SRM 2

22

ServicioDNS

Instalación y configuración

Francisco Moreno Rodrigo

Tabla de Contenido

[Preparar la maquina servidor 1](#_Toc116981476)

[ Crear maquina con dos interfaces de red 1](#_Toc116981477)

[ Verificar las interfaces de red 1](#_Toc116981478)

[ Actualización del sistema 1](#_Toc116981479)

[ Instalación paquete BIND9 1](#_Toc116981480)

[ Configuración /etc/default/named 1](#_Toc116981481)

[ Configuración de los ficheros principales 2](#_Toc116981482)

[ Comprobaciones de los ficheros 4](#_Toc116981483)

[ Iniciar y comprobar el servicio 4](#_Toc116981484)

[ Comprobar el servicio 4](#_Toc116981485)

[Practica 2 5](#_Toc116981486)

[ Configuración de las zonas directa y indirecta 5](#_Toc116981487)

[Pruebas Clientes 6](#_Toc116981488)

Preparar la maquina servidor

* Crear maquina con dos interfaces de red
* **1 NAT**
* **1 interna (10.0.0.254)**
* Verificar las interfaces de red

Una vez iniciado el sistema verificamos el estado de las interfaces por si hubiera algún problema.

1. Caso interfaz **Down** introducimos el siguiente comando:

# ip link set up [nombre de la interface]

1. Caso **look back** no este cargando correctamente, modificamos el siguiente fichero:

sudo nano /etc/resolve.conf

* sí aun necesitamos internet se nos cambiara el DNS cada vez que reiniciemos porque el resolve carga el servidor dns por defecto del dhcp
* Actualización del sistema

Una vez hallamos verificado las redes vamos a actualizar el sistema con el comando:

#sudo apt update -y; sudo apt upgrade -y

* El **-y** sirve para que el comando no pregunte si queremos instalarlas dependencias o actualizaciones necesarias.
* Instalación paquete BIND9

Para el servicio DNS necesitaremos instalar el paquete BIND9, utilizaremos el siguiente comando:

#sudo apt install bind9

* Configuración /etc/default/named

1. Empezaremos por configurar el fichero**/etc/default/named** para evitar mensajes de error innecesarios por el protocolo IPv6:

#/etc/default/named

* Deberemos cambiar la linea Option=”-4”solo añadimos el -4 lo otro lo dejamos igual.
* Configuración de los ficheros principales
* /etc/bind/named.conf.options(Fichero para configurar el servidor cache)

En este fichero agregaremos DNS oficiales como por ejemplo las de Google:

fran@dns:/etc/bind$ cat named.conf.options

options {

directory "/var/cache/bind";

// Ifthereis a firewall betweenyou and nameserversyouwant

// totalkto, youmayneedtofixthe firewall toallowmultiple

// portstotalk. See http://www.kb.cert.org/vuls/id/800113

// Ifyour ISP providedoneor more IP addressesforstable

// nameservers, youprobablywantto use them as forwarders.

// Uncommentthefollowing block, and inserttheaddressesreplacing

// the all-0's placeholder.

forwarders {

8.8.8.8;

};

//========================================================================

// If BIND logs error messagesabouttheroot key beingexpired,

// youwillneedto update yourkeys. See https://www.isc.org/bind-keys

//========================================================================

dnssec-validation auto;

listen-on-v6 { any; };

};

* /etc/bind/named.conf.local (Fichero donde se almacenaras las zonas)

fran@dns:/etc/bind$ cat named.conf.local

//

// Do any local configurationhere

//

// Consideraddingthe 1918 zones here, ifthey are notused in your

// organization

//include "/etc/bind/zones.rfc1918";

// be authoritativeforthe localhost forward and reverse zones, and for

// broadcast zones as per RFC 1912

***ZONA DIRECTA***

zone "franmoreno.local" {

type master;

file "/etc/bind/zones/franmoreno.db";

};

***ZONA INVERSA***

zone "0.0.10.in-addr.arpa" {

type master;

file "/etc/bind/zones/10.db";

};

* Fijarse mucho en el nombre de las zonas porque pueden ocasionar errores de enrutamiento
* /etc/bind/zones/[nombrezonadirecta].db (Fichero de nueva creación para la zona directa)

Por ultimo deberemos crear el fichero de zona directa en nuestra practica se llamara:

**Franmoreno.db** y estará almacenado en una carpeta creada llamada **zones** esto ultimo es una buena práctica para evitar mezclar ficheros.

