Configurando un DNS Cache Server

Autor: Sergio González D. **(sergio.gonzalez.duran@gmail.com)**

Un servidor DNS CACHE sirve para "cachar" las peticiones que los clientes de una red hacen a un servidor de nombres de dominio (DNS SERVER) que en la mayoría de los casos esta fuera de la propia LAN y que proporciona el proveedor de Internet (ISP - Internet Service Provider). Es decir, una red de 10, 20 o 30 equipos conectados a Internet a través de un servidor Linux por un lado y por la otra parte, una tarjeta de red esta conectado a un modem DSL como los del servicio de Telmex Infinitum en México; quien resuelve los nombres de dominio a su correspondiente IP, sería el DNS del proveedor, pero si implementamos un DNS Cache, entonces nuestro propio equipo Linux sería el que estaría resolviendo. Bueno, realmente va con el DNS del proveedor la primera vez o cuando necesita renovarse una dirección IP de un dominio, pero posteriormente el Cache server conserva esa IP y el siguiente usuario que solicite la página, el mismo servidor local Linux lo resolverá, sin necesidad de hacer el viaje hasta el proveedor, reduciendo enormemente los tiempos de consulta. Esa es mas o menos la idea de un DNS Cache. Y es bastante fácil implementarlo en Linux.

Para ejemplificar la enorme diferencia en tiempos de consulta, realizo un **`dig`** sin DNS cache server, usando los DNS de mi proveedor de Internet:

```
#> dig www.linuxtotal.com.mx
... se omiten varias líneas y solo se deja la última parte...

;; Query time: 76 msec
;; SERVER: 200.33.146.209#53(200.33.146.209)
;; WHEN: Wed Feb 20 19:31:16 2008
;; MSG SIZE  rcvd: 143
```

Ahora con el DNS Cache ya activado:

```
#> dig www.linuxtotal.com.mx
... se omiten varias líneas y solo se deja la última parte...

;; Query time: 1 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Wed Feb 20 19:35:21 2008
;; MSG SIZE  rcvd: 118
```

Nótese en la primera salida "Query Time: 76 msec", fue el tiempo que demoró resolver "linuxtotal.com.mx" a su correspondiente IP, en el segundo caso el tiempo fue de solo un milesegundo, también observa que el "SERVER: 127.0.0.1" fue el que me resolvió, es decir el equipo Linux localmente con su lista de DNS ya "cachada". Creo que con esto y tus propias pruebas que ya realizarás te convencerás de que vale la pena implementarlo. Veamos como.

Requisitos

Se requiere tener instalados los siguientes programas:

- **`bind`**: El servidor DNS, named.
- **`bind-utils`**: Utilerias complementarias para realizar consultas DNS (dig, host, entre otras).
- **`bind-libs`**: Librerías usadas por los dos programas previos.
- **`bind-chroot`**: Crea un subdirectorio especial donde se "enjaula" (chroot) bind, esto para más seguridad.
- **`caching-nameserver`**: Archivos de configuración para un servidor DNS Cache.

Puedes consultar si los tienes instalados con **`rpm`**:

```
#> rpm -qa | grep bind*
bind-utils-9.3.3-10.el5
bind-libs-9.3.3-10.el5
bind-9.3.3-10.el5
bind-chroot-9.3.3-10.el5
system-config-bind-4.0.3-2.el5.centos
#
# rpm -qa | grep caching-nameserver
caching-nameserver-9.3.3-10.el5
```

Si te faltara alguno y usas una distribución basada en **`yum`**, entonces usa:

```
# yum install bind
```

Para los que usan **`apt-get`**:

```
# apt-get install bind
```

O buscar los paquetes RPM en Internet, hay varios lugares como rpmfind.net desde donde puedes conseguirlos.

