



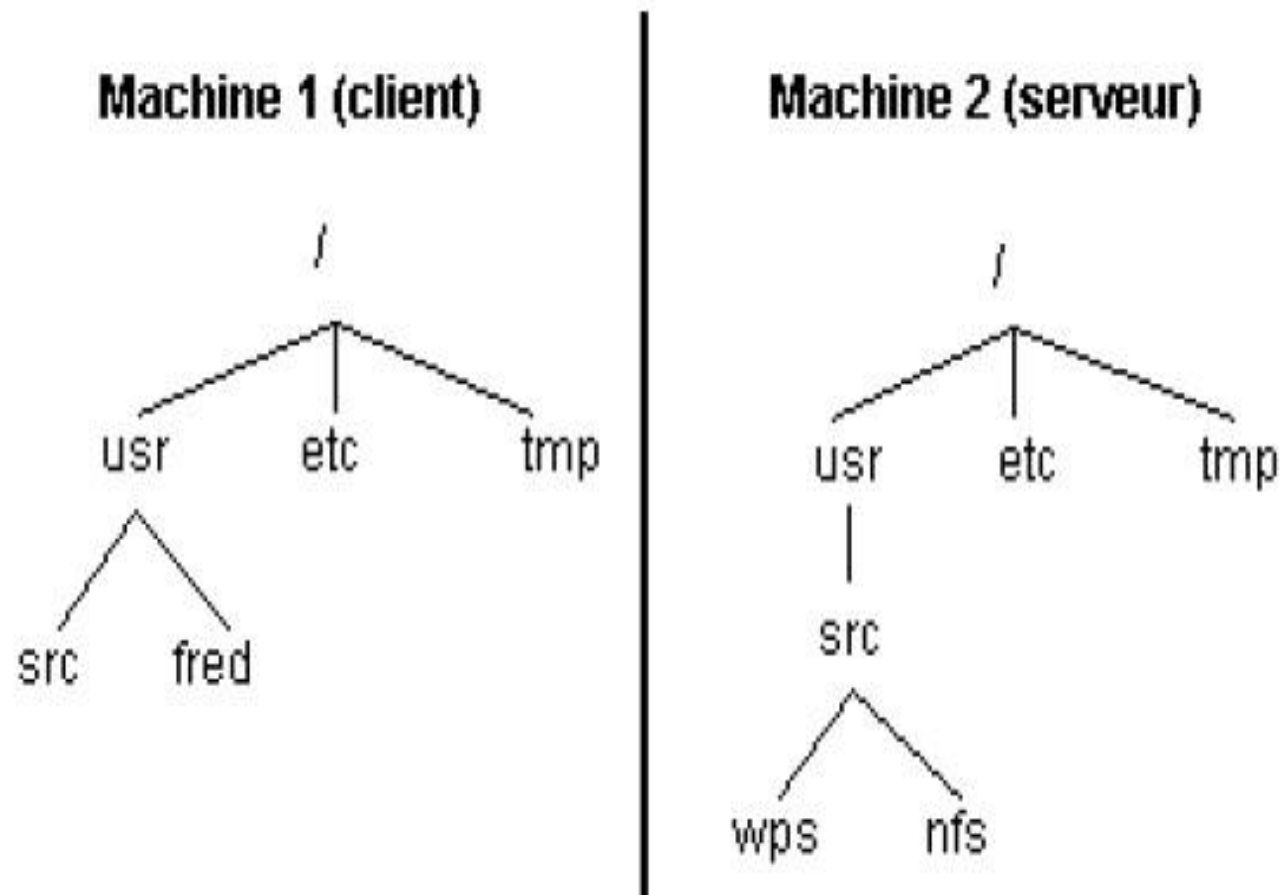
Mettre en œuvre un système NIS/NFS

Présentation du système NFS

- NFS (**Network File System**) est un système de partage de fichiers pour les systèmes UNIX/LINUX développé par SUN
- NFS permet de monter des répertoires situés dans des machines distantes sur la machine cliente et les faire apparaître comme des répertoires locaux.
- NFS fait référence aussi au protocole de communication qui permet un tel partage de ressources
- Le protocole de communication NFS est sans état:
 - Si au cours d'une session le client monte un répertoire distant via NFS et que le serveur NFS se plante, le client ne sera pas affecté et une fois le serveur est relancé le client reprend l'accès sur le répertoire
- Note: SAMBA est au contraire, un protocole avec état

