Actividad - Integración de Cliente Ubuntu con Active Directory

Autor: Rafael Ortiz Navarro **Asignatura:** Implantación de Sistemas Operativos (ISO) - UF2 **Fecha:** 13/12/2025

---

1. Introducción

Esta actividad documenta el procedimiento técnico completo para configurar un entorno de Active Directory centralizado. El proceso incluye la instalación y configuración de un Controlador de Dominio sobre Windows Server 2022, seguido de la integración de un cliente Ubuntu 24.04 al dominio mediante autenticación Kerberos y SSSD.

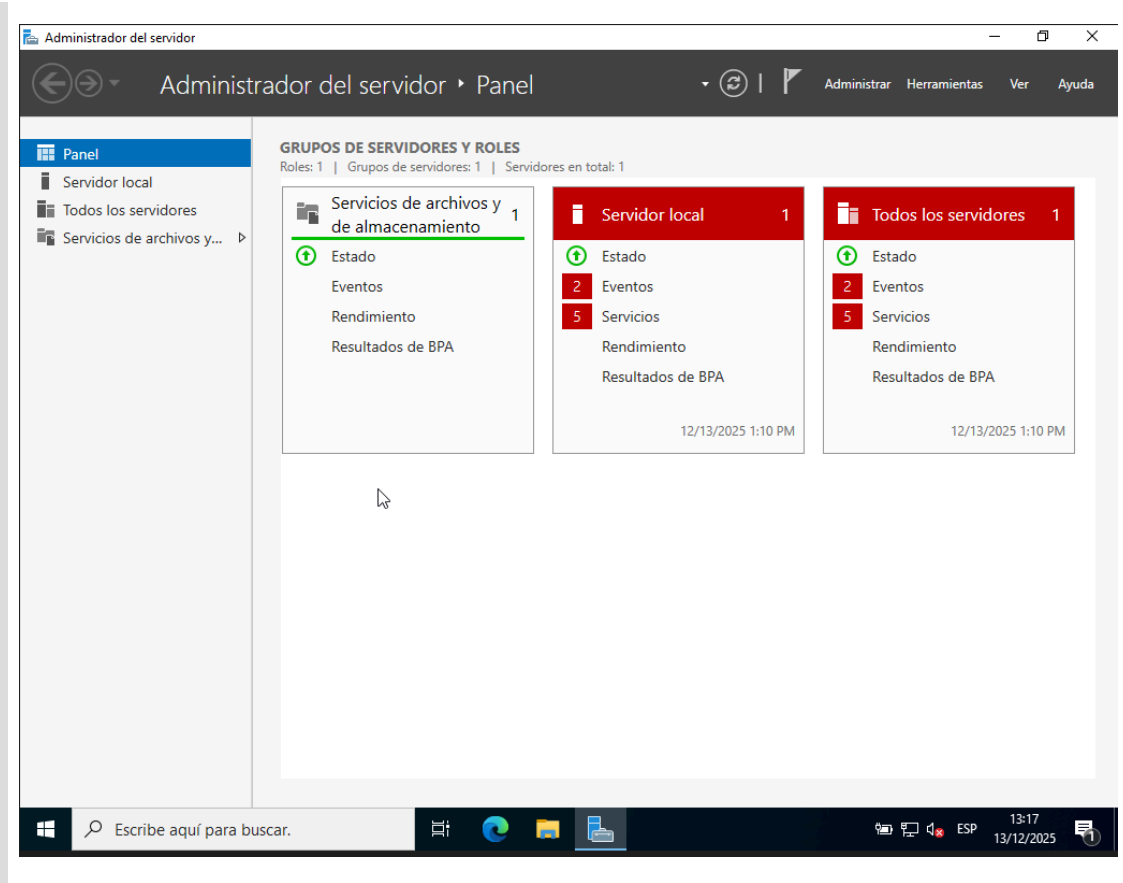
El objetivo es crear un sistema de autenticación centralizada donde los usuarios del dominio puedan iniciar sesión en equipos Linux utilizando sus credenciales de Active Directory.

---

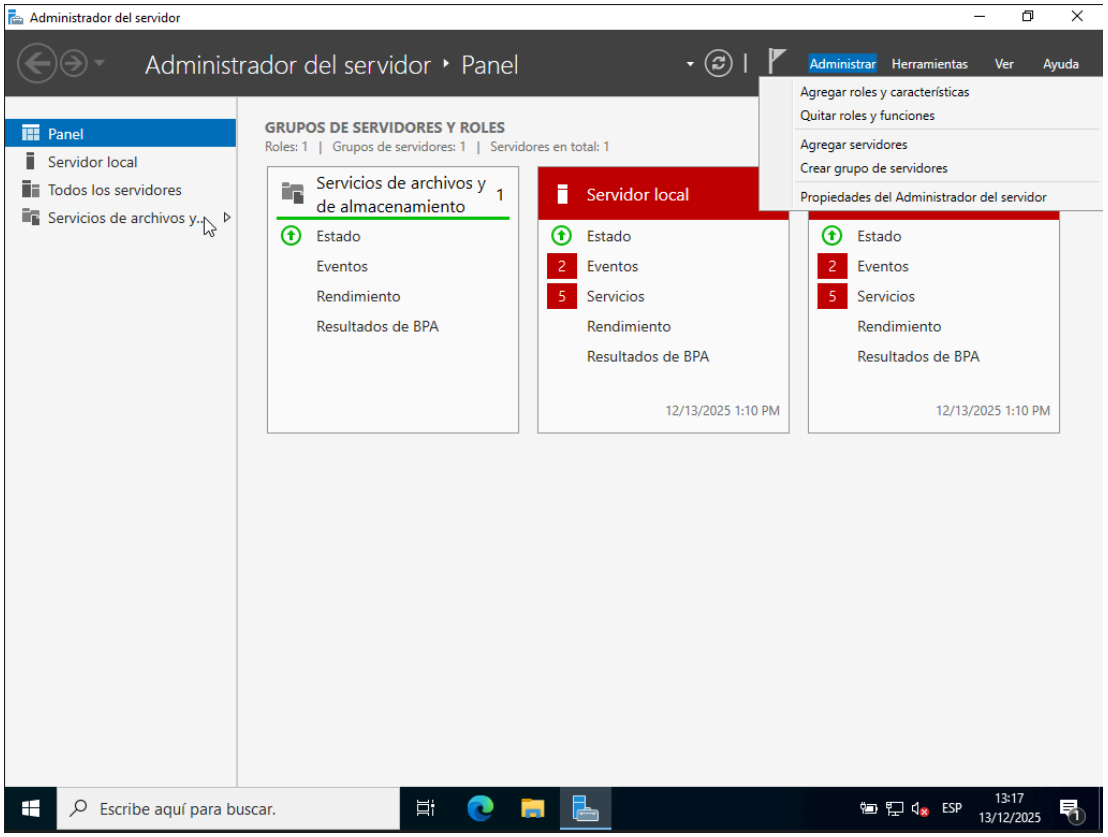
2. Fase 1: Configuración del Servidor Windows

2.1. Instalación del Rol AD DS

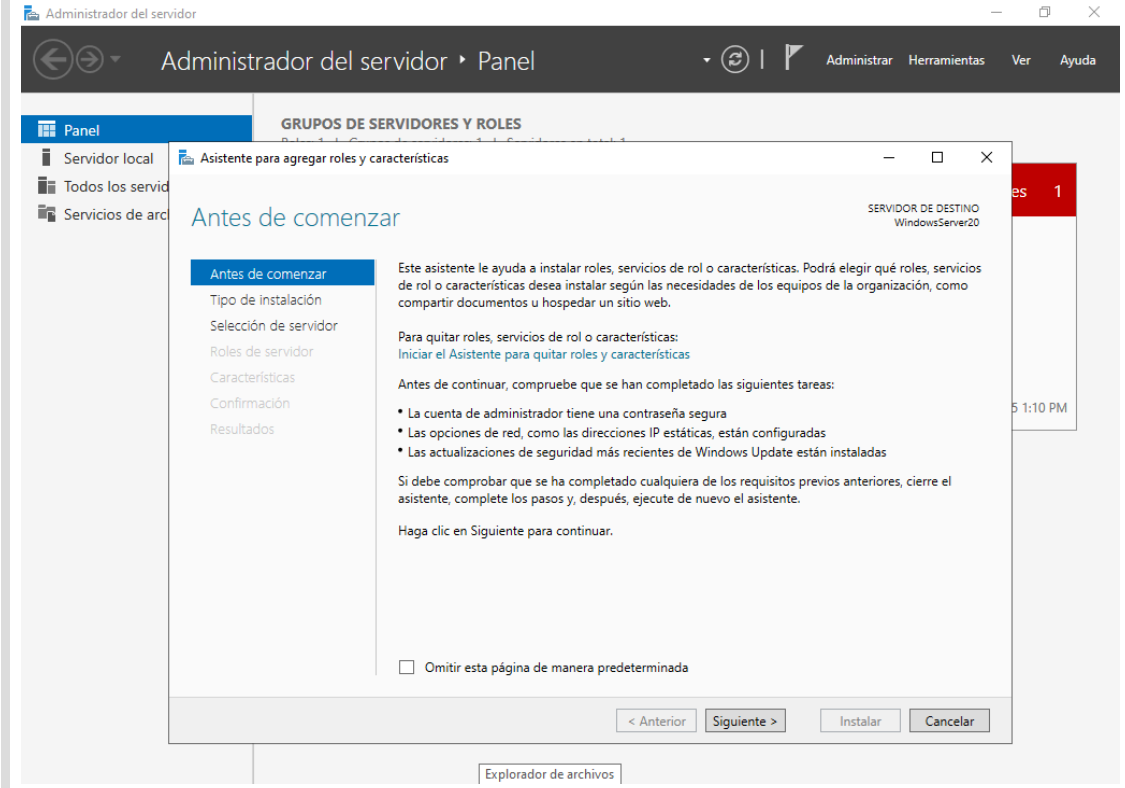
Accedemos al **Administrador del servidor** donde visualizamos el panel principal.



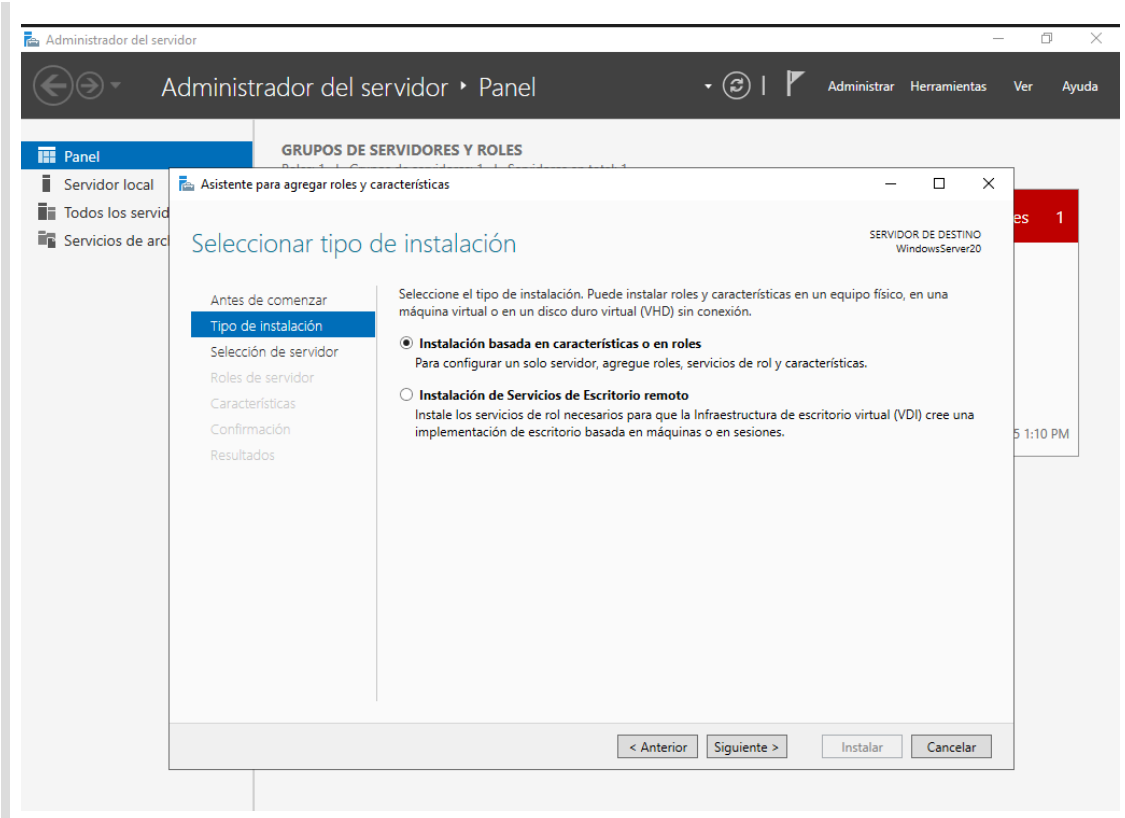
Desplegamos el menú **Administrar** y seleccionamos **Agregar roles y características**.



