Ficheros de Configuración de las Redes Linux '&' Comandos Básicos de Networking

Tópicos LPI-2 → Tema 205

carlos briso 30/09/2015

Proceso de Configuración de la Red

→ 0-script de inicio → init.d

→ 1-/etc/hosts

→ 2-/etc/host.conf

→ 3-/etc/resolv.conf

→ 4-/etc/networks

→ 5-/etc/nsswitch.conf

→ 6-/etc/protocols

→ 7-/etc/services

0-Script de inicio init.d

=> Diferente denominación según la variante de Linux.

→ **RedHat/CentOS** /etc/init.d/network *opción*

→ **Debian/Ubuntu** /etc/init.d/networking *opción*

opciones típicas: [start|stop|restart|status|reload]

=> Diferente ubicación.

→ **RedHat** /etc/sysconfig/network-scripts/ifcfg-eth**X**

→ **Debian** /etc/network/interfaces

=> Diferente configuración.

→ **Debian => /etc/network/interfaces**

```
auto eth0
iface eth0 inet static
    address         192.168.1.200
    netmask         255.255.255.0
    network         192.168.1.0
    broadcast       192.168.1.255
    gateway         192.168.1.1
```

→ **RedHat => /etcsysconfig/network-scripts/ifcfg-eth0**

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.200
NETMASK=255.255.255.0
GATEWAY=192.168.1.1
TYPE=ethernet
```

(Es importante configurar y grabar correctamente estos ficheros, porque las configuraciones realizadas con los comandos ifconfig, route o ip son volátiles, y se perderán al reiniciar el Stma.)

1-/etc/hosts

→ Asocia direcciones IP con nombres de hosts.

→ Permite consultar una dirección IP sin mediación del DNS.

=> La consulta es mas rápida que con DNS.

=> Si las IP's cambian la dirección es incorrecta.

→ El nombre y el dominio pueden obtenerse con el comando:

hostname [-d|-f]

→ Ejemplo de Configuración:

127.0.0.1	localhost.localdomain localhost
192.168.1.113	zentyal-academy.lan zentyal-academy.lan
192.168.1.101	ibm00.localdomain ibm
192.168.1.102	server-two.fhflpic2.net extranet.fhflpic2.net intranet.fhflpic2.net www.extranet.net www.intranet.net
192.168.1.103	workstation.fhflpic2.net workstation

→ Podemos Cambiar el Nombre del Host:

Debian:

sudo vi /etc/hostname

sudo vi /etc/hosts

/etc/init.d/networking restart

Red-Hat:

/etc/hostname **(o** /etc/sysconfig/network **o** /etc/HOSTNAME)

echo "192.168.2.200 **CentOS-Server" >> /etc/hosts**

hostname **CentOS-Server**

hostname

service network restart

2-/etc/host.conf

→ Configura el comportamiento de la Resolución de nombres.

→ Indica en que orden se resuelve.

→ En definitiva indica donde se resuelve primero: la dirección, o el nombre del nodo.

→ Su funcionalidad es reemplazada por: **/etc/nsswitch.conf**

→ Ejemplo:

```
order   host,bind
multi   on
```

=> Primero las tablas locales → /etc/hosts.

=> En segundo lugar el DNS.

=> Por último: multi on → Retorna las direcciones válidas que se encuentren en: /etc/hosts

3-/etc/resolv.conf

→ Especifica el dominio y los servidores DNS.

→ Ejemplo:

```
domain server-one.fhf.net
search server-one.fhf.net       fhf.net
nameserver 192.168.1.1
nameserver 192.168.1.100
nameserver 192.168.1.200
```

=> Un máximo de 3 nameserver's → Servidores DNS.

=> Si buscamos (*) un hostname sin dominio:

→ Si lo encuentra Añade: server-one.fhf.net

→ Si NO lo encuentra Añade: fhf.net

(*) Búsquedas DNS → Comandos: **nslookup**, **dig**, **host**

4-/etc/networks

→ Fichero que se mantiene por estandarización.

→ No es IMPRESCINDIBLE por tanto.

→ Asocia nombres a REDES. **(*)**

→ Ejemplo:

=> red-server-one 172.16.1.0

=> red-server-two 172.16.3.0

(*) ATENCIÓN. Se suele confundir con el fichero: /etc/hosts, que Asocia IP's con nombres de Máquinas o sus Alias, NO REDES. La relación se establece univocamente pero a la inversa.

5-/etc/nsswitch.conf

→ Centraliza la información de diferentes servicios para la resolución de nombres.

=> Indica las acciones a realizar para acceder a las diferentes BB. de DD. del Stma. → hosts, contraseñas, servicios, …

=> Reemplaza a: **/etc/host.conf**

=> Es introducido a partir de la versión 2 de la GNU.

→ **Ejemplo:**

hosts: **dns files**

networks: **files**

→ Primero buscará en DNS, después en **/etc/hosts**

→ La red solo buscará en **/etc/networks**

→ El comportamiento puede ser controlado mediante acciones.

→ **Ejemplo:**

hosts: dns[!UNAVAIL=return] files

=> Si el estado de DNS es diferente de **NO DISPONIBLE** consulta **/etc/hosts**

=> Valores de estado posibles:

→ **success** => Petición **SIN ERRORES** → **return**

→ **notfound** => **NO ERROR**, pero no encuentra nodo → **continue**

→ **unavail** => Servicio **NO DISPONIBLE** → **continue**

→ **tryagain** => Servicio **NO DISPONIBLE TEMPORALMENTE** → **continue**

6-/etc/protocols

→ **Muestra que protocolos reconoce nuestro S.O.**

→ Ejemplo:

