

# **Producto 1. Administración remota del servicio de directorio**

**Fast&Query**



## **Descripción**

Nos acabamos de incorporar a la plantilla de la empresa Trust SL y como administradores de sistemas lo primero que hemos hecho es analizar el estado del sistema actual. En la empresa ya disponen de un servidor y diversas estaciones de trabajo, ofrece servicios y recursos pero no hay ningún tipo de gestión ni control sobre ellos.

Nuestra tarea consiste en crear una infraestructura de dominio con el objetivo de centralizar la gestión y administración de los recursos y servicios de la red. Esta administración se podrá hacer de forma remota.

Para ello primero deberemos analizar el sistema actual y proponer un diseño de la solución de la estructura del dominio y sus objetos, junto con una matriz de control de acceso a los recursos del dominio, implementación de un mapa lógico y físico. Finalmente se llevará a cabo la implementación del dominio y la habilitación de servicios de administración remota para administrar el dominio y sus recursos.

## **Objetivos**

Analizar y diseñar la infraestructura lógica del dominio e instalar, configurar y administrar de forma remota el servicio de directorio, el dominio y sus objetos, así como la configuración del servidor DHCP y DNS.

A. El estudio del sistema actual debe contener como mínimo:	4
I. Toda la información relativa al parque informático de la empresa.....	4
II. Qué servicios y recursos ofrece el sistema.....	4
III. Quiénes son los usuarios que utilizan el sistema, qué tipo de organización o estructura tienen dentro del sistema informático y qué restricciones de seguridad se les aplica.....	4
IV. Qué restricciones de seguridad y acceso se aplican actualmente a cada recurso y/o servicio.....	5
B. El análisis del sistema debe contener como mínimo:	5
I. La situación a la que se desea llegar respecto al sistema informático.....	5
II. Los servicios y recursos que éste debe ofrecer.....	5
III. Diagrama con la estructura organizativa a implantar.....	5
IV. Diseñar una matriz de control de acceso sobre los recursos y los usuarios del sistema. Solamente se debe diseñar, se implementará posteriormente en otro producto. Se puede diseñar en forma de tabla, donde se deben representar los recursos y los grupos del dominio, junto con sus permisos.....	6
Recursos del sistema.....	6
Grupos de usuarios.....	7
Matriz de control de acceso (ACL).....	7
Consideraciones técnicas.....	8
V. Posibles ampliaciones/servicios que podría ofrecer el sistema en un futuro (prever qué más podría ofrecer el sistema informático a los usuarios y plantearlo como una mejora a medio plazo).....	8
VI. Crear un mapa físico con la disposición del nuevo sistema informático y un mapa lógico con todos los elementos y servicios que ofrece el sistema.	
En este apartado se trata de describir qué debería hacer el sistema y qué necesitamos. Además, se debe incluir en este apartado, qué necesitamos para poder integrar sistemas operativos libres y propietarios en el dominio.....	9
¿Qué debe hacer el sistema?.....	10
Inventario de equipos — Trust S.L.....	12
SERVIDORES DEL DOMINIO.....	12
DEPARTAMENTO TIC.....	12
ADMINISTRACIÓN Y FINANZAS.....	12
DEPARTAMENTO COMERCIAL.....	13
DEPARTAMENTO DE DISEÑO.....	13
GERENCIA.....	14
Resumen de red por bloques de IP .....	14
Requisitos comunes de red y autenticación.....	14
Integración de sistemas Windows (propietarios).....	15
Integración de sistemas Linux (libres).....	15
• Sincronización horaria (NTP).....	16
• Instalación de paquetes necesarios.....	16
• Autenticación en el servidor de Kerberos.....	16
• Configuración de Samba.....	16
• Unión al dominio Active Directory.....	17
• Configuración de resolución de usuarios del dominio.....	17
• Integración con PAM (autenticación del sistema).....	17

C. El diseño de la solución debe concretar la parte de análisis, indicando cómo se debe implementar el sistema para implantarlo.	
Solamente se debe diseñar, se implementará posteriormente. El diseño se puede hacer mediante un diagrama o esquema. Cualquier duda sobre el parque informático será resuelta por el consultor, el cual actuará como referente TIC del sistema.....	18
Flujo general de funcionamiento.....	18
<b>2. Implementar el diseño lógico mediante máquinas virtuales con sistemas operativos servidores (instalar tantos como se especifiquen en el diseño). Recuerda poner un nombre significativo al servidor, configurar la dirección IP estática, y reiniciar la “mac” desde virtualbox para evitar problemas.....</b>	<b>19</b>
Configuración red interna para el servidor.....	22
Unir Windows 11 al dominio.....	27
<b>3. Instalar el servicio de directorio tal como se ha especificado en el diseño de la solución. Crear un vídeo tutorial en el cual se demuestre la instalación y configuración del servicio de directorio.....</b>	<b>30</b>
A. Explicar el proceso de instalación.....	31
<b>4. Instalar y configurar el servicio DHCP y DNS en el servidor para que sea éste quién de las ip's a los equipos de la red. El rango de ip's no tiene que ser superior a 254, es decir, tendrá que ser un rango con máscara /24 o 255.255.255.0; Documentar el proceso de instalación mediante capturas de pantalla.....</b>	<b>37</b>
A. Explicar el proceso de instalación.....	37
Crear un ámbito.....	41
B. Detallar la configuración establecida y el contenido de los ficheros.....	44
Configurar una Zona Inversa.....	45
C. Demostrar el correcto funcionamiento del servidor DHCP y DNS.....	50
Mostrar el correcto funcionamiento de DNS.....	50
Mostrar el correcto funcionamiento de DHCP.....	50
<b>5. Instalar herramientas de administración remota para configurar el/los servidores. La configuración de este servicio, sólo permitirá acceder desde un rango de direcciones IP determinado y tan sólo a un usuario específico. Crear un vídeo tutorial en el cual se demuestre la instalación y configuración de herramientas de administración remota.....</b>	<b>51</b>
A. Explicar el proceso de instalación del Escritorio remoto.....	52
Habilitar Escritorio Remoto en el servidor:.....	52
Conectar desde el cliente:.....	52
Opciones avanzadas:.....	52
B. Configurar RSAT y mostrar el proceso de instalación y acceso.....	53
C. Mostrar y comentar qué ficheros son necesarios para su correcto funcionamiento.....	54
D. Detallar la configuración establecida y el contenido de los ficheros.....	54
E. Mostrar el funcionamiento y la conexión remota a la máquina.....	55
Configuración de RDP (Escritorio Remoto) Multi-sesión.....	57
Configurar Escritorio remoto para la máquina de Windows 11.....	58
F. Comprobar el correcto funcionamiento del nuevo sistema informático y el servicio de directorio.....	59
Bibliografía.....	60
Anexo.....	61
Instalación de Ubuntu Desktop y unirlo al dominio.....	61
SNAT en Windows Server 2025.....	63

## A. El estudio del sistema actual debe contener como mínimo:

### I. Toda la información relativa al parque informático de la empresa.

- 1 “servidor” ofimático que aloja: aplicación de **facturación web**, carpetas compartidas sin control y un **backup parcial** (sólo facturación).

Puestos de trabajo:

- **Windows** (propietario) para la mayoría.
- **Linux** (libre) para **Comercial**; a corto plazo también para **Administración**.

Periféricos:

- **Multifunción** en Administración.
- **Impresora láser A3 color** en Comercial .
- **Plotter** en Diseño.

Red local sin gestión centralizada; direccionamiento no documentado; sin DNS/DHCP gestionados.

### II. Qué servicios y recursos ofrece el sistema.

- Aplicación de facturación y contabilidad (acceso web local).
- Carpeta “compartida para todos” sin permisos ni auditoría.
- Copias de seguridad **manuales y parciales**.

### III. Quiénes son los usuarios que utilizan el sistema, qué tipo de organización o estructura tienen dentro del sistema informático y qué restricciones de seguridad se les aplica.

- **Gerente**: Francisco García.
- **Administración y Finanzas**: Ernesto Prats (Administración), Mario Donderis (Finanzas), **Benjamín Placeta** (coordinador).
- **Comercial**: Gabriel Gomera, Juan Machado; **Alexis Blasco** (coordina Comercial y Diseño).
- **Diseño**: Javier Gandía.
- **TIC**: equipo técnico (Rubén) bajo coordinación de Benjamín.
- **Seguridad actual**: inexistente; acceso abierto a todo; sin autenticación central ni segregación por funciones.

#### IV. Qué restricciones de seguridad y acceso se aplican actualmente a cada recurso y/o servicio.

- No hay **control de acceso** ni **trazabilidad**.
- No hay **perfiles** ni **grupos**; no hay **políticas**; backups insuficientes.

**Conclusión del estudio:** el sistema carece de gobierno de identidades, permisos y servicios básicos de infraestructura. Existe riesgo de pérdida de datos, fuga de información y tiempos muertos por dependencias físicas.

#### B. El análisis del sistema debe contener como mínimo:

##### I. La situación a la que se desea llegar respecto al sistema informático.

- Dominio **trust.lan** con **2 controladores de dominio** replicando.
- DC1: **AD DS + DNS + DHCP + servidor de archivos**.
- DC2: **AD DS + servidor de impresión**.
- Gestión de accesos mediante **grupos**.
- Administración remota desde un equipo de TIC con alcance IP restringido.

##### II. Los servicios y recursos que éste debe ofrecer.

- **Autenticación** y **autorización** centralizadas (AD DS).
- **DNS** interno para el dominio, **DHCP /24**.
- **Comparticiones SMB** con permisos NTFS conforme a matriz.
- **Impresión** publicada en el directorio y restringida por departamento.  
**Carpeta de escáner y carpetas personales**.
- Base para **GPO** (endurecimiento, mapeo de unidades, redirección de carpetas).

##### III. Diagrama con la estructura organizativa a implantar.

- OU raíz: **Trust SL**
  - OU **Usuarios**: Gerencia, Administración, Finanzas, Comercial, Diseño, TIC
  - OU **Equipos**
  - OU **Servidores**
- Grupos (Global/Security): **grupo.gerencia, grupo.administracion, grupo.finanzas, grupo.comercial, grupo.diseño, grupo.tic**
- Cuentas de usuario (formato **nombre.apellido**).

IV. Diseñar una matriz de control de acceso sobre los recursos y los usuarios del sistema. Solamente se debe diseñar, se implementará posteriormente en otro producto. Se puede diseñar en forma de tabla, donde se deben representar los recursos y los grupos del dominio, junto con sus permisos.

### *Recursos del sistema*

<b>Tipo de Recurso</b>	<b>Nombre / Ruta</b>	<b>Descripción</b>
Carpeta compartida general	\SRV-DC1\Public	Carpeta de acceso común a todos los usuarios (comunicaciones internas, plantillas).
Carpeta Administración y Finanzas	\SRV-DC1\AdminFinanzas	Documentación financiera, facturas, nóminas, presupuestos.
Carpeta Comercial	\SRV-DC1\Comercial	Presupuestos, pedidos, listados de clientes.
Carpeta Diseño	\SRV-DC1\Diseño	Archivos de diseño gráfico, materiales publicitarios.
Carpeta TIC	\SRV-DC1\TIC	Configuraciones, scripts, copias de seguridad, documentación técnica.
Carpeta Gerencia	\SRV-DC1\Gerencia	Informes y documentación privada de la dirección.
Aplicación de facturación y contabilidad	<a href="http://srv-dc1/appfacturacion">http://srv-dc1/appfacturacion</a>	Aplicación web contable centralizada.
Servidor de copias de seguridad	\SRV-DC2\Backup	Almacenamiento de copias programadas.
Impresora multifunción	IMP-AF01	Red — acceso general (controlado por dominio).
Impresora láser color	IMP-COM01	Red — solo acceso al grupo Comercial.
Plotter gran formato	IMP-DIS01	Red — solo acceso al grupo Diseño.

## Grupos de usuarios

Grupo / Departamento	Miembros
<b>Gerencia</b>	Francisco García
<b>Administración y Finanzas</b>	Benjamín Placeta, Ernesto Prats, Mario Donderis
<b>Comercial</b>	Alexis Blasco, Gabriel Gomera, Juan Machado
<b>Diseño</b>	Javier Gandía
<b>TIC</b>	Rubén
<b>Todos (Usuarios del Dominio)</b>	Todos los anteriores

## Matriz de control de acceso (ACL)

Recurso / Usuario o Grupo	Gerencia	Adm. y Finanzas	Comercial	Diseño	TIC	Todos
\SRV-DC1\Public	RW	RW	RW	RW	RW	RW
\SRV-DC1\AdminFinanzas	R	RW	-	-	RW	-
\SRV-DC1\Comercial	R	R	RW	R	RW	-
\SRV-DC1\Diseno	R	-	R	RW	RW	-
\SRV-DC1\TIC	R	R	R	R	RW	-
\SRV-DC1\Gerencia	RW	R	-	-	RW	-
App Facturación/Contabilidad	R	RW	-	-	RW	-
Servidor de Backup	R	R	-	-	RW	-
IMP-AF01 (Fotocopiadora)	R	RW	R	R	RW	R
IMP-COM01 (Impresora A3)	R	-	RW	-	RW	-
IMP-DIS01 (Plotter)	R	-	-	RW	RW	-

Leyenda:

- RW = Lectura y escritura (permiso completo)
- R = Solo lectura
- - = Sin acceso

## Consideraciones técnicas

- **Integración Linux-Windows:**

Los equipos Linux (Comercial y TIC) se unirán al dominio mediante **Samba** (cliente LDAP + Kerberos) para autenticarse y acceder a carpetas SMB con permisos del dominio.

- **Carpetas personales:** cada usuario tendrá su carpeta privada (\SRV-DC1\Usuarios\Nombre) con permisos exclusivos (RW propio).

- **Impresoras:** se publican en el servidor de impresión del dominio (Windows Print Server) y se asignan por **GPO** según grupo.

- **Aplicación web contable:** protegida con autenticación integrada (NTLM/Kerberos).

