

## Práctica A3.P1: Servicio DNS en Windows Server

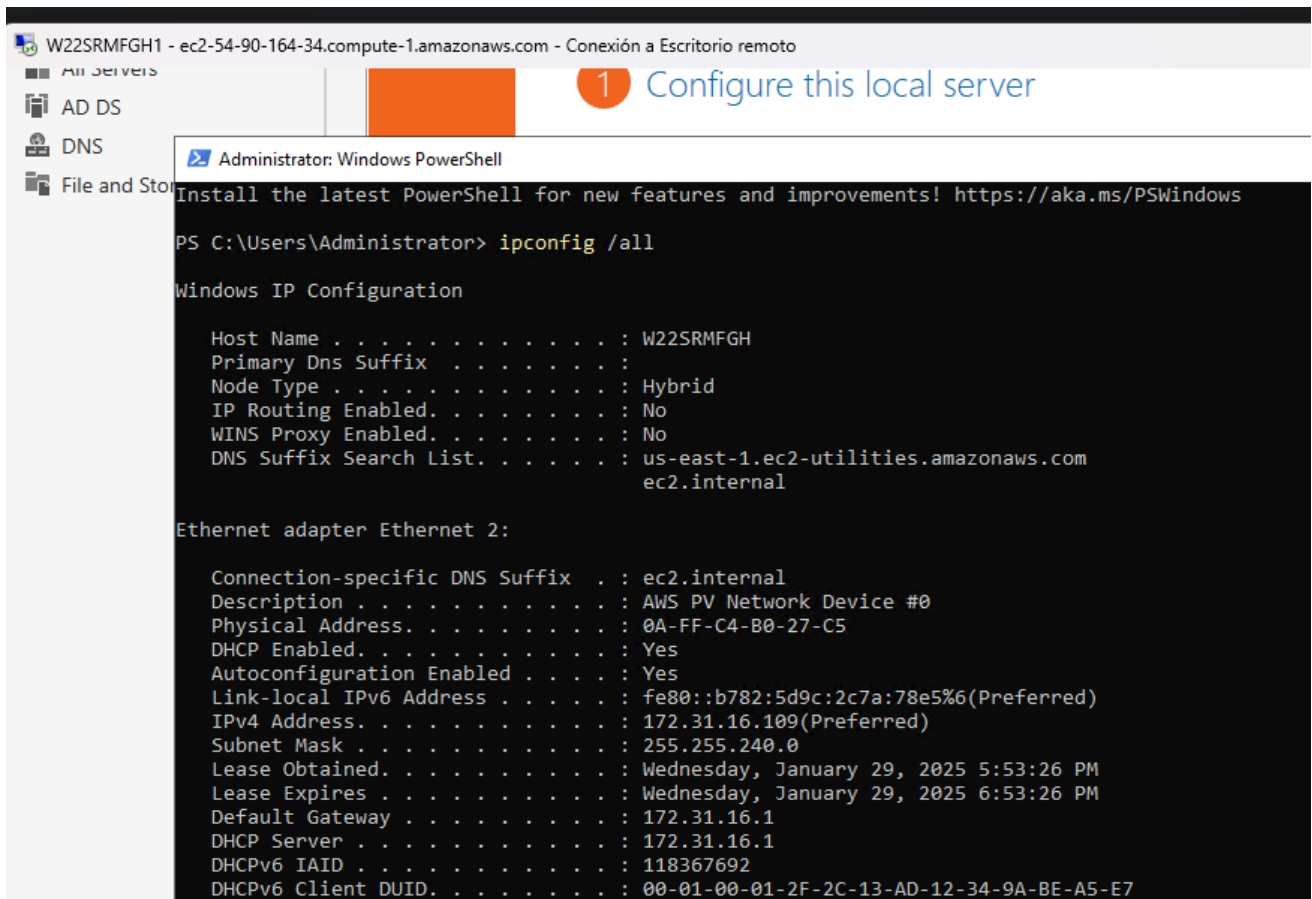
En esta práctica vamos a realizar la instalación y configuración del servicio DNS en un servidor Windows Server 2022 según las instrucciones presentadas.

Nuestro servidor Windows será una instancia EC2 que tendrá como nombre **W22SRXXX**. Será accesible desde internet por medio de la dirección IP pública de la VPC de AWS. No es necesario vincularle una IP elástica. Se recomienda utilizar una EC2 tipo *medium* con 4GB de RAM. Tenéis que mostrar una captura con la ejecución de `ipconfig /all` en la instancia. También debéis modificar el `hostname` a **W22SRXXX**. (1 pto.)

The screenshot shows the 'Launch Instance' wizard in the AWS Management Console. The 'Name and tags' section has the name 'W22SRMFGH'. The 'Images' section shows 'Microsoft Windows Server 2022' as the selected AMI. The 'Instance type' is 't2.medium'. The 'Summary' section on the right shows the configuration details and a 'Launch Instance' button.

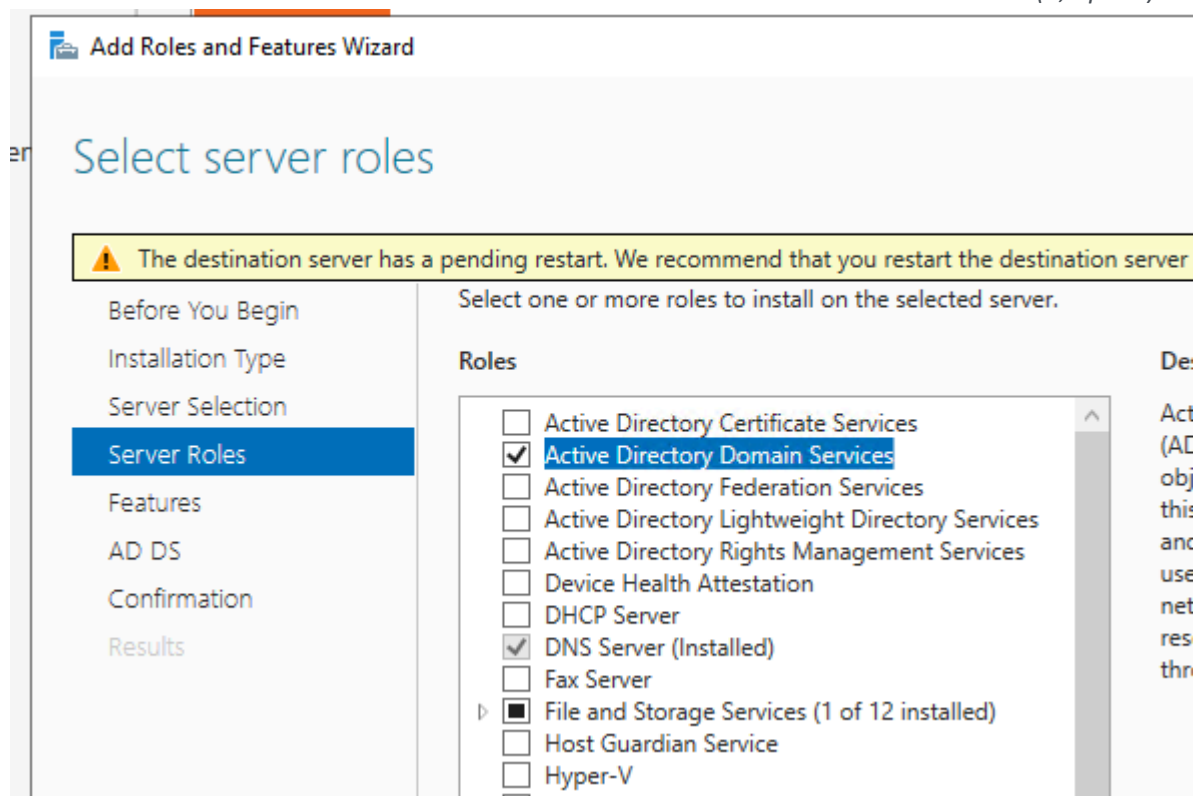
The screenshot shows the 'Edit Inbound Rules' page for the instance. It lists three inbound rules: RDP (TCP, port 3389), DNS (UDP, port 53), and DNS (TCP, port 53). Each rule has a '0.0.0.0/0' source IP range and an 'Anywh...' source type. There are 'Eliminar' buttons for each rule.

