Association LDAP, NFSv4 et autofs

Philippe Latu
philippe.latu(at)inetdoc.net

http://www.inetdoc.net

Résumé

Ce support reprend les deux précédents sur NFSv4 et LDAP en associant les services. Le système de fichiers réseau NFSv4 sert au partage des répertoires utilisateur tandis que l'annuaire LDAP sert au partage des attributs des comptes utilisateur et de la configuration du service d'automontage. Une fois que les deux services associés sont en place, les comptes utilisateurs peuvent être utilisés de façon transparente depuis n'importe quel poste client faisant appel à ces services.

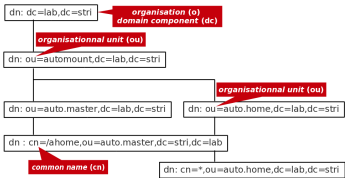


Table des matières

1. Copyright et Licence

1.1. Méta-information

Ce document est écrit avec DocBook[1] XML sur un système Debian GNU/Linux[2]. Il est disponible en version imprimable au format PDF : `sysadm-net.autofs-ldap-nfs.qa.pdf`[3].

2. Adressage IP des postes de travail

Tableau 1. Affectation des adresses IP des postes de travaux pratiques

Poste 1	Poste 2	Passerelle par défaut	Organisation
alderaan	bespin	`172.24.132.17/28`	o: zone1.lan-213.stri
centares	coruscant	`172.20.129.17/29`	o: zone2.lan-213.stri
dagobah	endor	`192.168.123.17/28`	o: zone3.lan-213.stri
felucia	geonosis	`192.168.125.49/28`	o: zone4.lan-213.stri
hoth	mustafar	`10.5.6.1/23`	o: zone5.lan-213.stri
naboo	tatooine	`172.20.136.81/28`	o: zone6.lan-213.stri

Pour chaque paire de postes de travaux pratiques, il faut attribuer les rôles de serveur et de client. Le serveur doit mettre en œuvre le service d'annuaire LDAP comprenant les propriétés des comptes utilisateurs et exporter l'arborescence du système de fichiers de ces mêmes comptes utilisateurs avec NFS. Le client doit accéder à ces ressources. Il doit permettre l'authentification auprès du serveur LDAP pour les comptes utilisateurs concernés et pouvoir monter dynamiquement à la demande le système de fichiers de ces comptes utilisateurs.

L'objectif en fin de séance de travaux pratiques est de pouvoir se connecter sur un poste client avec ses identifiants `login/password` et d'accéder à son répertoire utilisateur stocké sur le serveur de façon totalement transparente.

3. Mise en œuvre de l'annuaire LDAP

Cette partie reprend les étapes décrites dans le support Introduction aux annuaires LDAP avec OpenLDAP[4]. Il s'agit d'installer les paquets correspondants au logiciel OpenLDAP, d'initialiser une base avec le bon contexte de nommage puis d'implanter les deux unités organisationnelles et les entrées des comptes utilisateurs.

Q1. Comment installer le service d'annuaire LDAP sur le poste serveur ?

Choisir les paquets à installer et valider le bon fonctionnement du service en contrôlant la liste des processus et des numéros de ports ouverts.

[1] http://www.docbook.org
[2] http://www.debian.org
[3] http://www.inetdoc.net/pdf/sysadm-net.autofs-ldap-nfs.qa.pdf
[4] http://www.inetdoc.net/travaux_pratiques/index.html#sysadm-net.ldap

Reprendre les questions des parties Installation du serveur LDAP[5] et Analyse de la configuration du service LDAP[6]

Q2. Comment initialiser une nouvelle base et un nouveau contexte de nommage pour ce service d'annuaire ?

Réinitialiser la configuration du démon `slapd` avec le contexte de nommage défini dans la Section 2, « Adressage IP des postes de travail ».

Reprendre les questions de la partie Réinitialisation de la base de l'annuaire LDAP[7]

Q3. Comment activer la journalisation des transactions sur le service d'annuaire ?

