Simuler un serveur LDAP pour une démonstration

Pour simuler un serveur LDAP pour vos tests ou démonstrations, vous pouvez utiliser un outil comme **OpenLDAP** ou un serveur LDAP en conteneur (Docker). Voici une méthode simple et rapide pour configurer un serveur LDAP local.

---

1. Méthodes possibles

a. Installer OpenLDAP sur une machine locale

- Configuration manuelle du serveur LDAP sur votre machine.
- Utile pour un contrôle complet sur l'annuaire LDAP.

b. Utiliser un serveur LDAP Dockerisé

- Rapide à configurer et portable.
- Moins d'efforts pour la maintenance ou la suppression.

Dans cette démonstration, nous allons utiliser **Docker** pour simuler un serveur LDAP avec une image préconfigurée.

---

2. Utiliser Docker pour simuler un serveur LDAP

a. Installer Docker

Si Docker n'est pas encore installé :

- **Debian/Ubuntu** :

```
sudo apt update
sudo apt install docker.io
sudo systemctl start docker
sudo systemctl enable docker
```

- **CentOS/RHEL** :

```
sudo yum install docker
sudo systemctl start docker
sudo systemctl enable docker
```

b. Télécharger et exécuter un conteneur LDAP

Utilisez l'image Docker `osixia/openldap`, qui propose une configuration prête à l'emploi :

```
docker run -d \
  --name ldap-server \
  --hostname ldap.example.com \
  -p 389:389 -p 636:636 \
  -e LDAP_ORGANISATION="Example Organization" \
  -e LDAP_DOMAIN="example.com" \
  -e LDAP_ADMIN_PASSWORD="admin_password" \
  osixia/openldap:1.5.0
```

Explications des options :

- `--name` : Nom du conteneur Docker.
- `--hostname` : Nom d'hôte utilisé par le serveur LDAP.
- `-p 389:389` : Redirige le port 389 (LDAP).
- `-p 636:636` : Redirige le port 636 (LDAPS, sécurisé).
- `LDAP_ORGANISATION` : Nom de l'organisation pour le serveur LDAP.
- `LDAP_DOMAIN` : Domaine pour le serveur LDAP.
- `LDAP_ADMIN_PASSWORD` : Mot de passe pour l'administrateur LDAP.

c. Vérifier que le serveur fonctionne

1. Vérifiez que le conteneur est en cours d'exécution :

   ```
   docker ps
   ```

2. Vérifiez la connectivité avec `ldapsearch` (installez `ldap-utils` si nécessaire) :

   ```
   ldapsearch -x -H ldap://localhost:389 -D "cn=admin,dc=example,dc=com"
   -w admin_password -b "dc=example,dc=com"
   ```

---

3. Ajouter des utilisateurs et des groupes

a. Installer `ldap-utils`

Installez les outils pour interagir avec le serveur LDAP :

- **Debian/Ubuntu** :

  ```
  sudo apt install ldap-utils
  ```

- **CentOS/RHEL** :

```
sudo yum install openldap-clients
```

b. Créer des utilisateurs et groupes avec des fichiers LDIF

Les fichiers **LDIF** (LDAP Data Interchange Format) permettent d'ajouter des entrées au serveur LDAP.

1. **Créer un fichier LDIF pour un utilisateur** Fichier : `add-user.ldif`

```
dn: uid=john,ou=users,dc=example,dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
cn: John Doe
sn: Doe
uid: john
uidNumber: 1000
gidNumber: 1000
homeDirectory: /home/john
userPassword: john_password
```

2. **Créer un fichier LDIF pour un groupe** Fichier : `add-group.ldif`

```
dn: cn=admins,ou=groups,dc=example,dc=com
objectClass: top
objectClass: posixGroup
cn: admins
gidNumber: 1000
memberUid: john
```

3. **Importer les fichiers LDIF dans le serveur LDAP**

```
ldapadd -x -H ldap://localhost:389 -D "cn=admin,dc=example,dc=com" -w
admin_password -f add-user.ldif
ldapadd -x -H ldap://localhost:389 -D "cn=admin,dc=example,dc=com" -w
admin_password -f add-group.ldif
```

c. Vérifier les ajouts

- Recherchez l'utilisateur `john` :

```
ldapsearch -x -H ldap://localhost:389 -D "cn=admin,dc=example,dc=com"
-w admin_password -b "dc=example,dc=com" "(uid=john)"
```

- Recherchez le groupe `admins` :

```
ldapsearch -x -H ldap://localhost:389 -D "cn=admin,dc=example,dc=com"
-w admin_password -b "dc=example,dc=com" "(cn=admins)"
```

---

4. Intégrer avec Apache HTTPD

Configurer Apache pour utiliser ce serveur LDAP

Ajoutez cette configuration dans un Virtual Host Apache :

```
<VirtualHost *:443>
    ServerName secure.example.com
    DocumentRoot "/var/www/secure"

    SSLEngine On
    SSLCertificateFile "/etc/ssl/certs/example.com.crt"
    SSLCertificateKeyFile "/etc/ssl/private/example.com.key"

    <Directory "/var/www/secure">
        AuthType Basic
        AuthName "LDAP Authentication"
        AuthBasicProvider ldap
        AuthLDAPURL "ldap://localhost:389/dc=example,dc=com?uid?sub?
(objectClass=inetOrgPerson)"
        AuthLDAPBindDN "cn=admin,dc=example,dc=com"
        AuthLDAPBindPassword "admin_password"

        Require ldap-group cn=admins,ou=groups,dc=example,dc=com
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/secure-error.log
    CustomLog ${APACHE_LOG_DIR}/secure-access.log combined
</VirtualHost>
```

---

5. Tester la configuration complète

1. **Redémarrer Apache**

```
sudo systemctl restart apache2
```

2. **Accéder au site**

   - Ouvrez un navigateur et accédez à `https://secure.example.com`.
   - Une boîte de dialogue s'affichera pour demander un nom d'utilisateur et un mot de passe.

    - Connectez-vous avec :
        - Nom d'utilisateur : `john`
        - Mot de passe : `john_password`

3. **Résultats attendus**

    - Si l'utilisateur appartient au groupe `admins`, il peut accéder au site.
    - Sinon, l'accès est refusé.

---

6. Nettoyage après la démonstration

Si vous utilisez Docker, supprimez le conteneur LDAP une fois terminé :

```
docker rm -f ldap-server
```

Résumé

- **Outils utilisés** :
    - **Docker** : Pour configurer un serveur LDAP rapide et portable.
    - **ldap-utils** : Pour interagir avec le serveur LDAP.
    - **Apache HTTPD** : Pour intégrer l'authentification LDAP.