102

Enable StartTLS ⓘ ☒ Off

Use Truststore SPI ⓘ Always

Connection pooling ⓘ ☒ Off

Connection timeout ⓘ

Test connection

LDAP searching and updating

Edit mode * ⓘ WRITABLE

Users DN * ⓘ ou=users,dc=ef-fr,dc=net

Username LDAP attribute * ⓘ uid

RDN LDAP attribute * ⓘ uid

UUID LDAP attribute * ⓘ entryUUID

User object classes * ⓘ inetOrgPerson, posixAccount, shadowAccount, ldapPublicKey

User LDAP filter ⓘ

Search scope ⓘ One Level

Read timeout ⓘ

Pagination ⓘ ☒ Off

Referral ⓘ ignore

Configuration LDAP

Synchronization settings

Import users ⓘ ☒ On

Sync Registrations ⓘ ☒ On

Batch size ⓘ

Periodic full sync ⓘ ☒ On

Full sync period ⓘ

Periodic changed users sync ⓘ ☒ On

Changed users sync period ⓘ

Kerberos integration

Allow Kerberos authentication ⓘ ☐ Off

Use Kerberos for password authentication ⓘ ☐ Off

Cache settings

Cache policy ⓘ

Advanced settings

Enable the LDAPv3 password modify extended operation ⓘ ☒ On

Validate password policy ⓘ ☒ On

Trust Email ⓘ ☒ On

[Query Supported Extensions](#)

Mapping LDAP

sshPublicKey

ID

5db0e790-fabc-4241-8d82-bf213978daf1

Name * ⓘ

sshPublicKey

Mapper type * ⓘ

user-attribute-ldap-mapper

User Model Attribute * ⓘ

▼ sshPublicKey

LDAP Attribute * ⓘ

sshPublicKey

Read Only ⓘ

☐ Off

Always Read Value From LDAP ⓘ

☐ Off

Is Mandatory In LDAP ⓘ

☐ Off

Attribute default value ⓘ

Force a Default Value ⓘ

☒ On

Is Binary Attribute ⓘ

☐ Off

Mapping LDAP

groups-mapping

ID 3b2ed1b5-e6a9-4df3-a5d7-8601bb370f34

Name * ⓘ groups-mapping

Mapper type * ⓘ group-ldap-mapper

LDAP Groups DN * ⓘ ou=groups,dc=ef-fr,dc=net

Group Name LDAP Attribute ⓘ cn

Group Object Classes ⓘ groupOfNames

Preserve Group Inheritance ⓘ ☒ On

Ignore Missing Groups ⓘ ☐ Off

Membership LDAP Attribute ⓘ member

Membership Attribute Type ⓘ DN

Membership LDAP Attribute ⓘ member

Membership Attribute Type ⓘ DN

Membership User LDAP Attribute ⓘ uid

LDAP Filter ⓘ

Mode ⓘ LDAP_ONLY

User Groups Retrieve Strategy ⓘ LOAD_GROUPS_BY_MEMBER_ATTRIBUTE

Member-Of LDAP Attribute ⓘ memberOf

Mapped Group Attributes ⓘ

Drop non-existing groups during sync ⓘ ☐ Off

Groups Path ⓘ /

Groupes

The screenshot displays the Keycloak administration console. On the left is a dark sidebar with a menu containing: Manage, Clients, Client scopes, Realm roles, Users, Groups (highlighted), Sessions, Events, Configure, Realm settings, Authentication, Identity providers, and User federation. The main content area is divided into two panels. The left panel shows a search bar for groups, an 'Exact search' checkbox, and a list of groups including 'groups' and 'users'. The right panel is titled 'Groups' and includes a description: '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](#)'. Below this is a table with columns for 'Group name' and a list of groups: 'groups' and 'users'. The interface includes various controls like search filters, pagination (1-2), and a 'Create group' button.

