

UNIVERSIDAD CAPITÁN GENERAL GERARDO BARRIOS.



“Servidor DNS en Redhat”

Servidores informáticos.

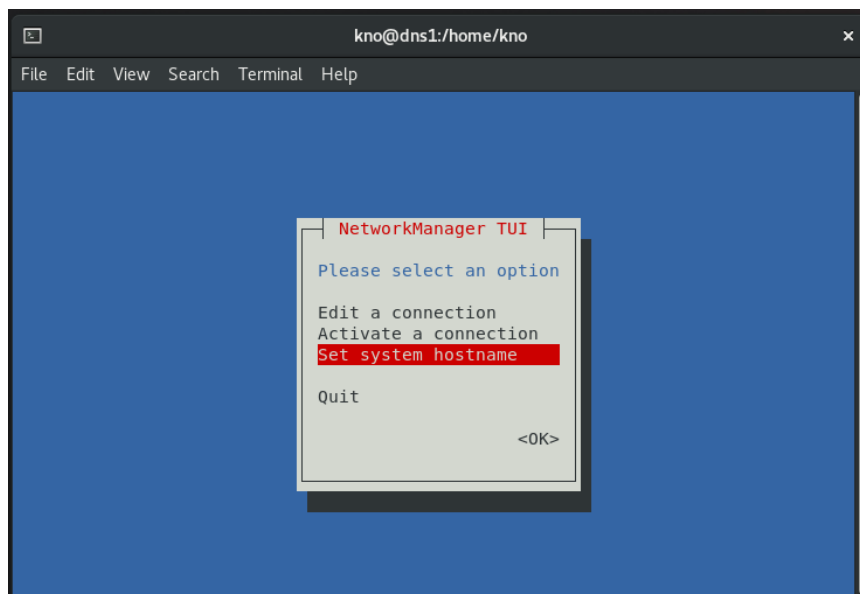
Requerimientos e indicaciones:

- Redhat Enterprise Linux Developer instalado versión 8.
- Tener una cuenta registrada en <https://developers.redhat.com/> configurado su usuario y contraseña.
- Instalar dos adaptadores de red (NAT y Solo Anfitrión)
- Suscribir su instalación de RedHat con su cuenta en Developers.redhat
- Configurar su adaptador de solo anfitrión de manera Estática.

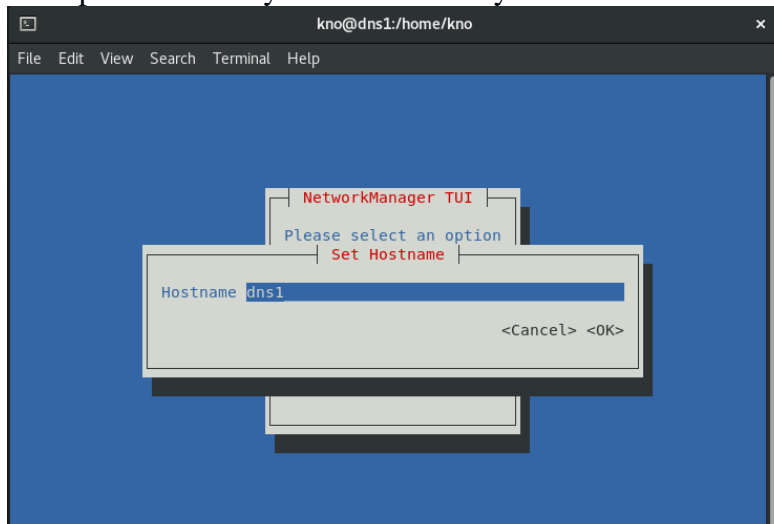
Generalidades:

Se deberá tener ya completada y funcional la guía práctica de la Semana 08.

Cambiar el nombre de Host predeterminado a dns1 de la siguiente manera con nmtui:



Seleccionaremos la opción de Set System Hostname y cambiamos el nombre de Hostname a dns1



Para verificar que se haya cambiado usamos el comando:

```
# hostname
```

```
[root@dns1 kno]# hostname  
dns1
```

PARTE I: Instalación de bind.

