Creación y gestión de las zonas DNS

Un servidor primario DNS gestiona una o varias zonas. Cada una corresponde a un dominio o a un subdominio de una arborescencia DNS. Opcionalmente puede proporcionar una copia de un archivo de zona, en solo lectura, a uno o a distintos servidores secundarios . Estos últimos pueden dar respuestas autoritativas a las solicitudes de resolución relacionadas con los registros de la zona. Sin embargo, solo el servidor primario puede actualizar el contenido del archivo de zona.

Un servidor DNS puede ser servidor primario para una o varias zonas y servidor secundario para otras zonas.

Para cada archivo de zona debería corresponder un archivo de zona de búsqueda inversa, que permite la resolución inversa (dar el nombre DNS relacionado con una dirección IP). También será necesaria la presencia de un archivo de zona de búsqueda inversa para las direcciones IPv6.

El contenido de un archivo de zona obedece a una sintaxis precisa y exacta, el mínimo error puede hacer que el servidor DNS no lo cargue.

1. Archivo de zona de búsqueda

La zona tiene que estar declarada en el archivo de configuración `named.conf` por una directiva `zone` especificando el nombre de la zona, su tipo y el nombre del archivo de zona.

El archivo de zona tiene que encontrarse en el directorio de datos declarado en el archivo de configuración `named.conf` , con la opción `directory` (por defecto `/var/named` o `/var/cache/bind`).

Ejemplo

Declaración de una zona en el archivo `named.conf` :

```
zone "lpic2test.com" IN {
    type master;
    file "lpic2.zone";
};
```

Se trata de una zona de tipo `master`, para la que el servidor DNS desempeña el rol de servidor principal.

Un archivo de zona contiene un registro de tipo SOA, que describe las características de la zona, y un conjunto de registros de recursos (tipo RR) para cada nombre de host o de servicio de la zona.

En un archivo de zona, los comentarios van desde el carácter ; hasta el final de la línea. El separador de los campos es un conjunto de caracteres espacio o tabulación, el separador de los registros está al final de la línea (excepto si el registro continúa a lo largo de varias líneas entre paréntesis).

a. Registro de zona (tipo SOA)

Este registro define la zona y sus atributos. Su sintaxis es la siguiente:

```
Dominio|@ IN SOA ServidorPrimario MailAdmin (
Serial
Refresh
Retry
Expire
MinimumTTL
)
```

Donde:

- `Dominio` o `@:` nombre del dominio o subdominio correspondiente a la zona. El carácter especial `@,` que se puede usar dentro del archivo de zona, designa el nombre del dominio o subdominio local, tal y como está definido en la directiva `zone` del archivo de configuración `named.conf`. Preste atención, el nombre del dominio o subdominio debe terminar con el carácter '.'.

- `IN`: clase del registro. Siempre `IN` (*Internet*).
- `SOA`: tipo del registro (*Start Of Authority*).
- `ServidorPrimario` : FQDN del servidor DNS principal de la zona. Cuidado, el nombre de dominio de subdominio tiene que terminar con el carácter '`.`'.
- `MailAdmin` : correo electrónico del responsable del servidor DNS. El carácter `@` en la dirección debe ser reemplazado por el carácter '`.`'. Si la dirección de correo electrónico tiene caracteres '`.`', deben ir precedidos por el carácter '`\`'. La dirección de correo electrónico debe terminar con el carácter '`.`'.
- `Serial` : este número, que tendrá como máximo diez dígitos, tiene que ser incrementado para cada conjunto de modificaciones. Esto permite que los servidores secundarios sepan si la versión del archivo está actualizada o si hay que actualizarla.
- `Refresh` : período de tiempo a partir del cual el servidor secundario tiene que interrogar al servidor principal para obtener el número de serie y saber si ha habido actualizaciones.
- `Retry` : si el servidor principal no responde a una solicitud del número de serie, período que se tiene que respetar antes de que el servidor secundario vuelva a interrogar al servidor principal.
- `Expire` : período de tiempo a partir del cual, en ausencia de actualizaciones del servidor primario, la información de zona de un servidor secundario será considerada como obsoleta.
- `MinimumTTL` : al principio, este campo especificaba el período de tiempo de validez (TTL, *Time To Live*) de un registro de la zona. Desde la RFC 2308, determina el período de tiempo de validez de una respuesta negativa a una demanda de resolución, en el caché de un servidor DNS.

