

## Tema 2.-Práctica5. Puertos y Servicios

El servicio DNS *bind9*, ejecuta un proceso llamado *named*

### Procesos:

Para ver los procesos que tienen bind como ejecución

```
root@profesor:/home/usuario# ps -aux | grep bind
warning: bad ps syntax, perhaps a bogus '-'?
See http://gitotious.org/procps/procps/blobs/master/Documentation/FAQ
root      1652  0.0  0.0   2376   812 ?        Ss   11:58   0:00 /sbin/rpcbind -
w
bind      2082  0.0  0.9  41932  9852 ?        Ssl  11:58   0:00 /usr/sbin/named
-u bind
root      2759  0.0  0.0   3568   840 pts/0    S+   12:09   0:00 grep bind
```

usuario que ejecuta el comando named

ejecución del comando named

Se muestran 3 procesos:

El proceso que nos interesa es el segundo, el usuario bind ejecuta el comando de usuario /usr/sbin/named

### Puertos:

Para ver los puertos abiertos por el servicio named

Netstat -atunp |grep named →

a → todos los registros.

t → TCP.

u → UDP.

n → números de IP y puertos en lugar de nombres.

p → procesos implicados.

```

root@profesor:/home/usuario# netstat -atunp |grep named
tcp        0      0 192.168.10.1:53      0.0.0.0:*             LISTEN      208
2/named
tcp        0      0 192.168.4.60:53      0.0.0.0:*             LISTEN      208
2/named
tcp        0      0 127.0.0.1:53         0.0.0.0:*             LISTEN      208
2/named
tcp        0      0 127.0.0.1:953        0.0.0.0:*             LISTEN      208
2/named
tcp6       0      0 :::53                :::*                  LISTEN      208
2/named
tcp6       0      0 :::1:953              :::*                  LISTEN      208
2/named
udp        0      0 192.168.10.1:53      0.0.0.0:*             208
2/named
udp        0      0 192.168.4.60:53      0.0.0.0:*             208
2/named
udp        0      0 127.0.0.1:53         0.0.0.0:*             208
2/named
udp6       0      0 :::53                 :::*                  208
2/named

```

En este caso los puertos abiertos (53, puerto DNS) del proceso named para todas las interfaces de red.

### ***Consulta a un servidor:***

Desde el windows 7 hacemos establecemos una conexión con el servidor DNS 192.168.4.60, aunque dicho sistema tenga como Servidores DNS otros:

```

C:\Users\eugenio>ipconfig /all

Configuración IP de Windows

Nombre de host. . . . . : Profesor
Sufijo DNS principal . . . . . :
Tipo de nodo. . . . . : híbrido
Enrutamiento IP habilitado. . . . : no
Proxy WINS habilitado . . . . . : no

Adaptador de Ethernet Conexión de área local:

Sufijo DNS específico para la conexión. . :
Descripción . . . . . : Atheros AR8151 PCI-E Gigabit Ethernet Controller (NDIS 6.20)
Dirección física. . . . . : 50-E5-49-41-B3-4B
DHCP habilitado . . . . . : no
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . : fe80::71c1:dc21:b696:ac37%10(Preferido)

Dirección IPv4. . . . . : 192.168.4.16(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . : 192.168.4.253
IAID DHCPv6 . . . . . : 240182601
DUID de cliente DHCPv6. . . . . : 00-01-00-01-1B-3C-8D-74-50-E5-49-41-B3-4B
Servidores DNS. . . . . : 194.179.1.100
NetBIOS sobre TCP/IP. . . . . : habilitado

```

Conexión con el servidor 192.168.4.60:

```

Administrador: C:\Windows\system32\cmd.exe - nslookup - 192.168.4.60
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.
C:\Users\eugenio>nslookup - 192.168.4.60
Servidor predeterminado: profesor.2asir.net
Address: 192.168.4.60

> www.google.es
Servidor: profesor.2asir.net
Address: 192.168.4.60

Respuesta no autoritativa:
Nombre: www.google.es
Addresses: 2a00:1450:4003:805::1018
           74.125.230.24
           74.125.230.31
           74.125.230.23

> pc1.2asir.net
Servidor: profesor.2asir.net
Address: 192.168.4.60

Nombre: pc1.2asir.net
Address: 192.168.4.61

>

```

Podemos ver los distintas consultas a hacer mediante las opciones

```

> help
Comandos: (los identificadores se muestran en mayúsculas, [] significa opcional)
NOMBRE - imprimir información acerca de NOMBRE de host o de dominio con
el servidor predeterminado
NOMBRE1 NOMBRE2 - igual que el anterior, pero se usa NOMBRE2 como servidor
help o ? - imprimir información acerca de comandos comunes
set OPCIÓN - establecer una opción
all - opciones de impresión, servidor actual y host
[no]debug - imprimir información de depuración
[no]d2 - imprimir información de depuración exhaustiva
[no]defname - anexar el nombre de dominio a cada consulta
[no]recurse - pedir respuesta recursiva a la consulta
[no]search - usar la lista de búsqueda de dominios
[no]vc - usar siempre un circuito virtual
domain=NOMBRE - establecer nombre de dominio predeterminado en NOMBRE
srchlist=N1[/N2/.../N6] - establecer dominio en N1 y lista de búsqueda en N1
,N2, etc.
root=NOMBRE - establecer servidor raíz en NOMBRE
retry=X - establecer número de reintentos en X
timeout=X - establecer intervalo de tiempo de espera inicial en X
segundos
type=X - establecer tipo de consulta (p. ej., A,AAAA,A+AAAA,ANY
,CNAME,MX,NS,PTR,SOA,SRV)
querytype=X - igual que type
class=X - establecer clase de consulta (p. ej., IN (Internet), A
NY)
[no]mxfr - usar transferencia de zona rápida MS
ixfrver=X - versión actual que se usará en la solicitud de transfe
rencia IXFR
server NOMBRE - establecer el servidor predeterminado en NOMBRE con el servi
dor predeterminado actual
lserver NOMBRE - establecer el servidor predeterminado en NOMBRE con el servi
dor inicial
root - establecer el servidor predeterminado actual en la raíz
ls [opt] DOMINIO [> ARCHIVO] - enumerar las direcciones de DOMINIO (opcional: en
viar el resultado a ARCHIVO)
-a - enumerar nombres canónicos y alias
-d - enumerar todos los registros
-t TIPO - enumerar los registros del tipo de registro RFC dado (p. ej.,
A,CNAME,MX,NS,PTR etc.)
view ARCHIVO - ordenar un archivo de resultados 'ls' y verlo con pg
exit - salir del programa
>

```

Para ver los distintos tipos de registro, el el fichero T2\_Registros\_Recursos.pdf