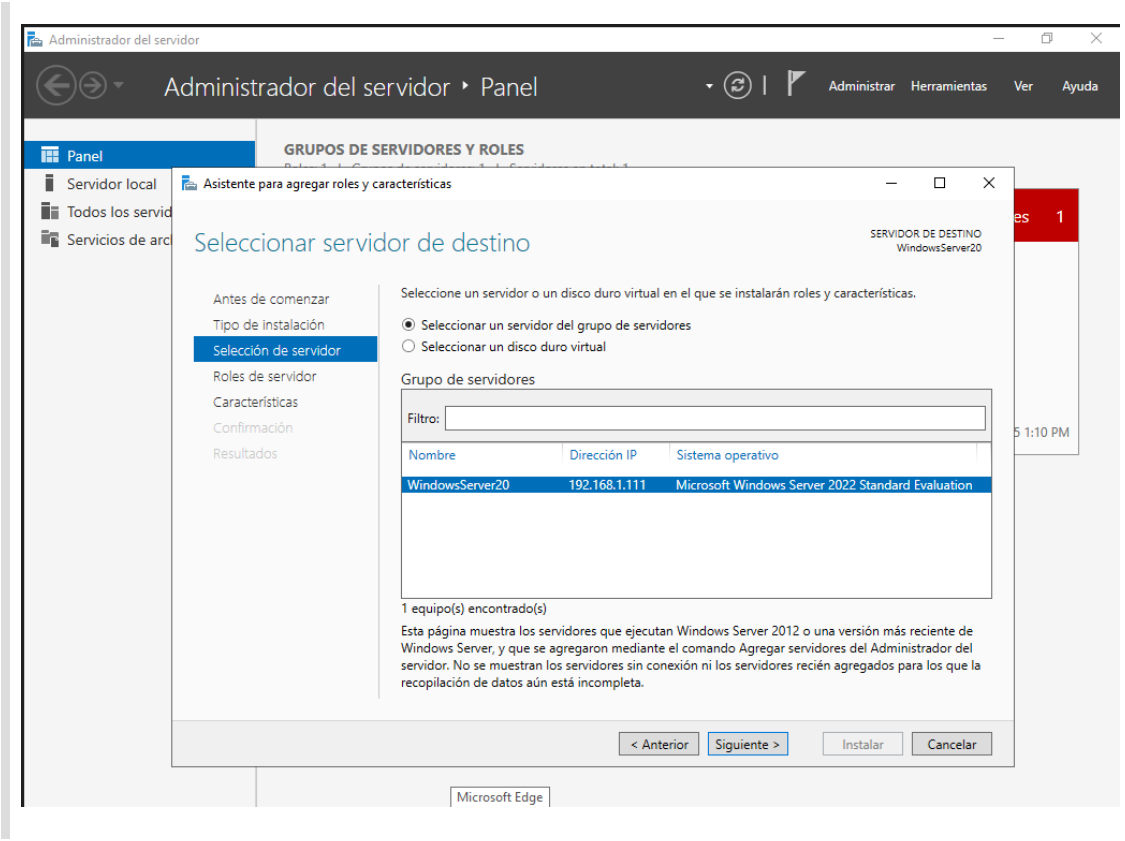
Se inicia el **Asistente para agregar roles y características**. Hacemos clic en **Siguiente**.



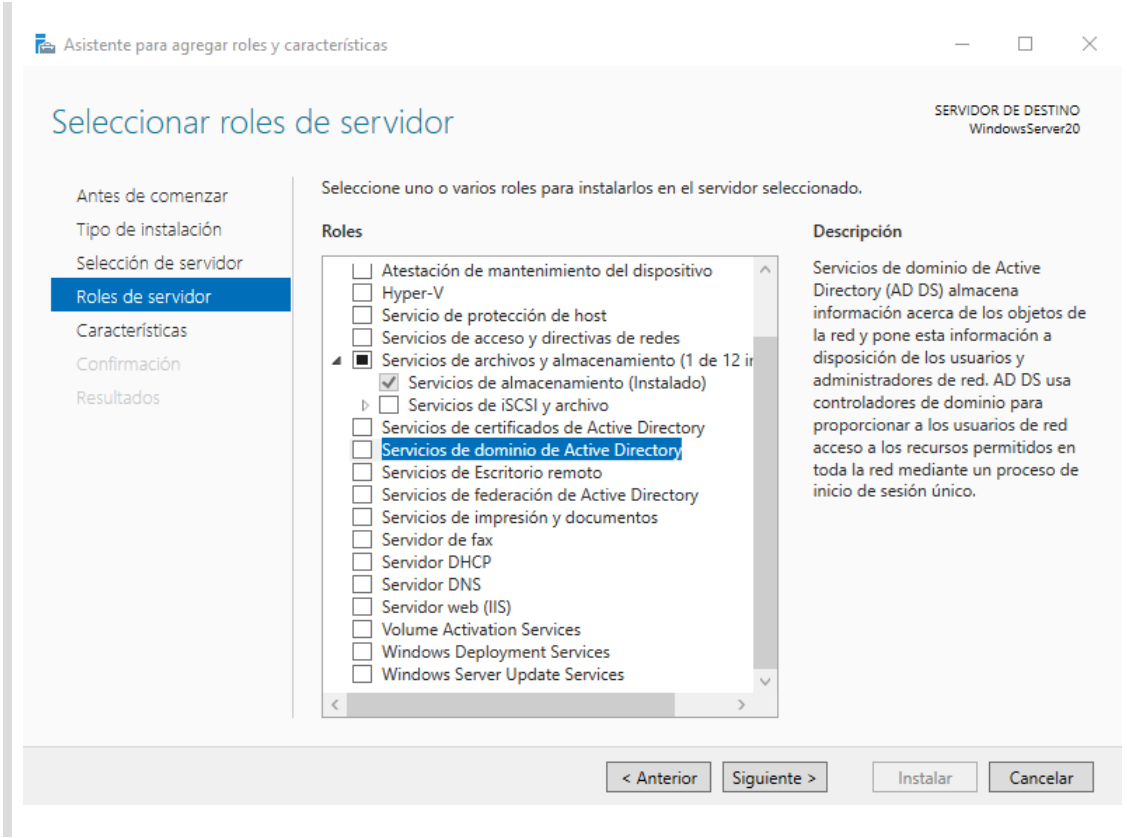
Seleccionamos **Instalación basada en características o en roles** como tipo de instalación.



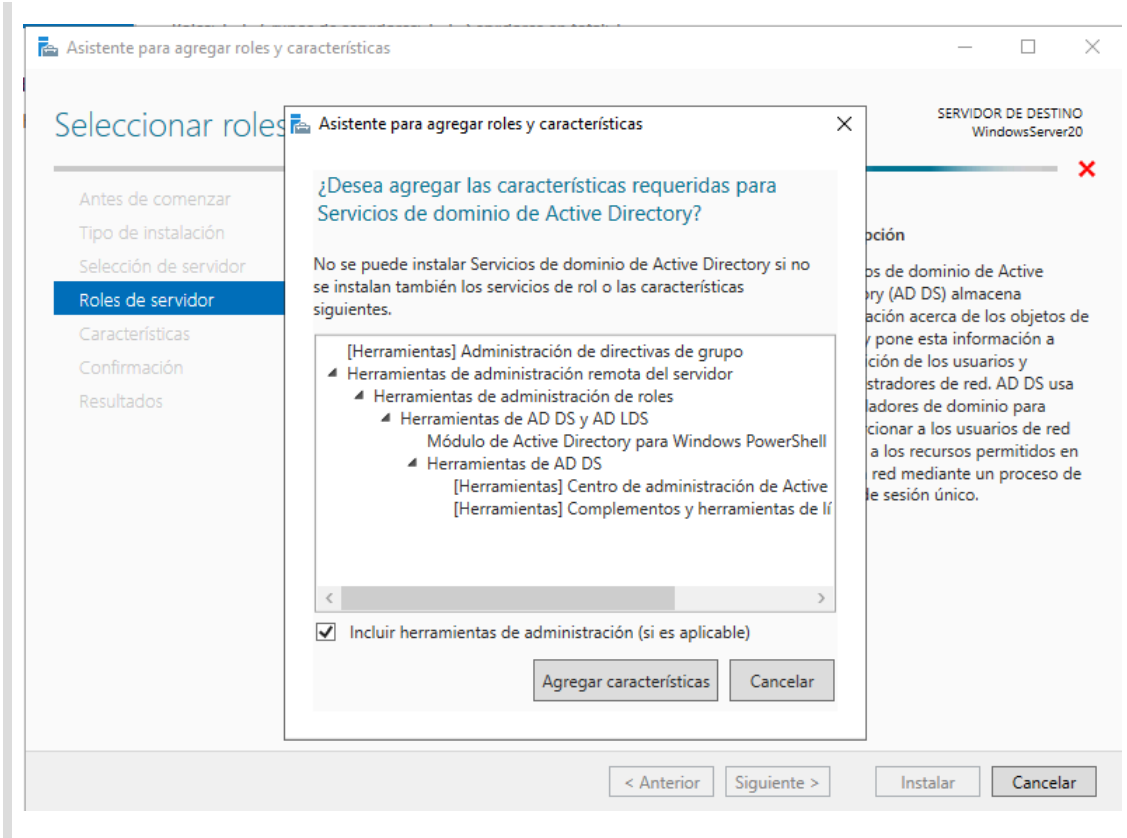
Seleccionamos nuestro servidor **WindowsServer20** (192.168.1.111) del grupo de servidores.



