TP d'administration UNIX 2
Les bases 2

Matthieu Pérotin

30 janvier 2006

Résumé

Ce deuxième TP a pour objectif de continuer l'apprentissage des commandes de bases lorsque l'on fait de l'administration.

1 Inventaire suite et fin

Nous allons commencer par compléter notre inventaire de la semaine dernière, qui demeure incomplet. Merci de vérifier qu'il ne reste pas de point d'intérrogation, et de mettre les références exactes des machines.

2 SSH

SSH signifie Secured SHell. Il s'agit d'un outil d'une grade puissance qui est tout à fait indispensable dès que l'on souhaite faire de l'administration à distance.

2.1 Prémisses

L'accès à un ordinateur à distance est géré par le service ssh. Lancez ce service. Créez un compte utilisateur pour les autres avec la commande `adduser invite` et rentrer toto comme mot de passe.

Connectez vous à distance sur une autre machine en utilisant la syntaxe :
`ssh invite@IPmachine`

2.2 Transfert de fichiers

La commande `scp` est équivalente à la commence `cp` classique à celà prêt qu'elle permet de copier des fichier à travers le réseau en utilisant ssh.

Regardez la syntaxe de scp dans sa page de manuel. Essayer de copier un fichier quelconque d'un poste distant vers votre poste.

2.3 Transfert de fichiers façon ftp

ssh fournit aussi un mécanisme client serveur à la façon de ftp. La syntaxe de la commande est `sftp user@host`

Connectez vous par sftp à un poste client. La commande ls permet de lister le contenu du répertoire distant. La commande get fichier permet de télécharger un fichier, et put fichier d'envoyer un fichier.

Testez sftp dans plusieurs cas de figure, envoie d'un fichier, réception, changement de répertoire local etc. Vous pouvez vous référer à la page de manuel correspondante pour plus de détail sur les commandes disponibles.

2.4 Authentification sans mot de passe

ssh utilise un système de cryptage asymétrique. Toutes les communications sont cryptées et de façon forte (RSA ou DSA).

On peut profiter de ce cryptage assymétrique pour se libérer de taper un mot de passe pour s'authentifier : on peut utiliser le seul fait de posséder la clef privée associée à un compte comme moyen d'authentification sûr.

Il faut commencer par créer une paire de clefs assymétriques associées à un compte. En tant qu'un utilisateur autre que knoppix tapez la commande

```
ssh-keygen -t dsa
```

Cela a pour effet de générer une paire de clef assymétrique. Ne rentrez rien comme "pass phrase".

La clef générée est stockée dans le fichier .id_dsa.pub et .id_dsa du répertoire .ssh de votre répertoire personnel.

Pour activer le login sans mot de passe sur un autre poste, notons le A, il faut que le fichier .ssh/authorized_keys2 contienne la clef publique du compte voulant accéder à A. À l'aide de la commande scp commencez par copier votre fichier .id_dsa.pub sur le poste distant auquel vous voulez accéder. Attention : votre clef privée doit bien évidemment rester confidentielle !

Une fois cette action effectuée, ajoutez le contenu de votre fichier .id_dsa.pub au contenu de authorized_keys2, en utilisant par exemple la commande cat et un opérateur de redirection.

Il ne vous reste plus qu'à tester. Que pensez vous de ce moyen de vous loguer à distance ?

3 NFS

3.1 Description

NFS propose un mécanisme simple et classique de partager des morceaux entiers de l'arborescence Unix. C'est une solution très utilisée et finalement très actuelle malgré son age.

3.2 Description des partages

La définition des répertoires que l'on souhaite partager se fait par l'intermédiaire du fichier `/etc/exports` (man exports). Essayez d'y ajouter une ligne "/cdrom *(sync,ro)" et lancez le serveur

- /etc/init.d/portmap start
- rpc.statd && rpc.mountd
- /etc/init.d/nfs-common start
- /etc/init.d/nfs-kernel-server start

3.3 Montage d'un dossier distant

La commande à utiliser est la commande mount. Sa syntaxe est :

```
mount -t nfs serveur:/repertoire/partage cheminlocal
```

Testez diverses configuration restrictive de /etc/exports. N'oubliez pas qu'après chaque modification nfs-kernel-server doit être relancé.

4 SSH avancé : forwarding de port

4.1 Configuration restrictive d'apache

Editez le fichier /etc/apache/httpd.conf pour interdir l'accès à tous sauf à l'IP locale et à 127.0.0.1 (C'est juste au dessus de ¡/Directory¿

Lancez apache et testez la connexion depuis l'ordinateur local, puis par un autre ordinateur.

D'un ordinateur distant lancez la commande :

```
ssh -L 9999:localhost:80 invite@IPServeurApache
```

Connectez vous depuis cet ordinateur sur l'url http ://localhost :9999.

Que se passe-t-il ?