Índice de contenido

Información de Derechos reservados de esta publicación.

Reconocimiento-NoComercial-CompartirIgual 2.1

Usted es libre de:

- Copiar, Distribuir y Comunicar públicamente la obra

Bajo las condiciones siguientes:

Reconocimiento. Debe reconocer y citar al autor original.

No comercial. No puede utilizar esta obra para fines comerciales.

Compartir bajo la misma licencia. Si altera o transforma esta obra, o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta.

- Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra.

- Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor

Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior.

Reconocimiento-NoComercial-CompartirIgual 2.1

Autor del manual: Javier Eduardo Duarte

Tema 8. Servidor DNS

8.1 Acerca de DNS

En la mayoría de las redes modernas, incluyendo la Internet, los usuarios localizan paginas web por su nombre de dominio *(ej. www.google.com)*,esto permite al usuario acceder a las millones de paginas web de la Internet sin necesidad de recordar todas y cada una de las direcciones IP asociadas al nombre de la pagina que desea visitar.

Una forma de solucionar este problema es mediante la complementación de un mecanismo que al momento que un usuario pregunte por el nombre de una pagina web este servidor conozca que dirección IP le corresponde al sitio web por el cual pregunta el usuario. El mecanismo del cual hablamos es un servidor de nombres mayormente conocido como servidor DNS (Domain Name Server)

Así mismo un servidor DNS tiene la función de almacenar la información asociada a los nombres de dominio existentes por los cuales el usuario pregunta, por ejemplo:

- www.linuxparatodos.net
- www.gmail.com
- www.yahoo.com

Por lo tanto el servidor DNS es capaz de asociar distintos tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio. Cuando un equipo cliente solicita información desde un servidor de nombres, usualmente se conecta al puerto 53

Falsamente se asocia a un DNS con una base de datos, cosa que es totalmente falso,pues los principios fundamentales de las bases de datos especifican que no pueden contener datos redundantes es decir, los datos no pueden ser la misma información la cual es almacenada varias veces en la misma base de datos

El mapeo de nombres a direcciones IP es ciertamente la función más conocida de los servidores DNS. Por ejemplo, si la dirección IP del sitio www.linuxparatodos.net es 254.192.169.20, la mayoría de la gente para acceder a ella teclea en un navegador web la dirección web *www.linuxparatodos.net* y no la dirección IP.

La institución encargada de asignar nombres de dominios en Internet es conocida como NIC (acrónimo de Network Information Center o Centro de Información sobre la Red) esta institución es la encargada de asignar los nombres de dominio en Internet, ya sean nombres de dominio genéricos o por países, permitiendo personas o empresas montar sitios de Internet mediante a través de un ISP mediante un DNS. Técnicamente existe un NIC por cada país en el mundo y cada uno de éstos es responsable por todos los dominios con la terminación correspondiente a su país. Por ejemplo: NIC México es la entidad encargada de gestionar todos los dominios con terminación .mx, la cual es la terminación correspondiente asignada a los dominios de México.

FQDN (acrónimo de Fully Qualified Domain Name o Nombre de Dominio Plenamente Calificado) es un Nombre de Dominio ambiguo que especifica la posición absoluta del nodo en el árbol jerárquico del DNS. Se distingue de un nombre regular porque lleva un punto al final.

Ejemplos:
www.hotmail.com
www.google.com

8.2 Componentes de un DNS

Un DNS se compone de tres componentes básicos, los cuales son:

- Cliente DNS
- Servidor DNS
- Zonas de Autoridad

8.2.1 Cliente DNS

Cuando hablamos del cliente DNS nos referimos al host o usuario que hace la petición; o sea, a la computadora del usuario la cual genera la petición al DNS preguntando por el nombre de algún dominio existente en internet.

8.2.2 Servidor DNS

Existen 3 tipos de servidores básicos de un DNS los cuales son:

- Servidor Maestro
- Servidor Esclavo
- Servidor de Cache

8.2.2.1 Servidor Primario o Maestro

Un servidor DNS maestro almacena los registros de las zonas originales y de autoridad. Ademas el servidor DNS maestro es el encargado de responder a las peticiones hechas por otros servidores DNS

8.2.2.2 Servidor Secundario o Esclavo

Un servidor DNS esclavo también tiene la capacidad de responder a las peticiones hechas por un Cliente DNS así como otro servidor de DNS, la diferencia radica en que los servidores esclavos obtienen la información acerca de los nombres de dominio desde los servidores maestros

8.2.2.3 Servidor De Cache

Este ofrece servicios de resolución de nombres como respuesta a las peticiones hechas por los clientes de dns, dichos servicios de resolución de nombres son guardados cierto espacio de tiempo para poder acceder a dicha información mas rápidamente.

