

Configuración servidor DNS (bind9) en Ubuntu

Abril 1, 2006 a las 3:56 pm | Categoría GPL Tarragona |

* Fragmentos de texto extraídos del tutorial "Cómo configurar BIND" de Hugo Madrid Luna (Crowley) bajo FDL.

BIND es el servidor de nombres de dominio más popular en Internet, que trabaja en todas las plataformas informáticas principales y se caracteriza por su flexibilidad y seguridad.

Domain Name Service (DNS) es el servicio que resuelve los nombres de dominio asociados a una dirección IP para direccionar las peticiones a un servidor en específico. Se utiliza cuando un nodo (o host) en Internet contacta a otro mediante el nombre de dominio de la máquina y no por su dirección IP.

A través de este documento se verán las generalidades del servicio de resolución de nombres, la configuración y mantenimiento de un servicio de nombres con BIND, bajo la plataforma Linux, aunque la mayoría de estos conceptos se pueden aplicar a la cualquier servicio de DNS sobre otras plataformas.

Regularmente, todos los equipos que están en Internet o una Intranet tienen una dirección IP única que los identifica, generalmente dividido en cuatro segmentos u 'octetos', cuya representación es, por ejemplo, '172.29.183.217', pero el recordar todas las direcciones en este formato sería sumamente difícil, por lo que utilizamos los nombres de dominio para referenciarlos.

Existen varios productos que realizan esta función y en todas las plataformas, pero el más usado es **BIND (Berkeley Internet Name Domain)**, que es distribuido bajo la GNU GPL.

La estructura básica del DNS es similar a un árbol, donde se tiene una raíz o root, los Dominios de Nivel Principal (Top Level Domains) y los dominios de segundo nivel.

Los nombres de dominio completamente calificados o FQDN (fully qualified domain name) se componen por lo general del nombre del host, un nombre de dominio secundario y un nombre de dominio primario o de nivel máximo (top-level domain), que son secciones organizadas jerárquicamente.

Por ejemplo: 'www.ejemplo.com'. Leyéndolo de derecha a izquierda tenemos un dominio primario ('COM'), un dominio secundario ('EJEMPLO') y el nombre del host ('WWW'). Algunos dominios primarios son:

org	Organizaciones no lucrativas.
com	Organizaciones lucrativas.
net	Organizaciones en Internet.
gob	Agencias gubernamentales en latinoamérica.
mx	Sufijo de México.
es	Sufijo de España.

Existen cuatro tipos diferentes de servidores de resolución de nombres:

- **Master** (maestro o primario). Aloja los registros autoritarios de una zona, responde las peticiones de resolución de nombres como servidor de autoridad y delega copias a los servidores esclavo.
- **Slave** (esclavo o secundario). Responde a las peticiones de resolución de nombres como servidor de autoridad, pero la información es distribuida por los servidores primarios. Se considera que como medida de seguridad, se requiere al menos uno de estos, preferentemente independiente de la infraestructura del primario (red, energía eléctrica y ubicación geográfica).
- **Caching-only** (sólo de cache). Responde a las peticiones de resolución de nombres pero no es servidor de autoridad, las respuestas las guarda en memoria por un período determinado.
- **Forwarding** (de reenvío). Reenvía las peticiones a una lista de servidores de nombres.

Tipos de registros.

Para ofrecer suficiente flexibilidad en la configuración, se pueden declarar diversos tipos de registros,

que hacen referencia a la función del host. A continuación veremos los más importantes.

- **A** (Address). Es el registro más usado, que define una dirección IP y el nombre asignado al host. Generalmente existen varios en un dominio.
- **MX** (Mail eXchanger). Se usa para identificar servidores de correo, se pueden definir dos o más servidores de correo para un dominio, siendo que el orden implica su prioridad. Debe haber al menos uno para un dominio.
- **CNAME** (Canonical Name). Es un alias que se asigna a un host que tiene una dirección IP válida y que responde a diversos nombres. Pueden declararse varios para un host.
- **NS** (Name Server). Define los servidores de nombre principales de un dominio. Debe haber al menos uno y pueden declararse varios para un dominio.
- **SOA** (Start Of Authority). Este es el primer registro de la zona y sólo puede haber uno en cada archivo de la zona y sólo está presente si el servidor es autoritario del dominio. Especifica el servidor DNS primario del dominio, la cuenta de correo del administrador y tiempo de refresco de los servidores secundarios.

Configuración

Veamos como configurar BIND9 para disponer de un servidor DNS en una intranet, que resuelva dominios internos. Por ejemplo, en la intranet se utilizarán dominios que terminen en "marblestation.homeip.net" como "saturno.marblestation.homeip.net" o "luna.marblestation.homeip.net". El servidor DNS se encargará de resolver esos dominios en sus respectivas IPs, además de resolver otros dominios de Internet como "google.com".