Los periodos son números enteros, se les pueden poner los sufijos: `W` (semanas), `D` (días), `H` (horas) o `M` (minutos). En la ausencia de un sufijo, el número será considerado como segundos.

Ejemplo

Registro SOA de la zona del dominio `lpic2test.com.` :

```
@ IN SOA centos8.lpic2test.com. admin.lpic2test.com. (
2020050501; serial
6H; refresh
1H; retry
2D; expire
1H); minimum
```

El correo electrónico del administrador es `admin@lpic2test.com` .

El carácter `@` *reemplaza a* `lpic2test.com` *, el nombre del dominio asociado a la zona en el archivo* `/etc/named.conf` :

```
zone "lpic2test.com" IN {
    type master;
    file "lpic2.zone";
};
```

b. Registros de recursos

Los elementos relativos a los nombres de host o de servicios y a las direcciones IP correspondientes están declarados en los registros de recursos (RR, *Resource Record*). El formato de un registro es el siguiente:

```
Nombre  [TTL]  Clase    Tipo Datos
```

Donde:

`Nombre`	Nombre simple o FQDN del recurso.
`TTL`	Periodo de validez (*Time To Live*) en la caché de un servidor DNS, opcional.
`Clase`	Clase del nombre. Siempre IN (Internet).
`Tipo`	Tipo del recurso.
`Datos`	Uno o más valores según el tipo de recurso.

El campo `TTL` es opcional. Se puede especificar un TTL por defecto declarando una variable `$TTL` antes de los registros de recursos:

```
$TTL    Valor
```

Los recursos pueden ser de tipos diferentes. Los tipos principales están descritos a continuación.

Servidor de nombres (tipo NS)

Este tipo (*Name server*) declara los servidores de nombres del dominio de la zona y opcionalmente de sus subdominios. Todos los servidores de nombres del dominio y de los subdominios tienen que estar declarados. El formato del registro es el siguiente:

```
NombreDominio   [TTL]   IN   NS   FQDN
```

También es necesario un registro de tipo Dirección (`A` o `AAAA`) para especificar la dirección IP de cada servidor de nombres.

Dirección (tipo A o AAAA)

Estos registros contienen información relativa a los nombres de hosts y su dirección IP. El tipo `A` corresponde a las direcciones IPv4, el tipo `AAAA` a las direcciones IPv6.

El nombre puede ser un nombre simple, automáticamente se le añade el sufijo del nombre de dominio de la zona.

Alias (tipo CNAME)

Este tipo (*Canonical name*) hace la correspondencia entre un nombre (*alias*) y un FQDN.

Servidor de mensajería (tipo MX)

Este tipo (*Mail eXchanger*) declara los servidores de mensajería del dominio de la zona. Podemos asignar distintos niveles de prioridad a cada servidor para determinar el orden de solicitud de los servidores de mensajería.

Ejemplo

Registros de recursos del archivo de zona del dominio `lpic2test.com.` , con dos servidores que se reparten los diferentes servicios:

```
$TTL 1D
; Servidores DNS:
@           IN    NS    centos8.lpic2test.com.
@           IN    NS    debian10.lpic2test.com.
; servidores de mensajería
@           IN    MX    10    centos8.lpic2test.com. ; servidor prioritario
@           IN    MX    20    debian10.lpic2test.com.
; Direcciones (IPv4):
centos8      IN    A     192.168.0.60
debian10          IN    A     192.168.0.70
station      IN   A 192.168.0.24
; Alias:
www          IN    CNAME   centos8
ftp          IN    CNAME   debian10
```