```
icmp 1    ICMP    # internet control message protocol
ip   0    IP      # internet protocol, pseudo protocol number
tcp  6    TCP     # transmission control protocol
...
```

7-/etc/services

→ Relaciona las aplicaciones con los puertos correspondientes, y protocolos básicos.

→ Ejemplo:

```
...
ssh             22/sctp         # SSH
ftp-data        20/sctp         # FTP
ftp             21/sctp         # FTP
telnet          23/tcp
telnet          23/udp
smtp            25/tcp
smtp            25/udp
...
```

Configuración DHCP (Servidor)

Configuración DHCP (Cliente)

** Comandos Networking **

→ 1-ifconfig

→ 2-route

→ 3-ip

→ 4-ping

→ 5-traceroute

→ 6-arp

→ 7-tcpdump

→ 8-nmap

→ 9-lsof

→ 10-netstat

→ 11-nc

→ 12-host

→ 13-nslookup

→ 14-dig

1-ifconfig

→ Configura un interfaz de red.

→ ifconfig interfaz [aftype] opciones | dirección ...

→ Ejemplos:

- → ifconfig
- → ifconfig -a
- → ifconfig eth0 [up|down]
- → ifconfig eth0 192.168.1.125 netmask 255.255.255.0 gw 192.168.1.1
- → ifconfig eth0:sub1 192.168.1.126

2-route

→ Manipula la tabla de encaminamiento IP.

→ **route [-Cfvnee]**

→ **route [-v] [add|del] [-net|-host] objetivo [netmask Nm] [gw Gw] [[dev] If]**

→ Opciones:

-n Muestra direcciones numéricas

-F Muestra la tabla de encaminamiento FIB del núcleo

-e Use el formato de netstat(8) para mostrar la tabla de encaminamiento.

-C Muestra la caché de rutas del núcleo.

→ Ejemplos:

→ route add -net 127.0.0.0

→ route add -net 192.56.76.0 netmask 255.255.255.0 dev eth0

→ route add default gw mango-gw

→ route add 224.0.0.0 netmask 240.0.0.0 dev eth0

→ route add 10.0.0.0 netmask 255.0.0.0 reject

3-ip

⟶ Mostrar o manejar enrutamientos y dispositivos de red.

⟶ Sustituye a **route** e **ifconfig**

→ Ejemplos:

- → ip addr [list|show]
- → ip link show => Capa 2 (enlace) APSTREF
- → ip link set eth0 [up|down]
- → ip addr list eth3
- → ip link set dev eth2 promisc [on|off]
- → ip addr add 10.0.0.100/24 broadcast 10.0.0.255 dev eth1
- → ip route add 192.168.123.254/24 dev eth2
- → ip route show
- → ip neighbor show
- → ip neighbor show dev eth0
- → ip link set lo [up|down] → loopback (*)

–

– **(*) interfaz virtual para emulación de tráfico de red a través de 2 procesos en el mismo host.**

4-ping

→ Envía paquetes ICMP ECHO_REQUEST a servidores de red.

→ ping [-dfnqrvR] [-c count] [-i wait] [-l preload] [-p pattern] [-s packetsize]

→ Opciones:

- → -c Número de ECPS
- → -b dirección broadcast
- → -i intervalo (Por defecto 1 seg.)

→ Ejemplos:

- → ping -c3 www.google.es
- → ping -c4 -i5 www.google.es
- → ping -b 192.168.1.42

5-traceroute[6]

→ Imprime la ruta de los paquetes enviados.

→ Opciones:

- → -I ICMP ECHO pruebas.
- → -T TCP SYNC pruebas.
- → -i interfaz de envio de paquetes de la traza.
- → -n Deshabilitar mapeo de direcciones host.
- → -6 Para IPv6

→ Ejemplo:

- → traceroute www.google.es

6-arp

→ Manipula la cache ARP del sistema de varias maneras. Las opciones primarias son las de eliminar una entrada de asociación de direcciones y configurar otra manualmente. Para propósitos de depuración el programa arp permite también un vaciado total de la cache ARP. (Address Resolution Protocol).

→ Modelo OSI de 7 capas → APSTREF.

→ capa 3 → RED → Dirección IP.

→ capa 2 → ENLACE → Dirección MAC

→ Para transmitir información desde la capa 3 se necesita un protocolo que posibilite el mapeo entre la capa 2 y la 3.

→ ARP → crea un 'mapping' entre una dirección IP y una dirección MAC, cuando la dirección IP es confirmada.

→ ARP REQUEST → Encuentra la MAC en la IP apropiada a través de Broadcast. Se envian las IP's con sus MAC asociadas que se almacenan en una caché local → Desde IP obtener MAC.

→ Opciones:

-n → Muestra IP's en vez de nombres de nodos.

