INSTALLATION D'UN SERVEUR NIS SOUS MANDRAKE LINUX
(pour l'instant encore en construction...)

29 novembre 2003

Table des matières

1 Introduction **1**

2 Installation du serveur **1**

2.1 Installation de la distribution 2

2.2 Copie de la distribution sur le serveur et exportation 2

2.3 installation de NIS sur le serveur 3

2.4 exportation et utilisateurs 4

2.5 Mise en place des quotas 5

3 Installation des postes clients par le réseau **5**

3.1 Installation semi-automatique 5

3.2 installation automatique 5

4 Configuration des postes clients sur une installation existante **6**

4.1 En se déplacant physiquement sur les machines 6

4.2 Avec une installation automatisée utilisant perl-expect 6

1 Introduction

Cet article décrit l'installation d'un serveur NIS sous Linux. Un serveur NIS permet de déporter la gestion des utilisateurs sur un serveur. Avec l'utilisation des services réseau de Linux, il est alors facile de localiser tous les répertoires personnels des utilisateurs sur un serveur, et de les exporter sur le réseau. Ainsi les utilisateurs peuvent changer de machines et retrouveront toujours leurs paramétrages personnels (bureau, paramétrage personnels des logiciels etc....).

Je décris aussi dans cet article comment gérer une parc de machines avec l'utilisation de ssh de perl et du module perl-expect de perl. Ces outils permettent de gérer un grand parc de machines, de manière automatique, et sans avoir à se déplacer physiquement sur les machines (à condition tout de même qu'elles soient démarrées sous Linux).

Je vais supposer que vous avez une machine que vous pouvez utiliser comme serveur (machine standard, avec assez de RAM, par exemple 256Mo ou plus). Nous allons installer Linux sur cette machine, que nous appellerons le serveur. On y placera la distribution, ensuite on utilisera une méthode pour installer Linux sur les autres machines à partir du serveur.

2 Installation du serveur

Ici on va effectuer une installation classique à partit des CD. Dans mon cas le serveur sert au moins pour stocker la distribution et les répertoires communs de tous les utilisateurs. Si vous avez deux disques durs je conseillerai

de mettre le */home* qui contiendra tous les utilisateurs sur ce disque. Bien sur, on a ici un serveur, donc s'il y a un autre OS installé, on reformate tout. Si l'ordinateur vous est livré avec windows, ne démarrer pas sur l'OS et penser peut-être a vous le faire rembourser : `http://www.linux-center.org/detaxe/` .

Je suppose évidemment que le serveur dispose d'une carte ethernet.

2.1 Installation de la distribution

Commencer par bouter sur le Cd et démarrer l'installation. Ensuite (de mémoire)

- lors du partitionnement passer en mode expert. Il va vous falloir au moins les partitions suivantes avec un exemple de taille pour un disque de 40Go
  - */* (1Go)
  - */usr* (5Go)
  - */var* (10Go). Il y aura la la distribution. On prévoit déja la place pour une base de données, des pages html etc, des paquetages supplémentaires à la distribution (update, contrib etc.).
  - */home* (le reste, ça dépend du nombre d'utilisateurs, de leurs besoins)
  - une partition de swap
- formater tout en utilisant un format de **fichiers journalisés** qui soit compatible avec les quotas (ainsi en cas de crash, on pourra si le disque dur vit toujours, retrouver les données). Pour ma part j'utilise *ext3*.
- lors de l'installation, demander l'installation des serveurs *NIS*, *openssh*, *NFS*, *webmin* ainsi que de ceux dont vous aurez l'utilité.
- lors de la demande du mot de passe *root*, donner un mot de passe suffisamment solide (au moins 8-10 caractères non triviaux).
- créer au moins un autre utilisateur. Dans mandrake le premier à un *uid et un gid de 501*, le deuxième un *uid et gid de 502* etc. Il faut au moins un autre utilisateur que *root* qui a tous les droits. Il servira pour le travail sur le serveur, les éventuelles connections distantes par ssh etc....
- Paramétrer l'installation réseau. Donner une IP statique à votre serveur et un nom de machine. Dans la suite je supposerai que le serveur a pour IP *192.168.114.155*
- on termine l'installation

Si vous êtes expérimenté, vous pouvez utiliser LVM *(logical volume manager)* pour créer vos partitions, mais alors vous n'avez certainement plus besoin de ce paragraphe.

