

Herramientas básicas de Linux

Introducción

Las herramientas siguientes son indispensables cuando utilizamos un sistema linux. Se puede obtener una descripción más amplia de los comandos con la opción `--help`, el comando `man` y el comando `info`. Ejemplo `netstat --help`, `man netstat` o `info netstat`. Recuerde que GNU/Linux distingue mayúsculas y minúsculas (el comando `ping` existe, pero no el comando `Ping`).

ping

Este comando es bien conocido. Existe en todos los sistemas. Permite verificar si una máquina remota responde. La sintaxis es muy simple: `ping -c 5 213.186.xx.xx` para enviar 5 pings a la máquina cuya dirección IP es `213.186.xx.xx`. También se puede utilizar el nombre de la máquina si está referenciado en el fichero `Hosts` o en un servidor DNS. Podemos, por ejemplo, utilizar `ping` para verificar si la conexión está todavía activa o para establecerla. Si no añade la opción `-c 5` para enviar sólo 5 pings el comando no se detiene. Hay que utilizar entonces `Ctrl C`. Existe otra herramienta más completa, pero no está instalada por defecto: `hping`.

ifconfig

`ifconfig` permite conocer y cambiar la configuración de las tarjetas de red.

- Para cambiar la configuración de las tarjetas de red, teclee:

```
ifconfig eth0 213.186.xx.xx netmask 255.255.255.0 broadcast 213.186.xx.255
```

- Como los valores que acabamos de dar son estándar, puede simplemente teclear:

```
ifconfig ETH0 213.186.xx.xx (la máscara de red y el broadcast propuestos corresponden a una dirección de clase C)
```

- Atención en el reinicio de la máquina, ya que este cambio se perderá. Hay que modificar el fichero:

```
clas/etc/sysconfig/network-script/ifcfg-eth0.
```

OVH

- Puede utilizar `linuxconf` para simplificar la tarea.
- También se puede desactivar una tarjeta de red :

```
ifconfig eth0 down
```

- Y por su puesto reactivarla:

```
ifconfig eth0 up
```

`arp`

El comando `arp` permite hacer la correspondencia entre las direcciones IP y las direcciones MAC. Las opciones posibles más importantes son:

- `arp -a` para obtener todas las entrada ARP de la tabla
- `arp -d nombre_de_la_máquina` para suprimir una entrada de la tabla
- `arp -s nombre_de_la_máquina dirección_mac` para añadir una nueva entrada en la tabla<

`route`

Este comando permite ver, añadir y eliminar las rutas declaradas en el la máquina. Para indicar a la máquina dónde encontrar las direcciones que no son las direcciones de la red local debe indicar la pasarela (o gateway) hacia la cual debe enviar todos los paquetes.

- Para ver las rutas indicar `route -n` (también `netstat -nr`). La opción `-n` permite no visualizar la resolución de los nombres.
- Para añadir una ruta por defecto: `route add default gateway 192.168.0.1` (La pasarela hacia la que envía todos los paquetes que no son para la red local).
- Para añadir una ruta hacia una máquina, indicar `route add -host 195.98.246.28 gateway 192.168.0.1` (Indicar el netmask si no es una máscara correspondiente a la clase de su dirección)

- Para añadir una ruta hacia una red indicar `route add -net 195.98.246.0 netmask 255.255.0.0 gateway 192.168.0.1`
- Para suprimir una de estas rutas reemplazar `add` por `del`. El gateway o pasarela corresponde la mayoría de las veces a su router.
- Para obtener la ruta que acaba de añadir cada vez que reinicie, situe el comando en el fichero `/etc/rc.d/rc.local` por ejemplo.

netstat

Permite conocer los puertos en escucha sobre la máquina, sobre qué interfaces, con qué protocolos de transporte (TCP o UDP), las conexiones activas y las rutas.

- Para ver las conexiones activas `netstat -nt`, para los puertos abiertos `netstat -ntl`.
- Podemos también verificar si existe una ruta por defecto, por ejemplo, hacia la máquina `213.186.xx.xx`; utilice `netstat -nr grep 213.186.xx.xx`
- La opción `-a` enumera los puertos en uso o aquéllos que son escuchados por el servidor.
- La opción `-i` proporciona información sobre los interfaces de red.
- La opción `-p` (protocolo) proporciona información (paquetes recibidos, perdidos, reenviados, talla, opciones...) sobre el tráfico de red en el protocolo dado: `netstat -p ip`

lsof

`lsof` permite listar los ficheros abiertos y los procesos activos.