Instalamos BIND9 y nos desplazamos a su directorio de configuración:

```
aptitude install bind9
cd /etc/bind/
```

Editamos named.conf.local y añadimos la zona "marblestation.homeip.net", haciendo referencia a su fichero de configuración:

```
zone "marblestation.homeip.net" {
    type master;
    file "/etc/bind/db.marblestation";
};
```

Creamos el fichero de configuración "db.marblestation" a partir de "db.local":

```
cp db.local db.marblestation
```

Editamos "db.marblestation", reemplazamos la palabra "localhost" por "marblestation.homeip.net", cambiamos la IP "127.0.0.1" por la que queramos asignar al dominio y añadimos al final del fichero todos los A, MX y CNAME que queramos, quedando:

```
;
; BIND data file for local loopback interface
;
$TTL      604800
@        IN      SOA  marblestation.homeip.net. root.marblestation.homeip.net. (
                                1          ; Serial
                                604800     ; Refresh
                                86400      ; Retry
                                2419200    ; Expire
                                604800 )   ; Negative Cache TTL
;
@        IN      NS   marblestation.homeip.net.
@        IN      A    192.168.48.32
@        IN      MX   0  marblestation.homeip.net.
www      IN      A    192.168.48.32
saturno  IN      CNAME marblestation.homeip.net.
```

En este ejemplo vemos primeramente el dominio a resolver, 'marblestation.homeip.net.' y el segundo es la cuenta de correo del administrador, 'root.marblestation.homeip.net.' (sustituyendo el primer punto por arroba, lo que dejaría 'root@marblestation.homeip.net'). Debemos notar que al final de cada dominio viene un punto, que identifica la raíz de este. El resto de los parámetros son:

- **Serial:** es un identificador del archivo, puede tener un valor arbitrario pero se recomienda que tenga la fecha con una estructura AAAA-MM-DD y un consecutivo.
- **Refresco:** número de segundos que un servidor de nombres secundario debe esperar para comprobar de nuevo los valores de un registro.
- **Reintentos:** número de segundos que un servidor de nombres secundario debe esperar después de un intento fallido de recuperación de datos del servidor primario.
- **Expiración:** número de segundos máximo que los servidores de nombre secundarios retendrán los valores antes de expirarlos.
- **TTL mínimo:** Significa Time To Live y es el número de segundos que los registros se mantienen activos en los servidores NS caché antes de volver a preguntar su valor real.

A continuación se definen los registros necesarios, cuyos tipos ya han sido explicados anteriormente en este documento.

Cada vez que se cambia la configuración de BIND9, debemos reiniciar el demonio:

```
/etc/init.d/bind9 restart
```

Para que nuestra máquina utilice el servidor de DNS que hemos configurado, debemos editar "/etc/resolv.conf" y dejamos únicamente la línea:

```
nameserver 127.0.0.1
```

Se debería hacer lo mismo con el resto de máquinas de la intranet que vayan a utilizar el servidor, con la única diferencia que habrá que substituir la IP 127.0.0.1 por la IP que tenga el servidor en la red.

Para comprobar el correcto funcionamiento, utilizamos el comando "host" el cual sirve para resolver dominios:

```
$ host marblestation.homeip.net
marblestation.homeip.net has address 192.168.48.32
marblestation.homeip.net mail is handled by 0 marblestation.homeip.net.
```

```
$ host saturno.marblestation.homeip.net
saturno.marblestation.homeip.net is an alias for marblestation.homeip.net.
marblestation.homeip.net has address 192.168.48.32
saturno.marblestation.homeip.net is an alias for marblestation.homeip.net.
saturno.marblestation.homeip.net is an alias for marblestation.homeip.net.
marblestation.homeip.net mail is handled by 0 marblestation.homeip.net.
```

Si deseamos también disponer de resolución de dominios inversa, es decir, que podamos preguntar por la IP "192.168.48.32" y el servidor DNS nos diga que pertenece a marblestation.homeip.net, debemos añadir a "/etc/bind/named.conf.local":

```
zone "192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.192";
};
```

Creamos el archivo de configuración "/etc/bind/db.192" a partir del "/etc/bind/db.127":

```
cd /etc/bind/
cp db.127 db.192
```

Editamos “/etc/bind/db.192”, sustituimos “localhost” por “marblestation.homeip.net” y cambiamos la última línea:

```
;
; BIND reverse data file for local loopback interface
;
$TTL      604800
@      IN      SOA  marblestation.homeip.net. root.marblestation.homeip.net. (
                1      ; Serial
                604800 ; Refresh
                86400  ; Retry
                2419200 ; Expire
                604800 ) ; Negative Cache TTL
;
@      IN      NS   marblestation.homeip.net.
32.48.168      IN  PTR marblestation.homeip.net.
```

De forma que, la última línea indica que la IP [192.]168.48.32 (escrita a la inversa y omitiendo el 192 que ya se especificó en “named.conf.local”) corresponde al dominio marblestation.homeip.net.

Podemos comprobar su funcionamiento reiniciando el demonio BIND9 y realizando una consulta:

```
$ /etc/init.d/bind9 restart
$ host 192.168.48.32
32.48.168.192.in-addr.arpa domain name pointer marblestation.homeip.net.
```

Autor: [Marble](#)