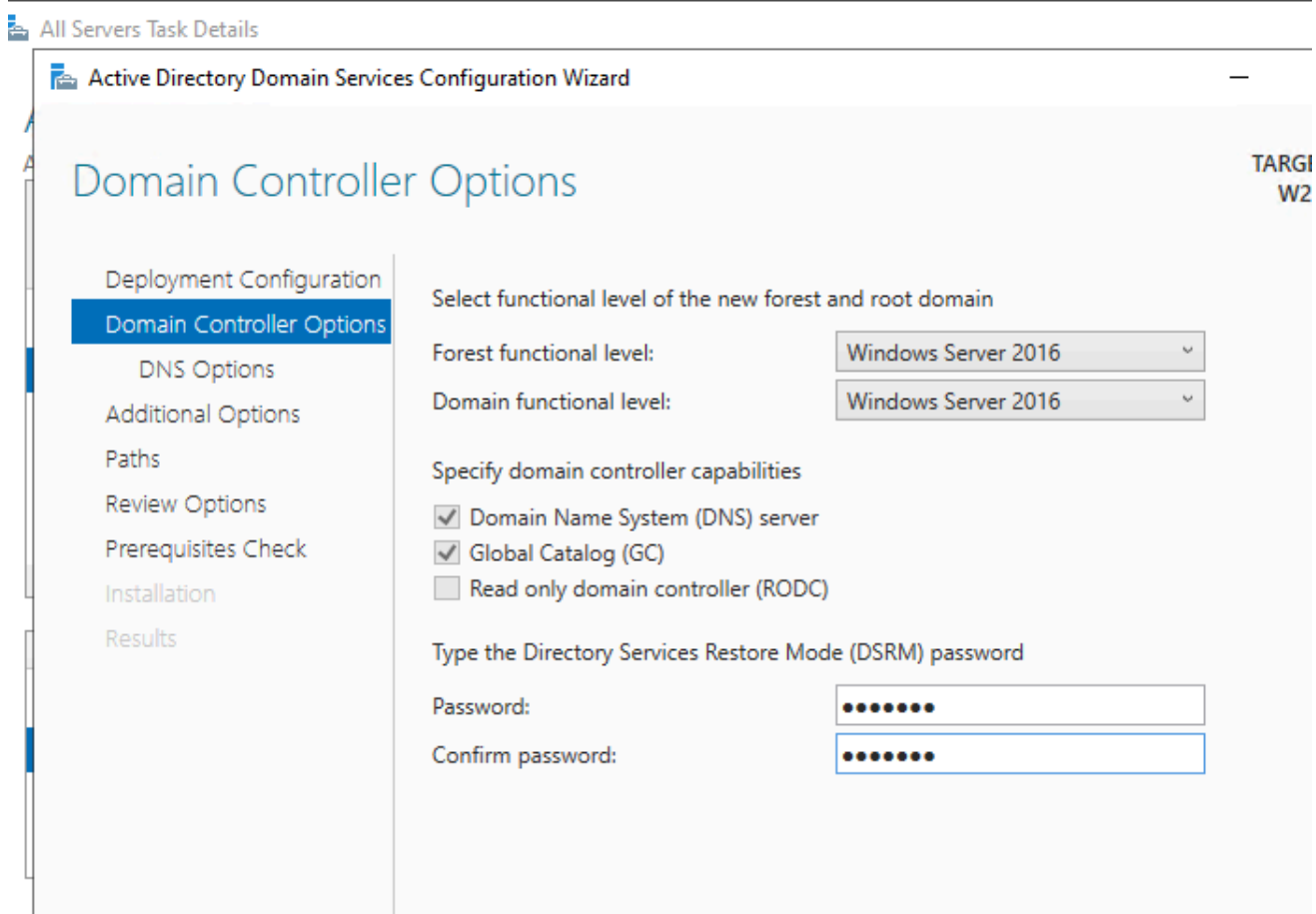
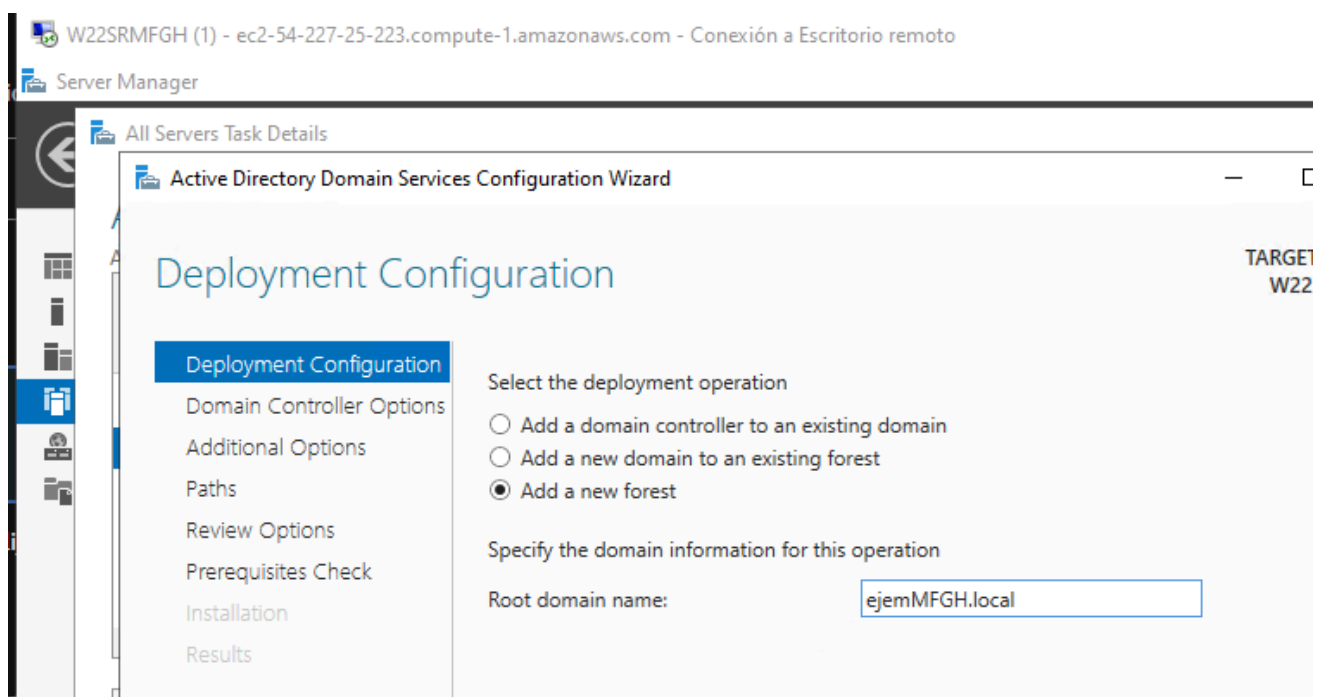
The screenshot shows the 'System Properties' dialog box in Windows Server. The 'Computer Name/Domain Changes' tab is active. The 'Computer name' is 'W22SRMFGH' and the 'Full computer name' is 'W22SRMFGH'. The 'Member of' section shows 'Workgroup: WORKGROUP' selected.



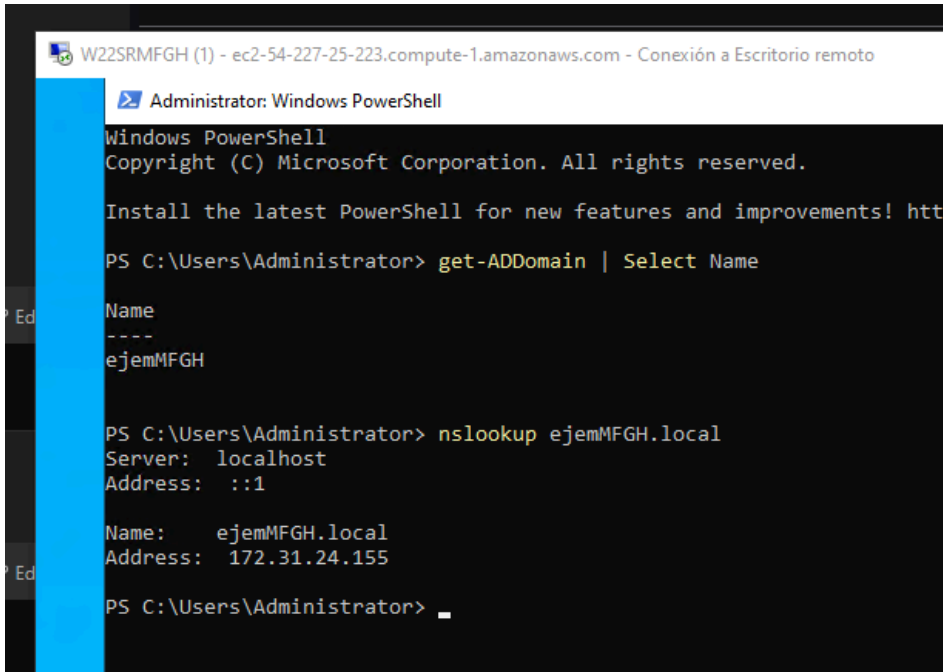
Se pide realizar:

- 1) Promociona nuestro servidor a controlador de dominio. Puedes usar como guía el documento adjunto a esta práctica en la Moodle pero recuerda que no es una guía a seguir al pie de la letra, debes adaptarla a este ejercicio. El nombre del dominio raíz del nuevo bosque será **ejemXXX.local** y el nivel funcional del bosque Windows Server 2016. No olvides dejar marcada la opción de instalar el servicio DNS . (1,5 pts.)





usuario.1



```

W22SRMFGH (1) - ec2-54-227-25-223.compute-1.amazonaws.com - Conexión a Escritorio remoto
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! http://aka.ms/PowerShellLatest

PS C:\Users\Administrator> get-ADDomain | Select Name

Name
----
ejemMFGH

PS C:\Users\Administrator> nslookup ejemMFGH.local
Server: localhost
Address: ::1

Name:     ejemMFGH.local
Address:  172.31.24.155

PS C:\Users\Administrator>

```

- 2) Haz una consulta desde tu equipo de clase al servidor DNS con el programa nslookup a la máquina *w22srxxx.ejemxxx.local* y comprueba que funciona correctamente el servicio DNS. Repite la consulta con el programa dig desde un linux. (1 pto.)

Es normal que desde windows no funcione por políticas de las compañías de wifi.

```

PS C:\Users\Manuel> nslookup w22srmfgh.ejemmfgh.local 172.31.16.109
DNS request timed out.
    timeout was 2 seconds.
Servidor: UnKnown
Address: 172.31.16.109

DNS request timed out.
    timeout was 2 seconds.