2.2 Copie de la distribution sur le serveur et exportation

On suppose ici qu'il existe un utilisateur autre que *root* nommé *toto*.

On se logue en tant que utilisateurs *toto* (si vous n'avez pas modifié les paramètres initiaux de votre installation, le login doit être graphique). Je vais considérer qu'on a démarré avec le gestionnaire de fenêtre par défaut de mandrake qui est *KDE*. Je préfère me loguer en tant que *toto,* et ensuite travailler en tant que *root* dans l'environnement graphique de *toto*, cela évite d'avoir à taper à chaque moment un mot de passe dans l'écran de veille de *root*, et puis c'est la bonne démarche. On va donc ouvrir une *console* d'autre disent un *terminal*.

Pour ouvrir une console, dans la barre des tâches, cliquer sur *K,* et dans le menu, il doit y avoir *terminaux*, et en l'activant vous pouvez alors ouvrir *konsole*, qui ouvre un *console*. Je vous conseille au passage de rajouter dans la barre des tâches un lien direct vers le programme *konsole*. Dans la barre des tâches, cliquer sur le bouton droit de la souris, puis
ajouter -> bouton d'application -> terminaux -> konsole

On devient *root*, qui est le superutilisateur en tapant dans la *konsole :*

```
$ su
```

on tape alors le mot de passe de *root*, et ça y est, toutes les applications que l'on va maintenant lancer à partir de la console auront les droits de *root*. Si vous voulez un gestionnaire de fichiers graphique, vous pouvez par exemple taper

```
$ konqueror &
```

Vous devriez alors voir s'ouvrir *konqueror,* qui est le gestionnaire de fichier de *KDE*. Mais là il est ouvert en tant que *root*. Vous auriez pu l'ouvrir en tant que toto, en cliquant sur votre maison dans la barre des tâches, mais cela ne nous intéresse pas pour le moment. Au passage remarquer le `&`, qui dit à *konqueror* de démarrer en arrière plan, ce qui permet de continuer à utiliser *la console root*. Pour la suite, je vais tout faire en mode *console*, vous pouvez donc fermer *konqueror* (ou faire la même chose avec si vous savez l'utiliser).

On va mettre la distribution sur le serveur. On va donc par exemple créer, si vous lui avez réservé assez de place un répertoire dans */var*

```
$ mkdir /var/distro
$ mkdir /var/distro/9.2
```

On dispose maintenant de */var/distro/9.2*, qui est un répertoire et dans lequel on va pouvoir placer le contenu des trois CDs de la distribution.

On va vider tout le premier CD dans */var/distro/9.2*. Ensuite il va falloir copier les deux autres. Là on ne recopie que les répertoires RPMS2 et RPMS3 qui sont dans le répertoire Mandrake des CD2 et CD3 de la distribution. On les copie */var/distro/9.2/Mandrake*. Ça y est la distribution est installée.

On va maintenant autoriser l'exportation de ce répertoire sur le réseau.

On modifie le fichier */etc/exports* pour exporter le répertoire en *nfs* sur le réseau local.

```
$ kwrite /etc/exports
```

si votre réseau est du type 255.255.0.0, on ajoute la ligne

```
/var/distro 192.168.0.0/255.255.0.0(ro)
```

si il est du type 255.255.255.0 avec IP de la forme 192.168.x. avec x qui est votre nombre on ajoute

```
/var/distro 192.168.x.0/255.255.255.0(ro)
```

on sauvegarde le fichier on quitte *kwrite* et on revient en mode *konsole*. Quelquefois, il y a des messages de kde qui se rajoutent dans la console, n'en tenez pas compte et faites "enter" jusqu'à avoir une ligne propre.

Vous pouvez éventuellement régler les fichiers */etc/hosts.deny* et */etc/hosts.allow* pour les droits d'exportations. Au passage, vous pouvez utiliser en tant que *root*, l'outil *webmin*, pour exporter votre répertoire en *nfs*, et en même tant régler les droits d'exportations. Tapez *webmin* dans la console et loguez vous, mais ceci est une autre histoire...

on valide les changements avec

```
$ exportfs -a
```

A ce stade, la distribution est chargée et elle peut être montée en *nfs* à partir des autres postes. Si par exemple l'IP du serveur est 192.168.0.1, on peut faire en *root* sur un autre poste

```
$ mkdir /mnt/nfs
```

```
$ mount -t nfs 192.168.114.155 ://var/distro/9.2 /mnt/nfs
```

dans */mnt/nfs*, on a alors la distribution de Mandrake. Ceci permet maintenant l'installation réseau des autres postes.