Este tipo de servidores no tiene ninguna autoridad sobre las zonas de autoridad.

Los servidores DNS son los encargados de hacer las consultas producto de las peticiones solicitadas por los clientes DNS. Para ello el servidor DNS hace uso de 2 tipos de consultas

- Consultas Iterativas
- Consultas Recursivas

8.2.2.3.1 Consultas Recursiva

Una consulta iterativa funciona de la siguiente manera:

Imagine que tenemos un cliente DNS el cual hace la petición a nuestro servidor dns-1 sobre el dominio ***"***www.ejemplo.com***",*** nuestro servidor dns-1 no sabe quien es ***"***www.ejemplo.com***"*** pero el conoce quien puede tener ese dominio por lo que ahora dns-1 le hace la petición a dns-2, dns-2 le responde a dns-1 que no sabe quien es "www.ejemplo.com" pero el sabe quien puede tener ese dominio registrado, por lo que ahora dns-2 le hace la petición a dns-3, dns-3 responde la petición hecha por dns-2 contestando que el si conoce quien es "www.ejemplo.com" por lo que dns-3 enviá la dirección IP asociada a "www.ejemplo.com" a dns-2, dns-2 le responde la petición a dns1 y dns-1 a su vez le responde a el cliente DNS.

8.2.2.3.2 Consultas Iterativas

Una consulta recursiva funciona de la siguiente manera:

Imagine que tenemos un cliente DNS el cual hace la petición a nuestro servidor dns-1 sobre el dominio “www.ejemplo.com”, nuestro servidor dns-1 no sabe quien es “www.ejemplo.com” pero el conoce quien puede tener ese dominio por lo que dns-1 le responde al Cliente DNS que le pregunte al dns-2, dns-2 no sabe quien es “www.ejemplo.com” pero el conoce quien puede tener ese dominio por lo que dns-2 le responde al Cliente DNS que le pregunte al dns-3, dns-3 sabe quien es “www.ejemplo.com” por lo que dns-3 responde a la petición hecha por el Cliente DNS devolviendo la IP que le corresponde a “www.ejemplo.com” .

8.2.2.3.3 Diferencias entre las Consultas Iterativas contra las Consultas Recursivas

Las diferencias entre las consultas iterativas contras las recursivas son:

- Cuando se hacen consultas iterativas quien asume toda la carga es nuestro cliente DNS (nuestra maquina)
- Cuando se hacen consultas recursivas quien asume toda la carga es el servidor DNS pues el es el encargado de proporcionar una respuesta completa a la petición hecha por el Cliente dns

Conociendo esta información se puede concluir que las consultas recursivas son mejores que las consultas iterativas, debido a que las consultas recursivas liberan a nuestro cliente DNS (nuestra maquina) de la tarea de responder las peticiones solicitadas por el mismo, haciendo que toda la carga la asuma el servidor DNS.

8.2.3 Zonas de Autoridad

Las zonas de autoridad contienen las características sobre las cuales nuestro dominio actuara, en ella se configuran los aspectos importantes así como las opciones especificas de cada zona, estas configuraciones hechas a las zonas son cargadas desde el servidor maestro.

La información de cada Zona de Autoridad es almacenada de forma local en un fichero en el Servidor DNS. Este fichero puede incluir varios tipos de registros como pueden ser:

CNAME	**Canonical Name – (Nombre Canónico) Se usa para crear nombres de hosts adicionales, o alias, para los hosts de un dominio.**
A	**Address – (Dirección) Este registro se usa para traducir nombres de hosts a direcciones IP.**
NS	**Name Server – (Servidor de Nombres) Define la asociación que existe entre un nombre de dominio y los servidores de nombres que almacenan la información de dicho dominio. Cada dominio se puede asociar a una cantidad cualquiera de servidores de nombres.**
MX	**Mail Exchange – (Intercambiador de Correo) Define el lugar donde se aloja el correo que recibe el dominio.**
PTR	**Pointer – (Indicador) También conocido como 'registro inverso', funciona a la inversa del registro A, traduciendo IPs en nombres de dominio.**
SOA	**Start of authority – (Autoridad de la zona) Proporciona información sobre la zona.**

HINFO	Host Information – (Información del sistema informático) Descripción del host, permite que la gente conozca el tipo de máquina y sistema operativo al que corresponde un dominio.
TXT	Text - (Información textual) Permite a los dominios identificarse de modos arbitrarios.
LOC	Localización - Permite indicar las coordenadas del dominio.
WKS	Generalización del registro MX para indicar los servicios que ofrece el dominio. Obsoleto en favor de SRV.
SRV	Servicios - Permite indicar los servicios que ofrece el dominio.

