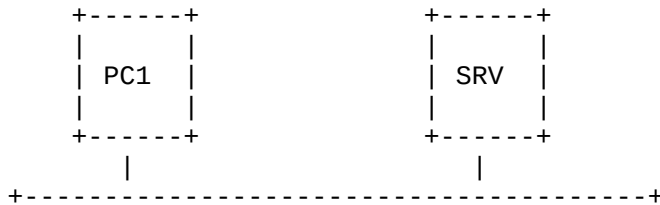


TP2 : utilisateurs et stockage

Contexte

On vous confie la responsabilité d'un serveur comprenant un annuaire LDAP et un espace de stockage partagé en NFS. L'architecture est simple : tout est sur le même LAN :



service sur la machine SRV : LDAP, NFS, DNS, WWW
répertoires home monté en NFS →

Cartographie, LDAP

Déterminer les adresses IP de SRV et PC1.
Configurer correctement la résolution de nom.
Déterminer la racine du serveur LDAP.

Import des utilisateurs

À partir du fichier "usr.csv", créer un fichier LDIF (LDAP Directory Interchange Format) puis l'importer dans l'annuaire du serveur dans la branche "ou=People,..."

Chaque utilisateur sera dans un groupe "primaire" dédié.

Ce groupe devra aussi être créé dans l'annuaire (branche "ou=Group,") et il portera comme nom le login de l'utilisateur.

Pour les uid/gid unix, générer des numéros uniques pour chaque utilisateur, dans l'ordre du fichier, en commençant à 1000

Suggestions :

- utiliser un langage de votre choix en vous aidant de modules (càd. "ne pas réinventer la roue")
- commande d'import :
`ldapadd -H ldap://nom_ou_adresse_du_serveur -D dn_de_l'admin -x -w mot_de_passe_de_l'admin -f fichier.ldif`

Exemple:

```
dn: cn=jdoe,ou=Group,...
cn: jdoe
objectclass: posixGroup
objectclass: top
gidnumber: 1000
```

```
dn: uid=jdoe,ou=People,...
objectclass: top
objectclass: inetOrgPerson
objectclass: person
objectclass: organizationalPerson
objectclass: posixAccount
objectclass: shadowAccount
cn: John Doe
sn: Doe
uid: jdoe
givenName: John
userpassword: {SSHA}H/YPhE05YT/REoiFFsoCCT6q34c+fBJp
loginshell: /bin/bash
gidnumber: 1000
uidnumber: 1000
homeDirectory: /home/jdoe !
```

Répertoires utilisateur

Le volume exporté en NFS sur la machine srv est déjà configuré. Il est situé dans /srv/home

Créer un répertoire pour chaque utilisateur (attention aux uid et gid !)

Vérifier qu'un utilisateur puisse se connecter depuis la machine PC1.

Quel mécanisme de sécurité est utilisé pour que les répertoires sur le serveur "SRV" soient accessible aux utilisateurs de PC1 ?

Affectation à des groupes secondaires

Créer deux groupes ("sales" et "eng") dans la branche "ou=Group,..." et y affecter les utilisateurs (cf. fichier "grp.csv").

NB: utiliser l'attribut multi-valué "memberuid" sous l'entrée du groupe (cf. objectClass "posixGroup").

Se déconnecter et se reconnecter sur pc1 et vérifier avec la commande "id" que le groupe secondaire est bien présent.

Création de partages

Créer sur le serveur un répertoire `"/srv/share"` et le partager en NFS (il sera monté sur `/share` au niveau du poste client). Pour cela, il est conseillé de s'inspirer des configurations existantes :

- côté serveur : fichier `"/etc/exports"` et commande `"exportfs -a"`
- côté client : fichier `"/etc/fstab"` et commande `"mount -a"`

Créer deux sous-répertoire (`"/srv/share/eng"` et `"/srv/share/sales"`) et faire en sorte qu'ils soient accessibles aux membre des groupes correspondants.

Vérifier qu'il n'est pas possible avec un compte du groupe `"sales"` de se positionner sur le répertoire partagé `"eng"`.

Authentification Apache

Rendre les 2 sous-répertoire NFS (`"eng"` et `"sales"`) accessible en HTTP mais authentifié par LDAP. Les répertoires doivent être restreints aux groupes correspondants.

Essayer de se connecter avec un navigateur web pour vérifier que les droits des utilisateurs authentifiés sont bien respectés.