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

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

Group name

groups

users

1-2

Groupes

LesSimpson

Action ▼

Child groups

Members

Attributes

Role mapping

Add member

☐ Include sub-group users

⋮

Refresh

1-2 ▼ < >

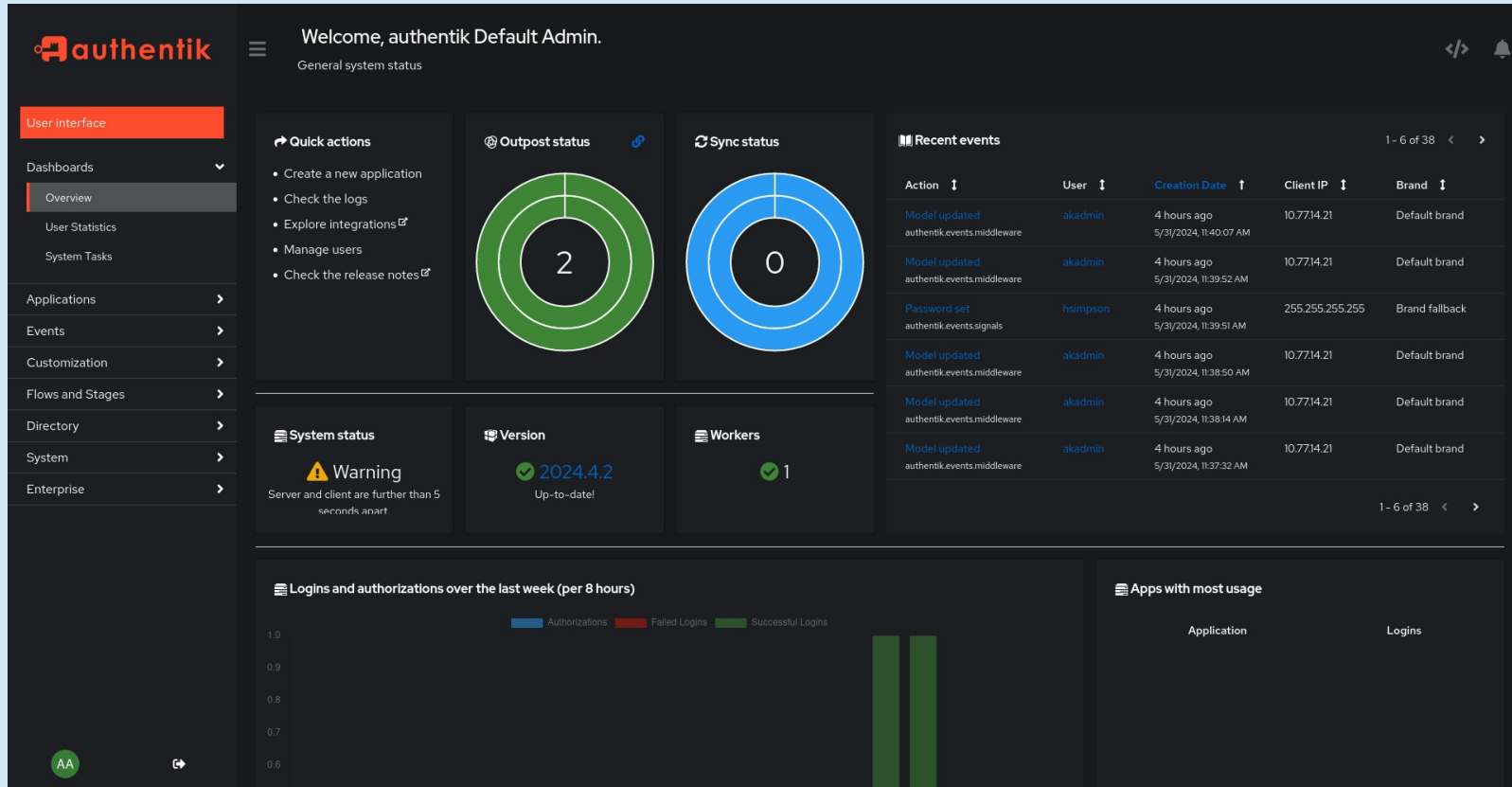
☐	Name	Email	First name	Last name	Membership	
☐	hsimpson	–	Homer Simpson	Simpson	/groups/LesSimpson	⋮
☐	lsimpson	–	Lisa	Simpson	/groups/LesSimpson	⋮

```
# 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

The screenshot displays the Authentik web interface for managing users. The interface is dark-themed with a blue header bar. The left sidebar contains a navigation menu with categories like Dashboards, Applications, Events, Customization, Flows and Stages, Directory, System, and Enterprise. The 'Users' option under the Directory category is selected. The main content area is titled 'Users' and features a 'User folders' tree on the left showing a hierarchy: Root > goauthentik.io > users. The main table lists users with columns for Name, Active status, Last login, Type, and Actions. The table shows five users: 'akadmin' (Internal), 'ldapservice' (Service account), 'ak-outpost-74ce4863a7bf478fbb550cd32251225d' (Service account (internal)), 'ak-outpost-5feb7297048946ae811cf3ffb16a6bf5' (Service account (internal)), and 'hsimpson' (Internal). Each user entry includes an 'Impersonate' button. The bottom of the interface shows a status bar with 'AA' and a refresh icon.

authentik Users

User folders

- Root
 - goauthentik.io
 - users

Search... Create Create Service account Refresh Hide deactivated user Delete

1 - 5 of 5

Name	Active	Last login	Type	Actions
akadmin authentik Default Admin	Yes	4 hours ago 5/31/2024, 11:04:39 AM	Internal	Impersonate
ldapservice <No name set>	Yes	4 hours ago 5/31/2024, 11:36:31 AM	Service account	Impersonate
ak-outpost-74ce4863a7bf478fbb550cd32251225d Outpost authentik Embedded Outpost Service-Account	Yes	-	Service account (internal)	Impersonate
ak-outpost-5feb7297048946ae811cf3ffb16a6bf5 Outpost LDAP Service-Account	Yes	-	Service account (internal)	Impersonate
hsimpson Homer Simpson	Yes	-	Internal	Impersonate

1 - 5 of 5

L'interface d'Authentik

The screenshot displays the Authentik web interface for managing groups. On the left is a dark sidebar with a navigation menu. The main content area is titled 'Groups' and includes a search bar, action buttons, and a table of existing groups.

Navigation Menu (Left Sidebar):

- User interface (highlighted)
- Dashboards
 - Overview
 - User Statistics
 - System Tasks
- Applications
- Events
- Customization
- Flows and Stages
- Directory
 - Users
 - Groups** (highlighted)
 - Roles
 - Federation and Social login
 - Tokens and App passwords
 - Invitations
- System
- Enterprise

Main Content Area: Groups

Group users together and give them permissions based on the membership.

Search: [Search...] [x] [Q] [Create] [Refresh] [Delete] 1 - 2 of 2 < >

Name ↓	Parent ↑	Members	Superuser privileges?	Actions
authentik Admins	-	1		[Edit]
ldapsearch	-	1		[Edit]

1 - 2 of 2 < >

At the bottom left of the sidebar, there is a green circle with 'AA' and a share icon.

Exemple d'utilisateur