Créer un fichier LDIF qui remplace la valeur par défaut de l'attribut `olcLogLevel` par `stats`.

Reprendre la question Comment activer la journalisation des manipulations sur les entrées de l'annuaire LDAP ?[8]

Q4. Comment implanter les deux unités organisationnelles `people` et `groups` dans le nouvel annuaire ?

Créer un fichier LDIF qui décrit la création des deux unités organisationnelles dans le bon contexte. Ajouter ces deux unités organisationnelles dans l'annuaire.

Reprendre les questions Quelle est la syntaxe du fichier LDIF qui permet d'ajouter les deux unités organisationnelles (organisational unit) ?[9] et Quelle est la commande à utiliser pour ajouter une ou plusieurs entrées dans l'annuaire ?[10]

Q5. Comment implanter les quatre comptes utilisateurs dans cet annuaire ?

Créer un fichier LDIF qui décrit la création des des quatre comptes utilisateurs dans le bon contexte avec un jeu d'attributs complet pour l'authentification et le système de fichiers. Ajouter ces comptes dans l'annuaire.

Reprendre la question Quelle est la syntaxe du fichier LDIF qui permet d'ajouter les quatre utilisateurs avec leurs attributs système ?[11]

4. Mise en œuvre de l'exportation NFS

Cette partie reprend les étapes décrites dans le support Introduction au système de fichiers réseau NFSv4[12]. Après avoir traité la partie commune de la configuration NFS, il s'agit d'installer le paquet correspondant au serveur NFS et de créer l'arborescence des comptes utilisateurs à exporter avec le bon contexte de nommage.

Q6. Comment installer et valider les services commun au client et au serveur NFS ?

Rechercher et installer le paquet puis contrôler la liste des processus et des numéros de port ouverts.

On reprend ici les questions de la partie Gestion des paquets NFS[13]

- Identification du paquet à installer.

[5] http://www.inetdoc.net/travaux_pratiques/sysadm-net.ldap.q/sysadm-net.ldap.srvr.html#sysadm-net.ldap.srvr.install
[6] http://www.inetdoc.net/travaux_pratiques/sysadm-net.ldap.q/sysadm-net.ldap.srvr.html#sysadm-net.ldap.srvr.config
[7] http://www.inetdoc.net/travaux_pratiques/sysadm-net.ldap.q/sysadm-net.ldap.srvr.html#sysadm-net.ldap.srvr.init
[8] http://www.inetdoc.net/travaux_pratiques/sysadm-net.ldap.q/sysadm-net.ldap.srvr.html#sysadm-net.ldap.srvr.q4-LogLevel
[9] http://www.inetdoc.net/travaux_pratiques/sysadm-net.ldap.q/sysadm-net.ldap.srvr.html#sysadm-net.ldap.srvr.q4-ou
[10] http://www.inetdoc.net/travaux_pratiques/sysadm-net.ldap.q/sysadm-net.ldap.srvr.html#sysadm-net.ldap.srvr.q4-ldapadd
[11] http://www.inetdoc.net/travaux_pratiques/sysadm-net.ldap.q/sysadm-net.ldap.srvr.html#sysadm-net.ldap.srvr.q4-posixAccount
[12] http://www.inetdoc.net/travaux_pratiques/index.html#sysadm-net.nfs
[13] http://www.inetdoc.net/travaux_pratiques/sysadm-net.nfs.q/sysadm-net.nfs.common.html#sysadm-net.nfs.synthese.nfs-common-package

```
# aptitude search ^nfs
v   nfs-client         -
p   nfs-common         - NFS support files common to client and server
p   nfs-kernel-server  - support for NFS kernel server
v   nfs-server         -
p   nfs4-acl-tools     - Commandline and GUI ACL utilities for the NFSv4 client
p   nfswatch           - Program to monitor NFS traffic for the console
```

- Identification des processus actifs après installation du paquet.

```
# ps aux | grep [r]pc
root      1988  0.0  0.1  18772   972 ?   Ss   Apr13   0:00 /sbin/rpcbind -w
statd     2763  0.0  0.2  22948  1128 ?   Ss   00:40   0:00 /sbin/rpc.statd
root      2769  0.0  0.0      0     0 ?   S<   00:40   0:00 [rpciod]
root      2778  0.0  0.0  31352   436 ?   Ss   00:40   0:00 /usr/sbin/rpc.idmapd
```

Q7. Quelles modifications faut il apporter au fichier de configuration des services NFS communs pour privilégier l'utilisation de la version 4 du protocole ?

