PRÀCTICA 5: DDNS (Dynamic Domain Name System)

1- Què és DDNS (Dynamic Domain Name System)

DDNS és un servei que permet actualitzar automàticament els registres DNS quan els equips clients d'una xarxa obtenen la seva configuració IP per mitjà d'un servidor DHCP. El responsable d'actualitzar els registres del servidor DNS serà el servidor DHCP.

Els equips clients d'un servidor DHCP envien el seu nom d'equip cada cop que demanen una adreça IP al servidor. El servidor DHCP enregistra aquest nom d'ordinador i també l'adreça IP assignada a l'equip. Si el servido DHCP té permís per modificar els registres del servidor DNS, llavors el servidor DHCP pot escriure o modificar els registres A del servidor DNS cada cop que assigna una adreça IP a un equip client.

Per poder treballar amb DDNS primer cal tenir un servidor DHPC i DNS plenament funcionals, i a continuació modificar les seves configuracions per poder muntar el sistema DDNS.

2- Configuració inicial del servidor DHCP

1- Configura el teu servidor **debian** amb l'adreça IP **192.168.1.2** i màscara **/24**. Fes que l'adreça IP del router sigui **192.168.1.1**. Fes que el servidor DNS sigui **192.168.1.2** (o sigui, ell és el seu propi servidor DNS). Fes que el domini de cerca sigui **xxxyyy.net** a on xxx són les 3 primeres lletres del teu nom i yyy són les 3 primeres lletres del teu cognom.

2- Fes que el nom del teu ordinador sigui **xxxyyy-m08.xxxyyy.net** a on on xxx són les 3 primeres lletres del teu nom i yyy són les 3 primeres lletres del teu cognom. Si no ho has fet durant la instal·lació del sistema, la manera de canviar el nom és la següent:

a) Canviar **/etc/hosts** de manera que tingui aquest contingut:

```
127.0.0.1       localhost
127.0.1.1       xxxyyy-m08.xxxyyy.net         xxxyyy-m08

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

b) Executa (com a **root**): `hostnamectl set-hostaname xxxyyy-m08.xxxyyy.net`

c) Reinicia el sistema i comprova que el nom ha canviat executant: `hostname -f`

3- Configura el servidor DHCP de manera que doni la següent configuració de xarxa als clients:
a) Servidor DHCP **autoritatiu**
b) ddns-update-style: **none**
c) Nom del domini: **xxxyyy.net**
d) Servidors DNS: **192.168.1.2**, **8.8.8.8**
e) IP del router **192.168.1.254**
f) Temps de lloguer per defecte: **1 hora**
g) Temps de lloguer màxim: **1 dia**
h) Subxarxa: **192.168.1.0 255.255.255.0**
i) Marge d'adreces IP: **192.168.1.10** a **192.168.1.250**

4- Comprova que un ordinador clients Windows i un ordinador client Ubuntu Linux poden aconseguir la configuració de xarxa per mitjà del servidor DHCP que has configurat.

3- Configuració inicial del servidor DNS

1- Configura el servidor DNS per donar servei a la zona directa **xxxyyy.net** com **DNS master**. El fitxer a on es desarà la configuració de zona és **xxxyyy.net.db**.

2- Configura el servidor DNS per donar servei a la zona inversa **1.168.192.in-addr.arpa** com **DNS master**. El fitxer a on es desarà la configuració de zona és **192.168.1.rev**.

3- Dins dels fitxer de configuració de la zona directa **xxxyyy.net.db**, només s'ha de configurar el registre **A** del propi servidor però no cal posar la dels client perquè no sabem quines poden ser les seves adreces. Així doncs, el fitxer quedaria una cosa com aquesta:

```
;
;Fitxer BIND de la zona (que inclou tot el domini) xxxyyy.net
;
$ORIGIN xxxyyy.net.
$TTL 1d
@               IN    SOA          xxxyyy-m08.xxxyyy.net.                    root.xxxyyy.net.    (
                      2018111301   ; Serial (Canvia'l per la data actual)
                      21600        ; Refresh
                      1800         ; Retry
                      604800       ;Expiry
                      900 )        ; Minimum
                IN    NS           xxxyyy-m08.xxxyyy.net.
                IN    MX           10   xxxyyy-m08.xxxyyy.net.
;A partir d'aquest punt, heu de posar els noms d'ordinadors del domini i les seves adreces IP
xxxyyy-m08      IN    A            192.168.1.2    ; Servidor DNS de xxxyyy.net
www             IN    CNAME        xxxyyy-m08     ; www és un àlies de xxxyyy-m08
mail            IN    CNAME        xxxyyy-m08     ; mail és també un àlies de xxxyyy-m08
```

4- Dins dels fitxer de configuració de la zona inversa **1.168.192**, només s'ha de configurar el registre **PTR** del propi servidor però no cal posar la dels client perquè no sabem quines poden ser les seves adreces. Així doncs, el fitxer quedaria una cosa com aquesta:

```
;
;Fitxer BIND de la zona (que inclou tot el domini) xxxyyy.net
;
$ORIGIN 1.168.192.in-addr.arpa.
$TTL 1d
@               IN    SOA          xxxyyy-m08.xxxyyy.net.                    root.xxxyyy.net.    (
                      2018111301   ; Serial (Canvia'l per la data actual)
                      21600        ; Refresh
                      1800         ; Retry
                      604800       ;Expiry
                      900 )        ; Minimum
                IN    NS           xxxyyy-m08.xxxyyy.net.
;A partir d'aquest punt, heu de posar els noms d'ordinadors del domini i les seves adreces IP
2               IN    PTR          xxxyyy-m08.xxxyyy.net   ; Servidor DNS de xxxyyy.net
```

4- Comprova que un ordinador client Windows i un ordinador client Ubuntu Linux poden fer consultes al servidor DNS utilitzant ping, host i nslookup.

4- Generació d'una clau compartida entre el servidor DNS i el servidor DHCP

a) El protcol TSIG (Transaction SIGnature) és un protocol de xarxa definit en el document RFC 2845.

b) Un dels seus propòsits principals és permetre a un servidor DNS autenticar a un altre servei com per exemple a un servidor DHCP a que realitzi actualitzacions a la seva base de dades.

c) També s'utilitza per fer actualitzacions de les bases de dades de servidors DNS slaves.

d) TSIG utilitza claus criptogràfiques secretes compartides i one-way hashing per proveir:

* Integritat dels missatges enviats entre el servidor DNS i el servidor DHCP (o també entre un DNS slave i un DNS master).
* Autènticació assegurada criptogràficament entre el servidor DNS i el servidor DHCP (o també entre un DNS slave i un DNS master).

e) Un servidor DHCP autenticat i els seus missatges si es pot assegurar la seva integritat poden ser utilitzats per realitzar actualitzacions de la base de dades DNS. Un servidor DNS master autenticat i els seus missatges si es pot assegurar la seva integritat poden ser utilitzats per realitzar actualitzacions de la base de dades DNS d'un servidor DNS slave.

f) El motiu pel qual cal utilitzar aquest protocol i claus secretes compartides és que aquestes peticions d'actualització poden arribar via un canal insegur. El servidor DHCP i el servidor DNS poden ser 2 ordinadors diferents i comunicar-se via Ethernet. Un servidor DNS master i un slave poden ser 2 equips que utilitzen Internet per comunicar-se.

f) Com a **root** i des de la teva carpeta personal de **root**, genera una clau compartida criptogràfica amb el programa **`dnssec-keygen`** de la següent manera:

```
dnssec-keygen  -a HMAC-MD5 -b 512 -r /dev/urandom -n USER CLAU_DDNS
```

A on HMAC-MD5 és l'algorisme HASH (recomanat per DDNS) utilitzat pel programa per generar la clau, 512 és la quantitat de bits de la clau, /dev/urandom és la font d'aleatorietat (l'ordinador ha de fer alguna activitat aleatòria) que cal per crear la clau,USER és el tipus de propietari (recomanat per DDNS) de la clau, i finalment CLAU_DDNS és simplement un nom que servirà com identificador de la clau.

g) Comprova que s'han creat dos fitxers:

Kclau_ddns.+157+nnnnn.key (116 bytes de mida, propietat de root i permisos r w - - - - - - -)
Kclau_ddns.+157+nnnnn.private (229 bytes de mida, propietat de root i permisos r w - - - - - - -)

A on **nnnnn** és una combinació qualsevol de 5 números que serveix com un número identificador de la clau.

h) El fitxer **Kclau_ddns.+157+nnnnn.key** té un registre tipus DNS KEY que s'ha d'insertar en el fitxer de zona (en el nostre cas normalment a **/etc/bind/named.conf.local**) directament o amb un **include**.

i) El fitxer **Kclau_ddns.+157+nnnnn.private** té diversos camps de dades que estan relacionades amb l'algorisme HASH utilitzat i també un camp anomenat **Key** a on també es pot veure el registre DNS KEY que s'ha d'utilitzar.

j) Tots 2 fitxers són de tipus text i llegibles només pel propietari, que en aquest cas és l'usuari **root**.

5- Configuració del servidor DNS per treballar amb DDNS

a) Per poder treballar amb la clau criptogràfica compartida que hem creat a l'apartat anterior, primer hem de saber el seu valor. Executa:

```
cat  Kclau_ddns.+157+nnnnn.private | grep "Key" | cut -d " " -f 2
```

i mostra la clau. Recorda que nnnnn és una combinació de 5 números que hi ha al nom del fitxer.

Per exemple:

En aquest exemple la clau criptogràfica compartida és:

```
Ie9kUxFzZZc1ZjKezWVQ1eiUbKi00+3MZrAZ3UpMEgBTdBvLqG4qbMykaaDXNPe8bzzZiT9TtjP0qLRr8MygQA==
```

b) Ara, amb **nano** i com a **root**, hem de crear un fitxer de nom **clau_ddns.key** dins del directori **/etc/bind** a on desar aquesta clau perquè pugui ser utilitzada pel servidor DNS. El contigut del fitxer serà aquest:

```
key CLAU_DDNS {
  algorithm HMAC-MD5.SIG-ALG.REG.INT;
  secret "Ie9kUxFzZZc1ZjKezWVQ1eiUbKi00+3MZrAZ3UpMEgBTdBvLqG4qbMykaaDXNPe8bzzZiT9TtjP0qLRr8MygQA==";
};
```

c) Farem que el grup amb permisos especial sobre el fitxer **clau_ddns.key** sigui **bind**, i que el grup tingui permís només de **lectura**. Així, el servidor DNS podrà llegir la clau però no canviar-la per equivocació. La resta **d'usuaris** evidentment no haurien de poder llegir aquest fitxer de manera que **no poden tenir cap permís**. Evidentment, **root** ha de ser el propietari amb permís de **lectura** i **escriptura** per poder fer canvis si cal. Així doncs, farem això:

d) Ara configurarem el servidor DNS perquè afegeixi el contingut d'aquest fitxer a la seva configuració, i d'aquesta manera, afegir la clau criptogràfica compartida a la seva configuracio. Això s'ha de fer dins dels fitxer **/etc/bind/named.conf.local** amb una directiva **include**. Així doncs, el fitxer quedarà d'aquesta manera:

```
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

include "/etc/bind/clau_ddns.key";

zone "dacomo.net" {
        type master;
        notify no;
        file "dacomo.net.db";
        allow-update {
                key CLAU_DDNS;
        };
};