8.3 Sobre BIND (Berkeley Internet Name Server)

BIND es el servidor DNS mas comúnmente implementado en Sistemas Operativos Linux, y actualmente el mas usando en Internet.

Originalmente BIND nació a principios de los años 80 bajo el patrocinio de DARPA (Agencia de Investigación de Proyectos Avanzados de Defensa) agencia del Departamento de Defensa de los Estados Unidos, el cual fue desarrollado en la Universidad de California, Berkeley por cuatro estudiantes. A mediados de los años 80 su desarrollo paso a manos de los empleados de DEC (Digital Equipment Corporation, compañía que mas tarde seria adquirida por Compaq y esta a su vez comprada por HP)

Paul Vixie,empleado de DEC continuó trabajando en BIND luego de desvincularse de DEC. Más adelante ayudaría a fundar la ISC (Internet Systems Consortium), la cual se convirtió en la responsable del mantenimiento de BIND.

El desarrollo de BIND 9 fue realizado con el auspicio conjunto del área comercial y militar. La mayoría de las funcionalidades de BIND 9 fueron impulsadas por proveedores de UNIX quienes querían asegurar que BIND se mantuviera competente con la oferta de Microsoft en el sector de soluciones DNS.

La versión mas actual de BIND, en particular la versión 9.0 fue reescrita desde cero, esto con el fin de reparar algunas de sus funcionalidades arquitectónicas de la misma (problemas en la programación de Bajo Nivel) que agrega características importantes como: TSIG, notificación DNS, nsupdate, IPv6, rndc flush, vistas, procesamiento en paralelo, y una arquitectura mejorada en cuanto a portabilidad.

8.4 Proceso de instalación del servidor DNS

La instalación de un servidor DNS requiere de los siguientes paquetes

```
[BASH]# yum install -y bind bind-chroot bind-libs \
> bind-utils caching-nameserver
```

Recuerde que este comando se debe ejecutar como root

8.4.1 Configuraciones previas que debe tener el servidor DNS

8.4.1.1 Configurando el fichero /etc/hosts

A este fichero deberemos agregar el nombre del equipo que desempeñara la función de servidor DNS asi como la dirección IP asignada a este equipo, al final este fichero deberá verse de una forma similar a esta.

```
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1          localhost.localdomain localhost
192.168.1.10       dns1.tuDominio.com  dns1
::1             localhost6.localdomain6 localhost6
```

Como ejemplo nosotros asignaremos al servidor DNS la dirección IP **192.168.1.10**, usted deberá adecuar esta dirección IP según sea su caso.

8.4.1.2 Configurando el fichero /etc/sysconfig/network

A este fichero deberemos agregar igualmente el nombre del equipo que desempeñara la función de servidor DNS, al final este fichero deberá verse de una forma similar a esta.

```
NETWORKING=yes
NETWORKING_IPV6=no
HOSTNAME=dns1.tuDominio.com
```

8.4.1.3 Configurando el fichero /etc/sysconfig/network-scripts/ifcfg-eth[N]

A este fichero deberemos agregar igualmente el nombre del equipo que desempeñara la función de servidor DNS, al final este fichero deberá verse de una forma similar a esta.

NOTA: La letra [N] indica el numero de la tarjeta de red sobre la cual escucha el DNS

```
# nVidia Corporation MCP61 Ethernet
DEVICE=eth0
BOOTPROTO=dhcp
HWADDR=00:E0:4D:3F:C3:39
ONBOOT=yes
DHCP_HOSTNAME=dns1.tuDominio.com
```

8.4.2 Ficheros de configuración del servidor DNS

La configuración del servidor DNS dependerá en gran medida de los siguientes ficheros.

