HowDoWeDoLDAP

Configurer authentic pour le LDAP LE

- Ajouter le code suivant dans /etc/authentic2-multitenant/config.py (ou /etc/authentic2/config.py pour un authentic monotenant):

```
LDAP_AUTH_SETTINGS=[
        {
            "url": "ldaps://ldap.libre-entreprise.org/",
            "basedn": "o=entrouvert,ou=companies,o=libre-entreprise",
            "user_filter": "uid=%s",
            "username_template": "{uid[0]}@{realm}",
            "groupsu": ["cn=ldapadmins,ou=groups,o=entrouvert,ou=companies,o=libre-entreprise"
],
            "groupstaff": ["cn=ldapadmins,ou=groups,o=entrouvert,ou=companies,o=libre-entrepri
se"],
            "group_filter": "(&(uniqueMember={user_dn})(objectClass=legroup))",
            "create_group": True,
            "attributes": [ "uid" ],
            "set_mandatory_groups": ["LDAP Entrouvert"]
         }
]
```

- Installer le paquet ee-ca qui contient le certificat racine de l'autorité de certification Easter-Eggs qui a produit le certificat du serveur LDAP LE
- Pour plus de sûreté on peut aussi ajouter notre copie du serveur ldaps://cresson.entrouvert.org et notre AC avec le paquet ca-certificates-entrouvert

BABA de la connexion à un LDAP

- Demander le root DSE, i.e., la description du serveur par lui même

```
ldapsearch -H ldap[s]://hostname[:port]/ -b '' -s base -x +
```

On trouvera la liste des base DN dans l'attribut namingContexts .

- Pour voir si la connexion est bloquée par des certificats tenté un ldapsearch avec LDAPTLS_REQCERT=never

Configuration

- user_filter : filtre LDAP permettant de trouver un utilisateur. Doit obligatoirement contenir au moins un **%s** qui sera remplacé par l'identifiant de l'utilisateur. Sans **%s** la tentative d'authentification est interrompue.