Remarque : Comme la distribution est maintenant disponible sur le serveur, on peut dire au système de ne plus utiliser que la distribution placé sur le disque dur. Pour ce faire, dans la *console* en mode *root*, taper

```
$ drakconf
```

et ensuite, dans *voir ou sont récupérer les logiciels*, vous donner un nom pour les paquetages de RPMS, par exemple 9.2_RPMS, vous dites que c'est en local, et vous donnez le lien vers le répertoire, ça devrait être ici */var/distro/9.2/Mandrake/RPMS*, puis on indique le de-scripteur des paquetages de RPMS dans chemin vers hdlist. On met *../base/hdlist1.cz* . Ça veut dire que avec *..* on revient dans */var/distro/9.2/Mandrake,* puis ensuite avec *../base* on est dans */var/distro/9.2/Mandrake,* et c'est la qu'il faut prendre le fichier *hdlist1.cz.* on recommence avec les deux autres. Après, vous pouvez décocher les CDs dans *voir ou sont récupérés les logiciels.* Maintenant quand vous ferez *urpmi* pour installer des paquetages de la distribution, le système ira les chercher sur le disque au lieu de vous demander les CD. Bien sur tout ceci peut aussi être fait avec *urpmi.addmedia.*

```
$ man urpmi.addmedia
```

et en exercice, faire la même chose en mode console, et avec *urpmi.removemedia* enlever les CDs de la distribution.

2.3 installation de NIS sur le serveur

Dans ce paragraphe on retrouve comme paramètres

mondomainenis qui est le nom de domaine de votre serveur *NIS*, choisissez ce que vous voulez, par exemple *lyceeNIS.*

serveur qui est le nom de votre serveur (ça peut être son nom *HOSTNAME* si vous avez un serveur de nom ou son adresse IP si elle est fixe, je préfère la deuxième solution pour un serveur).

1. Si ce n'est pas déjà fait, il faut installer les paquetages *ypserv* et *mawk.*
   `$ urpmi ypserv mawk`.
2. dans */etc/sysconfig/network* on ajoute la ligne *NISDOMAIN=mondomainenis.*
   `$ kwrite /etc/sysconfig/network`
   on ajoute donc la ligne *NISDOMAIN=mondomainenis,* on sauvegarde et on revient en mode *console*
3. dans */var/yp* qui a été créé par l'installation du paquetage ypserv on édite le fichier Makefile
   `$ kwrite /var/yp/Makefile`

on vérifie qu'il contient ou on le modifie de la sorte pour qu'il contienne
#pas de slave pour les maps
NOPUSH=true
MINUID=500
MINGID=500
MERGE_PASSWD=false
MERGE_GROUP=false
all : passwd group shadow

4. en mode console taper
   `$ domainname mondomainenis`
5. on lance les services si ils ne sont pas déjà démarrés
   `$ service ypserv restart`
   `$ service yppasswdd restart`
6. dans */var/yp* on tape make dans une console
   `$ cd /var/yp`
   `$ make`
   il se crée un répertoire *mondomainenis*
7. on édite maintenant le fichier /etc/ypserv.conf
   `$ kwrite /etc/ypserv.conf`
8. éventuellement on restreint l'exportation sur les sous réseaux à adapter en fonction de votre réseau
   `$ 192.168. : passwd.byname : port : yes`
   `$ 192.168. : passwd.byuid : port : yes`

