Servicio de Red e Internet

Volodimir Yarmash Yarmash

Índice

DNS
https://www.digitalocean.com/community/tutorials/how-to-configure-bind-as-a-caching-or-forwarding-dns-server-on-ubuntu-16-04
http://www.zytrax.com/books/dns/ch4/
https://help.ubuntu.com/community/BIND9ServerHowto

Libro Pro DNS and BIND (Chapter 4 DNS types)
http://it-ebooks.info/book/5022/

Ejercicio

Lee el artículo anterior. Instala y configura bin9 en primer lugar como servidor caché y por último como forwarding.

- Comprueba la sintaxis del archivo de configuración (named-checkconf)
- Visualiza el archivo log y comprueba que responde adecuadamente (/var/log/syslog)

Para instalar Bind9, debemos hacer un
sudo apt-get update y
sudo apt-get install bind9 bind9utils bind9-doc

Ahora tenemos que configurar Bind para que actúe como un servidor DNS de almacenamiento en caché.
Entramos a cd /etc/bind

```
user@user-Standard-PC-i440FX-PIIX-1996:~$ cd /etc/bind
user@user-Standard-PC-i440FX-PIIX-1996:/etc/bind$ ls
bind.keys  db.empty    named.conf.default-zones  zones.rfc1918
db.0       db.local    named.conf.local
db.127     db.root     named.conf.options
db.255     named.conf  rndc.key
user@user-Standard-PC-i440FX-PIIX-1996:/etc/bind$
```

Entramos en el archivo named.conf.options con el comando sudo nano named.conf.options
Y creamos un bloque introduciendo por encima alc goodclients {};
Lo que vamos a hacer es introducir ips que se les debe permitir usar este servidor DNS
Ahora tenemos que configurar el ACL para que Bind lo lea. Bind primero recurre a allow-query-cache, luego a allow-query y finalmente a localcost y localnet.
Agregamos recursion yes; allow-query { goodclients; }; a options y guardamos.

```
 GNU nano 2.5.3          File: named.conf.options                Modified

acl goodclients {
        localhost;
        localnets;
};

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

        recursion yes;
        allow-query { goodclients; };
        // If there is a firewall between you and nameservers you want
```

Ahora debemos cambiar la configuración para que el servidor ya no intente realizar consultas recursivas por sí mismo.
Para ello debemos configurar una lista de servidores de almacenamiento en cache a los que reenviar nuestras solicitudes.
Añadimos Forwarders {8.8.8.8; 8.8.4.4;}; que contiene las direcciones ip de los servidores dns de google.
Y escribimos forward only; para que el servidor SOLO reenvie todas las solicitudes y apra que no resuelva peticiones por su cuenta.

Comprobamos la configuración con el comando sudo named-checkconf; en mi caso ha resultado encontrar un fallo. Lo corregimos

```
user@user-Standard-PC-i440FX-PIIX-1996:/etc/bind$ sudo named-checkconf
[sudo] password for user:
/etc/bind/named.conf.options:24: unknown option 'foward'
user@user-Standard-PC-i440FX-PIIX-1996:/etc/bind$ sudo nano named.conf.options
user@user-Standard-PC-i440FX-PIIX-1996:/etc/bind$ sudo named-checkconf
user@user-Standard-PC-i440FX-PIIX-1996:/etc/bind$
```

Reiniciamos bing9 y podemos ver los registros del servicio Bind9 en tiempo real

```
user@user-Standard-PC-i440FX-PIIX-1996:/etc/bind$ sudo systemctl restart bind9
user@user-Standard-PC-i440FX-PIIX-1996:/etc/bind$ sudo ufw allow bind9
Rules updated
Rules updated (v6)
user@user-Standard-PC-i440FX-PIIX-1996:/etc/bind$ sudo journalctl -u bind9 -f
-- Logs begin at lun 2025-01-20 22:54:48 CET. --
ene 21 12:51:52 user-Standard-PC-i440FX-PIIX-1996 named[23275]: command channel
listening on ::1#953
ene 21 12:51:52 user-Standard-PC-i440FX-PIIX-1996 named[23275]: managed-keys-zon
e: loaded serial 0
ene 21 12:51:52 user-Standard-PC-i440FX-PIIX-1996 named[23275]: zone 127.in-addr
.arpa/IN: loaded serial 1
ene 21 12:51:52 user-Standard-PC-i440FX-PIIX-1996 named[23275]: zone localhost/I
N: loaded serial 2
ene 21 12:51:52 user-Standard-PC-i440FX-PIIX-1996 named[23275]: zone 0.in-addr.a
rpa/IN: loaded serial 1
ene 21 12:51:52 user-Standard-PC-i440FX-PIIX-1996 named[23275]: zone 255.in-addr
.arpa/IN: loaded serial 1
```