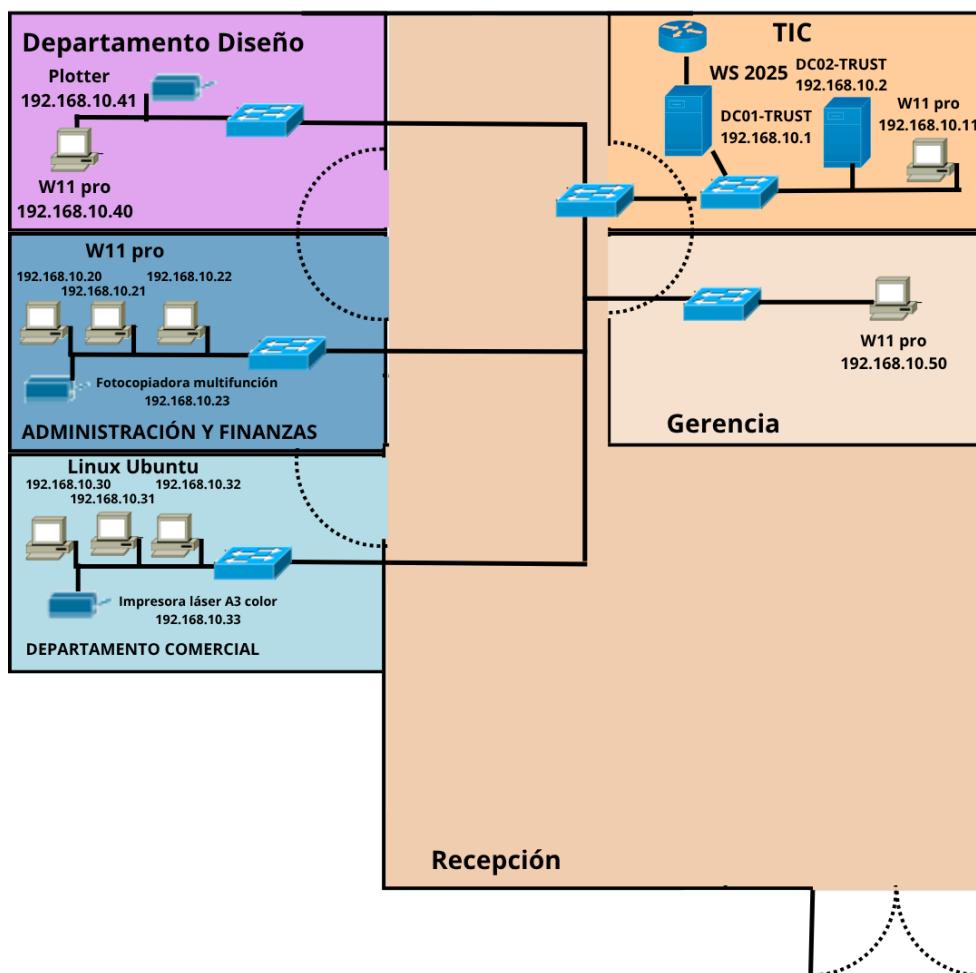
- **Copias de seguridad:** automatizadas por el usuario TIC con privilegios administrativos sobre \SRV-DC2\Backup.

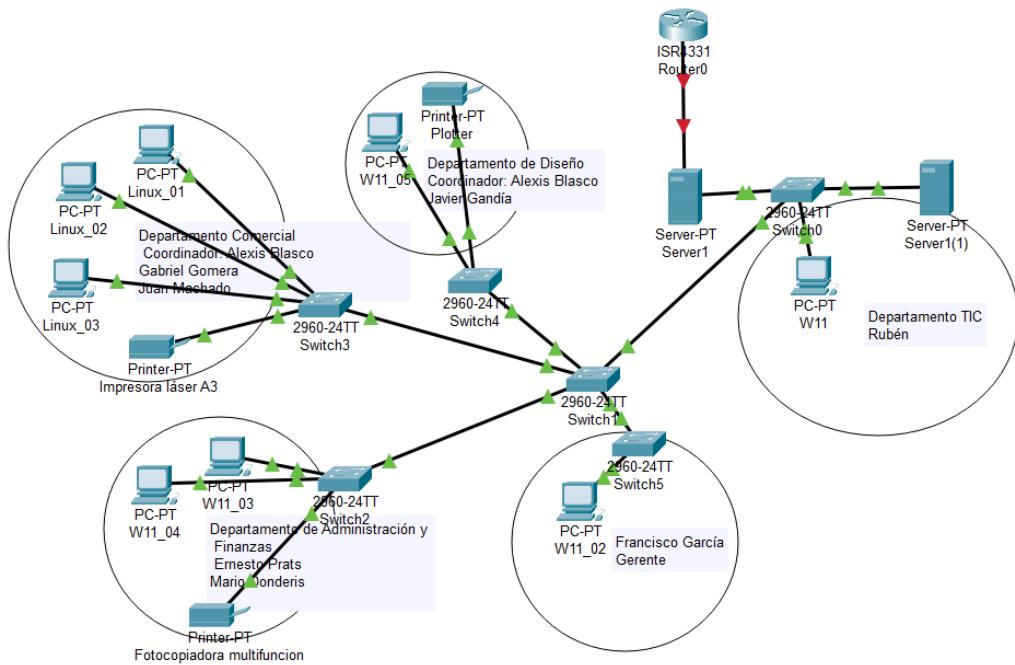
### v. Posibles ampliaciones/servicios que podría ofrecer el sistema en un futuro (prever qué más podría ofrecer el sistema informático a los usuarios y plantearlo como una mejora a medio plazo).

- Podríamos incluir en un futuro un servicio de copias de seguridad centralizado, con el objetivo de garantizar la integridad de la información y minimizar las pérdidas por fallos. Con las siguientes características:
  - Implantar un backup incremental automatizado .
  - Programar tareas automáticas (diarias/semanales) para respaldar servidores, carpetas compartidas y bases de datos.
  - Probar restauraciones periódicas y mantener histórico de versiones.
- Implantación de un servicio de correo electrónico corporativo, cuyo objetivo será profesionalizar la comunicación interna y externa.
  - Sincronización con el directorio (autenticación LDAP o AD)
  - Creación de grupos de correo por departamento.
- VPN para teletrabajo, para permitir el acceso remoto seguro a los usuarios desde fuera de la oficina.
- Servidor de actualizaciones y seguridad, para centralizar las actualizaciones del sistema operativo, aplicar mantenimiento programado, integrar con políticas GPO para instalación automática.

vi. Crear un mapa físico con la disposición del nuevo sistema informático y un mapa lógico con todos los elementos y servicios que ofrece el sistema.

En este apartado se trata de describir qué debería hacer el sistema y qué necesitamos. Además, se debe incluir en este apartado, qué necesitamos para poder integrar sistemas operativos libres y propietarios en el dominio.





El nuevo sistema implantado en Trust SL debe garantizar la **centralización de la administración**, la **seguridad en el acceso** y la **eficiencia en la gestión** de todos los recursos informáticos de la empresa.

El entorno debe permitir que cualquier usuario de la organización inicie sesión con sus **credenciales únicas** desde cualquier equipo autorizado, acceda únicamente a los recursos asignados a su **departamento o rol**, y que todos los servicios críticos (ficheros, impresoras, red) sean **gestionados de forma remota y segura** por el equipo TIC.

### ¿Qué debe hacer el sistema?

#### 1. Autenticación centralizada

- Todos los usuarios deben validarse contra el **servicio de directorio (Active Directory)**.
- El sistema debe gestionar contraseñas, políticas de acceso y bloqueo automático.
- Cada usuario tiene una cuenta única (formato nombre.apellido).

#### 2. Autorización por grupos

- Los permisos sobre recursos se asignan exclusivamente a **grupos de seguridad** (nunca a usuarios individuales).
- Cada departamento tiene su propio grupo (grupo.departamento), con control total sobre su carpeta y sus dispositivos asociados.

### 3. Gestión de archivos y recursos compartidos

- Se deben mantener **carpetas departamentales** y **carpetas personales** protegidas con permisos.
- Las carpetas compartidas y de escáner estarán disponibles para todos los usuarios, mientras que los departamentos solo tendrán acceso a sus propios directorios.
- El servidor DC1 administrará el **servicio SMB (Server Message Block)** para las comparticiones de red.

### 4. Gestión de impresión en red

- Todas las impresoras con tarjeta de red se publican en el dominio desde el **servidor DC2**.
- Los permisos de impresión se asignan también por grupo:
  - Multifunción: acceso general a todos.
  - Láser A3: solo grupo comercial.
  - Plotter: solo grupo diseño.
- Solo los **administradores** podrán gestionar las colas de impresión.

### 5. Gestión de red (DHCP y DNS)

- El **servidor DC1** será el encargado de distribuir direcciones IP (rango /24) y resolver nombres de dominio internos.
- El servicio **DNS** debe estar integrado con el directorio, para registrar automáticamente los equipos unidos al dominio.

### 6. Administración remota y seguridad

- El departamento TIC podrá gestionar el dominio y sus servicios desde una **estación de administración** mediante **RSAT** (Remote Server Administration Tools).
- También se habilitará **Escritorio Remoto (RDP)** en los servidores, limitado únicamente a IPs autorizadas.
- Toda la administración remota se auditará y se registrarán los intentos de conexión.

### 7. Alta disponibilidad y replicación

- Existirán **dos controladores de dominio** (DC1 y DC2) que replicarán entre sí la base de datos del Active Directory y los registros DNS.
- Si uno de los controladores falla, los usuarios podrán seguir autenticándose en el otro servidor.

## 8. Escalabilidad y mantenimiento

- El sistema debe admitir nuevas incorporaciones de personal sin afectar el funcionamiento.
- Las unidades organizativas (OUs) permiten aplicar políticas distintas por departamento o tipo de dispositivo.
- Se prevé la posibilidad de ampliar el sistema con nuevos roles (backup centralizado, WSUS, VPN, etc.).

### Inventario de equipos – Trust S.L.

Nº	Departamento	Usuario / Equipo	Descripción Función	/	Sistema Operativo	Dirección IP
----	--------------	------------------	---------------------	---	-------------------	--------------

### SERVIDORES DEL DOMINIO

1	TIC	DC-TRUST-01	Controlador de dominio principal	Windows Server 2025	192.168.10.1
2	TIC	DC-TRUST-02	Controlador de dominio secundario / réplica	Windows Server 2025	192.168.10.2

### DEPARTAMENTO TIC

3	TIC	TRUST-W11 (Ruben.vicente)	Administrador de sistemas	Windows Pro N	11	192.168.10.11
---	-----	------------------------------	---------------------------	---------------	----	---------------

### ADMINISTRACIÓN Y FINANZAS

4	Administración y Finanzas	EQUIPO-AF01 (Benjamín Placeta)	Coordinador Adm. y Finanzas / Coord. TIC	Windows Pro N	11	192.168.10.20
5	Administración y Finanzas	EQUIPO-AF02 (Ernesto Prats)	Administrativo contable	Windows Pro N	11	192.168.10.21

6	Administración y Finanzas	EQUIPO-AF03 (Mario Donderis)	Técnico facturación	de Windows Pro N	11	192.168.10.22
7	Administración y Finanzas	IMP-AF01	Fotocopiadora multifunción (en red)	Firmware propio (dispositivo)		192.168.10.23

***DEPARTAMENTO COMERCIAL***

8	Comercial	TRUST-UBUNTU (Alexis Blasco)	Coordinador Comercial y Diseño	Linux Ubuntu	192.168.10.30
9	Comercial	EQUIPO-COM02 (Gabriel Gomera)	Comercial	Linux Ubuntu	192.168.10.31
10	Comercial	EQUIPO-COM03 (Juan Machado)	Comercial	Linux Ubuntu	192.168.10.32
11	Comercial	IMP-COM01	Impresora láser A3 color (en red)	Firmware propio (dispositivo)	192.168.10.33

***DEPARTAMENTO DE DISEÑO***

12	Diseño	EQUIPO-DIS01 (Javier Gandía)	Diseñador gráfico	Windows Pro N	11	192.168.10.40
13	Diseño	IMP-DIS01	Plotter gran formato (en red)	Firmware propio (dispositivo)		192.168.10.41

## GERENCIA

14	Gerencia	EQUIPO-GER01 (Francisco García)	Gerente General	Windows 11 Pro N	192.168.10.50
----	----------	------------------------------------	-----------------	------------------	---------------

### Resumen de red por bloques de IP

Rango de IP	Departamento / Tipo
-------------	---------------------

Rango de IP	Departamento / Tipo
192.168.10.1 – 192.168.10.2	Servidores de dominio (DC1 / DC2)
192.168.10.11	TIC (Administración de sistemas)
192.168.10.20 – .29	Administración y Finanzas
192.168.10.30 – .39	Comercial
192.168.10.40 – .49	Diseño
192.168.10.50	Gerencia

El dominio **trust.lan** estará compuesto por estaciones de trabajo con **sistemas operativos propietarios (Windows 11 Pro)** y **sistemas operativos libres (Linux Ubuntu Desktop)**.

Para garantizar una **integración completa, segura y funcional**, es necesario cumplir una serie de **requisitos técnicos, de configuración y de servicios** en ambos entornos.

### Requisitos comunes de red y autenticación

- **DNS unificado:** todos los equipos deben resolver nombres a través de los servidores DNS integrados en el dominio (DC1 y DC2).
- **Sincronización horaria (NTP):** los equipos Linux y Windows deben sincronizar su hora con los controladores de dominio para que Kerberos funcione correctamente.

- **Autenticación Kerberos y LDAP:** el dominio utiliza Kerberos para la autenticación y LDAP para la resolución de identidades.
- **Políticas de contraseñas y bloqueo** unificadas mediante directivas del dominio (GPO en Windows y PAM en Linux).
- **Auditoría centralizada** de eventos de inicio de sesión y accesos a recursos compartidos.

### *Integración de sistemas Windows (propietarios)*

Los equipos Windows se unirán directamente al dominio **trust.lan** a través de las propiedades del sistema.

#### **Pasos esenciales:**

1. Asignar configuración IP estática o dinámica proporcionada por el **servidor DHCP del dominio**.
2. Configurar el **servidor DNS primario** como el DC1 (192.168.10.1).
3. Unir el equipo al dominio:  
Configuración del sistema > Nombre del equipo > Dominio: trust.lan.
4. Autenticación mediante **Kerberos/NTLM** gestionada por Active Directory.
5. Aplicación automática de **GPO** (políticas de grupo) para seguridad, redirección de carpetas y asignación de impresoras.
6. Mapeo de recursos compartidos (carpetas departamentales y personales) mediante **perfiles NTFS** y políticas del dominio.

#### **Servicios necesarios en el servidor:**

- Active Directory Domain Services (AD DS)
- DNS integrado con el dominio
- DHCP con ámbito /24
- Servidor de impresión en red (publicado en AD)

### *Integración de sistemas Linux (libres)*

Para integrar correctamente un sistema operativo Linux (Ubuntu Desktop) dentro del dominio Active Directory **trust.lan**, se realiza el siguiente procedimiento técnico.