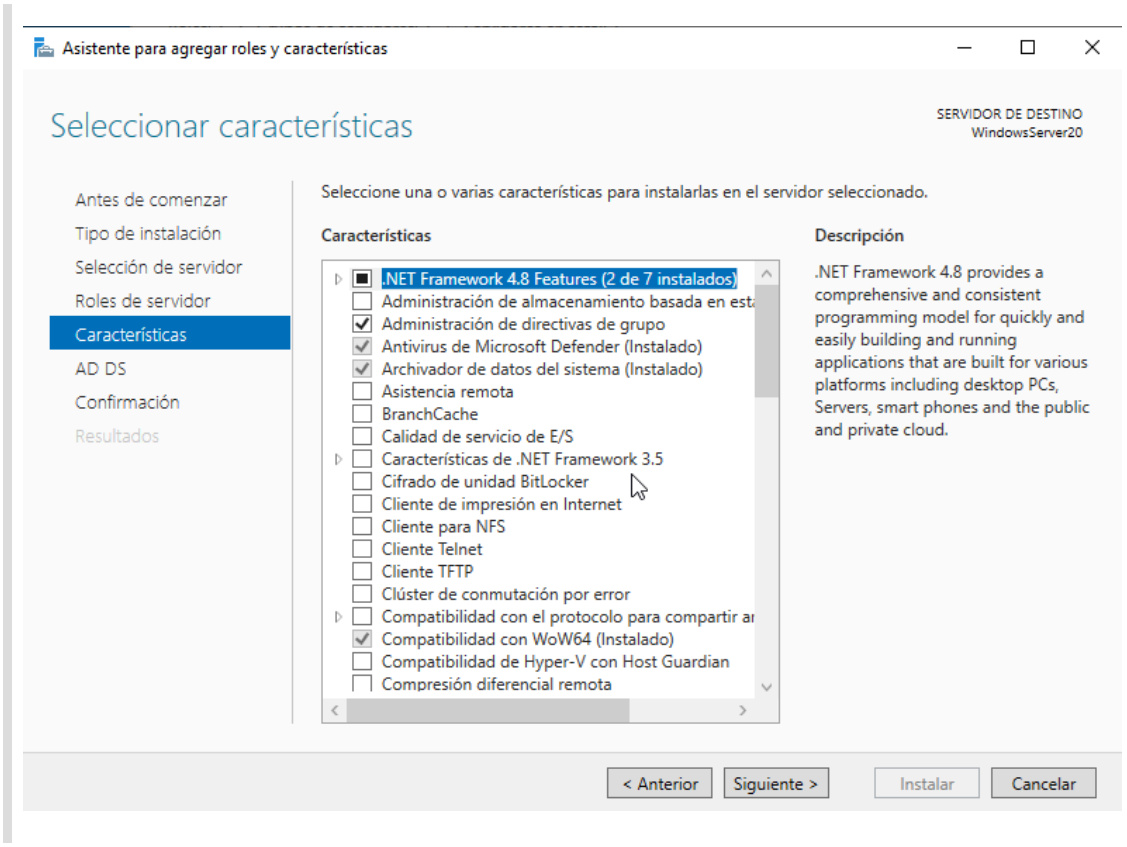
En la lista de roles disponibles, marcamos **Servicios de dominio de Active Directory**.



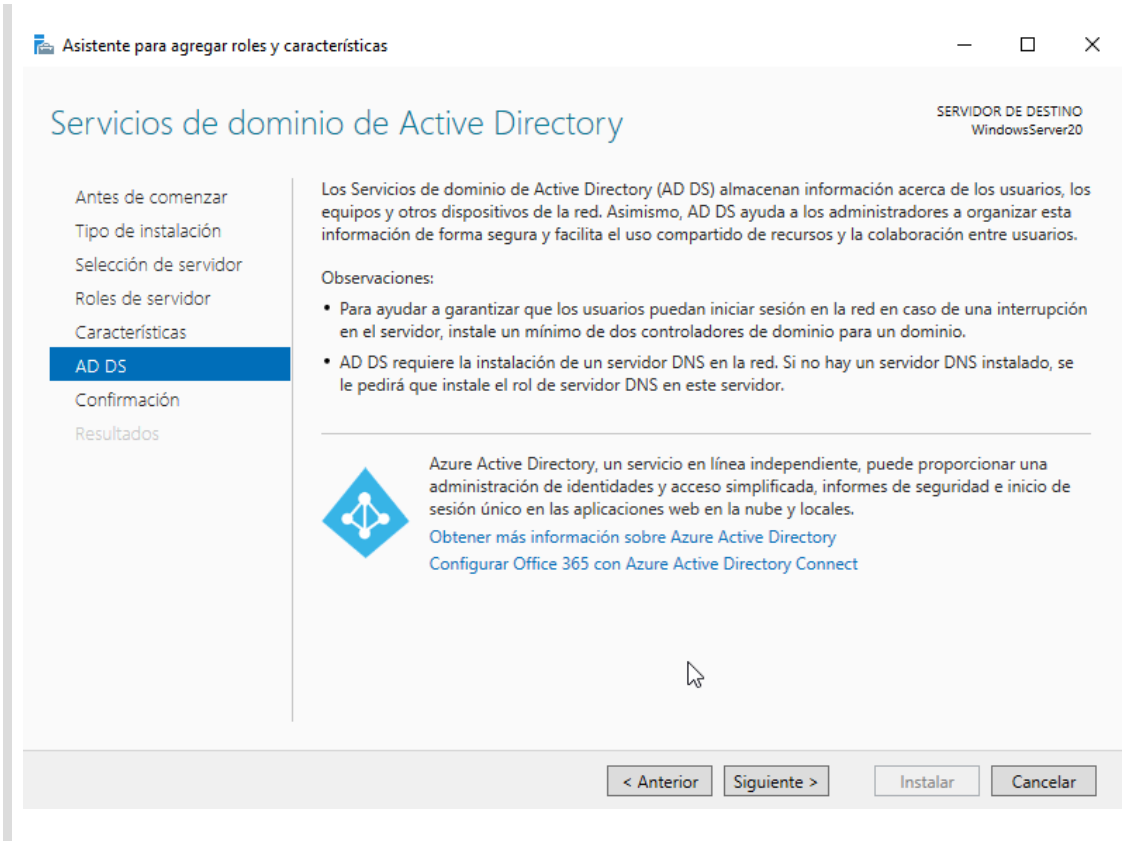
El sistema solicita agregar las características y herramientas de administración requeridas. Hacemos clic en **Agregar características**.



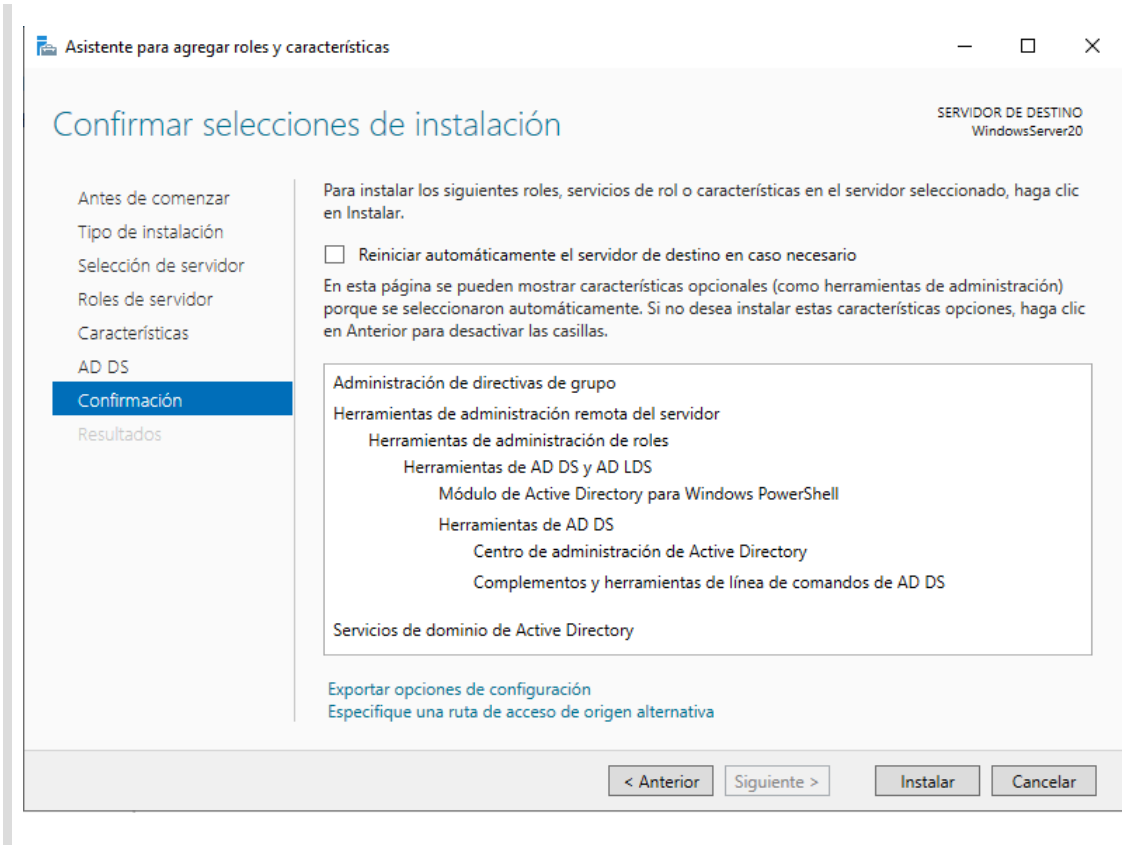
Continuamos con las características adicionales (dejamos la selección por defecto).



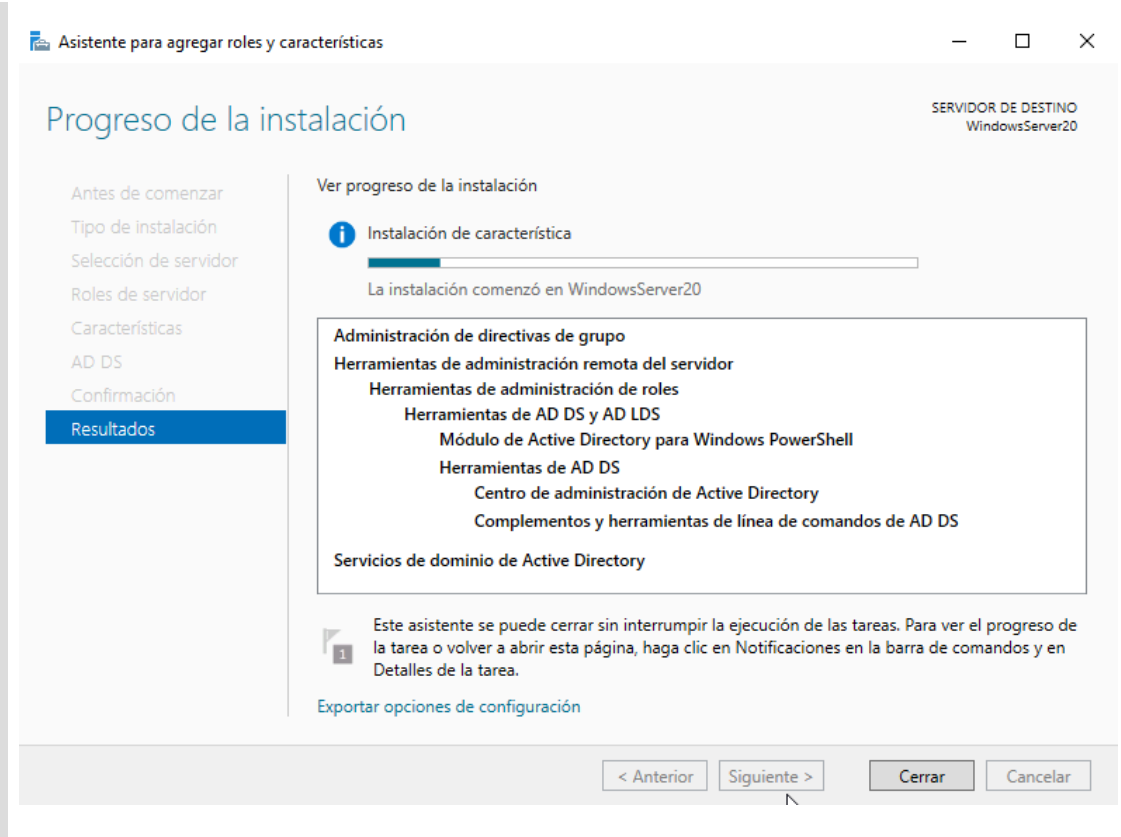
Revisamos la información sobre **Servicios de dominio de Active Directory**.



Confirmamos la instalación haciendo clic en **Instalar**.