zone "1.168.192.in-addr.arpa" {
        type master;
        notify no;
        file "192.168.1.rev";
        allow-update {
                key CLAU_DDNS;
        };
};
```

Aquest un exemple a on **xxxyyy.net** és **dacomo.net**. S'ha afegit l'opció **notify no** per optimitzar les prestacions del servei. Només estem treballant dins d'una xarxa privada i amb **notify no** evitem que es generin missatges extra de notificació de la configuració local cap servidors DNS externs. Però això és un extra , si ho volem, podem esborrar la linia.

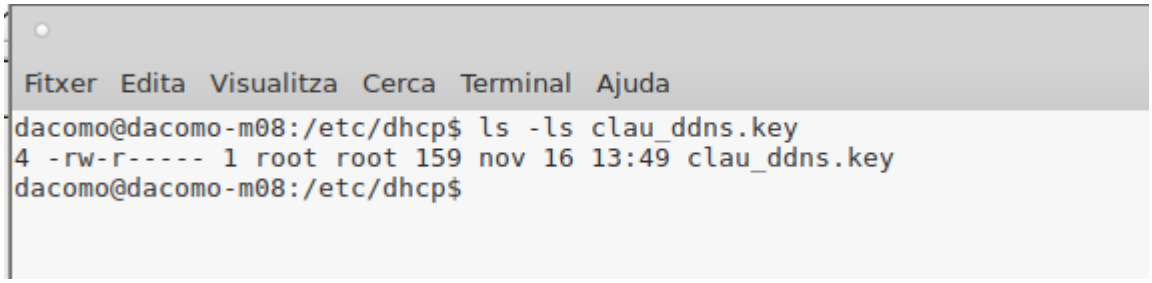
e) Reinicia el servidor i comprova que funciona correctament.

6- Configuració del servidor DHCP per treballar amb DDNS

a) Ara hem de configurar el servidor DHCP perquè afegeixi/canviï els registres de la base de dades DNS cada cop que assgina una adreça IP a un client aprofitant el fet que durant l'intercanvi de missatges del protocol DHCP, el client envia al servidor el seu nom d'equip. Primer hem de modificar la configuració del servidor DHCP i afegir o modifcar els següents paràmetres:

* Paràmetre **ddns-updates** --> El seu valor ha de ser **on**
*Paràmetre **ddns-update-style** --> Valors que pot tenir **none/interim/adhoc/standard**. El valor **adhoc** avui dia està desfasat. El recomanat, més modern i més adaptat a RFC és el tipus **standard**.

b) El servidor **DHCP** haurà d'utilitzar la clau criptogràfica compartida que es va crear a l'apartat **4** i que es troba al fitxer **clau_ddns.key** que es va crear a l'apartat **5.b**. Només cal copiar el fitxer dins del directori **/etc/dhcp** però el grup millor que sigui **root** perqué el servei **DHC**P s'executa amb els permisos de **root**.



i caldrà amb un **include** afegir aquesta clau al fitxer de configuració del servidor DHCP de la següent manera: `include "/etc/dhcp/clau_ddns.key";`

c) També cal configurar el servidor DHCP per indicar quina zona DNS s'ha d'actualitzar i quin és el servidor DNS. Dins del fitxer de configuració es pot afegir aquesta informació de la següent manera (amb un exemple pel domini dacomo.net):

```
zone dacom.net. {
  primary 192.168.1.2;
  key DDNS_UPDATE;
}
zone 1.168.192.in-addr.arpa. {
  primary 192.168.1.2;
  key DDNS_UPDATE;
}
```

d) En resum, la configuració del servidor DHCP (si treballen amb el domini dacomo.net) seria aquesta:

```
#
# INCLUDES
#
include "/etc/dhcp/clau_ddns.key";
#
# CONFIGURACIÓ BÀSICA
#
authoritative;
option domain-name "dacomo.net";
option domain-name-servers 192.168.1.2, 8.8.8.8;
option routers 192.168.1.254;
default-lease-time 7200;
max-lease-time 86400;
subnet 192.168.1.0 netmask 255.255.255.0 {
        range 192.168.1.10 192.168.1.250;
}
```

```
#
# CONFIGURACIÓ DDNS
#
ddns-updates on;
ddns-update-style standard;
zone dacomo.net. {
        primary 192.168.1.2;
        key CLAU_DDNS;
}
zone  1.168.192.in-addr.arpa. {
        primary 192.168.1.2;
        key CLAU_DDNS;
}
```

e) Reinicia el servidor i comprova que funciona correctament.

7- Comprovacions

a) Comprova que dins del directori **/var/cache/bind** no existeix cap fitxer amb extensió **.jnl**.

b) Assegura't que els fitxer **xxxyyy.net.db** i **192.168.1.rev** només tenen el contingut introduït a l'apartat 3.

c) Posa en marxa un client **Windows** i un client **Ubuntu** amb configuració de xarxa via DHCP. Comprova:

* Els seus noms.
* Que han obtingut una configuració de xarxa donada pel servidor DHCP
* Que poden fer pings a **xxxyyy-m08.xxxyyy.net**, **www.xxxyyy.net** i **mail.xxxyyy.net** .

d) Accedeix al directori /var/cache/bind. Comprova que han aparegut dos fitxers **.jnl**. Un seria el fitxer **xxxyyy.net.db.jnl** i l'altre **192.168.1.rev.jnl**.

e) Comprova que des de Windows pots fer un ping a l'ordinador Ubuntu utilitzant el nom de l'ordinador Ubuntu. Comprova que des d'Ubuntu pots fer un ping a l'ordinador Windows utilitzant el nom de l'ordinador Windows.

f) Comprova que pots fer una consulta amb l'ordre host des d'Ubuntu i trobar l'adreça IP de Windows, i que pots fer una consulta amb l'ordre nslookup des de Windows i trobar l'adreça IP d'Ubuntu.