c. Ejemplo de archivo

Este archivo de zona de búsqueda corresponde al dominio `lpic2test.com.` , con dos servidores DNS:

```
; Archivo de zona lpic2test.com.
$TTL 1D
@ IN SOA centos8.lpic2test.com. admin.lpic2test.com. (
2020050501; serial
6H; refresh
1H; retry
2D; expire
1H); minimum
; Servidores DNS:
@           IN    NS    centos8.lpic2test.com.
@           IN    NS    debian10.lpic2test.com.
; servidores de mensajería
@           IN    MX    10    centos8.lpic2test.com. ; servidor prioritario
@           IN    MX    20    debian10.lpic2test.com.
; Direcciones (IPv4):
centos8      IN    A     192.168.0.60
debian10          IN    A     192.168.0.70
station      IN   A 192.168.0.24
; Alias:
www          IN    CNAME  centos8
ftp          IN    CNAME  debian10
```

2. Archivo de zona de búsqueda inversa

El archivo de zona de búsqueda inversa (*forward lookup*) tiene la misma estructura que un archivo de zona directa, pero sus registros de recursos son de tipo PTR.

a. Declaración de la zona en named.conf

El nombre de la zona está formado por los bytes de la parte de red de la dirección IP,

ordenados en sentido inverso y con el sufijo del nombre de dominio « `.in-addr.arpa` ».

Ejemplo

Declaración de la zona de búsqueda inversa de la red `192.168.0.0/24` en el archivo `named.conf` :

```
zone "0.168.192.in-addr.arpa" IN {
    type  master;
    file  "db.192.168.0";
};
```

b. Registro SOA

Es necesario un registro de tipo SOA, al igual que para una zona de búsqueda de nombres.

Ejemplo

Registro SOA de una zona de búsqueda inversa, administrada por el servidor principal `centos8.lpic2test.com.` :

```
@ IN SOA centos8.lpic2test.com. admin.lpic2test.com. (
2020050501; serial
6H; refresh
1H; retry
2D; expire
1H); minimum
```

c. Registros de recursos

Hay que declarar los servidores DNS de la zona de búsqueda inversa, con registros de tipo `NS`.

Los registros de tipo `PTR` asocian a la parte del host de la dirección IP un nombre DNS. Se le añade automáticamente a la dirección como sufijo el nombre de la zona.

Ejemplo

Registros de recursos de diferentes hosts en la zona de búsqueda inversa de la red `192.168.0.0/24` :

```
; servidor de nombres:
@       NS      centos8.lpic2test.com.
@       NS      debian10.lpic2test.com.
; Address records:
60              IN      PTR     centos8.lpic2test.com.
70              IN      PTR     debian10.lpic2test.com.
24              IN      PTR     station.lpic2test.com.
```

d. Ejemplo de archivo

Este archivo de zona de búsqueda inversa corresponde a la red `192.168.0.0/24` , con dos servidores DNS:

```
$TTL 1D
@ IN SOA centos8.lpic2test.com. admin.lpic2test.com. (
2020050501; serial
6H; refresh
1H; retry
2D; expire
1H) ; minimum
; servidor de nombres:
@       NS      centos8.lpic2test.com.
@       NS      debian10.lpic2test.com.
; Address records:
60              IN      PTR     centos8.lpic2test.com.
70              IN      PTR     debian10.lpic2test.com.
24              IN      PTR     station.lpic2test.com.
```

3. Gestión de zonas secundarias

Cada Zona DNS es en general copiada hacia servidores secundarios, para asegurar un buen nivel de tolerancia a fallos. Un servidor secundario puede responder a las solicitudes de resolución de nombres o de direcciones de elementos de su zona, pero no puedo actualizarla.