```

Desde ubuntu server:

```

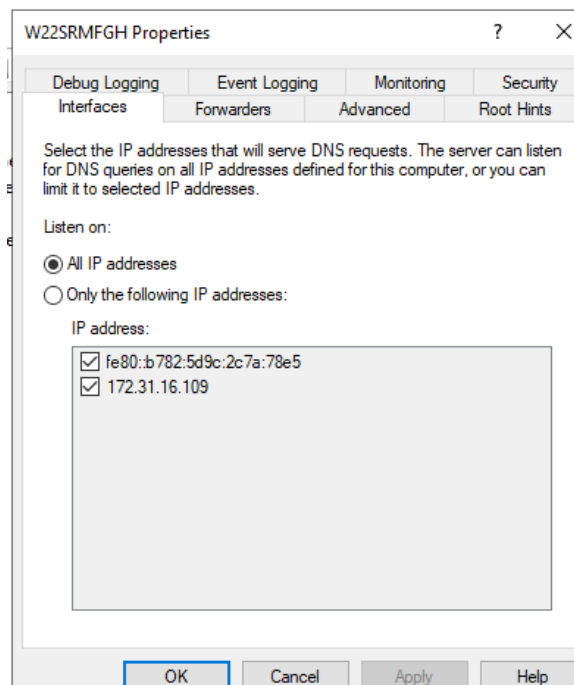
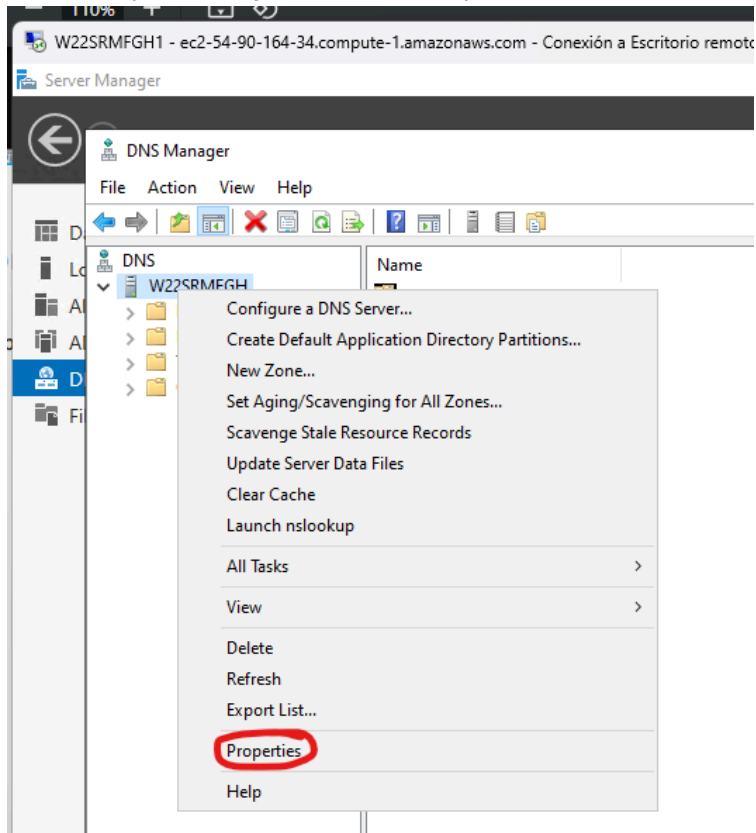
ubuntu@ip-172-31-82-232:~$ dig @172.31.16.109 w22srmfgh.ejemmfgh.local
; <<>> DiG 9.18.30-0ubuntu0.24.04.1-Ubuntu <<>> @172.31.16.109 w22srmfgh.ejemmfgh.local
; (1 server found)
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58226
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;w22srmfgh.ejemmfgh.local.      IN      A
;; ANSWER SECTION:
w22srmfgh.ejemmfgh.local. 3600 IN      A      172.31.16.109
;; Query time: 3 msec
;; SERVER: 172.31.16.109#53(172.31.16.109) (UDP)
;; WHEN: Wed Jan 29 18:05:31 UTC 2025
;; MSG SIZE rcvd: 69

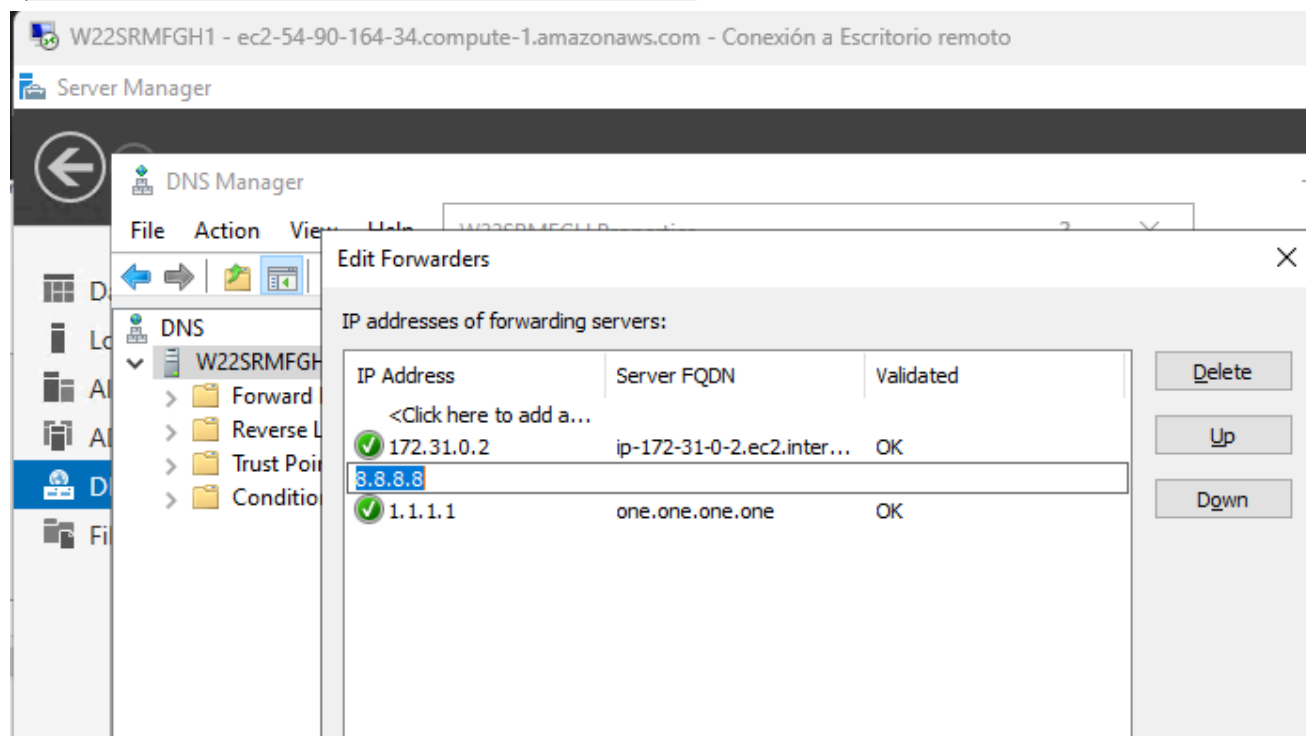
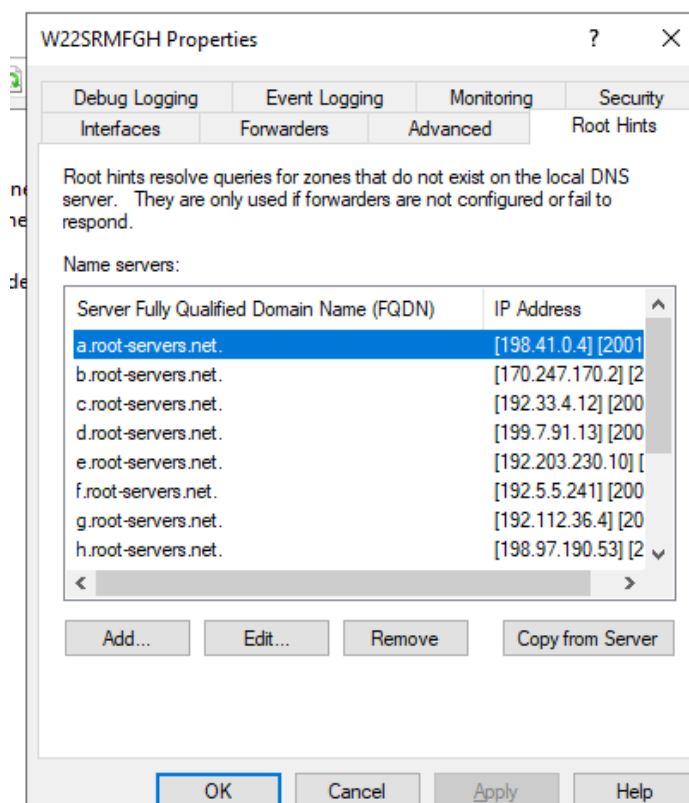
ubuntu@ip-172-31-82-232:~$

