

TUTORIAL INSTALACIÓN Y CONFIGURACIÓN SERVIDOR DNS
"BIND9"

NET-DAEMONS

ADRIAN PEÑA
JOHAN LOPEZ
FELIPE PANIAGUA
RICARDO HENAO

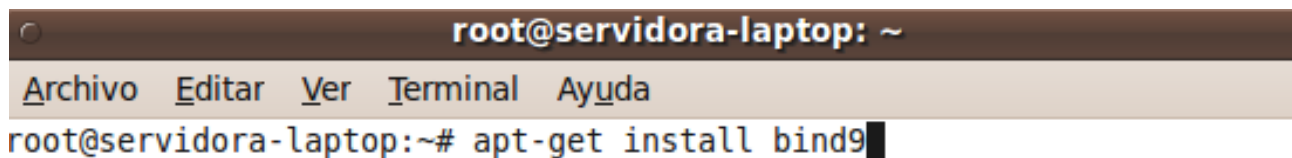
LINA MCKOLL

ADMINISTRACION DE REDES
SENA
2009

Este tutorial está hecho con el fin de mostrar cada uno de los pasos para la instalación y configuración de un servidor DNS en Linux con BIND9 y dicho servidor con dos esclavos que servirán de respaldo de nuestro servidor maestro.

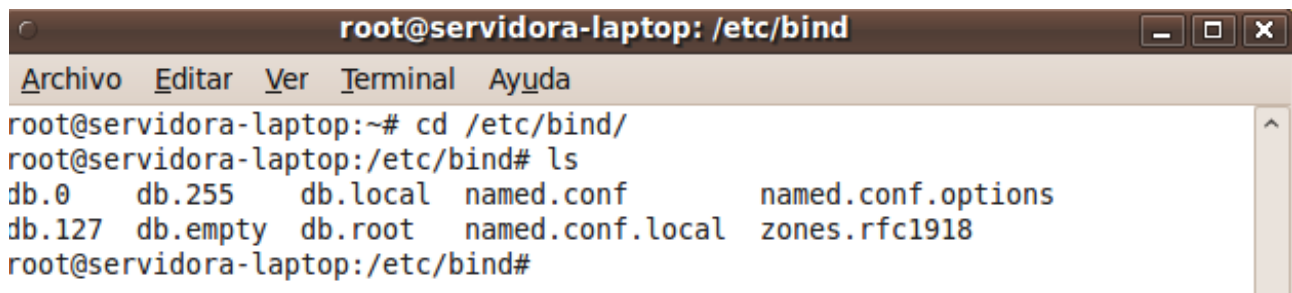
Primero que todo veremos cómo configurar un servidor maestro

En primer lugar instalaremos BIND9 en Ubuntu lo pueden hacer desde un terminal con el comando `apt-get install bind9` o `aptitude install bind 9`



```
root@servidora-laptop: ~  
Archivo Editar Ver Terminal Ayuda  
root@servidora-laptop:~# apt-get install bind9
```

Luego de tener instalado BIND9 habrá que ubicar la carpeta con los archivos de configuración los cuales estarán en la carpeta `/etc/bind`



```
root@servidora-laptop: /etc/bind  
Archivo Editar Ver Terminal Ayuda  
root@servidora-laptop:~# cd /etc/bind/  
root@servidora-laptop:/etc/bind# ls  
db.0 db.255 db.local named.conf named.conf.options  
db.127 db.empty db.root named.conf.local zones.rfc1918  
root@servidora-laptop:/etc/bind#
```

El siguiente paso es editar el archivo `name.conf` con el comando `nano` o `gedit` y allí pondremos la zona directa y la zona inversa con la ubicación de su archivo de configuración y allí mismo pondremos la ip de los servidores esclavos.

