Índice de contenido

Información de derechos reservados de esta publicación.

Autor del manual: Rodrigo Mendoza Martinez

TEMA 11. SERVICIO DNS

11.0 Servidor DNS.

El servicio DNS “Domain Name System”, se utiliza para traducir un nombre de dominio en direcciones IP.

DNS permite ya una vez configurado que tu sitio WEB y Correo sean localizados desde cualquier parte de la WWW.

Los DNS se utilizan para distintos propósitos:

- **Resolución de nombres.**
- **Resolución inversa de direcciones.**
- **Resolución de servidores de correo**.

Existen varios tipos de servidores de DNS como Bind, PowerDNS, djbdns y todos trabajan sobre el puerto 53 protocolo TCP/UDP.

11.1 Tipos de DNS

Existen 4 tipos de servidores DNS:

- **Maestro:** Nuestro servidor se comportara como un autentico servidor DNS, ya que atenderá las peticiones de resolución de nombres. Así mismo responde a consultas de otro servidores DNS.
- **Esclavo:** Este tipo de servidor solamente sirve como espejo de un servidor DNS Maestro, cuando el servidor DNS Maestro tiene alguna modificación, se vera reflejado en servidor DNS esclavo ya que están sincronizados.
- **Cache:** Este tipo de servidor se utilizan dentro de una red local, cuando hace una consulta a un servidor DNS Cache y no contiene la resolución envía una petición a un DNS Maestro y la resolución quedara guardada en la cache del DNS local hasta que expire el tiempo de vida.
- **Reenvío:** Reenvía las peticiones a una lista especifica de servidores DNS para la resolución de nombres.

Un servidor DNS puede ser de varios tipos configurados en el mismo servidor DNS.

11.2 Servidor Bind

Bind (Berkeley Internet Name Domain), es el servidor de DNS mas utilizado en el internet, fue escrito en los años 80 bajo el patrocinio de la DARPA.

Actualmente se encuentra nos encontramos en la versión 9 del BIND, la cual fue escrita desde cero para poder superar las dificultades de las diferentes plataformas.

11.2.1 Instalación de Bind.

Para poder hacer la instalación de Bind ejecutamos el siguiente comando:

```
root@server1:~# apt-get install bind9
```

Al terminar de instalar toda la configuración de bind estará dentro de:

```
/etc/bin
```

Pero tendremos que modificar esta configuración para tener un DNS chroot.

11.3 DNS chroot.

Es recomendable ejecutar el servicio de DNS en un entorno aislado o enjaulado, para que el servicio DNS no se comprometido hacia un ataque y esto pueda afectar al resto de los servicios disponibles o al sistema operativo.

11.3.1 Configuración de DNS chroot.

A partir de este momento comenzáramos la configuración de DNS chroot.

11.3.1.1 Detener servicios.

Tenemos que detener nuestro servicio de DNS.

```
root@server1:~# /etc/init.d/bind9 stop
 * Stopping domain name service... bind           [ OK ]
root@server1:~#
```

Ahora detendremos el servicio apparmor el cual es el encargado de la seguridad de nuestro sistema.

```
root@server1:~# /etc/init.d/apparmor stop
Unloading AppArmor profiles : done.
root@server1:etc#
```

11.3.1.2 Modo de ejecución.

En este paso configuremos el archivo /etc/default/bind9, el cual espeficaremos que usuario va ejecutar el servicio de bind y en donde se encuentra ubicado.

Para eso tendremos que usar nuestro editar de texto:

```
root@server1:~# vim /etc/default/bind9
```

Dentro de este archivo tendremos agregar o modificar los siguientes parámetro de OPTIONS.

```
OPTIONS="-u bind"
por
OPTIONS="-u bind -t /var/lib/named"
```

11.3.1.3 Creando el árbol chroot.

Tendremos que crear el árbol de directorios de chroot.

```
root@server1:~# mkdir -p /var/lib/named/etc
root@server1:~# mkdir /var/lib/named/dev
root@server1:~# mkdir -p /var/lib/named/var/cache/bind
root@server1:~# mkdir -p /var/lib/named/var/run/bind/run
```

11.3.1.4 Moviendo configuración bind al chroot.

Lo procederemos hacer es mover toda la configuración del servicio bind dentro de **/etc/bind** a **/var/lib/named/etc** para poder utilizar el chroot.

```
root@server1:~# mv /etc/bind /var/lib/named/etc
```

