Servidor DNS Bind 9

José Domingo Muñoz

IES Gonzalo Nazareno

Noviembre 2021

Servidor DNS bind9. Configuración básica

Configuración de bind9

Fichero /etc/bind/named.conf.local:

```
include "/etc/bind/zones.rfc1918";
zone "example.com" {
    type master;
    file "db.example.com";
};

zone "0.0.10.in-addr.arpa" {
    type master;
    file "db.0.0.10";
};
```

Zona directa

Fichero /var/cache/bind/db.example.com:

```
$TTL    86400
@    IN    SOA    dns-1.example.com. root.example.com. (
                  1        ; Serial
             604800        ; Refresh
              86400        ; Retry
            2419200        ; Expire
              86400 )    ; Negative Cache TTL
;
@    IN    NS          dns-1.example.com.
@    IN    MX    10    correo.example.com.

$ORIGIN example.com.

dns-1        IN    A        10.0.0.11
correo       IN    A        10.0.0.200
www          IN    CNAME    dns-1
```

Zona inversa

Fichero /var/cache/bind/db.0.0.10:

```
$TTL    86400
@    IN    SOA    dns-1.example.com. root.example.com. (
                  1         ; Serial
              604800        ; Refresh
               86400        ; Retry
             2419200        ; Expire
               86400 )    ; Negative Cache TTL
;
@    IN    NS    dns-1.example.com.

$ORIGIN 0.0.10.in-addr.arpa.

11        IN    PTR    dns-1.example.com.
200        IN    PTR    correo.example.com.
```

Consultas desde el cliente

```
$ cat /etc/resolv.conf
...
nameserver 10.0.0.11
```

Consultas con dig:

```
dig ns example.com
dig mx example.com
dig www.example.com
dig -x 10.0.0.11
dig ptr 11.0.0.10.in-addr.arpa
```

bind9 es un servidor dns recursor/caché:

```
dig www.josedomingo.org
...
;; Query time: 1543 msec
```

```
dig www.josedomingo.org
...
;; Query time: 1 msec
```

Servidor DNS maestro/esclavo

DNS maestro/esclavo

Un servidor esclavo contiene una réplica de las zonas del servidor maestro.

- DNS maestro: dns-1.example.com (10.0.0.11)
- DNS escalvo: dns-2.example.com (10.0.0.5)

Se debe producir una **transferencia de zona** (el esclavo hace una solicitud de la zona completa al maestro) para que se sincronicen los servidores.

Por seguridad, sólo debemos aceptar transferencias de zonas hacía los esclavos autorizados, para ello en el fichero /etc/bind/named.conf.options, deshabilitamos la transferencia:

```
options {
    ...
    allow-transfer { none; };
    ...
```

Fichero `etc/bind/named.conf.local`:

```
include "/etc/bind/zones.rfc1918";
zone "example.com" {
    type master;
    file "db.example.com";
    allow-transfer { 10.0.0.5; };
    notify yes;
};
zone "0.0.10.in-addr.arpa" {
    type master;
    file "db.0.0.10";
    allow-transfer { 10.0.0.5; };
    notify yes;
};
```

DNS esclavo

Fichero /etc/bind/named.conf.local:

```
include "/etc/bind/zones.rfc1918";
zone "example.com" {
    type slave;
    file "db.example.com";
    masters { 10.0.0.11; };
};

zone "0.0.10.in-addr.arpa" {
    type slave;
    file "db.0.0.10";
    masters { 10.0.0.11; };
};
```

Zona directa

Fichero /var/cache/bind/db.example.com:

```
$TTL    86400
@    IN    SOA    dns-1.example.com. root.example.com. (
                  1         ; Serial
             604800         ; Refresh
              86400         ; Retry
            2419200         ; Expire
              86400 )     ; Negative Cache TTL
;
@    IN    NS        dns-1.example.com.
@    IN    NS        dns-2.example.com.
@    IN    MX    10    correo.example.com.

$ORIGIN example.com.

dns-1        IN    A    10.0.0.11
dns-2        IN    A    10.0.0.5
correo       IN    A    10.0.0.200
www          IN    CNAME    dns-1
```