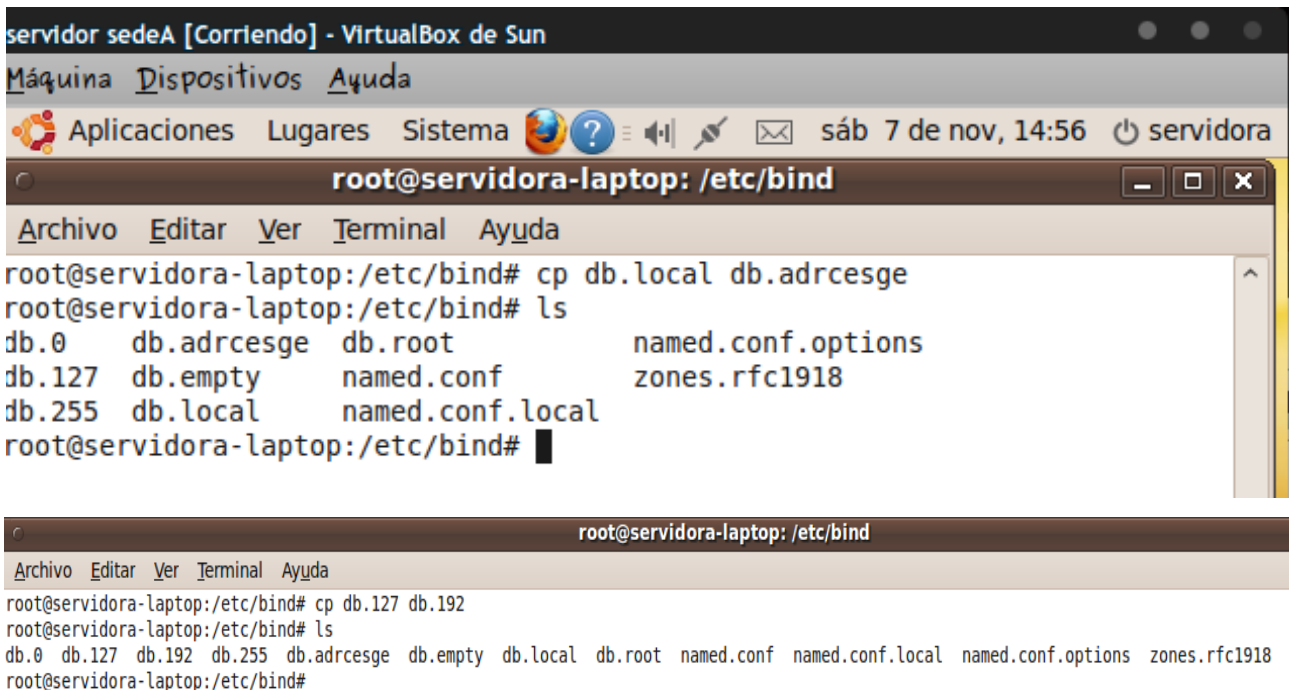
```
// be authoritative for the localhost forward and reverse zones, and for
// broadcast zones as per RFC 1912

zone "adrcesge.com" {
    type master;
    file "/etc/bind/db.adrcesge";
    also-notify {192.168.1.2; 192.168.1.3;};
};

zone "1.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.192";
    also-notify {192.168.1.2; 192.168.1.3;};
};
```

En la imagen la línea `also-notify` es una línea que hay que agregar si queremos que el servidor máster conozca sus esclavos en el campo de la zona inversa colocaremos la dirección a la inversa y según la red se trabajar sobre el cuarto, tercer o segundo octeto.

Luego de tener la zona directa y la zona inversa en el archivo `name.conf` crearemos el archivo de configuración de que definir las direcciones a resolver de cada una de estas zonas lo podemos hacer a partir de los archivos `db.local` y `db.127` con el comando `cp`



```
servidor sedeA [Corriendo] - VirtualBox de Sun
Máquina Dispositivos Ayuda
Aplicaciones Lugares Sistema sáb 7 de nov, 14:56 servidora
root@servidora-laptop: /etc/bind
Archivo Editar Ver Terminal Ayuda
root@servidora-laptop:/etc/bind# cp db.local db.adrcesge
root@servidora-laptop:/etc/bind# ls
db.0      db.adrcesge  db.root      named.conf.options
db.127   db.empty     named.conf   zones.rfc1918
db.255   db.local     named.conf.local
root@servidora-laptop:/etc/bind#
```

```
root@servidora-laptop:/etc/bind# cp db.127 db.192
root@servidora-laptop:/etc/bind# ls
db.0 db.127 db.192 db.255 db.adrcesge db.empty db.local db.root named.conf named.conf.local named.conf.options zones.rfc1918
root@servidora-laptop:/etc/bind#
```

