Configuration de FreeRADIUS avec LDAP

membres

Salif Biaye

Ndeye Astou Diagouraga

Mouhamadou Tidiane Seck

Ouleymatou Sadiya Cissé

LDAP (Lightweight Directory Access Protocol) est un protocole qui permet d'accéder à un annuaire centralisé contenant des informations sur les utilisateurs, groupes, et autres ressources (par exemple : noms, mots de passe, permissions).

Pourquoi le coupler avec FreeRADIUS ?

On couple LDAP avec FreeRADIUS pour centraliser et gérer facilement l'authentification des utilisateurs. FreeRADIUS utilise LDAP pour vérifier les identifiants des utilisateurs et appliquer des politiques d'accès. Cela permet de simplifier la gestion des accès réseau dans des environnements avec beaucoup d'utilisateurs.

Configurations

1. Installation des paquets nécessaires

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

Cette commande permet d'installer les paquets nécessaires pour obtenir FreeRADIUS et LDAP.
Durant l'installation, on va nous demander de créer un mot de passe pour l'admin.

---

2. Configurer le module LDAP dans FreeRADIUS

```
sudo nano /etc/freeradius/3.0/mods-available/ldap
```

Définissez les paramètres du serveur LDAP :

```
server = "localhost"  # Remplacez par l'adresse de votre serveur LDAP
identity = "cn=admin,dc=dic,dc=sn"  # Utilisateur LDAP
password = "votre_mot_de_passe"
base_dn = "dc=dic,dc=sn"
```

Enlevez le `-` devant `ldap` dans la section `authorize`.

Décommentez les lignes nécessaires dans le fichier.

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

---

3. Activer le module LDAP

Créez un lien symbolique pour activer le module :

```
sudo ln -s /etc/freeradius/3.0/mods-available/ldap /etc/freeradius/3.0/mods-enabled/
```

---

4. Configurer le fichier `sites-enabled/default`

Ajoutez `ldap` dans les sections `authorize` et `authenticate`.

---

5. Redémarrer FreeRADIUS

Une fois la configuration terminée, redémarrez FreeRADIUS :

```
sudo systemctl restart freeradius
sudo systemctl status freeradius
```

---

6. Ajout d'un utilisateur dans notre annuaire LDAP

Il faut au préalable renommer le dossier `/etc/ldap/slapd.d/` :

```
cd /etc/ldap/
mv /etc/ldap/slapd.d/ /etc/ldap/slapd.d.old
updatedb
locate slapd.conf
cp /usr/share/doc/slapd/examples/slapd.conf /etc/ldap
```

Éditez le fichier `/etc/ldap/slapd.conf` et configurez les paramètres suivants :

1. Type de base de données : `hdb` , `hbm` , ou `dbm`
2. Nom de la racine ou base DN de l'annuaire (exemple : `suffix: dc=dic,dc=sn`)
3. Administrateur de l'annuaire (exemple : `rootdn: cn=admin,dc=dic,dc=sn`)
4. Mot de passe de l'administrateur (exemple : `rootpw: passer`)
5. Droits d'accès : spécifiez le DN de la personne ayant les droits de lecture/écriture.

---

7. Création de fichier LDIF et remplissage de l'annuaire

Création du fichier `racine.ldif`

```
dn : dc=dic,dc=sn
objectclass: organization
objectclass: dcobject
o:dic
dc:dic
```

Pour que LDAP prenne en compte notre fichier `racine.ldif` , saisissez la commande :

```
ldapadd -x -D "cn=admin,dc=dic,dc=sn" -W -f racine.ldif
```

Création de l'unité organisationnelle :
Créez le fichier `ou.ldif` contenant les groupes `dgi` , `info` , et `telecoms` :

```
nano ou.ldif

dn: ou=dic2,dc=dic,dc=sn
objectclass: organizationalUnit
ou:dic2

dn: ou=telecoms,ou=dic2,dc=dic,dc=sn
objectclass: organizationalUnit
ou:telecoms

dn: ou=info,ou=dic2,dc=dic,dc=sn
objectclass: organizationalUnit
ou:info

dn: ou=ia,ou=dic2,dc=dic,dc=sn
objectclass: organizationalUnit
ou:ia

dn: ou=ssi,ou=dic2,dc=dic,dc=sn
objectclass: organizationalUnit
ou:ssi
```

Puis appliquez le avec :

```
ldapadd -x -D "cn=admin,dc=dic,dc=sn" -W -f ou.ldif
```

Création du fichier `user.ldif` :

```
dn: uid=salif,ou=info,ou=dic2,dc=dic,dc=sn
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: salif
userPassword: passer
uidNumber: 2000
gidNumber: 2001
cn: salif biaye
homeDirectory: /home/astou
sn: biaye
jpegPhoto: < file:///home/astou/Documents/salif.jpg
```

Ajout de l'utilisateur avec LDAP :

```
# ldapadd -x -D "cn=admin,dc=dic,dc=sn" -W -f user.ldif
Enter LDAP Password:
adding new entry "uid=salif,ou=info,ou=dic2,dc=dic,dc=sn"
```

8 Test de l'authentification avec `radtest` :

```
# radtest salif passer localhost 0 testing123
Sent Access-Request Id 62 from 0.0.0.0:34216 to 127.0.0.1:1812 length 75
    User-Name = "salif"
    User-Password = "passer"
    NAS-IP-Address = 10.106.115.152
    NAS-Port = 0
    Cleartext-Password = "passer"
Received Access-Accept Id 62 from 127.0.0.1:1812 to 127.0.0.1:34216 length 38
    Message-Authenticator = 0x659a9da2e42ae05a5dd0294ddd3cf2cb0e
```