Présentation du système NFS (suite)

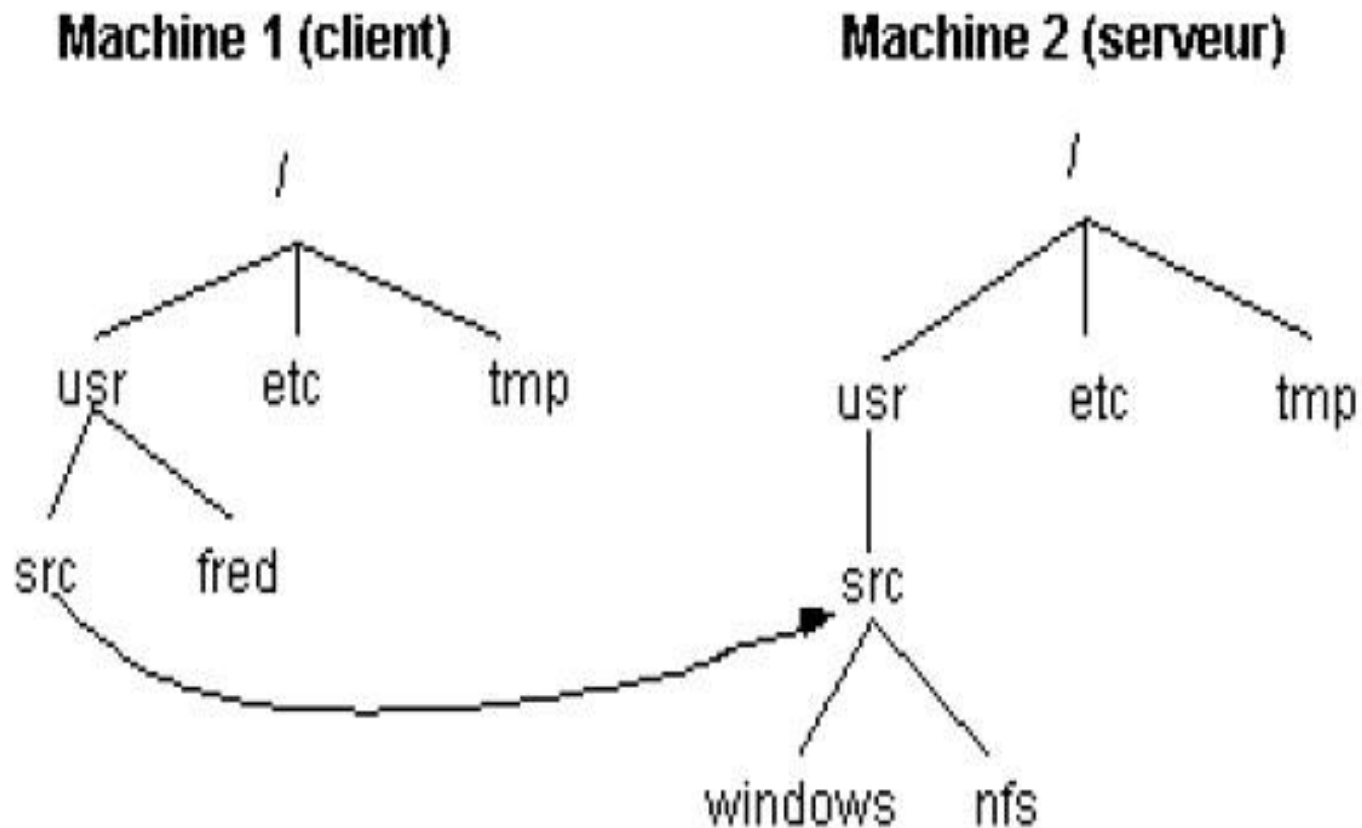
Avant le Montage



Présentation du système NFS (suite)

Après le montage :

```
mount mach2:/usr/src /usr/src
```



Présentation du système NFS (suite)

Les intérêts d'un tel système:

