



Université Sidi Mohamed Ben Abdellah
Ecole Supérieure de Technologie de Fès
Filière: : Réseaux & Télécoms



Services réseau sous Linux

NFS : Network File System

Présenté par:

- MOHAMMED JANATI

Année universitaire : 2019-2020



Introduction

- Network File System:

- Partage de données entre plusieurs machines
- Données potentiellement stockées sur une autre machine
- Lecture et écriture doivent se faire à travers le réseau
- Aussi appelé systèmes de fichiers distribués

- Avantages des systèmes de fichiers réseau (NFS)

- Facile à partager si les fichiers sont disponibles sur plusieurs machines
- Plus facile d'administrer le serveur que les clients

- Désavantages (NFS)

- Réseau plus lent que le disque local
- Réseau ou serveur peuvent échouer même lorsque le client OK
- Complexité, problème de sécurité (en cas de mal configuration)

NFS et les RPC

- NFS repose sur les RPC (Remote Procedure Calls)
 - Utilisation du portmapper (programme *portmap* de Linux)
 - Portmapper = conversion des n° de prog RPC en n° de ports)
- Déroulement d'une RPC
 - Serveur RPC:
 - Indique à *portmap* le port qu'il utilise et les n° de prog RPC qu'il gère
 - Envoi d'une requête RPC par un client:
 - Il contacte *portmap* du serveur pour connaître le numéro de port du programme souhaité
 - Il envoie les données au port correspondant

Description du protocole NFS



- NFS est composé de 4 protocoles utilisant les RPC
- 1. nfs = programme **nfsd**
 - Authentification + Création, recherche, lecture et écriture de fichiers
- 2. mountd
 - Montage des systèmes exportés (mount et unmount)
- 3. nsm (Network Status Monitor) = programme **statd**
- 4. nlm (Network Lock Manager) = programme **lockd**
 - Section critique (lock les fichiers utilisés)

Installation

- Installation des paquets
 - Apt-cache search nfs : nfs-kernel-server, nfs-common
- Lancement des démons
 - Vérifier **portmap** : rpcinfo-p
 - Lancer **mountd** et **nfs** s'ils ne le sont pas

```
rpcinfo -p
  program no_version protocole  no_port
    100000      2    tcp      111  portmapper
    100000      2    udp      111  portmapper
    100005      2    udp      745  mountd
    100005      1    tcp      747  mountd
    100003      2    udp      2049 nfs
    100003      1    tcp      2049 nfs
```

Configuration du serveur

- Fichier /etc/exports
 - Chaque ligne contient le répertoire à exporter et la liste des machines autorisées à y accéder
 - Ex : /home gtrnet01(rw) gtrnet02(ro) ...
- Formulation des noms de clients:
 - Nom de machine : attention à la résolution des noms
 - Un netgroup si on utilise NIS : @gtrlinux
 - Une adresse IP
- Les options:
 - rw et ro : le client peut lire et écrire ou lire uniquement
 - Man exports pour avoir la liste complète des options



Redémarrage du serveur

- Pour que les modifications soient prises en compte:
 - **Exportfs** : transmet les modifications au serveur
 - Ou **/etc/init.d/nfs-kernel-server restart** (qui fait appel à exportfs)
- Fichiers important dans **/var/lib/nfs/**
 - **rmtab, etab, xtab** : utilisés par le noyau pour savoir si un client est autorisé à monter un répertoire NFS



Client

- Pour monter un SF NFS, il existe deux solutions:
 - 1. `mount nom_serveur:/nom_rep /nom_point_de_montage`
 - 2. `/etc/fstab` : ajouter une ligne
 - `/gtr-serv:/home /home nfs defaults 0 0`
- Options de montage (`man nfs(5)`):
 - `Rsize, wsize` : taille des blocs en lecture ou en écriture
 - `Soft, hard`: type de gestion des pannes du serveur
 - `Noexec, nosuid` : gestion de l'exécution de programme sur le SF NFS

Exemple complet

- gtr-serv veut partager le répertoire /gtr-serv0 avec gtrnet01 pour un espace de sauvegarde.
- Sur gtr-serv
 - Ajouter la ligne suivante à /etc/exports
/gtr-serv0 gtrnet01(rw)
 - Relancer nfs :
/etc/init.d/nfs-kernel-server restart *ou* exportfs
- Sur gtrnet01 : Monter le répertoire /gtr-serv0
 - mkdir /gtr-serv0 : on crée le point de montage
 - mount gtr-serv:/gtr-serv0 /gtr-serv0



Lenteur de NFS

- NFS = protocole lent
 - Sur-coût en bande passante
 - Plus lent que ftp, http, ssh ...
- Utilise les RPC et 4 protocoles
- Selon les options de montage, les problèmes de contact avec le serveur peuvent bloquer la machine un certain temps
- NFS n'est utilisable que sur un réseau local à débit élevé
 - N'essayer pas avec un modem

Sécurité de NFS

- Sécurité côté client : ne pas faire confiance au root du serveur
 - Option *nosuid* de mount : pas de démarrage de programmes suid depuis le système nfs
- Sécurité côté serveur
 - Option *root_squash* dans /etc/exports : transforme l'UID 0 en UID de l'utilisateur *nobody* (active par défaut : vérifier simplement que *no_root_squash* n'est pas présente)
- Firewalls
 - Routeurs ou firewall : couper les ports 2049 (nfsd), 749 (portmapper), 745 et 747 (mountd)

Sécurité de NFS : portmapper

- Portmapper utilisé par nfsd, mountd,
- Fichiers /etc/hosts.allows et /etc/hosts.deny
 - Editer /etc/hosts.deny : portmap : ALL (on refuse l'accès à quiconque)
 - Puis /etc/hosts.allow pour rouvrir à quelques machines connues
- Exemple : ajouter toutes les machines d'un réseau
 - /etc/hosts.allow : portmap :
194.56.88.0/255.255.255.0
 - ATTENTION : mettre les @IP non les noms de machines

Récapitulatif