Zona inversa

Fichero /var/cache/bind/db.0.0.10:

```
$TTL    86400
@    IN    SOA    dns-1.example.com. root.example.com. (
                  1         ; Serial
             604800         ; Refresh
              86400         ; Retry
            2419200         ; Expire
              86400 )    ; Negative Cache TTL
;
@    IN    NS    dns-1.example.com.
@    IN    NS    dns-2.example.com.

$ORIGIN 0.0.10.in-addr.arpa.

11        IN    PTR    dns-1.example.com.
5         IN    PTR    dns-2.example.com.
200       IN    PTR    correo.example.com.
```

Transferencia de zona

Cuando reiniciamos el servidor esclavo podemos ver como se ha producido una transferencia de las zonas:

```
root@dns-2:~# systemctl restart bind9
root@dns-2:~# tail /var/log/syslog
Nov 13 21:04:06 dns-2 named[5739]: zone 0.0.10.in-addr.arpa/IN: transferred serial 1
Nov 13 21:04:06 dns-2 named[5739]: transfer of '0.0.10.in-addr.arpa/IN' from 10.0.0.11#53: Transfer status: success
Nov 13 21:04:06 dns-2 named[5739]: transfer of '0.0.10.in-addr.arpa/IN' from 10.0.0.11#53: Transfer completed: 1 messages
Nov 13 21:04:06 dns-2 named[5739]: managed-keys-zone: Key 20326 for zone . acceptance timer complete: key now trusted
Nov 13 21:04:06 dns-2 named[5739]: resolver priming query complete
Nov 13 21:04:06 dns-2 named[5739]: zone example.com/IN: Transfer started.
Nov 13 21:04:06 dns-2 named[5739]: transfer of 'example.com/IN' from 10.0.0.11#53: connected using 10.0.0.5#58461
Nov 13 21:04:06 dns-2 named[5739]: zone example.com/IN: transferred serial 1
Nov 13 21:04:06 dns-2 named[5739]: transfer of 'example.com/IN' from 10.0.0.11#53: Transfer status: success
Nov 13 21:04:06 dns-2 named[5739]: transfer of 'example.com/IN' from 10.0.0.11#53: Transfer completed: 1 messages, 8 reco
```

Consultas desde el cliente

```
$ cat /etc/resolv.conf
...
nameserver 10.0.0.11
nameserver 10.0.0.5
```

Si hacemos una consulta desde un cliente, y el dns maestro no responde, responderá el esclavo.

```
dig ns example.com
...
;; ANSWER SECTION:
example.com.        86400    IN    NS    dns-1.example.com.
example.com.        86400    IN    NS    dns-2.example.com.
```

Podemos comprobar que podemos preguntar a los dos servidores:

```
dig @10.0.0.11 www.example.com
dig @10.0.0.5 www.example.com
```

¿Cuándo se hacen las copias?

- Los esclavos interrogan al maestro periódicamente, ésto es el “Intervalo de actualización” (**refresh interval**), para obtener actualizaciones.
- El maestro también puede notificar a los esclavos cuando hay cambios (**notify yes;**), pero como puede haber pérdida de paquetes sigue siendo necesario interrogar periódicamente.
- El esclavo sólo iniciará la copia cuando el número de serie, configurado en el registro SOA de la zona, **AUMENTE**.
- Formato recomendado: **YYMMDDNN**
- Si se decrementa el número de serie, los esclavos nunca se actualizarán hasta que el número sea mayor que el valor anterior.
- El número de serie es un entero de 32 bits, si se incrementa el límite superior será truncado sin avisar por lo que el número de serie se habrá decrementado.