- Optimiser les capacités en espace disque des serveurs existants
- Permettre aux utilisateurs de stocker leur environnement de travail (répertoire d'accueil) sur un serveur NFS, et donc avoir plus de libertés de mouvement
 - Permet également de limiter le nombre de périphériques de stockages amovibles dans le réseau (Lecteurs disque, USB, etc..)
- Mettre en place un serveur de stockage centralisé
 - Très utilisé dans le cadre d'un Cluster, utiliser un serveur de stockage centralisé partagé par plusieurs serveurs frontaux
 - Dans le cadre d'un système centralisé de sauvegardes et d'archivage

Composants du système NFS

Le serveur NFS

- NFS fonctionne en collaboration avec d'autres outils qui doivent tous être supportés au niveau du noyau:
`rpc, nfs, nfslock, portmap, rquotad` et `mountd`
- L'installation du serveur NFS sous UBUNTU se fait par la commande:
`Apt-get install nfs-kernel-server nfs-common portmap`
- La configuration du serveur se trouve dans le fichier `/etc/exports` et la commande `exportfs` permet de rendre le partage effectif

Le client NFS

- Le client utilise la commande Linux `mount` pour monter un système de fichiers distants sur un répertoire local
- Les services : `netfs, nfslock, portmap` doivent être installés
- Pour que le client fonctionne correctement s'assurer de l'installation des paquets `nfs-common` et `portmap`

Configuration de base pour NFS

- Reconfigurer le serveur `portmap` pour écouter sur le réseau (par défaut il écoute l'adresse de bouclage lo)

`dpkg-reconfigure portmap`

- Créer ou identifier le répertoire à exporter:

Par exemple: `mkdir /var/partage-nfs`

- Configurer le fichier `/etc/exports` pour permettre le partage (ou l'exportation) du répertoire partagé.

- Chaque ligne de ce fichier contient la description d'un répertoire à partager de la forme

`/home/partage/ nom-machine1(ro,sync,no_root_squash) .. nom-machine2(ro,sync,no_root_squash) plage-ip(,,,,)`

Configuration d'un serveur NFS

Les options d'exports:

- Déclarer la liste des machines ayant le droit de monter le répertoire partagé suivi des options d'accès:
 - **ro**: lecture seulement
 - **rw**: lecture/écriture
 - **sync**: écritures bloquantes sur le serveur (option par défaut **async**) évite la compromission des données en cours de transfert en assurant qu'une opération d'écriture ne peut se faire que lorsque l'opération précédente se termine
 - **no_root_squash**: donne au client les privilèges du root en ce qui concerne l'accès au répertoire partagé (déconseillée)
- Pour exporter effectivement les répertoires déclarés lancer la commande: **exportfs -a**
 - Ou bien sous UBUNTU:
`/etc/init.d/nfs-kernel-server restart`

Configuration d'un serveur NFS(suite)

- Sécurité de l'accès aux services NFS à travers le programme TCP Wrapper:
- Déclarer les machines/réseaux qui ont le droit d'accéder au service dans le fichier /etc/hosts.allow
- Interdire toutes les autres dans le fichier /etc/hosts.deny

Exemple : Dans /etc/hosts.allow

- portmap: 192.168.0.1 , 192.168.0.2
- lockd: 192.168.0.1 , 192.168.0.2
- rquotad: 192.168.0.1 , 192.168.0.2
- mountd: 192.168.0.1 , 192.168.0.2
- Statd: 192.168.0.1 , 192.168.0.2

Dans /etc/hosts.deny

- portmap: ALL
- lockd: ALL

● Montage manuelle d'un répertoire NFS

- Le client NFS peut monter un répertoire exporté par un serveur NFS distant en utilisant la commande mount:

```
mount serveur-nfs:/chemin-rep /mnt/rep- local
```

- Une fois monté, l'utilisateur peut manipuler le répertoire distant comme s'il faisait partie de son système (en utilisant les commandes ls, cp, mv etc....)

