Cours 2 : Gestion des utilisateurs

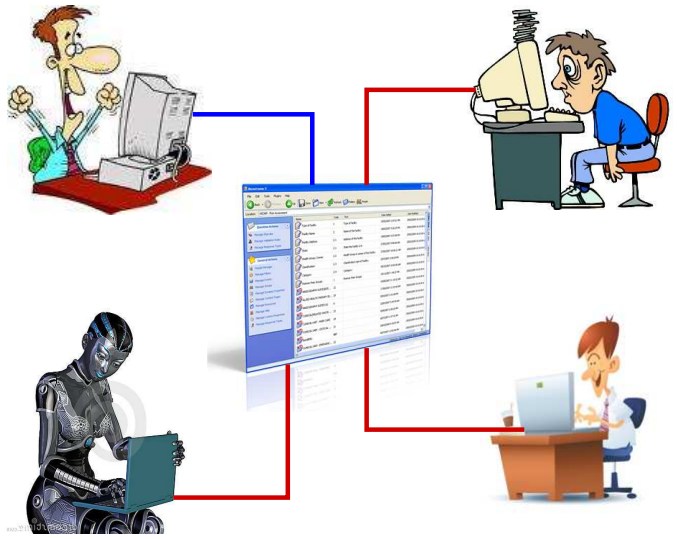
Christophe Gonzales

3I015 — Principes et pratiques de l'administration des systèmes

Plan du cours

1. Les utilisateurs sous unix/linux

De la confidentialité des données



Besoin d'identification

Identification

```
[toto@msLDAP toto]$ ls -la
total 32
drwx------. 4      503   503 4096 Feb 11 16:32 .
drwxr-xr-x. 6 root     root  4096 Feb 11 16:31 ..
-rw-r--r--. 1      503   503   18 Jun 22   2010 .bashrc
-rw-r--r--. 1 mail     mail   176 Jun 22   2010 .bashrc
-rw-r--r--. 1      502   503  124 Jun 22   2010 .xfig
drwxr-xr-x. 2      503   503 4096 Sep 29 06:15 .gnome2
drwxr-xr-x. 4 gonzales users 4096 Feb 10 11:23 .mozilla
-rw-------. 1      503   503   54 Feb 11 16:32 .xauthqXYeA1
```

Identification : par nom + nombre (ID)

Utilisateur sous unix

utilisateur

utilisateur = celui qui s'est loggué en donnant un nom de login.

utilisateur = ce login ou l'activité menée en son nom.

[J.-M. Moreno (1998) « Unix administration »]

⚠ Un utilisateur n'est pas forcément humain : mail, ftp, *etc.*

identifications

- nom de login
- identifiant numérique d'utilisateur : User ID (UID)
- identifiant numérique de groupe : GID

données associées

- home directory
- mot de passe
- le shell utilisé par l'utilisateur (bash, csh, ksh, ash, *etc.*)
- le nom long de l'utilisateur (GECOS)

Où sont stockées ces informations ?

- `/etc/passwd` :

  login, UID, GID, GECOS, home dir, shell

- `/etc/shadow` :

  mot de passe, dates de validité des mots de passe...

- `/etc/group` :

  nom des groupes, GID, listes de membres

- `/etc/gshadow` :

  mots de passe, administrateurs...

Modification des données associées (1/4)

donnée	commande
mot de passe	`passwd`
shell	`chsh`

⚠ vérifier que le shell fourni à `chsh` est valide :

```
[toto@msLDAP home]$ chsh
Changing shell for toto.
Password:
New shell [/bin/bash]: /sbin/nologin
Shell changed.
[toto@msLDAP home]$ su toto
Password:
This account is currently not available.
```

Modification des données associées (2/4)

donnée	commande
mot de passe	`passwd`
shell	`chsh`
GECOS	`chfn`

```
[toto@msLDAP gonzales]$ finger toto
Login: toto                Name: toto
Directory: /home/toto      Shell: /bin/bash
[toto@msLDAP gonzales]$ chfn -f "my real name"
Changing finger information for toto.
Password:
Finger information changed.
[toto@msLDAP gonzales]$ finger toto
Login: toto                Name: my real name
Directory: /home/toto      Shell: /bin/bash
```


