

## NF2 – EL SERVEI DNS || UF1: DNS I DHCP

---

### PROJECTE 1 – ETAPA 2 – REVERSES I CONFIGURACIONS DE SERVEI

---

NOM DE L'ALUMNE/s: Nil Massó

#### OBJECTIU

- Configurar la zona reversa pel rang preassignat de cada estudiant i treballar amb diferents modes de configuració del servei DNS.

#### INSTRUCCIONS

- Aquesta etapa té un valor del 20% sobre la nota final del projecte.
- Cal continuar utilitzant el que hem preparat a l'etapa anterior del projecte.
- De totes maneres, us aconsello fer un *snapshot* com a punt de partida de l'etapa.
- Per defecte, cal que justifiqueu les respostes amb captures de pantalla.
- Si a la captura no hi ha cap valor que la identifiqui de forma única, cal que es vegi el fons d'escriptori, *notepad* o eines similars amb el vostre nomcognom!
- Totes les captures que mostrin les comandes han d'incloure, a part del resultat, la comanda i/o els paràmetres, per tal de veure com la feu.

---

Seguim amb el projecte i en aquesta segona etapa ens basarem principalment a la configuració d'una zona reversa pel vostre rang particular d'IPs, fer-hi comprovacions i treballar amb alguns modes de configuració del servei DNS.

Així doncs, el primer que caldrà fer és definir la reversa per la vostra zona 172.25.X.0/16, i com servidor DNS autoritatiu on crear-la utilitzarem la Ubuntu Server.

- a Per tal que funcioni, haureu d'indicar-li al BIND que sigui autoritatiu i primari per la zona DNS corresponent pel vostre rang de xarxa. Adjunteu una captura amb el valor d'executar la comanda [sudo cat /etc/bind/named.conf.local | grep . | grep -v ^/ ]. 1 punt.

```
root@us-nmc:/etc/bind# sudo cat /etc/bind/named.conf.local | grep . | grep -v ^/
/
zone "nilmasso.edu" {
    type master;
    file "/var/cache/bind/db.nilmasso.edu";
};
zone "35.25.172.in-addr.arpa" {
    type master;
    file "/var/cache/bind/db.35.25.172";
};
```

Un cop fet, caldrà preparar el fitxer de zona amb el seu corresponent contingut. Per això caldrà que tingueu en compte que haureu de configurar el SOA, excepte la part de *option-slaves*, que la podeu deixar amb els valors numèrics per defecte.

Pel SOA, el seu autoritatiu ha de ser ns1.nomcognom.edu i el correu el vostre, i com a NS també només ha de constar ns1.nomcognom.edu.

A nivell d'entrades PTR cal que genereu les següents:

- www.nomcognom.edu: 172.25.X.5
- webmail.nomcognom.edu: 172.25.X.20
- mail.nomcognom.edu: 172.25.X.55
- olot.cognomnom.edu: 172.25.X.133
- ripoll.cognomnom.edu: 172.25.X.166
- figueres.cognomnom.edu: 172.25.X.199

on evidentment substituïu la X pel vostre rang assignat, i nomcognom, i cognomnom pels vostres en cada cas.

- b Adjunteu una captura amb els valors del fitxer de zona reversa. 2 punts.

Captura de la zona directa, he seguit l'exemple i deia que s'havia de fer la directa, però a internet deia que a la inversa es posava a darrera de cada alinea ; i la ip enlloc de fer una directa.

```
$TTL 6h
@      IN      SOA      ns1.nilmasso.edu. nmasso.nilmasso.edu. (
                                2016101902 ; Serial
                                6h ; Refresh
                                1h ; Retry
                                1w ; Expire
                                1h ) ; Minimum TTL

;
@      IN      NS       ns1.nilmasso.edu.
www    IN      A        172.25.35.5
webmail IN      A        172.25.35.20
mail   IN      A        172.25.35.55
olot   IN      A        172.25.35.133
ripoll IN      A        172.25.35.166
figueres IN      A      172.25.35.199
```

```
$TTL 6h
@      IN      SOA      ns1.nilmasso.edu. nmasso.nilmasso.edu. (
                                2016101901 ; Serial
                                6h ; Refresh
                                1h ; Retry
                                1w ; Expire
                                1h ) ; Minimum TTL

;
@      IN      NS       ns1.nilmasso.edu.
5      IN      PTR      www.nilmasso.edu.
20     IN      PTR      webmail.nilmasso.edu.
55     IN      PTR      mail.nilmasso.edu.
133    IN      PTR      olot.massonil.edu.
166    IN      PTR      ripoll.massonil.edu.
199    IN      PTR      figueres.massonil.edu.
```

Un cop activat, tocarà fer comprovacions de funcionament.

- c Adjunteu una captura de la consulta del registre SOA per la vostra reversa utilitzant la comanda 'dig'. *1 punt.*

```
root@us-nmc:/var/cache/bind# dig nilmasso.edu. @localhost SOA

; <<>> DiG 9.18.1-lubuntu1.2-Ubuntu <<>> nilmasso.edu. @localhost SOA
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43537
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 31bb4ce7ea33a61b0100000063556458b65653cf588a7760 (good)
;; QUESTION SECTION:
;nilmasso.edu.                IN      SOA

;; ANSWER SECTION:
nilmasso.edu.                21600   IN      SOA      ns1.nilmasso.edu. nmasso.nilmass
o.edu. 2016101902 21600 3600 604800 3600

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(localhost) (UDP)
;; WHEN: Sun Oct 23 15:57:12 UTC 2022
;; MSG SIZE rcvd: 116
```

- d També adjunteu una captura de la consulta del valor 172.25.X.199. Utilitzeu la comanda que vulgueu. *1 punt.*