Identifier le fichier de configuration et les paramètres (in)utiles pour NFSv4

Après avoir repéré le fichier `/etc/default/nfs-common`, on reprend la question sur les paramètres à éditer pour privilégier l'utilisation de la version 4 du protocole NFS[14]. On utilise le patch qui désactive le lancement du processus `rpc.statd` et impose le lancement du processus `rpc.idmapd`.

```
# diff -uBb nfs-common.dist nfs-common
--- nfs-common.dist     2011-04-14 10:50:16.000000000 +0200
+++ nfs-common  2011-04-14 10:51:33.000000000 +0200
@@ -3,7 +3,7 @@
 # for the NEED_ options are "yes" and "no".

 # Do you want to start the statd daemon? It is not needed for NFSv4.
-NEED_STATD=
+NEED_STATD=no

 # Options for rpc.statd.
 #   Should rpc.statd listen on a specific port? This is especially useful
@@ -13,7 +13,7 @@
 STATDOPTS=

 # Do you want to start the idmapd daemon? It is only needed for NFSv4.
-NEED_IDMAPD=
+NEED_IDMAPD=yes

 # Do you want to start the gssd daemon? It is required for Kerberos mounts.
 NEED_GSSD=
```

Pour appliquer le patch, les instructions sont les suivantes.

[14] http://www.inetdoc.net/travaux_pratiques/sysadm-net.nfs.q/sysadm-net.nfs.common.html#sysadm-net.nfs.common.statd.default

```
# service nfs-common stop
[ ok ] Stopping NFS common utilities: idmapd statd.
# cd /etc/default/
# patch -p0 </home/etu/nfs-common.patch
patching file nfs-common
# cat nfs-common
# If you do not set values for the NEED_ options, they will be attempted
# autodetected; this should be sufficient for most people. Valid alternatives
# for the NEED_ options are "yes" and "no".

# Do you want to start the statd daemon? It is not needed for NFSv4.
NEED_STATD=no

# Options for rpc.statd.
#   Should rpc.statd listen on a specific port? This is especially useful
#   when you have a port-based firewall. To use a fixed port, set this
#   this variable to a statd argument like: "--port 4000 --outgoing-port 4001".
#   For more information, see rpc.statd(8) or http://wiki.debian.org/SecuringNFS
STATDOPTS=

# Do you want to start the idmapd daemon? It is only needed for NFSv4.
NEED_IDMAPD=yes

# Do you want to start the gssd daemon? It is required for Kerberos mounts.
NEED_GSSD=
# service nfs-common start
[ ok ] Starting NFS common utilities: idmapd.
```

Q8. Comment installer et configurer le paquet relatif à l'exportation d'une arborescence avec le protocole NFS ?

On reprend ici les questions de la partie Configuration du serveur NFS[15]

- Identification du paquet à installer.

```
# aptitude search '?and(nfs, server)'
p   nfs-kernel-server   - support for NFS kernel server
v   nfs-server
```

- Création de l'arborescence d'exportation NFS.

```
# mkdir -p /home/exports/home
```

- Ajout des instructions d'exportation dans le fichier de configuration du serveur NFS : `/etc/exports`.

```
# grep -v ^# /etc/exports
/home/exports           198.51.100.0/24(rw,sync,fsid=0,crossmnt,no_subtree_check)
/home/exports/home      198.51.100.0/24(rw,sync,no_subtree_check)
```

Q9. Comment valider la configuration de l'exportation réalisée par le serveur NFS ?

