Parametrage

Tips: http://blog.clemanet.com/freeradius-et-openldap/

Installation freeradius et openldap

```
 # apt-get install freeradius freeradius-ldap slapd ldap-utils
```

Ajout du schema radius dans le ldap

```
# cp /usr/share/doc/freeradius/examples/openldap.schema /etc/ldap/schema/radius.schema
# echo "include /etc/ldap/schema/radius.schema" > /tmp/schema-convert
# mkdir /tmp/ldap_schema && slaptest -f /tmp/schema-convert -F /tmp/ldap_schema
```

Ouvrir le fichier /tmp/ldap_schema/cn=config/cn=schema/cn={0}radius.ldif et remplacer:

```
  dn: cn={0}radius
    objectClass: olcSchemaConfig
    cn: {0}radius
```

par:

```
  dn: cn=radius,cn=schema,cn=config
    objectClass: olcSchemaConfig
    cn: radius
```

Puis supprimer les lignes suivantes à la fin du fichier:

```
  structuralObjectClass: olcSchemaConfig
  entryUUID: d3f8dbfa-297a-1031-9222-176c711ae4e0
  creatorsName: cn=config
  createTimestamp: 20120503144845Z
  entryCSN: 20120503144845.283270Z#000000#000#000000
  modifiersName: cn=config
  modifyTimestamp: 20120503144845Z
```

```
# ldapadd -Y EXTERNAL -H ldapi:/// -f /tmp/ldap_schema/cn\=config/cn\=schema/cn\=\{0\}radius.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=radius,cn=schema,cn=config"
```

Configuration du module ldap

Editer /etc/freeradius/modules/ldap

```
server = "127.0.0.1"
  identity = "cn=admin,dc=entrouvert,dc=org"
  password = motdepassecomplique
  basedn = "dc=entrouvert,dc=org"
  filter = "(uid=%{%{Stripped-User-Name}:-%{User-Name}})"
  dictionary_mapping = ${confdir}/ldap.attrmap
```

Activation de ldap pour l'authentification

Dans le fichier /etc/freeradius/sites-available/default:

```
Section authorize {
    ...
```

```
    ldap
    ...
    }
```

puis

```
authenticate {
    ...
        Auth-Type LDAP {
            ldap
        }
    ...
    }
```

Tester la connexion

Arrêter le serveur:

```
   # service freeradius stop
```

Lancer le serveur en mode debug:

```
# freeradius -X
```

Vérifier si le serveur répond bien:

```
radtest <user> <passwd> 127.0.0.1 1 testing123
```

par exemple:

```
# radtest 99c543e03c1649de87de47044c86cce3 fef3db94593e4944a8b2cf103b890ea8  127.0.0.1 1 testing12
3
Sending Access-Request of id 98 to 127.0.0.1 port 1812
    User-Name = "99c543e03c1649de87de47044c86cce3"
    User-Password = "fef3db94593e4944a8b2cf103b890ea8"
    NAS-IP-Address = 127.0.1.1
    NAS-Port = 1
    Message-Authenticator = 0x00000000000000000000000000000000
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=98, length=20
```