

12.3. Archivos de zona

Los *Archivos de zona* contienen información sobre un espacio de nombres particular y son almacenados en el directorio de trabajo `named`, por defecto `/var/named/`. Cada archivo de zona es nombrado de acuerdo a la opción `file` en la declaración `zone`, usualmente en una forma que relaciona al dominio en cuestión e identifica el archivo como conteniendo datos de zona, tal como `example.com.zone`.

Cada archivo de zona contiene *directivas* y *registros de recursos*. Las directivas le dicen al servidor de nombres que realice tareas o aplique configuraciones especiales a la zona. Los registros de recursos define los parámetros de la zona y asignan identidades a hosts individuales. Las directivas son opcionales, pero los registros de recursos se requieren para proporcionar servicios de nombres a la zona.

Todas las directivas y registros de recursos deberían ir en sus propias líneas individuales.

Los comentarios se pueden colocar después de los punto y comas (;) en archivos de zona.

12.3.1. Directivas de archivos de zona

Las directivas comienzan con el símbolo de dollar (\$) seguido del nombre de la directiva. Usualmente aparecen en la parte superior del archivo de zona.

Lo siguiente son directivas usadas a menudo:

- `$INCLUDE` — Dice a `named` que incluya otro archivo de zona en el archivo de zona donde se usa la directiva. Así se pueden almacenar configuraciones de zona suplementarias aparte del archivo de zona principal.
- `$ORIGIN` — Anexa el nombre del dominio a registros no cualificados, tales como aquellos con el nombre de host solamente.

Por ejemplo, un archivo de zona puede contener la línea siguiente:

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

Cualquier nombre utilizado en registros de recursos que no terminen en un punto (.) tendrán `example.com` anexado.



Nota

El uso de la directiva `$ORIGIN` no es necesario si la zona es especificada en `/etc/named.conf` porque la zona es usada como el valor de la directiva `$ORIGIN` por defecto.

- `$TTL` — Ajusta el valor *Time to Live (TTL)* predeterminado para la zona. Este es el tiempo, en segundos, que un registro de recurso de zona es válido. Cada recurso puede contener su propio valor TTL, el cual ignora esta directiva.

Cuando se decide aumentar este valor, permite a los servidores de nombres remotos hacer

caché a la información de zona para un período más largo de tiempo, reduciendo el número de consultas para la zona y alargando la cantidad de tiempo requerido para proliferar cambios de registros de recursos.

12.3.2. Registros de recursos de archivos de zona

El componente principal de un archivo de zona es su registro de recursos.

Hay muchos tipos de registros de recursos de archivos de zona. A continuación le mostramos los tipos de registros más frecuentes:

- **A** — Registro de dirección que especifica una dirección IP que se debe asignar a un nombre, como en el ejemplo:

<code><host></code>	<code>IN</code>	<code>A</code>	<code><IP-address></code>
---------------------------	-----------------	----------------	---------------------------------

Si el valor `<host>` es omitido, el registro `A` apunta a una dirección IP por defecto para la parte superior del espacio de nombres. Este sistema es el objetivo para todas las peticiones no FQDN.

Considere el siguiente ejemplo de registro `A` para el archivo de zona `example.com`:

	<code>IN</code>	<code>A</code>	<code>10.0.1.3</code>
<code>server1</code>	<code>IN</code>	<code>A</code>	<code>10.0.1.5</code>

Las peticiones para `example.com` son apuntadas a `10.0.1.3`, mientras que las solicitudes para `server1.example.com` son dirigidas a `10.0.1.5`.

- **CNAME** — Registro del nombre canónico, que enlaza un nombre con otro: también conocido como un alias.

El próximo ejemplo indica a `named` que cualquier petición enviada a `<alias-name>` apuntará al host, `<real-name>`. Los registros `CNAME` son usados normalmente para apuntar a servicios que usan un esquema de nombres común, tal como `www` para servidores Web.

<code><alias-name></code>	<code>IN</code>	<code>CNAME</code>	<code><real-name></code>
---------------------------------	-----------------	--------------------	--------------------------------

En el ejemplo siguiente, un registro `A` vincula un nombre de host a una dirección IP, mientras que un registro `CNAME` apunta al nombre host comúnmente usado `www` para este.

<code>server1</code>	<code>IN</code>	<code>A</code>	<code>10.0.1.5</code>
<code>www</code>	<code>IN</code>	<code>CNAME</code>	<code>server1</code>

- **MX** — Registro de Mail eXchange, el cual indica dónde debería de ir el correo enviado a un espacio de nombres particular controlado por esta zona.

