



Fonctionnement de NIS

*Le service NIS (Network Information System),
permet de centraliser les connexions sur un réseau local*

Généralités

- L'objectif central de tout serveur de fichiers d'un réseau local est de permettre aux utilisateurs du réseau de se connecter au serveur de fichier sous un compte centralisé au niveau du réseau, et non pas défini machine par machine et aussi d'accéder à ses fichiers (répertoire personnel, ...)
- Dans un réseau homogène Linux, la connexion et l'authentification sont du ressort du service NIS, tandis que les accès aux répertoires personnels et partagés sont permis par le service complémentaire NFS, qu'il faut aussi mettre en oeuvre.
Pour utiliser des stations M\$-Windows dialoguant avec un serveur Linux, l'alternative à NIS+NFS est la mise en oeuvre du serveur Samba.
- NIS maintient une base de données (ou annuaire) centralisée au niveau d'un groupe de machines appelé domaine NIS.
Supposons que le nom NIS attribué soit *ecole*. Ces informations sont alors stockées dans le répertoire */var/yp/ecole*, sous forme d'un ensemble de fichiers binaires appelés *cartes* ou *maps*.
- Les types d'informations que les stations "clientes", celles des utilisateurs, viennent chercher sont essentiellement les correspondances entre noms et adresse IP des machines du réseau, les vérifications des noms de login, mots de passe et groupe d'appartenance des comptes utilisateurs existants sur le serveur.
Toutes ces informations sont contenues habituellement dans les fichiers */etc/hosts* (annuaire des machines connues), */etc/passwd*, (annuaires des utilisateurs qui contient les répertoires à la connexion) et */etc/group* (annuaire des groupes) et */etc/shadow* (mots de passe cryptés).
- Plus concrètement, soit une station Linux, cliente du serveur NIS. Un utilisateur remplit un formulaire de connexion (demande de login). Le client NIS de cette station cherche à obtenir une réponse du serveur NIS du même domaine, à une question du genre "me connais-tu comme station autorisée, et l'utilisateur que j'accueille possède t-il un compte chez toi, mon serveur?"
- Les réponses sont contenues dans 6 maps usuels, situés dans */var/yp/ecole*, et appelés *hosts.byname*, *hosts.byaddr*, *passwd.byname*, *passwd.byuid*, *group.byname* et *group.bygid*
- Les applications NIS utilisent les fonctions RPC = *Remote Procedure Calls*, fonctionnalités supplémentaires (logées dans la couche session au dessus de TCP/IP), gérées par un service appelé *portmap*.

Configuration du serveur NIS

• Installation

Le paquetages RPM à installer (sur des systèmes de type RedHat) est *ypserv* (et *ypbind* et *yp-tools* sur les stations)

Son installation va créer des fichiers dans :

- */usr/sbin*, notamment les serveurs *ypserv* et *rpc.yppasswd*,
- */etc/rc.d/init.d/*, les scripts de controle *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

Du côté serveur, les services à lancer sont *portmap*, *ypserv* (le serveur NIS) et *yppasswd* (le service spécialisé dans le changement des mots de passe).

Conformément au [système d'initialisation System V](#), on trouve dans le répertoire */etc/rc.d/init.d* les fichiers de contrôle des services *ypserv*, *yppasswd* (et *portmap*). On procède alors au lancement ou à l'arrêt manuel de NIS par

:

```
/etc/rc.d/init.d/portmap start
/etc/rc.d/init.d/ypserv start
/etc/rc.d/init.d/ypasswd start
```

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 (ou avec `kysv` sous X-KDE)

• Configuration

1. Choisir un nom de domaine NIS, soit `ecole` par exemple, indépendamment du nom de domaine du réseau, par exemple `factice.ac-creteil.fr` ("formation continue dans le secteur TICE"), et également sans rapport avec un éventuel nom de domaine Samba.
Supposons de plus que le serveur ait pour adresse IP : 10.177.240.1 avec un masque 255.255.255.0

2. Déclaration du domaine NIS

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

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

Vérification : la commande **domainname** doit obtenir comme réponse ce nom de domaine NIS.