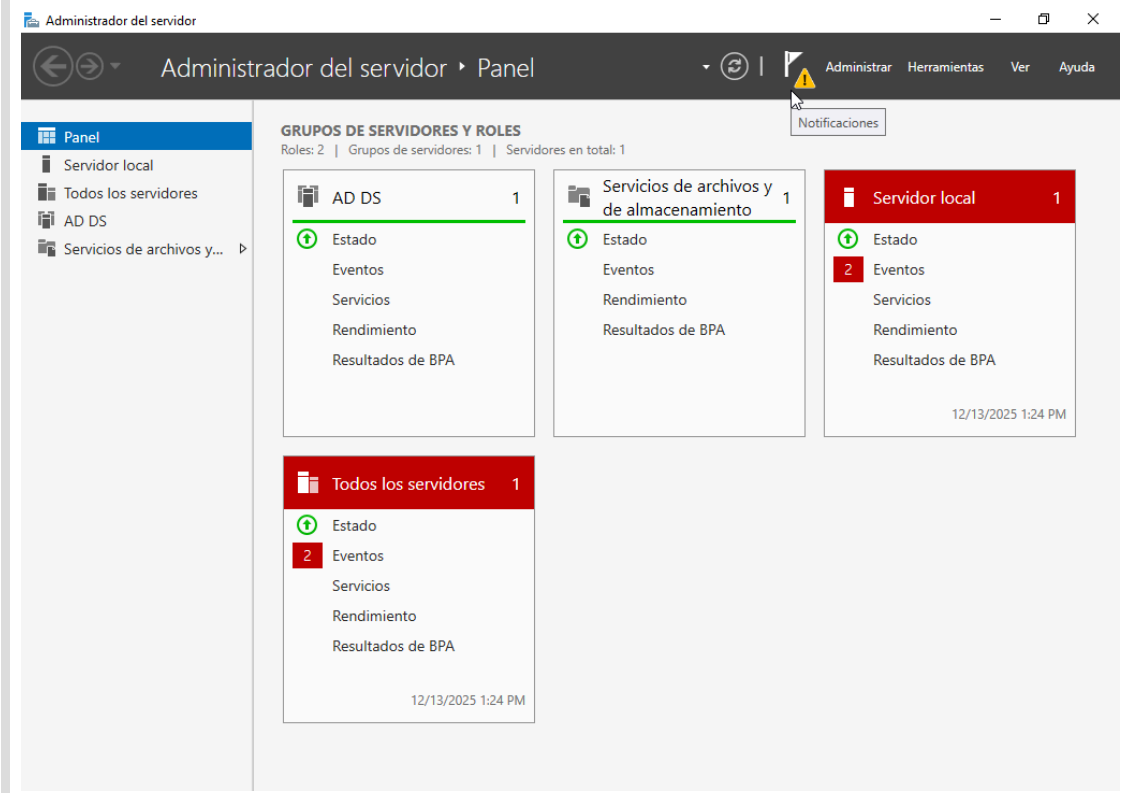


Esperamos a que finalice el progreso de la instalación.

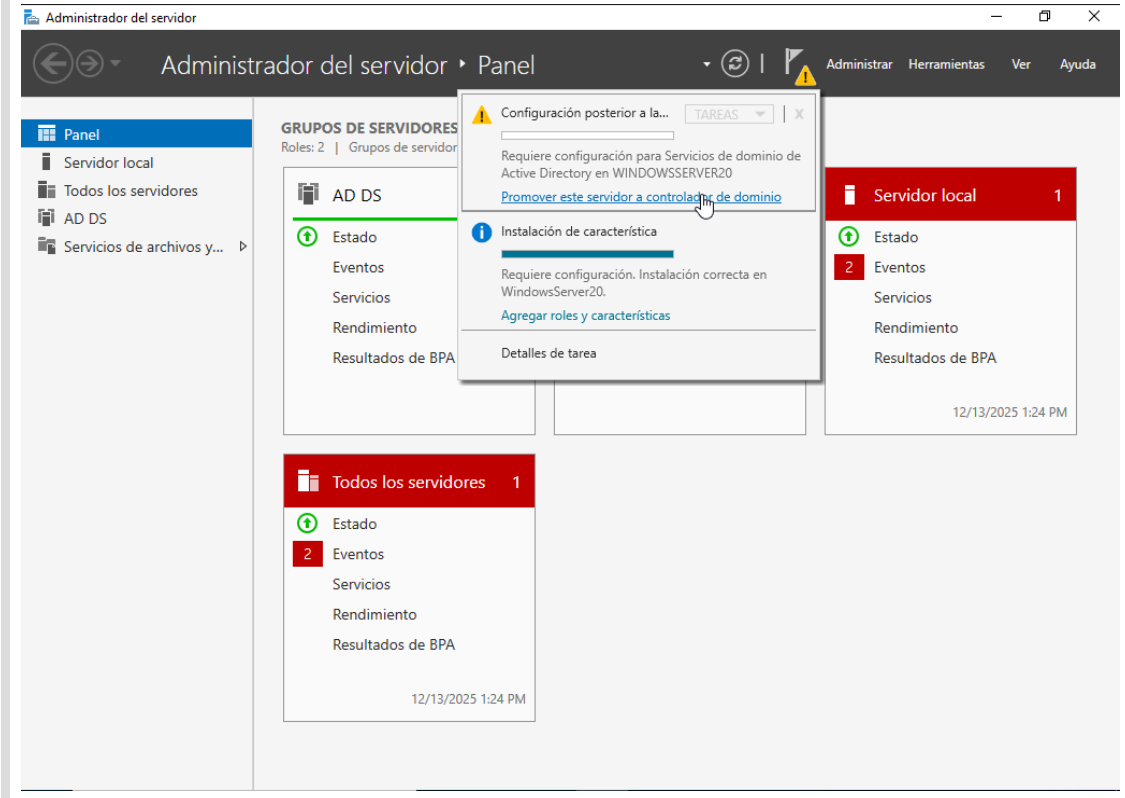


2.2. Promoción a Controlador de Dominio

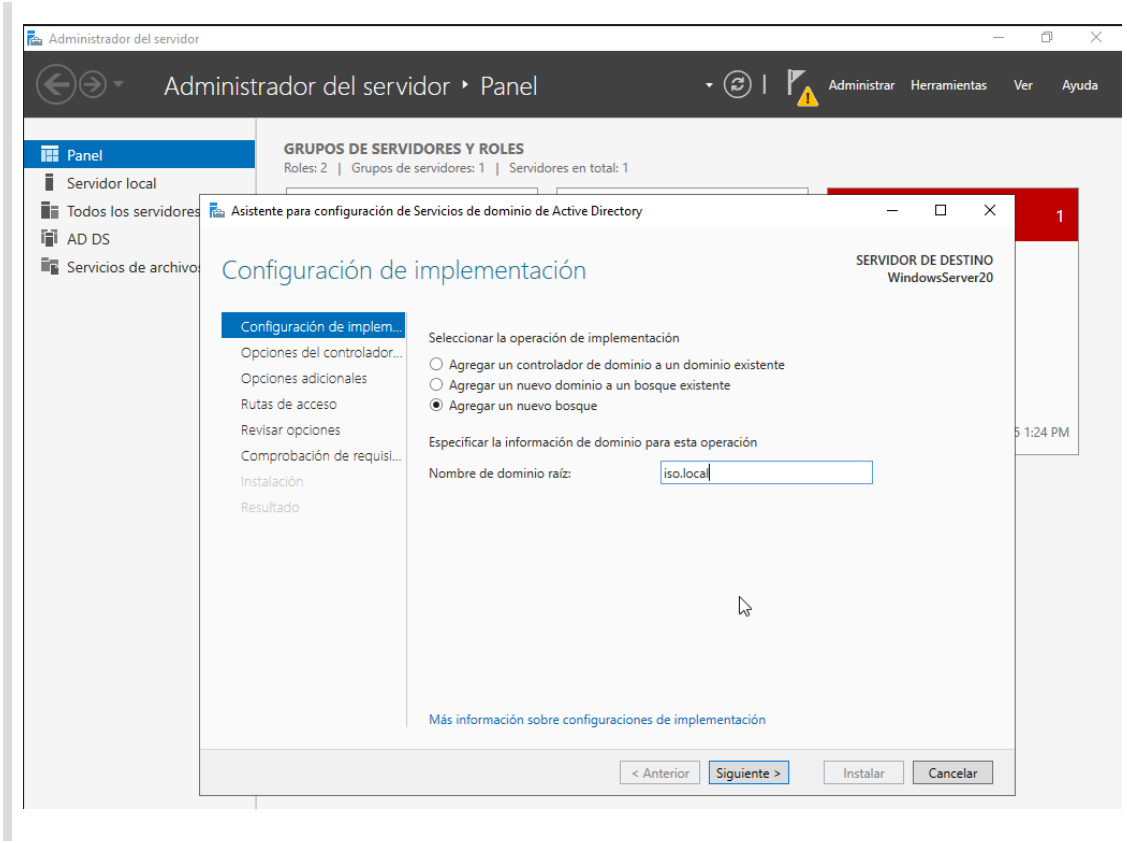
Una vez finalizada la instalación, aparece una notificación en el panel. Observamos que **AD DS** está instalado pero requiere configuración adicional.



Hacemos clic en la notificación amarilla que muestra el enlace **"Promover este servidor a controlador de dominio"**.

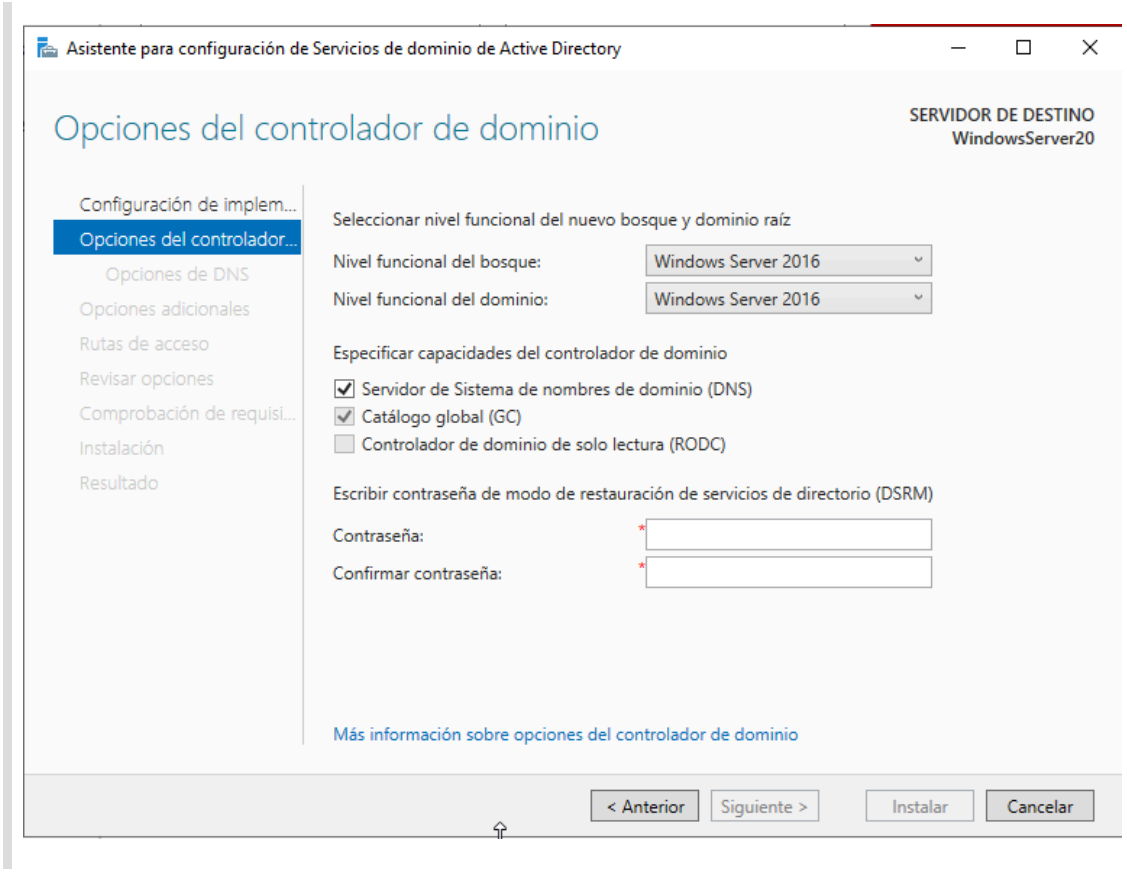


En la ventana de **Configuración de implementación**, seleccionamos **Agregar un nuevo bosque** e introducimos el nombre de dominio raíz: **iso.local**