En este punto Bind esta configurado para actuar como servidor dns.
Entramos al equipo cliente
Modificamos el archivo resolv.conf con sudo nano /etc/resolv.conf
Agregamos un nameserver y la ip de nuestro dns server

```
  GNU nano 6.2                                          /etc/resolv.conf *
# This is /run/systemd/resolve/stub-resolv.conf managed by man:systemd-resolved(8).
# Do not edit.
#
# This file might be symlinked as /etc/resolv.conf. If you're looking at
# /etc/resolv.conf and seeing this text, you have followed the symlink.
#
# This is a dynamic resolv.conf file for connecting local clients to the
# internal DNS stub resolver of systemd-resolved. This file lists all
# configured search domains.
#
# Run "resolvectl status" to see details about the uplink DNS servers
# currently in use.
#
# Third party programs should typically not access this file directly, but only
# through the symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a
# different way, replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

nameserver 127.0.0.53
nameserver 192.168.195.36
options edns0 trust-ad
search home.arpa
```

Hacemos ping a Google.com y estos son los resultados

```
user@user-Standard-PC-i440FX-PIIX-1996:~$ ping -c 1 google.com
PING google.com (142.250.184.174) 56(84) bytes of data.
64 bytes from mad07s23-in-f14.1e100.net (142.250.184.174): icmp_seq=1 ttl=114 time=41.8 ms

--- google.com ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 41.790/41.790/41.790/0.000 ms
```

Y estos son los logs del DNS server:

```
ene 23 18:10:31 user-Standard-PC-i440FX-PIIX-1996 named[1052]: running
ene 23 18:10:31 user-Standard-PC-i440FX-PIIX-1996 named[1052]: managed-keys-zone
: Key 20326 for zone . acceptance timer complete: key now trusted
ene 23 18:10:31 user-Standard-PC-i440FX-PIIX-1996 named[1052]: managed-keys-zone
: Key 38696 for zone . acceptance timer complete: key now trusted
ene 23 18:37:21 user-Standard-PC-i440FX-PIIX-1996 named[1052]: no valid RRSIG re
solving '168.192.in-addr.arpa/DS/IN': 8.8.8.8#53
ene 23 18:37:21 user-Standard-PC-i440FX-PIIX-1996 named[1052]: no valid RRSIG re
solving '168.192.in-addr.arpa/DS/IN': 8.8.4.4#53
ene 23 18:37:21 user-Standard-PC-i440FX-PIIX-1996 named[1052]: no valid DS resol
ving '44.195.168.192.in-addr.arpa/PTR/IN': 8.8.8.8#53
ene 23 18:37:21 user-Standard-PC-i440FX-PIIX-1996 named[1052]: validating 44.195
.168.192.in-addr.arpa/PTR: bad cache hit (168.192.in-addr.arpa/DS)
ene 23 18:37:21 user-Standard-PC-i440FX-PIIX-1996 named[1052]: broken trust chai
n resolving '44.195.168.192.in-addr.arpa/PTR/IN': 8.8.4.4#53
ene 23 18:37:21 user-Standard-PC-i440FX-PIIX-1996 named[1052]: validating 44.195
.168.192.in-addr.arpa/PTR: bad cache hit (168.192.in-addr.arpa/DS)
ene 23 18:37:21 user-Standard-PC-i440FX-PIIX-1996 named[1052]: broken trust chai
n resolving '44.195.168.192.in-addr.arpa/PTR/IN': 8.8.8.8#53
```

