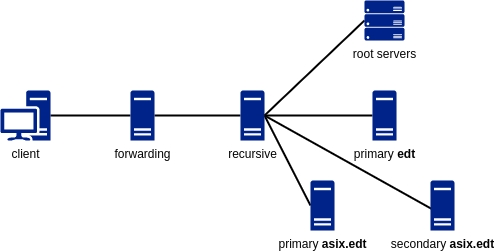
B ghDNS Pràctica

Desplega una infraestructura DNS com la representada al següent diagrama:



Hauràs de crear (clonar) 6 màquines virtuals. Totes han d'estar dintre de la mateixa xarxa virtual aïllada (isolated). A més a més, la màquina recursive haurà d'estar connectada a una xarxa NAT (per a poder accedir als root servers).

El client tindrà configurat com a **resolver** el servidor forwarding.

El forwarding reenviarà les peticions al servidor recursive.

El recursive resoldrà les peticions de la zona "edt" reenviant-les (forward) al servidor primary edt. Les peticions de la zona "." les resoldrà utilitzant els root servers.

El servidor primary edt delegarà la zona "asix.edt" en els servidors primary asix.edt i secondary asix.edt

El servidor secondary asix.edt serà de type secondary i el seu primariy serà el servidor primary asix.edt

Ni el servidor primary asix.edt ni el secondary asix.edt han de funcionar en mode recursiu.

Tots els servidors han de tenir activa l'opció dnssec-validation.

La zona "asix.edt" tindrà els següents **Resource Records:**

*asix.edt A 192.168.200.1*

*www.asix.edt CNAME asix.edt*

*alumne1.asix.edt A 192.168.10.1*

*alumne2.asix.edt A 192.168.10.2*

*; --- fins a*

*alumne100.asix.edt A 192.168.10.100*

*asix.edt MX 1 aspmx.l.google.com*

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

ENTREGA:

Entrega la pràctica en un arxiu de text. Inclou els arxius de configuració rellevants de cada màquina. Indica la màquina amb cinc iguals seguit del nom, i la ruta dels fitxers d'aquesta màquina amb cinc guions. No incloguis els comentaris.

Exemple:

*===== primary edt*

*----- /etc/network/interfaces*

*auto enp7s0*

*iface enp7s0 inet static*

*address 192.128.0.1/24*

**ULL ALFINAL PER TENIR SSH I PODER COPIAR ARXIUS DE LES MAQUINES VIRTUALS AL HOST S’HA HABILITAT LA NAT I LES IP DINAMIQUES (DHCP)**

*----- /etc/network/interfaces*

*auto enp7s0*

*iface enp7s0 inet* ***dhcp***

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

*options {*

*directory "/var/cache/bind";*

*dnssec-validation yes;*

};

**Més apunts de DNS:**

<https://elpuig.xeill.net/Members/vcarceler/c1/didactica/apuntes/ud4/na8>

**CONFIGURACIONS**

Recordar que hem habilitat totes les interficies en NAT, i les IPs es donen de forma dinámica. ( *dhclient -r nom\_interficie* ).

Com fer que agafant NAT no canvií el ***/etc/resolv.conf*** de client ?

echo “supersede domain-name-servers 192.168.122.95 >> /etc/dhcp/dhcliend.conf

(LA IP ES LA DEL FORWARDING)

Ifdown enp1s0

Ifup enp1s0

systemctl restart networking.service

cat /etc/resolv.conf → BINGO

**Connexió via ssh:**

**ssh name\_user@IP\_servidor** per accedir-hi.

**IPs:**

IP Client: 192.168.122.**236/**24

DNS edt 192.168.122.**50**/24

DNS forwarding 192.168.122.**242**/24

DNS recursive 192.168.122.**95**/24

DNS asix primary 192.168.122.**163**/24

DNS asix secundary 192.168.122.**66**/24

**====== MAQUINA CLIENT:**

**CONFIGURACIÓ CLIENT:**

**/etc/dhcp/dhclient.conf**

option rfc3442-classless-static-routes code 121 = array of unsigned integer 8;

send host-name = gethostname();

request subnet-mask, broadcast-address, time-offset, routers,

domain-name, domain-name-servers, domain-search, host-name,

dhcp6.name-servers, dhcp6.domain-search, dhcp6.fqdn, dhcp6.sntp-servers,

netbios-name-servers, netbios-scope, interface-mtu,

rfc3442-classless-static-routes, ntp-servers;

supersede domain-name-servers 192.168.122.59;