11.3.1.5 Creando enlaces chroot.

Deberemos crear un enlace simbólico de **/etc/bind** a **/var/lib/named/etc/bind**.

```
root@server1:~# ln -s /var/lib/named/etc/bind /etc/bind
```

11.3.1.6 Dispositivos chroot.

Crearemos los dispositivos null y random, dentro del chroot y cambiaremos los permisos de los mismos de modo de Lectura/escritura para todos.

```
root@server1:~# mknod /var/lib/named/dev/null c 1 3
root@server1:~# mknod /var/lib/named/dev/random c 1 8
root@server1:~# chmod 666 /var/lib/named/dev/null
root@server1:~# chmod 666 /var/lib/named/dev/random
```

11.3.1.7 Dueño en árbol chroot.

Solamente cambiaremos quien sera el encargado del arbol de chroot.

```
root@server1:~# chown -R bind:bind /var/lib/named/var/*
root@server1:~# chown -R bind:bind /var/lib/named/etc/bind
```

11.3.1.8 Configuración de syslogd.

Necesitamos modificar el archivo de configuración de syslogd, para poder tener el registro de los logs de nuestro servicio de DNS.

```
root@server1:~# vim /etc/default/syslogd
```

Tendremos que buscar el parámetro SYSLOGD, el cual no contiene ninguna información tendremos que agregarle lo siguiente.

```
SYSLOGD=""
SYSLOGD="-a /var/lib/named/dev/log"
```

11.3.1.9 Configuración de apparmor.

Tendremos que modificar y agregar algunas opciones dentro del archivo de configuración para poder agregar las rutas de servidor DNS.

```
root@server1:~# vim /etc/apparmor.d/usr.sbin.named
```

Ya estando ahí tendremos que modificarlo.

```
#### Agregado por el Administrador
#### indicamos el path del servidor DNS.
  /var/lib/named/etc/bind/* rw,
#####
  /etc/bind/** r,
  /var/lib/bind/** rw,
  /var/lib/bind/ rw,
  /var/cache/bind/** rw,
  /var/cache/bind/ rw,
####Agregado/modificar por Administrador
#### comentamos la linea por defualt y agregamos la nuestra
#### de la ubicación del pid del DNS
  /var/lib/named/var/run/bind/run/named.pid w,
  # /var/run/bind/run/named.pid w,
############
  # support for resolvconf
#### Agregado/modificar por Administrador
#### Comentada la linea por default y agregando la ruta
#### en donde se encuentra el archivo opciones de Bind.
```

```
  #/var/run/bind/named.options r,
  /var/lib/named/var/run/bind/named.options r,
#####
#### Agregado por el Administrador
#### Agregamos lineas para dispositivos chroot.
  /var/lib/named/dev/null rw,
  /var/lib/named/dev/random rw,
###  Agregamos las zonas de dominio
  /var/lib/named/etc/bind/zones/* rw,
#####
```

Guardamos los cambios realizados.

11.3.1.10 Inicio/Reinicio de los servicios.

Primero tendremos que reiniciar sysklogd.

```
root@server1:~# /etc/init.d/sysklogd restart
```

Después iniciamos el apparmor.

```
root@server1:~# /etc/init.d/apparmor restart
```

Por ultimo iniciamos bind9.

```
root@server1:~# /etc/init.d/bind9 start
```

Con esto ya tendremos configurado nuestro DNS Chroot.

11.4 Zonas DNS.

En las zonas DNS es donde configuramos todos los dominios que vaya a tener nuestro servidor, se debe crear archivo por archivo por cada dominio que se tenga.

Esta configuración deberá ser guardada en:

```
/etc/bind/zones
```

Tenemos que crear el archivo de configuración del domino que se agregar a nuestro DNS.

```
root@server1:zones# touch ascariote.net.db
```

El siguiente archivo a crear debe contener los 3 primero segmentos de nuestra red, ejemplo nuestra red es 192.168.1.0, ya este archivo es de tipo resolucion inversa quedaria de la siguiente manera 1.168.192.in-addr.arpa.

```
root@server1:zones# touch 1.168.192.in-addr.arpa
```

11.4.1 Tipos de registro de zonas.

En la configuración de los archivos de zonas se dividen por columnas de datos y separadas por espacios, que definen todos los registros del recurso de la zona asociada.