On reprend la question sur la la commande qui permet d'identifier l'arborescence disponible à l'exportation[16].

- Côté client, on utilise la commande **showmount** suivie de l'option `-e` et de l'adresse IP du serveur à interroger.

- Côté serveur, on utilise la commande **exportfs**.

Q10. Quel est le montage local à mettre en place pour garantir la cohérence du schéma de nommage entre les postes serveur et client ?

[15] http://www.inetdoc.net/travaux_pratiques/sysadm-net.nfs.q/sysadm-net.nfs.server.html
[16] http://www.inetdoc.net/travaux_pratiques/sysadm-net.nfs.q/sysadm-net.nfs.client.html#sysadm-net.nfs.client.manual.exports

On reprend ici la question sur la distinction entre les versions 3 et 4 du protocole NFS[17] et sur le contexte de nommage.

- Création de la racine commune entre client et serveur.

```
# mkdir /ahome
```

- Montage local entre racine commune et arborescence exportée.

```
# mount --bind /home/exports/home /ahome
```

Q11. Comment créer automatiquement l'arborescence d'un utilisateur qui n'existe que dans l'annuaire LDAP ?

Rechercher les fonctions de création automatique de répertoire utilisateur dans la liste des modules PAM.

Avertissement

Cette opération se déroule en plusieurs étapes dans la mesure où il est impossible de créer un répertoire utilisateur directement depuis le client.

1. Activer l'appel au module PAM de création de répertoire utilisateur sur le serveur NFSv4.
2. Effectuer une première connexion directe sur le serveur, via SSH par exemple, permet de réaliser l'opération de création de l'arborescence initiale.
3. Toute nouvelle connexion sur un client NFSv4 utilise l'arborescence utilisateur créée lors de l'étape précédente.

Sur le serveur on complète le fichier commun de gestion de session : `/etc/pam.d/common-session`.

```
# grep -v ^# /etc/pam.d/common-session

session [default=1]                     pam_permit.so
session requisite                       pam_deny.so
session required                        pam_permit.so
session required                        pam_mkhomedir.so
session required                        pam_unix.so
session optional                        pam_ldap.so
session optional                        pam_ck_connector.so nox11
```

5. Configuration de l'automontage avec le service LDAP

Le principe de l'automontage veut que le montage d'une arborescence de système de fichiers réseau se fasse automatiquement et uniquement à l'utilisation. En effet, il n'est pas nécessaire de mobiliser les ressources du protocole NFS tant qu'une arborescence n'est pas effectivement parcourue. Dans le contexte de ce support, il n'est pas nécessaire de monter l'arborescence d'un répertoire utilisateur si celui-ci n'est pas connecté sur le poste client. On optimise ainsi les ressources du système et du réseau.

Du point de vue administration système, il est essentiel que la configuration des postes clients ne soit pas remise en question à chaque évolution du serveur ou à chaque ajout de nouveau compte utilisateur. C'est ici que le service LDAP intervient. Ce service sert à publier la configuration de l'automontage en direction des clients.

Pour appliquer ces principes, cette section doit couvrir les étapes suivantes.

- Pour compléter les informations publiées par le service LDAP, il faut ajouter un schéma spécifique à la fonction d'automontage et ensuite importer le contenu d'un fichier de description LDIF contenant les paramètres de configuration à diffuser vers les clients.

[17] http://www.inetdoc.net/travaux_pratiques/sysadm-net.nfs.q/sysadm-net.nfs.server.html#sysadm-net.nfs.server.local-mount

- Pour que le montage des arborescences soit automatique, il faut ajouter un paquet spécifique sur les systèmes clients et désigner le service LDAP comme fournisseur de la configuration. Cette désignation se fait à l'aide du Name Service Switch.

La principale difficulté dans le traitement des questions suivantes vient du fait qu'il est nécessaire d'échanger des informations entre le client et le serveur.

Dans le contexte de ce support, le service LDAP et le serveur NFS sont implantés sur le même système.

