Gestion des utilisateurs et des groupes

- **useradd** : ajout d'un utilisateur (pas de création des repertoires).
- **usermod** : modification d'un utilisateur.
- **userdel** : suppression d'un utilisateur.
- **adduser** : ajout d'un utilisateur de manière interactive.
- **groupadd** : ajout d'un groupe.
- **groupmod** : modification d'un groupe.
- **groupdel** : suppression d'un groupe.
- **grpck** : vérifier le fichier group.
- **pwck** : vérifie le fichier passwd.
- **finger** : affiche les info d'un user.
- **passwd** : modifie le mots de passe .
- **su** : se connecte en tant u'utilisateur via la console.
- **id** : affiche les info de la personne connecter.
- **groups** : liste des groupes d'un utilisateur.

Exemples :
useradd stagex
useradd toto -u 800 -g 520 -G gr1,grp2 -s /bin/bash –e 12/23/2011
passwd stagex
passwd -l pass : désactive le compte
passwd -u pass : réactive le compte
userdel -r totox
-r supprime aussi le rép personnel et les fichiers de l'utilisateur.
usermod –G stagiaire,prof totox
-G ajoute stagex dans les 2 groupes stagiaire et profs (qui existent).

groupadd stagiaire
groupdel totox
lister tous les groupes d'un utilisateur : **groups stagex**

Pour ajouter un utilisateur à un groupe : éditer le fichier **/etc/group** et d'ajouter une liste d'utilisateurs (séparés par des virgules) sur la ligne du groupe.

Note :
> Les infos et authentification des utilisateurs est dans **/etc/passwd**
> La gestion des groupes est assurée par **/etc/group**
> Les mpasse cryptés sont dans **/etc/shadow**, lisible que par **root**.

Structure de *:etc/passwd :*
login:x:uid:gid:commentaires:home:shell
Structure de *:etc/group :*
groupe:x:gid:liste-groupes-secondaires
Numeroutilisateur & numerodegroupe >=500

Gestion des droits

Chmod : changer le mode d'exécution.
Chown : changer le propriétaire.
Chgrp : changer le groupe.

Gestion de processus

En avant plan : Emacs, pour récupérer la main : Ctrl+Z et tappez bg, pour le tuer CTRL+C dans le terminal.
En tache de fond : Emacs &, pour passer en foreground tapez fg

Mise en place de quotas

"soft" : il s'agit d'une tolérance, cette limite peut être franchie.
"hard" : franchie par un utilisateur ou un groupe, celui-ci ne peut plus écrire sur le disque, tant qu'elle est dépassée.

Installation avec : **urpmi quota**
Liste des fichiers installés : **rpm –qil quota**
Prise en compte de la gestion des quotas : modifier **/etc/fstab**
/dev/… ext3 defaults,usrquota,grpquota 1 2
Remonter la partition sans redémarrage: **mount –o remount –force**
Initialiser les tables de quotas : **quotacheck /dev/hda1**
Attribuer des limites : **edquota –u utilisateur**

quotaon/quotaoff partition|-a : active/désactive les quotas sur la|toutes partition(s)
repquota –a : affiche un rapport complet par utilisateur et par groupe
quota -v toto : état des quotas pour l'utilisateur
quotacheck <partition> : Met à jour les tables de quotas. Lancé à chaque démarrage
edquota -u toto| -g groupe : Edition sous vi des limites utilisateur ou groupe
edquota -p toto liste : Impose les quotas de toto aux membres de la liste
edquota –t : Edition sous vi de la durée de la "grace"

Note : Pour attribuer les mêmes quotas à tout un ensemble d'utilisateurs, il n'est pas question de les traiter un par un avec ***edquota –u,*** L'option **-p** de **edquota** permet de proposer un utilisateur comme modèle à tous les autres. La ligne de commande suivante est souvent adoptée :
edquota -p toto `awk -F: '$3 >500 {print $1}' /etc/passwd `

Initialisation du syteme

Gestion des services : Dans **/etc/rc.d/init.d** on trouve des scripts permettant de lancer des services (daemons). On peut activer | désactiver | redémarrer | voir l'état d'un service :

/etc/rc.d/init.d/ start
/etc/rc.d/init.d/ stop
/etc/rc.d/init.d/ restart
/etc/rc.d/init.d/ status

Dans chaque distribution linux on trouve dans **/etc/inittab** les différents niveaux d'exécution (runlevel) et leurs utilités.
Exemple mandriva:
 # 0 - halt
 # 1 - Single user mode
 # 2 - Multiuser, without NFS
 # 3 - Full multiuser mode
 # 4 - unused
 # 5 - X11
 # 6 - reboot

Dans le répertoire **/etc/** se trouve les répertoires **rc0.d, rc1.d, rc2.d, rc3.d, rc4.d, rc5.d, rc6.d**. Ils correspondent chacun à un runlevel.