El objetivo es permitir la autenticación de usuarios de dominio, el acceso a recursos compartidos SMB y la gestión centralizada de identidades desde los controladores de dominio (DC1 y DC2).

- *Sincronización horaria (NTP)*

El protocolo Kerberos requiere que el cliente y el servidor mantengan sincronizada la hora. Por ello, se instala y configura el servicio ntpdate apuntando al controlador de dominio principal:

```
sudo apt-get install ntpdate
sudo ntpdate -q trust.lan
sudo ntpdate trust.lan
```

- *Instalación de paquetes necesarios*

Se instalan los componentes que permiten la integración de Ubuntu con Active Directory a través de Samba, Kerberos y Winbind:

```
sudo apt-get install samba krb5-config krb5-user winbind libpam-winbind libnss-winbind
```

Estos paquetes proporcionan compatibilidad con LDAP, autenticación Kerberos y servicios de resolución de identidades (usuarios y grupos de dominio).

- *Autenticación en el servidor de Kerberos*

Antes de unir el equipo al dominio, se comprueba la conexión y autenticación contra el servidor de Kerberos con la cuenta de administrador:

```
kinit Administrador@TRUST.LAN
```

Si la autenticación es correcta, el sistema no devolverá errores y se generará un ticket temporal de acceso.

- *Configuración de Samba*

Se crea una copia de seguridad del archivo de configuración original y se prepara un nuevo smb.conf adaptado al dominio:

```
sudo mv /etc/samba/smb.conf /etc/samba/smb.conf.initial
sudo nano /etc/samba/smb.conf
```

En este archivo se deben definir los parámetros del dominio, el nombre del grupo de trabajo y los controladores de dominio (por ejemplo, workgroup = TRUST, realm = TRUST.LAN, security = ADS).

Reiniciar los servicios de Samba y NetBIOS:

```
sudo systemctl restart smbd nmbd
sudo systemctl enable smbd nmbd
```

- *Unión al dominio Active Directory*

Se realiza la unión del equipo Ubuntu al dominio mediante el comando net ads join:

```
sudo net ads join -U Administrador
```

Una vez completado el proceso, el equipo **aparecerá en “Usuarios y equipos de Active Directory”** bajo el nombre **TRUST-UBUNTU**.

- *Configuración de resolución de usuarios del dominio*

Editar el archivo /etc/nsswitch.conf para permitir la resolución de usuarios y grupos del dominio a través de winbind:

```
sudo nano /etc/nsswitch.conf
```

Reiniciar el servicio Winbind:

```
sudo systemctl restart winbind
```

Verificar que se reconocen los usuarios del dominio:

```
wbinfo -u
```

- *Integración con PAM (autenticación del sistema)*

Permitir que los usuarios del dominio puedan iniciar sesión directamente en Ubuntu y que se creen sus carpetas personales automáticamente:

```
sudo pam-auth-update
```

Editar el archivo /etc/pam.d/common-account para habilitar la creación automática de directorios personales:

```
sudo nano /etc/pam.d/common-account
```

c. El diseño de la solución debe concretar la parte de análisis, indicando cómo se debe implementar el sistema para implantarlo.

Solamente se debe diseñar, se implementará posteriormente. El diseño se puede hacer mediante un diagrama o esquema. Cualquier duda sobre el parque informático será resuelta por el consultor, el cual actuará como referente TIC del sistema.

El diseño de la solución concreta la parte del análisis anterior y define **cómo se implantará técnicamente el sistema** de dominio para Trust SL.

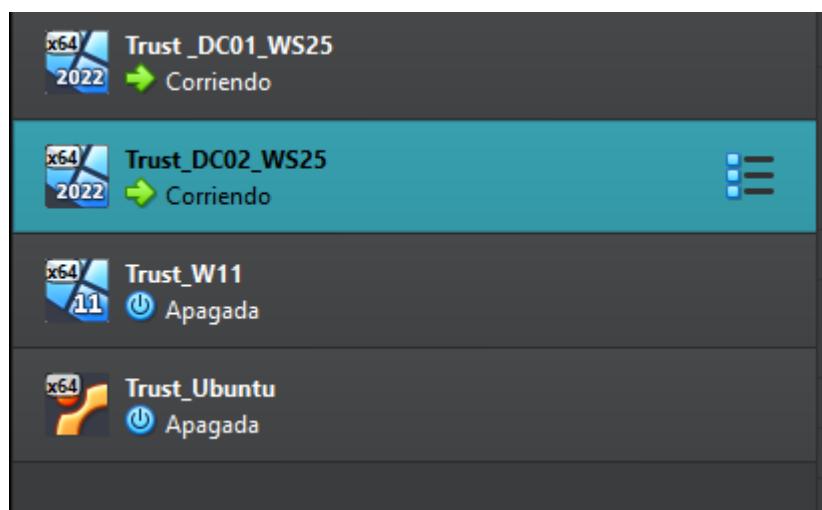
El objetivo principal es disponer de una infraestructura **centralizada, segura y administrable de forma remota**, capaz de integrar estaciones Windows y Linux, y de gestionar recursos comunes (archivos, impresoras y red).

- **Centralización de la administración:** todos los usuarios, equipos y permisos estarán gestionados desde un único dominio: trust.lan.
- **Seguridad y segregación:** la estructura de OUs y grupos garantiza que cada departamento solo acceda a sus propios recursos.
- **Alta disponibilidad:** dos controladores de dominio replican entre sí la base de datos de Active Directory.
- **Escalabilidad:** el sistema permitirá añadir más servidores o departamentos sin alterar la estructura base.
- **Compatibilidad multiplataforma:** el entorno admitirá tanto sistemas operativos propietarios (**Windows**) como libres (**Linux**) mediante autenticación Kerberos/SSSD.

### *Flujo general de funcionamiento*

1. **Inicio de sesión:** el usuario introduce sus credenciales en un equipo unido al dominio.  
→ Autenticación mediante AD DS (Kerberos).
2. **Asignación de IP y resolución:** el equipo obtiene IP del DHCP (DC1) y resuelve nombres mediante DNS.
3. **Asignación de permisos:** los accesos a carpetas o impresoras se controlan por pertenencia a grupos.
4. **Administración remota:** el equipo TIC gestiona todo desde RSAT o RDP, sin acceder físicamente a los servidores.
5. **Replicación:** los cambios en AD (usuarios, grupos, GPOs) se replican automáticamente entre DC1 y DC2.

2. Implementar el diseño lógico mediante máquinas virtuales con sistemas operativos servidores (instalar tantos como se especifiquen en el diseño). Recuerda poner un nombre significativo al servidor, configurar la dirección IP estática, y reiniciar la “mac” desde virtualbox para evitar problemas.

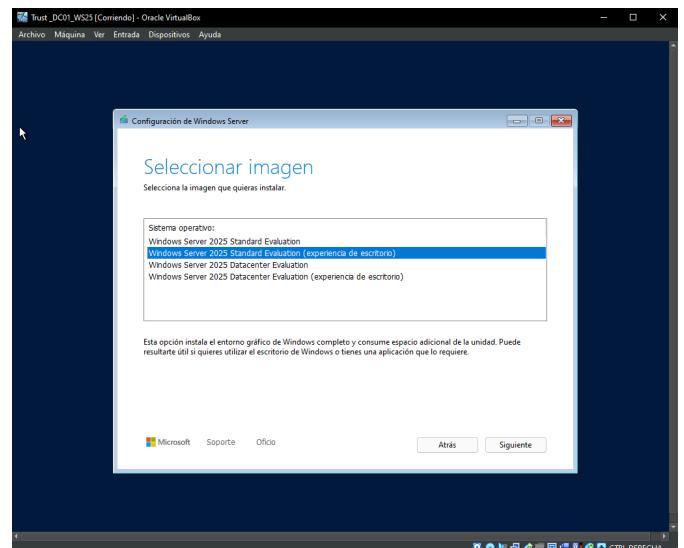


Se añade a DC1 dos adaptadores de red, uno para la red interna, donde estarán los equipos del dominio y una en NAT para el acceso a internet.

Posteriormente se configurará un servicio de SNAT (Source Network Address Translation) en Windows Server para permitir que los equipos que están en una red privada puedan acceder a la red pública (Internet).

Arrancamos nuestra máquina virtual de Windows Server 2025

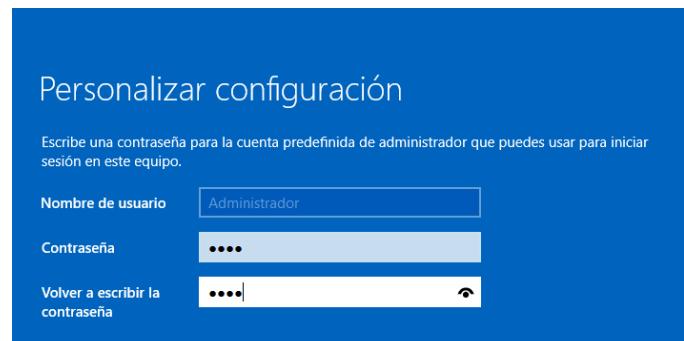
Instalamos la versión deseada, en nuestro caso Standard con experiencia de escritorio.



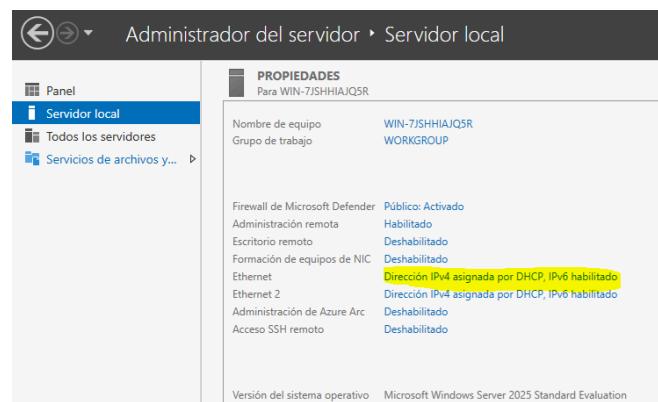
Siguiente, e instalar. Siguiendo los pasos de instalación.



Introducimos la contraseña que deseamos para el usuario Administrador

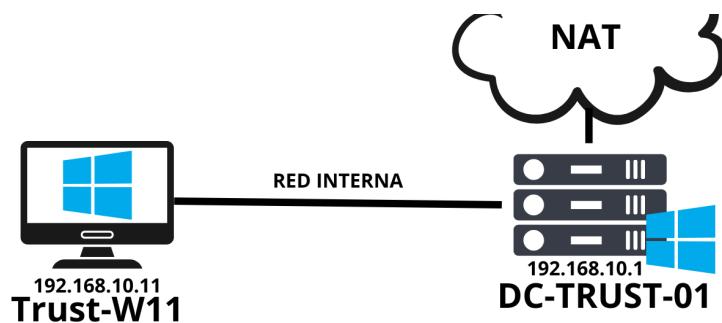


Una vez iniciada la sesión podemos acceder al panel de administración del servidor para empezar con la configuración.



Repetimos el proceso de instalación para nuestro servidor DC02

Una vez instalado Windows Server 2025 vamos a proceder a instalar Windows 11, es importante instalar Windows 11 pro o pro N para poder unir la máquina al dominio. Como he mencionado al inicio de esta práctica, los equipos que forman parte del dominio utilizarán el adaptador de red de VirtualBox en modo red interna. Para vincular el equipo al dominio y al servidor y puesto que es el equipo que vamos a utilizar nosotros le asignaremos la configuración de red manualmente.

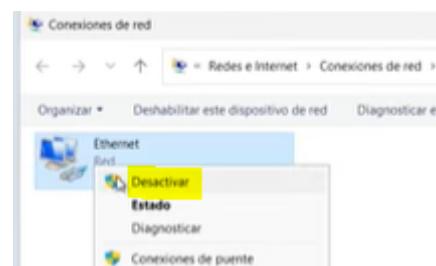


Procedemos con la instalación de W11 pro N siguiendo el proceso normal.

El único inconveniente es que realizaremos un bypass para no iniciar sesión con una cuenta Microsoft, en lugar de esto crearemos un usuario local.

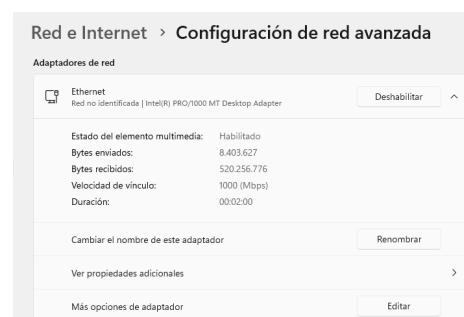


- SHIFT + F10 > se abrirá el cmd y escribimos
- ncpa.cpl > y desactivamos el adaptador de red



oobe\bypassnro > la instalación volverá a ejecutarse desde el principio y nos permitirá crear un usuario local

Una vez instalado W11 pro n, volvemos a habilitar el adaptador de red.

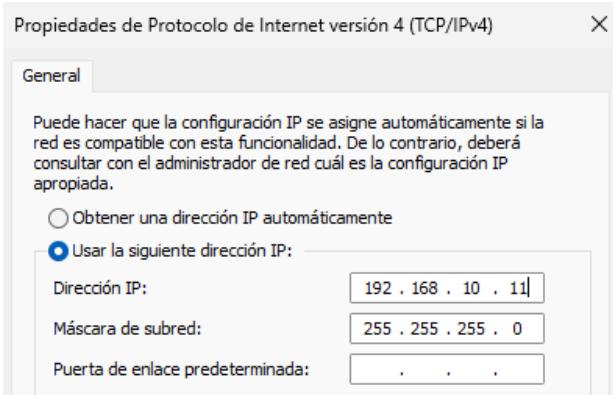


Editamos las Propiedades del protocolo IPv4 y añadimos las siguientes:

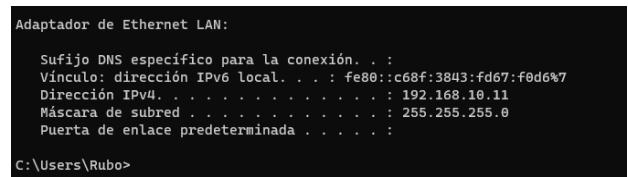
Dirección IP: 192.168.10.11

Máscara de subred: 255.255.255.0

La puerta de enlace la configuraremos más adelante pero si lo deseamos podemos añadir ya la Ip del servidor DC-TRUST-01 - 192.168.10.1



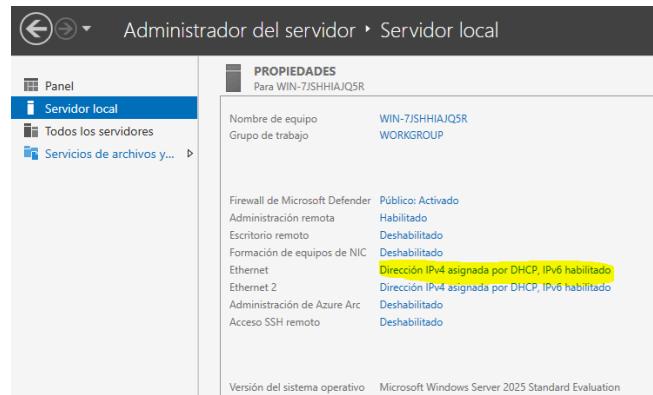
Revisamos la configuración mediante ipconfig



## *Configuración red interna para el servidor.*

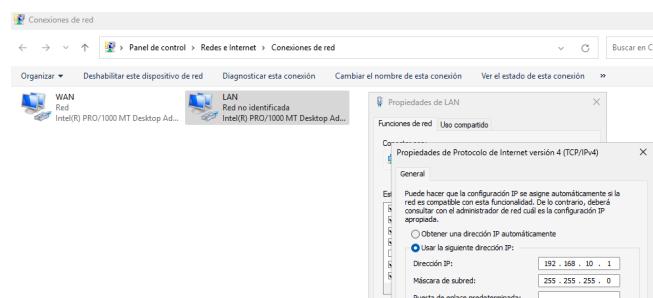
Volvemos a nuestro Windows Server 2025, en el panel de administración pulsamos en:  
Servidor local > Dirección IPv4 por DHCP habilitado.