/var/named/chroot/etc	En esta ruta se deberá crear el fichero "named.conf"
/var/named/chroot/var/named	En esta ruta se crearan los ficheros de zona que serán invocados por named.conf

8.4.2.1 Creación de los ficheros de zona

Procederemos con la creación de nuestras zonas de dominio, para ello teclearemos en terminal lo siguiente:

```
[BASH]# touch /var/named/chroot/var/named/tuDominio.com.zone

[BASH]# touch /var/named/chroot/var/named/1.168.192.in-addr-arpa.zone
```

Lo que hicimos fue crear dos ficheros vacíos a los cuales nombramos

```
tuDominio.com.zone
```

y

```
1.168.192.in-addr-arpa.zone
```

El siguiente paso ahora sera añadir las instrucciones para que puedan ser identificados como ficheros de zona y que a su vez puedan ser invocados por **"named.conf"**

8.4.2.1.1 Editando el fichero "tuDominio.com.zone"

El siguiente paso sera editar el fichero **"tuDominio.com.zone**" al cual deberemos añadir el siguiente contenido.

```
[BASH]# vi /var/named/chroot/var/named/tuDominio.com.zone
------------------------------------------------------------------------
$TTL    86400
@       IN      SOA     dns1.tuDominio.com.com. admin.tuDominio.com. (
                2008061001; Numero de Serie
                28800; Tiempo de Refresco
                7200; Tiempo de Reintentos
                604800; Expiracion
                86400; Tiempo Total de Vida
                )
@       IN      NS      dns1
@       IN      MX      10      correo
@       IN      A       192.168.1.10
dns1    IN      A       192.168.1.10
correo  IN      A       192.168.1.11
```

Los parámetros mas importantes del fichero anterior son descritos en la siguiente tabla

dns1	La palabra dns1 se refiere al nombre del equipo que fungirá como servidor DNS, es este caso hacemos el supuesto que nuestro equipo tiene asignada la dirección IP 192.168.1.10
admin	El nombre admin corresponde al usuario que administrara el servidor DNS.

tuDominio.com	Éste es nuestro dominio referencial con el que estamos trabajando,otros ejemplos de dominio son: *linuxparatodos.net *gmail.com
PUNTO AL FINAL	Recuerde no olvidar poner el punto al final de las sentencias: dns1.tuDominio.com. <---------- root.tuDominio.com. <----------
correo	Estamos haciendo el supuesto que ademas de un DNS contamos con un servidor de correo electrónico al cual hemos asignado la dirección Ip 192.168.1.11
NS (Name Server)	Asigna Nombre al DNS
MX (Mail Exchanger)	Registro de Mail Exchange, el cual indica a dónde debe ser dirigido el correo
A (Address)	Registro de dirección que especifica una dirección IP que se debe asignar a un nombre
SOA (Start of Authority)	Registro de recursos que declara información importante de autoridad relacionada con espacios de nombres al servidor de nombres

8.4.2.1.2 Editando el fichero "1.168.192.in-addr.arpa.zone"

A este fichero deberemos añadir el siguiente contenido.

```
[BASH]# vi /var/named/chroot/var/named/ 1.168.192.in-addr.arpa.zone
-------------------------------------------------------------------------
$TTL    86400
@       IN      SOA     dns1.tuDominio.com. root.tuDominio.com. (
                2008061002; Numero de Serie
                28800; Tiempo de Refresco
                7200; Tiempo de Reintentos
                604800; Expiracion
                86400; Tiempo Total de Vida
                )
@       IN      NS      dns1.tuDominio.com.
10      IN      PTR     dns1.tuDominio.com.
```

El numero **[10]** hace referencia al ultimo octeto de la dirección IP asignada a nuestro DNS, nos referimos a la dirección IP **192.168.1.10.**

Por ejemplo si la dirección IP del servidor DNS fuera la 254.168.1.25, el numero que debiera ir colocado en la parte inferior de su izquierda debiera ser el numero [**25]**

Ejemplo:

```
25      IN      PTR     dns1.tuDominio.com.
```

8.4.2.2 Creación y configuración del fichero “named.conf”

Abra una terminal y genere el fichero **“named.conf”** dentro de la ruta **“/var/named/chroot/etc/”**

```
[BASH]# touch /var/named/chroot/etc/named.conf
```

Una vez creado asegúrese de agregarle los siguientes propietarios

```
[BASH]# chown root:named named.conf
```