Modification des données associées (3/4)

donnée	commande
mot de passe	`passwd`
shell	`chsh`
GECOS	`chfn`
groupe	`gpasswd` (administrateur)

```
[root@msLDAP gonzales]# gpasswd -A toto toto
[root@msLDAP gonzales]# exit
[toto@msLDAP gonzales]$ id gonzales
uid=500(gonzales) gid=500(gonzales)
groups=500(gonzales),504(3I015)
[toto@msLDAP gonzales]$ gpasswd -a gonzales toto
Adding user gonzales to group toto
[toto@msLDAP gonzales]$ id gonzales
uid=500(gonzales) gid=500(gonzales)
groups=500(gonzales),502(toto),504(3I015)
```


Modification des données associées (4/4)

donnée	commande
mot de passe	`passwd`
shell	`chsh`
GECOS	`chfn`
groupe	`gpasswd` (administrateur)
toutes	`usermod` (root)

```
[root@msLDAP gonzales]# id toto
uid=502(toto) gid=502(toto) groups=502(toto),504(3I015)
[root@msLDAP gonzales]# usermod -g 503 toto
[root@msLDAP gonzales]# id toto
uid=502(toto) gid=503(xxx) groups=503(xxx),504(3I015)
```


connexions/déconnexions locales, distantes

accès local :

- débuter une session : `login`
- changer d'identité : `su`
  - ⚠ `sudo` = changer d'identité le temps de l'exécution d'une commande (par ex. un shell : `sudo -s`) (voir `/etc/sudoers`)
- changer de groupe : `newgrp`
- terminer l'exécution d'un shell : `exit`
  - ⚠ `exit` dans le shell exécuté au login = logout

accès distant :

- login, exécution non sécurisés : `rlogin`, `rsh`, `rexec` ✖
- login sécurisé : `ssh` ✔

Propriété des fichiers

- par défaut, fichier $\in$ créateur, groupe du créateur

```
[toto@msLDAP ~]$ touch zzz
[toto@msLDAP ~]$ ls -l zzz
-rw-r--r--. 1 toto toto 0 Feb 12 17:30 zzz
```

- changer le groupe d'un fichier : `chgrp`

```
[toto@msLDAP ~]$ ls -l zzz
-rw-r--r--. 1 toto toto 0 Feb 12 17:30 zzz
[toto@msLDAP ~]$ id
uid=502(toto) gid=502(toto) groups=502(toto),504(3I015)
[toto@msLDAP ~]$ chgrp 3I015 zzz
[toto@msLDAP ~]$ ls -l zzz
-rw-r--r--. 1 toto 3I015 0 Feb 12 17:30 zzz
[toto@msLDAP ~]$ chgrp users zzz
chgrp: changing group of ‘zzz’: Operation not permitted
```


Propriété des fichiers

- changer le propriétaire d'un fichier : `chown`

```
[toto@msLDAP ~]$ su
Password:
[root@msLDAP toto]# ls -l zzz
-rw-r--r--. 1 toto 3I015 0 Feb 12 17:30 zzz
[root@msLDAP toto]# chown gonzales zzz
[root@msLDAP toto]# ls -l zzz
-rw-r--r--. 1 gonzales 3I015 0 Feb 12 17:30 zzz
[root@msLDAP toto]# chown toto:gonzales zzz
[root@msLDAP toto]# ls -l zzz
-rw-r--r--. 1 toto gonzales 0 Feb 12 17:30 zzz
```


2 Gestion ≪ locale ≫ des utilisateurs

Opérations de gestion

Gestion des comptes utilisateurs :

- création/modification/suppression de comptes :
  - outils graphiques (`system-config-users`)
  - commandes sous shell
  - modifications de fichiers système