A continuación le mostramos los tipos de registros más frecuentes:

Tipo de registro.	Descripción.
A	Registro de dirección IP que se le asigna un nombre.
AAAA	Registro de dirección Ipv6 que se le asigna un nombre, en este caso también se puede ocupar el tipo de registro A6.
CNAME	Registro del nombre canónico que dice al servidor de nombres que otros nombres son conocidos hacia un registro. Permite la creación de nombre alias hacia nombre de dominio.
MX	Registro de servidor de correo electrónico, que indica a donde se tiene que dirigir el correo.
PTR	Registro sirven sobre todo para la resolución inversa de nombre se orienta a través de la direcciones IP
NS	Registro de servidor de nombres que permite definir una lista de nombres con autoridad a un dominio.
SOA	Registro que proclama información importante sobre la autoridad de determinados servidores sobre determinados espacios de nombres. Este registro contiene la datos de correo electrónico, números de serie y parámetro de expiración.
TXT	Registro de texto que permite al administrador insertar texto arbitrariamente en un registro DNS.

11.4.2 Tiempos de expiración zonas.

Dentro de la configuración de los dominios tendremos que configurar los tiempos de expiración de la zonas, la información debe estar en segundos, pero también existen otros valores que nos permiten configurar nuestros tiempos.

Segundos.	Unidades.	Descripción.
60	**1M**	A un minuto.
1800	**30M**	A 30 minutos
3600	**1H**	Una hora.
10800	**3H**	3 horas.
21600	**6H**	6 horas.
43200	**12H**	12 horas.
86400	**1D**	Un dia.
259200	**3D**	3 dias.
604800	**1W**	Una semana.

11.4.3 Configurar el archivo zona.

Editaremos el archivo de configuración de nuestro dominio.

```
root@server1:zones# vim ascariote.net.db
```

Agregaremos las siguientes opciones.

```
$TTL    1W
@       IN      SOA     ascariote.net. admin.ascariote.net. (
                        2       ; Serial Number
                        1W      ; Time To Refresh
                        1D      ; Time To Retry
                        28D     ; Time To Expire
                        1W )    ; Negative Cache TTL
;
@       IN      NS      ascariote.net.
@       IN      A       192.168.1.243
```

```
@       IN      MX      10      ascariote.net
www     IN      A       192.168.1.243
```

Ahora explicaremos:

- Todo lo que esta después de un punto y coma (;) es comentario.
- **$TTL 1W:** directiva obligatoria que indica el tiempo de vida de la información contenida en la BDs.
- **@ IN SOA ascariote.net. admin.ascariote.net. (** : el dominio ascariote.net se encuentra en la maquina ascariote.net y el encargado del dominio es admin.ascariote.net.
- **2 ;Serial Number:**Es un numero que se incrementa por cada vez que sea modificado el archivo.
- **1W ; Time To Refresh:** indica a los servidores eslavos cuanto tiempo deben esperar antes de preguntar a su servidor primario si se ha hecho algún cambio.
- **1D ; Time to Retry :** Indica el tiempo de espera para reintentar conectarse a nuestro servidor DNS.
- **28D ; Time To Expire :** Tiempo que no hubo comunicación con el servidor DNS, toda la informacion del primero se vuelve inservible y deja de responder peticiones.
- **1W); Negative Cache TTL:** indica el tiempo de los DNS almacenados en cache.
- **@ IN NS ascariote.net:** Especificamos en donde se encontrara el servidor DNS.
- **@ IN A 192.168.1.243:** Especificamos la IP del servidor DNS.
- **@ IN MX 10 ascariote.net:** Indicamos que se utiliza como servidor de correo con prioridad máxima 10.
- **www IN A 192.168.1.243 :** Indicamos que el servidor web se encuentra en la dirección IP.

11.4.4 Configurar el archivo zona inversa.

Editaremos el archivo de configuración zona inversa.

```
root@server1:zones# vim 1.168.192.in-addr.arpa
```

Y agregaremos los siguientes parámetros:

```
$TTL    1W
@       IN      SOA     ascariote.net. admin.ascariote.net. (
                              2         ; Serial Number
                             1W         ; Time To Refresh
                             1D         ; Time To Retry
                            28D         ; Time To Expire
                             1W )       ; Negative Cache TTL
;
```

```
@       IN      NS      ascariote.net.
243.1.168       IN      PTR     ascariote.net.
```

Como pueden ver casi tiene la misma configuración que el archivo de las zonas a excepción de un parámetro.