++++++++++++++++++++++++++++++++++++++++++++++++++++++++

Ha de tenir com a servidor DNS la IP del servidor FORDWARDING.

*----- /****etc/resolv.conf*** (igual /etc/dhcp/dhcpclient.conf)

nameserver 192.168.122.242

**====== TOTS ELS SERVIDORS:**

S’instalaran les claus públiques del nostre PC a cada MV, per poder accedir-hi per ssh.

Activem la seguretat:

*-----* ***/etc/bind/named.conf.options :***

*options {*

*directory "/var/cache/bind";*

*dnssec-validation yes;*

};

**====== SERVIDOR FORWARDING:**

Té que reenviar totes les peticions de resolució cap al recursive, res més.

(en un ambient amb moltes més màquines seria un servidor DNS que actuaria com a servidor caché)

*-----* ***/etc/bind/named.conf.options***posem:

*Forwarded {*

*192.168.122.95;*

*};*

dnssec-validation yes;

**====== SERVIDOR RECURSIVE:**

------ **/etc/bind/db.recursive**, l’editem i s’ha d’afegir la IP del servidor edt:

*Zone “edt” {*

*Type: forward;*

*Forwarders 192.168.122.50;*

*};*

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

*No hem de fer res.*

Qualsevol petició de domini edt li preguntarà al servidor primari edt. Qualsevol altre petició d’un domini diferent anirà a preguntar als root servers (això es automàtic). Com no hem dit a ***/etc/bind/named.conf.options*** “*recursion no” si edt no té la resposta directa, (sobre el subdomini pregutnat) ens respondrá quí te la resposta (retorna IP del servidor qui la té), i així recursivament el servidor recursive seguirà preguntant la IP del domini buscat (a tots els DNS cap enrrera) fins a obtenir resposta,*

**====== SERVIDOR EDT:**

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

**Afegim:**

*Zone “edt” {*

*type: primary;*

*file “/etc/bind/db.edt“;*

*};*

**----- /etc/bind/db.edt**

*@ SOA dns.edt. Yo.gmail.com 1 4 4 4 4 #INDICA QUIN ËS EL DNS PRINCIPAL DEL EDT (A QUI HA DE PREGUNTAR PRIMER)*

*NS dns*

*dns A 192.168.122.50 # GLUE RECORDS (IP d’ELL MATEIX)*

*asix NS dns.asix*

*dns.asix A 192.168.122.163*

*asix NS dns2.asix*

*dns2.asix A 192.168.122.66*

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

recursion no;

**====== SERVIDOR DELEGAT ASIX PRIMARY:**

**----- /etc/bind/db.asix.edt**

@ SOA dns asix.gmail.com. 202110131 42000 400 3h 1d

NS dns

A 92.18.122.13

MX 10 aspmx.l.google.com.

dns A 192.168.122.163

$GENERATE 1-100 alumne$ A 192.168.10.$

www CNAME @

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

**Afegim:**

*Zone “asix.edt” {*

*type: primary;*

*file “/etc/bind/db.asix.edt“;*

*};*

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

*recursion no;*

**====== SERVIDOR DELEGAT ASIX SECUNDARY (REDUNDANT):**

**----- /etc/bind/db.asix.edt**

No s’ha de fer res perquè agafarà la mateixa configuració que el primary.

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

**Afegim:**

*Zone “asix.edt” {*

*type: secondary;*

*file “/var/lib/bind/db.asix.edt“;*

*Masters {*

*192.168.122.163;*

*};*

*};*

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

*recursion no;*