Registro SOA

```
@    IN    SOA    dns-1.example.com. root.example.com. (
                      1             ; Serial
                      604800        ; Refresh
                      86400        ; Retry
                      2419200       ; Expire
                      86400 )   ; Negative Cache TTL
```

- **El intervalo de actualización (refresh)**: frecuencia con la que el esclavo debe revisar el número de serie del maestro para hacer una transferencia de zona.
- **Intervalo de reintento (retry)**: frecuencia con la que reintenta si el servidor maestro no responde.
- **Tiempo de caducidad (expiry)**: Si el esclavo no puede comunicarse con el maestro durante este intervalo, debe borrar su copia de la zona.
- **TTL negativo (negative)**: Significa tiempo de vida negativo, el tiempo durante el cual se debe almacenar en la cache de cualquier otro servidor DNS una respuesta negativa. Eso significa que si otro servidor DNS preguntas por `no-existe.example.com` y esa entrada no existe, ese servidor DNS considerará como válida esa respuesta (no existe) durante el tiempo indicado.

Evitar y comprobar errores (I)

- Cada vez que realice una modificación recuerda incrementar el número de serie.
- Para detectar errores de sintaxis puedes usar el siguiente comando:

```
named-checkzone example.com /var/cache/bind/db.example.com
```

- Para detectar errores de configuración en named.conf, podemos usar:

```
named-checkconf
```

Evitar y comprobar errores (II)

- Reinicia el servicio y comprueba los logs del sistema:

```
rndc reload
rndc reload example.com
```

- Realiza una consulta al servidor maestro y los esclavos para comprobar que las respuestas son autorizadas (bit AA), además asegúrate que coinciden los número de serie:

```
dig +norec @x.x.x.x example.com. soa
```

- Solicita una copia completa de la zona y comprueba que sólo se puede hacer desde los esclavos:

```
dig @x.x.x.x example.com. axfr
```

Subdominios en bind9

Subdominios en bind9

Por ejemplo, tenemos el dominio example.com y queremos crear un subdomimio es.example.com por lo que podríamos tener los siguientes nombres:

- Nombre de dominio principal: **example.com**
- Nombre de un host en el dominio principal: **www.example.com**
- Nombre del subdominio: **es.example.com**
- Nombre de un host en el subdominio: **www.es.example.com**

Para conseguir configurar subdominios tenemos dos alternativas:

- **Crear un subdominio virtual**, en este caso es un sólo servidor DNS el que va a tener autoridad sobre el dominio y sobre el subdominio.
- **Delegar el subdominio**, es decir el servidor DNS autorizado para el dominio va a delegar la gestión y autorización del subdominio a otro servidor DNS.

Dominio virtual

Fichero /var/cache/bind/db.example.com:

```
...
$ORIGIN example.com.

dns-1           IN      A       10.0.0.11
dns-2           IN      A       10.0.0.5
correo          IN      A       10.0.0.200
www             IN      CNAME   dns-1

$ORIGIN es.example.com.
web             IN      A       10.0.0.100
www             IN      CNAME   web
```

Podemos realizar la consulta:

```
dig @10.0.0.11 www.es.example.com

...
;; QUESTION SECTION:
;www.es.example.com.         IN    A

;; ANSWER SECTION:
www.es.example.com.    86400    IN    CNAME   web.es.example.com.
web.es.example.com.    86400    IN    A    10.0.0.100

; AUTHORITY SECTION:
example.com.         86400    IN    NS    dns-1.example.com.
```

El servidor con autoridad (registro NS) es el servidor `dns-1.example.com`.

Delegación de subdominios

En esta ocasión partimos de:

- Un servidor DNS con autoridad sobre el dominio **example.com**: (**dns-1.example.com**),
- que va a delegar la gestión del subdominio **es.example.com** a otro servidor DNS (**dns-3.es.example.com**).

DNS del dominio principal (example.com)

En el fichero de zona `/var/cache/bind/db.example.com`, tendremos que indicar cual es el servidor DNS con autoridad para el subdominio (servidor DNS al que vamos a delegar la gestión del subdominio **es.example.com**):

```
...
$ORIGIN es.example.com.
@           IN      NS      dns-3
dns-3       IN      A       10.0.0.13
```

Como podemos observar el servidor DNS con autoridad sobre la zona **es.example.com**, será **dns-3.es.example.com** que se encuentra en la dirección **10.0.0.13**.

