

### PROJECTE 1 – ETAPA 3 – SISTEMA DNS MESTRE/ESCLAU

NOM DE L'ALUMNE/s: Nil Massó

#### OBJECTIU

- Configurar i treballar sota un sistema DNS mestre/esclau complet i sota diferents opcions de funcionament.

#### INSTRUCCIONS

- Aquesta etapa té un valor del 60% 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.

Ara que ja tenim els dominis de nomcognom.edu i cognomnom.edu activats a nivell de DNS als diferents servidors configurats com a rols primaris, caldrà que els reconfigureu perquè facin de primari-secundari entre ells.

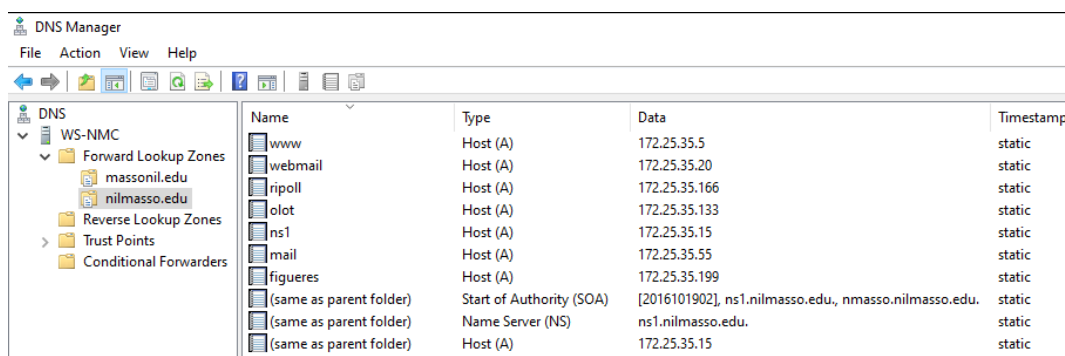
D'aquesta manera doncs, cal que configureu el Windows Server perquè faci de secundari de nomcognom.edu, i la Ubuntu Server perquè ho faci de cognomnom.edu.

Novament, a nivell de xarxa, seguirem treballant amb un adaptador en mode 'xarxa NAT' associat al rang preassignat que teniu pel MP.

Primer de tot, comencem amb nomcognom.edu i per tant, heu de fer els corresponents canvis als servidors DNS per tal que el Windows Server la serveixi com autoritatiu secundari.

- a Adjunteu les captures que demostren que la zona de nomcognom.edu al Windows Server està configurada com a secundaria i quin servidor mestre té configurat. *0,5 punts*.

T'adjunto captures de tot per si veus alguna cosa que no s'avalua, però que potser està malament igualment i me la pots comentar si tens temps, gràcies.



DNS	Name	Type	Data	Timestamp
WS-NMC	www	Host (A)	172.25.35.5	static
Forward Lookup Zones	webmail	Host (A)	172.25.35.20	static
massonil.edu	ripoll	Host (A)	172.25.35.166	static
nilmasso.edu	olot	Host (A)	172.25.35.133	static
Reverse Lookup Zones	ns1	Host (A)	172.25.35.15	static
Trust Points	mail	Host (A)	172.25.35.55	static
Conditional Forwarders	figueres	Host (A)	172.25.35.199	static
	(same as parent folder)	Start of Authority (SOA)	[2016101902], ns1.nilmasso.edu., nmasso.nilmasso.edu.	static
	(same as parent folder)	Name Server (NS)	ns1.nilmasso.edu.	static
	(same as parent folder)	Host (A)	172.25.35.15	static

nilmasso.edu Properties

nilmasso.edu Properties

Name Servers WINS Zone Transfers

General Start of Authority (SOA)

Status: Running Pause

Type: Secondary Change...

Replication: Not an Active Directory-integrated zone Change...

Zone file name:  
nilmasso.edu.

Master Servers:

IP Address	Server FQDN
172.25.35.15	<Unable to resolve>

nilmasso.edu Properties

nilmasso.edu Properties

Name Servers WINS Zone Transfers

General Start of Authority (SOA)

Serial number:  
2016101902 Increment

Primary server:  
ns1.nilmasso.edu. Browse...