- **243.1.168 IN PTR ascariote.net. :** Enlazamos la IP con el nombre del servidor,para la resolución inversa.

11.4.5 Configurar named.conf.

Es el archivo de configuración de nuestro servidor DNS, dentro de el tendremos que agregar algunos parámetros para que mande a llamar los archivos que hemos creados.

```
root@server1:zones# vim /etc/bind/named.conf
```

Agregaremos algunos parámetros casi al final del archivo y antes del include.

```
zone "255.in-addr.arpa" {
        type master;
        file "/etc/bind/db.255";
};
########################################
#### Agregado por el Administrador #####
########################################
zone "ascariote.net" {
        type master;
        file "/etc/bind/zones/ascariote.net.db";
};
zone "1.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/zones/1.168.192.in-addr.arpa";
};
########################################

include "/etc/bind/named.conf.local";
```

Solamente agregamos la zona ascariote.net, adentro indicamos que es tipo maestro y la ruta donde se encuentra el archivo de configuración de la zona. Como también se agrego la resolución inversa, indicamos tipo maestro y la ruta del archivo de configuración.

Ahora tendremos que reiniciar el servicio de bind9.

```
root@server1:zones# /etc/init.d/bind9 restart
```

11.5 Comprobación de DNS.

Vamos a verificar que nuestro servidor DNS ya se encuentra en linea, primero haremos la comprobación localmente en nuestro servidor.

Para esto usaremos el comando host.

```
root@server1:~# host ascariote.net 127.0.0.1
Using domain server:
Name: 127.0.0.1
Address: 127.0.0.1#53
Aliases:


ascariote.net has address 192.168.1.243
ascariote.net mail is handled by 10 ascariote.net.ascariote.net.
root@server1:~#
```

Por medio del comando netstat, para verificar que el servicio esta en escucha.

```
root@server1:~# netstat -tanp | grep named
tcp   0  0 192.168.1.243:53  0.0.0.0:*   LISTEN      7132/named
tcp   0  0 127.0.0.1:53      0.0.0.0:*   LISTEN      7132/named
tcp   0  0 127.0.0.1:953     0.0.0.0:*   LISTEN      7132/named
root@server1:~#
```

Para poder hacer una comprobación desde otra máquina tenemos que agregar la IP de nuestro servidor DNS.

```
lucifer:~# vim /etc/resolv.conf
```

Modificaremos para quede de la siguiente manera.

```
nameserver 192.168.1.243
```

Y comprobamos.

```
lucifer:~# dig ascariote.net

; <<>> DiG 9.5.0-P2 <<>> ascariote.net
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57068
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1,
ADDITIONAL: 0

;; QUESTION SECTION:
;ascariote.net.                IN    A

;; ANSWER SECTION:
ascariote.net.          604800IN    A     192.168.1.243

;; AUTHORITY SECTION:
ascariote.net.          604800IN    NS    ascariote.net.

;; Query time: 0 msec
;; SERVER: 192.168.1.243#53(192.168.1.243)
;; WHEN: Wed Mar  4 14:25:34 2009
;; MSG SIZE  rcvd: 61

lucifer:~#
```

11.6 Logs de DNS.

Nuestro DNS guarda los log dentro de **/var/log/syslog**, para poder ver los ultimos sucesos de los log de DNS tendremos que ejecutar el siguiente comando

```
root@server1:~# tail -f /var/log/syslog | grep named
```

Nos deberá mostrar algo parecido a esto.

```
Mar  4 14:37:22 server1 named[7957]: zone 127.in-addr.arpa/IN:

Mar  4 14:37:22 server1 named[7957]: zone ascariote.net/IN: loaded
serial 2

Mar  4 14:37:22 server1 named[7957]: running

Mar  4 14:37:22 server1 named[7957]: zone 1.168.192.in-
addr.arpa/IN: sending notifies (serial 2)

Mar  4 14:37:22 server1 named[7957]: zone ascariote.net/IN:
sending notifies (serial 2)
```

En este archivo encontraremos si tenemos algún error en la configuración, un posible problema o indicando que servicio se levanto bien y sin ningún problema.