Configuración

La idea principal de un nameserver cache es realizar las consultas un servidor de nombres de dominio (tu proveedor de Internet) y cachar o guardar los resultados. Para realizar lo anterior modifiquemos el archivo de

configuración *named.conf*, ubicado en */var/named/chroot/etc*. Aunque es posible que solo encuentres dentro de este directorio el archivo llamado named.caching-nameserver.conf, que es el original, asi que basta que lo copies:

```
# cp named.caching-nameserver.conf named.conf
```

Este archivo de configuración lo dejaremos como esta y solo le agregaremos la dos siguientes en la sección de options:

```
  forwarders { 200.33.146.209; 200.33.146.217; };
  forward only;

...
  Asi debe de quedar:

  options {
        listen-on port 53 { 127.0.0.1; };
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        query-source    port 53;
        query-source-v6 port 53;
        allow-query     { localhost; };
        forwarders { 200.33.146.209; 200.33.146.217; };
        forward only;
  };
```

Con la línea *forwarders* estamos indicando los servidores DNS de nuestro proveedor de Internet (ISP), en este caso corresponden a los DNS de Prodigy Infinitum de Telmex México, si tienes otro servicio, localiza o pregunta a tu proveedor por sus direcciones IP de sus servidores DNS.

Con *forward only* se solicitan las peticiones no encontradas en el cache y en los DNS del proveedor, las solicitudes ya cachadas se resuelven automáticamente por el equipo Linux local.

Es conveniente verificar que el archivo *named.conf* no tenga errores, asi que puedes utilizar la herramienta **`named-checkconf`**:

```
# named-checkconf named.conf
```

Ahora hay que modificar el archivo de configuración de red que permite indicarle al sistema quien(es) es nuestro resolvedor de nombres de dominio. Actualiza el archivo */etc/resolv.conf* para que luzca como lo siguiente:

```
# vi /etc/resolv.conf

#nameserver 200.33.146.209
#nameserver 200.33.146.217
nameserver 127.0.0.1
```

Con esto indicamos que sea nuestro propio servidor DNS Cache el que resuleve las consultas de los usuarios

cuando accedan a un sitio. Solo comentamos las previamente establecidas (por si las necesitaras usar de nuevo) y agregamos 127.0.0.1 como nameserver, es decir, localhost. Asi que ahora solo resta iniciar el servicio:

```
# service named start
Iniciando named:   [  OK  ]
#

(Y lo agregamos a que arranque por defecto al inicio del sistema)
# chkconfig named on
(o indicar en un nivel de ejecución específico)
# chkconfig --level 5 named on

(más sobre la configuración de servicios) (index.php?cont=info_admon_003)
```

Un problema que pudieras tener es que cuando tu equipo se reinicie y la tarjeta que apunta hacía Internet esta en protocolo DHCP, entonces es posible que el archivo */etc/resolv.conf* vuelva a alterarse con los nameservers del proveedor, eliminando lo que habías hecho, para evitar lo anterior modifica el script de configuración de tu tarjeta de red, ubicado generalmente en */etc/sysconfig/network-scripts/* y en este directorio ubica el archivo de configuración de tu tarjeta de red, si fuera la eth0, entonces el archivo es *ifcfg-eth0*.

Agrega la siguiente línea al final de las que ya existen o simplemente verifica que ya exista y modifícala si fuera necesario. Con esto se logra que no se modifique */etc/resolv.conf*

```
PEERDNS=no
```

Firewall

Si tienes un firewall con políticas de DROP por defecto o que este bloqueando los puertos bien conocidos (1 al 1024), entonces necesitarás agregar una línea al firewall que permite recibir peticiones en el puerto 53, que es donde escucha (LISTEN) por default el servidor DNS. Esto es muy sencillo, tan solo agrega a tu script de firewall, la siguiente línea:

```
iptables -A INPUT -s 192.168.0.0/24 -p udp --dport 53 -j ACCEPT
```

Sustituye la red (192.168.0.0) por la tuya y listo.

Clientes

La configuración de los clientes puede variar demasiado, porque quizás ya tienes un servidor Proxy Squid corriendo en el mismo equipo Linux, asi que no habría que hacer nada con los clientes, si no es asi, entonces tendrás que cambiar su configuración de red para que el DNS principal apunte a la IP de tu servidor Linux del lado de la LAN.

Por último, puedes realizar una prueba similar a la mostrada al inicio del artículo, para que compruebes tu mismo en cuanto bajo el "Query time". Tan solo cambia quien quieres que te resuelva en el archivo */etc/resolv.conf*.

¿Requieres de una instalación o configuración de Linux o sus servicios?
¿Un desarrollo WEB empresarial a la medida?
¿Un curso o capacitación a la medida?
Revisa el sitio de SERVICIOS (index.php?cont=servicios) de LinuxTotal

---

info@linuxtotal.com.mx · linuxtotal.com.mx@gmail.com