* Los mas practico es copiar el fichero que lleva una preconfiguración llamado db.local así que vamos a ejecutar el siguiente comando:*importante deberemos esta en la carpeta /etc/bind*

# sudo cpdb.local zones/franmoreno.db

Una vez tenemos el fichero procederemos a configurarlo:

fran@dns:/etc/bind$ cat zones/franmoreno.db

;

; BIND data file for local loopback interface

;

$TTL 604800 ;tiempo de respuesta de las DNS

@ IN SOA dns.franmoreno.local. admin.franmoreno.local. (

20221015 ; Serial

604800 ;Refresh

86400 ;Retry

2419200 ; Expire

604800 ) ; Negative Cache TTL

;

IN NS dns.franmoreno.local.

IN MX 10 mail.franmoreno.local.

dns IN A 10.0.0.254

mail IN A 10.0.0.254

PC1 IN A 10.0.0.1

PC2 IN A 10.0.0.2

PC3 IN A 10.0.0.3

PC4 IN A 10.0.0.4

www IN A 10.0.0.253

ftp IN CNAME www

moodle IN CNAME ftp

* Es importante fijar en que los nombres de domino finalicen con un .
* El fichero es sensible a los espaciados y pueden ocasionar errores
* Si ha dominios que están en la misma Ip para ahórranos trabajo podemos utilizar el CNAME apuntando al domino donde con la Ip
* /etc/bind/zones/[ipinversa].db (Fichero de nueva creación para la zona inversa)ejm.18.168.192.db
* Los más practico es copiar el fichero que lleva una preconfiguración llamado db.local así que vamos a ejecutar el siguiente comando:*importante deberemos está en la carpeta /etc/bind*

# sudo cpdb.local zones/0.0.10.db

fran@dns:/etc/bind$ cat zones/10.db

;

; BIND reverse data file for local loopback interface

;

$TTL 604800

@ IN SOA dns.franmoreno.local. admin.franmoreno.local. (

20221015 ; Serial

604800 ;Refresh

86400 ;Retry

2419200 ; Expire

604800 ) ; Negative Cache TTL

;

@ IN NS dns.franmoreno.local.

254 IN PTRdns.franmoreno.local.

254 IN PTR mail.franmoreno.local.

1 IN PTR pc1.franmoreno.local.

2 IN PTR pc2.franmoreno.local.

3 IN PTR pc3.franmoreno.local.

4 IN PTR pc4.franmoreno.local.

253 IN PTR www.franmoreno.local.

253 IN PTR ftp.franmoreno.local.

253 IN PTR moodle.franmoreno.local.

* Este fichero solo necesitara declara el nombre del servicio DNS y después apuntar la Ip a los distintas Ip, en nuestro caso al ser una mascara /24 solo deberemos pasar el último número.
* Comprobaciones de los ficheros

Aunque no son muy fiables pueden ayudarnos si el servicio no nos funciona:

1. named-checkconf
   1. sirve para encontrar fallos en los ficheros de zona

#sudo named-checkconf [nombre del fichero]

1. named-checkzone
   1. sirve para comprobar errores en zonas

#sudo named-checkzone[nombre de la zona] [nombre del fichero]

* Iniciar y comprobar el servicio

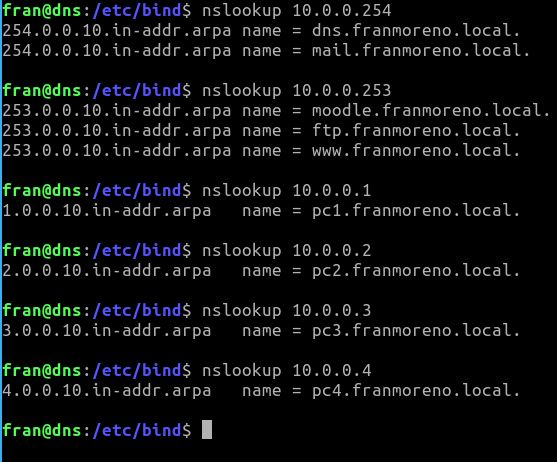
#sudo systemctlstart bind9

#sudo systemctlstatus bind9

* Comprobar el servicio

# sudo nslookup [nombre del dominio Completo]

Funcionamiento del servicio desde el servidor:

****

Practica 2

* Configuración de las zonas directa y indirecta

En esta practica el grueso lo tenemos hecho ya y solo necesitaremos añadir las dos zonas con los nombres que nos pide la práctica.

