

Listas de control de acceso para BIND

Se pueden configurar el BIND para ver quién puede usar el servidor DNS y quién no.

Recordar que todos los archivos de configuración cuelgan de /etc/
y concretamente los de Bind cuelgan de **/etc/bind/**

Abriremos el archivo **named.conf.options**:

```
acl listadelosbuenos
{
    10.2.23.199; //aquí creamos una lista con un listado de IP's , incluso redes: 192.168.100/24
};

options
{
    directory "/var/cache/bind";

    allow-query
    {
        listadelosbuenos; //aquí indicamos la lista de quien puede usar el Bind como servidor DNS
    };

    blackhole
    {
        10.2.23.188; //aquí indicamos la lista de quien NO puede usar el Bind como servidor DNS
    };

    forwarders
    {
        8.8.8.8; //usamos los DNS de google y el
        80.58.61.254; //DNS de telefonica
    };

    auth-nxdomain no; # conform to RFC1035
    listen-on-v6 { any; };
};
```

Para que funcione hay que reiniciar bind: `/etc/init.d/bind9 restart`

Si da error es que te has dejado algún ; o alguna llave mal o algo así

Puedes ver el log del sistema en:

`/var/log/syslog`

Ahora debes probar con una máquina virtual que haga de cliente DNS.

- Ponle como IP, la de la lista **listadelosbuenos**

- y como DNS la IP de la Máquina con el BIND

Observaras que sí que resuelve, puedes entrar a internet y te responde bien con el **nslookup**

Luego, con otra máquina, o con la misma:

- Ponle como IP, la que sale en el **blackhole**

- y como DNS la IP de la Máquina con el BIND

Observaras que NO que resuelve, NO puedes entrar a internet y NO te responde con el **nslookup**

Probad también a usar las listas: **any**, **none** y **localhost**

NOTA:

Recordar que el verdadero archivo de configuración es **named.conf**, que sólo contiene:

```
include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
```