3. Préciser les machines autorisées à accéder au service NIS

Editer le fichier `/var/yp/securenets` et insérer les lignes

```
# pour permettre l'accès sur le serveur même
255.0.0.0 127.0.0.1
# pour permettre l'accès de toutes les machines du sous-réseau (masque et adresse réseau)
255.255.255.0 10.177.240.0
```

4. Préciser les informations que NIS doit gérer

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

all: passwd group hosts

Il est recommandé de ne rien modifier d'autre sauf "si on sait ce que l'on fait ...", car pour l'essentiel il a été correctement paramétré lors de l'installation de la distribution.

5. Générer les cartes

Il s'agit maintenant de créer les 3 cartes (maps) correspondant aux 3 fichiers `/etc/passwd`, `/etc/group` et `/etc/hosts`.

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

```
# cd /var/yp
# make
```

Il y a création d'un sous-répertoire `/var/yp/ecole` (portant le nom du domaine NIS) contenant les 6 fichiers binaires de permissions 600 :

`hosts.byname`, `hosts.byaddr`, `passwd.byname`, `passwd.byuid`, `group.byname` et `group.bygid`

6. Renseigner le fichier de configuration de NIS

Editer le fichier `/etc/ypserv.conf` et indiquer l'adresse IP du réseau comme ci-dessous :

```
# Host          : Map          : Security   : Passwd_mangle
#
10.177.240.     : passwd.byname  : port       : yes
10.177.240.     : passwd.byuid   : port       : yes
```

7. Relancer le serveur

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

Le serveur devrait être fonctionnel. Vérification

```
# ps ax | grep yp
root  550  .....  ypserv
root  823  .....  rpc.yppasswdd
```

Configuration d'une machine cliente

• 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 (ce qui exécute rpc.portmap)
/etc/rc.d/init.d/ypbind start
```

• Configuration

1. Dans `/etc/sysconfig/network`, comme sur le serveur il faut déclarer le nom du domaine en ajoutant la ligne

```
NISDOMAIN = "ecole"
```

2. Editer `/etc/yp.conf`, et y ajouter les 2 lignes

```
domain ecole server 10.177.240.1
ypserver fctice
```

3. Editer `/etc/nsswitch.conf`, et veillez à la présence active des lignes

```
passwd:      files nis
group:       files nis
hosts:       files nis dns
```

4. 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: fctice.ac-creteil.fr
```

• Tests

1. Premières vérifications

- `ps ax |grep yp` doit montrer 2 processus `ypbind` en exécution.
- La commande `ypwhich` doit donner le nom complet de la machine qui héberge le serveur
- `ypcat passwd` permet d'afficher la carte des comptes utilisateurs

2. Première connexion : le grand moment est arrivé, toto tente fébrilement une connexion

```
login: toto
Password: jules
Last login: ...
No directory /home/toto!
Logging in with home = "/".
bash-2.04$
```

Que s'est-il passé ?

Tout est normal, toto n'a pas de répertoire personnel sur la station !

(ce qu'on peut vérifier par l'absence de lignes pour : `cat /etc/passwd | grep toto`).

3. Si NFS n'est pas en oeuvre, l'utilisateur peut-il, tout de même travailler dans son répertoire personnel sur le serveur ?

Avec `telnet` (ou mieux via [ssh](#))

```
$ telnet fctice
Trying 10.177.240.1 ..
Connected to fctice.ac-creteil.fr
.....
login: toto
Password: jules
[toto@fctice toto] $
```

4. Changement de mot de passe

La commande `yppasswd toto` permet à l'utilisateur de changer son mot de passe comme s'il se trouvait à la console du serveur.

Cela provoque la mise à jour usuelle dans `/etc/shadow`, mais biensûr doit mettre à jour les 2 cartes `passwd` en relançant `/usr/bin/make`

Problèmes rencontrés, mini-FAQ

Problèmes serveurs, difficultés rencontrées par l'administrateur

Comment éviter de relancer "à la main" la procédure Makefile de génération des maps ?

En mettant en place un script bash tout simple qui sera activé périodiquement, par le [service crontab](#)

```
#!/bin/bash
# script à placer dans /usr/sbin (ou un répertoire listé dans le PATH)
# à nommer par exemple nis.sh
cd /var/yp
make
if [ $? = 0 ]
then
echo "Mise à jour des cartes de NIS effectuée"
fi
```

Problèmes clients, en supposant le serveur fonctionnant correctement .

