

Servidor DNS en CentOS 8

El servicio DNS se utiliza para la resolución de nombres de hosts a dirección IP y viceversa. Es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada. Este sistema asocia información variada con nombres de dominios asignado a cada uno de los participantes. Su función más importante, es traducir (resolver) nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

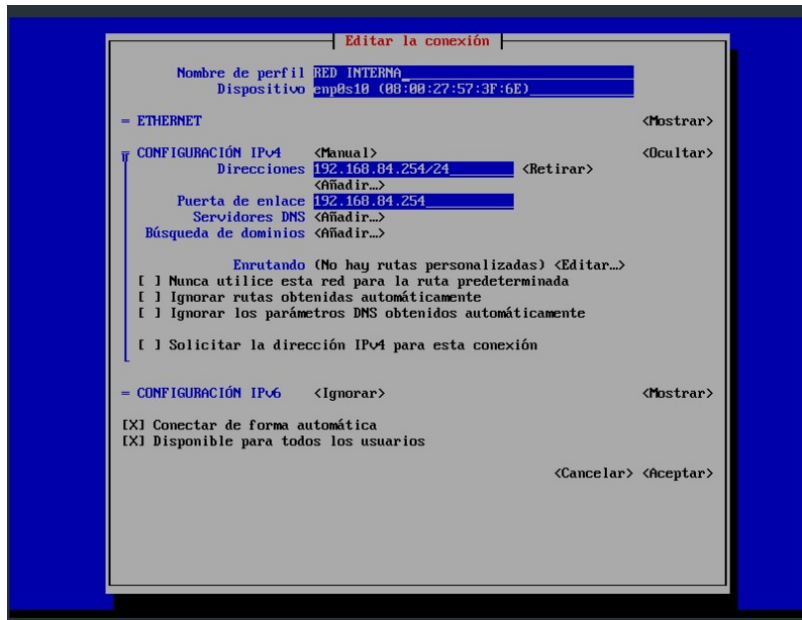
En la presente guía implementará el servidor DNS en CentOS 8. Para el desarrollo de la implementación Ud. previamente debe configurar las interfaces de red del cliente y el servidor en red interna, con direccionamiento en el mismo segmento de red.

CONFIGURACIÓN EN EL SERVIDOR

Instalamos el paquete DNS.

```
[root@localhost dhcp]# yum install bind
```

Nota: la tarjeta de red debe tener la siguiente estructura en su configuración y estar en red LAN o local.



Editamos el archivo de configuración del servicio con su editor de texto preferido.

```
[root@localhost ~]# nano /etc/named.conf
```

Configuramos las opciones de nuestro servidor:

```
GNU nano 2.9.8 /etc/named.conf Modificado
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//

options {
    listen-on port 53 {192.168.84.254; 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";
    secroots-file "/var/named/data/named.secroots";
    recursing-file "/var/named/data/named.recursing";
    allow-query { any ; };

    /*
    - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.
    - If you are building a RECURSIVE (caching) DNS server, you need to enable
    recursion.
    - If your recursive DNS server has a public IP address, you MUST enable access
    control to limit queries to your legitimate users. Failing to do so will
    cause your server to become part of large scale DNS amplification
    attacks. Implementing BCP38 within your network would greatly
    reduce such attack surface
    */
    recursion yes;
}

Ver ayuda Guardar Buscar Cortar txt Justificar Posición Deshacer
Salir Leer fich. Reemplazar Pegar txt Ortografía Ir a línea Rehacer
```

Listen-on port 53: Colocar la IP de la interfaz que escuchará las consultas DNS.

Allow-query: De quien se escuchará consultas.

Copiamos y modificamos los parámetros de las zonas directa e inversa de nuestro servidor DNS: La zona directa resuelve de nombre de host a dirección IP. La zona inversa resuelve de dirección IP a nombre de host.

```
//
zone "devnat.uttt.edu.mx"{
    type master;
    file "/var/named/bd.devnat.uttt.edu.mx";
};
zone "84.168.192.in-addr.arpa"{
    type master;
    file "/var/named/rev.192.168.84";
};
zone "." IN {
    type hint;
    file "named.ca";
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
```

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.

Elaborado por: Uriel Adolfo Cruz Ventura

Fecha: 15/03/2021

```
[root@localhost ~]# named-checkconf /etc/named.conf
[root@localhost ~]#
```

Ingresamos a la ruta donde se guardan los archivos del servicio en /var/named/ en el cual vamos a crear un archivo

```
[root@localhost ~]#
[root@localhost ~]# cd /var/named/
[root@localhost named]# touch db.devnat.uttt.edu.mx
```

Ahora sí, modificamos el archivo de acuerdo a nuestros hosts y teniendo en cuenta los registros; algunos de estos son:

NS: Name Server. Hace referencia al nombre del servidor.

