Samba ou PC-NFS ?

Présenté le 13 février 1995 au groupe

Sécurité Unix et Réseaux

Christophe Wolfhugel - wolf@pasteur.fr

Accéder aux ressources Unix

- Utilisation d'imprimantes gérées par des vrais systèmes
- Utilisation d'espace disque privé ou partagé, sur un serveur
- La où la solution Apple (Appleshare) existe et fonctionne depuis des lustres, les PC ne bénéficient que de solutions bizarres
- Samba et PC-NFS sont deux de ces solutions

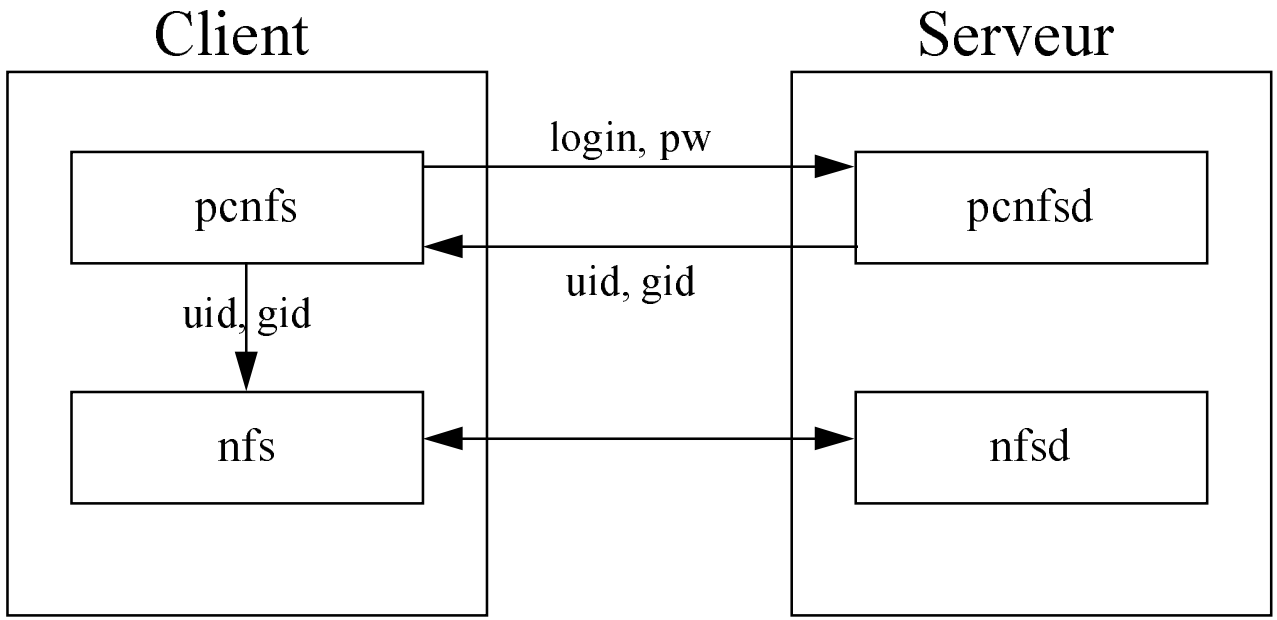
Ressources partageables

- Imprimantes
  - protocole standard : lpd, supporté par certains logiciels (Chaméléon TCP/IP par exemple)
  - impression par NFS (PC-NFS)
  - SMB (Samba), Netbios dans TCP/IP
- Fichiers
  - NFS est un protocole standard, mais sans sécurité
  - SMB (Samba), Netbios dans TCP/IP

Fonctionnement de PC-NFS

- Un serveur d'authentification
  - programme pcnfsd sur le serveur Unix
  - reçoit des requêtes de clients, vérifie l'identité du demandeur, renvoie son *uid* et son *gid*
- Un client qui demande *uid* et *gid* à son serveur pcnfsd
- Accès aux ressources par NFS, mais sans aucun lien avec l'authentification

Relation entre pcnfsd et nfsd



L’arnaque dans PC-NFS

- L’accès aux ressources et l’authentification sont deux opérations totalement disjointes
- La confiance que l’on accord à un client est reportée sur la confiance accordée au logiciel client (zéro avec un micro)
- Toute personne connaissance *uid*, *gid* et point de montage peut passer à travers la sécurité de PC-NFS et accéder aux ressources