Configuración del DNS del subdominio (es.example.com)

En el servidor **dns-3.es.example.com** (**10.0.0.13**), creamos una nueva zona. En el fichero `/etc/bind/named.conf.local`:

```
zone "es.example.com" {
  type master;
  file "db.es.example.com";
};
```

Configuración del DNS del subdominio (es.example.com)

Y el fichero de zona /var/cache/bind/db.es.example.com:

```
$TTL    86400
@       IN      SOA     dns-3.es.example.com. root.es.example.com. (
                              1             ; Serial
                              604800         ; Refresh
                              86400         ; Retry
                              2419200         ; Expire
                              86400 )       ; Negative Cache TTL
;
@       IN      NS      dns-3.es.example.com.
$ORIGIN es.example.com.

dns-3   IN      A       10.0.0.13
web     IN      A       10.0.0.100
www     IN      CNAME   web
```

Consultas desde el cliente

```
cat /etc/resolv.conf
...
nameserver 10.0.0.11
```

Realizamos la consulta:

```
dig @10.0.0.11 www.es.example.com

...
;; QUESTION SECTION:
;www.es.example.com.        IN    A

;; ANSWER SECTION:
www.es.example.com.    86400    IN    CNAME   web.es.example.com.
web.es.example.com.    86400    IN    A    10.0.0.100

; AUTHORITY SECTION:
example.com.        86400    IN    NS    dns-3.es.example.com.
```

El servidor con autoridad (registro NS) es el servidor `dns-3.es.example.com`.

Servidor DNS dinámico

DNS dinámico

Es muy cómodo utilizar DHCP en una red local, pero tiene un inconveniente: no sabemos qué dirección tiene en cada momento un equipo. Una solución para esto es **sincronizar el servidor DHCP con el DNS, creando lo que se denomina un servidor DNS dinámico (DDNS)**.

Cada vez que se modifique una dirección IP (servidor DHCP), se registre el cambio en los ficheros que controlan la zona local (servidor DNS).

DNS dinámico. Configuración del DNS

El fichero `/etc/bind/rndc.key` contiene una clave para el rndc, que será muy importante en la sincronización con el servidor DHCP:

```
key "rndc-key" {
        algorithm hmac-md5;
        secret "5ydObFazIkZ3jUxlL5IvTw==";
};
```

Para utilizar dicha clave, añadimos al fichero `/etc/bind/named.conf.options`:

```
include "/etc/bind/rndc.key";
controls {
inet 127.0.0.1 port 953
allow { 127.0.0.1; } keys { "rndc-key"; };
```

Se permiten actualizaciones de las entradas DNS, pero sólo a quien facilite la clave y sólo desde localhost.

Creación de las zonas locales

Fichero `etc/bind/named.conf.local`:

```
include "/etc/bind/zones.rfc1918";
zone "example.com" {
    type master;
    file "db.example.com";
    allow-update { key "rndc-key"; };
};

zone "0.0.10.in-addr.arpa" {
    type master;
    file "db.0.0.10";
    allow-update { key "rndc-key"; };
};
```

Zona directa

Fichero /var/cache/bind/db.example.com:

```
$TTL    86400
@    IN    SOA    dns-1.example.com. root.example.com. (
                  1         ; Serial
             604800         ; Refresh
              86400         ; Retry
            2419200         ; Expire
              86400 )    ; Negative Cache TTL
;
@    IN    NS        dns-1.example.com.
@    IN    MX    10    correo.example.com.

$ORIGIN example.com.

dns-1        IN    A    10.0.0.11
```

¡¡¡No hemos nombrado ninguna máquina!!!

