

Réseaux et Administration Web

Outils d'Administration Système

2015

Les TPs seront réalisés sous GNU/Linux. Pour commencer, démarrez une machine sous GNU/Linux et connectez-vous en utilisant vos login et mot de passe habituels.

Partie 1 Outil d'Administration Système

Exercice 1 : Introduction

Pour pouvoir utiliser les outils d'administration système, vous devez être **root** (administrateur) sur votre machine. Pour cela, on utilisera une machine virtuelle.

1. Téléchargez l'image de la machine virtuelle depuis la page de l'UE <http://cedric.cnam.fr/~taktaks/NFA083/>
2. Importez la machine virtuelle dans VirtualBox
 - (a) Ouvrir VirtualBox
 - (b) Dans le menu *File*, cliquez sur *Import Appliance*

Deux comptes utilisateurs sont définis :

1. Un compte utilisateur standard
 - identifiant (*login*) : **eleve**
 - mot de passe (*password*) : **azeaze**
2. Un compte administrateur :
 - identifiant (*login*) : **root**
 - mot de passe (*password*) : **azeaze**

Exercice 2 : `sudo`

1. Installez le programme **sudo** avec la commande suivante (figure 1) :

```
$ apt-get install sudo
```

2. Ajoutez votre identifiant à la liste des personnes appartenant au groupe **sudo** avec la commande **usermod** ;
3. Connectez vous avec votre identifiant et vérifiez que vous appartenez bien au groupe **sudo** avec la commande **id** ;

```

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@NFA083-VM:~# apt-get install sudo
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Les NOUVEAUX paquets suivants seront installés :
  sudo
0 mis à jour, 1 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 611 ko dans les archives.
Après cette opération, 967 ko d'espace disque supplémentaires seront utilisés.
Réception de : 1 http://security.debian.org/ squeeze/updates/main sudo amd64 1.7
.4p4-2.squeeze.4 [611 kB]
611 ko réceptionnés en 0s (1 342 ko/s)
Sélection du paquet sudo précédemment désélectionné.
(Lecture de la base de données... 48172 fichiers et répertoires déjà installés.)
Dépaquetage de sudo (à partir de ../sudo_1.7.4p4-2.squeeze.4_amd64.deb) ...
Traitement des actions différées (« triggers ») pour « man-db »...
Paramétrage de sudo (1.7.4p4-2.squeeze.4) ...
No /etc/sudoers found... creating one for you.
root@NFA083-VM:~#

```

FIGURE 1 – Installation de la commande `sudo`

4. Tentez de lister le contenu du répertoire `/root`

```
$ ls /root
```

5. Maintenant essayez de lister le contenu du répertoire `/root` en utilisant la commande `sudo`

Exercice 3 : Création d'un nouvel Utilisateur

1. Créez un nouvel utilisateur en utilisant la commande `useradd`. Cette utilisateur devra avoir comme groupe secondaire le groupe `sudo` en utilisant une option de la commande `useradd`;

Remarque 1 *Pour localiser une commande, vous pouvez utiliser `whereis` :*

```
$ whereis useradd
useradd: /usr/sbin/useradd
/usr/share/man/man8/useradd.8.gz
```

2. Initialisez le mot de passe de ce nouvel utilisateur en utilisant la commande `passwd`;
3. Connectez vous avec l'identifiant de ce nouvel utilisateur pour vérifier qu'il a bien été créé et qu'il appartient au groupe `sudo`

Exercice 4 : Fichier de Configuration

1. Listez le contenu du répertoire `/etc` ;
2. À quoi correspondent les fichiers et répertoires suivants ?

- `debian_version`
- `group`
- `passwd`
- `protocols`
- `services`
- `shadow`
- `sudoers`
- `bind/`
- `apache2/`

Utiliser les pages de manuels ou info pour obtenir des renseignements sur ces fichiers.

3. Utilisez un éditeur de texte pour modifier le fichier `hostname`. Le fichier `hostname` doit contenir un seul mot composé de caractères alphanumériques ;
4. Redémarrez la machine en utilisant la commande `shutdown` :

```
> sudo shutdown -r now
```

Que constatez-vous ?

Partie 2 Outils d'Administration Réseaux

Exercice 1 : ip

Cette commande permet de configurer les interfaces réseau de la machine. Avec l'argument `addr` elle permet d'afficher la liste des interfaces disponibles et les adresses associées. Cette commande remplace la commande `ifconfig`. Les interfaces Ethernet ont pour nom « `eth` » plus un numéro d'ordre.