La zona está configurada para especificar la periodicidad con la que el servidor secundario interroga al servidor primario para obtener el número de versión actual del archivo de zona. Si el archivo de zona del servidor secundario no está actualizado, el servidor solicita al servidor primario la transferencia de su archivo de zona.

a. Declaración de la zona secundaria en named.conf

La zona tiene que estar declarada en el archivo `named.conf` , con el tipo `slave` y el o los servidores a los que hay que solicitar el número de versión del archivo de zona actual. Durante la carga de la configuración, el daemon `named` contacta con uno de los servidores especificados y recupera el archivo de zona.

El servidor especificado en el atributo `masters` no tiene por qué ser el servidor principal, puede ser un servidor secundario, lo que permite repartir la carga de las transferencias de zona. Si hay distintos servidores especificados, se contactará con ellos en el orden de declaración.

Ejemplo

Declaración de una zona para un servidor secundario, en una distribución Debian 10, en el archivo `/etc/bind/named.conf.local` *:*

```
zone "lpic2test.com" {
type slave;
file "lpic2.zone";
masters {192.168.0.60;};
};
```

Por defecto, los archivos de zona almacenados por un servidor DNS secundario se encuentran en formato binario, poco legible. Se puede configurar la zona en el servidor secundario para que el archivo transferido desde el servidor principal esté en formato de texto. Hay que añadir la directiva siguiente en la declaración de la zona:

```
masterfile-format text;
```

4. Delegación de zona

La delegación de zona tiene como objetivo confiar la responsabilidad de un subdominio de la zona a otros servidores DNS. Es así como se gestiona la arborescencia de un sistema DNS como el de Internet. Los servidores DNS de los dominios de primer nivel (TLD) delegan la gestión de los dominios de segundo nivel a servidores DNS, estos últimos delegan la gestión de sus subdominios, etc.

En el archivo de zona del servidor delegatario, es necesario que haya un registro de tipo `NS` y un registro de tipo dirección (`A` o `AAAA`) para cada servidor DNS del subdominio delegado. El registro de tipo de dirección se llama DNS asociado (*glue record*), porque permite conocer la dirección IP del o de los servidores delegados al servidor DNS. Estos últimos son la autoridad en el subdominio delegado (con un servidor primario y uno o varios servidores secundarios).

La configuración de la zona delegada, en el servidor principal delegado, será parecida a la que se ha visto anteriormente.

Ejemplo

Definición de servidores DNS delegados para el subdominio `intra` del dominio `lpic2test.com`, en el archivo de zona delegataria:

```
intra.lpic2test.com.      IN   NS   srv1.intra.lpic2test.com.
intra.lpic2test.com.      IN   NS   srv2.intra.lpic2test.com.
srv1.intra.lpic2test.com. IN    A   192.168.0.80
srv2.intra.lpic2test.com. IN    A   192.168.0.90
```

5. Control de un archivo de zona

Los comandos `named-checkzone` y `named-compilezone` permiten comprobar la sintaxis del contenido del archivo de zona cuyo nombre y camino de acceso han sido utilizados como argumento:

```
named-checkzone [Opciones] NombreZona CaminoArchivoZona
named-compilezone [Opciones] NombreZona CaminoArchivoZona
```

El comando `named-compilezone` además puede convertir en salida el archivo de zona de un formato binario a un formato de texto, para leer un archivo de zona de servidor secundario o, por el contrario, optimizar su tiempo de carga.

Ejemplo

```
named-checkzone lpic2test.com. /var/named/lpic2.zone
zone lpic2test.com/IN: loaded serial 2020050501
OK
```

El archivo de zona es correcto desde el punto de vista de la sintaxis.

Modificamos un registro quitándole el carácter punto al final de un FQDN:

```
@           IN    NS     centos8.lpic2test.com
named-checkzone lpic2test.com. /var/named/lpic2.zone
zone lpic2test.com/IN: NS 'centos8.lpic2test.com.lpic2test.com' has no
address records (A or AAAA)
zone lpic2test.com/IN: not loaded due to errors.
```

El comando muestra el error. Podemos constatar que en ausencia del carácter '`.`' final, el nombre de dominio de la zona es automáticamente añadido al FQDN, lo que hace que sea incorrecto.