	<code>IN</code>	<code>MX</code>	<code><preference-value></code>	<code><email-server-name></code>
--	-----------------	-----------------	---------------------------------------	--

En este ejemplo, *<preference-value>* permite una clasificación numérica de los servidores de correo para un espacio de nombres, dando preferencia a algunos sistemas de correo sobre otros. El registro de recursos **MX** con el valor más bajo *<preference-value>* es preferido sobre los otros. Sin embargo, múltiples servidores de correo pueden tener el mismo valor para distribuir el tráfico de forma pareja entre ellos.

El *<email-server-name>* puede ser un nombre de servidor o FQDN.

IN	MX	10	mail.example.com.
IN	MX	20	mail2.example.com.

En este ejemplo, el primer servidor de correo mail.example.com es preferido al servidor de correo mail2.example.com cuando se recibe correo destinado para el dominio example.com.

- **NS** — Registro NameServer, el cual anuncia los nombres de servidores con autoridad para una zona particular.

Este es un ejemplo de un registro **NS**:

IN	NS	<nameserver-name>
----	----	-------------------

El *<nameserver-name>* debería ser un FQDN.

Luego, dos nombres de servidores son listados como con autoridad para el dominio. No es importante si estos nombres de servidores son esclavos o si son maestros; ambos son todavía considerados con autoridad.

IN	NS	dns1.example.com.
IN	NS	dns2.example.com.

- **PTR** — Registro PoinTeR o puntero, diseñado para apuntar a otra parte del espacio de nombres.

Los registros **PTR** son usados principalmente para la resolución inversa de nombres, pues ellos apuntan direcciones IP de vuelta a un nombre particular. Consulte la [Sección 12.3.4](#) para más ejemplos de registros **PTR** en uso.

- **SOA** — Registro de recursos Start Of Authority, que declara información importante de autoridad relacionada con espacios de nombres al servidor nombres.

Está situado detrás de las directivas, un registro **SOA** es el primer registro en un archivo de zona.

El ejemplo siguiente muestra la estructura básica de un registro de recursos **SOA**:

@	IN	SOA	<primary-name-server> <serial-number> <time-to-refresh> <time-to-retry> <time-to-expire> <minimum-TTL>	<hostmaster-email> ()
---	----	-----	---	------------------------

El símbolo @ coloca la directiva \$ORIGIN (o el nombre de la zona, si la directiva \$ORIGIN no está configurada) como el espacio de nombres que esta siendo definido por este registro de recursos SOA. El nombre del host del servidor de nombres que tiene autoridad para este dominio es la directiva <primary-name-server> y el correo electrónico de la persona a contactar sobre este espacio de nombres es la directiva <hostmaster-email>.

La directiva <serial-number> es un valor numérico que es incrementado cada vez que se cambia el archivo de zona para así indicar a named que debería recargar esta zona. La directiva <time-to-refresh> es el valor numérico que los servidores esclavos utilizan para determinar cuánto tiempo debe esperar antes de preguntar al servidor de nombres maestro si se han realizado cambios a la zona. El valor <serial-number> es usado por los servidores esclavos para determinar si esta usando datos de la zona desactualizados y si debería refrescarlos.

La directiva <time-to-retry> es un valor numérico usado por los servidores esclavo para determinar el intervalo de tiempo que tiene que esperar antes de emitir una petición de actualización de datos en caso de que el servidor de nombres maestro no responda. Si el servidor maestro no ha respondido a una petición de actualización de datos antes que se acabe el intervalo de tiempo <time-to-expire>, los servidores esclavo paran de responder como una autoridad por peticiones relacionadas a ese espacio de nombres.

La directiva <minimum-TTL> es la cantidad de tiempo que otros servidores de nombres guardan en caché la información de zona.

Cuando se configura BIND, todos los tiempos son siempre referenciados en segundos. Sin embargo, es posible usar abreviaciones cuando se especifiquen unidades de tiempo además de segundos, tales como minutos (M), horas (H), días (D) y semanas (W). La [Tabla 12-1](#) le muestra la cantidad de tiempo en segundos y el tiempo equivalente en otro formato.

