TP LDAP avec TurnKey et Ubuntu

Auteur: JB DODEMONT

Table of Contents

1. Introduction . . . 1
2. Objectifs . . . 2
3. Prérequis . . . 3
4. Installation de TurnKey LDAP . . . 4
   4.1. Création de la VM . . . 4
   4.2. Installation . . . 4
   4.3. Accès à l'interface . . . 4
5. Découverte des Commandes LDAP . . . 5
   5.1. Tester la connexion LDAP avec `ldapsearch` . . . 5
   5.2. Ajouter une entrée avec `ldapadd` . . . 5
   5.3. Modifier une entrée avec `ldapmodify` . . . 5
   5.4. Supprimer une entrée avec `ldapdelete` . . . 6
6. Concepts LDAP : Attributs et Héritage . . . 7
   6.1. Exploration des schémas LDAP . . . 7
   6.2. Ajouter un nouvel attribut . . . 7
   6.3. Héritage d'objets . . . 7
7. Intégration avec une VM Ubuntu . . . 8
   7.1. Configuration du client LDAP . . . 8
   7.2. Configuration de `nsswitch.conf` . . . 8
   7.3. Test de connexion . . . 8
8. Gestion des sudoers via LDAP . . . 9
   8.1. Créer une OU admin . . . 9
   8.2. Associer des utilisateurs à l'OU admin . . . 9
   8.3. Configurer sudoers . . . 9
9. Prolongement : Domaine LDAP Ubuntu . . . 10
10. Conclusion . . . 11

Chapter 1. Introduction

Ce TP vous guidera à travers la configuration d'un serveur LDAP à l'aide de TurnKey Linux LDAP et son intégration avec une machine Ubuntu. Vous découvrirez les commandes `ldapadd` et `ldapmodify`, les concepts d'attributs, d'héritage, et les configurations pour permettre l'authentification des utilisateurs via LDAP.

Chapter 2. Objectifs

- Découvrir les bases du protocole LDAP.
- Utiliser les commandes principales : `ldapadd`, `ldapmodify`, et `ldapdelete`.
- Comprendre les notions d'attributs et d'héritage des objets LDAP.
- Configurer un domaine LDAP pour l'authentification sur des postes Ubuntu.
- Gérer les permissions pour que les membres d'une unité organisationnelle (OU) soient sudoers.

Chapter 3. Prérequis

- Une VM VirtualBox avec TurnKey Linux LDAP Appliance.
- Une VM Ubuntu Desktop et une VM Ubuntu Server pour les tests.
- Un réseau local configuré pour la communication entre les VMs.

Chapter 4. Installation de TurnKey LDAP

4.1. Création de la VM

- Type : Linux.
- Distribution : Debian 64 bits.
- RAM : 2 Go.
- Réseau : Configuration en "Réseau interne" avec une adresse fixe `192.168.X.2`.

4.2. Installation

1. Télécharger l'image ISO de TurnKey LDAP depuis https://www.turnkeylinux.org/ldap.
2. Monter l'ISO dans VirtualBox et démarrer la VM.
3. Suivre les étapes d'installation :
    - Définir le domaine LDAP : `dc=XYZ,dc=dom`.
    - Configurer un utilisateur admin LDAP : `cn=admin,dc=XYZ,dc=dom`.

4.3. Accès à l'interface

- Utiliser le navigateur pour accéder à Webmin : `https://192.168.X.2:12321`.

Chapter 5. Découverte des Commandes LDAP

5.1. Tester la connexion LDAP avec `ldapsearch`

Exécutez une recherche simple :

```
ldapsearch -x -LLL -H ldap://192.168.X.2 -b "dc=XYZ,dc=dom"
```

5.2. Ajouter une entrée avec `ldapadd`

Créez un fichier `user.ldif` :

```
dn: uid=jdoe,ou=users,dc=XYZ,dc=dom
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: jdoe
sn: Doe
givenName: John
cn: John Doe
displayName: John Doe
uidNumber: 10000
gidNumber: 10000
userPassword: password
homeDirectory: /home/jdoe
```

Ajoutez l'entrée avec la commande suivante :

```
ldapadd -x -D "cn=admin,dc=XYZ,dc=dom" -W -f user.ldif
```

5.3. Modifier une entrée avec `ldapmodify`

Créez un fichier `modify.ldif` :

```
dn: uid=jdoe,ou=users,dc=XYZ,dc=dom
changetype: modify
replace: displayName
displayName: Jonathan Doe
```

Appliquez la modification avec :

```
ldapmodify -x -D "cn=admin,dc=XYZ,dc=dom" -W -f modify.ldif
```

5.4. Supprimer une entrée avec `ldapdelete`

Supprimez un utilisateur avec la commande suivante :

```
ldapdelete -x -D "cn=admin,dc=XYZ,dc=dom" -W "uid=jdoe,ou=users,dc=XYZ,dc=dom"
```

Chapter 6. Concepts LDAP : Attributs et Héritage

6.1. Exploration des schémas LDAP

Listez les schémas actifs dans le serveur :

```
ldapsearch -x -LLL -H ldap://192.168.56.2 -b "cn=schema,cn=config"
```

Identifiez les attributs et les classes d'objets (`inetOrgPerson`, `posixAccount`, etc.).

6.2. Ajouter un nouvel attribut

Étendez un schéma en ajoutant un attribut personnalisé comme `preferredLanguage`.

6.3. Héritage d'objets

- Créez une nouvelle OU (exemple : `admin`) héritant de `organizationalUnit`.
- Ajoutez des utilisateurs à cette OU.

Chapter 7. Intégration avec une VM Ubuntu

7.1. Configuration du client LDAP

Installez les paquets nécessaires :

```
sudo apt update
sudo apt install libnss-ldap libpam-ldap ldap-utils nscd
```

Configurez le client LDAP : - Serveur : `ldap://192.168.X.2` - Base de recherche : `dc=XYZ,dc=dom` - DN admin : `cn=admin,dc=XYZ,dc=dom`

7.2. Configuration de `nsswitch.conf`

Modifiez le fichier `/etc/nsswitch.conf` pour inclure LDAP dans la gestion des utilisateurs :

```
passwd: files ldap
group: files ldap
shadow: files ldap
```

7.3. Test de connexion

Vérifiez les utilisateurs LDAP avec :

```
getent passwd
```

Connectez-vous avec un utilisateur LDAP :

```
su - jdoe
```

Chapter 8. Gestion des sudoers via LDAP

8.1. Créer une OU admin

Ajoutez une OU "admin" avec le fichier suivant :

```
dn: ou=admin,dc=XYZ,dc=dom
objectClass: organizationalUnit
ou: admin
```

8.2. Associer des utilisateurs à l'OU admin

Déplacez les utilisateurs dans `ou=admin`.

8.3. Configurer sudoers

Ajoutez une règle LDAP dans `/etc/sudoers` :

```
%admin ALL=(ALL) ALL
```

Tester…

Chapter 9. Prolongement : Domaine LDAP Ubuntu

1. Configurez un serveur LDAP Ubuntu (slapd).
2. Implémentez une structure similaire à celle de TurnKey LDAP.
3. Créez un script pour automatiser l’ajout d’utilisateurs.

Chapter 10. Conclusion

Ce TP permet une introduction complète au protocole LDAP et à ses cas d'usage dans un environnement réseau. Les prolongements incluent la mise en œuvre d'un domaine LDAP complet sur Ubuntu pour une gestion centralisée des utilisateurs.