Tampoc dona resposta

```
root@us-nmc:/var/cache/bind# dig -x 172.25.35.199 @localhost

; <<>> DiG 9.18.1-lubuntu1.2-Ubuntu <<>> -x 172.25.35.199 @localhost
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48142
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 1c2a7e81110ed75b0100000063556f2effb086a92c66d869 (good)
;; QUESTION SECTION:
;199.35.25.172.in-addr.arpa.  IN      PTR

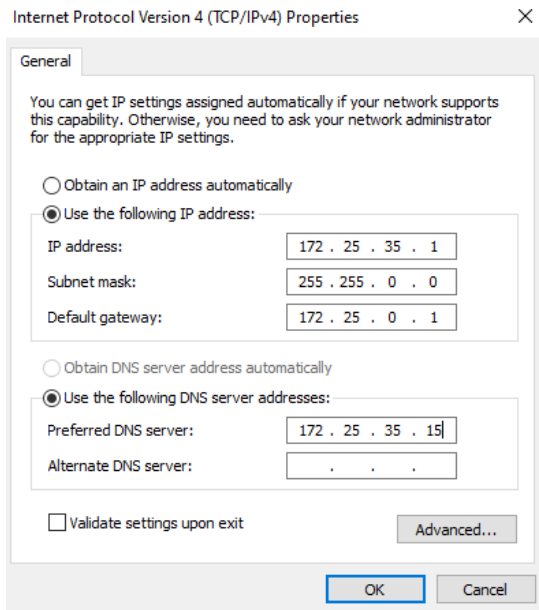
;; ANSWER SECTION:
199.35.25.172.in-addr.arpa. 21600   IN      PTR      figueres.massonil.edu.

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(localhost) (UDP)
;; WHEN: Sun Oct 23 16:43:26 UTC 2022
;; MSG SIZE rcvd: 118
```

Ara treballarem amb el Windows. No té massa sentit que allà hi hagi la zona inversa novament creada, i ara mateix només hem definit un únic NS pel que no pot actuar de secundari. Així doncs, quan se li facin peticions sobre la reversa, no les resoldrà.

No obstant, cal que configureu el Windows perquè tingui el servei DNS de la Ubuntu Server com a *forwarding* i així les consultes que rebi sobre les reserves les passarà al Linux i hauria d'obtenir-ne resposta.

- e Adjunteu doncs una captura del Windows Server conforme té la IP de la Ubuntu Server com a servidor on reenviar les peticions DNS. *1 punt.*



Per demostrar que funciona correctament, caldrà que feu una comprovació en dos parts. Per una banda activeu el *tcpdump* a la Ubuntu Server per tal que faci *d'sniffer* sobre el port DNS i per l'altra feu una consulta DNS al Windows Server.

- f Així doncs, adjunteu dues captures: la primera, des de la Ubuntu Server, llançant la comanda [sudo tcpdump -i any -n port 53 and udp], que permetrà veure el trànsit DNS que passi per la Ubuntu, i l'altra, un nslookup al Windows Server per tal de consultar la IP 172.25.X.166. Evidentment, la de Linux ha de mostrar el contingut de dades que genera la consulta client al Windows. *1,5 punts.*

```
root@us-nmc:/var/cache/bind# tcpdump -i any -n port 53 and udp
tcpdump: data link type LINUX_SLL2
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144 bytes
18:42:03.316604 ens3 In IP 172.25.35.1.55655 > 172.25.35.15.53: 1+ PTR? 15.35.25.172.in-addr.arpa. (43)
18:42:03.316994 ens3 Out IP 172.25.35.15.53 > 172.25.35.1.55655: 1 NXDomain* 0/1/0 (102)
18:42:03.319174 ens3 In IP 172.25.35.1.55656 > 172.25.35.15.53: 2+ PTR? 166.35.25.172.in-addr.arpa. (44)
18:42:03.319570 ens3 Out IP 172.25.35.15.53 > 172.25.35.1.55656: 2* 1/0/0 PTR ripoll.massonil.edu. (77)

C:\Users\Administrator>nslookup 172.25.35.166
Server: UnKnown
Address: 172.25.35.15

Name: ripoll.massonil.edu
Address: 172.25.35.166
```

- g Tot seguit, adjunteu una captura de la comanda 'dig' consultant el nom DNS ns1.nomcognom.edu a la Ubuntu Server. *1 punt.*

```

root@us-nmc:/var/cache/bind# dig ns1.nilmasso.edu @localhost

; <<>> DiG 9.18.1-1ubuntu1.2-Ubuntu <<>> ns1.nilmasso.edu @localhost
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49777
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 746137f7c49433920100000063558dd9db20aca1a1bce112 (good)
;; QUESTION SECTION:
;ns1.nilmasso.edu.                IN      A

;; ANSWER SECTION:
ns1.nilmasso.edu.                21600   IN      A      172.25.35.15

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(localhost) (UDP)
;; WHEN: Sun Oct 23 18:54:17 UTC 2022
;; MSG SIZE rcvd: 89

```

Per acabar, heu de configurar el Windows Server i la Ubuntu Server per tal que no responguin peticions que no tinguin ells com autoritatives (per tant als dominis actius i la reversa si), com per exemple, si pregunteu sobre sapalomera.cat. Us adjunto un parell de captures conforme el que us hauria de sortir quan ho tingueu realitzat.

```

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 7323
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

```

```
no encuentra sapalomera.cat: Server failed
```

- h Adjunteu les explicacions i captures corresponents del que heu canviat, configurat, activat, etc. per tal de que els servidors DNS es comportin de la manera indicada. *1,5 punts.*

Al Windows: Eliminem qualsevol forwarder o configuració de dns del adaptador. Seguidament anem a propietats del server dns i activem la deshabilitació de la recursió i eliminem tots els root servers

