LDAP (esup 4)

> ⚠ **Prérequis**
>
> L'annuaire LDAP doit être en ligne et joignable par le portail.

Le fichier de propriétés

filters/esup.properties

```
################################################################################
## Configuration LDAP                                                         ##
################################################################################
environment.build.ldap.url=ldaps://ldap1.univ.fr:636 ldaps://ldap2.univ.fr:636
environment.build.ldap.baseDn=ou=people,dc=univ,dc=fr
environment.build.ldap.userName=
environment.build.ldap.password=
environment.build.ldap.pooled=false
environment.build.ldap.uidAttr=uid
```

Voici à quoi correspondent les différentes propriétés :

Propriété	Définition	Valeurs
`environment.build.ldap.url`	URLs des LDAP (principal et répliquas)	Les différentes URL sont séparées par des espaces.
`environment.build.ldap.baseDn`	Nœud principal de la recherche.	L'annuaire étant compatible supAnn, cette propriété devrait être valuée à "ou=people,dc=univ,dc=fr"
`environment.build.ldap.userName`	Nom de l'utilisateur se connectant au LDAP pour faire des requêtes.	Vide si le LDAP ne requiert pas d'authentification
`environment.build.ldap.password`	Mot de passe de l'utilisateur se connectant au LDAP pour faire des requêtes	Vide si le LDAP ne requiert pas d'authentification
`environment.build.ldap.pooled`	Permet de gérer un pool de connexions.	Peut prendre les valeurs "true" ou "false" : • "false" : Le portail ne gère pas de pool de connexions au LDAP ; • "true" : Le portail gère un pool de connexions au LDAP Pool de connexion : Cache de connexions (ouvertes), ce qui permet des gains de performances car les connexions ne sont pas à ouvrir à chaque besoin
`environment.build.ldap.uidAttr`	Nom de l'attribut utilisé pour identifier l'entrée (utilisateur) de l'annuaire. Lors de la requête pour la recherche d'un utilisateur, c'est ce champ qui sera utilisé pour le discriminer.	Dans le cadre de supAnn, la valeur uid est à paramétrer

Exemples d'attributs

Voici un extrait du fichier liant les attributs supAnn avec les attributs du portail :

uportal-war\src\main\resources\properties\contexts\personDirectoryContext.xml

```
<property name="resultAttributeMapping">
    <map>
        <entry key="eduPersonPrimaryAffiliation">   <value>eduPersonPrimaryAffiliation</value><
/entry>
                ...
        <entry key="telephoneNumber">               <value>telephoneNumber</value></entry>
        <entry key="${ldap.uidAttr}">
            <set>
                <value>${ldap.uidAttr}</value>
                <value>username</value>
                <value>user.login.id</value>
            </set>
        </entry>
        <entry key="supannCodeINE">                 <value>supannCodeINE</value></entry>
                ...
        <entry key="supannorganisme">               <value>supannorganisme</value></entry>
        </map>
</property>
```

Cela signifie que la "key" (supAnn) est liée à la "value" (uPortal).

D'autre part, des liens plus complexes peuvent être générés, comme, par exemple, la valeur "${ldap.uidAttr}" de l'annuaire qui est liée à trois valeurs différentes dans uPortal : "${ldap.uidAttr}", "username" et "user.login.id".

Portlets et groupes PAGS

Les attributs utilisés par les portlets et les groupes PAGS du portail sont à déclarer dans cette configuration !

Avec des certificats (LDAPS)

Prérequis

L'annuaire en ligne doit gérer les connexions sécurisées

En plus de la configuration dans le fichier de propriétés, il faut réaliser les actions suivantes :

1. Récupérer le certificat à l'aide de la commande openssl :

```
openssl s_client -connect <IP_LDAPS>:<PORT_LDAPS>
```

Dans cette commande, <IP_LDAPS> et <PORT_LDAPS> sont idéalement les mêmes que ceux du fichier de propriétés.

Le résultat de cette commande affiche une section ressemblant à cela :

```
-----BEGIN CERTIFICATE-----
MIIBeDCCASICBgE8bQdqBDANBgkqhkiG9w0BAQUFADBCMQswCQYDVQQGEwJVUzEM
MAoGA1UEChMDQVNGMRIwEAYDVQQLEwlEaXJlY3RvcnkxETAPBgNVBAMTCEFwYWNo
ZURTMB4XDTEzMDEyNDE0NDc0N1oXDTE0MDEyNDE0NDc0N1owRzELMAkGA1UEBhMC
VVMxDDAKBgNVBAoTA0FTRjESMBAGA1UECxMJRGlyZWN0b3J5MRYwFAYDVQQDEw1G
Ui1DWkMyMDM2UDBRMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAIGEZUq5G4utdzeR
8yEq2fef8pMDUL6YDiYrtG+jsjb3iX6B8tueDGBRyeb5XAEq3Ag3uhhoBNVi/F1/
ba0GWMMCAwEAATANBgkqhkiG9w0BAQUFAANBAEv7sKnVbmbt2Jd1BDzZqSoTUnIJ
KgFM3/k+HMcSgH9UP7wPYlXVUx2jino9nFpRoLkxxGw9t5Ul+lElbGlpYEs=
-----END CERTIFICATE-----
```

Il faut copier / coller cette section ("BEGIN / END CERTIFICATE" compris) dans un fichier que l'on nommera ldap.pem, par exemple.

2. Importer ce certificat dans le magasin de la JVM :

```
keytool -import -trustcacerts -alias ldap -file [full_path_to_the.pem] -keystore "%JAVA_HOME%/jre/lib
/security/cacerts" -storepass changeit
```

Si elle s'affiche, répondre "oui" à la question de confiance.

Et pour les répliquas...

La même manipulation est à effectuer pour chacun des répliquas de l'annuaire LDAP.

Références

https://wiki.jasig.org/display/UPM40/LDAP
https://wiki.jasig.org/display/UPM40/LDAP+User+Attribute+Sources
https://www.cru.fr/documentation/supann/2009/classesattributs
https://wiki.jasig.org/display/PDM15/LDAP+Attribute+Source
Exemple de fichier de configuration