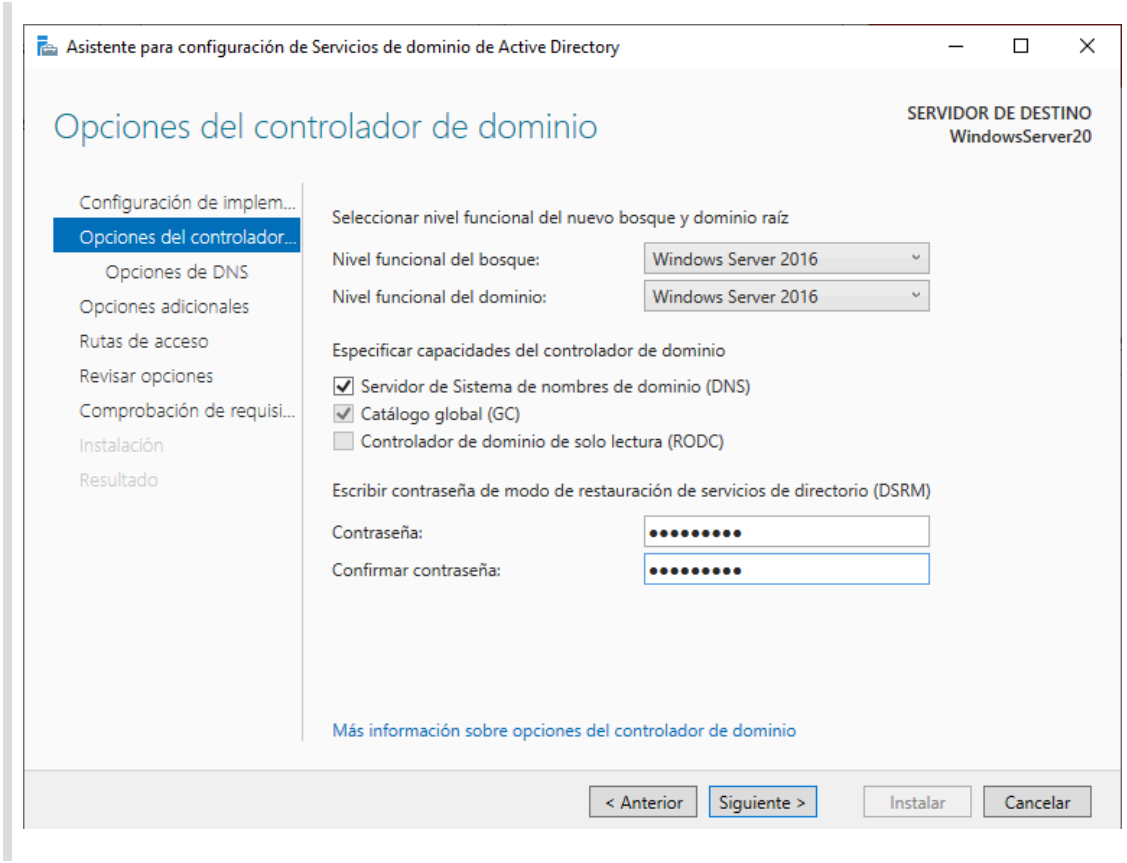


2.3. Opciones del Controlador de Dominio

Configuramos el nivel funcional del bosque y del dominio (Windows Server 2016). Marcamos las opciones **Servidor de Sistema de nombres de dominio (DNS)** y **Catálogo global (GC)**. A continuación, introducimos la contraseña de restauración de servicios de directorio (DSRM).

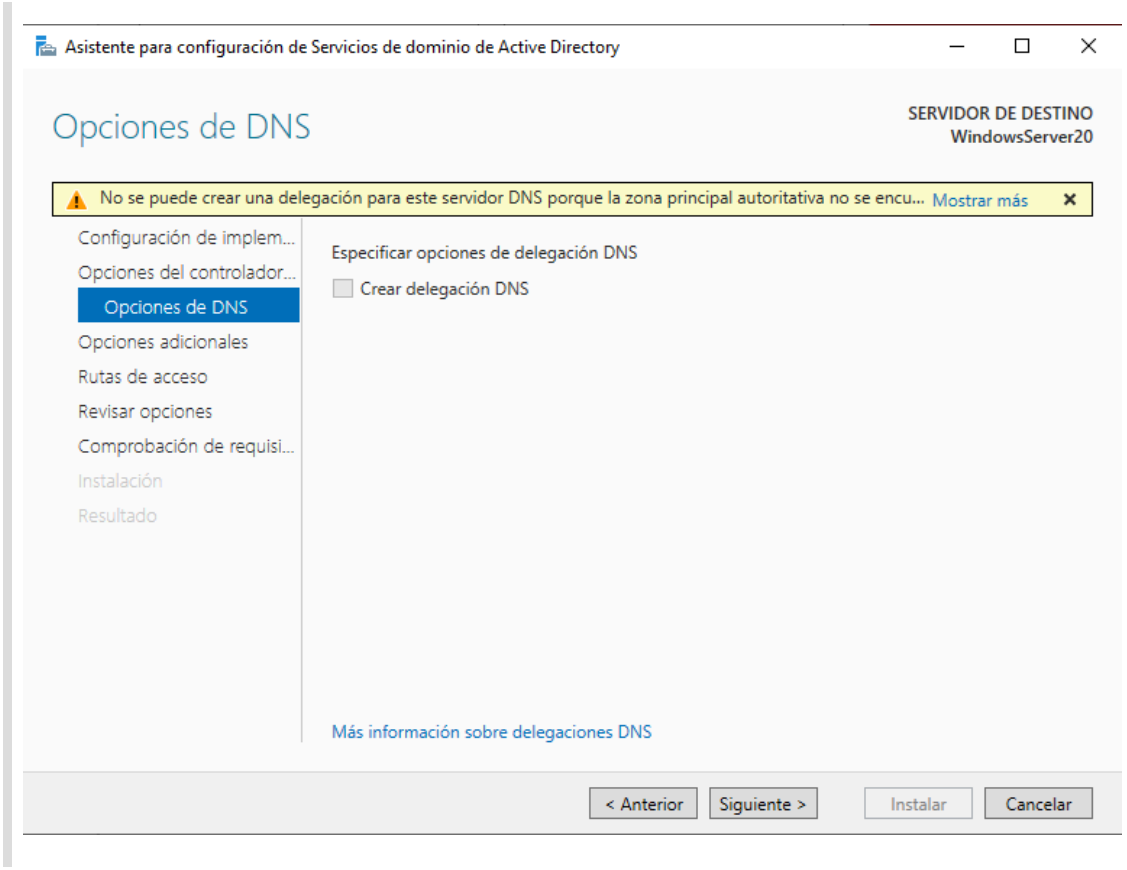


Confirmamos las contraseñas ingresadas.