```

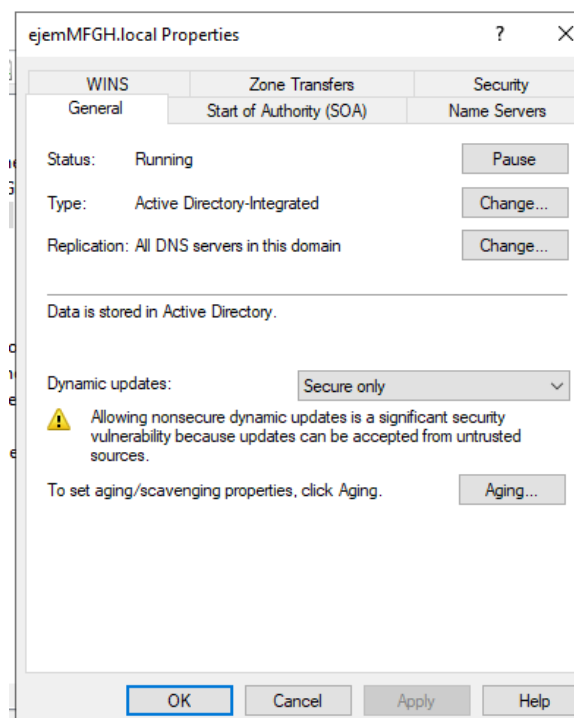
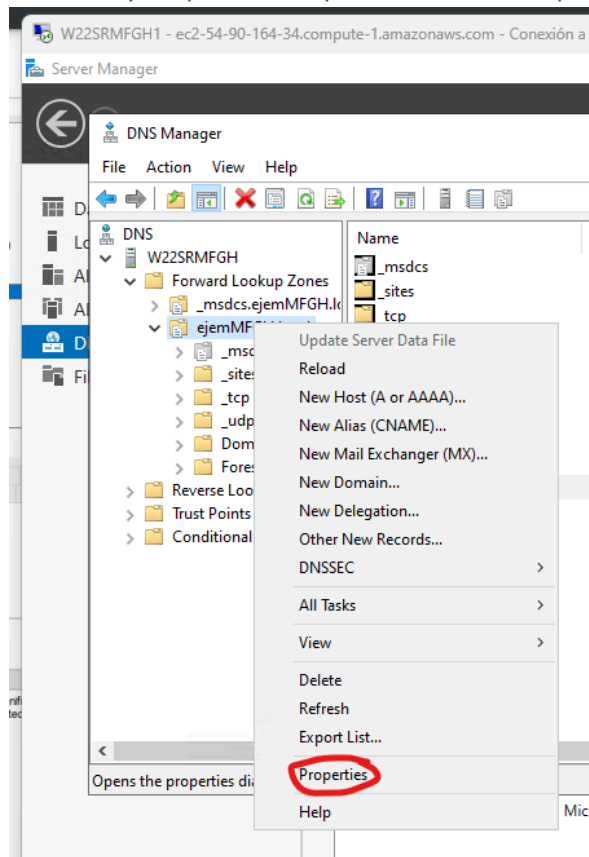
Utilizando el DNS Manager examina y configura el servidor DNS de la siguiente forma:

- 3) Comprueba las opciones generales del servidor DNS: interfaces, forwarders, Root hints. Captura su contenido y añade el *forwarder* 8.8.8.8 y el 1.1.1.1 (1 pto.)





- 4) Examina la zona directa Forward Lookup Zones *ejemxxx.local*: (3 ptos.)
- Comprueba que tiene un RR de tipo **SOA**, un **NS** y otros de tipo **A**
  - Examina y captura las pantallas con la propiedades de la zona directa **ejemxxx.local**



ejemMFGH.local Properties

WINS    Zone Transfers    Security

General    Start of Authority (SOA)    Name Servers

Serial number:

Primary server:

Responsible person:

Refresh interval:

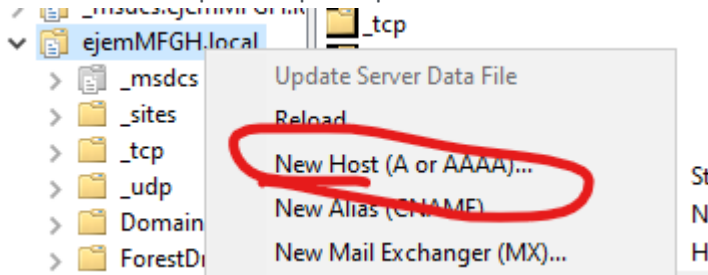
Retry interval:

Expires after:

Minimum (default) TTL:

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

- c) Añade dos registros de tipo **A** (Host) para los equipos **ser1.ejemxxx.local**, **ser2.ejemxxx.local** y cuatro más para **pc1.ejemxxx.local** al **pc4.ejemxxx.local**. Pon IPs ficticias dentro de tu subnet de AWS. Comprueba que se pueden resolver esos nombres con nslookup o con dig



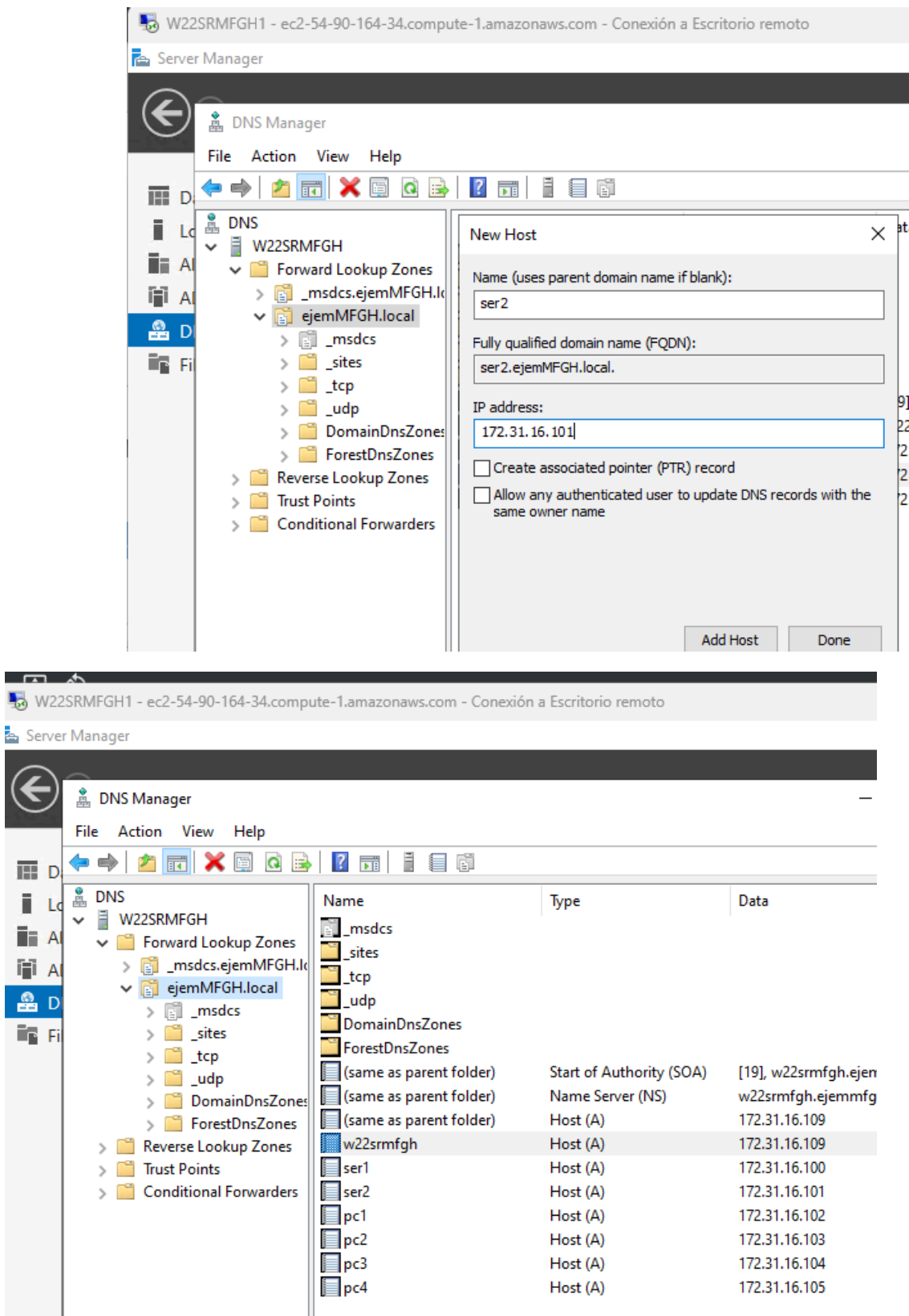
Subredes (1/1) Información

Find resources by attribute or tag

ID de subred: subnet-0478ded80ee037df0

Name	ID de subred	Estado	VPC	Bloquear el ...	CIDR IPv4
-	subnet-0478ded80ee037df0	Available	vpc-0fbaf47b7d5425b0e	Desactivado	172.31.16.0/20