Podemos ver registros como:
managed-keys-zone: Key 20326… El servidor DNS ha confiado en una clave pública específica asociada con DNSSEC. Esto es parte del proceso de validación de DNSSEC, donde el servidor verifica las claves para garantizar que las respuestas DNS sean seguras.
no valid RRSIG resolving El servidor Bind intentó validar un registro de firma DNSSEC pero no encontró uno válido. Esto puede ocurrir si la zona DNS no está firmada con DNSSEC
validating 44.195.168.192.in-addr.arpa/DS Bind está intentando validar un registro `DS` (Delegation Signer) para la zona `44.195.168.192.in-addr.arpa`, pero encontró datos en caché que no son válidos. El mensaje "bad cache hit" indica que el servidor tiene un registro en su caché que no pasó la validación. Esto puede deberse a un problema de sincronización dns o que el registro esta caducado.

Vamos a probar si se guarda información en al cache. Escribimos dig linixfoundation.org 2 veces

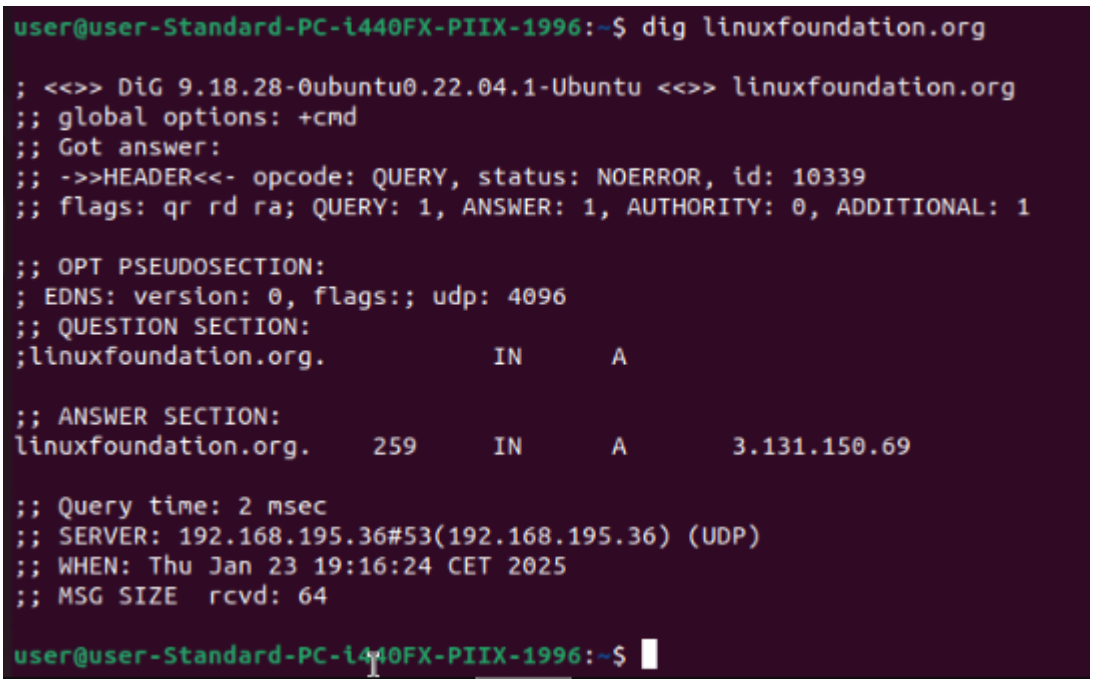
```
user@user-Standard-PC-i440FX-PIIX-1996:~$ dig linuxfoundation.org

; <<>> DiG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<>> linuxfoundation.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9950
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;linuxfoundation.org.           IN      A

;; ANSWER SECTION:
linuxfoundation.org.    600     IN      A       3.131.150.69

;; Query time: 68 msec
;; SERVER: 192.168.195.36#53(192.168.195.36) (UDP)
;; WHEN: Thu Jan 23 19:10:44 CET 2025
;; MSG SIZE  rcvd: 64
```



Como podemos observar, la diferencia del Query time es bastante. Eso es porque si está configurado correctamente.