-a IP → Muestra entrada por nodo.

-d IP → Elimina entrada.

-s IP MAC → Crea una entrada → **arp -s 192.168.1.104 00:FA:AB:...**

-f nombre_fichero → Toma información desde **/etc/ethers**

7-tcpdump

→ Analizar tráfico de la Red.

→ Capturar y mostrar en tiempo real los paquetes transmitidos y recibidos por la red => **POR PANTALLA.**

→ Opciones:

- → **-i interfaz**
- → **-vv** → Detallado.
- → **-n** → Indica IP's, NO nombres de conexiones.
- → **-s ventana** → limitar tramas capturadas (max. 65535).
- → **-w archivo** → formato **libcap** **NO en texto plano**.

→ Ejemplo:

- → **tcpdump -vv -w arch.cap -i eth0 -s0 -n port 22**

8-nmap

→ Exploración de redes sondeo de seguridad de puertos.

→ Escanea Puertos, Identifica servicios en ejecución, versión de los servicios y SO en ejecución.

→ Opciones:

- → **-A host** → Versión de Servicios.
- → **-F** → Fast Scan.

→ Ejemplos:

- → **nmap -F 192.168.1.104**
- → **nmap -A localhost**

9-lsof

→ Muestra ficheros abiertos del Stma.

→ Muestra también determinados puertos abiertos de la conexión.

→ Opciones:

- → **-i** → Lista IP sockects.
- → **-n** → No resuelve hostname.
- → **-P/+P** → No resuelve/resuelve puertos.

→ Ejemplos:

- → **lsof -i**
- → **lsof -n**
- → **lsof /var/lib/mysql**
- → **lsof | grep httpd**

10-netstat

→ Muestra puertos abiertos del Stma.

→ Muestra también información de la red y protocolos utilizados.

→ Opciones:

- → **-a** →Todos los sockects, establecidos o NO.
- → **-e** → Modo extendido.
- → **-inet** → Solo conexiones IP.
- → **-l** → Solo LISTENNING.
- → **-n** → Números IP.
- → **-p** → PID number.
- → **-r** → Tabla Enrutamiento → Equivale a route.
- → **-t** → TCP → Como **-inet.**
- → **-u** → UDP.
- → **-i** → Estado de todas las interfaces → **ifconfig -a.**
- → Ejemplos:
- → **netstat -panetu**
- → **netstat -ei**

11-nc(netcat)

→ Usar, Supervisar y escribir sobre conexiones TCP/UDP.

→ Puede abrir conexiones TCP y enviar paquetes UDP..

→ Opciones:

- → **-v** →verbosidad.
- → **-z** → Puertos TCP.
- → **-u** → Puertos Abiertos UDP.
- → **-l** → Por puerto LISTENNING.

→ Ejemplos:

→ **nc -vz 192.168.1.104 21-25**

→ **nc -zu 192.168.1.104 68-125**

→ **nc 192.168.1.104 80**

GET/ → Muestra index Apache.

12-host

→ Utilidad de Búsqueda de DNS.

→ Opciones:

→ **-t** → Tipo → CNAME, NS, SOA, SIG, MX, KEY, AXFR...

→ **-a** → Cualquier Registro.

→ **-v** → Cualquier Registro.

→ -**vvv** → Mas verbosidad.

→ Ejemplos:

→ **host -vvv google.es**

→ **host -t mx google.es**

14-dig

→ Utilidad de Búsqueda de DNS.

→ Formato:

→ **dig @server name type**

→ Tipos:

→ **ANY**,**CNAME, NS, SOA, A, AAA, MX, ...**

→ **-x** → Consulta inversa.

→ Ejemplos:

→ **dig @www.google.es any**

- → **dig @208.67.222.222 google.com NS**

→ **dig -x 173.194.34.233**

** Networking Wifi **

→ **iwlist** => Escanea redes wifi para obtener información.

=> iwlist wlan0 scanning

→ **iwconfig** => Muestra información y realiza la configuración de la red wireless.

=> iwconfig wlan0 channel3

→ **iwspy** => Monitorea una lista de direcciones wifi y muestra la calidad del servicio para cada una de ellas.

=> iwspy wlan0

(*) Utiliza las **wireless-tools**

TCP Wrappers

→ Servicio que permite el control de acceso al Stma. A través de **xinetd**.

→ Ficheros de Configuración: **/etc/hosts.allow, /etc/hosts.deny**.

→ Primero se consulta **/etc/hosts.allow**

→ Utiliza la librería **libwrap**

→ **tcpd** es el daemon que lee los ficheros **allow** y **deny.**

→ Formato: **servicio/s: lista_clientes**

- → **servicio/servicios** →**telnet,sshd,ftpd**...
- → **lista_clientes** → **ALL, LOCAL, UNKNOW, KNOW, EXCEPT**...

- → Ejemplos:
- → **ALL: 192.168.1.0/24 EXCEPT 192.168.1.56**
- → **ftpd,vsftpd: ALL EXCEPT 192.168.1.15**

NOTAS