2.4 exportation et utilisateurs

1. si votre réseau est du type *255.255.0.0* ajouter la ligne
   /home 192.168.0.0/255.255.0.0(rw)
   dans */etc/exports*
   `$ kwrite /etc/exports`
   s'il est du type *255.255.255.0* avec IP de la forme *192.168.x.* avec x qui est votre nombre vous ajouterez la ligne
   /home 192.168.x.0/255.255.255.0(rw)
   vous sauvegardez, et éventuellement vous réglez les fichiers */etc/hosts.deny* et */etc/hosts.allow* pour les droits d'exportations.
   on valide les changements avec
   `$ exportfs -a`
2. on veut garder des utilisateurs locaux sur les clients, donc le */home* local des ordinateurs clients. Les fichiers vont être exportés en utilisant *autofs*, ce qui obligent à les monter dans un répertoire vide sur les ordinateurs clients. On créera sur les clients un répertoire */export,* puis on montera le répertoire */home* du serveur dans ce répertoire */export* avec *autofs.* Sur les clients l'accès au répertoire se fera donc à travers */export/home.* Pour pouvoir se loguer sur le serveur comme client avec un répertoire commençant par */export/home* au lieu de */home,* on créé le répertoire */export* et le lien symbolique suivant
   `$ mkdir /export`
   `$ ln -s /home /export`
   sur le serveur, les utilisateurs ont maintenant leur répertoire accessible par */home* et par */export/home.*
3. on modifie le $HOME des utilisateurs :
   dans */etc/passwd* on remplace les /home des utilisateurs qui doivent être exporter par /export/home, par exemple
   veronique :3GGWf/uWiPoWM :4002 :4000 : :/home/veronique :/bin/bash
   devient :
   veronique :3GGWf/uWiPoWM :4002 :4000 : :/export/home/veronique :/bin/bash
4. Bien penser que lorsque l'on créera de nouveaux utilisateurs, il faudra placer leur répertoire personnel $HOME dans /export/home/$HOME
5. Suite aux modifications de /etc/passwd, il faut régénérer les pages jaunes du serveur NIS. La commande à faire est
   `$ cd /var/yp`
   `$ make`
   Il faudra regénérer les pages jaunes avec cette commande à chaque fois que l'on aura ajouté ou modifié le fichier des utilisateurs.

2.5 Mise en place des quotas

1. on installe le paquetage pour la gestion des quotas
   `$ urpmi quota`
2. mettre les quotas dans le répertoire */home* qui sera exporté
   `$ touch /home/aquota.user`
   `$ chmod 600 aquota.user`
3. Si le répertoire /home est monté à partir de la partition */dev/truc*, on rajoute dans */etc/fstab* l'argument *usrquota*. Par exemple :
   /dev/hda7 /home ext3 defaults 1 2
   devient
   /dev/hda7 /home ext3 defaults,usrquota 1 2
4. j'ai trouvé l'éditeur *vi* trop récalcitrant pour mettre les quotas directement, aussi j'ai utilisé *webmin* pour mettre les quotas en place. Dans *webmin*, il y a une icône *userquota*, et on met des quotas dans le répertoire */home* pour un des utilisateurs (en supposant que les autres auront les mêmes volumes offerts). Par exemple mettre 40000 blocks comme limite soft (avertissements) et 50000 comme limite dure donne environ 40Mo de données enregistrables avant des avertissement, et 50Mo de limite maximum.
   `$ webmin`
   on le démarre donc en *root* sinon on génère une erreur dans la console. Il faut que les cookies soient activés sur le navigateur. Dites que vous acceptez une authentification pour cette cession seulement. Ensuite on se logue en tant que *root* et il y a le mot de passe à entrer pour entrer sur la machine (c'est normal, c'est un outil d'administration distant) et regarder quel bel outil nous avons là. Aller ensuite dans *system* et cliquer sur *disk quotas*. Vous devez alors voir les utilisateurs. On va juste mettre des quotas pour un utilisateurs, après on va les recopier. Enregistrer et quitter *webmin*.
   On suppose maintenant que *user* est un utilisateur avec quota.
5. Pour mettre le même quota à *autre_ user*, on fait
   `$ edquota -p user autre_user`
6. pour visualiser tous les quotas
   `$ repquota -a`

3 Installation des postes clients par le réseau

3.1 Installation semi-automatique

Dans la distribution on va se placer dans le répertoire */images*. Ici sur le serveur on va donc dans */var/distro/9.2/Mandrake/im*
Il y a un fichier nommé *network.img* qui permet une installation par réseau (non automatique). On va copier ce fichier sur une disquette bits à bits.

`$ dd if=network.img of=/dev/fd0`

Ça y est, si vous bootez un ordinateur sur votre disquette, il vous demandera une IP, puis ou chercher votre distribution. Dans notre exemple, c'est un réseau *nfs* et la distribution se trouve sur *192.168.114.115 ://var/distro/9.2*
Si le serveur à le droit d'exporter sur cette IP, il va commencer l'installation standard (comme sur les CD). Après il vous faudra passer au paragraphe *Configuration des postes clients sur une installation existante* pour configurer l'ordinateur en client NIS. Vous n'aurez cependant plus besoin des CDs, car il y dira directement rechercher les paquetages sur le serveur.