Exécuter la commande `ip` et identifier :

- les interfaces actives ;
- l'adresse physique de la carte réseau active ;
- l'adresse IP correspondante et sa classe ;
- l'adresse de sous-réseau ;
- le masque correspondant ;
- l'adresse de broadcast.

Exercice 2 : ping

La commande `ping` permet de vérifier si une machine est présente sur le réseau en envoyant des messages ICMP de type « *echo request* ». La machine distante répond par des messages ICMP de type « *echo reply* ». Cet outil indique le RTT (*Round Trip Time*) qui est le temps d'aller retour des paquets entre les machines ainsi que le TTL (*Time to Live*) qui est le temps de vie des paquets.

La commande `ping` s'utilise de la façon suivante :

```
ping -options nom_de_la_machine
```

Le nom de la machine peut être remplacé par son adresse IP. L'option `-c` permet de spécifier le nombre de paquets que l'on souhaite envoyer. L'option `-s` permet de spécifier la taille des paquets que l'on souhaite envoyer.

```
ping -c 10 ma_machine permet d'envoyer 10 paquets à ma_machine
ping -s 100 ma_machine permet d'envoyer des paquets de 100 octets à ma_machine
```

1. Exécuter `ping` sur la machine locale ;
2. Exécuter `ping` à destination d'adresse IP ou URL quelconques et regarder :
 - la valeur du RTT. Cette valeur est-elle pertinente pour estimer la charge du réseau ?
 - la valeur de TTL. Quelle est la machine qui fixe cette valeur ?
3. Tester différentes options comme le nombre, la taille ou la durée de vie des paquets.
4. Tester la commande suivante `ping -M do -s 4000 -c 10 www.cnam.fr` ;
 - Quel résultat obtenez-vous ?
 - Que signifie l'option `-M do` ? À quoi cela peut-il servir ?

Exercice 3 : arp

Le protocole de résolution dynamique d'adresses, ARP (*Address Resolution Protocol*), permet à un ordinateur de trouver l'adresse physique d'un ordinateur cible situé sur le même réseau local. La commande `arp` (`/usr/sbin/arp`) permet d'afficher et de modifier le cache ARP qui contient la table des associations adresse IP, adresse physique pour chaque carte réseau.

1. Afficher et analyser la table ARP ;
2. Trouver la façon d'ajouter à la table le couple d'adresse physique/logique d'une machine du même réseau local ;
3. Déterminer le fabricant des cartes Ethernet à partir de leurs adresses physiques présentes dans le cache. Pour cela se rendre à l'URL http://coffer.com/mac_find/ ;
4. Déterminer l'option de la commande `ip` permettant d'afficher la table ARP.

Exercice 4 : traceroute

Cette commande permet de connaître la route (ensemble des nœuds d'interconnexion) qui ont été traversés avant d'arriver à destination. C'est le même protocole que pour `ping` qui est utilisé, avec des options différentes. La commande est utilisable pour détecter des problèmes sur les différentes machines traversées entre un émetteurs et un destinataire. La commande `traceroute` comporte comme principal paramètre une adresse IP ou un nom de domaine.

1. Lancer la commande et commenter les différents champs des lignes de réponse ;
2. Que peut-on en déduire concernant le chemin emprunté ?

Exercice 5 : route

Pour permettre à une machine d'envoyer des paquets sur un réseau qui ne lui est pas directement connecté, il faut positionner les tables de routage. Cela peut se faire grâce à un protocole de routage dynamique (comme RIP, EGRP, ...) ou de manière statique avec la commande `route`. Cette commande permet de préciser quel sortie doit prendre un paquet pour atteindre une destination.

1. Exécuter la commande `route` pour afficher la table de routage et identifier :
 - les différents champs de la table ;
 - la route utilisée pour communiquer avec une machine qui se trouve sur le même réseau ;
 - la route par défaut ;
 - l'adresse IP de la passerelle.
2. Exécuter la commande `ip` avec l'option `route`. Comparer le résultat obtenu avec celui de la commande `route`.

Exercice 6 : netstat

`netstat` est un utilitaire permettant d'obtenir des informations sur l'état des interfaces réseau, des tables de routage, des connexions TCP, UDT, ...

Exécuter la commande `netstat` avec différentes options et afficher :

1. toutes les connexions TCP actives et les ports TCP et UDP sur lesquels l'ordinateur écoute ;
2. les statistiques Ethernet comme le nombre d'octets et de paquets envoyés et reçus ;
3. les interfaces réseaux et leur statistiques ;
4. le contenu de la table de routage ;
5. les statistiques par protocole.