Se pueden resolver

```
ubuntu@ip-172-31-82-232:~$ dig pc1.ejemmfgh.local @54.90.164.34

; <<>> DiG 9.18.30-0ubuntu0.24.04.1-Ubuntu <<>> pc1.ejemmfgh.local @54.90.164.34
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47140
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;pc1.ejemmfgh.local.          IN      A

;; ANSWER SECTION:
pc1.ejemmfgh.local.    3600    IN      A      172.31.16.102

;; Query time: 2 msec
;; SERVER: 54.90.164.34#53(54.90.164.34) (UDP)
;; WHEN: Wed Jan 29 18:19:34 UTC 2025
;; MSG SIZE rcvd: 63

ubuntu@ip-172-31-82-232:~$ dig ser1.ejemmfgh.local @54.90.164.34

; <<>> DiG 9.18.30-0ubuntu0.24.04.1-Ubuntu <<>> ser1.ejemmfgh.local @54.90.164.34
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58421
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

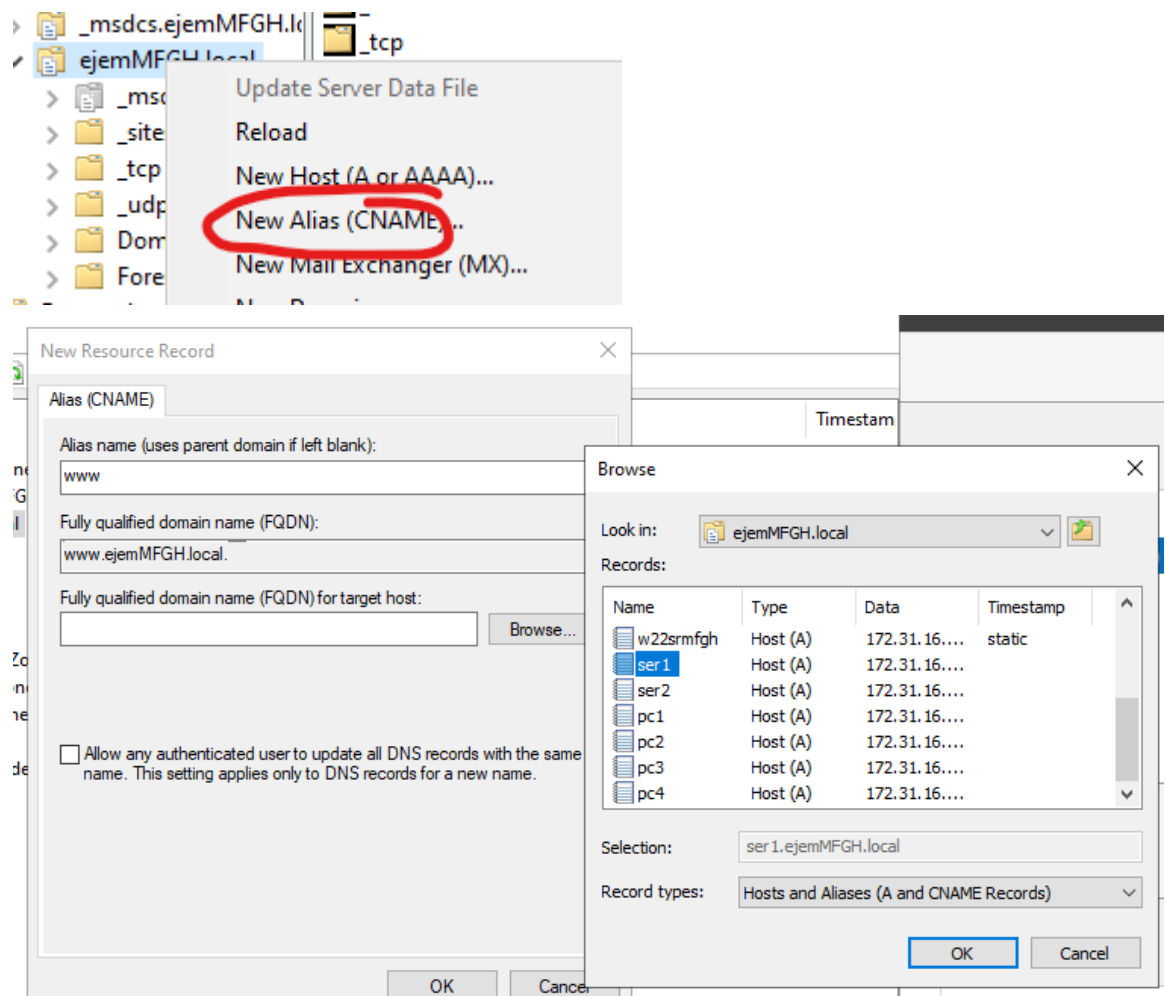
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;ser1.ejemmfgh.local.          IN      A

;; ANSWER SECTION:
ser1.ejemmfgh.local.    3600    IN      A      172.31.16.100

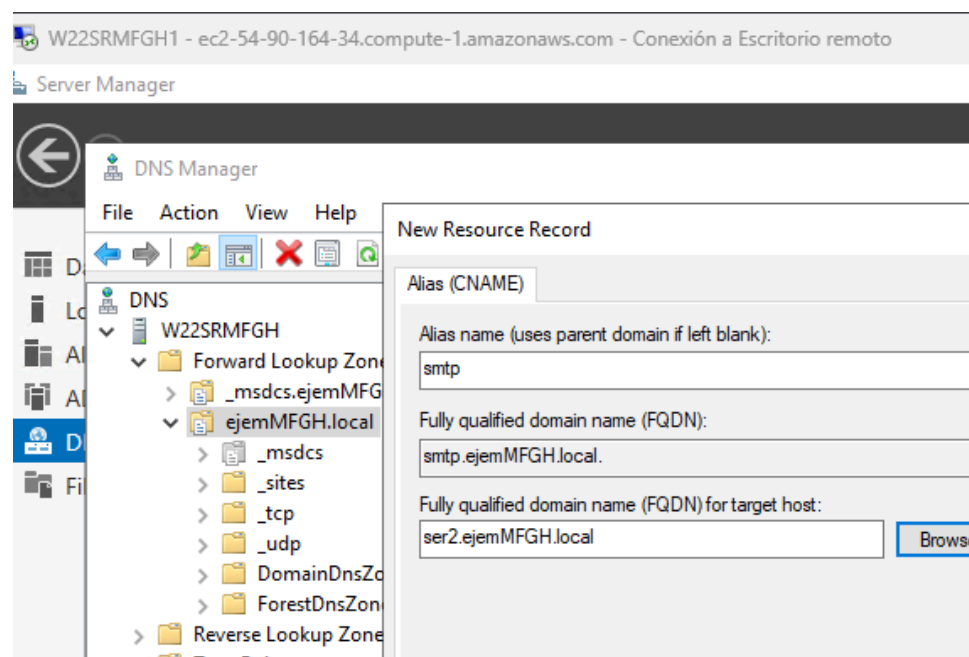
;; Query time: 0 msec
;; SERVER: 54.90.164.34#53(54.90.164.34) (UDP)
;; WHEN: Wed Jan 29 18:19:39 UTC 2025
;; MSG SIZE rcvd: 64

ubuntu@ip-172-31-82-232:~$
```

- d) Crea un RR de tipo **CNAME** para **ser1.ejemxxx.local** llamado **www.ejemxxx.local**



- e) Crea un RR de tipo **CNAME** para **ser2.ejemxxx.local** llamado **smtp.ejemxxx.local**



f) Comprueba que los **CNAME** anteriores se pueden resolver desde tu PC anfitrión

5	(same as parent folder)	Host (A)	172.31.16.102	172.31.16.102
	w22srmfgh	Host (A)	172.31.16.109	static
	ser1	Host (A)	172.31.16.100	
5	ser2	Host (A)	172.31.16.101	
	pc1	Host (A)	172.31.16.102	
	pc2	Host (A)	172.31.16.103	
	pc3	Host (A)	172.31.16.104	
	pc4	Host (A)	172.31.16.105	
	www	Alias (CNAME)	ser1.ejemMFGH.local	
	smtp	Alias (CNAME)	ser2.ejemMFGH.local	

```
ubuntu@ip-172-31-82-232:~$ nslookup www.ejemmfgh.local 54.90.164.34
Server:          54.90.164.34
Address:         54.90.164.34#53

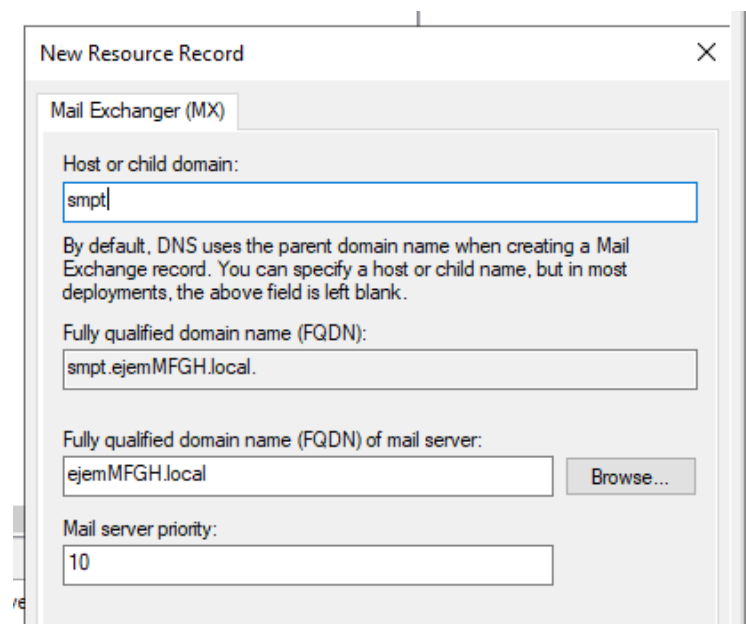
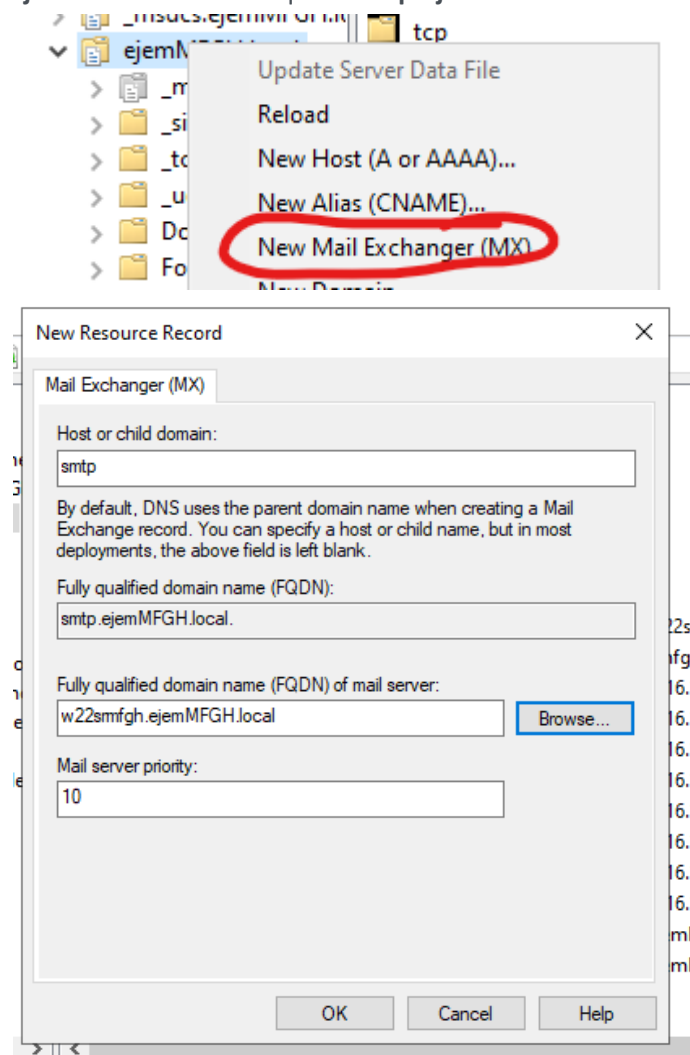
www.ejemmfgh.local    canonical name = ser1.ejemmfgh.local.
Name:   ser1.ejemmfgh.local
Address: 172.31.16.100

ubuntu@ip-172-31-82-232:~$ nslookup smtp.ejemmfgh.local 54.90.164.34
Server:          54.90.164.34
Address:         54.90.164.34#53

smtp.ejemmfgh.local   canonical name = ser2.ejemmfgh.local.
Name:   ser2.ejemmfgh.local
Address: 172.31.16.101

ubuntu@ip-172-31-82-232:~$ |
```

