Mise en place d'un serveur d'authentification LDAP avec intégration à un intranet web

À quoi ça sert :

- Centraliser l'authentification des utilisateurs à travers un annuaire LDAP (OpenLDAP).
- Simplifier la gestion des utilisateurs en évitable la duplication de comptes sur différents services.
- Connecter un site intranet web à l'annuaire LDAP pour que les utilisateurs puissent se connecter avec leurs identifiants LDAP.
- Mettre en place une authentification sécurisée et une architecture modulaire facile à intégrer à d'autres outils (mail, messagerie, WiFi, etc.).

1) Serveur LDAP (OpenLDAP sur Ubuntu Server)

2) Serveur web (Apache2 + intranet PHP)

3) Client (poste de test utilisateur)



Nous choisissons ici de ne pas omettre la configuration d'OpenLDAP afin de pouvoir définir manuellement les paramètres de notre annuaire LDAP.

| Configuration de slapd |
|--------------------------------------------------------------------------------------------------------------|
| Si vous choisissez cette option, aucune configuration par défaut et aucune base de données ne seront créées. |
| Voulez-vous omettre la configuration d'OpenLDAP ? |
| <oui></oui> |
| |
| |

Nous renseignons ici le nom de domaine DNS fictif intranet.local, ce qui définira la base DN de notre annuaire sous la forme dc=intranet,dc=local.

| Configuration de slapd Le nom de domaine DNS est utilisé pour établir le nom distinctif de base (« base DN » ou « Distinguished Name ») de l'annuaire LDAP. Par exemple, si vous indiquez « toto.example.org » ici, le nom distinctif de base sera « dc=toto, dc=example, dc=org ». Nom de domaine : |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <0k> |
| |

Nous vérifions ici que notre annuaire LDAP a bien été initialisé avec la base dc=intranet,dc=local, confirmant que la configuration a été prise en compte.

ilyes@ilyes-VirtualBox:~\$ sudo slapcat | grep dn: dn: dc=intranet,dc=local

Nous créons maintenant un fichier base.ldif qui contiendra la structure de base de notre annuaire, notamment l'unité organisationnelle et le premier utilisateur LDAP.

nano base.ldif

Nous ajoutons maintenant une unité organisationnelle users ainsi qu'un premier utilisateur LDAP nommé ilyes, que nous utiliserons pour tester l'authentification sur notre annuaire.



Nous importons maintenant le fichier base.ldif dans notre annuaire LDAP afin de créer l'unité organisationnelle users ainsi que l'utilisateur ilyes.

```
ilyes@ilyes-VirtualBox:~$ sudo ldapadd -x -D cn=admin,dc=intranet,dc=local -W -f base.ldif
Enter LDAP Password:
adding new entry "ou=users,dc=intranet,dc=local"
```

adding new entry "uid=ilyes,ou=users,dc=intranet,dc=local"

Nous effectuons une recherche LDAP pour vérifier que l'utilisateur ilyes a bien été ajouté à l'annuaire sous l'unité organisationnelle users.



Nous installons maintenant Apache2 ainsi que PHP et les modules nécessaires pour permettre à notre serveur web de communiquer avec l'annuaire LDAP.

sudo apt install apache2 php libapache2-mod-php php-ldap -y

Nous créons maintenant la page login.php dans le répertoire web pour y développer notre formulaire d'authentification connecté à l'annuaire LDAP.

sudo nano /var/www/html/login.php

Nous développons ici un formulaire PHP qui permet de tester la connexion d'un utilisateur en s'authentifiant directement auprès de notre annuaire LDAP avec ses identifiants.



Une fois le formulaire enregistré, nous pouvons quitter et nous rendre sur la page d'authentification en entrain l'adresse ip de la machine, ici 192.168.1.50.

Nous nous trouvons maintenant en face d'une page de connexion, dans laquelle nous allons entrer les identifiants de notre utilisateur ilyes et le mot de passe choisi préalablement.

| BERRADA II | lyes 2025 | |
|------------|------------------------|--|
| | Connexion Intrenet | |
| | | |
| | Connexion LDAP reussie | |
| | ilyes | |
| | | |
| | Connexion | |
| | | |

Nous confirmons que la connexion LDAP fonctionne correctement grâce à un retour visuel clair indiquant une connexion réussie.

En conclusion, nous avons mis en place un annuaire LDAP fonctionnel et sécurisé, puis intégré un système d'authentification web à travers un formulaire PHP. Cette solution nous permet de centraliser la gestion des utilisateurs et d'assurer une connexion fiable via une interface simple.