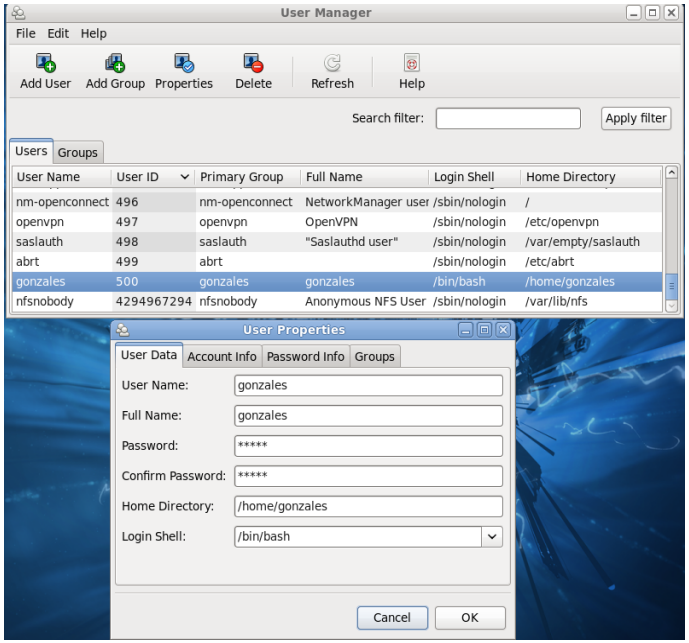
Gestion des groupes :

- création/modification/suppression des groupes :
  - outils graphiques (`system-config-users`)
  - commandes sous shell
  - modifications de fichiers système

Opérations de gestion de comptes en TME

1. création d'utilisateurs « test » avec l'outil graphique
2. création d'un utilisateur avec les commandes du shell
3. création d'un utilisateur en éditant les fichiers système

system-config-users



Les fichiers système (1/6)

- fichier des utilisateurs : `/etc/passwd`

```
[root@msLDAP toto]# tail -n 5 /etc/passwd
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
gonzales:x:500:500:gonzales:/home/gonzales:/bin/bash
vboxadd:x:492:1::/var/run/vboxadd:/bin/false
toto:x:502:503:xx:/home/toto:/bin/bash
xxx:x:503:503:my real name:/home/xxx:/bin/bash
```

champ	signification
1	nom de login
2	x = password sauvegardé ailleurs
3	UID : identifiant de l'utilisateur
4	GID : groupe par défaut
5	GECOS : description de l'utilisateur
6	home directory
7	shell pour se logguer

Les fichiers système (2/6)

- fichier des mots de passe : `/etc/shadow`

```
[root@msLDAP gonzales]# tail -n 3 /etc/shadow
vboxadd: ! !:15015:::::
toto:$6$Eks5GKAoFIfr6TLp:15016:0:99999:7:::
xxx:$6$YKvXALerFttkqcKP:15016:0:99999:7:::
```

champ	signification
1	nom de login
2	mot de passe chiffré
3-7	changements de mot de passe
8	date d'expiration du compte
9	champ réservé pour usage futur

⚠ fichier lisible (en lecture) uniquement par root !

Les fichiers système (3/6)

- fichier des groupes : `/etc/group`

```
[root@msLDAP gonzales]# tail -n 4 /etc/group
vboxsf:x:501:
toto:x:502:
xxx:x:503:gonzales
3I015:x:504:gonzales,toto
```

champ	signification
1	nom du groupe
2	mot de passe chiffré utilisé avec `newgrp`
3	GID
4	liste des membres du groupe

⚠ champ 4 = uniquement les membres dont ce n'est pas le groupe par défaut

Les fichiers système (4/6)

- fichier « caché » des groupes : `/etc/gshadow`

```
[root@msLDAP gonzales]# tail -n 4 /etc/gshadow
vboxsf:!!::
toto:!!:toto,gonzales:
xxx:!!:xxx:gonzales
3I015:$6$Eks5GKAoFIfr6TLp::gonzales,toto
```

champ	signification
1	nom du groupe
2	mot de passe chiffré pour les non membres
3	liste des administrateurs du groupe
4	liste des membres du groupe

Les fichiers système (5/6)

- configuration du package login : `/etc/login.defs`

```
#
# /etc/login.defs - Control definitions for the login package.
#

# MAIL_DIR defines the location of users mail spool files
MAIL_DIR        /var/mail

# Enable logging and display of /var/log/faillog login failure info.
FAILLOG_ENAB                yes

# Enable logging of successful logins
LOG_OK_LOGINS                no

# Enable "syslog" logging of su activity
# SYSLOG_SG_ENAB does the same for newgrp and sg.
SYSLOG_SU_ENAB                yes
SYSLOG_SG_ENAB                yes

# *REQUIRED*  The default PATH settings, for superuser and normal users.
ENV_SUPATH PATH=/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
ENV_PATH   PATH=/usr/local/bin:/usr/bin:/bin
```


Les fichiers système (6/6)