- g) Añade un RR de tipo **MX** que nos indique que el servidor de correo para el dominio de correo **ejemxxx.local** es la máquina **smtp.ejemxxx.local**.



- h) Resuelve los registros de tipo **MX** para el dominio de correo **ejemxxx.local** usando los comandos **nslookup** y **dig**

```
PS C:\Users\Manuel> nslookup -q=MX ejemmfgh.local 54.90.164.34
Servidor:  ec2-54-90-164-34.compute-1.amazonaws.com
Address:  54.90.164.34
```

```
ejemmfgh.local
    primary name server = w22srmfgh.ejemmfgh.local
    responsible mail addr = hostmaster.ejemmfgh.local
    serial = 29
    refresh = 900 (15 mins)
    retry = 600 (10 mins)
    expire = 86400 (1 day)
    default TTL = 3600 (1 hour)
PS C:\Users\Manuel>
```

```
ubuntu@ip-172-31-82-232:~$ dig mx ejemmfgh.local @54.90.164.34
; <<>> DiG 9.18.30-0ubuntu0.24.04.1-Ubuntu <<>> mx ejemmfgh.local @54.90.164.34
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
-->HEADER<<- opcode: QUERY, status: NOERROR, id: 42137
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;ejemmfgh.local.                IN      MX

;; AUTHORITY SECTION:
ejemmfgh.local.                3600    IN      SOA     w22srmfgh.ejemmfgh.local. hostmaster.ejemmfgh.local. 29 900 600 86400 3600

;; Query time: 0 msec
;; SERVER: 54.90.164.34#53(54.90.164.34) (UDP)
;; WHEN: Wed Jan 29 18:36:51 UTC 2025
;; MSG SIZE rcvd: 100
```

- i) Resuelve los registros de tipo **NS** para la zona **ejemxxx.local** usando los comandos **nslookup** y **dig** desde tu PC anfitrión

```
PS C:\Users\Manuel> nslookup -q=NS ejemmfgh.local 54.90.164.34
Servidor:  ec2-54-90-164-34.compute-1.amazonaws.com
Address:  54.90.164.34
```

```
ejemmfgh.local nameserver = w22srmfgh.ejemmfgh.local
w22srmfgh.ejemmfgh.local      internet address = 172.31.16.109
PS C:\Users\Manuel>
```

```
ubuntu@ip-172-31-82-232:~$ dig ns ejemmfgh.local @54.90.164.34
; <<>> DiG 9.18.30-0ubuntu0.24.04.1-Ubuntu <<>> ns ejemmfgh.local @54.90.164.34
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
-->HEADER<<- opcode: QUERY, status: NOERROR, id: 6125
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2

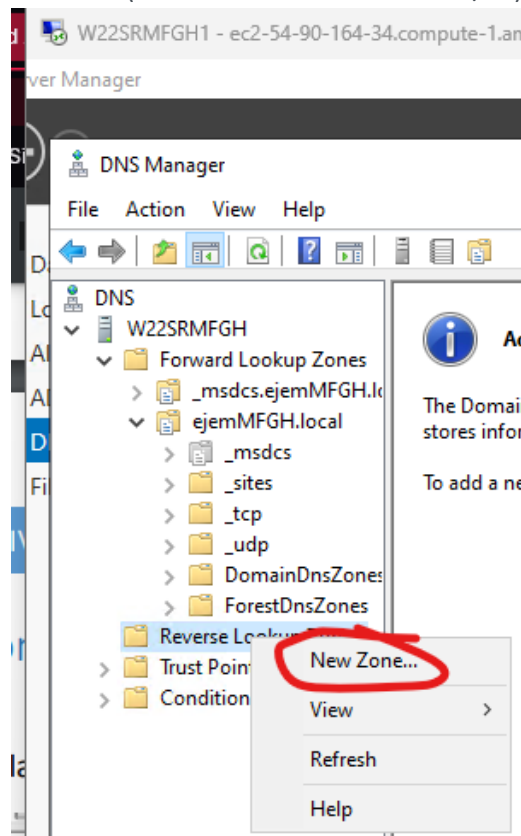
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;ejemmfgh.local.                IN      NS

;; ANSWER SECTION:
ejemmfgh.local.                3600    IN      NS      w22srmfgh.ejemmfgh.local.

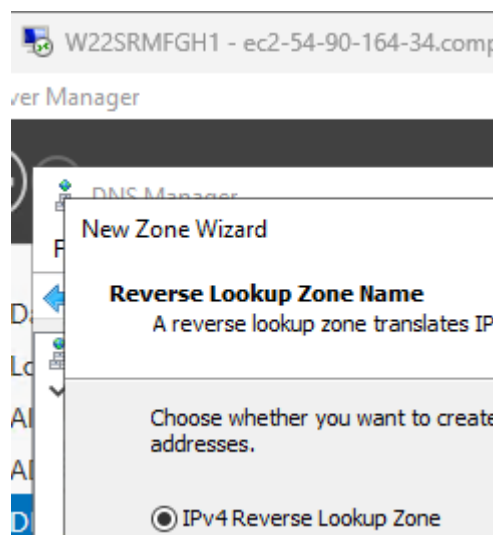
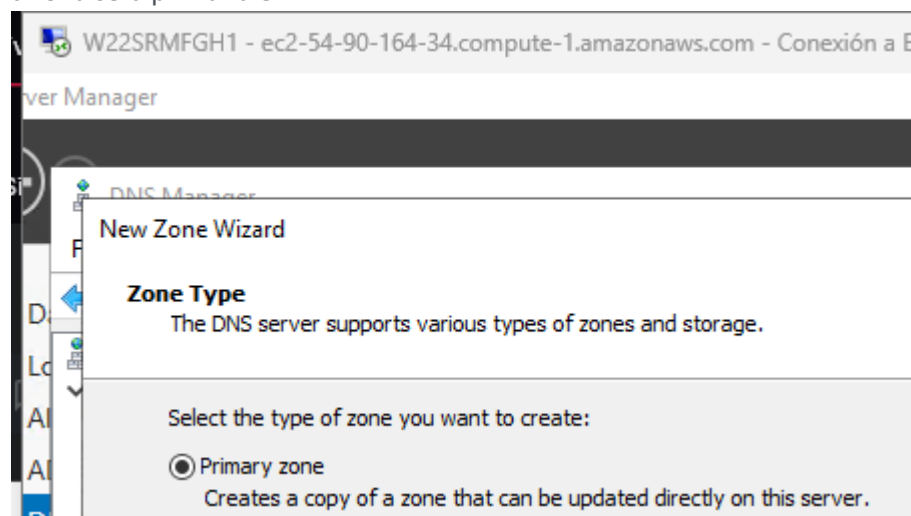
;; ADDITIONAL SECTION:
w22srmfgh.ejemmfgh.local. 1200    IN      A       172.31.16.109

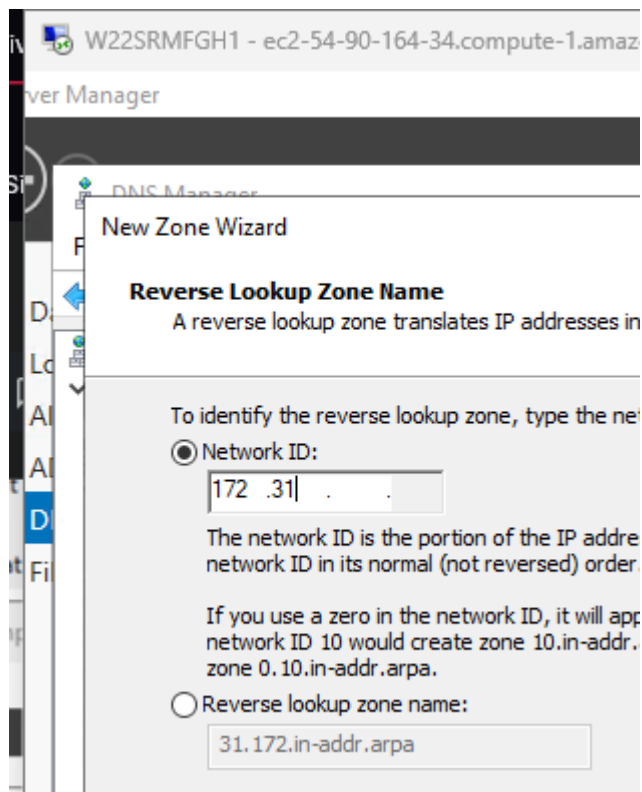
;; Query time: 1 msec
;; SERVER: 54.90.164.34#53(54.90.164.34) (UDP)
;; WHEN: Wed Jan 29 18:35:11 UTC 2025
;; MSG SIZE rcvd: 83
```