Responsible person:  
nmasso.nilmasso.edu. Browse...

Refresh interval: 6 hours

Retry interval: 1 hours

Expires after: 7 days

Minimum (default) TTL: 1 hours

TTL for this record: 0 :6 :0 :0 (DDDD:HH.MM.SS)

OK Cancel Apply Help

nilmasso.edu Properties

nilmasso.edu Properties

General Start of Authority (SOA)

Name Servers WINS Zone Transfers

A zone transfer sends a copy of the zone to the servers that request a copy.

☒ Allow zone transfers:

- ☒ To any server
- ☐ Only to servers listed on the Name Servers tab
- ☐ Only to the following servers

IP Address	Server FQDN
------------	-------------

Edit

To specify secondary servers to be notified of zone updates, click Notify. Notify...

OK Cancel Apply Help

nilmasso.edu Properties

nilmasso.edu Properties

General Start of Authority (SOA)

Name Servers WINS Zone Transfers

To add name servers to the list, click Add.

Name servers:

Server Fully Qualified Domain Name (FQDN)	IP Address
ns1.nilmasso.edu.	[172.25.35.15]

- b Tot seguit, adjunteu una captura dels logs de la Ubuntu Server que demostrin la transferència completa de zona entre els dos servidors. *1 punt.*

```
root@us-nmc:~# sudo tail -f /var/log/syslog
Dec 28 11:54:42 us-nmc named[1940]: client @0x7fe5a00350e8 172.25.35.1#53300 (nilmasso.edu): transfer of 'nilmasso.edu/IN': AXFR started (serial 2016101902)
Dec 28 11:54:43 us-nmc named[1940]: client @0x7fe5a00350e8 172.25.35.1#53300 (nilmasso.edu): transfer of 'nilmasso.edu/IN': starting maxtime timer 7200000 ms
Dec 28 11:54:43 us-nmc named[1940]: client @0x7fe5a00350e8 172.25.35.1#53300 (nilmasso.edu): transfer of 'nilmasso.edu/IN': AXFR ended: 1 messages, 11 records, 293 bytes, 0.001 secs (293000 bytes/sec) (serial 2016101902)
```

- c Ara, utilitzant nslookup (des d'un client Windows o des del propi Windows Server) feu una consulta DNS sobre l'entrada nord.nomcognom.edu i que la consulta es faci al servei DNS del Windows Server. *0,75 punts.*

Crec recordar que això estava malament, ja que nord era dels exercicis no del projecte, suposant això tu substitueixo per un registre que si que esta al windows

DNS Manager

File Action View Help

DNS		Name	Type	Data
WS-NMC	Forward Lookup Zones	www	Host (A)	172.25.35.200
	massonil.edu	ws-nmc	Host (A)	172.25.35.1
	nilmasso.edu	us-nmc	Host (A)	172.25.35.15
	Reverse Lookup Zones	ripoll	Host (A)	172.25.35.166
	Trust Points	olot	Host (A)	172.25.35.133
	Conditional Forwarders	mail	Host (A)	172.25.35.31
		figueres	Host (A)	172.25.35.199
		correu	Host (A)	172.25.35.30
		blanes	Alias (CNAME)	www.massonil.edu.
		(same as parent folder)	Start of Authority (SOA)	[38], ws-nmc.massonil.edu...
		(same as parent folder)	Name Server (NS)	ws-nmc.massonil.edu.
		(same as parent folder)	Name Server (NS)	us-nmc.massonil.edu.
		(same as parent folder)	Host (A)	172.25.35.1
		(same as parent folder)	Mail Exchanger (MX)	[25] mail.massonil.edu.
		(same as parent folder)	Mail Exchanger (MX)	[50] correu.massonil.edu.

```
C:\Users\Administrator>nslookup ripoll.massonil.edu 172.25.35.1
Server: UnKnown
Address: 172.25.35.1

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

Ara configurar el servei DNS de la Ubuntu Server per tal que actuï com a *slave* del domini cognomnom.edu. `

- d Un cop fet els canvis corresponents, adjunteu una captura de llançar la comanda [sudo cat /etc/bind/named.conf.local | egrep -v ^// | grep .]. 1,25 punts.