Esto abrirá el directorio donde se encuentran los adaptadores de red. En mi caso para que sea más claro les he asignado los nombres de WAN y de LAN



Click derecho en el adaptador LAN > propiedades > Propiedades de Protocolo de IPv4 > Propiedades >

Asignamos la IP deseada - 192.168.10.1



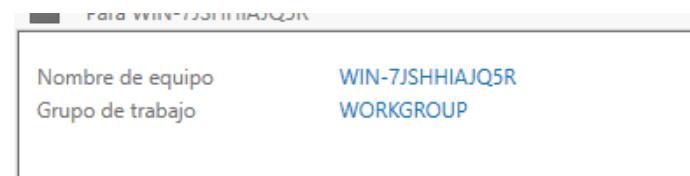
Para comprobar la configuración mediante un ping hay que crear una regla de firewall que nos permita realizar un ping mediante protocolo ICMPv4. Estamos en un entorno de pruebas, podemos habilitar cualquier dirección o únicamente la dirección de nuestro servidor.

```
C:\Users\Administrador>ping 192.168.10.11
```

```
Haciendo ping a 192.168.10.11 con 32 bytes de datos:  
Respuesta desde 192.168.10.11: bytes=32 tiempo<1m TTL=128  
  
Estadísticas de ping para 192.168.10.11:  
Paquetes: enviados = 4, recibidos = 4, perdidos = 0  
(0% perdidos),  
Tiempos aproximados de ida y vuelta en milisegundos:  
Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

```
C:\Users\Administrador>
```

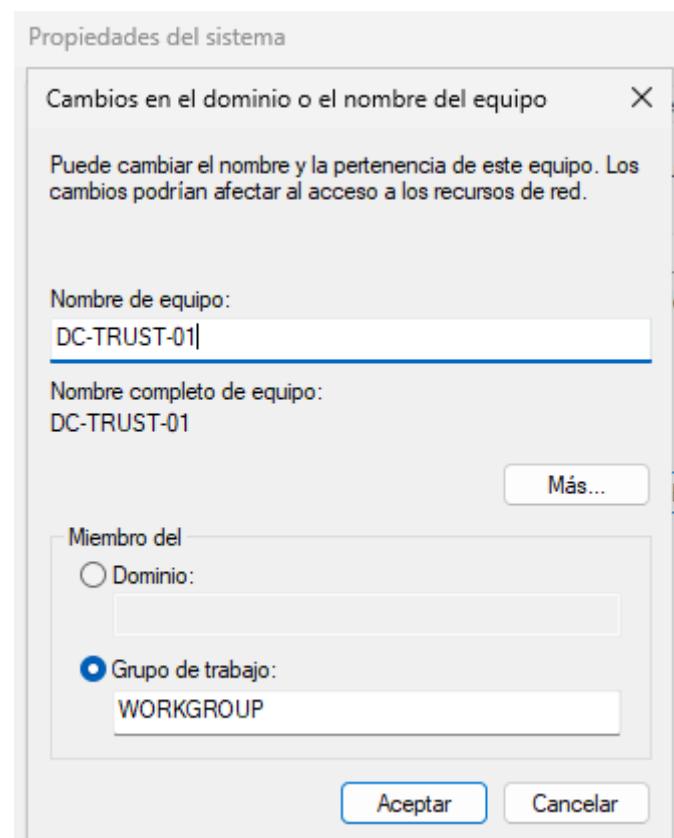
Ahora vamos a proceder a asignarle  
un nombre al servidor para ello:  
Pulsamos en Nombre de equipo



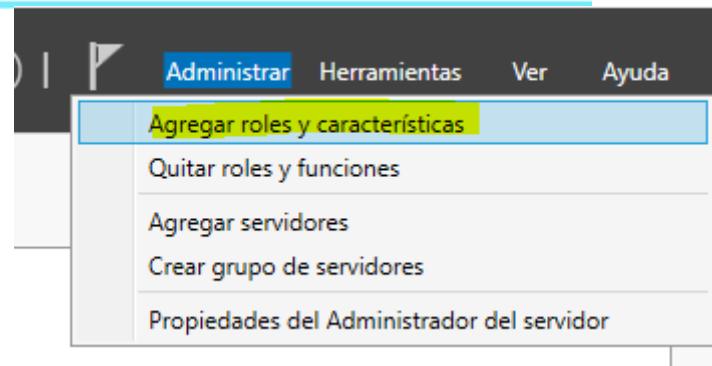
Nombre de equipo: DC-TRUST-01

y Aceptar.

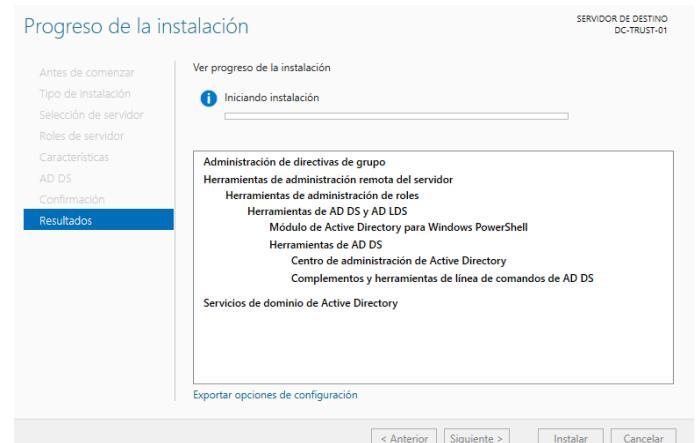
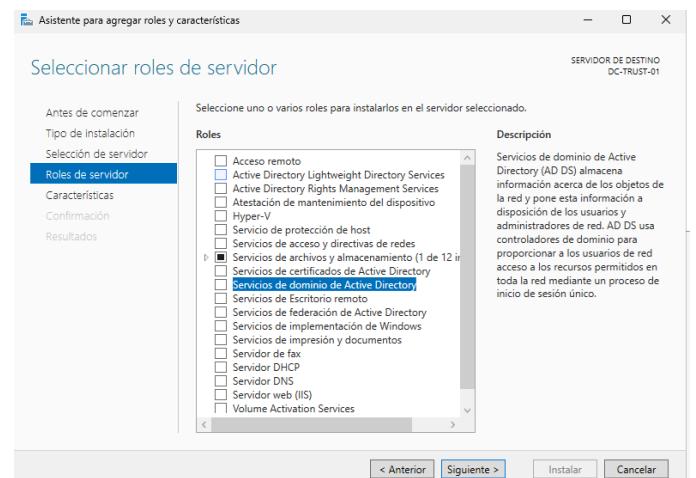
Después de hacer esto el servidor se reiniciará.



Ahora vamos a promover a controlador de dominio, para ello necesitamos agregar roles y características.



Lo que vamos a agregar es el rol de “Servicios de dominio de Active Directory”



Pulsamos en Promover este servidor a controlador de dominio.

Debemos promover este servidor a controlador de dominio. Vamos a agregar un nuevo bosque y le tenemos que dar un nombre de Dominio raíz.

trust.lan

Ver progreso de la instalación

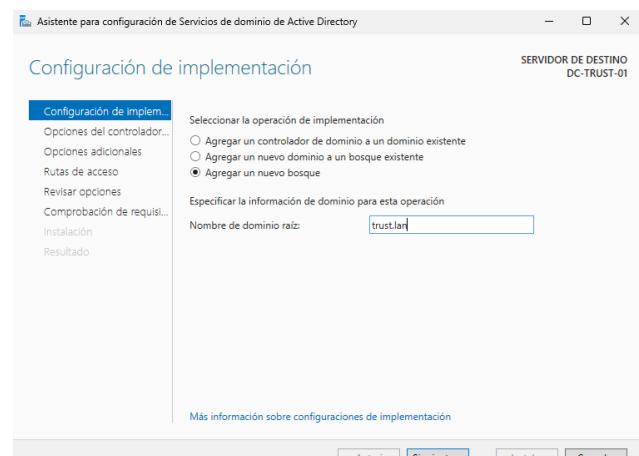
**Instalación de característica**

Requiere configuración. Instalación correcta en DC-TRUST-01.

**Servicios de dominio de Active Directory**

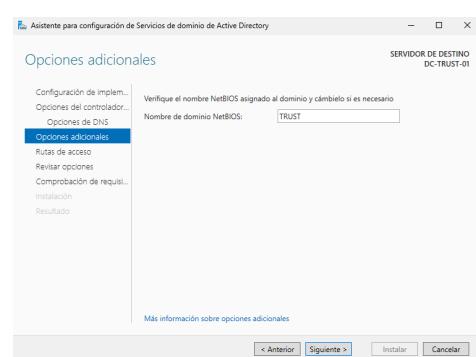
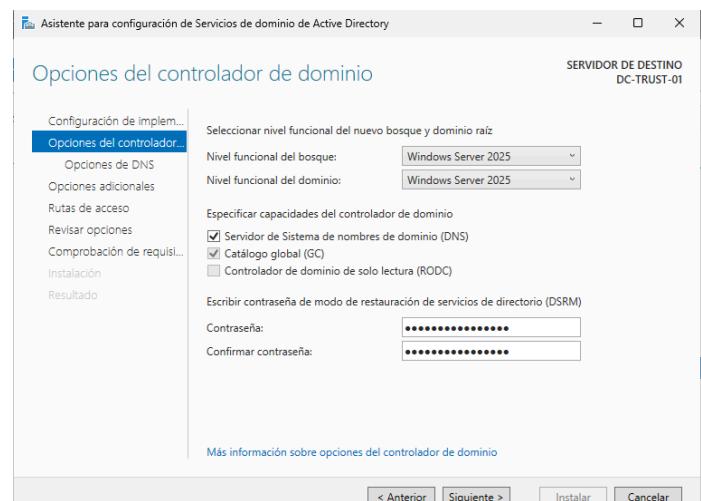
Se requieren pasos adicionales para que esta máquina sea un controlador de dominio.

**Promover este servidor a controlador de dominio.**



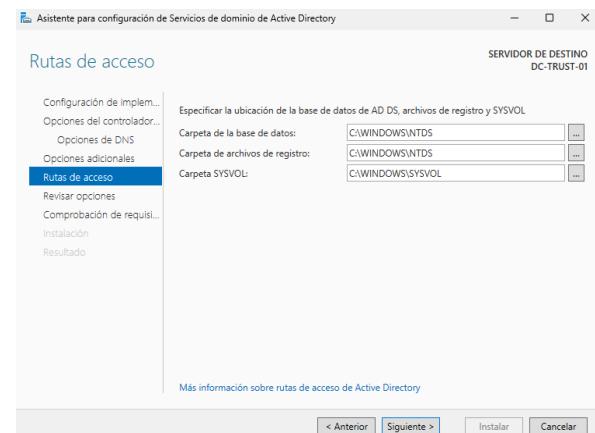
Insertamos la contraseña para el modo de restauración de directorios.

Es importante recordarla para poder restaurar las copias de seguridad en caso de por ejemplo borrar el dominio por completo.



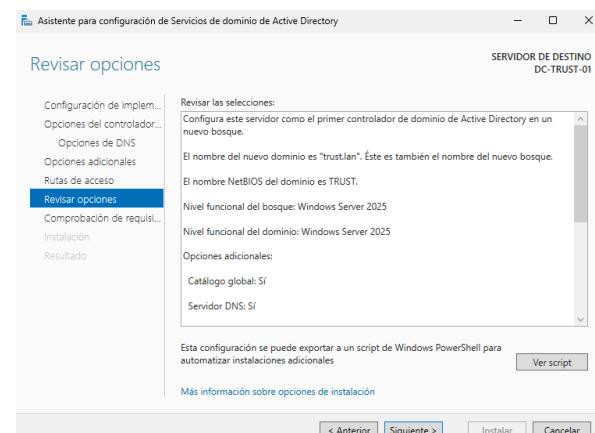
Se crean las carpetas donde se van a almacenar las bases de datos, los archivos de registro y la carpeta SYSVOL.

Lo dejamos por defecto.



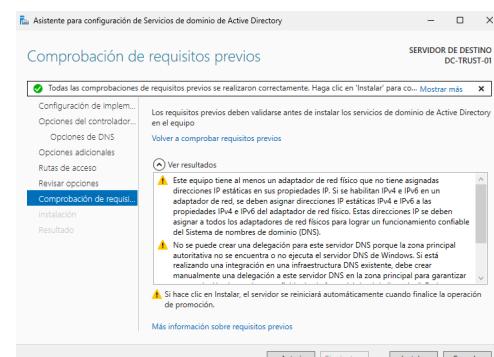
Este apartado es el resumen de la configuración que vamos a crear.

Algo interesante es que podemos ver el script de PowerShell que se utilizará.

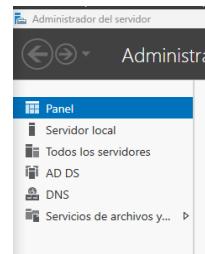


