Configuración propia del servidor DNS

/etc/bind/named.conf - .default-zones

- .options

- .local

En el archivo .option, tenemos # forwarders 0.0.0.0 comentado, pq?

**MODOS/TIPOS DE resolución DNS:**

**MODO servidor caché :**

Tenemos un primer servidor que pregunta al servidor DNS de google 8.8.8.8 y este servidor se guarda en caché las respuestas, así no satura el 8.8.8.8 i es más rápido si pregunta las mismas direcciones una y otra vez.

BindForward es un servidor caché DNS

**MODO servidor forward / reenvío:**

El fichero ***/etc/bind/named.conf.options*** indica que se deben guardar las direcciones ya resueltas para su uso posterior y a quién preguntar si no se sabe resolver cualquier dirección:

/etc/bind/named.conf.options

options {

directory "/var/cache/bind";

forwarders {

192.168.1.1; (ESTA IP SERA LA DEL EL RECURSIVE)

};

Ejemplo cliente hace “ *host smx.edt “*→ pero esta petición no deberia mandarse a 8.8.8.8 (DNS google) sino que debería preguntar a sus servidores DNS por si lo tienen.

Vim /**etc/bind.named.conf.options**

Descomentamos y entonces el servidor forwarded enviará todas las peticiones que no sean de sus zonas al servidor 8.8.8.8 (o el que esté puesto). De no ser así preguntará a los servidores raiz. (root servers)

named-checkzones → Per comprobar (sintaxi) sobre un arxiu **db.**

**MODO DE TRABAJO DEL DNS EN MODO RESOLUCION RECURSIVO**

**El servidor se buscará la vida para devolver la respuesta directamente.**

(TENIENDO EL FORWARDED COMENTADO/DESHABILITADO )

host google.com, lo puede resolver nuestro servidor principal (el .1) porque lo tiene en caché de consultas anteriores.

Vim /usr/share/dns/root.hints (AQUI ESTAN LAS IP DE LOS SERVIDORES ROOT A PREGUNTAR)

**MODO DE RESOLUCION ITERATIVO:**

A una petición (mi.dominio.com) el primer servidor (**1er root server)** devuelve la IP de quien tiene la información del dominio (.com). Así el cliente deberá preguntar a este servidor si tiene la IP del dominio (.dominio.com). I si la tiene volverà a preguntar si tiene la mi.domini.com

EN EL **SERVIDOR EDT**

Vim /etc/bind/named.conf.options

Añadimos la linea: recursion no;

I probamos *host alum1.smx.edt* → NO FUNCIONA, NO POT PREGUNTAR A NINGUN DELEGAT

EN EL **SERVIDOR SMX.EDT**

Vim /etc/bind/named.conf.options

Añadimos la linea: recursion no;

I probamos *host alum1.smx.edt* → FUNCIONA, NO LI CAL PREGUNTAR A NINGU PQ ELL TÉ LA RESOSTA I TAMPOC TE DELEGATS

Se usa principamente en para los servidores terminales (smd.edt, asx.edt)

La recursión es MUY PELIGROSA. ¿ PQ ?

Si hacemos muchas peticiones a un servidor DNS pero las respuestas (voluminosas) las mandamos a una IP distinta (vector de ataque)

Si exponemos un servidor recursivo exponemos a que puedan usarlo mal intencionadamente.

MONITORIZAR SERVICIO DNS:

rndc querylog → Activa el registro de todas las consultas a este DNS.

Journalctl -u named -f & (en el servidor)

Si desde el cliente hacemos un host, aparecerá en el servidor los mensajes de info.

Systemctl restart bind9 (reiniciem servidor DNS)

Rdnc stats , guarda en /var/cache/bind/rndc. Estadísticas de uso, fallos etc DNS

----------------------------------------------------------------------------------------------------

Dentro de un archivo db. En BIND podemos hacer:

$GENERATE 1-150 alu$ A 192.168.0.$ (para permitir todas las 150 IP)

---------------------------------------------------------------------------------------------------------

En BIND hay servidores primarios y secundarios:

Ejemplo definimos

@ smx.edt SOA dns0 email 1 4 4 4 4 (zona)

NS dns0 (servidores)

NS dns1 → PRIMARIO

ND dns2 → SECUNDARIO (POR SI CAE EL PRIMARIO QUE SIGA RESOLVIENDO DNS)

Luego glurecords (para asignar IPs) Ex: dns1 A 192...3

dns2 A 192..4

MASTER- primary-primario

SLAVE- secondary-secundarios

Smx.edt es del tipo PRIMARY

Clonamos la máquina smx.edt y lo ponemos como SECONDARY i le cambiamos la IP (una no usada)

En el /etc/bind/named.config.defaults-zones, cambiamos lo azul→

Zone “smx.edt” {

Type secondary

File **“/var/lib/bind/db.smx.edt”**; #← OJO permisos de root o permisos de name (“name” es el administrador de BIND)

masters { 192.168.0.3;

};

};

Editem vim /etc/network/interfaces → Canviem la IP p.e a la .5

A la maquina original smx.edt canviem (opcional) :

Zone “smx.edt” {

Type master per Type primary

Afegim ara al servidor principal EDT, el servidor clon secundari-SMX.

Anem a db.edt i li afegim aquestes lineas:

smx.edt NS dns2.smx

dns2.smx A 192.168.0.5

<https://linuxserver.webcindario.com/dns/Configuracion_del_servidor_DNS.html>

-------------------