- 5) Crea una zona inversa (*Reverse Lookup Zone*) para la red de AWS que se usa en la zona directa ejemxxx.local ( en mi caso era la 172.31.0.0/16) (2,5 ptos)

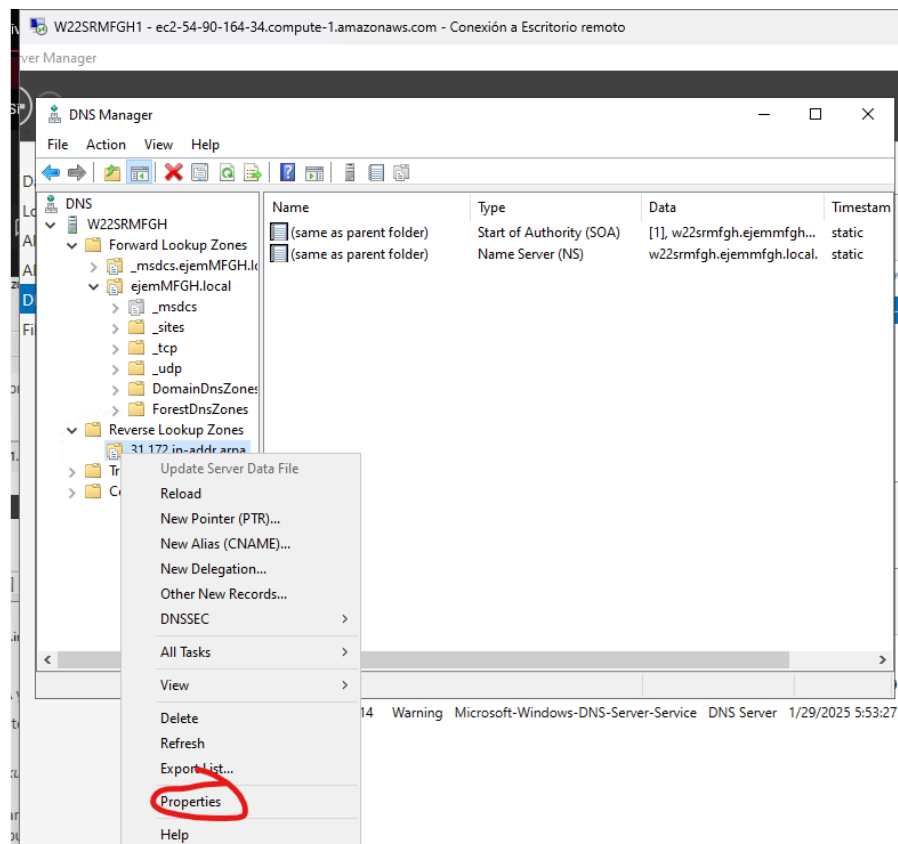


- a) La zona será primaria e IPv4

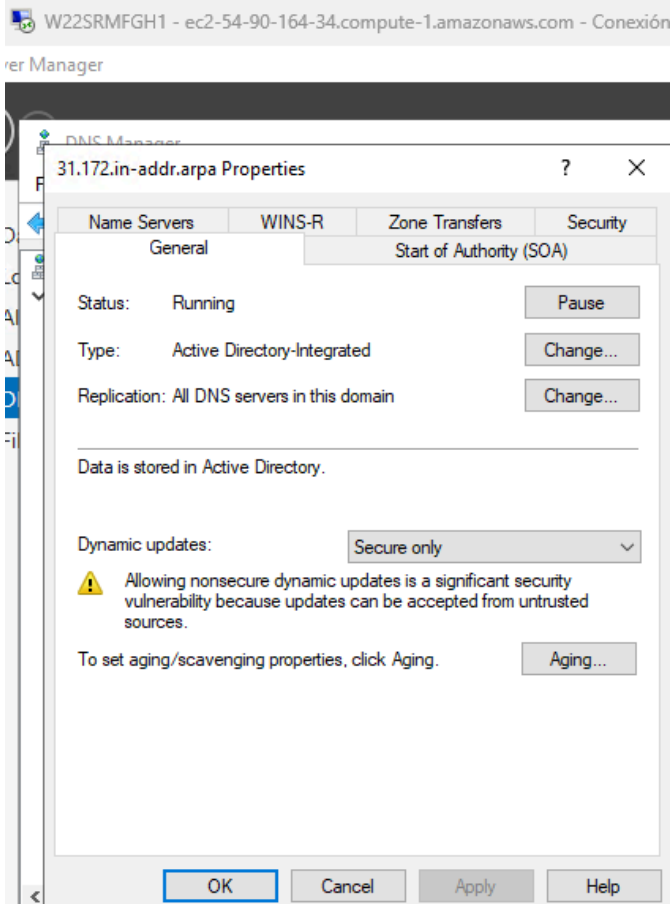
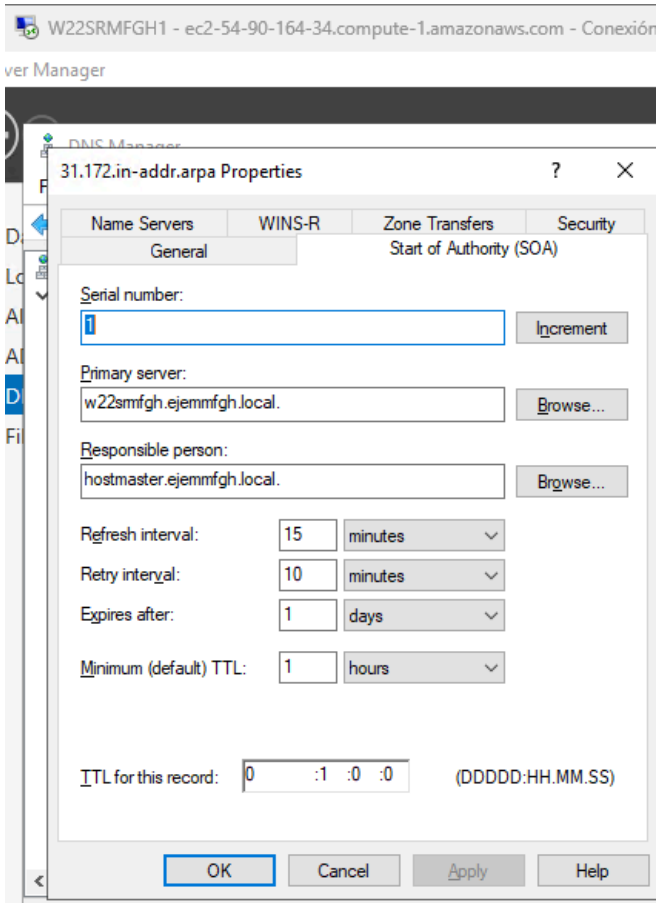




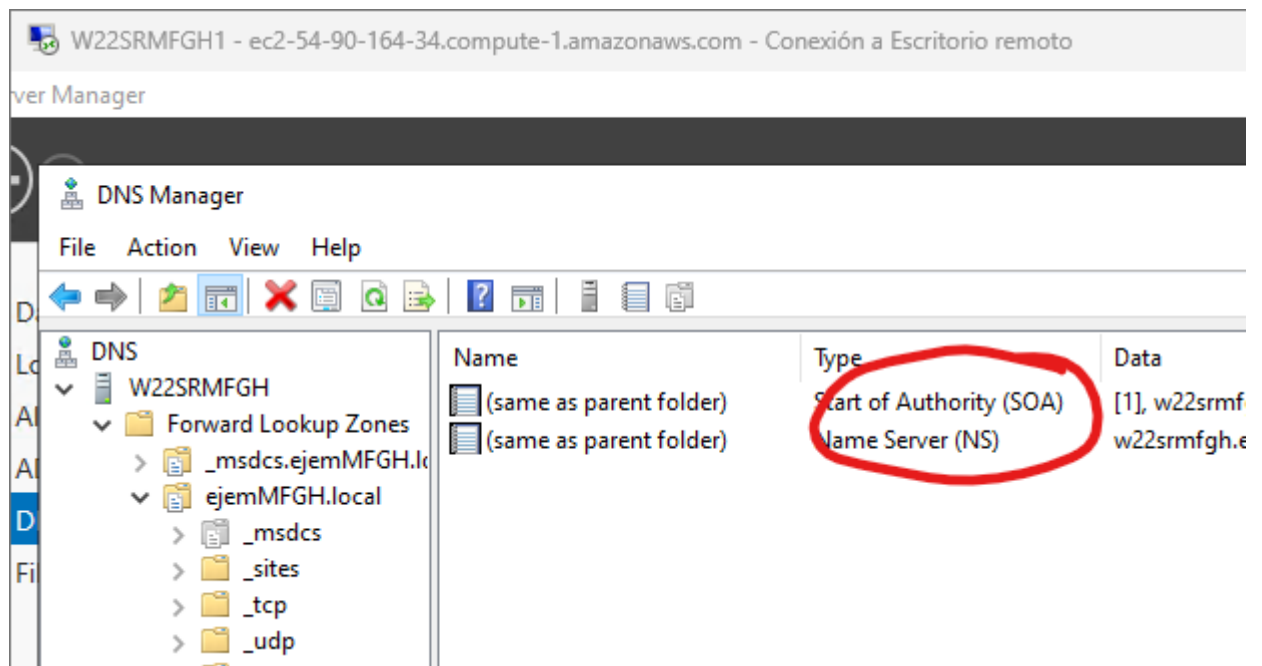
- b) Examina y captura las pantallas con la propiedades de la zona inversa **31.172.in-addr.arpa** (o la que te corresponda)