```
tmpSEC7.tmp: Bloc de notas
Archivo Edición Formato Ver Ayuda
#
# Script de Windows PowerShell para
#
Import-Module ADDSDeployment
Install-ADDSForest
-CreateOnsDelegation:$false
-DatabasePath "C:\WINDOWS\NTDS"
-DomainMode "Win2025"
-DomainName "trust.lan"
-DomainNetbiosName "TRUST"
-ForestMode "Win2025"
-InstallDns:$true
-LogPath "C:\WINDOWS\NTDS"
-NoRebootOnCompletion:$false
-SysvolPath "C:\WINDOWS\SYSVOL"
-Force:$true
```

Pulsamos en instalar, suele tardar varios minutos. Y se reiniciará el servidor al finalizar.



En el panel ya podemos ver algunas herramientas que se han instalado al crear el dominio. Como el AD DS y el servicio de DNS que es uno de los requisitos al promover un dominio.



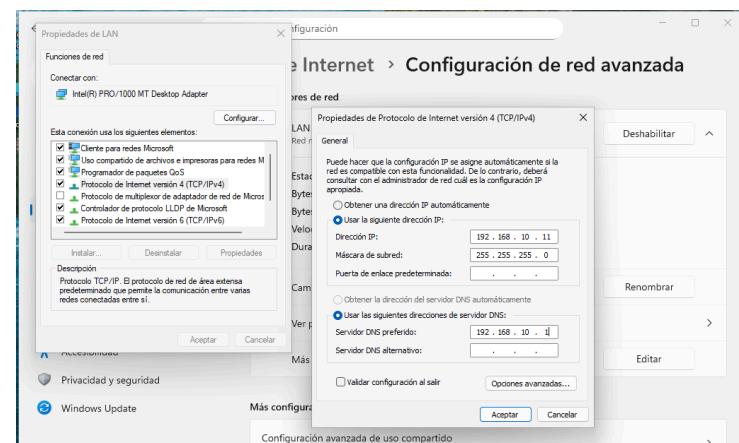
## *Unir Windows 11 al dominio.*

En la máquina Windows 11 vamos a acceder a redes e Internet > Configuración avanzada > editar > Protocolo de Internet versión > Propiedades

Añadimos la IP de nuestro Windows Server 2025 como Servidor de DNS preferido  
192.168.10.1

Para comprobar si funciona realizamos un ping a trust.lan

Y como vemos nuestro servicio de DNS está funcionando.



```
c:\Users\Rubo>ping trust.lan

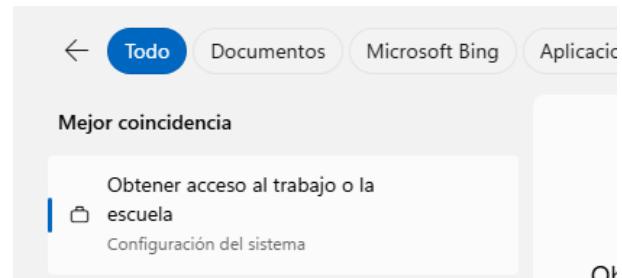
Haciendo ping a trust.lan [192.168.10.1] con 32 bytes de datos:
Respuesta desde 192.168.10.1: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.10.1:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\Rubo>
```

Ahora ya podemos agregar el equipo al dominio trust.lan

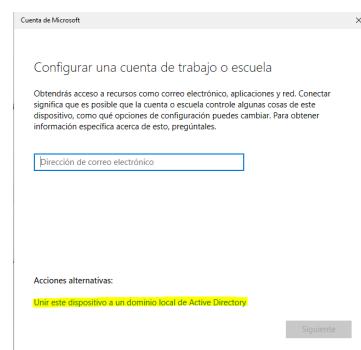
Buscamos obtener acceso al trabajo o la escuela.



Pulsamos en conectar.

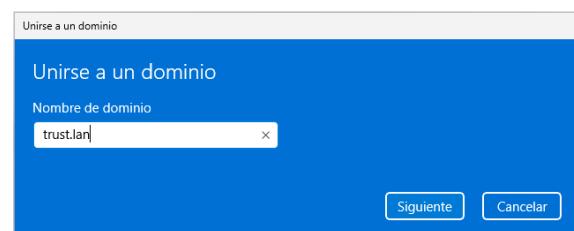


Unir este dispositivo a un dominio local de Active Directory



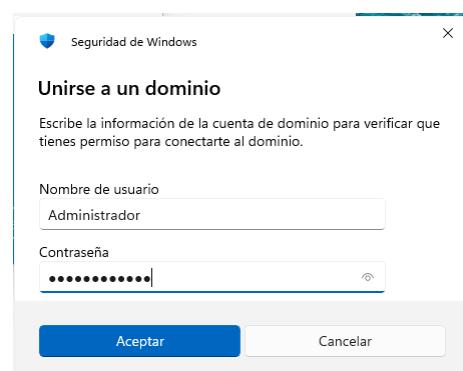
Nombre de dominio:  
trust.lan

Y siguiente.



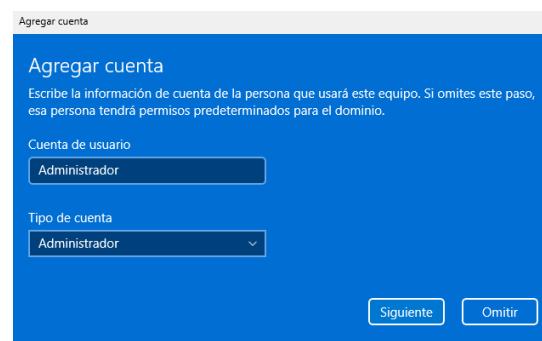
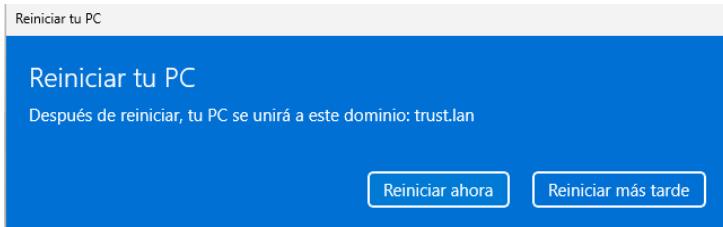
Ahora nos solicitan las credenciales de una de las cuentas del dominio. Por el momento la única cuenta del dominio es Administrador.

Así que ingresamos estas credenciales. En el producto 2 deshabilitamos estas credenciales siguiendo las buenas prácticas recomendadas y crearemos nuestro usuario administrador.



Es un tipo de cuenta Administrador.

Se nos solicitará reiniciar el equipo.

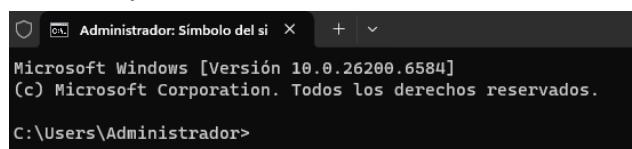


Una vez reiniciada la máquina de Windows 11 debería de aparecer el nombre de dominio y el usuario.

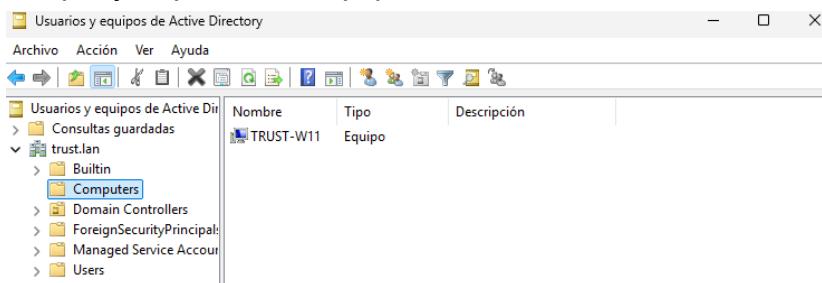
TRUST\Administrador



Vemos que accedemos como Administrador



En el servidor vemos que ya aparece el equipo enlazado.



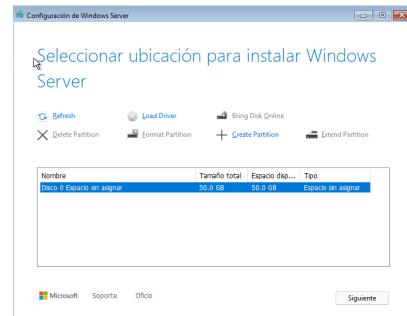
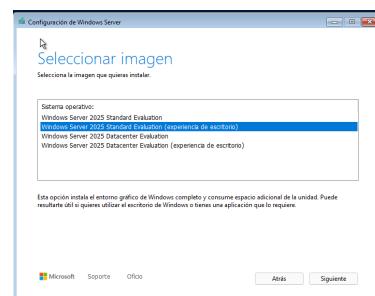
### 3. Instalar el servicio de directorio tal como se ha especificado en el diseño de la solución. Crear un vídeo tutorial en el cual se demuestre la instalación y configuración del servicio de directorio.

Un segundo controlador de dominio en Windows Server es un servidor adicional configurado dentro de un dominio existente para proporcionar redundancia, balanceo de carga y mayor seguridad en la infraestructura de Active Directory (AD). Este segundo controlador, conocido como controlador de dominio adicional (Additional Domain Controller o ADC), replica automáticamente la base de datos de AD del controlador de dominio principal. Esto significa que el segundo controlador almacena una copia completa y sincronizada de todos los datos de Active Directory, incluyendo usuarios, grupos, permisos y políticas de seguridad.

El propósito de un segundo controlador de dominio es fortalecer la disponibilidad y confiabilidad de los servicios de autenticación y autorización de una red. Si el controlador de dominio principal falla o está temporalmente fuera de servicio, el segundo controlador puede continuar proporcionando acceso y servicios de autenticación a los usuarios, de modo que las operaciones de la red no se interrumpen.

#### A. Explicar el proceso de instalación.

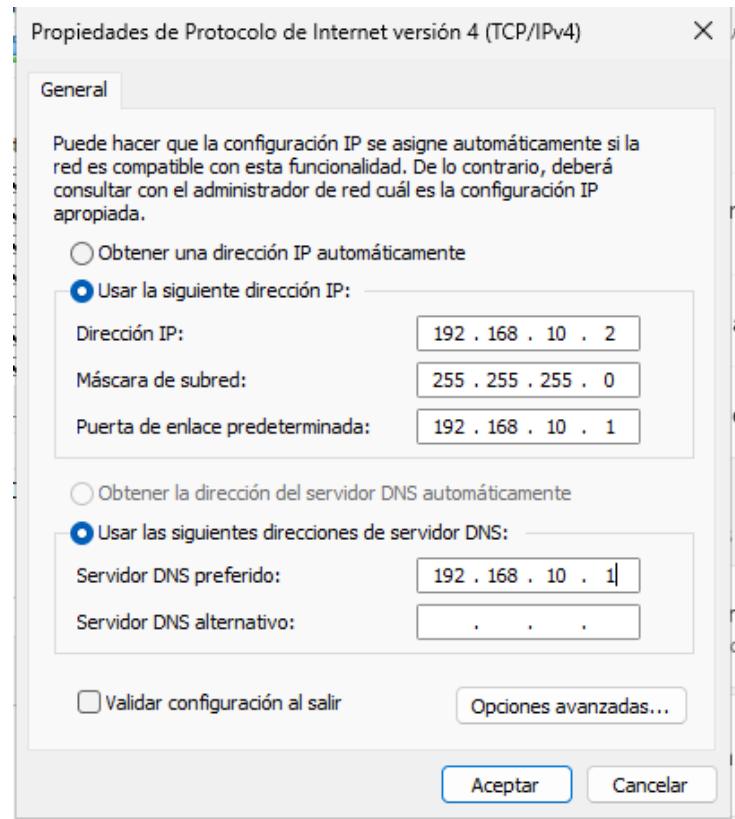
Iniciamos el proceso de instalación igual que hicimos con nuestro primer servidor.



Seguimos los pasos del instalador del mismo modo.

Repetimos los pasos que hemos seguido para Trust\_DC01\_SW25.

Asignamos la IP en base a nuestro mapa lógico.



Revisamos que el servicio de DNS funcione correctamente.

```
c:\Users\Administrador>ping 192.168.10.1

Haciendo ping a 192.168.10.1 con 32 bytes de datos:
Respuesta desde 192.168.10.1: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.10.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\Administrador>ping trust.lan