1. Fichero configuración de zonas /etc/bind/named.conf.local

fran@dns:/etc/bind$ cat named.conf.local

//

// Do any local configurationhere

//

// Consideraddingthe 1918 zones here, ifthey are notused in your

// organization

//include "/etc/bind/zones.rfc1918";

// be authoritativeforthe localhost forward and reverse zones, and for

// broadcast zones as per RFC 1912

zone "franmoreno.local" {

type master;

file "/etc/bind/zones/franmoreno.db";

};

zone "0.0.10.in-addr.arpa" {

type master;

file "/etc/bind/zones/10.db";

};

Las dos zonas nuevas

zone "franmoreno2.local" {

type master;

file "/etc/bind/zones/franmoreno2.db";

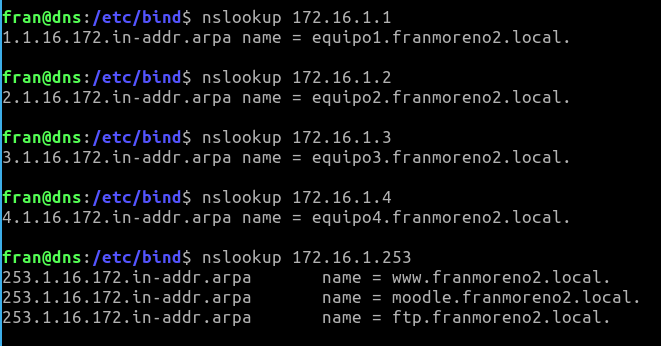
};

zone "1.16.172.in-addr.arpa" {

type master;

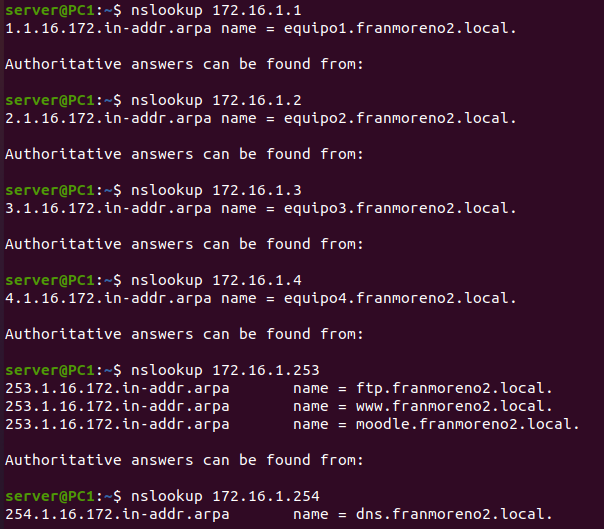
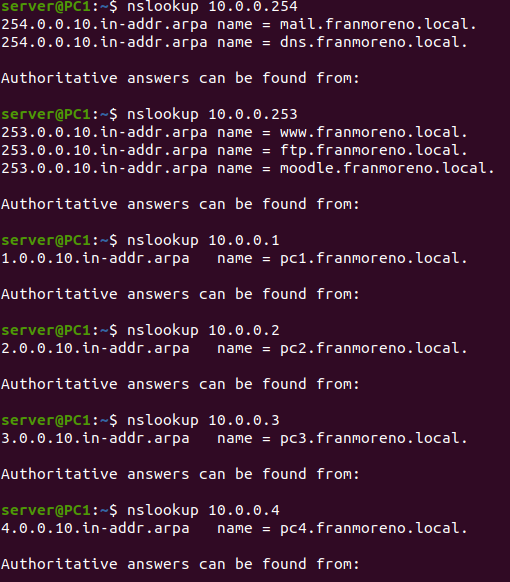
file "/etc/bind/zones/172.db";

};

1. Fichero zona directa /etc/bind/zones/franmoreno2.db
2. Fichero zona indirecta /etc/bind/zones/172.db
3. Cosas importantes a tener en cuenta deberemos añadi:
   1. Añadir otra interface de red para la red nueva
   2. Fijarle la Ip 172.16.1.254
   3. muestra del servicio desde el servidor

Pruebas Clientes

Para este caso iniciaremos un cliente con la interfaz de red en **SERVIDOR\_DNS** y probaremos si nos responde el servicio DNS.

****