

Fiabilité et sécurité du DNS



Quelques bases UNIX

Notre plateforme

FreeBSD 9.1 64 bit

- UNIX OS, version BSD
- Plus de 30 ans d'histoire
- Pas d'interface graphique, on utilise SSH pour administrer
- On pourrait utiliser d'autres plateformes...
 - Ubuntu, Debian, CentOS/RedHat, ...
- Ceci n'est pas un cours d'admin UNIX
 - Les exercices sont souvent pas à pas
 - Demandez de l'aide à vos voisins ou à l'instructeur



Quelques choses à savoir...

Être *root* quand cela est nécessaire:

```
sudo <cmd>
```

Installation de paquets:

```
pkg add <package_name>
```

Rédiger un fichier:

```
sudo ee /etc/motd
```

```
sudo vi /etc/motd
```

Les éditeurs installés sont ee, jed, joe and vi*

L'éditeur vi

- L'éditeur par défaut sous UNIX
- Difficile au premier abord
- Si vous connaissez déjà vi, allez-y!
- Il y a un PDF de référence disponible dans les ressources supplémentaires sur le wiki



Autres éditeurs

ee

- ESC fait apparaître un menu
- Les touches fléchées fonctionnent

jed

- F10 fait apparaître un menu
- Les touches fléchées fonctionnent

joe

- Ctrl-k-h fait apparaître un menu
- Ctrl-c pour annuler
- Les touches fléchées fonctionnent

Autre outils

Arrêt d'un programme au 1er plan: CTRL+C

```
$ ping yahoo.com
```

```
PING yahoo.com (67.195.160.76): 56 data bytes
```

```
64 bytes from 67.195.160.76: icmp_seq=0 ttl=45 time=221.053 ms
```

```
64 bytes from 67.195.160.76: icmp_seq=1 ttl=45 time=224.145 ms
```

```
^C ← ici appuyer sur CTRL + C
```

Naviguer le système de fichiers:

```
- cd /etc
```

```
- ls
```

```
- ls -l
```

Renommer et supprimer des fichiers:

```
- mv file file.bak
```

```
- rm file.bak
```

Arrêt et démarrage des services

Méthode standard:

```
sudo service named [stop|start|  
restart]
```

Vérifier qu'un processus tourne, par nom:

```
-ps auxwww | grep http
```

```
gollum# ps auxwww | grep http  
root      2694  0.0  0.2 147672  6592 ??  Ss   5:32AM  0:00.03 /usr/local/sbin/httpd -DNOHTTPACCEPT  
www       2695  0.0  0.2 147672  6900 ??  I    5:32AM  0:00.00 /usr/local/sbin/httpd -DNOHTTPACCEPT  
www       2696  0.0  0.2 147672  6900 ??  I    5:32AM  0:00.00 /usr/local/sbin/httpd -DNOHTTPACCEPT  
www       2697  0.0  0.2 147672  6588 ??  I    5:32AM  0:00.00 /usr/local/sbin/httpd -DNOHTTPACCEPT  
www       2698  0.0  0.2 147672  6588 ??  I    5:32AM  0:00.00 /usr/local/sbin/httpd -DNOHTTPACCEPT  
www       2699  0.0  0.2 147672  6588 ??  I    5:32AM  0:00.00 /usr/local/sbin/httpd -DNOHTTPACCEPT  
www       2700  0.0  0.2 147672  6908 ??  I    5:32AM  0:00.00 /usr/local/sbin/httpd -DNOHTTPACCEPT  
www       2701  0.0  0.2 147672  6780 ??  I    5:32AM  0:00.00 /usr/local/sbin/httpd -DNOHTTPACCEPT  
www       2702  0.0  0.2 147672  6704 ??  I    5:32AM  0:00.00 /usr/local/sbin/httpd -DNOHTTPACCEPT  
www       2749  0.0  0.2 147672  6896 ??  I    5:34AM  0:00.00 /usr/local/sbin/httpd -DNOHTTPACCEPT  
root      4072  0.0  0.0  10056  1088 v0  I+   5:40AM  0:00.00 tail -f /var/log/httpd-access.log  
root      4091  0.0  0.0  16424   1472  2  S+   5:44AM  0:00.00 grep http
```

Viewing files

Parfois on visualise les fichiers via un visualisateur texte page à page (“more”, “less”, “cat”). Exemples:

```
man sudo
```

```
less /usr/local/etc/nagios/nagios.cfg-sample
```

- `<espace>` pour passer à la page suivante
- `“b”` pour aller en arrière
- `“q”` pour quitter
- `“/”` et une chaîne à rechercher (`/text`)

Dépannage: les fichiers de journaux

Les fichiers de journaux sont indispensable pour faire du dépannage d'application. La plupart d'entre eux se trouvent sous /var/log

Quelques fichiers de journaux biens connus:

`/var/log/messages`

`/var/log/httpd-error.log`

`/var/log/maillog`

`/etc/namedb/log/*` (dans cet atelier)

Pour voir la fin d'un fichier de journaux:

```
tail /var/log/messages
```

Pour voir les nouveaux messages au fur et à mesure qu'ils arrivent

```
tail -f /var/log/messages
```

Se connecter par SSH à vos machines virtuelles

Logez vous à l'aide ssh sur votre machine.

Sous windows, on peut utiliser putty:

<http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe>

ou

<http://noc.ws.nsrc.org/>

Se connecter en tant que “*sysadm*” à:

- auth1.grpX → 10.10.X.1
- auth2.grpX → 10.10.X.2
- resolv.grpX → 10.10.X.3

... où “X” est le numéro de votre groupe. Le mot de passe vous est donné en classe.

Se connecter:

Linux/MacOS

Ouvrir un terminal, puis:

```
ssh -l sysadm auth1.grpX.ws.nsrc.org
```

Windows

Putty (ou un autre client SSH) puis ouvrir:

```
auth1.grpX.ws.nsrc.org
```

1. En tant qu'utilisateur "*sysadm*"
2. Accepter la clé
3. Refaire pour `resolv.grpX` et `auth2.grpX` (si présents)

"X" est le numéro de votre groupe

Une fois logés...

- Expérimenter avec l'éditeur `ee`
 - ... ou `vi` ou `joe` ou `jed` si vous préférez
- Changez le message `/etc/motd` pour “personnaliser” votre machine.
 - `sudo ee /etc/motd`
- Dé-logez vous et relogez vous pour voir l'effet de vos changements. Répéter pour `auth2` et `resolv`

Questions

?