1. Quand je lance le service NIS sur une station cliente, j'obtiens des messages d'erreur du genre (les libellés dépendent des distributions et de leur version) :

```
# /etc/rc.d/init.d/ypbind start
Binding to the NIS domain ... [failed]
Listening for an NIS domain server .... ypwhich: ne peut communiquer par ypbind
# domainname
```

```
-- > Le nom du domaine NIS n'a pas été précisé
Indiquer ce nom en passant la commande
# domainname ecole
# /etc/rc.d/init.d/ypbind start
Binding to the NIS domain ... [OK]
Listening for an NIS domain server: fctice.ac-creteil.fr
```

2. Le nom du domaine est bien reconnu, mais il y a un blocage quand le client cherche à se lier au serveur du domaine par ypwhich.

```
# /etc/rc.d/init.d/ypbind start
Binding to the NIS domain ... [OK]
Listening for an NIS domain server .... ypwhich: ne peut communiquer par ypbind
```

La première cause à suspecter est un dysfonctionnement de la connexion réseau. Commencer par "pinguer" le serveur.

3. Le service client fonctionne correctement comme en témoignent les requêtes :

```
# domainname
ecole
# ypwhich
fctice.ac-creteil.fr
# ypcat hosts.byname
toto:<password crypté>:502:506:M. le stagiaire Toto:/home/toto:/bin/bash
.....
```

En particulier, la précédente commande me montre que le compte toto existe bien sur le serveur NIS. Et pourtant quand je tente de me "loguer" comme toto/jules, je me retrouve connecté à ma propre machine ! pourquoi ?

--> probablement le même compte existe aussi sur la station cliente, il y a alors un conflit ! Ce qui est alors déterminant est l'ordre indiqué dans le fichier /etc/nsswitch.conf qui devrait être probablement :

```
# extrait de /etc/nsswitch.conf
passwd: files nis
group: files nis
hosts: files nis dns
```

Attention, changer le mot de passe du compte local ne résoudra rien : l'existence du compte local fait écran au compte NIS.

Donc une station cliente NIS+NFS ne devrait pas héberger des comptes locaux (bien sûr à part root).

L'administrateur devrait les supprimer : `# userdel -r user`

4. Je me connecte sur une station en mode console sans problème, mais je n'y parviens pas si la station démarre automatiquement en mode graphique. Pourquoi ?
 - A coup sûr, le passage en mode graphique n'a pas permis les mêmes démarrages de programmes, en particulier **ypbind**. Là, il faut faire appel à l'administrateur root des stations de la salle. Il doit faire effectuer ces exécutions aussi en niveau graphique, en copiant ou en créant des liens symboliques vers des scripts de contrôle.
 - Par exemple sur une station "Mandrake 7.2", j'ai été amené à effectuer les copies de

```
/etc/rc.d/rc 3.d/@S17ypbind vers /etc/rc.d/rc5.d/
```

- Créer si nécessaire les liens symbolique pour l'arrêt (niveau 0) ou le reboot (niveau 6)

```
ln -s /etc/rc.d/rc.d/ypbind /etc/rc.d/rc0.d/@K83ypbind
ln -s /etc/rc.d/rc.d/ypbind /etc/rc.d/rc6.d/@K83ypbind
```

- On peut utiliser l'outil graphique convivial **ksysv**. Finalement les services suivants doivent être en fonctionnement : portmap, ypbind, netfs et nfslock

5. L'administrateur(e) du réseau de mon établissement vient de créer mon compte sur le serveur et mon répertoire personnel.

Tout content, je me précipite sur la première station libre, et là j'essuie un échec quand je tente de me connecter ! Pourquoi ?

Tout simplement il faut se rappeler que les maps ne sont pas mis à jour dynamiquement ! L'administrateur doit impérativement relancer manuellement le Makefile, ou mettre en place un script périodique.

6. Je suis maintenant un "client NIS-NFS" satisfait. Mais, puis-je changer mon mot de passe sans déranger M/Mme root ?

```
bash-2.04$ yppasswd toto
Changing NIS account information for toto on fctice.ac-creteil.fr
Please enter old password: jules
Please enter new password : jules1
retype ...
The NIS password has been changed on ....
```