1. Instalación:

Como siempre emitiremos el comando yum:

```
sudo yum install -y bind-chroot bind-utils
```

Al emitir el siguiente comando:

```
sudo systemctl status named.service
```

Nos deberá aparecer el servicio como que no esta ejecutandose

2. Habilitamos el servicio para que arranque al iniciar e iniciamos el servicio:

Emitimos el siguiente comando:

```
sudo systemctl enable named.service
sudo systemctl status named.service
sudo systemctl start named.service
sudo systemctl status named.service
```

Esto básicamente nos asegura que el servicio **named.service** arrancarán por defecto y que a este momento ya el named.service esta ejecutandose.

3. Creación de nuestra zona:

```
nano /etc/named.conf
```

Agregar al principio del archivo:

```
options {
    listen-on port 53 { 192.168.23.4; };
    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";
    secroots-file "/var/named/data/named.secroots";
    recursing-file "/var/named/data/named.recursing";
    forward first;
    forwarders { 8.8.8.8; };
    allow-query { any; };
}
```

Agregar al final del archivo:

```
zone "cano.com.co" IN {
    type master;
    file "directa";
};

zone "23.168.192.in-addr.arpa" IN {
    type master;
    file "inversa";
};
```

Guardamos, salimos y verificamos que no tengamos errores en el archivo de configuración con el siguiente comando. En caso de tener algún error, nos mostrará la línea en que se encuentra.

```
named-checkconf /etc/named.conf
```

4. Creación de nuestros archivos de zona:

Ingresamos a la ruta donde se guardan los archivos del servicio en /var/named/ y buscamos el archivo named.empty

```
[root@dns1 kno]# cd /var/named/  
[root@dns1 named]# ls  
chroot named.empty    named.loopback  
data  dynamic named.ca named.localhost slaves
```

Copiamos el archivo named.empty con el nombre del archivo de la zona directa definido en el archivo de configuración named.conf:

```
[root@dns1 kno]# cp named.empty directa  
[root@dns1 named]# ls  
chroot named.empty directa named.loopback  
data  dynamic named.ca named.localhost slaves
```

Luego configuremos nuestra primera zona llamada “directa”, como copiamos por defecto al named.empty, únicamente modificaremos unas cosas, comparemos lo siguiente con el archivo que tenemos.

5. Agregar registros a nuestra zona directa:

```
$TTL 3H
@      IN SOA  @ dns1.cano.com.co. (
                                0      ; serial
                                1D     ; refresh
                                1H     ; retry
                                1W     ; expire
                                3H )   ; minimum

@      NS     dns1.cano.com.co.
@      A      192.168.23.4
dns1    A      192.168.23.4
www     CNAME  dns1
web     CNAME  dns1
ftp     CNAME  dns1
```

Guardamos, salimos y verificamos que no tengamos errores en la zona directa con el siguiente comando.

```
[root@dns1 named]# named-checkzone 192.168.23.2 directa
zone 192.168.23.2/IN: loaded serial 0
OK
[root@dns1 named]#
```

Copiamos el archivo de zona directa con el nombre del archivo de zona inversa dado en el archivo de configuración del servidor y después editarlo:

```
[root@dns1 kno]# cp directa inversa
[root@dns1 named]# ls
chroot named.empty directa inversa named.loopback
data  dynamic named.ca named.localhost slaves
```

6. Agregar registros a nuestra zona inversa:

```
$TTL 3H
@      IN SOA  @ dns1.cano.com.co. (
                                0      ; serial
                                1D     ; refresh
                                1H     ; retry
                                1W     ; expire
                                3H )   ; minimum
      NS      dns1.cano.com.co.
2      PTR    dns1.cano.com.co.
2      PTR    www.cano.com.co.
2      PTR    web.cano.com.co.
2      PTR    ftp.cano.com.co.
```

Guardamos, salimos y verificamos que no tengamos errores en la zona directa con el siguiente comando.

```
[root@dns1 named]# named-checkzone 192.168.23.2 inversa
zone 192.168.23.2/IN: loaded serial 0
OK
[root@dns1 named]#
```