Exemple : En listant le répertoires rc3.d avec la commande ls
K10webmin@
S10network@
S99local@
S11portmap@

S pour Start, K pour Kill. Le chiffre précise le niveau d'ordre d'exécution (ici le service network et activé avant portmap). La présence de @ veut dire que c'est un lien qui pointe vers fichier, dans notre cas le service pointe vers le script qui active le démon dans le répertoire **/etc/rc.d/init.d**

Pour que le script soit pris en compte par **chkconfig**, on doit :
Ajouter les lignes :
 # chkconfig : 2345 99 00
 # decription : mon script bla bla
Copier le script dans **/etc/init.d** :
cp monscript /etc/init.d/monscript

chkconfig –level 0123456 daemons on|on|reset

Installation de paquet

Urpme : enlever des paquets.
Urpmi : installer des paquets.
Urpmq : rechercher des paquets.
Urpmf : rechercher un fichier dans les paquets.

Serveur NFS

Paquets **portmap- ..** et **nfs-utils : urpmi nfs-utils**

Le fichier **/etc/exports** contient la liste des exportations.

Pour valider un changement opéré dans ce fichier de configuration, exécuté la commande : **exportfs -a**

Montage dans le client : **mount -t nfs nom-machine:arborescence point-montage**

Automatisation du montage : Pour cela, il suffit d'ajouter le contenu de la commande précédente dans une ligne du fichier /etc/fstab : **p01:/home/httpd /mnt/nfs nfs auto, user**

Serveur NIS

Installer **ypserv** sur le serveur et **ypbind** et **yp-tools** sur le client
L'installation va créer des fichiers dans :

/usr/sbin, notamment les serveurs ypserv et rpc.yppasswd,
/etc/rc.d/init.d/, les scripts de contrôle ypserv et yppasswd des serveurs
/etc/ypserv.conf, le fichier de configuration du serveur
/var/yp, place des cartes et du fichier Makefile qui permet leur génération
/usr/lib/yp, autres exécutables.

Lancement ou à l'arrêt manuel de NIS

/etc/rc.d/init.d/portmap start
/etc/rc.d/init.d/ypserv start
/etc/rc.d/init.d/yppasswd start

Note: Si cela n'a pas été fait lors de l'installation des paquetages, activer le lancement de ces services au prochain redémarrage de la machine, à l'aide de l'utilitaire **ntsysv**, en cochant ces 2 programmes.

Configuration du serveur:

✓ Déclaration du domaine NIS

domainname Nom

Editer le fichier **/etc/sysconfig/network**, et y ajouter cette ligne : **NISDOMAIN ="** Nom**"**

Relancer le serveur par **/etc/rc.d/init.d/ypserver restart**

Vérifier que la commande **domainname** nous donne le même nom de domaine spécifié.

✓ Informations gérer par NIS

Editer le fichier **/var/yp/Makefile** et lister sur la ligne commençant par all: les données à gérer :

all: passwd shadow group hosts

✓ Générer les cartes

Création des 4 cartes (maps) correspondant aux 4 fichiers /etc/passwd, /etc/shadow, /etc/group et /etc/hosts.

L'utilitaire **/usr/bin/make** doit être exécuté par root dans le répertoire du Makefile

cd /var/yp
make

Note: Il y a création d'un sous-répertoire **/var/yp/**Nom contenant les 6 fichiers binaires de permissions 600 : *hosts.byname, hosts.byaddr, passwd.byname, passwd.byuid, group.byname et group.bygi.*

✓ Autorisation d'accès

Préciser les machines autorisées à accéder au service NIS dans le fichier **/var/yp/securenets**

#permettre l'accès sur le serveur même
255.0.0.0 127.0.0.0
#permettre l'accès de toutes les machines du sous-réseau
255.255.255.0 10.177.240.0
#permettre l'accès à tout le monde
0.0.0.0 0.0.0.0

✓ Option d'accès

Editer **/etc/ypserv.conf**

Syntaxe : hôte : domaine : map : sécurité

Note : Sécurité :
none : toujours permettre l'accès
port : accès seulemtn si le port client < 1024
deny : pas d'accès à la map

✓ Relancer le serveur

/etc/rc.d/init.d/ypserv restart

Le serveur devrait être fonctionnel. Vérification :

Note : **ypcat –x** : liste des maps disponibles
ypcat hosts.byname : lecture d'une map.