Q12. Quel est le paquet de la distribution Debian GNU/Linux qui fournit le service d'automontage via LDAP ?

Rechercher le mot clé automount dans le champ description du catalogue des paquets disponibles.

```
# aptitude search "?description(automount)"
p   autodir          - Automatically creates home and group directories for LDAP/NIS/SQL/local acc
p   autofs           - kernel-based automounter for Linux
p   autofs-hesiod    - Hesiod map support for autofs
p   autofs-ldap      - LDAP map support for autofs
p   halevt           - generic handler for HAL events
p   libamu-dev       - Support library for amd the 4.4BSD automounter (development)
p   libamu4          - Support library for amd the 4.4BSD automounter (runtime)
p   libnss-cache     - NSS module for using nsscache-generated files
p   ltspfsd          - Fuse based remote filesystem hooks for LTSP thin clients
p   nsscache         - asynchronously synchronise local NSS databases with remote directory servic
p   udisks-glue      - simple automount daemon with support for user-defined actions
```

Le paquet `autofs-ldap` correspond au besoin. On peut obtenir des informations supplémentaires en consultant sa description complète à l'aide de la commande **`# aptitude show autofs-ldap`**.

Q13. Sur quel type de poste ce paquet doit il être installé ?

Le service d'automontage est a exécuter sur le poste qui ne détient pas le système de fichiers dans lequel se trouvent les répertoires utilisateur.

Ce paquet doit être installé sur le poste client puisque le processus `automount` doit être exécuté sur ce même client. Son installation se fait simplement avec la commande usuelle **`# aptitude install autofs-ldap`**.

Q14. Quelles sont les informations relatives au service LDAP à transférer entre client et serveur ?

Pour publier la configuration de l'automontage via le service LDAP, il est nécessaire de disposer du schéma de définition des attributs dans l'annuaire. Ce schéma est fourni avec le paquet `autofs-ldap` et doit être transféré vers le serveur LDAP pour compléter le catalogue des objets qu'il peut contenir.

```
# dpkg -L autofs-ldap | grep schema
/etc/ldap/schema
/etc/ldap/schema/autofs.schema

# scp /etc/ldap/schema/autofs.schema etu@198.51.100.2:~
```

L'adresse IP utilisée dans la copie d'écran ci-dessus correspond au serveur LDAP et NFS.

Q15. Dans quel répertoire les informations transférées doivent elles être placées ?

Rechercher le répertoire de stockage des fichiers de schémas dans l'arborescence du serveur LDAP.

Une fois le fichier de schéma de transféré du client vers le serveur, celui-ci doit être placé dans l'arborescence du service LDAP avec les autres fichiers du même type.

```
# ls -lAh /etc/ldap/schema/autofs.schema
-rw-r--r-- 1 etu etu 830 sept. 27 10:29 /etc/ldap/schema/autofs.schema
```

Q16. Comment intégrer ces nouvelles informations d'automontage dans la configuration du service LDAP ?

L'intégration du nouveau schéma dans la configuration du serveur se fait en plusieurs étapes. Le fichier délivré avec le paquet `autofs-ldap` doit être converti en fichier LDIF avant d'être ajouté au DIT de configuration du démon `slapd`.

La conversion en fichier LDIF se fait à l'aide de la commande **slaptest** fournie avec le paquet `slapd`.

1. Création du répertoire de stockage du résultat de la conversion.

```
# mkdir schema-convert
```

2. Création du fichier de traitement des schémas. Comme de schéma `autofs` utilise des définitions issues des schémas de rang supérieur, il est nécessaire d'inclure les autres fichiers de schémas fournis avec le paquet.

```
# cat schema-convert.conf
include /etc/ldap/schema/core.schema
include /etc/ldap/schema/cosine.schema
include /etc/ldap/schema/inetorgperson.schema
include /etc/ldap/schema/autofs.schema
```

3. Conversion des fichiers de schémas au format LDIF.

```
# slaptest -f schema-convert.conf -F schema-convert
config file testing succeeded
```

4. Extraction des définitions utiles et formatage du résultat de la conversion. La commande ci-dessous élimine toutes les informations relatives à l'horodatage et à l'identification de l'utilisateur.