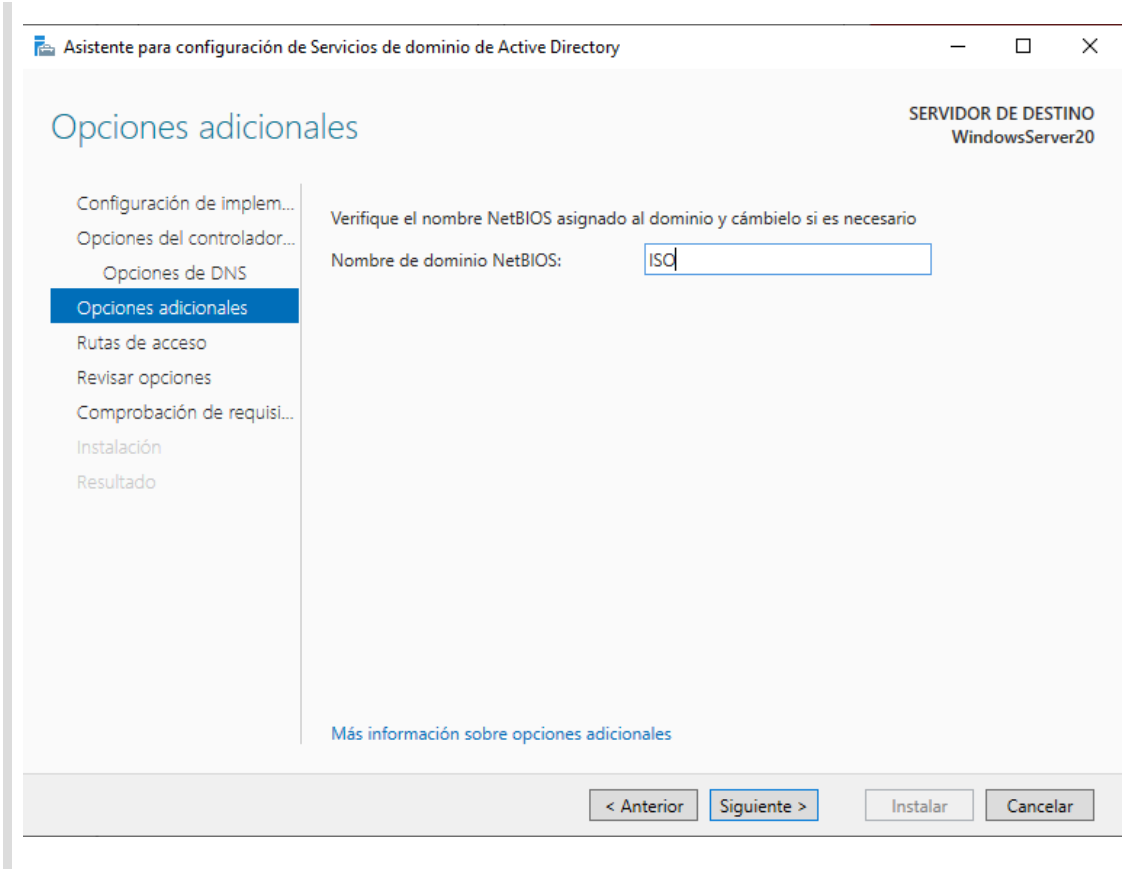


2.4. Opciones de DNS y Configuración

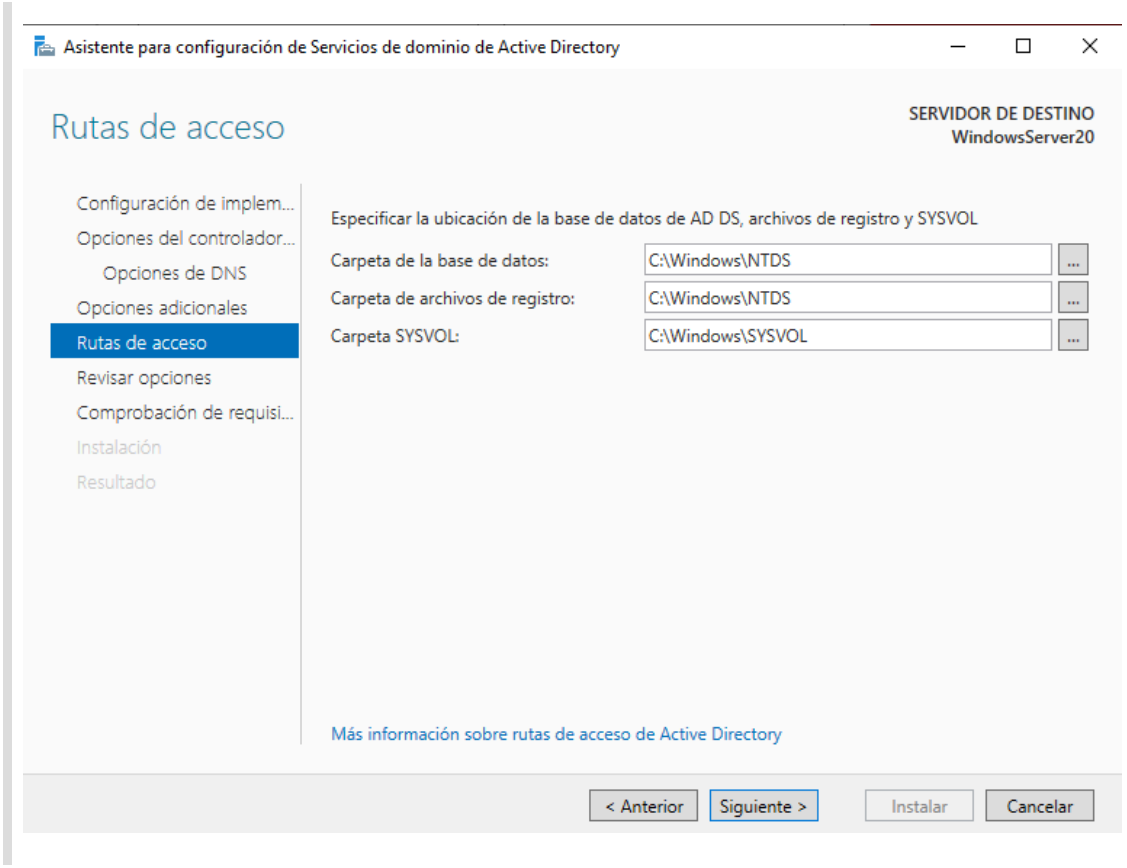
Aparece una advertencia sobre la delegación DNS. En este caso, no es necesario crear una delegación DNS, continuamos.



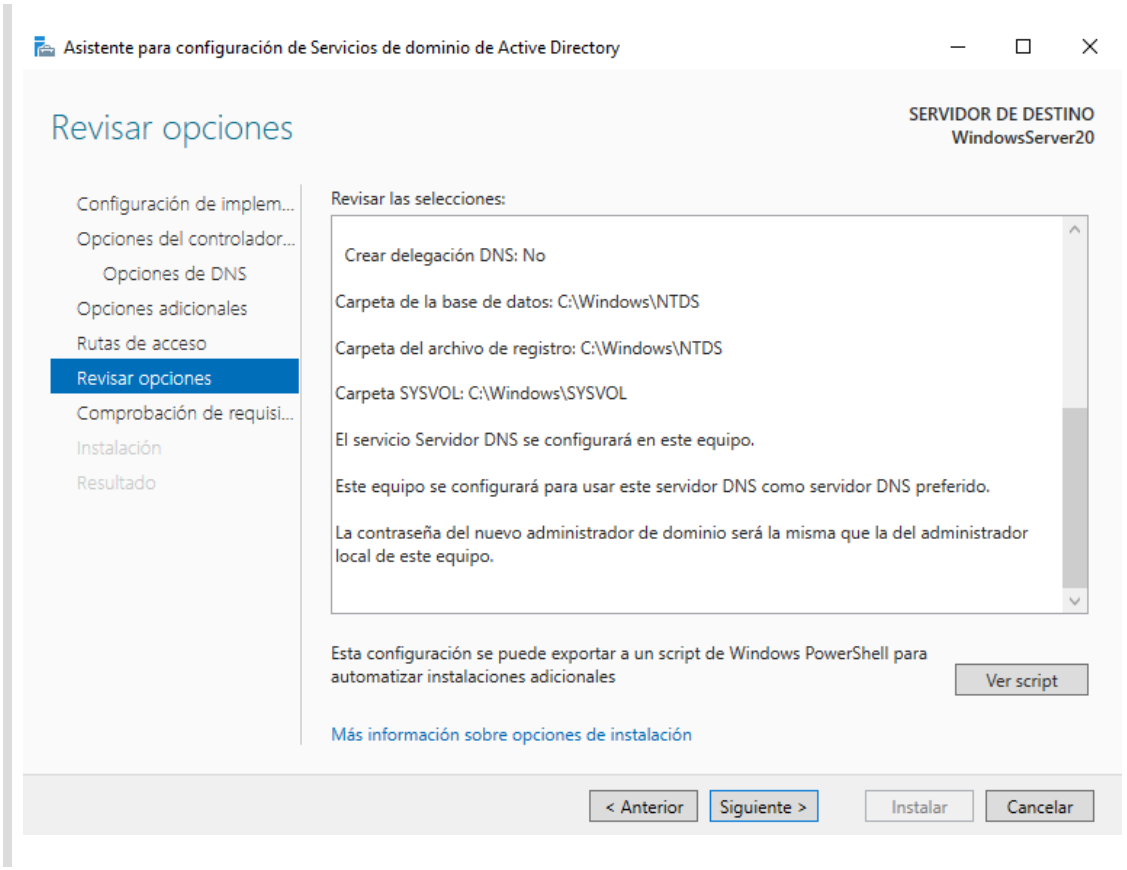
Verificamos el nombre NetBIOS asignado automáticamente: **ISO**



Confirmamos las rutas de la base de datos, archivos de registro y SYSVOL (valores por defecto en **C:\Windows\NTDS** y **C:\Windows\SYSVOL**).

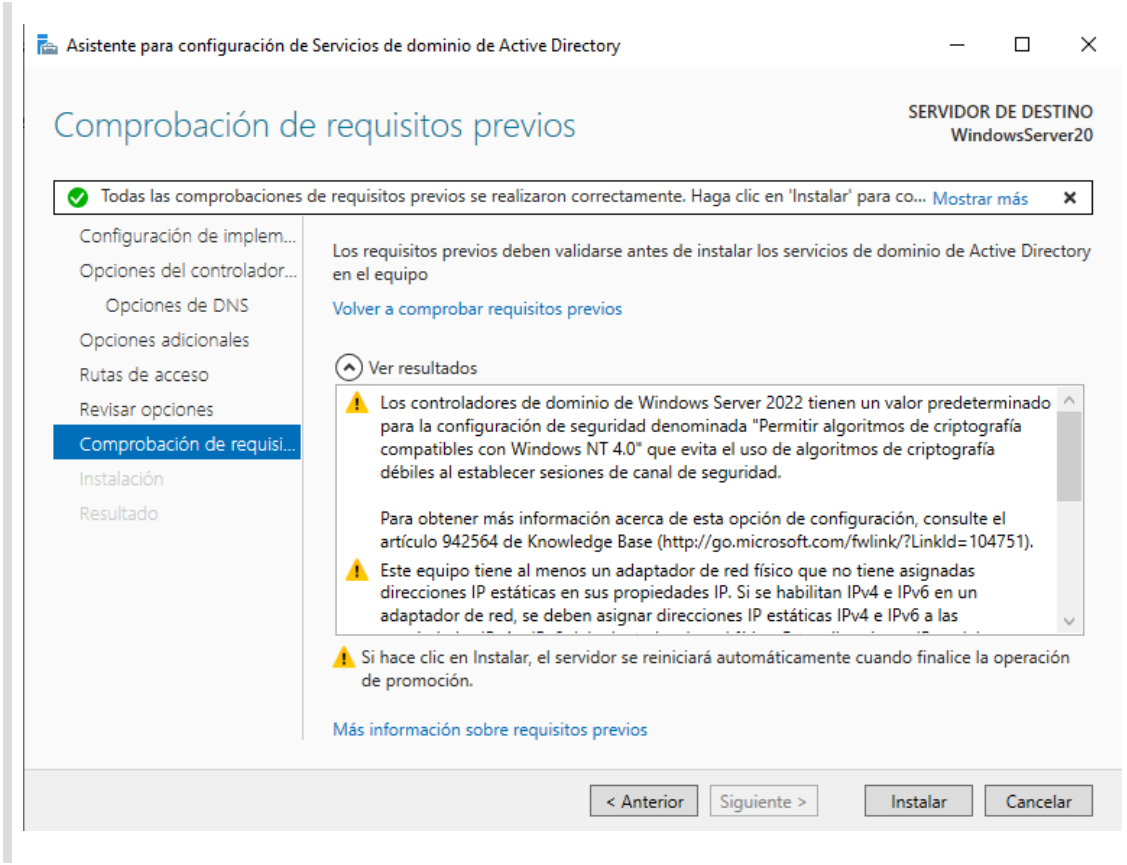


Revisamos el resumen de todas las opciones seleccionadas.