Haciendo ping a trust.lan [192.168.10.1] con 32 bytes de datos:
Respuesta desde 192.168.10.1: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.10.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\Administrador>
```

Cambiamos el nombre del servidor por

**PROPIEDADES**  
Para DC-TRUST-02

Nombre de equipo	DC-TRUST-02
Grupo de trabajo	WORKGROUP
Firewall de Microsoft Defender	Público: Activado
Administración remota	Habilitado
Escritorio remoto	Deshabilitado
Formación de equipos de NIC	Deshabilitado
Ethernet	192.168.10.2, IPv6 habilitado
Administración de Azure Arc	Deshabilitado
Acceso SSH remoto	Deshabilitado

En DC-TRUST-01 creamos un nuevo host en el administrador de DNS

The screenshot shows the Windows DNS Manager interface. On the left, the tree view shows the 'DC-TRUST-01.trust.lan' zone with sub-sections like '\_msdcs', 'sites', 'tcp', 'uds', and 'DomainDnsZones'. On the right, a table lists existing hosts and their details. A modal dialog box titled 'Host nuevo' is open, prompting for the host name ('dc-trust-02'), domain ('dc-trust-02.trust.lan'), IP address ('192.168.10.2'), and other DNS-related information. Buttons at the bottom of the dialog are 'Agregar host' and 'Cancelar'.

Ahora en DC-TRUST-02 vamos Administrar > Agregar Roles y características

The screenshot shows the 'Agregar roles y características' (Add Roles and Features) step of the wizard. The left pane lists steps: 'Antes de comenzar', 'Tipo de instalación', 'Selección de servidor', 'Roles de servidor' (which is selected), 'Características', 'AD DS', 'Confirmación', and 'Resultados'. The right pane displays a list of available roles, with 'Servicios de dominio de Active Directory' checked. A detailed description of this role is provided on the right. Navigation buttons at the bottom are 'Anterior', 'Siguiente >', 'Instalar', and 'Cancelar'.

Seleccionamos Servicios de dominio de Active Directory y pulsamos en siguiente.

The screenshot shows the 'Selección de roles de servidor' (Select Server Roles) step. It asks to select one or more roles for the selected server. The 'Roles' section lists various options, with 'Servicios de dominio de Active Directory' checked. A detailed description of this role is provided on the right. Navigation buttons at the bottom are 'Anterior', 'Siguiente >', 'Instalar', and 'Cancelar'.

Esperamos a que finalice la instalación y procedemos a promover este servidor a controlador de dominio.

### Progreso de la instalación

SERVIDOR DE DESTINO  
DC-TRUST-02

Antes de comenzar  
Tipo de instalación  
Selección de servidor  
Roles de servidor  
Características  
AD DS  
Confirmación  
**Resultados**

Ver progreso de la instalación

**Instalación de característica**

Requiere configuración. Instalación correcta en DC-TRUST-02.

#### Servicios de dominio de Active Directory

Se requieren pasos adicionales para que esta máquina sea un controlador de dominio.

Promover este servidor a controlador de dominio

#### Administración de directivas de grupo

#### Herramientas de administración remota del servidor

Herramientas de administración de roles

Módulo de Active Directory para Windows PowerShell

Herramientas de AD DS

Centro de administración de Active Directory

Este asistente se puede cerrar sin interrumpir la ejecución de las tareas. Para ver el progreso de la tarea o volver a abrir esta página, haga clic en Notificaciones en la barra de comandos y en Detalles de la tarea.

Exportar opciones de configuración

< Anterior Siguiente > Cerrar Cancelar

### Configuración de implementación

SERVIDOR DE DESTINO  
DC-TRUST-02

#### Configuración de implementación

Opciones del controlador...

Opciones adicionales

Rutas de acceso

Revisar opciones

Comprobación de requisiti...

Instalación

Resultado

#### Seleccionar la operación de implementación

- Agregar un controlador de dominio a un dominio existente
- Agregar un nuevo dominio a un bosque existente
- Agregar un nuevo bosque

#### Especificar la información de dominio para esta operación

Dominio:

Seleccionar...

Proporcionar las credenciales para realizar esta operación

<No se proporcionaron credenciales>

Cambiar...

Más información sobre configuraciones de implementación

Búsqueda < Anterior Siguiente > Instalar Cancelar

Ingresamos nuestras credenciales de administrador del dominio.



Seguridad de Windows



### Credenciales para la operación de implementación

Proporcionar credenciales para la operación de implementación

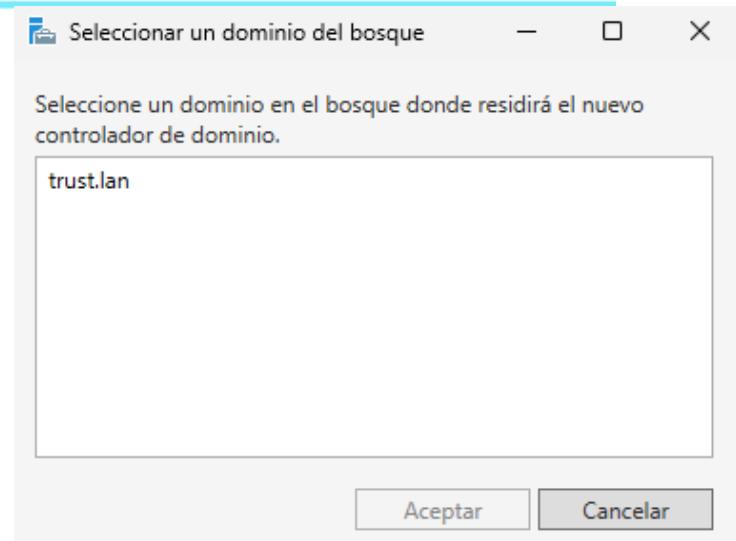
Administrador@trust.lan

••••••••••••

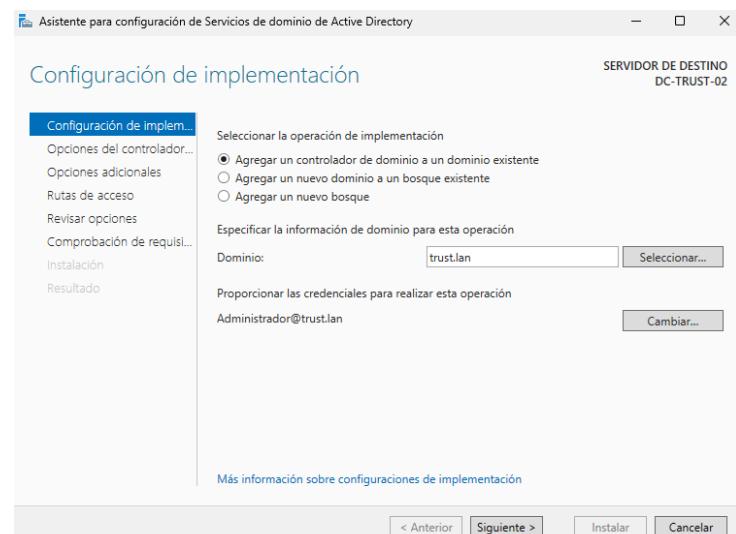
Aceptar

Cancelar

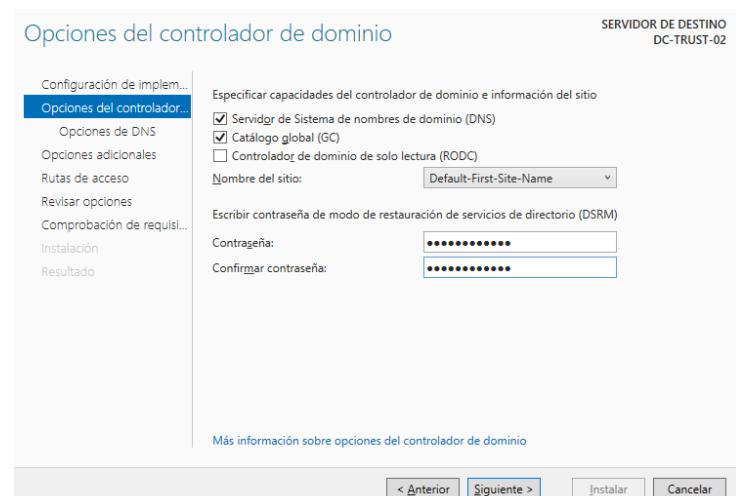
Seleccionamos el dominio en el bosque donde residirá el nuevo controlador de dominio.



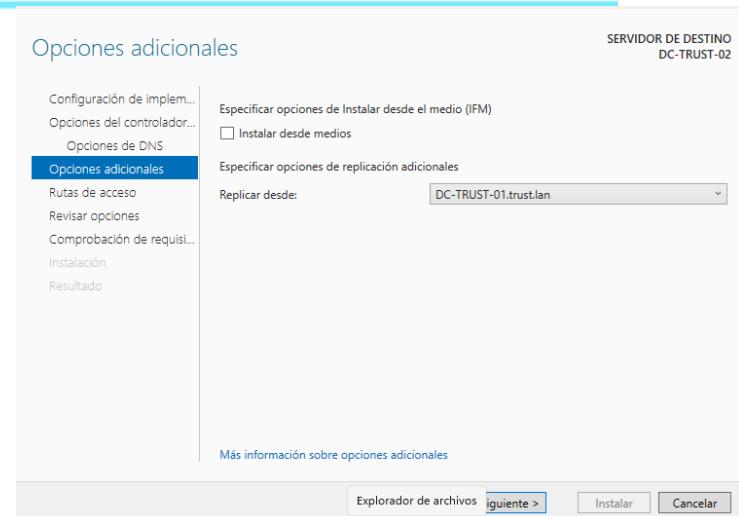
Vemos que en el apartado de Dominio nos aparece trust.lan.



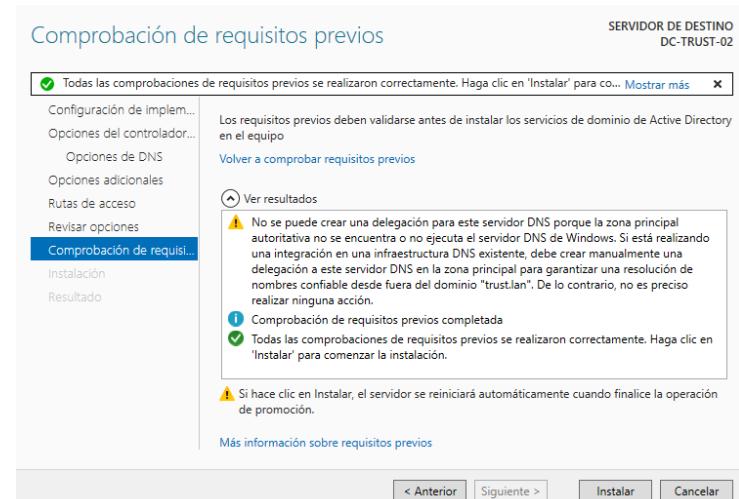
Ingresamos las contraseñas para el modo restauración.



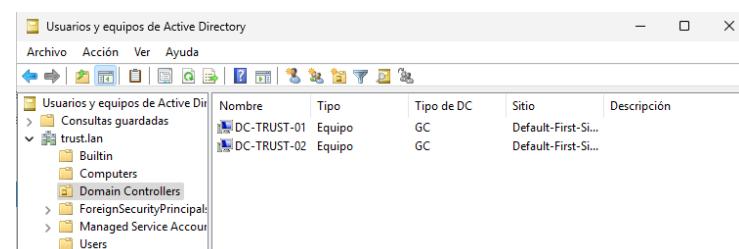
Indicamos que deseamos que se replique desde DC-TRUST-01.trust.lan que es nuestro Windows server 2025 que configuramos primero.



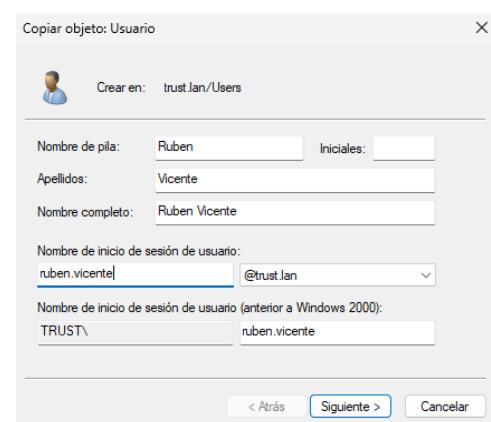