Zona inversa

Fichero /var/cache/bind/db.0.0.10:

```
$TTL    86400
@    IN    SOA    dns-1.example.com. root.example.com. (
                  1         ; Serial
             604800         ; Refresh
              86400         ; Retry
            2419200         ; Expire
              86400 )    ; Negative Cache TTL
;
@    IN    NS    dns-1.example.com.

$ORIGIN 0.0.10.in-addr.arpa.

11        IN    PTR    dns-1.example.com.
```

¡¡¡No hemos nombrado ninguna máquina!!!

Configuración del servidor DHCP

En el fichero `/etc/dhcp/dhcpd.conf`:

```
server-identifier dns-1;
ddns-updates on;
ddns-update-style interim;
ddns-domainname "example.com.";
ddns-rev-domainname "0.0.10.in-addr.arpa.";
deny client-updates;
include "/etc/bind/rndc.key";

zone example.com. {
  primary 127.0.0.1;
  key rndc-key;
}

zone 0.0.10.in-addr.arpa. {
  primary 127.0.0.1;
  key rndc-key;
}
```

Comprobación

- Nos quedaría comprobar que al añadir un cliente que tome direccionamiento desde el servidor DHCP, el servidor DNS podrá resolver su nombre.
- Si posteriormente cambia su dirección IP automática se actualizará en el servidor DNS.

Vistas en bind9

Control de acceso

Por defecto podemos consultar a un servidor DNS desde clientes que están en la misma red privada.

Si preguntamos desde otra red tenemos que configurar en el fichero `/etc/bind/named.conf.options`, los siguientes parámetros:

- **allow-query**: Especifica cuáles hosts tienen permitido consultar este servidor de nombres.
- **allow-recursion**: Parecida a la anterior, salvo que se aplica a las peticiones recursivas.

En ambos parámetros se puede poner **any;** para indicar todas las direcciones.

- En alguna circunstancia nos puede interesar que un mismo nombre que resuelve nuestro DNS devuelve direcciones IP distintas según en qué red esté conectada el cliente que realiza la consulta.

Ejemplo Una máquina a una red interna con direccionamiento 10.0.0.0/24 y a una red externa 172.22.0.0/16. Vamos a configurar bind9 para que cuando se consulte el nombre del servidor desde la red externa devuelva la ip flotante (172.22.0.129) y cuando la consulta se realice desde la red interna se devuelva la ip fija (10.0.0.13).

En este ejemplo tenemos dos vistas:

- Vista interna
- Vista externa

Definición de las vistas. Vista interna.

Fichero `etc/bind/named.conf.local`:

```
view interna {
    match-clients { 10.0.0.0/24; 127.0.0.1; };
    allow-recursion { any; };

        zone "example.org"
        {
                type master;
                file "db.interna.example.org";
        };
        zone "0.0.10.in-addr.arpa"
        {
                type master;
                file "db.0.0.10";
        };
        include "/etc/bind/zones.rfc1918";
        include "/etc/bind/named.conf.default-zones";
};
```

Definición de las vistas. Vista externa.

Fichero `etc/bind/named.conf.local`:

```
view externa {
    match-clients { 172.22.0.0/16; };
    allow-recursion { any; };

        zone "example.org"
        {
                type master;
                file "db.externa.example.org";
        };
        zone "22.172.in-addr.arpa"
        {
                type master;
                file "db.22.172";
        };
        include "/etc/bind/zones.rfc1918";
        include "/etc/bind/named.conf.default-zones";
};
```

¿Cómo funcionan las vistas?

- En la zona definida en **db.interna.example.org** y **db.0.0.10** se define el direccionamiento **10.0.0.0/24**.
- En la zona definida en **db.externa.example.org** y **db.22.172** se define el direccionamiento **172.22.0.0/16**.
- El parámetro **match-clients** nos permite que diferenciar la vista que se va a ofrecer según la ip de la petición de la consulta.
- Todas las zonas definidas deben estar dentro de una zona, por lo tanto las zonas de resolución inversa definidas en el RFC1918 y las zonas por defecto, la hemos incluido en cada una de las vistas.
- Debemos eliminar las zonas por defecto del fichero **named.conf**:

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