```
root@us-nmc:~# cat /etc/bind/named.conf.local | egrep -v ^// | grep .
zone "nilmasso.edu" {
    notify no;
    type master;
    file "/var/cache/bind/db.nilmasso.edu";
};
zone "172.25.35.in-addr.arpa" {
    type master;
    file "/var/cache/bind/db.35.25.172";
};
zone "massonil.edu" {
    type slave;
    file "/var/cache/bind/db.massonil.edu";
masters { 172.25.35.1; };
};
```

- e Adjunteu una captura dels logs DNS del Windows Server conforme s'ha executat el procés de transferència, primer, amb l'enviament del SOA i després, amb la transferència completa pròpiament dita. 0,75 punts.

No he trobat l'enviament del soa

Information	28/12/2022 12:54:43	DNS-Server-Service	6522	None
Information	28/12/2022 12:53:37	DNS-Server-Service	6001	None
Information	28/12/2022 12:38:39	DNS-Server-Service	3150	None

Event 6522, DNS-Server-Service

General Details

A more recent version, version 2016101902 of zone nilmasso.edu was found at the DNS server at 172.25.35.15. Zone transfer is in progress.

Log Name: DNS Server  
Source: DNS-Server-Service  
Event ID: 6522  
Level: Information  
User: SYSTEM  
OpCode: Info  
More Information: [Event Log Online Help](#)

Logged: 28/12/2022 12:54:43  
Task Category: None  
Keywords: (4)  
Computer: WS-NMC

- f Utilitzant nslookup, feu una consulta a la Ubuntu Server per tal d'obtenir el valor de figueres.cognomnom.edu. 0,75 punts.

```
root@us-nmc:~# nslookup figueres.massonil.edu 172.25.35.1
Server:          172.25.35.1
Address:         172.25.35.1#53

Name:   figueres.massonil.edu
Address: 172.25.35.199
```

Un cop tinguem els dos dominis amb serveis de primari-secundari, és el moment de fer canvis a les zones DNS i veure com aquestes es propaguen automàticament als seus secundaris.

Començarem pel Windows Server, i farem un canvi a la zona de `cognomnom.edu` per tal d'afegir l'entrada `projecte.cognomnom.edu` i que quedi associada a la IP `172.25.X.245`.

- h Adjunteu una captura dels logs del servei `named` de la Ubuntu Server conforme es veu com arriba el `notify` des del Windows Server i es produeix la transferència de la zona de domini. *1 punt.*

```
Dec 28 23:01:27 us-nmc named[717]: client @0x7f6648001e28 172.25.35.1#61069: received notify for zone 'massonil.edu'
Dec 28 23:01:27 us-nmc named[717]: zone massonil.edu/IN: notify from 172.25.35.1#61069: serial 39
Dec 28 23:01:27 us-nmc named[717]: zone massonil.edu/IN: Transfer started.
Dec 28 23:01:27 us-nmc named[717]: transfer of 'massonil.edu/IN' from 172.25.35.1#53: connected using 172.25.35.1#53
Dec 28 23:01:27 us-nmc named[717]: zone massonil.edu/IN: transferred serial 39
Dec 28 23:01:27 us-nmc named[717]: transfer of 'massonil.edu/IN' from 172.25.35.1#53: Transfer status: success
Dec 28 23:01:27 us-nmc named[717]: transfer of 'massonil.edu/IN' from 172.25.35.1#53: Transfer completed: 1 messages, 5 records, 226 bytes, 0.020 secs (11300 bytes/sec) (serial 39)
Dec 28 23:01:27 us-nmc named[717]: zone massonil.edu/IN: sending notifies (serial 39)
Dec 28 23:01:57 us-nmc named[717]: client @0x7f6640028ca8 172.25.35.1#59678: received notify for zone 'massonil.edu'
Dec 28 23:01:57 us-nmc named[717]: zone massonil.edu/IN: notify from 172.25.35.1#59678: zone is up to date
```

- i Ara cal comprovar amb la comanda `'dig'` i fent la consulta a la Ubuntu Server, quin és el valor de `projecte.cognomnom.edu`. *0,5 punts.*