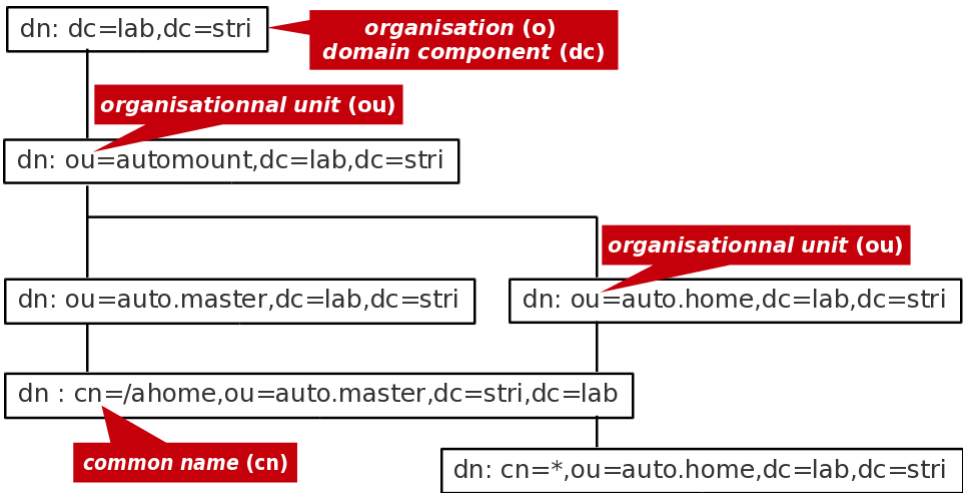
```
# cat schema-convert/cn\=config/cn\=schema/cn\=\{3\}autofs.ldif | \
egrep -v structuralObjectClass\|entryUUID\|creatorsName | \
egrep -v createTimestamp\|entryCSN\|modifiersName\|modifyTimestamp | \
sed 's/dn: cn={.}autofs/dn: cn=autofs,cn=schema,cn=config/g' | \
sed 's/{.}autofs/autofs/' > autofs.ldif
```

5. Ajout du schéma `autofs` dans la configuration du service.

```
# ldapadd -Y EXTERNAL -H ldapi:/// -f autofs.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=autofs,cn=schema,cn=config"
```

Q17. Quelle est la syntaxe du fichier de description LDIF contenant la configuration de l'automontage ?

Le fichier de description ci-dessus correspond à l'arborescence suivante.



Arborescence LDAP de l'automontage - vue complète[18]

```
# cat ou-autofs.ldif
dn: ou=automount,dc=lab,dc=stri
ou: automount
objectClass: top
objectClass: organizationalUnit

dn: ou=auto.master,ou=automount,dc=lab,dc=stri
ou: auto.master
objectClass: top
objectClass: automountMap

dn: cn=/ahome,ou=auto.master,ou=automount,dc=lab,dc=stri
cn: /ahome
objectClass: top
objectClass: automount
automountInformation: ldap:ou=auto.home,ou=automount,dc=lab,dc=stri

dn: ou=auto.home,ou=automount,dc=lab,dc=stri
ou: auto.home
objectClass: top
objectClass: automountMap

dn: cn=*,ou=auto.home,ou=automount,dc=lab,dc=stri
cn: *
objectClass: top
objectClass: automount
automountInformation: -fstype=nfs4 198.51.100.2:/home/&
```

Q18. Comment intégrer ces définitions dans l'annuaire LDAP ?

Retrouver la syntaxe de la commande **ldapadd** qui permet d'insérer de nouvelles entrées dans l'annuaire.