Al terminar solo deberá añadir al fichero el siguiente contenido

```
[BASH]# vi named.conf
---------------------------------------------------------------------
options {
       directory "/var/named/";
       dump-file "/var/named/data/cache_dump.db";
       statistics-file "/var/named/data/named_stats.txt";
       allow-recursion {
              127.0.0.1;
              192.168.1.0/24;
       };
       forwarders {
              200.33.146.209;
              200.33.146.217;
       };
       forward first;
};
zone "." {
       type hint;
       file "named.ca";
};
zone "localhost" {
       type master;
       file "localhost.zone";
       allow-update { none; };
};
zone "tuDominio.com" {
       type master;
       file "tuDominio.com.zone";
       allow-update { none; };
};
zone "1.168.192.in-addr.arpa" {
       type master;
       file "1.1.192.in-addr.arpa.zone";
       allow-update { none; };
};
```

Los parámetros mas importantes del fichero anterior son descritos en la siguiente tabla

zone	Define las características de una zona, tal como la ubicación de su archivo de configuración y opciones especificas de la zona.
"tuDominio.com"	Aquí debe ir el nombre de nuestro dominio
file "tuDominio.com.zone";	Contiene los ficheros de configuración de tus zonas de tu dominio.
allow-update{ none; };	Especifica los host que están autorizados para actualizar dinamicamente la información en sus zonas. Por defecto, no se autoriza la actualización dinámica de la información. Esto se logra añadiendo la palabra none.
"1.168.192.in-addr.arpa"	IP de resolución inversa. En este caso estamos usando nuestra IP referencial 192.168.1.10
type master;	Designa el servidor de nombres actual como el servidor autoritario para esa zona
file "1.168.192.in-addr.arpa.zone";	Contiene los ficheros de configuración de tus zonas de tu dominio.

8.5 Iniciar , detener o reiniciar el servidor DNS

Para iniciar el servidor FTP por primera vez solo deberá teclear en terminal el siguiente comando:

```
[root@ localhost ~]# /etc/init.d/named start
```

Igualmente existen opciones ya sea para reiniciar, detener, recargar o conocer el status en el que se encuentra el servidor DNS. Estas opciones pueden ser consultadas en la siguiente tabla:

start	Inicia el servicio
stop	Detiene el servicio
restart	Reinicia el servicio.-La diferencia con reload radica en que al ejecutar un restart este mata todos los procesos relacionado con el servicio y los vuelve a generar de nueva cuenta
reload	Recarga el servicio.-La diferencia con restart radica en que al ejecutar un reload este solamente carga las actualizaciones hechas al fichero de configuración del servicio sin necesidad de matar los procesos relacionados con el mismo, por lo que podría entenderse que hace el cambio en caliente.
condrestart	Reinicio Condicional.- Solamente se inicia si el servicio se encuentra ejecutándose.
status	Da a conocer el estado en el que se encuentra el servicio

Como alternativa también podemos ocupar el siguiente comando para iniciar el servidor FTP

```
[root@ localhost ~]# service named start
```

Y de igual manera podemos usar las opciones antes descritas en la tabla anterior.

Recuerde que estos comandos se ejecutan como root.

Para verificar que bind esta cargando las zonas, deberemos ejecutar el siguiente comando

```
[BASH]#tail -80 /var/log/messages | grep named
```

8.6 Etapa de Pruebas

Compruebe que el dominio resuelve correctamente ejecutando los siguientes comandos:

```
[BASH]# host tuDominio.com 192.168.1.10
[BASH]# dig @192.168.1.10 tuDominio.com
[BASH]# dig @192.168.1.10 tuDominio.com MX
```

Al ejecutar el comando **"dig @192.168.1.10 tuDominio.com MX"** deberíamos observar lo siguiente:

```
[BASH]# dig @192.168.1.10 tuDominio.com MX
; <<>> DiG 9.5.0rc1 <<>> @192.168.1.10 tuDominio MX
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32324
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
; tuDominio.com.           IN      MX

;; ANSWER SECTION:
tuDominio.com.     86400   IN      MX      10 mail. tuDominio.com.

;; AUTHORITY SECTION:
tuDominio.com.     86400   IN      NS      dns1.tuDominio.com.

;; ADDITIONAL SECTION:
tuDominio.com. 86400 IN A      192.168.1.10

;; Query time: 1 msec
;; SERVER: 192.168.1.117#53(192.168.1.10)
;; WHEN: Thu Jun 12 17:39:33 2008
;; MSG SIZE  rcvd: 99
```

8.7 Errores Comunes

No olvide desactivar el Firewall del servidor DNS, de otro modo nuestras peticiones al DNS serán rebotadas