Al finalizar la Instalación se reiniciará el equipo.



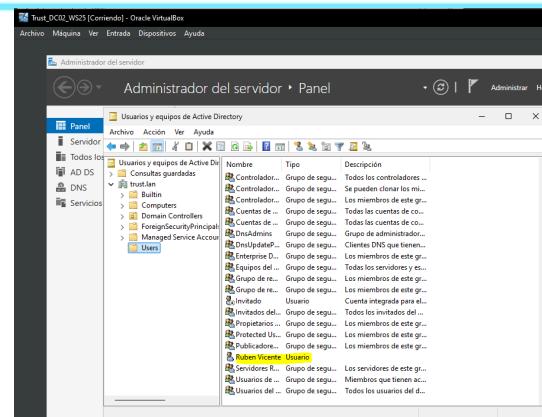
Y como podemos ver en Usuarios y equipos de Active Directory dentro del apartado de Domain Controllers tenemos nuestros 2 servidores.



En DC-TRUST-01 creamos un usuario nuevo



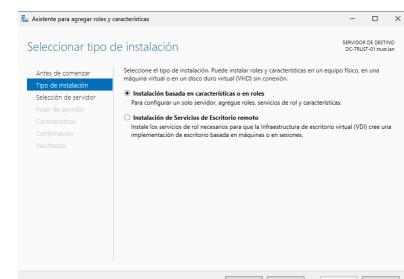
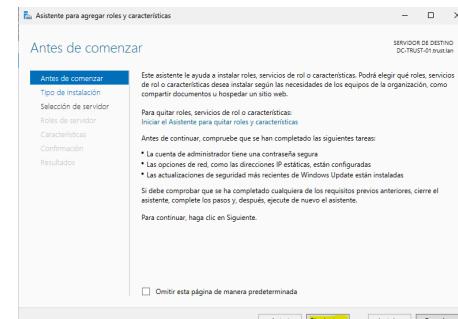
Y como vemos en DC-TRUST-02 Aparece el usuario que hemos creado anteriormente en DC-TRUST-01



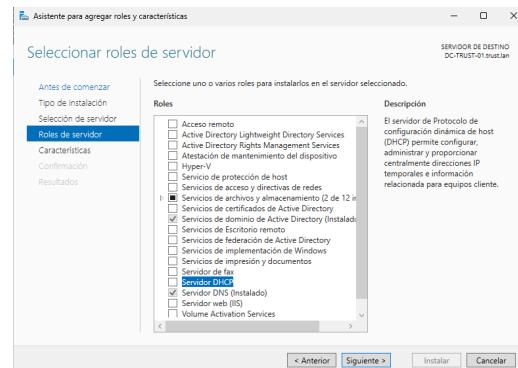
## 4. Instalar y configurar el servicio DHCP y DNS en el servidor para que sea éste quién de las ip's a los equipos de la red. El rango de ip's no tiene que ser superior a 254, es decir, tendrá que ser un rango con máscara /24 o 255.255.255.0; Documentar el proceso de instalación mediante capturas de pantalla.

### A. Explicar el proceso de instalación.

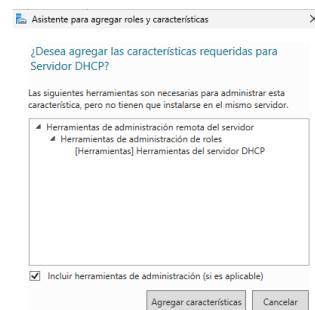
Instalar roles y características DHCP  
Igual que hemos hecho anteriormente con Active Directory.



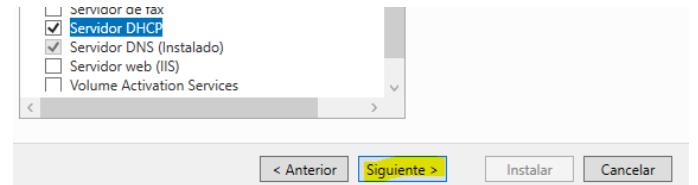
## Agregamos los roles del servidor DHCP



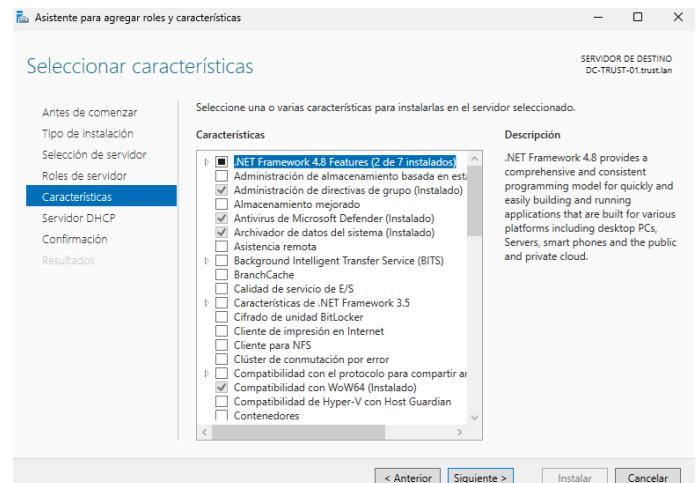
## Agregar características



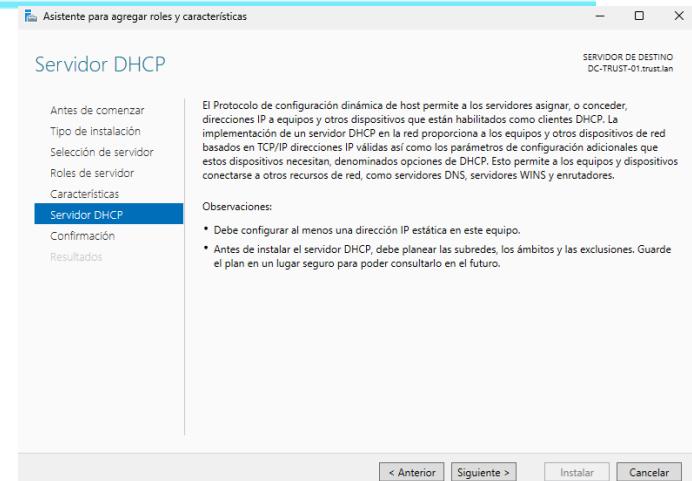
Siguiente



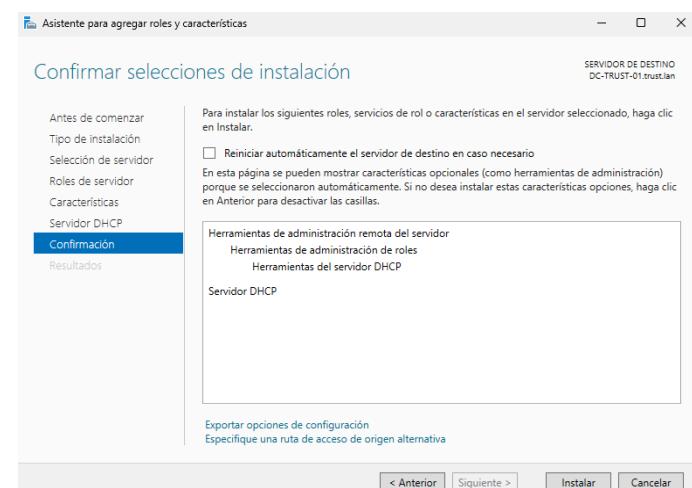
Siguiente



Siguiente



Instalar



## Ver progreso de la instalación



## Instalación de característica

Requiere configuración. Instalación correcta en DC-TRUST-01.trust.lan.

**Servidor DHCP**

Iniciar el Asistente posterior a la instalación de DHCP

Completar configuración de DHCP

**Herramientas de administración remota del servidor**

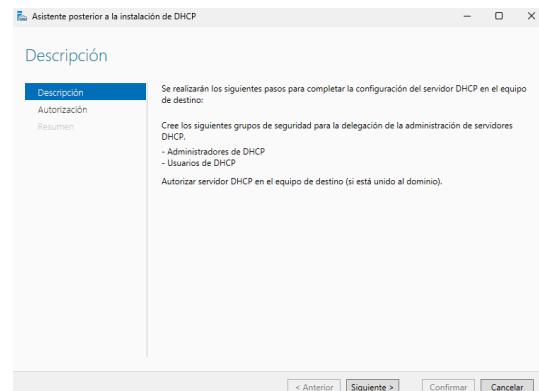
Herramientas de administración de roles

Herramientas del servidor DHCP

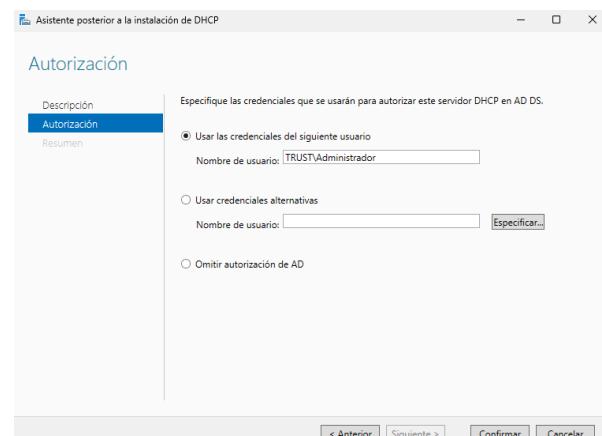
El alcance (scope) define el rango de direcciones IP que el servidor DHCP puede asignar a los clientes. También se configuran otros parámetros importantes dentro del alcance, como:

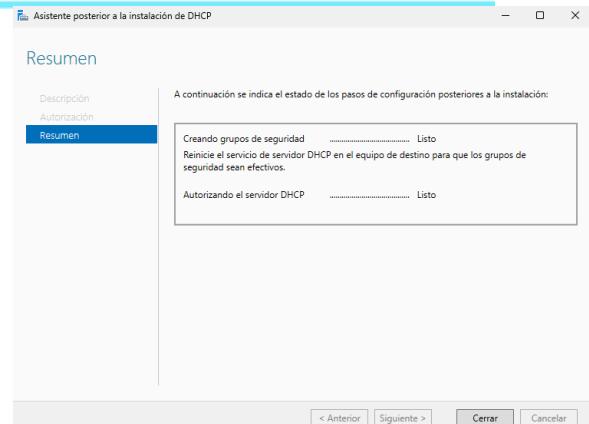
- Rango de direcciones IP: La lista de direcciones que el servidor puede asignar.
- Duración del arrendamiento (lease): El tiempo durante el cual un cliente puede utilizar una dirección IP antes de que necesite renovarla.
- Exclusiones de IP: Direcciones IP que no se asignarán automáticamente, ya sea porque están reservadas para servidores u otros dispositivos específicos.
- Opciones de DHCP: Otros parámetros como la puerta de enlace predeterminada (gateway), el servidor DNS, y otros que se asignan junto con la dirección IP.

Vamos a completar la configuración de DHCP

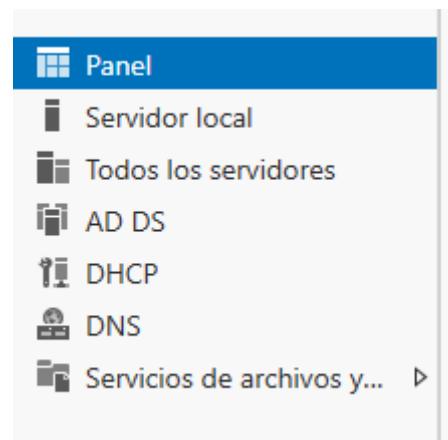


Utilizar las credenciales de Administrador.  
Seguiremos la configuración por defecto.





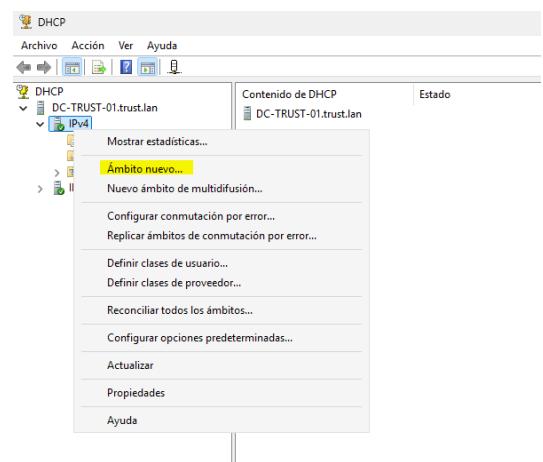
Podemos ver que en el menú del panel ya aparece nuestro servicio de DHCP



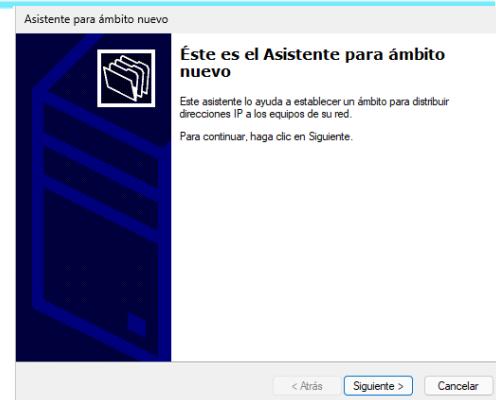
### Crear un ámbito

Vamos a crear un ámbito nuevo, para ver las características que hemos comentado al finalizar la instalación del DHCP. Por ejemplo, finanzas con 10 IPs 192.168.10.20 a .30

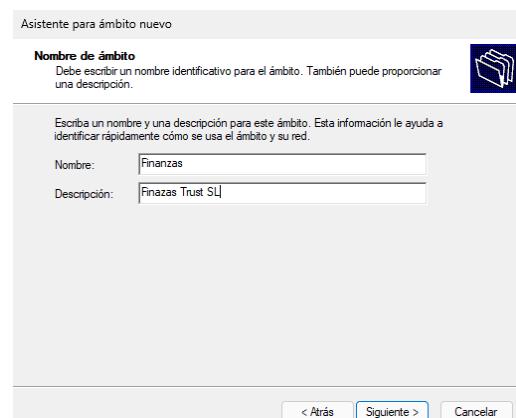
Click derecho en IPv4  
y Ámbito nuevo.



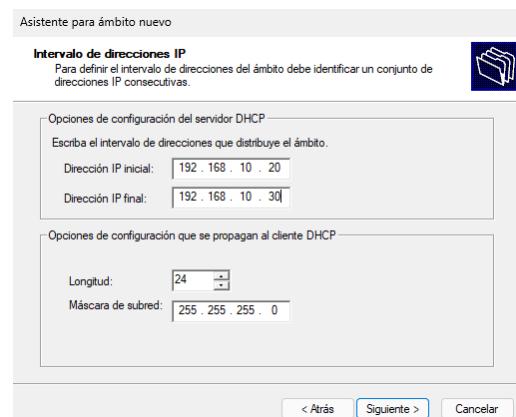
Seguimos el asistente que nos guiará en la configuración.



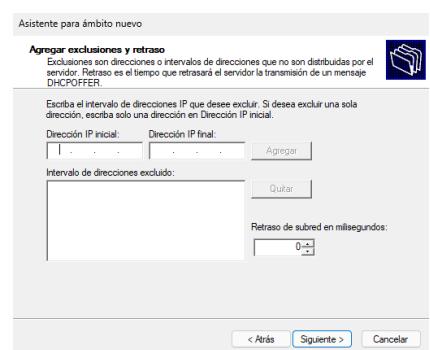
Añadimos un nombre  
y una descripción.



El rango de IP que queremos asignar a este ámbito.

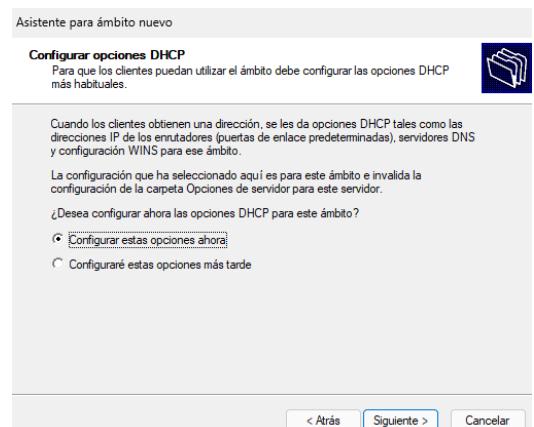
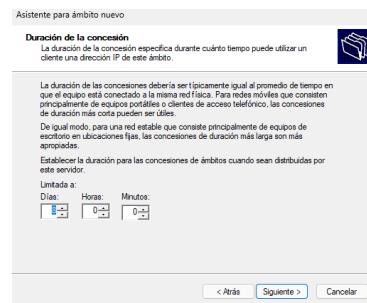


Aquí podemos excluir direcciones IP por ejemplo si tenemos la IP de alguna impresora y no deseamos cambiarle puesto que está dentro de este rango. En nuestro caso lo dejamos en blanco puesto que aún no hemos configurado impresoras u otros equipos.



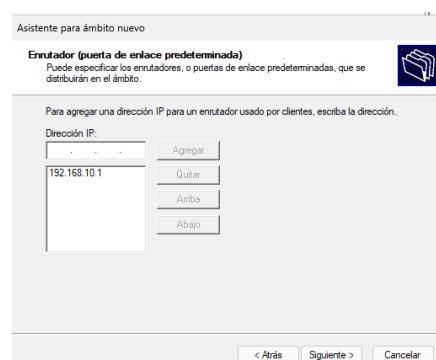
Dejamos por defecto 8 días. Lo que nos interesa es después poder resolver por hostname el servidor DNS será el encargado de indicarnos cual es la IP en caso de alguna modificación pasado este tiempo.

Ahora vamos a proceder a añadir la configuración de las opciones que deseamos que se configuren en nuestros equipos.

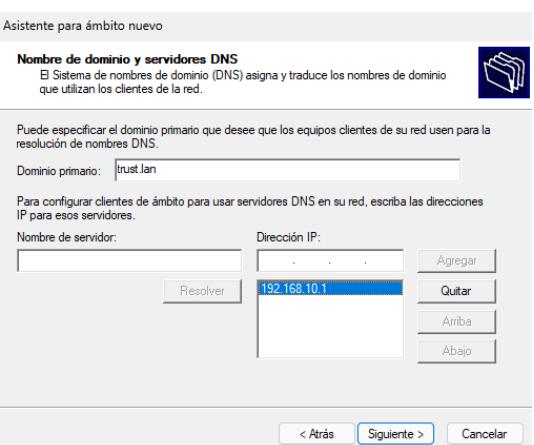


### Puerta de enlace predeterminada:

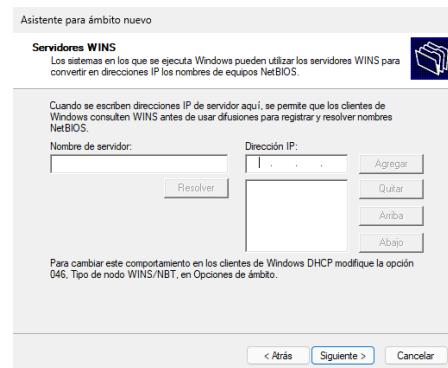
Ya está por defecto la de nuestro Windows Server 2025.



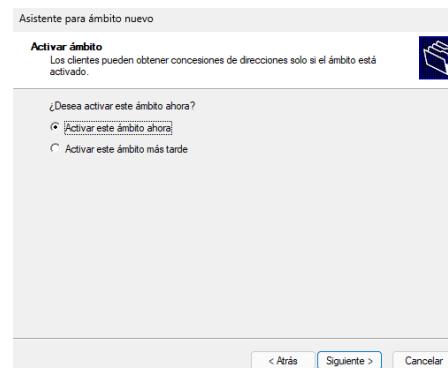
Y por defecto también está configurado nuestro dominio predeterminado y la dirección IP de nuestro servicio de DNS.



No tenemos nada configurado para los servidores WINS, así que lo dejamos en blanco.



Activamos el ámbito ahora



Como podemos ver en nuestro DHCP aparece el ámbito activo y configurado.

## B. Detallar la configuración establecida y el contenido de los ficheros.

El servidor de DNS ha sido instalado automáticamente al promover el dominio de Active Directory por lo tanto no hemos tenido que instalar el Rol de Servidor DNS.

- En el Administrador del servidor, seleccionar la opción de "Aregar roles y características" y luego seleccionar el rol Servidor DNS.

Nuestra zona directa se ha configurado al unir el equipo de Windows 11. Podemos revisarlo en nuestra máquina virtual mediante los comando ping y nslookup utilizando el hostname del equipo Trust-W11.