Configuration du client:

✓ Installation et lancement

Les paquetages à installer sont d'abord **ypbind**, puis **yp-tools**

Avec l'utilitaire **ntsysv**, on peut activer NIS au démarrage en cochant **ypbind**, programme exécuté sur le client, ainsi que **portmap**

Pour lancer à la main les services passer les 2 commandes dans l'ordre

/etc/rc.d/init.d/portmap start *(exécute rpc.portmap)*
/etc/rc.d/init.d/ypbind start

✓ Configuration

- Dans **/etc/sysconfig/network**, comme sur le serveur il faut déclarer le nom du domaineNIS **NISDOMAIN = "**Nom**"**
- Editer **/etc/yp.conf**, ajouter les 2 lignes

Spécification du serveur : nom d'hôte ou adresse ip
ypserver nisserver
Serveur qui gère le domaine NIS Nom
domain Nom **server 10.177.240.1**

✓ Sélection des maps

Editer **/etc/nsswitch.conf**, principe : pour chaque service, spécifier l'ordre d'accès.

nis : accès par serveur NIS.
dns : accès par serveur DNS.
file : accès par fichier système.

✓ Relancer le client

En ligne de commande, (re)lancer le service client. On devrait obtenir 2 messages : recherche d'un domaine NIS, puis tentative de liaison à un serveur NIS.

/etc/rc.d/init.d/ypbind start
Binding to the NIS domain: [OK]
Listening for an NIS domain server: nisserver

Note : yppasswd toto, permet à toto de changer son mot de passe. Cela provoque la mise à jour usuelle dans /etc/shadow, mais biensûr doit mettre à jour les maps en relançant /usr/bin/make

Une station cliente NIS ne devrait pas héberger des comptes locaux (bien sûr à part root).

Serveur DNS

Installation de Bind 9 :

apt-get install bind9

Fichier de configuration principale :

le Fichier **/etc/bind/named.conf** contient la liste des zones (domaines) que le serveur DNS doit prendre en charge

gedit /etc/bind/named.conf

```
zone "Nom.org" {
    type master ;
    file "/etc/bind/db.ouahabi.org" ;
    };
```

- Nom.org : Nom de la zone à prendre en charge
- type master : notre serveur est le serv principal du domaine
- file "/etc/bind/db. Nom.org " : chemin du fichier qui contiendra la correspondance entre les noms et les adresses IP pour ce domaine.

Résolution inverse (trouver le nom à partir de l'adresse IP)

```
zone "0.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db. Nom.org.inv";
        };
```

- 0.168.192.in-addr.arpa : adresse réseau à l'envers et ajouter .in-addr.arpa

Création des fichiers de zone :

Il faut créer le fichier **db.** Nom**.org** et **db.** Nom**.org.inv** dans /etc/bind/

gedit /etc/bind/db. Nom**.org**

Contenu de ce fichier :

```
$TTL 604800 // Time To Live en secondes
@ IN SOA debian.ouahabi.org. Root. Nom.org. (
//debian le nom du serveur & adresse mail admin
2008030201 ; serial    // année-mois-jour-version
604800 ; refresh  // exprimé en seconde
86400 ; retry
2419200 ; expire
604888 ; default_ttl   // Durée de vie minimum du cache en secondes
)
@ IN NS debian. Nom.org.  // Nom du serveur
Serveur IN A 192.168.0.1     // La table entre les noms et les IP
client IN A 192.168.0.15
www IN CNAME serveur     // Alias entre des noms et d'autres noms
Clientdb IN CNAME client
```

gedit /etc/bind/db. Nom**.org.inv**

Contenu de se fichier :

```
$TTL  604800
@ IN SOA debian. Nom.org. Root. Nom.org. (
2008030201 ; serial
604800 ; refresh
86400 ; retry
2419200 ; expire
604800 ; default_ttl
)
@ IN NS debian. Nom.org.
1 IN PTR serveur
15 IN PTR client
```

Après chaque modification des fichiers de configuration, il faut redémarrer le démon : **/etc/init.d/bind9 restart**

Note : A : Address (nom vers address)
CNAME : Canonical name (alias)
MX : Mail eXchange (Serveur de courrier)
NS : Name Server (Serveur de nom)
PTR : Pointer Record (IP vers nom)
SOA : Start Of Authority (Informations principales de la zone)

Tester la résolution des noms :