- fichiers installés à la création de comptes : `/etc/skel`

```
[root@msLDAP gonzales]# ls -la /etc/skel
total 36
drwxr-xr-x.   4 root root  4096 Feb 10 11:26 .
drwxr-xr-x. 119 root root 12288 Feb 13 10:53 ..
-rw-r--r--.   1 root root    18 Jun 22  2010 .bash_logout
-rw-r--r--.   1 root root   176 Jun 22  2010 .bash_profile
-rw-r--r--.   1 root root   124 Jun 22  2010 .bashrc
drwxr-xr-x.   2 root root  4096 Sep 29 06:15 .gnome2
drwxr-xr-x.   4 root root  4096 Feb 10 11:23 .mozilla
```

⚠ Création d'utilisateur en éditant les fichiers système
$\Longrightarrow$ ne pas oublier de recopier le contenu de l'/etc/skel !

Vérifications d'intégrité (1/2)

Intégrité des groupes : grpck

```
[root@msLDAP gonzales]# grpck
[root@msLDAP gonzales]#
[root@msLDAP gonzales]# vi /etc/group
[root@msLDAP gonzales]# tail -n 3 /etc/group
3I015:x:504:gonzales,toto,zzz
yyy:x:505:
3I015_ens:x:3000:
[root@msLDAP gonzales]# tail -4 /etc/gshadow
3I015:toto::gonzales,toto,zzz
yyy:!::
zzz:!::
3I015_ens:!::
[root@msLDAP gonzales]# grpck
no matching group file entry in /etc/group
delete line 'zzz:!::' ? y
grpck: the files have been updated
```


Vérifications d'intégrité (2/2)

Conversions group ↔ gshadow : grpconv

```
[root@msLDAP gonzales]# echo zzz:x:510: >> /etc/group
[root@msLDAP gonzales]# tail -n 2 /etc/gshadow
yyy:!::
3I015_ens:!::
[root@msLDAP gonzales]# grpconv
[root@msLDAP gonzales]# tail -n 3 /etc/gshadow
yyy:!::
3I015_ens:!::
zzz:x::
```

Intégrité des utilisateurs : pwck

Conversions passwd ↔ shadow : pwconv

Résumé sur la création par édition de fichiers système

1. ajouter l'utilisateur dans l'/etc/passwd
2. ajouter une entrée dans l'/etc/shadow
3. vérifier l'intégrité avec pwck
4. créer le répertoire de l'utilisateur et y recopier l'/etc/skel
5. en utilisant chown -R, faire en sorte que les fichiers du répertoire appartiennent à l'utilisateur et à son groupe
6. tester que tout est ok en vous loguant en tant que ce nouvel utilisateur

Outils de manipulation des fichiers système (1/6)

Créer un nouvel utilisateur : useradd

```
[root@msLDAP gonzales]# useradd titi
[root@msLDAP gonzales]# tail -n 3 /etc/passwd
toto:x:502:503:xx:/home/toto:/bin/bash
xxx:x:503:503:my real name:/home/xxx:/bin/bash
titi:x:504:505::/home/titi:/bin/bash

[root@msLDAP gonzales]# mkdir /users
[root@msLDAP gonzales]# useradd -d /users/yyy -g users
-G 3I015 yyy
[root@msLDAP gonzales]# tail -n 3 /etc/passwd
xxx:x:503:503:my real name:/home/xxx:/bin/bash
titi:x:504:505::/home/titi:/bin/bash
yyy:x:505:100::/users/yyy:/bin/bash
[root@msLDAP gonzales]# grep 3I015 /etc/group
3I015:x:504:gonzales,toto,yyy
```

Outils de manipulation des fichiers système (2/6)

Modifier un compte utilisateur : usermod

```
[root@msLDAP gonzales]# useradd zzz
[root@msLDAP gonzales]# tail -1 /etc/passwd
zzz:x:505:506::/home/zzz:/bin/bash
[root@msLDAP gonzales]# usermod -d /users/yyy
-g users -G 3I015 -s /bin/tcsh zzz
[root@msLDAP gonzales]# tail -1 /etc/passwd
zzz:x:505:100::/users/yyy:/bin/tcsh
[root@msLDAP gonzales]# grep 3I015 /etc/group
3I015:x:504:gonzales,toto,zzz
```


Outils de manipulation des fichiers système (3/6)