- `lsof -i` indica los procesos de tipo internet.
- Sólo se puede preguntar por un protocolo `lsof -ni tcp:25` o hacia una máquina `lsof -ni @213.186.xx.xx:25`
- Para conocer todos los ficheros abiertos por `/hda1` utilice `lsof /dev/hda1`.
- `lsof -i -a -p 1234` permite conocer todos los puertos abiertos por el proceso 1234 (`-a` es interpretado como AND).
- `lsof -p 1234, 12345 -u 500, nombre_usuario` permite conocer todos los ficheros abiertos por el usuario 500 ou `nombre_usuario` o por el proceso 1234 o 12345.
- Existen comandos para hacer esto (`fuser,ps, netstat..`),pero este es muy completo.

traceroute

Traceroute permite determinar la ruta tomada por un paquete para alcanzar su destino en internet. Podemos utilizar la dirección IP o el nombre de host. Atención: algunos firewall o router no se dejan ver con el comando traceroute.

El comando traceroute es muy útil para saber dónde se puede encontrar un bloqueo (ralentizamiento). Hay un gran número de opciones, entre otras la posibilidad de elegir los gateway (hasta 8) para alcanzar una máquina.

telnet

Telnet es una herramienta indispensable. Existe como cliente en todos los sistemas y como servidor en los Unix. Atención: cada vez es menos frecuente que venga instalado por defecto en las nuevas distribuciones, en su versión servidor.

En su versión servidor permite dar un acceso remoto a la máquina y con él un shell para administrarlo. De todas formas, y por razones de seguridad es preferible utilizar SSH, ya que las contraseñas no viajan en claro en la red. Existen clientes SSH para Windows.

En cambio, el cliente telnet permite hacer otras cosas. Como cliente,

OVH

telnet permite enviar y leer sus mensajes. Permite también comprobar los otros protocolos. Por ejemplo, podemos hacer un telnet Mi_Servidor:ftp 21 para conectarse a un servidor FTP.

Lo mismo con un servidor web: telnet Mi_Servidor:ftp 80.

ftp

FTP es una herramienta que permite descargar ficheros entre máquinas. Hay clientes ftp como ws_ftp. Bajo linux hay un servidor ftp que se activa en /etc/inetd.conf. Viene instalado por defecto en todas las distribuciones. Este servidor ftp no está ligado a la instalación de apache, como en los sistemas Microsoft, donde debe instalar IIS para beneficiarse de este servicio. Atención: el servidor ftp presenta un problema de seguridad importante, utilice SFTP, que está disponible con SSH.

Aquí tiene los comandos que más va a utilizar :

- dir : listar un directorio
- cd nombre_directorio : cambiar de directorio
- get fichero : copiar un fichero hacia el cliente. Se copia en el directorio donde se encuentre.
- mget *: copia todos los ficheros del directorio hacia la estación.
- put fichero : copia un fichero hacia el servidor.
- mput *: copia todos los ficheros que se encuentren en el directorio.
- binary : para copiar en modo binario.
- exit : salir

nslookup

La herramienta nslookup permite preguntar a un servidor de nombres (servidor dns) a fin de obtener información sobre un dominio o una máquina. Por defecto, nslookup utiliza el servidor de nombre configurado sobre su máquina, pero siempre puede preguntar a otro servidor dns
root@xxxxxx / nslookup

host

Comando casi equivalente, pero más fácil de usar

host 213.186.xx.xx Proporciona información sobre el dominio.

host -v -t mx su_dominio Proporciona información sobre los MX del dominio.

host -l -t any su_dominio proporciona todas las máquinas del dominio.

who

Permite conocer los usuarios que están conectados a la máquina.

last

Este comando permite ver las últimas conexiones que han tenido lugar. En realidad, lee el fichero `/var/log/wtmp`.

last presenta todas la información

last david, todas las conexiones del usuario david

last reboot, todos los reboot de la máquina con su fecha.

lastb es una variante de last, en la medida que sólo busca los login incorrectos (fichero `/var/log/btmp`)

finger

Servicio que permite obtener información sobre las cuentas de usuario de la máquina.

Su sintaxis es sencilla: `finger toto@servidor_remoto`

Para obtener más información utilice la opción `-l`

```
root@xxxxx finger -l
```

Netcat

Permite crear conexiones (socket) entre máquinas. Se comporta como un cliente `netcat mi_servidor.com 200` (conexión al puerto 23 de la máquina `mi_servidor.com`) o como servidor `netcat -l -p 80` (escucha el puerto 80). También permite hacer scan de puertos:

- `netcat -t ns213.186.xx.xx 23` Se comporta como un cliente telnet
- `netcat -l -p 23 > espia.log` Escucha el puerto 23 (telnet) y registra en `espia.log` todo lo que teclea el cliente.
- `netcat -l -p 23 < mis_comandos` Ejecuta los comandos que hay en `mis_comandos`
- `netcat -l -p 23 -e mi_comando` Ejecuta el comando tras la conexión.
- `netcat -vv la_machine_a_scanner 1-100` Permite lanzar un scan sobre máquinas remotas.
- `netcat -vv -z -i 10000 -r 127.0.0.1 1-200` Permite hacer un scan aleatoriamente en los puertos 1 a 100 con un timeout. Evitamos la detección.