```
root@us-nmc:~# dig projecte.massonil.edu @localhost

; <<>> DiG 9.18.1-1ubuntu1.2-Ubuntu <<>> projecte.massonil.edu @localhost
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63327
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 337e5dbf463c08800100000063accb456a613d909b3d66b6 (good)
;; QUESTION SECTION:
;projecte.massonil.edu.      IN      A

;; ANSWER SECTION:
projecte.massonil.edu.  32400   IN      A      172.25.35.245

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(localhost) (UDP)
;; WHEN: Wed Dec 28 23:03:33 UTC 2022
;; MSG SIZE rcvd: 94
```

Ara ens tocarà fer-ho a la Ubuntu Server, de forma que ens caldrà crear l'entrada `projecte.nomcognom.edu` apuntant a la IP `172.25.X.245`. Si tot va com espero que vagi, la zona no s'haurà propagat al Windows.

- j Investigueu perquè i solucioneu-ho. Podeu fer qualsevol tipus de canvi que necessiteu (de configuració, de funcionament, de valors a les zones DNS, etc.). Tot ha de quedar explicat i justificat amb les corresponents captures i si ho arregleu, cal acabar amb una consulta DNS final sobre el Windows Server demostrant que resol de forma Autoritativa `projecte.nomcognom.edu`. *1,5 punts.*

Amb la configuració actual, el nostre BIND no hauria de resoldre cap consulta que no sigui dirigida a un dels dominis dels quals n'és autoritatiu, ja

sigui com a primari o com a secundari. No obstant, ens interessa que ens resolgui peticions de qualsevol domini, però per tenir-ho controlat, només si aquestes peticions venen des del Windows Server, ja que aquest darrer té la Ubuntu Server configurada com a *forwarder* en etapes anteriors.

Així doncs, realitzeu els canvis convenients a la configuració del BIND per tal que s'accepti recursivitat però només si prové de peticions que venen del Windows Server.

k Caldrà que adjunteu diferents captures (1,5 punts):

- Captures dels fitxers de configuració editats i indiqueu quins canvis heu fet.
- `nano /etc/bind/named.conf.options`

```
recursion no;  
allow-recursion { 172.25.35.1; };  
allow-query { any; };  
forwarders { 8.8.8.8; };
```

- També caldrà una captura conforme es fa una petició sobre un domini extern (grn.es per exemple) des del Windows Server al BIND i aquesta es resol. Quan feu la petició, heu de tenir l'*sniffer* engegat a la Ubuntu Server amb la comanda [sudo tcpdump -i any -n port 53 and udp].  
Em surt refused no entenc perquè, si torno a activar recursion igualment em surt server failed tot i que té el dns de google com a forwarded.
- Captura conforme si feu la petició (amb dig) des de la Ubuntu Client a la IP de la Ubuntu Server i aquesta us dona 'Refused'. Mantingueu l'*sniffer* obert aquí també.  
També dona refused, però entenc que si l'altra dona vol dir que no està permetent de enlloc per tant està malament.
- Adjunteu la captura dels valors de l'*sniffer* també (hi ha de constar la petició des del Windows i la directa des de la Ubuntu Server).

Per acabar, cal que configureu la Ubuntu Server per tal que només accepti peticions (*queries*) des del Windows Server, fins i tot pels seus dominis autoritatius, tant si és primari com secundari.

l Adjunteu captures dels canvis fets als arxius de configuració del BIND i una demostració de petició amb 'dig' des de la Ubuntu Client conforme voleu saber els NS de cognomnom.edu. 0,5 punts.

`nano /etc/bind/named.conf.options`  
`allow-query { 172.25.35.1; };`