Supprimer un compte utilisateur : userdel

```
[root@msLDAP gonzales]# ls -a /users/yyy
.  ..  .bash_logout  .bash_profile  .bashrc  .gnome2
[root@msLDAP gonzales]# userdel yyy
[root@msLDAP gonzales]# ls -a /users/yyy
.  ..  .bash_logout  .bash_profile  .bashrc  .gnome2
[root@msLDAP gonzales]# useradd yyy
Creating mailbox file : File exists
[root@msLDAP gonzales]# ls -a /home/titi
.  ..  .bash_logout  .bash_profile  .bashrc  .gnome2
[root@msLDAP gonzales]# userdel -r titi
[root@msLDAP gonzales]# ls -a /home/titi
ls : cannot access /home/titi : No such file or directory
```


Outils de manipulation des fichiers système (4/6)

Créer un nouveau groupe : groupadd

```
[root@msLDAP gonzales]# groupadd -g 2000 3I015_ens
[root@msLDAP gonzales]# groupadd 3I015_etuds
[root@msLDAP gonzales]# tail -n 2 /etc/group
3I015_ens:x:2000:
3I015_etuds:x:2001:
```

Modifier la définition d'un groupe : groupmod

```
[root@msLDAP gonzales]# tail -n 2 /etc/group
3I015_ens:x:2000:
3I015_etuds:x:2001:
[root@msLDAP gonzales]# groupmod -g 3000 3I015_ens
[root@msLDAP gonzales]# tail -n 2 /etc/group
3I015_ens:x:3000: 3I015_etuds:x:2001:
```


Outils de manipulation des fichiers système (5/6)

Modifier les membres d'un groupe : gpasswd

```
[root@msLDAP gonzales]# tail -n 2 /etc/group
3I015_ens:x:3000:
3I015_etuds:x:2001:
[root@msLDAP gonzales]# gpasswd -M toto,xxx,zzz 3I015_etuds
[root@msLDAP gonzales]# tail -n 2 /etc/group
3I015_ens:x:3000:
3I015_etuds:x:2001:toto,xxx,zzz
[root@msLDAP gonzales]# gpasswd -d toto 3I015_etuds
Removing user toto from group 3I015_etuds
[root@msLDAP gonzales]# gpasswd -a yyy 3I015_etuds
Adding user yyy to group 3I015_etuds
[root@msLDAP gonzales]# tail -n 2 /etc/group
3I015_ens:x:3000: 3I015_etuds:x:2001:xxx,zzz,yyy
```

Outils de manipulation des fichiers système (6/6)

Supprimer un groupe : `groupdel`

```
[root@msLDAP gonzales]# groupdel 3I015_etuds
[root@msLDAP gonzales]# tail -n 2 /etc/group
zzz:x:506:
3I015_ens:x:3000:
```


Les mots de passe (1/2)

Édition des mots de passe : `passwd`

```
[root@msLDAP gonzales]# passwd zzz
Changing password for user zzz.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@msLDAP gonzales]# passwd -d zzz
Removing password for user zzz.
passwd: Success
[root@msLDAP gonzales]# echo xxxyyyzzz | passwd --stdin zzz
Changing password for user zzz.
passwd: all authentication tokens updated successfully.
```


Les mots de passe (2/2)

Modification des mots de passe en batch : `chpasswd`

```
[root@msLDAP gonzales]# chpasswd
zzz:aaabbbccc
yyy:abc12345
^D
```

Création de mots de passe chiffrés : `htpasswd`

```
[root@msLDAP gonzales]# htpasswd -nb yyy abcdef
yyy:xS7XQBM7eeZYw
```


batchs de créations d'utilisateurs

- créations/mises à jour de comptes en batch : `newusers`

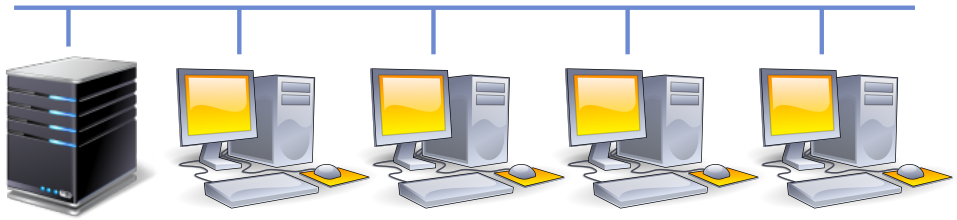
  syntaxe : `newusers fichier`
  `newusers` (lecture entrée standard)