- dig –x 192.168.0.1 // 192.168.0.15
- dig www.test.org // serveur.test.org // client.test.org // clientdb.test.org

```
abdel:/home/abdel# host www.mondomaine.ma
www.mondomaine.ma is an alias for serveur.mondomaine.ma.
serveur.mondomaine.ma has address 169.254.204.14
abdel:/home/abdel# host client.mondomaine.ma
client.mondomaine.ma is an alias for abdel5.mondomaine.ma.
abdel5.mondomaine.ma has address 169.254.204.13
abdel:/home/abdel# nslookup serveur.mondomaine.ma
Server:         169.254.204.14
Address:        169.254.204.14#53

Name:   serveur.mondomaine.ma
Address: 169.254.204.14

abdel:/home/abdel# nslookup abdel5.mondomaine.ma
Server:         169.254.204.14
Address:        169.254.204.14#53

Name:   abdel5.mondomaine.ma
Address: 169.254.204.13

abdel:/home/abdel#
```

Serveur DHCP

apt-get install dhcp3-server

Le fichier de configuration du serveur est **/etc/dhcp3/dhcpd.conf**

```
option domain-name "ouahabi.org";
option domain-name-servers 192.0.0.1, 192.0.0.2;
option routers 192.0.0.254;
default-lease-time 3600; // délai du bail en secondes
subnet 192.0.0.0 netmask 255.255.255.0 {
 range 192.0.0.100 192.0.0.200;
 authoritative;
}
```

Fournir une adresse IP en fonction de l'adresse MAC du client

```
host ma_station {
    hardware ethernet 00:00:88:88:aa:aa;
    fixed-address 192.168.0.2;
 }
```

Après modification il faut redémarrer le serveur :

/etc/init.d/dhcp3-server stop / start / restart

Pour configurer un poste client sous Linux, il faut modifier le fichier : **/etc/network/interfaces**

```
auto lo eth0
iface lo inet loopback
iface eth0 inet dhcp
```

Redémarrer le service de gestion de réseau :

/etc/init.d/networking restart

Liste des addresses IP deliver : **/var/lib/dhcp3/dhclient.leases**

Serveur SSH

apt-get install openssh-server

Sécurisation de l'accès SSH

Le fichier de configuration du démon ssh se trouve dans **/etc/ssh/sshd_config**

Après chaque modification de ce fichier, on doit redémarrer le démon **/etc/init.d/ssh restart**

Dans notre première connexion, on a pu se loger avec l'utilisateur root, Nous allons maintenant désactiver cette possibilité

Nano /etc/ssh/sshd_config

Cherchez la ligne **PermitRootLogin yes** et changez-la en **PermitRootLogin no**

Maintenant, on va autoriser uniquement un utilisateur précis à se connecter via SSH (tech-net). Pour cela on ajoute la ligne suivante (dans le fichier /etc/ssh/sshd_config)

AllowUsers tech-net

Si vous avez plusieurs utilisateurs, faite un espace entre chaqu'un. (Même chose pour : AllowGroups, DenyUsers et DenyGroups)

On va aussi changer le port par default (22), cherchez la ligne contenant **Port 22** et changez le port par défaut.

Maintenant, on va afficher un avertissement aux utilisateurs se connectant au serveur SSH, on modifie le fichier issue.net pour mettre notre message

Nano /etc/issue.net

On modifie le fichier de configuration de ssh en supprimant le **#** devant la ligne **Banner /etc/issue.net**

Serveur FTP

apt-get install pure-ftpd *(pure-ftpd-common)*

Création d'utilisateurs virtuels

groupadd ftpgroup

useradd -g ftpgroup -d /dev/null -s /etc ftpuser

Ensuite, il faut créer les utilisateurs virtuels avec la commande suivante :

pure-pw useradd toto -u ftpuser -d /DossierDeToto –N 500

// -N 500 definit le quota d'espace disque à 500 Mo

Note: Le dossier 'DossierDeToto' indiqué sera créé automatiquement à la première connexion si le fichier '/etc/pure-ftpd/conf/CreateHomeDir' contient 'yes'

La liste des utilisateurs virtuels se trouve dans le fichier

/etc/pure-ftpd/pureftpd.passwd

Il est possible de changer le mot de passe avec la commande :

pure-pw passwd toto

Il est possible de modifier un utilisateur avec la commande :

pure-pw usermod toto -d /UnautreDossierPourToto

Après chaque création ou modification d'un utilisateur, il faut générer la base de données avec la commande:

pure-pw mkdb

Pour finir, il faut créer un lien symbolique pour activer l'authentification des utilisateurs virtuels :

cd /etc/pure-ftpd/auth/

ln -s ../conf/PureDB 50puredb

Redémarrez le serveur : **/etc/init.d/pure-ftpd restart**