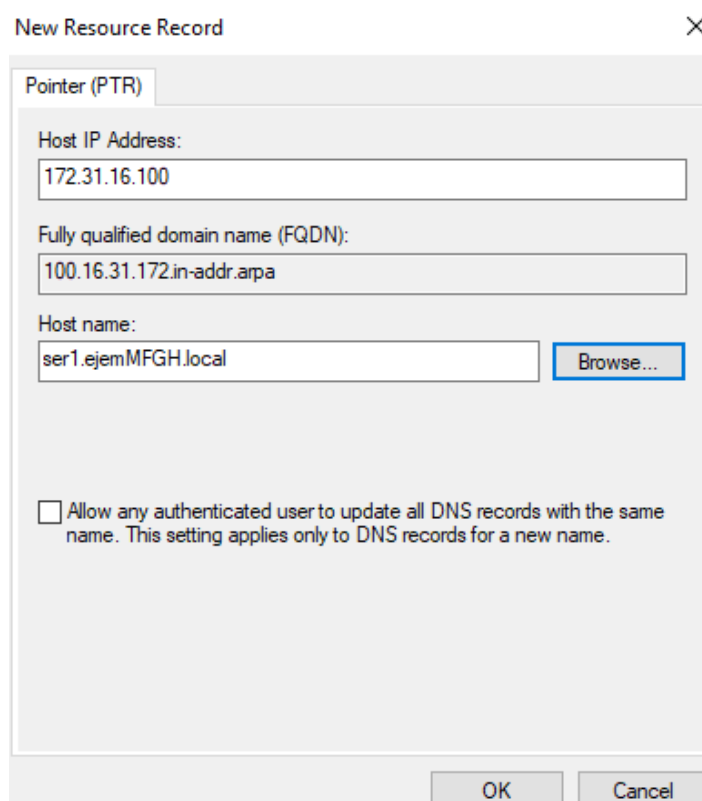
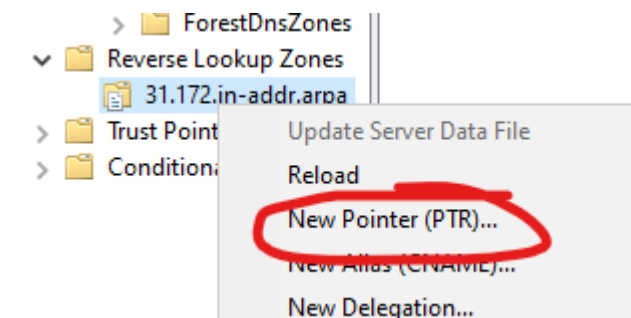


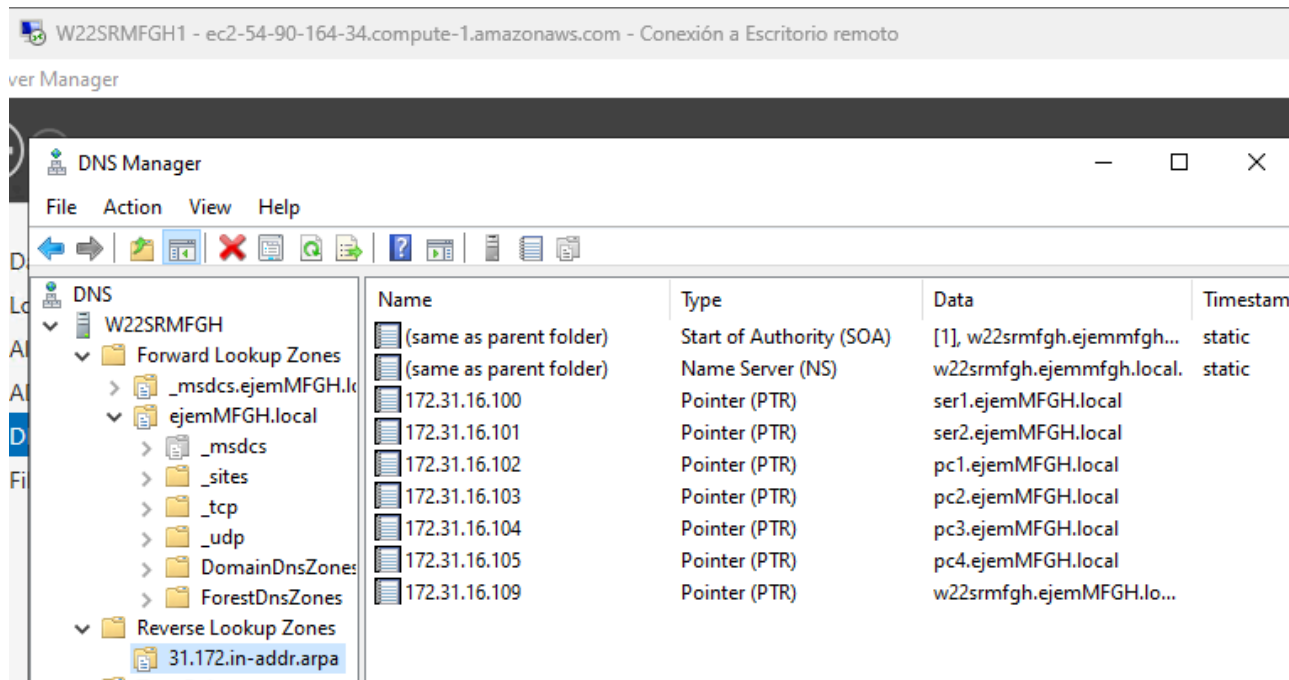


- a) Comprueba que tiene un RR de tipo **SOA** y un **NS**



- b) Añade los registros **PTR** correspondientes a todos los registros de tipo **A** de la zona directa (deberían ser 7)





c) Resuelve los registros PTR usando *nslookup* y *dig*

```
ubuntu@ip-172-31-82-232:~$ nslookup 172.31.16.100 54.90.164.34
100.16.31.172.in-addr.arpa      name = ser1.ejemMFGH.local.

ubuntu@ip-172-31-82-232:~$ nslookup 172.31.16.101 54.90.164.34
101.16.31.172.in-addr.arpa      name = ser2.ejemMFGH.local.

ubuntu@ip-172-31-82-232:~$ nslookup 172.31.16.102 54.90.164.34
102.16.31.172.in-addr.arpa      name = pc1.ejemMFGH.local.

ubuntu@ip-172-31-82-232:~$ nslookup 172.31.16.103 54.90.164.34
103.16.31.172.in-addr.arpa      name = pc2.ejemMFGH.local.

ubuntu@ip-172-31-82-232:~$ nslookup 172.31.16.104 54.90.164.34
104.16.31.172.in-addr.arpa      name = pc3.ejemMFGH.local.

ubuntu@ip-172-31-82-232:~$ nslookup 172.31.16.105 54.90.164.34
105.16.31.172.in-addr.arpa      name = pc4.ejemMFGH.local.
```

```
ubuntu@ip-172-31-82-232:~$ dig -x 172.31.16.100 @54.90.164.34

; <<>> DiG 9.18.30-0ubuntu0.24.04.1-Ubuntu <<>> -x 172.31.16.100 @54.90.164.34
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25436
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;100.16.31.172.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
100.16.31.172.in-addr.arpa. 3600 IN      PTR      ser1.ejemMFGH.local.

;; Query time: 1 msec
;; SERVER: 54.90.164.34#53(54.90.164.34) (UDP)
;; WHEN: Wed Jan 29 18:47:16 UTC 2025
;; MSG SIZE rcvd: 88

ubuntu@ip-172-31-82-232:~$ dig -x 172.31.16.101 @54.90.164.34

; <<>> DiG 9.18.30-0ubuntu0.24.04.1-Ubuntu <<>> -x 172.31.16.101 @54.90.164.34
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57059
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;101.16.31.172.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
101.16.31.172.in-addr.arpa. 3600 IN      PTR      ser2.ejemMFGH.local.

;; Query time: 0 msec
;; SERVER: 54.90.164.34#53(54.90.164.34) (UDP)
;; WHEN: Wed Jan 29 18:47:21 UTC 2025
;; MSG SIZE rcvd: 88

ubuntu@ip-172-31-82-232:~$ dig -x 172.31.16.102 @54.90.164.34

; <<>> DiG 9.18.30-0ubuntu0.24.04.1-Ubuntu <<>> -x 172.31.16.102 @54.90.164.34
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57094
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
```