- format d'entrée : `name:passwd:uid:gid:gecos:dir:shell`

champ	signification
name	nom de login
passwd	mot de passe non chiffré
uid	user ID
gid	group ID
gecos	GECOS
dir	home directory
shell	shell exécuté lors des connexions

3 Gestion centralisée : LDAP

Principe de LDAP

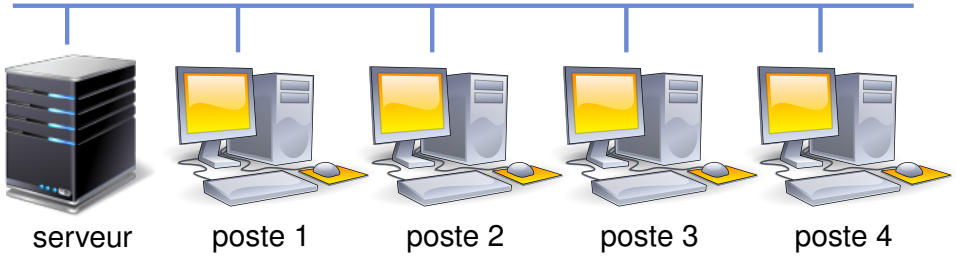


Problème : comment faire pour qu'un utilisateur soit reconnu sur chaque poste ? 2 alternatives :

1. créer une entrée dans `/etc/passwd` et `/etc/shadow` sur chaque machine
2. sauvegarder ces données sur un serveur
   $\Longrightarrow$ LDAP : Lightweight Directory Access Protocol

Architecture

Architecture client-serveur



- poste *i* demande les informations au serveur
- le serveur conserve les infos et les envoie aux postes

Principe : la centralisation

LDAP + NFS : accès transparent sur tout le réseau

Avantages de la centralisation pour l'utilisateur :

- 1 seul password sur tout le réseau
- changement de password $\Longrightarrow$ synchronisation

Avantages de la centralisation pour l'administrateur :

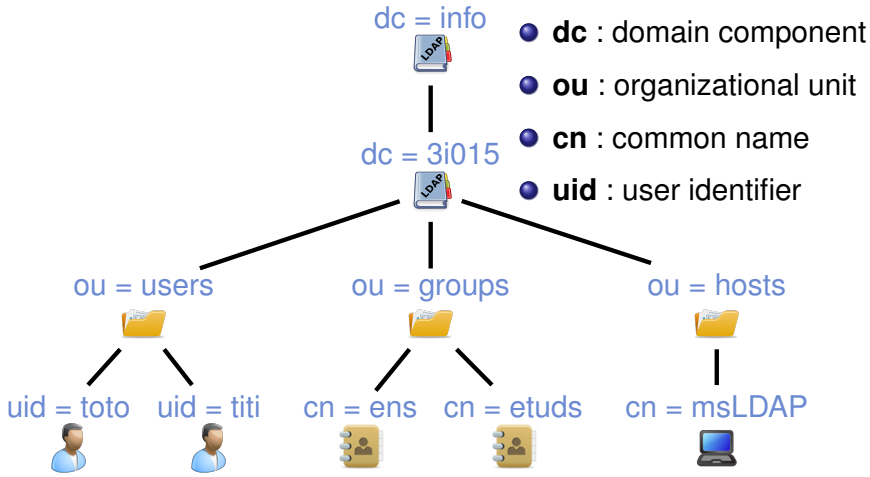
- pas de copie de passwords
- administration simple et flexible
- si plusieurs serveurs : 1 maître et des esclaves (réplication)

. . . Mais LDAP fournit d'autres services (hosts, *etc.*)

Gestion des utilisateurs par LDAP

- LDAP = annuaire $\Longrightarrow$ arborescence
- Nœud de l'arborescence = enregistrement
- Structure des enregistrements $\Longrightarrow$ schémas
- Utilisateurs $\Longrightarrow$ schéma NIS (Network Information System)

Structure d'un annuaire LDAP



- **dc** : domain component
- **ou** : organizational unit
- **cn** : common name
- **uid** : user identifier

