Instalación de DNS Server en Debian

Sumario

Instalación de DNS BIND9 en Debian

```
# Instalación de bind9
apt-get install bind9

# Arranque y parada del servicio:
service bind9 start | stop | status | restart | reload

#Ficheros de configuración:
/etc/bind/named.conf

#Ficheros referenciados dentro de named.conf:
/etc/bin/named.conf.options
/etc/bin/named.conf.local
/etc/bin/named.conf.default-zones
```

Parámetros de configuración a revisar en la Instalación DNS

Suponiendo que estamos trabajando con un servidor con la IP 192.168.1.10, y queremos instalar el servicio DNS y crear un nuevo dominio llamado **pruebas.local** en ese servidor. Seguiremos los siguientes pasos:

NOTA: Se recomienda que el servidor de nombres se llame dns. Si hay dos, pues dns1 y dns2. También le podríamos llamar ns o ns1, ns2.

- Revisaremos que la configuración IP del servidor que sea correcta.

```
nano /etc/network/interfaces
auto lo eth0
iface lo inet loopback

# The primary network interface
allow-hotplug eth0

iface eth0 inet static
        address 192.168.1.10
        netmask 255.255.255.0
        broadcast 192.168.1.255
        gateway 192.168.1.1


#nano /etc/hosts
127.0.0.1   localhost
127.0.0.1   dns.pruebas.local  dns


#nano /etc/hostname
ns
```

- Una vez hecho ésto, instalaremos el servicio DNS BIND:

```
apt-get install bind9
```

- Crearemos la **zona inversa** para la red 192.168.1

- Crearemos la **zona master** para pruebas.local

- Nos aseguraremos que en servidor Maestro aparezca escrito: **dns.pruebas.local**
- Agregaremos un **registro de tipo A llamado ns (el glue record)** y que apunte a la IP 192.168.1.10 de nuestro servidor DNS.
- A partir de aquí ya podremos añadir todos los registros que necesitemos.

Configuración de DNS Primario y Secundario

Cuando tenemos dos servidores de DNS primario y secundario, generalmente en el servidor secundario crearemos las zonas esclavas del DNS primario.

Nos aseguraremos de permitir la transferencia de zona para la IP del DNS secundario, y también la opción de notificar actualizaciones de forma automática.

La configuración de los resolv.conf de cada uno de los servidores será la siguiente:

```
# Para el DNS primario:
nano /etc/resolv.conf
127.0.0.1

# Para el DNS secundario:
nano /etc/resolv.conf
127.0.0.1
```

Podríamos poner debajo de cada 127.0.0.1 las IP's del otro servidor, pero no es buena idea, ya que si falla el servidor DNS de nuestra máquina nos interesa saber que está fallando, y si añadimos esa IP adicional, no nos enteraremos de que nuestro servicio DNS falla hasta que falle el otro DNS. De esta manera no creamos dependencias entre ellos.

Sobre los Nameservers de cada zona

Deberemos tener la precaución de tener configurados (**en la zona Master**) en la sección de **nameservers**, las direcciones IP de los dos servidores de DNS primario y secundario. Ésto es necesario ya que, cuando se realiza la transferencia de zona al secundario, ésta deberá incluir las direcciones IP de los dos Nameservers.

Reenvío y Transferencias

Si queremos que en nuestro servidor DNS cuando preguntemos por una zona determinada lo haga a un servidor DNS determinado, tendremos que configurar el Reenvío en la sección de "**Reenvío y Transferencias**" (en webmin).

- Podremos configurar una dirección de **Reenvío Global** (en la sección global de Webmin). Ésto implica que todos los dominios que nuestro servidor no entienda, reenviará las consultas al servidor especificado en la zona global de reenvío.
- Podremos configurar **Reenvíos Selectivos** (creando nuevas Zonas de Reenvío).