3.2 installation automatique

On va automatiser tous les processus d'installation, définir les paquetages à l'avance, les services, et faire une post-installation. Tout ceci est bien expliqué dans le paquetage
drakx-autoinstall-doc-9.0.1-2mdk.noarch.rpm. Suivant votre distribution, il faut le récupérer sur le net et l'installer. Il peut ensuite se lire localement à l'URL

/usr/share/doc/drakx-autoinstall-doc-9.0.1/AutoInstall-9.0.1.html
Il va falloir construire pour chaque machine un fichier de configuration qu'on mettra sur le serveur et une disquette.

4 Configuration des postes clients sur une installation existante

4.1 En se déplacant physiquement sur les machines

1. Installer autofs pour l'importation automatique de répertoire distant
   `$ urpmi autofs`
2. on édite */etc/auto.master*
   `$ kwrite /etc/auto.master`
   on doit avoir les lignes
   /misc /etc/auto.misc –timeout=60
   /net /etc/auto.net –timeout=60
   on peut enlever ces lignes si on ne s'en sert pas et on rajoute
   /export /etc/auto.home –timeout=60
3. on quitte puis on crée le répertoire /export et /etc/auto.home
   `$ mkdir /export`
   `$ mkdir /etc/auto.home`
4. dans /etc/auto.home on ajoute la ligne
   home -fstype=nfs serveur :/home
   où serveur est ici le nom du serveur NIS ou son IP
5. on relance autofs par
   `$ service autofs restart`
6. on installe les librairies pour le login déporté
7. `$ urpmi ypbind yp-tools`
8. on édite le fichier */etc/sysconfig/network* et on y ajoute la ligne
   NISDOMAIN=mondomainenis
   où mondomainenis et le nom de votre **domaine** NIS
9. on édite le fichier */etc/yp.conf* et on y ajoute
   domain mondomainenis server serveur
   avec mondomainenis et serveur à remplacer par vos noms.
   on peut rajouter des serveurs esclaves si on à un serveur de secours....
   ypserver nom-du-serveur-slave
   mais ça je n'ai pas encore essayé....
10. Maintenant on modifie */etc/nsswitch.conf* pour les lignes hosts, group et passwd (uniquement pour les maps exportés par le serveur NIS), pour prendre en compte d'abord les fichiers */etc/hosts*, */etc/group* et */etc/passwd* locaux puis ceux du serveur *NIS*, on aura donc pour les lignes en question :
    passwd : files nis
    group : files nis
    hosts : files nis dns
11. on informe le système du nom de domaine NIS utilisé
    `$ domainname mondomainenis`
12. on démarre ou redémarre les services *portmap* et *ypbind*
    `$ service portmap start`
    `$ service ypbind start`
13. on test pour voir si ça a fonctionné
    `$ ypwhich`
    on devrait récupérer une réponse de la forme serveur ou IP du serveur NIS. Il m'est déjà arrivé de ne rien avoir à ce stade, mais je crois que j'avais démarré *ypbind* avant de lancer ou relancé *portmap*.

4.2 Avec une installation automatisée utilisant perl-expect

Voir le script urpmi.pl, qui supprime la recherche des paquetages sur les cd d'installations et permet d'avoir des installations automatiques des paquetages (à condition toutes fois de monter en nfs le répertoire distant sur lequel existe la distribution.

Les sécurités (à reprendre)

Sous Mandrake, les utilisateurs sont créés en même temps qu'un groupe qui à le même nom qu'eux. Mais par défaut (en tous les cas au niveau de sécurité standard, il y a lecture par défaut pour tous les utilisateurs). Pour l'enlever je mets un umask de 027 pour tout le monde (sauf root). Ainsi les autres utilisateurs n'ont aucun droit de lecture sur les fichiers créés. Donc sur les clients, mais on peut le faire aussi sur le serveur, je modifie les fichiers

- /etc/profile
- /etc/baschrc
- /etc/sysconfig/msec
- /etc/profile.d/msec.csh
- /etc/profile.d/msec.sh

et je remplace dans chacun la ligne umask 022 qui correspond à celle des utilisateurs (uid et gid supérieur à 500) en umask 027. On ne le fait pas pour root sinon, après l'installation de nouveaux programmes, il faut d'abord redonner des droits d'exécution etc...

Normalement il faudrait n'autoriser pour portmap que les ordinateurs de votre réseau ce qui se règle dans /etc/hosts.deny et /etc/hosts.allow. Il est de bonne augure aussi de mettre un firewall sur le serveur mais ceci sera peut être l'objet d'un autre article....