The screenshot displays the Authentik web interface. The top navigation bar includes the Authentik logo, a hamburger menu, the user profile 'User hsimpson' (Homer Simpson), and icons for code editor and notifications. The left sidebar contains a 'User interface' section with a list of navigation items: Dashboards, Overview, User Statistics, System Tasks, Applications, Events, Customization, Flows and Stages, Directory (expanded), Users (selected), Groups, Roles, Federation and Social login, Tokens and App passwords, Invitations, System, and Enterprise. The main content area is titled 'User hsimpson' and 'Homer Simpson'. It features a tabbed interface with 'Overview' selected, and other tabs for Groups, User events, Credentials / Tokens, Applications, and Permissions. The 'Overview' tab is divided into two columns. The left column, 'User Info', lists fields: Username (hsimpson), Name (Homer Simpson), Email (dummy@dummy.local), Last login (-), Active (Yes), Type (Internal), Superuser (No), and Actions (Edit, Deactivate, Impersonate). The right column, 'Actions over the last week (per 8 hours)', contains a chart with a legend for Failed Logins (red), Successful Logins (green), and Application authorizations (blue). The chart shows a flat line at 0.0 on the y-axis (0.1 to 1.0) across the x-axis.

User Info

Field	Value
Username	hsimpson
Name	Homer Simpson
Email	dummy@dummy.local
Last login	-
Active	Yes
Type	Internal
Superuser	No

Actions

- Edit
- Deactivate
- Impersonate

Actions over the last week (per 8 hours)

Legend: Failed Logins (red), Successful Logins (green), Application authorizations (blue)

Y-axis: 0.1 to 1.0

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

The screenshot displays the 'Licenses' management page in the Authentik web interface. The left sidebar contains a navigation menu with categories like 'User interface', 'Dashboards', 'Applications', 'Events', 'Customization', 'Flows and Stages', 'Directory', 'System', and 'Enterprise'. The 'Enterprise' section is expanded, showing 'Licenses' as the active item. The main content area is titled 'Licenses' with the subtitle 'Manage enterprise licenses'. It features four summary cards: 'Get a license' with a 'Go to Customer Portal' button and an 'Your Install ID' (d064f5f2-d26d-4df3-aebc-a2d2b02ff5ca); 'Forecast internal users' showing ~38 users; 'Forecast external users' showing ~0 users; and 'Expiry' showing a cumulative license expiry date. Below these cards is a table for installed licenses. The table has columns for 'Name', 'Users', 'Expiry date', and 'Actions'. It currently shows 'No licenses found.' with an 'Install' button. The interface is dark-themed with orange accents.

authentik

Licenses
Manage enterprise licenses

Get a license

Go to Customer Portal

Your Install ID
d064f5f2-d26d-4df3-aebc-a2d2b02ff5ca

Forecast internal users
~ 38
Estimated user count one year from now based on 2 current internal users and 36 forecasted internal users.

Forecast external users
~ 0
Estimated user count one year from now based on 0 current external users and 0 forecasted external users.

Expiry
-
Cumulative license expiry

Search... [x] [Q] [Install] [Refresh] [Delete] 0 - 0 of 0 < >

Name ↓	Users	Expiry date	Actions
 No licenses found. [Install]			

0 - 0 of 0 < >

Les problèmes que j'ai rencontré

- Le déploiement de Keycloak est assez long, la configuration peut être assez fastidieuse
- Des soucis liés à 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 :)