A: Nombre del host. Para resolver de nombre de host a dirección IP.

CNAME: Canonical Name. Alias de un host.

PTR: Pointer. Puntero para resolver de IP a nombre de host.

MX: Mail Exchange. Indica el servidor de correo electrónico.

```
GNU nano 2.9.8 bd.devnat.uttt.edu.mx
$TTL 9648
@      IN      SOA      dns.devnat.uttt.edu.mx. root.devnat.uttt.edu.mx (
                        2021031302;
                        604800;
                        86400;
                        604800;
                        86400);
@      IN      NS       dns.devnet.uttt.edu.mx.
@      IN      A        192.168.84.254
dns.devnet.uttt.edu.mx. IN      A        192.168.84.254
dhcp   IN      CNAME    dns
win7   IN      A        192.168.84.1
```

Guardamos, salimos

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@localhost named]# cp bd.devnat.uttt.edu.mx /var/named/rev.192.168.84
```

Abrimos el archivo copiado.

```
[root@localhost named]# ls
bd.devnat.uttt.edu.mx  dynamic  named.empty  named.loopback  slaves
data                  named.ca  named.localhost  rev.192.168.84
[root@localhost named]# nano rev.192.168.84
```

Elaborado por: Uriel Adolfo Cruz Ventura

Fecha: 15/03/2021

```
GNU nano 2.9.8 rev.192.168.84
$TTL 86400
@      IN      SOA     dns.devnet.utt.edu.mx. root.devnet.utt.edu.mx. (
                                2021031502;
                                604800;
                                86400;
                                604800;
                                86400);
@      IN      NS      dns.devnet.utt.edu.mx.
254    IN      PTR     dns.devnet.utt.edu.mx.
254    IN      PTR     dhcp.devnet.utt.edu.mx.
1      IN      PTR     win7.devnet.utt.edu.mx.
```

Iniciamos el servicio:

```
[root@localhost named]# systemctl start named
[root@localhost named]# _
```

Una vez hecha la prueba local abrimos el puerto 53 en el firewall para poder hacer pruebas con un cliente. Esto lo podemos hacer ya sea agregando los puertos y protocolo uno por vez o agregando el servicio. Una vez agregado, comprobamos.

```
[root@localhost named]# systemctl start named
[root@localhost named]# firewall-cmd --add-service=dns --permanent
success
[root@localhost named]# firewall-cmd --add-service=dhcp --permanent
success
[root@localhost named]#
```

Miramos en el cliente el direccionamiento y constatar la dirección IP en el mismo segmento del servidor:

Nota: si utilizamos el cliente con que configuramos el DHCP, debemos quitar la denegación de dirección para poder recibir una IP por DHCP o también podemos asignarle una manualmente.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\CUriel>ipconfig /renew

Configuración IP de Windows

Adaptador de Ethernet Conexión de área local:

    Sufijo DNS específico para la conexión. . . : devnet.utt.edu.mx
    Vínculo: dirección IPv6 local. . . . . : fe80::283c:1ff7:6ebf:5851%11
    Dirección IPv4. . . . . : 192.168.84.1
    Máscara de subred. . . . . : 255.255.255.0
    Puerta de enlace predeterminada. . . . . : 192.168.84.254

Adaptador de túnel isatap.devnet.utt.edu.mx:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . . : devnet.utt.edu.mx

C:\Users\CUriel>
```

Probamos con nslookup y con ping a nombre que el asignaste a cada host la resolución desde el cliente Windows 7

```
C:\Windows\system32\cmd.exe

Haciendo ping a dns.devnat.uttt.edu.mx [192.168.84.254] con 32 bytes de datos:
Respuesta desde 192.168.84.254: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.84.254: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.84.254: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.84.254: bytes=32 tiempo=1ms TTL=64

Estadísticas de ping para 192.168.84.254:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 1ms, Media = 0ms

C:\Users\CUriel>ping win7

Haciendo ping a win7.devnat.uttt.edu.mx [192.168.84.1] con 32 bytes de datos:
Respuesta desde 192.168.84.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.84.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.84.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.84.1: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.84.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\CUriel>ping dns

Haciendo ping a dns.devnat.uttt.edu.mx [192.168.84.254] con 32 bytes de datos:
Respuesta desde 192.168.84.254: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.84.254: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.84.254: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.84.254: bytes=32 tiempo=1ms TTL=64

Estadísticas de ping para 192.168.84.254:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 1ms, Media = 0ms

C:\Users\CUriel>nslookup dns
Servidor:  dns.devnat.uttt.edu.mx
Address:  192.168.84.254

Nombre:   dns.devnat.uttt.edu.mx
Address:  192.168.84.254

C:\Users\CUriel>
```