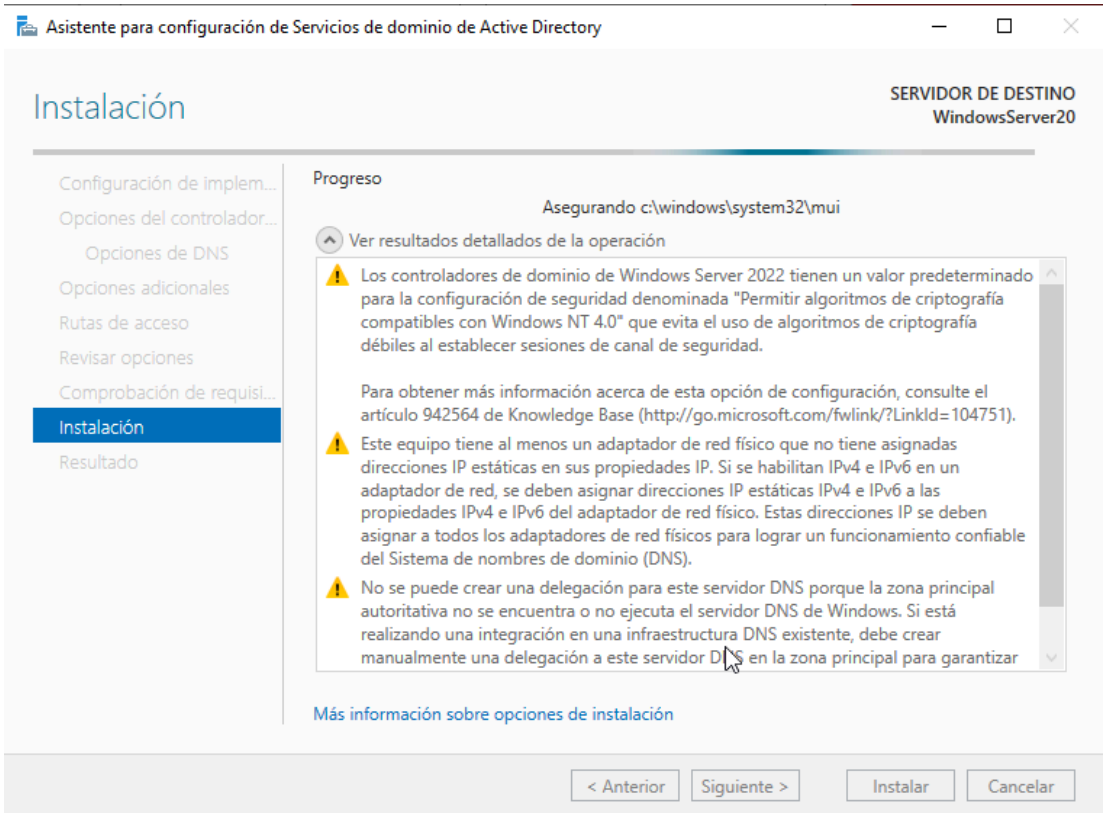


2.5. Instalación y Finalización

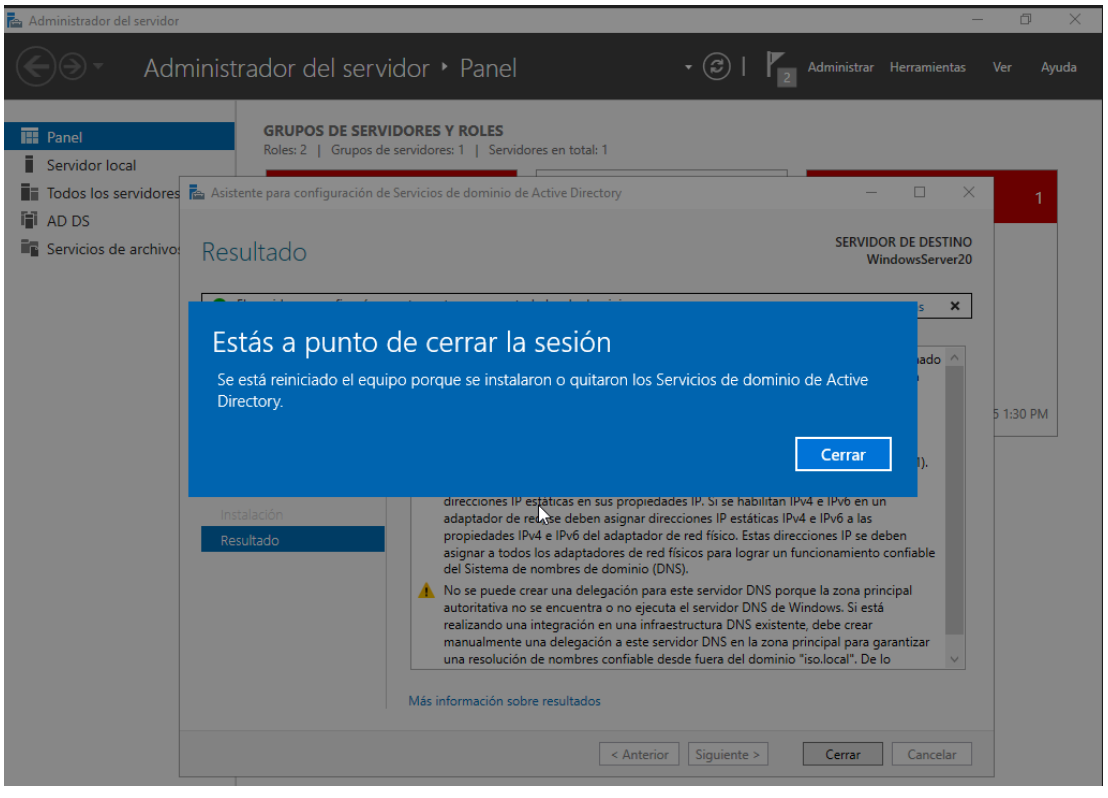
El asistente realiza la comprobación de requisitos previos. Verificamos que todas las comprobaciones se completaron correctamente (marca verde). Hacemos clic en **Instalar**.



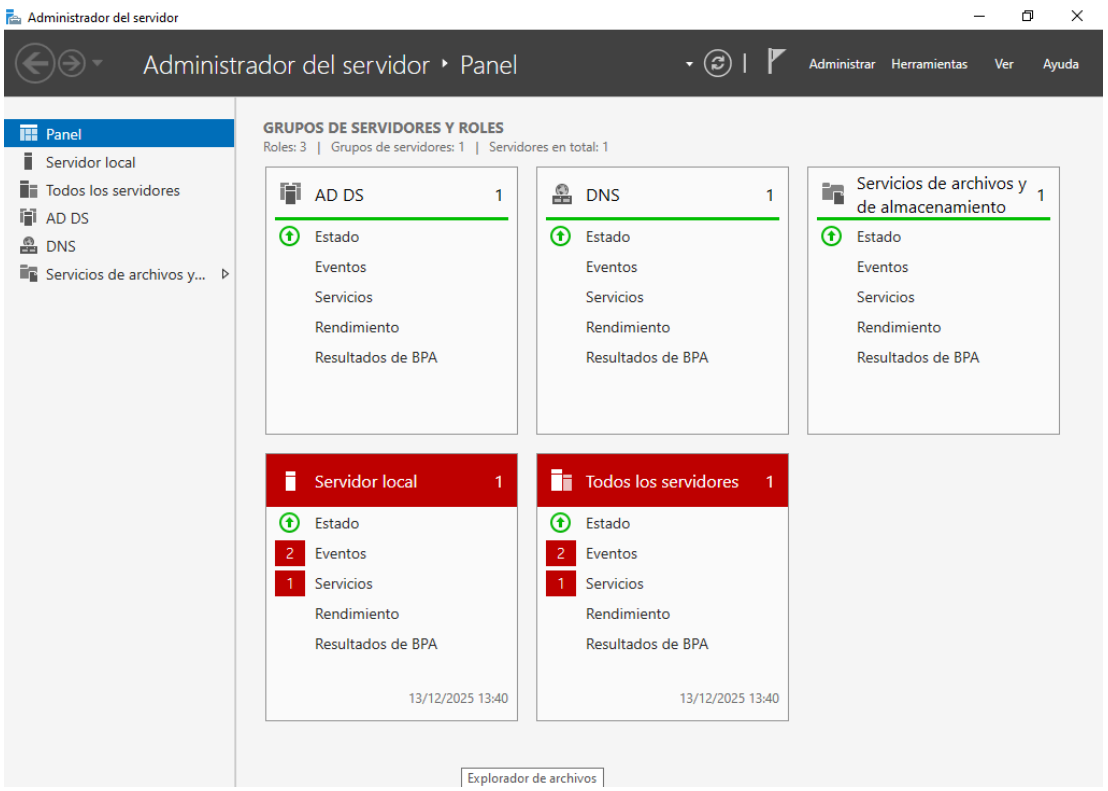
Comienza el proceso de instalación de AD DS.



El servidor aplica la configuración y se reinicia automáticamente.



Una vez reiniciado el servidor, accedemos al panel del **Administrador del servidor** y verificamos que los roles **AD DS** y **DNS** están operativos y en estado correcto.



---

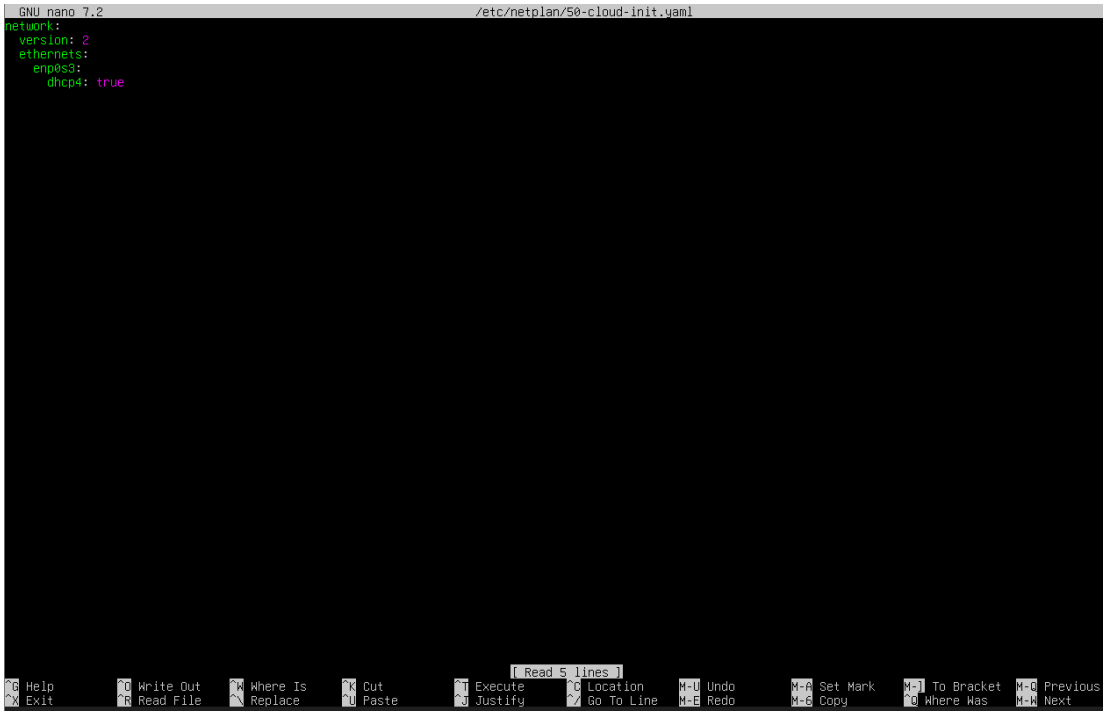
3. Fase 2: Configuración del Cliente Ubuntu

3.1. Configuración de Red

Verificamos la interfaz de red.

```
rafik@ubuntulab:~$ ip link
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT group default qlen 1000
    link/ether 08:00:27:58:97:24 brd ff:ff:ff:ff:ff:ff
rafik@ubuntulab:~$ ls /etc/netplan
50-cloud-init.yaml
rafik@ubuntulab:~$ sudo nano /etc/netplan/50-cloud-init.yaml_
```

Editamos el archivo de configuración de Netplan con `sudo nano /etc/netplan/50-cloud-init.yaml`.
Inicialmente, el archivo muestra una configuración básica con DHCP.



Modificamos el archivo para agregar los servidores DNS y el dominio de búsqueda:

- **nameservers**: `[192.168.1.111, 8.8.8.8]` (IP del controlador de dominio y DNS público)
- **search**: `[iso.local]`

Aplicamos la configuración con `sudo netplan apply` y verificamos la conectividad con el dominio ejecutando `ping iso.local`. Observamos respuestas exitosas desde el controlador de dominio (192.168.1.111).

```
rafik@ubuntulab:~$ ping iso.local
PING iso.local (192.168.1.111) 56(84) bytes of data.
64 bytes from WindowsServer20.home (192.168.1.111): icmp_seq=1 ttl=128 time=1.17 ms
64 bytes from WindowsServer20.home (192.168.1.111): icmp_seq=2 ttl=128 time=1.12 ms
64 bytes from WindowsServer20.home (192.168.1.111): icmp_seq=3 ttl=128 time=0.725 ms
64 bytes from WindowsServer20.home (192.168.1.111): icmp_seq=4 ttl=128 time=1.92 ms
64 bytes from WindowsServer20.home (192.168.1.111): icmp_seq=5 ttl=128 time=2.02 ms
64 bytes from WindowsServer20.home (192.168.1.111): icmp_seq=6 ttl=128 time=1.47 ms
^C
--- iso.local ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 6628ms
rtt min/avg/max/mdev = 0.725/1.406/2.023/0.455 ms
rafik@ubuntulab:~$
```

3.2. Instalación de Paquetes

Ejecutamos la actualización de repositorios e instalamos los paquetes necesarios para la integración con Active Directory. Introducimos la contraseña de sudo cuando se solicita:

`sudo apt update && apt install -y realmd sssd sssd-tools samba-common krb5-user packagekit samba-common-bin samba-libs adcli`

```
rafik@ubuntulab:~$ sudo apt update && apt install -y realmd sssd sssd-tools samba-common krb5-user packagekit samba-common-bin samba-libs adcli
[sudo] password for rafik: _
```