Por defecto el servidor de DNS sólo responderá a los equipos que estén en su misma red. Si queremos que responda a consultas desde cualquier equipo, independientemente de la red del servidor, tendremos que hacer lo siguiente:

```
nano /etc/bind/named.conf.options

# Añadiremos la siguiente cláusula dentro de las llaves pertenecientes a options:
  allow-query { any; };

# Si queremos permitir consultas recursivas desde cualquier red,
# añadiremos, que tiene más rango de cobertura en principio.
  allow-recursion { any; };

# ATENCIÓN: Si tenemos problemas con las consultas activar la opción DNSSEC !!,
# Ya que según la versión de BIND que tengamos, puede ser que sólo admita respuestas
# de servidores que tengan DNSSEC activado.

# El resultado puede ser algo similar a este ejemplo:
more /etc/bind/named.conf.options

options {
```

```
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0s placeholder.

        // forwarders {
        //      0.0.0.0;
        // };

        auth-nxdomain no;    # conform to RFC1035
        listen-on-v6 { any; };
        forwarders {
                213.172.33.35;
                8.8.8.8;
                };

        allow-query {
                any;
                };

        allow-recursion{
                any;
                };

};

# Reiniciamos el servicio y listo.
service bind9 restart

# Si queremos borrar la caché del DNS, lo haremos con:
service nscd restart

# Si nos dice que es un comando incorrecto o no se encuentra, instalamos la aplicación nscd:
apt-get install nscd

# Si queremos realizar la modificación en WEBMIN, iremos a la página principal
# del servicio DNS BIND, y entraremos en Valores por Defecto de Zona:
# Una vez dentro, iremos a Permitir consultas desde...
# Marcaremos la opción Listado.... y teclearemos la palabra any
```

Para más información sobre query consultar: http://www.zytrax.com/books/dns/ch7/queries.html

Comandos para comprobar funcionamiento DNS

Desde la línea de comandos podemos comprobar si está funconando correctamente nuestro servicio de DNS realizando algunas consultas como:

- En Windows:

nslookup -debug dominio [ip del servidor DNS opcional]

- En Mac y Linux:

dig @[IP servidor DNS] nombre del dominio

- Información adicional sobre comando dig: http://www.madboa.com/geek/dig/

Por ejemplo una muestra del resultado con nslookup:

```
nslookup -debug www.terra.es

------------
Got answer:
    HEADER:
```

```
        opcode = QUERY, id = 1, rcode = NOERROR
        header flags:  response
        questions = 1,  answers = 2,  authority records = 0,  additional = 0

    QUESTIONS:
        1.1.168.192.in-addr.arpa, type = PTR, class = IN
    ANSWERS:
    ->  1.1.168.192.in-addr.arpa
        name = Comtrend
        ttl = 10000 (2 hours 46 mins 40 secs)
    ->  1.1.168.192.in-addr.arpa
        name = Comtrend.Home
        ttl = 10000 (2 hours 46 mins 40 secs)

------------
Servidor:  Comtrend
Address:  192.168.1.1

------------
Got answer:
    HEADER:
        opcode = QUERY, id = 2, rcode = NOERROR
        header flags:  response, want recursion, recursion avail.
        questions = 1,  answers = 1,  authority records = 2,  additional = 2

    QUESTIONS:
        www.terra.es, type = A, class = IN
    ANSWERS:
    ->  www.terra.es
        internet address = 213.4.130.210
        ttl = 17737 (4 hours 55 mins 37 secs)
    AUTHORITY RECORDS:
    ->  terra.es
        nameserver = dns1.terra.es
        ttl = 17714 (4 hours 55 mins 14 secs)
    ->  terra.es
        nameserver = dns2.terra.es
        ttl = 17714 (4 hours 55 mins 14 secs)
    ADDITIONAL RECORDS:
    ->  dns1.terra.es
        internet address = 213.4.132.1
        ttl = 17714 (4 hours 55 mins 14 secs)
    ->  dns2.terra.es
        internet address = 213.4.141.1
        ttl = 17714 (4 hours 55 mins 14 secs)

------------
Respuesta no autoritativa:
------------
Got answer:
    HEADER:
        opcode = QUERY, id = 3, rcode = NOERROR
        header flags:  response, want recursion, recursion avail.
        questions = 1,  answers = 0,  authority records = 1,  additional = 0

    QUESTIONS:
        www.terra.es, type = AAAA, class = IN
    AUTHORITY RECORDS:
    ->  terra.es
        ttl = 1435 (23 mins 55 secs)
        primary name server = dns1.terra.es
        responsible mail addr = dnsadmin.corp.terra.es
        serial  = 2012051600
        refresh = 28800 (8 hours)
        retry   = 7200 (2 hours)
        expire  = 2592000 (30 days)
        default TTL = 172800 (2 days)

------------
Nombre:  www.terra.es
Address:  213.4.130.210
```

--Veiga 09:12 19 may 2012 (CEST)