6. Pruebas de un servidor DNS

La configuración de los servidores DNS es relativamente compleja, y un error de sintaxis en uno de los archivos de configuración puede provocar que el servidor no arranque. También hay que configurar los diferentes clientes, a través del archivo `/etc/resolv.conf` , incluyendo los mismos servidores DNS.

Distintos comandos permiten comprobar el buen funcionamiento de los servidores DNS, primarios, secundarios, de caché o de tránsito para la resolución de nombres y para la resolución inversa.

a. El comando nslookup

Este comando de origen Unix ha sido, durante mucho tiempo, la herramienta más eficaz para comprobar los servidores DNS. En Linux, está considerado como en vía de obsolescencia, y es remplazado por el comando `dig`.

El comando puede funcionar en modo línea de comandos (con opciones y argumentos) o en modo interactivo si se ejecuta sin argumentos.

Sintaxis

```
nslookup  [ Opciones ] Nombre|Dirección [DirServidor]
```

Parámetros principales

`Opciones`	Comandos del modo interactivo, precedidos por un guión.
`Nombre|Dirección`	Nombre o dirección que se va a resolver.
`DirServidor`	Dirección del servidor DNS, si no a través de `/etc/resolv.conf` .

Ejemplo

Interrogación del servidor BIND de la máquina local:

```
nslookup www.redhat.com
Server:         127.0.0.1
Address:        127.0.0.1#53

Non-authoritative answer:
www.redhat.com  canonical name = ds-www.redhat.com.edgekey.net.
ds-www.redhat.com.edgekey.net   canonical name =
ds-www.redhat.com.edgekey.net.globalredir.akadns.net.
ds-www.redhat.com.edgekey.net.globalredir.akadns.net    canonical name =
e3396.dscx.akamaiedge.net.
Name:   e3396.dscx.akamaiedge.net
Address: 2.22.195.226
Name:   e3396.dscx.akamaiedge.net
Address: 2a02:26f0:e3:3a4::d44
Name:   e3396.dscx.akamaiedge.net
Address: 2a02:26f0:e3:3ac::d44
```

Interrogación del servidor DNS `8.8.8.8` (ofrecido por Google):

```
nslookup www.debian.org 8.8.8.8
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   www.debian.org
Address: 149.20.4.15
Name:   www.debian.org
Address: 128.31.0.62
Name:   www.debian.org
Address: 130.89.148.77
Name:   www.debian.org
Address: 2001:67c:2564:a119::77
```

Interrogación del servidor DNS local sobre un nombre de su propia zona:

```
nslookup www.lpic2test.com
Server:         127.0.0.1
Address:        127.0.0.1#53

www.lpic2test.com       canonical name = centos8.lpic2test.com.
Name:   centos8.lpic2test.com
Address: 192.168.0.60
```

La respuesta es autoritaria, al contrario que en las interrogaciones anteriores.

b. El comando dig

El comando `dig` permite comprobar exhaustivamente el funcionamiento de un servidor DNS. Dispone de numerosas opciones para gestionar diferentes aspectos de la resolución de nombres.

Sintaxis

```
dig   [ Opciones ] [@DirServidor] Nombre|Dirección
```

Parámetros principales

`-t Tipo`	Tipo de registro que se va a buscar (`A`, `AAAA`, `MX`, `NS`, `PTR`…).
`-4`	Usar IPv4.
`-6`	Usar IPv6.
`-x`	Búsqueda inversa utilizando la dirección IP especificada como argumento.
`Nombre|Dirección`	Nombre o dirección que se va a resolver.
`@DirServidor`	Dirección del servidor DNS, si no estuviera especificada se usaría `/etc/resolv.conf` .

