TP 5 - Authentification centralisée : LDAP

Pour ce TP on se propose de mettre en place une authentification centralisée pour l'ensemble des services de l'entreprise afin de faciliter la gestion des comptes pour l'arrivée et le départ des employées. Nous donc intégrer LDAP dans :

- Authentification Unix des postes.
- Service Jenkins.
- Service redmine.
- Résolution DNS.

Rappels sur LDAP

Exercice 5.1

Quel est l'objectif du protocole LDAP ?

Exercice 5.2

Dans quel cadre est-il principalement utilisé ?

Exercice 5.3

Est-il limité à cet usage ?

Exercice 5.4

À quoi doit-on faire attention en ce qui concerne les informations habituelles que l'on place dans LDAP ?

Exercice 5.5

Donner les particularités de LDAP comparé à une base de données classique de type MySQL.

Mise en place du serveur

Exercice 5.6

Installez le serveur LDAP sur la machine virtuelle fournie (*ldap-utils* et *slapd*).

Exercice 5.7

Créez votre base de données pour votre domaine (*dc=istycorp,dc=fr*) :

```
dpkg-reconfigure -plow slapd
```

Regardez le contenu de la base actuelle avec *slapcat*. Repérez les différents éléments importants.

Exercice 5.8

Créez le schéma de votre annuaire afin de structurer les deux branches habituelles *people* et *groups*. Pour ce faire, créez un fichier du type (en remplaçant les champs nécessaires) :

```
dn: ou=people,{{TODO}}
objectClass: organizationalUnit
ou: people

dn: ou=groups,{{TODO}}
objectClass: organizationalUnit
ou: groups
```

Vous pouvez alors charger ce contenu dans LDAP avec la commande :

```
ldapadd -x -D "cn=admin,{{TODO}}" -f create-struct.ldiff -W
```

Exercice 5.9

Ajoutez un utilisateur dans la branche *people* :

```
dn: cn={{LOGIN}},{{TODO}}
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
uid: {{LOGIN}}
uidNumber: {{TODO}}
gidNumber: {{TODO}}
userPassword: {{TODO}}
gecos: {{FULL_NAME}}
loginShell: /bin/bash
homeDirectory: {{TODO}}
```

Exercice 5.10

Ajoutez un groupe (*user*) et ajoutez-y l'utilisateur précédent :

```
dn: cn={{NAME}},{{TODO}}
objectClass: top
objectClass: posixGroup
cn: {{NAME}}
memberUid: {{UID}}
gidNumber: 1000
```

Exercice 5.11

Vérifiez le bon fonctionnement de l'authentification avec cet utilisateur en listant ses informations avec une requête de type *ldapsearch* :

```
ldapsearch -x -D "cn={{USER}},{{TODO}}" -W -b"cn={{USER}},{{TODO}}"
```

Exercice 5.12

Changez le mot de passe de votre utilisateur avec la commande *ldappasswd* :

```
ldappasswd -x -D 'cn={{USER}},{{TODO}}' -W -S
```

Gestion graphique : phpldapadmin

Exercice 5.13

Afin de se faciliter la vie, il est possible d'utiliser l'interface graphique *phpldapadmin*. Installez le paquet debian et connectez vous-dessus (vérifier la redirection du port de votre VM).

Exercice 5.14

Pensez à adapter le fichier */etc/phpldapadmin/config.php* pour que l'éditeur travail sur le bon chemin LDAP (dc=....).

Exercice 5.15

Créez un deuxième utilisateur avec l'interface et ajoutez-le au groupe.

Intégration à PAM

Nous allons maintenant intégrer LDAP dans l'authentification Unix de nos postes de travail. Afin de ne pas compliquer la tâche, nous allons effectuer l'opération directeur sur la VM fournie.

Exercice 5.16

Installez les paquets nécessaires au support LDAP pour PAM et NSS : *libpam-ldapd* et *libnss-ldapd*..

Exercice 5.17

Apt-get a fait le travail pour nous, mais cherchez les lignes de configuration LDAP dans les fichiers de configuration du dossier /etc/pam.d et dans /etc/nslcd.conf.

Exercice 5.18

Configurez PAM pour qu'il crée automatiquement les dossiers utilisateurs lors de leur première authentification. Éditez le fichier */etc/pam.d/common-session* :

```
session     required      pam_mkhomedir.so skel=/etc/skel umask=0022
```

Exercice 5.19

On pourra vérifier le bon fonctionnement entre NSS et LDAP avec la commande :

```
getent passwd
```

En cas d'erreur, vous pouvez arrêter le service nslcd et lancer le démon (nslcd) à la main en mode debug (option -d) pour obtenir rapidement les messages d'erreurs.

Exercice 5.20

Vérifiez le bon fonctionnement de l'authentification vers votre utilisateur par ssh ou en local dans la VM.

Intégration à divers services

Exercice 5.21

Intégrez LDAP dans le service *Jenkins* installé sur le serveur. On fera en sorte que seuls les utilisateurs appartenant au groupe *Jenkins* soient pris en compte.

Exercice 5.22

Gérez les noms d'hôtes locaux de votre réseau avec LDAP. On pourra s'inspirer de la documentation d'Archlinux : `https://wiki.archlinux.org/index.php/LDAP_Hosts`.

Exercice 5.23

Intégrez LDAP dans le service *redmine* installé sur le serveur.

Filtrage par groupe dans PAM

Activez le filtrage pour n'autoriser l'authentification Unix que pour les utilisateurs membres du groupe *Unix*. On pourra s'aider de l'aide Debian : `https://wiki.debian.org/LDAP/PAM`.