- Pour démonter ce répertoire il suffit d'utiliser la commande inverse

```
umount /mnt/rep-local
```

- Pour monter un répertoire distant lors du démarrage du système, il faut configurer le fichier `/etc/fstab` comme pour les autres répertoires du système

Montage automatique au démarrage du système

- Pour monter un répertoire distant lors du démarrage du système, il faut configurer le fichier `/etc/fstab` comme pour les autres répertoires du système

Les lignes à rajouter dans ce fichier sont de la forme:

```
repertoire distant # point de montage # type de FS # options# dump # fsckorder  
serveur-nfs:/chemin/rep /mnt          nfs      rw      0 0 ...
```

- Les autres options de montage:
 - **rw/ro**: lecture et écriture ou bien lecture uniquement
 - **soft**: permet de tolérer les erreurs lors d'une interruption du transfert de fichier, mais n'assure pas l'intégrité de ces fichiers
 - **hard**: permet de stopper le transfert de fichiers en cours si un incident se produit, de préférence le combiner avec l'option
 - **Intr**: permet la reprise d'un transfert interrompu
 - **rsize/wsize**: définissent les tailles des blocs de données échangées entre le client et le serveur NFS (par défaut 4K)

Vérifications des exports

Au niveau du serveur:

`showmount -e nom-machine-cliente/ip-machine-cliente`

Résultat:

`/var/nfs-patage IP-client`

Au niveau du client:

La commande `mount` qui donne la liste de tous les systèmes de fichiers montés.

Le service NIS

- **NIS (Network Information Server)**: est un service qui permet de gérer d'une façon centralisée les informations d'authentification (login/mot de passe) des machines et des services dans un réseau de systèmes LINUX.
- NIS était connu sous le nom **Pages Jaunes (Yellow pages)** mais du fait qu'il s'agit d'une marque appartenant à British Telecom, le concepteur du projet (SUN) a remplacé YP par NIS, la plupart des programmes NIS commencent par yp (comme Yellow Pages).
- Le client NIS n'a pas besoin de maintenir les informations d'authentification qui sont configurées par l'administrateur au niveau du serveur.

Le fonctionnement de NIS

- NIS permet de gérer plusieurs domaines au sein du réseau, chacun doit avoir un serveur Maître.
- Pour un domaine donné, le serveur maître peut fonctionner avec un ou plusieurs serveurs esclaves.
- Le serveur NIS maître maintient les informations du réseau, les autres ne font que répliquer ces données:
 - Les modifications ne peuvent survenir qu'au niveau du serveur maître pour qu'il les réplique sur les serveurs esclaves (via le programme yppush)
- Un client NIS peut contacter indifféremment l'un des serveurs NIS disponibles sur le réseau

Le serveur NIS

- Pour installer NIS sur UBUNTU lancer la commande suivante:

`apt-get install portmap nis`

Fournir le nom du domaine en réponse à la question demandée

- Le maitre doit exécuter les programmes suivants:

- `ypserv`

- `ypbind`

- `ypwhich,`

- `ypcat,`

- `yppoll,`

- `ypmatch`

- Le serveur esclave exécute tous les programmes précédents sauf `ypserv`

Configuration du serveur NIS

Fichiers de configuration:

[/etc/default/portmap](#)

Commenter la ligne `ARGS="-i 127.0.0.1"`

[/etc/defaultdomain](#)

rajouter le nom de domaine au début du fichier

[/etc/default/nis](#)

Fixer les options

`NISSERVER=master`

`NISCLIENT=true`

Configuration du serveur NIS

`/etc/yp.conf`

Rajouter une ligne de la forme:

`domain <domainname> server <servername>`

`Ypserver 127.0.0.1`

Éditer le fichier `/etc/ypserv.securenets`

`Host 192.168.1.1`

Ne pas laisser une ligne de la forme `0.0.0.0` qui autorise tout le monde à utiliser notre serveur NIS.

Configuration du serveur NIS

Fichiers de configuration:

`/var/yp/MakeFile`

Éditer les fichiers que vous voulez rendre disponibles via NIS

`ALL hosts, group, passwd, shadow, rpc, services netid protocols, netgrp`

`MINUID`

`MINGID`

`ALL += auto.master auto.home`

Créer les fichier auto.master et auto.home

`touch /var/yp/auto.master`

`touch /var/yp/auto.home`

Configuration du serveur NIS

- Construire la base de données NIS :

`/usr/lib/yp/ypinit -m`

Les fichiers générés lors de cette compilation sont:

passwd.byname, passwd.byuid, group.byname, group.bygid, hosts.byname,
hosts.byaddr, rpc.byname, rpc.bynumber, services.byname,
services.byservicename, netid.byname, protocols.bynumber, protocols.byname,
netgroup, netgroup.byhost, netgroup.byuser, auto.master, auto.home...
shadow.byname...