luego de crear estos archivos los editaremos y allí pondremos la información de esta zona con el comando nano pondremos esta información que en este caso tendremos el dominio adrcesge.com y partiendo de él pondremos los host que el servidor DNS resolverá.

```
root@servidora-laptop: /etc/bind
Archivo Editar Ver Terminal Ayuda
GNU nano 2.0.9 Fichero: db.adrcesge

;
; BIND data file for adrcesge.com
;
$TTL      604800
@         IN      SOA    adrcesge.com. root.adrcesge.com. (
                2      ; Serial
                604800 ; Refresh
                86400  ; Retry
                2419200; Expire
                604800 ) ; Negative Cache TTL
;
                IN      NS     dns.adrcesge.com.
                IN      NS     dns2.adrcesge.com.
                IN      NS     dns3.adrcesge.com.

                IN      MX     0      mail.adrcesge.com.

ccnac2    IN      A       192.168.1.2
panduit   IN      A       192.168.1.2
dns2      IN      A       192.168.1.2
dns3      IN      A       192.168.1.3
dns       in      A       192.168.1.1
mail      IN      A       192.168.1.1
```

El campo en verde son los host que el servidor DNS va a traducir el campo en fucsia por defecto es localhost lo editamos a nuestro dominio y el campo en azul son los parámetros que seguirán los esclavos.

Estos son los parámetros que los esclavos tendrán en cuenta

- 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 que expiren.
- 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.

Términos en el campo a resolver.

- 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.

Ahora el siguiente paso será configurar la zona inversa hay que tener en cuenta si en el archivo name.comf los octetos de la red en los cuales se está trabajando estos son puestos a la inversa dos ejemplo de cómo puede hacerse son los siguientes en el name.conf poner los 3 primero octetos a la inversa de la dirección 192.168.1.0 obtendríamos 1.168.192 y en el archivo de configuración pondríamos solo el octeto faltante y en caso que solo usáramos el primer octeto como 192 en el archivo de configuración completamos de la siguiente manera el numero del host X.1.168 quedando de la siguiente manera.

```
BIND reverse data file for 192.168.1.0
TTL      604800
IN       SOA      adrcesge.com. root.adrcesge.com. (
                2          ; Serial
                604800    ; Refresh
                86400     ; Retry
                2419200   ; Expire
                604800 ) ; Negative Cache TTL

IN       NS       dns.adrcesge.com.
IN       NS       dns2.adrcesge.com.
IN       NS       dns3.adrcesge.com.

IN       PTR      ccnac2.adrcesge.com.
IN       PTR      panduit.adrcesge.com.
IN       PTR      dns2.adrcesge.com.
IN       PTR      dns3.adrcesge.com.
IN       PTR      dns.adrcesge.com.
```

En este punto ya podemos hacer pruebas para observar si el servidor está traduciendo las direcciones tal como se quiere, reiniciamos el DNS y luego con el comando host haremos pruebas.

```
root@servidora-laptop: /et
Archivo Editar Ver Terminal Ayuda
root@servidora-laptop:/etc/bind# /etc/init.d/bind9 restart
* Stopping domain name service... bind9
rndc: neither /etc/bind/rndc.conf nor /etc/bind/rndc.key was found

* Starting domain name service... bind9
root@servidora-laptop:/etc/bind# host 192.168.1.1
1.1.168.192.in-addr.arpa domain name pointer dns.adrcesge.com.
1.1.168.192.in-addr.arpa domain name pointer mail.adrcesge.com.
root@servidora-laptop:/etc/bind# host 192.168.1.2
2.1.168.192.in-addr.arpa domain name pointer ccnac2.adrcesge.com.
2.1.168.192.in-addr.arpa domain name pointer panduit.adrcesge.com.
2.1.168.192.in-addr.arpa domain name pointer dns2.adrcesge.com.
root@servidora-laptop:/etc/bind# host 192.168.1.3
3.1.168.192.in-addr.arpa domain name pointer dns3.adrcesge.com.
root@servidora-laptop:/etc/bind#
```