- User toto $\Longrightarrow$ "uid=toto,ou=users,dc=3i015,dc=info"
- Schéma NIS $\Longrightarrow$ décrit les feuilles de l'arbre ci-dessus

Enregistrements de l'annuaire LDAP

- structure type d'un enregistrement d'utilisateur :

```
dn : uid=toto,ou=users,dc=3i015,dc=info
objectClass : account
objectClass : posixAccount
uid : toto
cn : toto
displayName : toto
uidNumber : 2000
gidNumber : 2000
gecos : utilisateur toto
loginShell : /bin/bash
homeDirectory : /users/toto
description : User account
```

- **dn** : distinguished name

Installation d'un serveur LDAP

- 2 packages à installer : `slapd` et `ldap-utils`
- arborescence LDAP : configurée automatiquement à partir du nom de domaine de la machine

msLDAP.upmc.fr $\Longrightarrow$ dc = fr / dc = upmc

$\Longrightarrow$ reconfiguer slapd :

```
dpkg-reconfigure slapd
```

. . . le serveur LDAP est installé

Configuration du client

- fichier de configuration : `/etc/ldap/ldap.conf`

```
BASE   dc=3i015,dc=info
URI    ldap://adresse_IP_ou_hostname_du_serveur
```

- `BASE` : haut de l'arborescence LDAP
- `URI` : adresses des serveurs LDAP

⚠ on peut indiquer plusieurs serveurs :

```
URI ldap://serveur1 ldap://serveur2
```

$\Longrightarrow$ esclaves/réplications !

Test du client

```
[root@msLDAP /]# ldapsearch -x dn
# extended LDIF
#
# LDAPv3
# base <dc=3i015,dc=info> (default) with scope subtree
# filter: (objectclass=*)
# requesting: dn

# 3i015.info
dn: dc=3i015,dc=info

# admin, 3i015.info
dn: cn=admin,dc=3i015,dc=info

# search result
search: 2
result: 0 Success

# numResponses: 3
# numEntries: 2
```


Ajout à la main d'informations dans le serveur LDAP

1. Créer un fichier au format LDIF :

```
dn: ou=groups,dc=3i015,dc=info
objectClass: organizationalUnit
ou: groups

dn: cn=ens,ou=groups,dc=3i015,dc=info
objectClass: posixGroup
cn: ens
gidNumber: 2000
description: Group account
```

2. Mettre à jour les données du serveur :

```
[root@msLDAP /]# ldapadd -x
-D cn=admin,dc=3i015,dc=info -W -f toto.ldif

adding new entry "ou=groups,dc=3i015,dc=info"
adding new entry "cn=ens,ou=groups,dc=3i015,dc=info"
```


Package ldapscripts (1/2)

- Package ldapscripts : utilitaires pour manipuler les enregistrements des utilisateurs et des groupes dans LDAP
- Configuration : `/etc/ldapscripts/ldapscripts.conf`

```
SUFFIX="dc=3i015,dc=info"   # base de l'arborescence
GSUFFIX="ou=groups"         # suffixe des groupes de users
USUFFIX="ou=users"          # suffixe des utilisateurs
MSUFFIX="ou=hosts"          # suffixe des machines
BINDDN="cn=admin,dc=3i015,dc=info"
BINDPWDFILE="/etc/ldapscripts/ldapscripts.passwd"
GIDSTART="2000"             # Group ID minimum
UIDSTART="2000"             # User ID minimum
MIDSTART="2000"             # Machine ID minimum
# User properties
# DEBIAN : values from /etc/adduser.conf are used.
CREATEHOMES="yes"
```

⚠ penser à saisir le mot de passe de l'admin LDAP dans `/etc/ldapscripts/ldapscripts.passwd`

Package ldapscripts (2/2)

- Ajouter un utilisateur :
  `ldapadduser nom_user nom_group`
- Assigner un mot de passe à un utilisateur :
  `ldapsetpasswd nom_user`
- Ajouter un groupe :
  `ldapaddgroup nom_groupe`
- Pour supprimer : `ldapdeleteuser`, `ldapdeletegroup`

⚠ Pour l'instant, seul l'annuaire LDAP est modifié !
Le système Linux ne tient pas encore compte du LDAP.

Comment utiliser LDAP pour l'authentification ?