On suit la même démarche que pour les comptes utilisateurs.

```
# ldapadd -cxWD cn=admin,dc=lab,dc=stri -f ou-autofs.ldif
Enter LDAP Password:
adding new entry "ou=automount,dc=lab,dc=stri"

adding new entry "ou=auto.master,ou=automount,dc=lab,dc=stri"

adding new entry "cn=/ahome,ou=auto.master,ou=automount,dc=lab,dc=stri"

adding new entry "ou=auto.home,ou=automount,dc=lab,dc=stri"

adding new entry "cn=*,ou=auto.home,ou=automount,dc=lab,dc=stri"
```

6. Accès aux ressources LDAP & NFS depuis le client

Dans cette section, on suppose que l'annuaire LDAP du poste serveur est disponible et accessible. Dans un premier temps, on configure le poste client pour qu'il obtienne de façon transparente les informations sur les comptes utilisateurs desservis par l'annuaire. Dans un second temps, on complète sa configuration pour qu'il obtienne, toujours de façon transparente les informations sur le système de fichiers réseau.

Cette partie reprend les étapes décrites dans la section Configuration Name Service Switch[19] du support Introduction aux annuaires LDAP avec OpenLDAP[20].

6.1. Configuration LDAP

Q19. Quels sont les paquets de bibliothèques LDAP relatifs au mécanisme Name Service Switch et au gestionnaire d'authentification PAM ?

[18] http://www.inetdoc.net/travaux_pratiques/sysadm-net.autofs-ldap-nfs/images/ldap-automount.png
[19] http://www.inetdoc.net/travaux_pratiques/sysadm-net.ldap.q/sysadm-net.ldap.clnt.html#sysadm-net.ldap.clnt.nss
[20] http://www.inetdoc.net/travaux_pratiques/index.html#sysadm-net.ldap

Rechercher la liste des paquets dont le nom débute par `libnss`.

Les deux paquets utiles sont : `libnss-ldap` et `libpam-ldap`

Q20. Quelles sont les étapes de la configuration des paquets de bibliothèques NSS et PAM ?

Lors de l'installation des deux paquets, on passe par une série de menus debconf.

Voici un récapitulatif des réponses.

Pour le paquet `libnss-ldap` :

- URI d'accès au serveur LDAP : ldap://198.51.100.2
- Nom distinctif de la base de recherche : dc=lab,dc=stri
- Version du protocole LDAP : 3
- La base LDAP demande-t-elle une identification ? non
- Privilèges LDAP spécifiques pour le superutilisateur ? oui
- Rendre le fichier de configuration lisible et modifiable uniquement par son propriétaire ? oui
- Compte LDAP pour le superutilisateur (« root ») : cn=admin,dc=lab,dc=stri
- Mot de passe du compte du superutilisateur LDAP : *****
- Le fichier nsswitch.conf n'est pas géré automatiquement !

Pour le paquet `libpam-ldap` :

- Identifiant uniforme de ressource (« URI ») d'accès au serveur LDAP : ldap://198.51.100.2
- Nom distinctif (DN) de la base de recherche : dc=lab,dc=stri
- Version de LDAP à utiliser : 3
- Donner les privilèges de superutilisateur local au compte administrateur LDAP ? oui
- La base de données LDAP demande-t-elle une identification ? non
- Compte de l'administrateur LDAP : cn=admin,dc=lab,dc=stri
- Mot de passe du compte de l'administrateur LDAP : *****
- Algorithme de chiffrement à utiliser localement pour les mots de passe : Chiffré
- Profils PAM à activer : Unix authentication + LDAP Authentication

Q21. Quelles sont les modifications à apporter au fichier de configuration /etc/nsswitch.conf pour activer l'accès aux ressources de l'annuaire LDAP ?

Rechercher la syntaxe permettant de lancer des recherches dans l'annuaire en plus des fichiers locaux au système.

Il faut remplacer `compat` par `compat ldap` pour chaque catégorie concernée.

```
# sed -i 's/compat/& ldap/g' /etc/nsswitch.conf
```

Q22. Comment valider la configuration de l'accès à l'annuaire LDAP ?

Rechercher une commande permettant d'effectuer un appel système au bibliothèques standard `libc`.