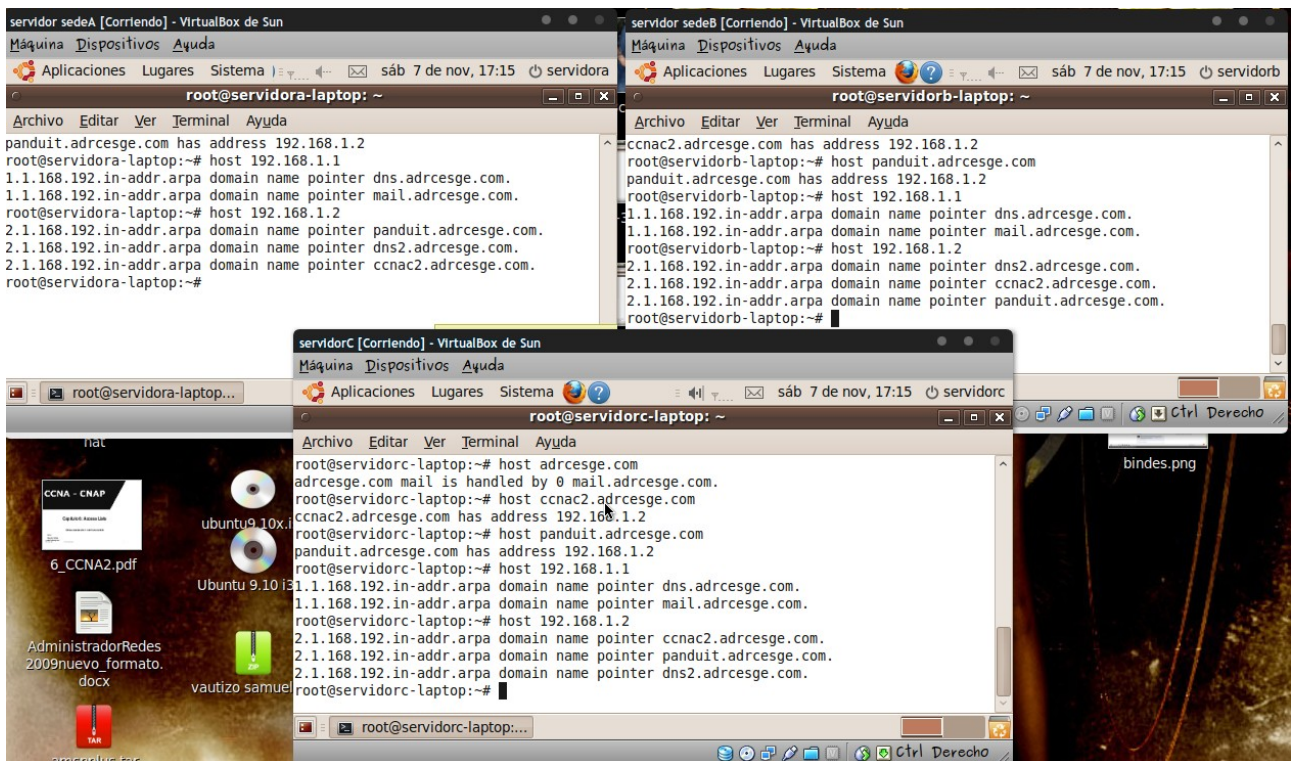
Ahora configuraremos los servidores esclavos en los archivos de configuración de los servidores esclavos lo único que haremos es editar el archivo name.conf y pondremos la zona especificar que es tipo esclavo y pondremos el servidor masters agregando esa línea luego es importante antes de reiniciar los servidores esclavos en el servidor maestro en los archivos de configuración de la zona directa e inversa ponerle una unidad mas al parámetro serial para que se sincronicen y lo mismo haremos cada que se cambie algo en estos archivos de configuración.

```
Archivo Editar Ver Terminal Ayuda
GNU nano 2.0.9 Fichero: named.conf

zone "adrcesge.com" {
    type slave;
    file "db.adrcesge";
    masters {192.168.1.1;};
};

zone "1.168.192.in-addr.arpa" {
    type slave;
    file "db.192";
    masters {192.168.1.1;};
};
```

Ahora cada maquina la configuraremos para que sea su propio servidor DNS y haremos las pruebas en todas ellas para verificar que todo sali3o bien.



Hasta acá tenemos un servidor DNS maestro con dos esclavos funcionando bien para una red local si queremos que estos servidores no resuelvan dominios remotos en la carpeta /etc/bind el archivo name.conf.options y colocaremos los servidores DNS de manera jerárquica para que cuando nuestro servidor no pueda resolver la peticiones reenvié estas a los servidores que tal vez si puedan

GNU nano 2.0.9

FILE #0: named.conf.options

```
options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    forwarders {
        200.118.2.66;
        200.118.2.85;
        200.13.249.101;
        200.13.224.254;
    };
};
```