- 2 mécanismes à combiner :
  - **PAM** : Pluggable Authentication Modules
    Gère toute l'authentification sous Linux
  - **NSS** : Name Service Switch
    Permet de remplacer les fichiers de configuration `/etc/passwd`, `/etc/shadow`, `/etc/hosts`, *etc.*, par divers mécanismes
- Installer le package `libnss-ldap` pour déployer ces 2 mécanismes

Pluggable Authentication Modules (PAM)

- PAM = implantation de mécanismes d'authentification
  séparés de leur invocation dans les programmes
- support PAM dans un programme $\Longrightarrow$ compilation spéciale
- mécanismes d'authentification = librairies dynamiques appelées modules PAM :

```
[root@msLDAP /]# ls /lib/x86_64-linux-gnu/security/
pam_access.so   pam_localuser.so   pam_rootok.so
pam_deny.so     pam_loginuid.so    pam_rootok.so
pam_env.so      pam_mail.so        pam_securetty.so
pam_exec.so     pam_mkhomedir.so   pam_selinux.so
pam_group.so    pam_nologin.so     pam_systemd.so
pam_ldap.so     pam_permit.so      pam_time.so
```

- `/etc/pam.d/` $\Longrightarrow$ règles d'authentification pour chaque prog

Règles d'authentification

4 groupes d'identification

- account : vérifie si le compte demandé est disponible (teste si expiration, autorisation de connexion à cette heure de la journée, etc.)
- auth : assure l'authentification réelle (check du nom d'utilisateur, mot de passe, etc), accorde des privilèges, définit des « certificats d'identité » (kerberos).
- password : permet de mettre à jour le jeton d'authentification (en général un mot de passe), soit parce qu'il a expiré, soit parce que l'utilisateur veut le modifier.
- session : met en place et ferme la session de l'utilisateur. Il lui fournit certaines ressources et certains services, par exemple en montant son répertoire personnel, en rendant sa boîte aux lettres disponible, etc.

Pour chaque groupe, on indique les modules PAM à réaliser.

Configuration LDAP pour PAM

- `dpkg-reconfigure libpam-ldap`

  Met à jour automatiquement les fichiers :
  - /etc/pam.d/common-account
  - /etc/pam.d/common-session
  - /etc/pam.d/common-auth
  - /etc/pam.d/common-passwd

Configuration NSS : `/etc/nsswitch.conf`

nsswitch : Name Service Switch

Service $\Longrightarrow$ accès à partir de plusieurs bases :

- ldap : accès par serveur LDAP
- dns : accès par serveur DNS
- file : accès par fichier système
- compat : compatibilité avec d'anciens formats

Principe : pour chaque service, spécifier l'ordre d'accès :

```
passwd :  files ldap
hosts :   files ldap dns
...
```


NSS : accès au LDAP

- Dans `/etc/nsswitch.conf` :

  `passwd : files ldap`

  $\Longrightarrow$ lecture passwd $\Longrightarrow$ lecture LDAP

  $\Longrightarrow$ comment accéder aux données de LDAP ?

- Fichier `/etc/libnss-ldap.conf` :

```
# The distinguished name of the search base.
base dc=3i015,dc=info
# Another way to specify your LDAP server
uri ldap://adresse_IP_ou_hostname_du_serveur_LDAP
# The distinguished name to bind to the server with
# if the effective user ID is root. Password is
# stored in /etc/libnss-ldap.secret (mode 600)
rootbinddn cn=admin,dc=3i015,dc=info
```

- Fichier `/etc/libnss-ldap.secret` : mot de passe admin LDAP
- `dpkg-reconfigure libnss-ldap` met à jour ces fichiers !

Pérennisation

- Avant pérennisation, vérifier que tout fonctionne bien en se connectant en tant qu'utilisateur ajouté avec `ldapadduser`
- Vérifier `/etc/default/slapd` :

  `SLAPD_SERVICES` doit contenir

  "`ldap://adresse_ip_du_serveur_LDAP`"

- `systemctl enable slapd`

Quelques lectures. . .

- Le Network Administration Guide :
  `http://tldp.org/LDP/nag2/index.html`
- Page générale sur les annuaires LDAP :
  `https://fr.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol`
- Installation d'un serveur LDAP sous ubuntu :
  `https://help.ubuntu.com/lts/serverguide/openldap-server.html`
- Installation d'un serveur LDAP sous debian :
  `https://www.server-world.info/en/note?os=Debian_8&p=openldap`