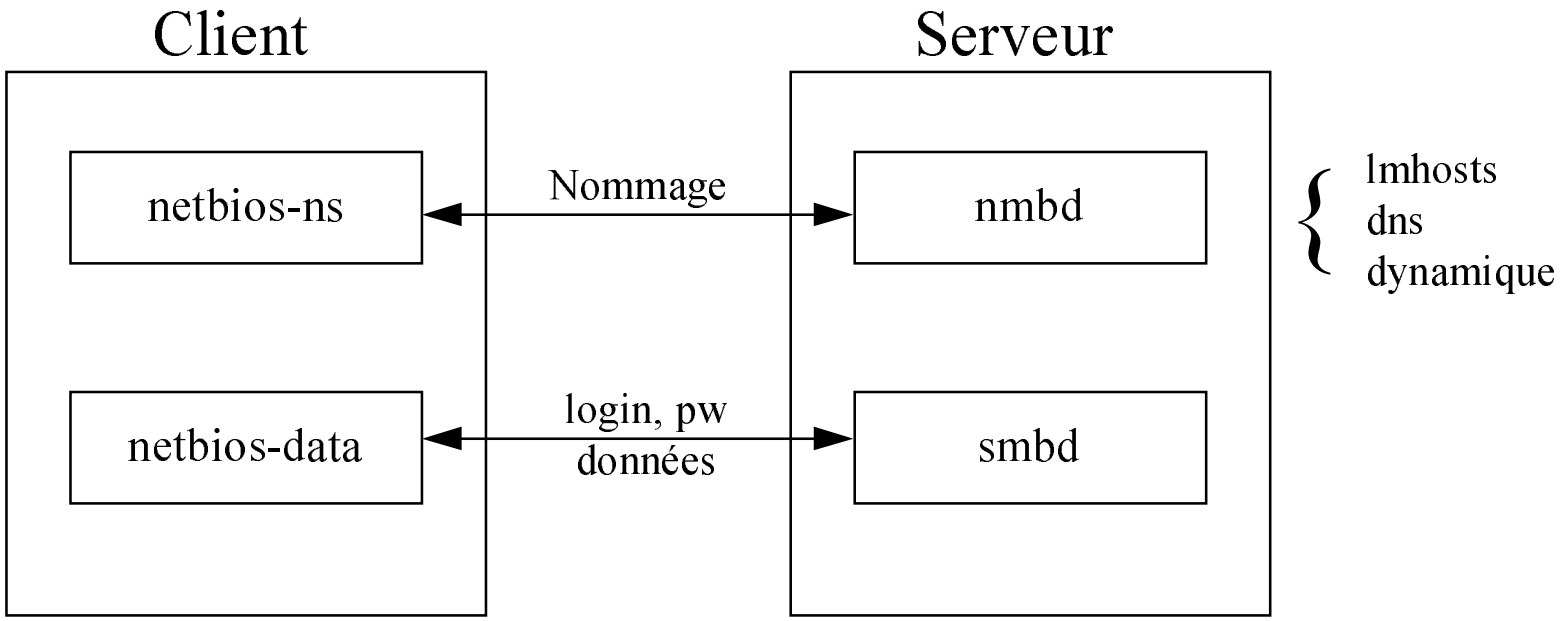
Fonctionnement de Samba

- SMB au-dessus de TCP (en gros du Netbios)
- NMD au-dessus d'UDP (service de nommage, le DNS de Netbios)
- Fonction serveur WINS très limitée
- Fonction Master Browster d'un domaine assez réduites et difficiles à utiliser
- Permet à tout client SMB (WfW, WNT, W95) de se connecter à un serveur Unix

Identification des utilisateurs

- Possibilité de ressources accessibles sans restrictions (compte nobody en général)
- Identification des utilisateurs par mot de passe
  - limite dans les mots de passe du réseau Microsoft
    - sont convertis en majuscules, tous les caractères ne sont pas autorisés
- Les sessions étant en TCP, l'identification se fait à l'ouverture de chaque session
- Il y a donc une vraie sécurité d'accès

Identification des machines

- Le réseau Microsoft utilise beaucoup la diffusion
- Il est possible d'utiliser un serveur de noms WINS
  - dispose d'une base locale
  - assure l'enregistrement dynamique de nouveaux noms
- Utilisation d'une base statique sur chaque machine
  - fichier lmhosts
- Utilisation du DNS pour résoudre les noms
  - nommage peu adapté au DNS

Relations entre client et serveur