Segundos	Otras unidades de tiempo
60	1M
1800	30M
3600	1H
10800	3H
21600	6H
43200	12H
86400	1D
259200	3D
604800	1W
31536000	365D

Tabla 12-1. Segundos comparados a otras unidades de tiempo

El ejemplo siguiente ilustra la forma que un registro de recursos SOA puede tomar cuando es configurado con valores reales.

```
@      IN      SOA      dns1.example.com.      hostmaster.example.com. (
                                2001062501 ; serial
                                21600      ; refresh after 6 hours
                                3600       ; retry after 1 hour
                                604800    ; expire after 1 week
                                86400 )    ; minimum TTL of 1 day
```

12.3.3. Ejemplo de archivo de zonas

Vistos individualmente, las directivas y registros de recursos pueden ser difíciles de comprender. Sin embargo, cuando se colocan juntos en un mismo archivo, se vuelven más fáciles de entender.

El ejemplo siguiente muestra un archivo de zona muy básico.

```
$ORIGIN example.com.
$TTL 86400
@      IN      SOA      dns1.example.com.      hostmaster.example.com. (
                                2001062501 ; serial
                                21600      ; refresh after 6 hours
                                3600       ; retry after 1 hour
                                604800    ; expire after 1 week
                                86400 )    ; minimum TTL of 1 day

      IN      NS       dns1.example.com.
      IN      NS       dns2.example.com.

      IN      MX       10      mail.example.com.
      IN      MX       20      mail2.example.com.

      IN      A        10.0.1.5

server1      IN      A        10.0.1.5
server2      IN      A        10.0.1.7
dns1         IN      A        10.0.1.2
dns2         IN      A        10.0.1.3

ftp          IN      CNAME    server1
mail         IN      CNAME    server1
mail2        IN      CNAME    server2
www          IN      CNAME    server2
```

En este ejemplo, las directivas estándar y los valores SOA son usados. Los servidores de nombres con autoridad se configuran como `dns1.example.com` y `dns2.example.com`, que tiene archivos A que los juntan a `10.0.1.2` y a `10.0.1.3`, respectivamente.

Los servidores de correo configurados con los registros MX apuntan a `server1` y `server2` a través de registros CNAME. Puesto que los nombres `server1` y `server2` no terminan en un punto (`.`), el dominio `$ORIGIN` es colocado después de ellos, expandiéndolos a `server1.example.com` y a `server2.example.com`. A través de registros de recursos relacionados A, se puede determinar sus direcciones IP.

Los servicios FTP y Web, disponibles en los nombres estándar `ftp.example.com` y `www.example.com`, son apuntados a los servidores apropiados usando registros `CNAME`.

12.3.4. Archivos de zona de resolución de nombres inversa

Se usa un archivo de zona de resolución inversa de nombres para traducir una dirección IP en un espacio de nombres particular en un FQDN. Se vé muy similar a un archivo de zona estándar, excepto que se usan registros de recursos `PTR` para enlazar las direcciones IP a un nombre de dominio completamente cualificado.

Un registro `PTR` se vería similar a esto:

```
<last-IP-digit>      IN      PTR      <FQDN-of-system>
```

El valor `<last-IP-digit>` se refiere al último número en una dirección IP que apunta al FQDN de un sistema particular.

En el ejemplo siguiente, las direcciones IP de la `10.0.1.20` a la `10.0.1.25` apuntan a los FQDNs correspondientes.

```
$ORIGIN 1.0.10.in-addr.arpa.
$TTL 86400
@      IN      SOA      dns1.example.com.      hostmaster.example.com. (
                        2001062501 ; serial
                        21600      ; refresh after 6 hours
                        3600       ; retry after 1 hour
                        604800     ; expire after 1 week
                        86400 )    ; minimum TTL of 1 day

      IN      NS       dns1.example.com.
      IN      NS       dns2.example.com.

20     IN      PTR      alice.example.com.
21     IN      PTR      betty.example.com.
22     IN      PTR      charlie.example.com.
23     IN      PTR      doug.example.com.
24     IN      PTR      ernest.example.com.
25     IN      PTR      fanny.example.com.
```

Este archivo de zona se colocará en funcionamiento con una declaración `zone` en el archivo `named.conf` el cual se ve similar a lo siguiente:

```
zone "1.0.10.in-addr.arpa" IN {
    type master;
    file "example.com.rr.zone";
    allow-update { none; };
};
```

Hay muy poca diferencia entre este ejemplo y una declaración de `zone` estándar, excepto por el nombre de la zona. Observe que una zona de resolución de nombres inversa requiere que los primeros tres bloques de la dirección IP estén invertidos seguido por `.in-addr.arpa`. Esto permite asociar con la zona a un bloque único de números IP usados en el archivo de zona de

resolución de nombres inversa.

[Anterior](#)
[/etc/named.conf](#)

[Inicio](#)
[Subir](#)

[Siguiente](#)
Uso de `rndc`