On qualifie le mécanisme Name Service Switch à l'aide de la commande **getent**.

```
# getent passwd
root:x:0:0:root:/root:/bin/bash
<snipped/>
etu:x:1000:1000:Etudiant,,,:/home/etu:/bin/bash
padme:x:10000:10000:Padme Amidala Skywalker:/ahome/padme:/bin/bash
anakin:x:10001:10001:Anakin Skywalker:/ahome/anakin:/bin/bash
leia:x:10002:10002:Leia Organa:/ahome/leia:/bin/bash
luke:x:10003:10003:Luke Skywalker:/ahome/luke:/bin/bash
```

On qualifie l'authentication PAM à l'aide de la commande **su**.

```
$ su luke
Mot de passe :
:/home/etu$
```

6.2. Configuration NFS avec automontage

On considère que le paquet `autofs-ldap` a déjà été installé pour fournir le schéma de la partie automontage au serveur LDAP. Voir Section 5, « Configuration de l'automontage avec le service LDAP ».

Q23. Quelle est la modification à apporter au fichier de configuration /etc/nsswitch.conf pour que le démon automount accède aux ressources de l'annuaire LDAP ?

Il faut ajouter une directive supplémentaire qui spécifie l'ordre de recherche des informations pour le démon `automount`.

La syntaxe est la suivante.

```
# echo -e "\nautomount:      files ldap" >> /etc/nsswitch.conf
```

Q24. Quel est le fichier de configuration du service d'automontage dans lequel sont définis ses paramètres globaux ?

Rechercher le répertoire dans lequel sont placés les fichiers de paramétrage de tous les services.

Il s'agit du fichier `/etc/default/autofs`.

Q25. Quelles sont les modifications à apporter à ce fichier pour que le démon accède à l'annuaire LDAP et que la journalisation soit active ?

Il faut éditer le fichier avec les éléments suivants.

- Désigner l'unité organisationnelle qui contient les entrées de configuration de l'automontage
- Faire apparaître les évènements du service d'automontage dans les journaux système
- Désigner le serveur LDAP à contacter
- Spécifier le point d'entrée pour les recherches dans l'annuaire

```
# grep -v ^# /etc/default/autofs
MASTER_MAP_NAME="ou=auto.master,ou=automount,dc=lab,dc=stri"
TIMEOUT=300
BROWSE_MODE="no"
LOGGING="verbose"
LDAP_URI="ldap://198.51.100.2"
SEARCH_BASE="ou=automount,dc=lab,dc=stri"
```

Q26. Quelles sont les méthodes qui permettent de valider le fonctionnement du service d'automontage ?

Donner deux moyens d'acquérir l'identité d'un utilisateur ou d'une utilisatrice défini(e) dans l'annuaire LDAP uniquement.

ne pas oublier le consulter les journaux système pour observer les étapes de ces connexions utilisateur.

- Connexion SSH depuis un autre hôte
- Changement d'identité sur le même hôte avec la commande **su**
- Utilisation du gestionnaire de connexion graphique

7. Documents de référence

OpenLDAP Software 2.4 Administrator's Guide
: Le guide OpenLDAP Software 2.4 Administrator's Guide[21] est la référence essentielle sur le service LDAP.

Systèmes de fichiers réseau : NFS & CIFS
: Systèmes de fichiers réseau[22] : présentation des modes de fonctionnement des systèmes de fichiers réseau NFS & CIFS.

Linux NFS-HOWTO
: Linux NFS-HOWTO[23] : documentation historique complète sur la configuration d'un serveur et d'un client NFS jusqu'à la version 3 inclue.

Nfsv4 configuration
: Nfsv4 configuration[24] : traduction française extraite des pages du projet CITI de l'université du Michigan.

[21] http://www.openldap.org/doc/admin24/
[22] http://www.inetdoc.net/presentations/network-filesystems/
[23] http://nfs.sourceforge.net/nfs-howto/
[24] https://wiki.linux-nfs.org/wiki/index.php/Nfsv4_configuration_fr