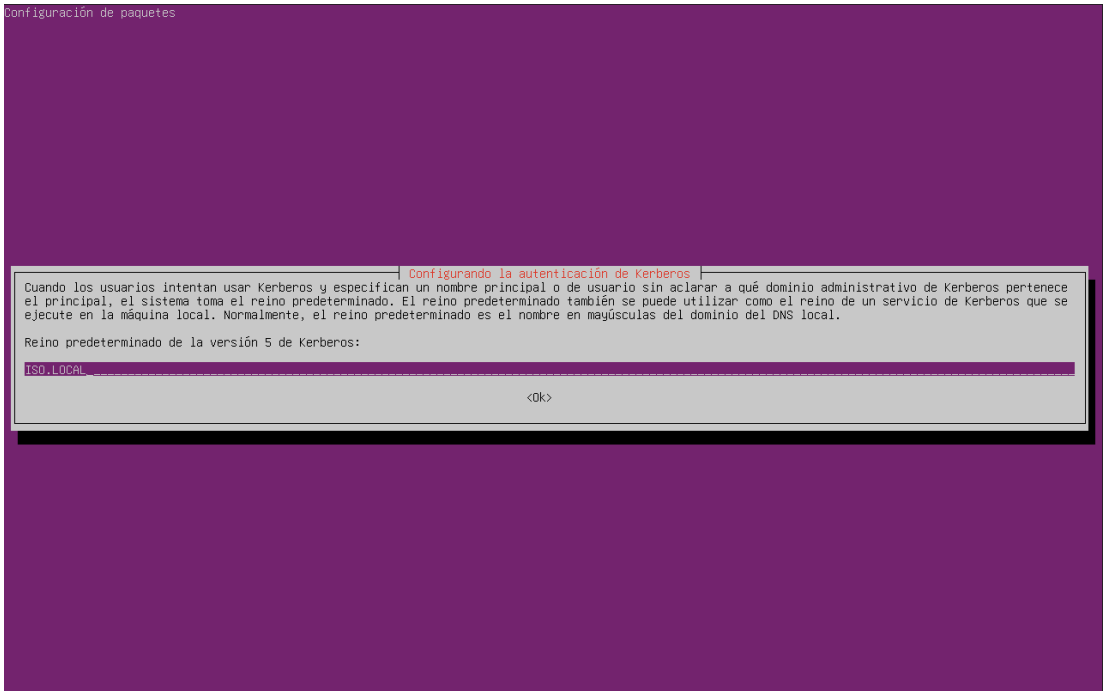
Continuamos con la instalación del cliente Kerberos:

`sudo apt update && sudo apt install -y krb5-user`

```
rafik@ubuntulab:~$ sudo apt update && sudo apt install -y krb5-user
```

3.3. Configuración de Kerberos

Durante la instalación de **krb5-user**, el sistema solicita el **reino predeterminado de Kerberos**. Introducimos: **ISO.LOCAL** (en mayúsculas).



3.4. Unión al Dominio

Ejecutamos el comando para unir el cliente Ubuntu al dominio Active Directory:

```
sudo realm join -v iso.local -U administrador
```

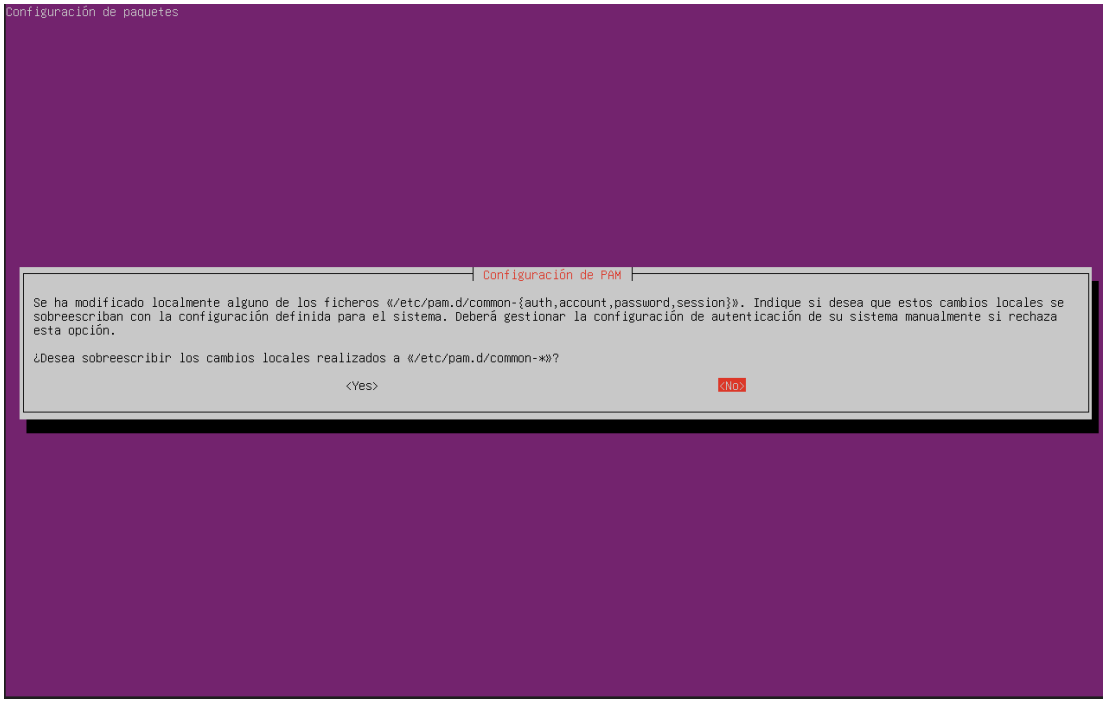
El proceso realiza múltiples operaciones:

- Resolución DNS del dominio
- Lookup LDAP
- Descubrimiento del dominio
- Autenticación del usuario administrador
- Configuración de Kerberos
- Creación de la cuenta del equipo en AD
- Configuración de SSSD
- Inscripción exitosa del equipo en el dominio

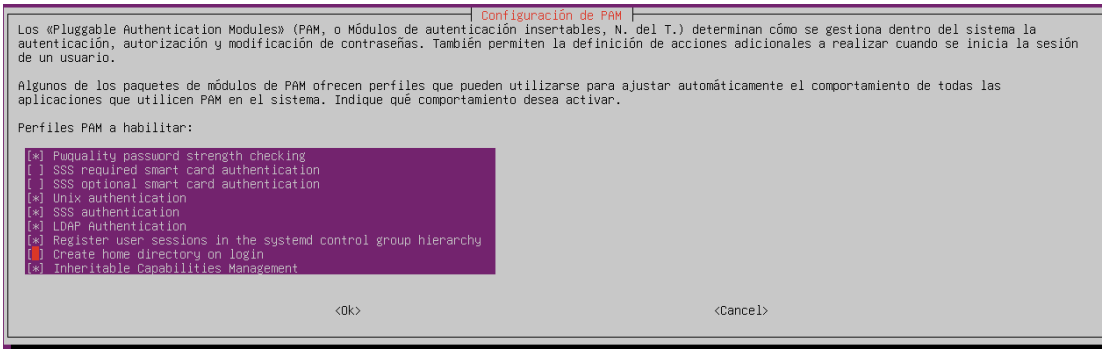
```
rafik@ubuntulab:~$ sudo realm join -v iso.local -U administrador
 * Resolving: _ldap._tcp.iso.local
 * Performing LDAP DSE lookup on: 192.168.1.111
 * Successfully discovered: iso.local
Password for administrador:
 * Unconditionally checking packages
 * Resolving required packages
 * LANG=C /usr/sbin/adcli join --verbose --domain iso.local --domain-realm ISO.LOCAL --domain-controller 192.168.1.111 --login-type user --login-user administra
dor --stdin-password
 * Using domain name: iso.local
 * Calculated computer account name from fqdn: UBUNTULAB
 * Using domain realm: iso.local
 * Sending NetLogon ping to domain controller: 192.168.1.111
 * Received NetLogon info from: WindowsServer20.iso.local
 * Wrote out krb5.conf snippet to /var/cache/realmd/adcli-krb5-RmfYuP/krb5.d/adcli-krb5-conf-Op9ohr
 * Authenticated as user: administrador@ISO.LOCAL
 * Using GSS-SPNEGO for SASL bind
 * Looked up short domain name: ISO
 * Looked up domain SID: S-1-5-21-921112308-292009824-2475114784
 * Received NetLogon info from: WindowsServer20.iso.local
 * Using fully qualified name: ubuntulab
 * Using domain name: iso.local
 * Using computer account name: UBUNTULAB
 * Using domain realm: iso.local
 * Calculated computer account name from fqdn: UBUNTULAB
 * Generated 120 character computer password
 * Using keytab: FILE:/etc/krb5.keytab
 * A computer account for UBUNTULAB$ does not exist
 * Found well known computer container at: CN=Computers,DC=iso,DC=local
 * Calculated computer account: CN=UBUNTULAB,CN=Computers,DC=iso,DC=local
 * Encryption type [3] not permitted.
 * Encryption type [1] not permitted.
 * Created computer account: CN=UBUNTULAB,CN=Computers,DC=iso,DC=local
 * Trying to set computer password with Kerberos
 * Set computer password
 * Retrieved kvno '2' for computer account in directory: CN=UBUNTULAB,CN=Computers,DC=iso,DC=local
 * Checking RestrictedKrbHost/UBUNTULAB
 *    Added RestrictedKrbHost/UBUNTULAB
 * Checking host/UBUNTULAB
 *    Added host/UBUNTULAB
 * Discovered which keytab salt to use
 * Added the entries to the keytab: UBUNTULAB$@ISO.LOCAL: FILE:/etc/krb5.keytab
 * Added the entries to the keytab: host/UBUNTULAB@ISO.LOCAL: FILE:/etc/krb5.keytab
 * Added the entries to the keytab: RestrictedKrbHost/UBUNTULAB@ISO.LOCAL: FILE:/etc/krb5.keytab
 * /usr/sbin/update-rc.d sssd enable
 * /usr/sbin/service sssd restart
 * Successfully enrolled machine in realm
rafik@ubuntulab:~$ _
```

3.5. Configuración de PAM

El sistema solicita sobrescribir la configuración local de PAM. Seleccionamos **No** para mantener nuestra configuración personalizada.



Ejecutamos `sudo pam-auth-update` para configurar los módulos PAM. Marcamos la opción **"Create home directory on login"** para que se cree automáticamente el directorio personal de los usuarios del dominio en su primer inicio de sesión.

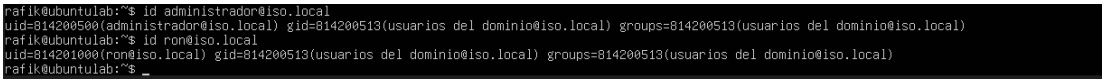


3.6. Verificación y Pruebas

Verificamos que los usuarios del dominio son reconocidos por el sistema ejecutando:

`id administrador@iso.local` `id ron@iso.local`

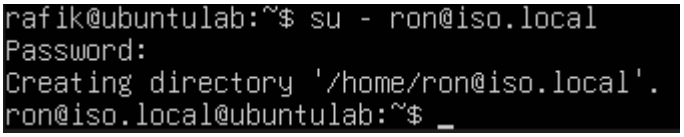
El comando `id` muestra la información de UID, GID y grupos de los usuarios del dominio, confirmando la correcta integración.



Probamos el cambio de usuario al usuario del dominio **ron@iso.local** con:

`su - ron@iso.local`

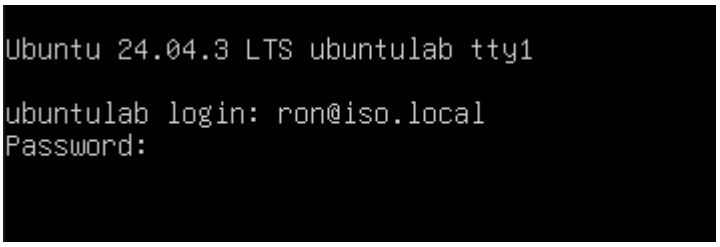
El sistema solicita la contraseña y crea automáticamente el directorio home en `/home/ron@iso.local`.



Finalmente, probamos el inicio de sesión desde otra terminal:

`ssh ron@iso.local@ubuntulab` (o usando la IP del cliente)

El login se completa exitosamente como **ron@iso.local**, confirmando que la autenticación centralizada funciona correctamente.



---

4. Conclusión

Se ha completado exitosamente la integración del cliente Ubuntu con el dominio Active Directory **iso.local**. Los usuarios del dominio pueden ahora autenticarse en el sistema Linux utilizando sus credenciales de Active Directory, con creación automática de directorios personales en el primer inicio de sesión.

Este tipo de configuración permite centralizar la gestión de usuarios en entornos mixtos Windows/Linux, facilitando la administración y mejorando la seguridad mediante políticas de dominio unificadas.

Fin de la práctica.