6. Cambiamos de grupo de permiso nuestros archivos:

Listamos el contenido del directorio /var/named. Mirar el grupo propietario que debe ser named.

```
[root@dns1 named]# ll
total 24
drwxr-x---. 7      root    named    61   Mar  8 21:25 chroot
drwxrwx---. 2      named   named    23   Mar  8 21:26 data
-rw-r-----. 1      root    root     259  Mar  8 21:39 directa
drwxrwx---. 2      named   named    60   Mar  9 06:55 dynamic
-rw-r-----. 1      root    root     283  Mar  8 21:43 inversa
-rw-r-----. 1      root    named    2253 Aug 19 2021 named.ca
-rw-r-----. 1      root    named    152  Aug 19 2021 named.empty
-rw-r-----. 1      root    named    152  Aug 19 2021 named.localhost
-rw-r-----. 1      root    named    168  Aug 19 2021 named.loopback
drwxrwx---. 2      named   named     6   Aug 19 2021 slaves
[root@dns1 named]# chgrp named directar inversa
[root@dns1 named]# ll
total 24
drwxr-x---. 7      root    named    61   Mar  8 21:25 chroot
drwxrwx---. 2      named   named    23   Mar  8 21:26 data
-rw-r-----. 1      root    named    259  Mar  8 21:39 directa
drwxrwx---. 2      named   named    60   Mar  9 06:55 dynamic
-rw-r-----. 1      root    named    283  Mar  8 21:43 inversa
-rw-r-----. 1      root    named    2253 Aug 19 2021 named.ca
-rw-r-----. 1      root    named    152  Aug 19 2021 named.empty
-rw-r-----. 1      root    named    152  Aug 19 2021 named.localhost
-rw-r-----. 1      root    named    168  Aug 19 2021 named.loopback
drwxrwx---. 2      named   named     6   Aug 19 2021 slaves
```

PARTE II: Settings adicionales

1. Configuramos nuestro servidor dns como sigue:

```
nano /etc/resolv.conf
```

Borramos todo y agregamos lo siguiente:

```
# Generated by NetworkManager
search cano.com.co
nameserver 192.168.23.4
```

Debido a que nuestro adaptador NAT está por DHCP debemos colocar el siguiente comando para que el archivo resolv.conf no se modifique

```
[root@dns1 ~]# chattr +i /etc/resolv.conf
```

Guardamos en nano y luego salimos.

2. Abrimos el siguiente archivo.

Editamos el archivo hosts y colocamos la IP del servidor así como el nombre del mismo.

```
[root@dns1 named]# nano /etc/hosts
```

```
File Edit View Search Terminal Help
GNU nano 2.9.8 /etc/hosts
1 127.0.0.1    localhost localhost.localdomain localhost4 localhost4.localdom$
::1          localhost localhost.localdomain localhost6 localhost6.localdom$
192.168.23.4 dns1.cano.com.co cano.com.co
```

3. Iniciamos Servicios.

```
[root@dns1 ~]# systemctl start named
[root@dns1 ~]#
```

Hacemos pruebas con el comando nslookup

```
root@dns1 ~]# nslookup cano.com.co
Server:      192.168.23.4
Address:     192.168.23.4#53

Name: cano.com.co
Address: 192.168.23.4

[root@dns1 ~]#
[root@dns1 ~]# nslookup www.cano.com.co
Server:      192.168.23.4
```

Address: 192.168.23.4#53

www.cano.com.co canonical name = dns1.cano.com.co.

Name: dns1.cano.com.co

Address: 192.168.23.4

[root@dns1 ~]#

[root@dns1 ~]# nslookup web.cano.com.co

Server: 192.168.23.4

Address: 192.168.23.4#53

web.cano.com.co canonical name = dns1.cano.com.co.

Name: dns1.cano.com.co

Address: 192.168.23.4

[root@dns1 ~]#

PARTE III: Configuración de nuestro firewall

1. Verificar servicios permitidos en firewall-cmd

```
firewall-cmd --zone="public" --list-services
```

Agremos las siguientes reglas:

```
firewall-cmd --zone="public" --add-service="dns" --permanent  
firewall-cmd --zone="public" --add-port="53/tcp" --permanent  
firewall-cmd --zone="public" --add-port="53/udp" --permanent  
firewall-cmd --reload
```

Verificamos que estae correctamente configurada nuestra zona

```
firewall-cmd --zone="public" --list-all
```

En este apartado se pretende que se vaya familiarizando con el firewall y que además vaya deduciendo que puertos va a tener que utilizar para diferentes servicios que se vayan instalando.

Emitir en la terminal el siguiente comando:

```
ping cano.com.co
```