Operación y Seguridad de DNS

Conceptos básicos de Unix

Nuestra opción de plataforma

FreeBSD 9.0 64 bits

- UNIX, variante BSD
- 30 años de historia
- Sin GUI, todo sobre SSH

- Se podría usar otras plataformas:
  - Ubuntu, Debian, CentOS/RedHat, …
- Este no es un curso de administración de UNIX
  - Las hojas de trabajo son prácticamente paso a paso
  - Por favor, ayúdense unos a otros y pidan ayuda

Algunas cosas que tendremos que hacer

Ser *root* cuando sea necesario: `sudo <cmd>`

Instalar paquetes:

```
pkg_add -r <package_name>
```

Editar ficheros:

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

Los editores instalados son ee, jed, joe y vi*

Editor vi

- El editor por defecto en todos los UNIX
- Puede ser difícil de usar al principio
- Si lo conoce, utilícelo
- Hay una hoja de referencia en la wiki del taller

Otros editores

ee

- Se saca el menú con ESC
- Los cursores funcionan como se espera

jed

- F10 muestra el menú
- Los cursores funcionan como se espera

joe

- Ctrl-k-h muestra el menú
- Ctrl-c aborta
- Los cursores funcionan como se espera

Otras herramientas

Terminar el programa en primer plano: 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      ← aquí haga CTRL + C
```

Curiosear por el sistema de ficheros:

- `cd /etc`
- `ls`
- `ls -l`

Renombrar y borrar ficheros

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

Iniciar y detener servicios

Método estándar

- `/etc/rc.d/named restart`

Revisar si un proceso está corriendo

- `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
```

Visualizar ficheros

A veces los ficheros se ven a través de programas de paginación (“more”, “less”, “cat”). Ej:

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

- Barra espaciadora para pasar la página
- “b” para moverse hacia atrás
- “q” para salir (quit)
- “/” y un patrón (/texto) para buscar

“`less` is more”

Depuración: Bitácoras (logs)

Los logs son esenciales para resolver problemas. Residen (generalmente) en /var/log/

Algunos logs famosos son:

/var/log/messages
/var/log/httpd-error.log
/var/log/maillog
/etc/namedb/log/* (this class only)

Para ver las últimas entradas en el log:

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

Para ver las líneas a medida que ocurren:

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

Conectarse remotamente via SSH

Ingrese a su máquina virtual con ssh. En Windows, use SecureShell o Putty. Descárguelo de la wiki del taller.

Conéctese como usuario "*adm*" a:

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

Donde "X" es su número de grupo. El password se revelará en clase.

Ingresar

Linux/MacOS

Primero, abra una terminal, y luego:

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

Windows

Putty (u otro programa de SSH) conéctese a:

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

1. Como user "*adm*"
2. Acepte la clave pública
3. Repita para `auth2.grpX` y `resolv.grpX`

"X" es el número de su grupo

Una vez haya ingresado…

- Experimente con el editor `ee`
  - … o `vi` o `joe` o `jed` si prefiere
- Edite el “mensaje del día” para identificar su máquina virtual como la suya:
  - `sudo ee /etc/motd`
- Salga e ingrese de nuevo para ver sus cambios. Repita lo mismo para cada máquina virtual…

Preguntas?

?