- Redémarrer le tout :

`/etc/init.d/portmap restart`

`/etc/init.d/nis restart`

Configuration du serveur NIS

Rajouter des utilisateurs NIS avec la commande usuelle:

```
useradd - d/home/login -uid 20XX login
```

Rentrer /var/yp, puis lancer la commande make pour compiler les nouvelles informations **Make**

NIS et la sécurité

- NIS peut être un service dangereux à l'entreprise si des précautions ne sont pas prises.
- Toute personne présente sur le réseau peut avoir accès aux informations d'authentification (login/password)
 - Même si les mots de passes sont cryptés, il est possible de les utiliser pour prendre l'identité d'un utilisateur et fournir le mot de passe crypté.
- Sécuriser NIS à travers:
 - La limitation des machines qui ont le droit d'accéder au service (à travers le TCP Wrapper)
 - Limiter à quel système NIS va répondre à travers le fichier [/etc/securenets](#)

Configuration du client NIS

- Installer le paquet nis: `apt-get install nis`
- Rajouter une entrée du serveur NIS dans le fichier `/etc/hosts`
- Dans `/etc/defaultdomain`, comme sur le serveur il faut déclarer le nom du domaine en ajoutant la ligne
`"nom-domaine"`
- Editer `/etc/yp.conf`, et y ajouter les 2 lignes
`domain nom-domaine-nis server ip-server`
`ypserver nom-domaine`
- Editer les fichiers `/etc/passwd`, `/etc/shadow` et `/etc/group` suivant le format suivant
`echo "+::::::" >>/etc/passwd`
`echo "+:::::::" >>/etc/shadow`
`echo "+:::" >>/etc/group`

Configuration du client NIS

- Editer `/etc/nsswitch.conf`, et veuillez à la présence active des lignes:

`passwd: files nis`

`group: files nis`

`hosts: files nis dns`

- Relancer le serveur NIS
- Se connecter en tant qu'utilisateur NIS en fournissant le login/pass NIS

NIS et NFS

- Nous voudrions créer un système de fichiers NFS exporté et partagé entre les utilisateurs NIS de telle sorte que :
 - Lorsque l'utilisateur s'authentifie en utilisant un compte NIS à partir de sa machine, il se connecte à un service NFS.
 - Une fois connecté, son répertoire personnel situé dans le serveur NFS sera automonté sur sa machine cliente
- Ce système va permettre
 - plus de liberté de mobilité à l'utilisateur qui se connecte de n'importe quel machine autorisée
 - Plus de contrôle sur les utilisateurs

NIS et NFS

- Préparer le partage NFS dans le serveur à travers le fichier `/etc/exports`
`mkdir /home/nis`
- Dans `/etc/exports`
`/home/nis 192.168.0.1/24(sync,rw,no_root_squash,no_subtree_check)`
- Exporter le répertoire avec la commande
`Exportfs -a`
- Préparer le système NIS
 - Éditer `/etc/auto.master` et rajouter:
`/home/nis /etc/auto.home`
- Éditer le fichier `/etc/auto.home`
* `-rw,hard,intr,nosuid,rsize=8192,wsiz=8192 machine-client:/home/nis/&`
- Dans le répertoire `/var/yp` exécuter la commande `make` pour mettre à jours le système NIS

NIS et NFS

- Coté client:
 - Il faut installer le paquet autofs avec la commande :
`apt-get install autofs`
 - Éditer le fichier `/etc/auto.master` et rajouter la ligne:
`+auto.master`
 - Redémarrer le service autofs
`/etc/init.d/autofs restart`
 - Vérifier l'état d'autofs
`/etc/init.d/autofs status`
- Tester son compte NIS:

Se connecter avec le compte client NFS et vérifier que son répertoire personnel est un répertoire monté du serveur NFS