Ejemplo

Interrogación del servidor BIND de la machine local:

```
dig www.redhat.com
; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el8 <<>> www.redhat.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 8, ADDITIONAL: 10

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 3ed87960f0fd37a5bd52e7655eb3024f7be50a9da739d4dd (good)
;; QUESTION SECTION:
;www.redhat.com.                IN      A

;; ANSWER SECTION:
www.redhat.com.         3081    IN      CNAME   ds-www.redhat.com.edgekey.net.
ds-www.redhat.com.edgekey.net. 21081 IN CNAME
```

```
ds-www.redhat.com.edgekey.net.globalredir.akadns.net.
ds-www.redhat.com.edgekey.net.globalredir.akadns.net. 3081 IN CNAME
e3396.dscx.akamaiedge.net.
e3396.dscx.akamaiedge.net. 20   IN     A      2.22.195.226

;; AUTHORITY SECTION:
dscx.akamaiedge.net.    3481    IN      NS      n6dscx.akamaiedge.net.
dscx.akamaiedge.net.    3481    IN      NS      n4dscx.akamaiedge.net.
dscx.akamaiedge.net.    3481    IN      NS      n0dscx.akamaiedge.net.
dscx.akamaiedge.net.    3481    IN      NS      n1dscx.akamaiedge.net.
dscx.akamaiedge.net.    3481    IN      NS      n5dscx.akamaiedge.net.
dscx.akamaiedge.net.    3481    IN      NS      n7dscx.akamaiedge.net.
dscx.akamaiedge.net.    3481    IN      NS      n2dscx.akamaiedge.net.
dscx.akamaiedge.net.    3481    IN      NS      n3dscx.akamaiedge.net.

;; ADDITIONAL SECTION:
n1dscx.akamaiedge.net.  3481    IN      A       84.53.147.62
n4dscx.akamaiedge.net.  3481    IN      A       95.100.171.39
n2dscx.akamaiedge.net.  3481    IN      A       95.100.171.77
n5dscx.akamaiedge.net.  3481    IN      A       95.100.171.37
n6dscx.akamaiedge.net.  3481    IN      A       95.100.171.75
n3dscx.akamaiedge.net.  3481    IN      A       2.23.92.63
n7dscx.akamaiedge.net.  3481    IN      A       92.123.182.100
n0dscx.akamaiedge.net.  3481    IN      A       88.221.81.192
n0dscx.akamaiedge.net.  3481    IN      AAAA    2600:1480:e800::c0

;; Query time: 2 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: mier. mayo 06 19:30:39 BST 2020
;; MSG SIZE  rcvd: 553
```

Interrogación del servidor DNS `8.8.8.8` (proporcionado por Google):

```
dig @8.8.8.8 www.debian.org
; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el8 <<>> @8.8.8.8 www.debian.org
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13087
```

```
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.debian.org.                IN      A

;; ANSWER SECTION:
www.debian.org.         299     IN      A       130.89.148.77

;; Query time: 25 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: mier. mayo 06 19:32:28 BST 2020
;; MSG SIZE  rcvd: 59
```

Interrogación del servidor DNS local, sobre un nombre de su zona:

```
dig www.lpic2test.com
; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el8 <<>> www.lpic2test.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22241
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 1c60bf8a18e21cda13e6d2a25eb30308a44a9619eb7e5c21 (good)
;; QUESTION SECTION:
;www.lpic2test.com.             IN      A

;; ANSWER SECTION:
www.lpic2test.com.      86400   IN      CNAME   centos8.lpic2test.com.
centos8.lpic2test.com.  86400   IN      A       192.168.0.60

;; AUTHORITY SECTION:
lpic2test.com.          86400   IN      NS      centos8.lpic2test.com.
lpic2test.com.          86400   IN      NS      debian10.lpic2test.com.

;; ADDITIONAL SECTION:
```

```
debian10.lpic2test.com.  86400  IN    A      192.168.0.70

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: mier. mayo 06 19:33:44 BST 2020
;; MSG SIZE  rcvd: 164
```