```
C:\Users\Administrador>hostname
Trust-W11
C:\Users\Administrador>ping Trust-W11

Haciendo ping a Trust-W11.trust.lan [fe80::c6af:3843:fd67:fd6w%7] con 32 bytes de datos:
Respuesta desde fe80::c6af:3843:fd67:fd6w%7: tiempo<1m
Respuesta desde fe80::c6af:3843:fd67:fd6w%7: tiempo<1m
Respuesta desde fe80::c6af:3843:fd67:fd6w%7: tiempo<1m
Respuesta desde fe80::c6af:3843:fd67:fd6w%7: tiempo<1m

Estadísticas de ping para fe80::c6af:3843:fd67:fd6w%7:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\Administrador>nslookup Trust-W11
Servidor: Unknown
Address: 192.168.10.1

Nombre: Trust-W11.trust.lan
Address: 192.168.10.11
```

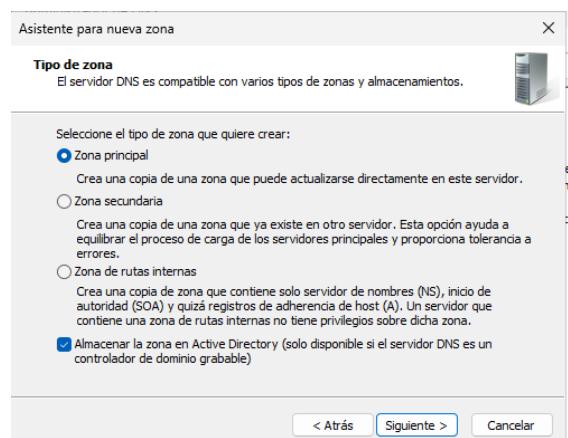
## Configurar una Zona Inversa

Configurar una zona inversa para gestionar la resolución inversa, es decir, de direcciones IP a nombres de dominio. Esto es esencial para ciertos servicios que requieren esta funcionalidad.

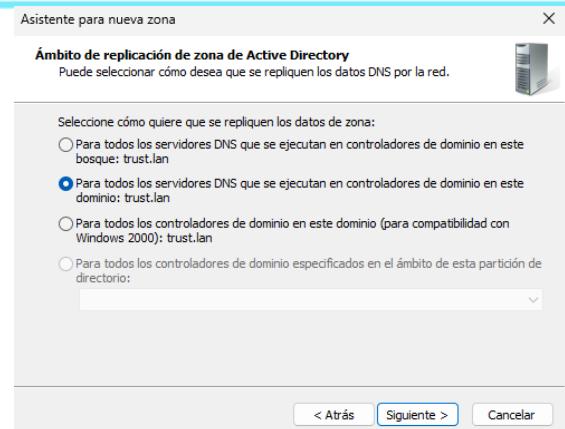
Seguimos los pasos del asistente



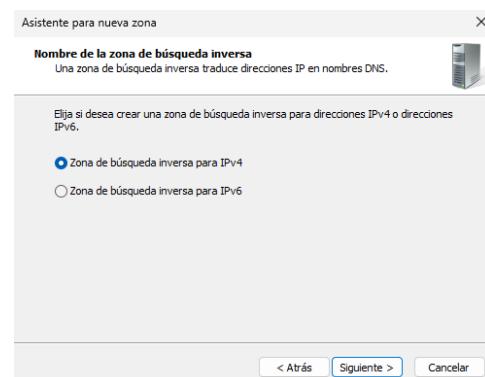
Creamos una zona principal



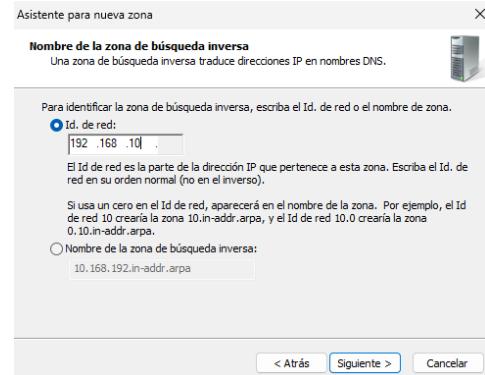
Para todos los servidores de DNS que se ejecutan en ordenadores de dominio en este dominio trust.lan



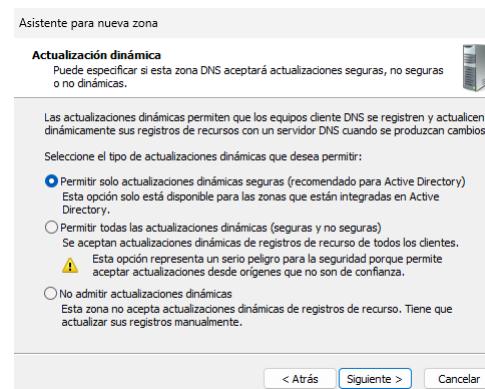
## Zona de búsqueda IPv4



Añadimos la Id. de red  
192.168.10.



## Permitir sólo actualizaciones dinámicas seguras.



Finalizamos el asistente



Como podemos ver en el Administrador de DNS se ha asignado para la IP 192.168.10.1 el nombre de DC-TRUST-01.trust.lan

Administrador de DNS

Archivo Acción Ver Ayuda

Nombre	Tipo	Datos	Marca de
(igual que la carpeta principal)	Inicio de autoridad (SOA)	[2], dc-trust-01.trust.lan, ...	static
(igual que la carpeta principal)	Servidor de nombres (NS)	dc-trust-01.trust.lan.	static
192.168.10.1	Puntero (PTR)	DC-TRUST-01.trust.lan.	28/10/202

Árbol de navegación: DNS > DC-TRUST-01.trust.lan > Zonas de búsqueda directa > Zonas de búsqueda inversa > 10.168.192.in-addr.arpa

Ahora en nuestro servidor de DNS es capaz de resolver la IP 192.168.10.1 con el hostname de nuestro Windows Server 2025

```
C:\Users\Administrador>nslookup 192.168.10.1
Servidor:  DC-TRUST-01.trust.lan
Address:  192.168.10.1

Nombre:  DC-TRUST-01.trust.lan
Address: 192.168.10.1
```

Vamos a añadir un nuevo puntero que sea capaz de resolver nuestra máquina Windows 11

Administrador de DNS

Archivo Acción Ver Ayuda

Nombre	Tipo	Datos	Marca de
(igual que la carpeta principal)	Inicio de autoridad (SOA)	[2], dc-trust-01.trust.lan, ...	static
(igual que la carpeta principal)	Servidor de nombres (NS)	dc-trust-01.trust.lan.	static
192.168.10.1	Puntero (PTR)	DC-TRUST-01.trust.lan.	28/10/202

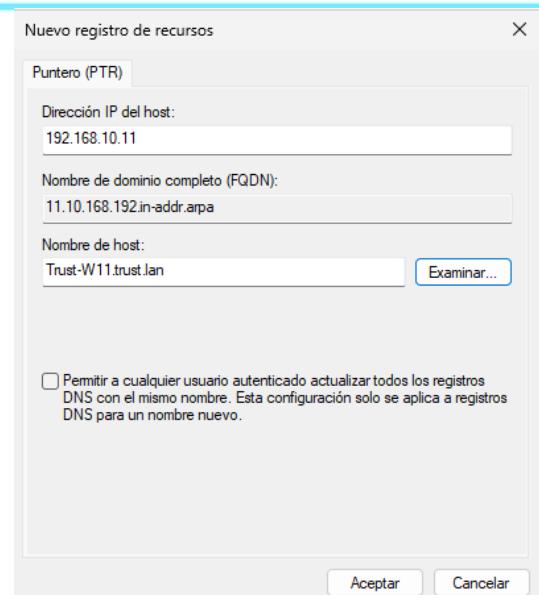
Árbol de navegación: DNS > DC-TRUST-01.trust.lan > Zonas de búsqueda directa > Zonas de búsqueda inversa > 10.168.192.in-addr.arpa

Menú contextual:

- Actualizar archivo de datos del servidor
- Volver a cargar
- Nuevo puntero (PTR)...**
- Alias nuevo (CNAME)...
- Delegación nueva...
- Registros nuevos...
- DNSSEC

Asignamos la IP del host.  
en este caso 192.168.10.11

Y añadimos el nombre del host:  
Trust-W11.trust.lan



Como podemos ver se ha creado correctamente nuestro puntero y al utilizar nslookup 192.168.10.11, nuestro servidor DNS es capaz de resolver con el Hostname de nuestra máquina Windows 11

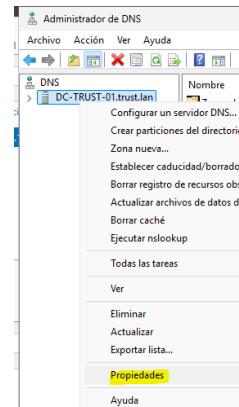
Nombre	Tipo	Datos	Marca de
(igual que la carpeta princip...)	Inicio de autoridad (SOA)	[2], dc-trust-01.trust.lan, ...	static
(igual que la carpeta princip...)	Servidor de nombres (NS)	dc-trust-01.trust.lan.	static
192.168.10.1	Puntero (PTR)	DC-TRUST-01.trust.lan.	28/10/202
192.168.10.11	Puntero (PTR)	Trust-W11.trust.lan	

```
C:\Users\Administrador>nslookup 192.168.10.11
Servidor:  DC-TRUST-01.trust.lan
Address:  192.168.10.1

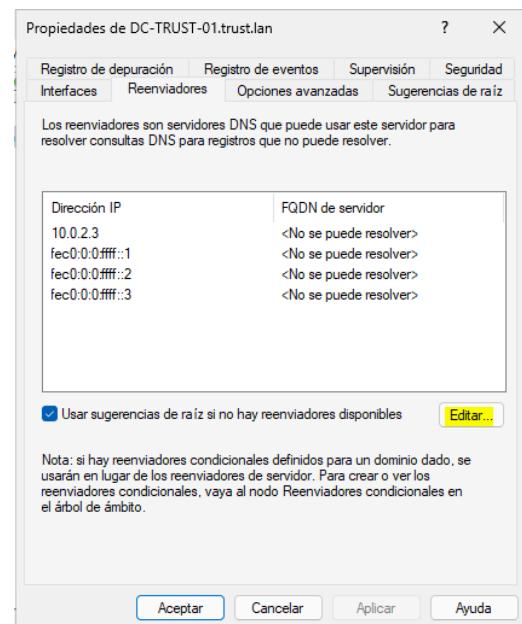
Nombre:  Trust-W11.trust.lan
Address:  192.168.10.11
```

De todos modos aún no somos capaces de resolver direcciones como google.com o uoc.edu. Nuestra mejor opción es añadir un reenviador. En este caso añadiremos el DNS de google (8.8.8.8)

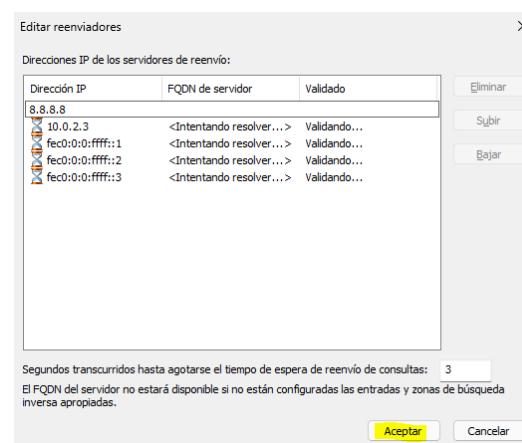
En nuestro administrador de DNS click derecho >  
Propiedades



Ahora pulsamos en Editar



Añadimos la dirección IP 8.8.8.8 y pulsamos en aceptar.



Como vemos el servidor nos indica que es el dns.google



## c. Demostrar el correcto funcionamiento del servidor DHCP y DNS.

### *Mostrar el correcto funcionamiento de DNS*

En mi maquina Windows 11 utilizamos “nslookup” para confirmar que funciona el servicio de DNS.

```
C:\Users\Administrador>hostname
Trust-W11

C:\Users\Administrador>ping Trust-W11
Haciendo ping a Trust-W11.trust.lan [fe80::c68f:3843:fd67:f0d6%7] con 32 bytes de datos:
Respuesta desde fe80::c68f:3843:fd67:f0d6%7: tiempo=1ms
Respuesta desde fe80::c68f:3843:fd67:f0d6%7: tiempo=1ms
Respuesta desde fe80::c68f:3843:fd67:f0d6%7: tiempo=1ms
Respuesta desde fe80::c68f:3843:fd67:f0d6%7: tiempo=1ms

Estadísticas de ping para fe80::c68f:3843:fd67:f0d6%7:
  Paquetes: enviados = 4, recibidos = 4, perdidos = 0
  (% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
  Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\Administrador>nslookup Trust-W11
Servidor:  Unknown
Address:  192.168.10.1

Nombre:  trust.lan
Addresses:  fd17:625c:f037:2:3daa:6bf:9d0b:45e7
           192.168.10.1
           10.0.2.15

C:\Users\Administrador>

C:\Users\Administrador>nslookup google.es
Servidor:  DC-TRUST-01.trust.lan
Address:  192.168.10.1

Respuesta no autoritativa:
Nombre:  google.es
Addresses:  2a00:1450:4003:80d::2003
           142.250.200.67

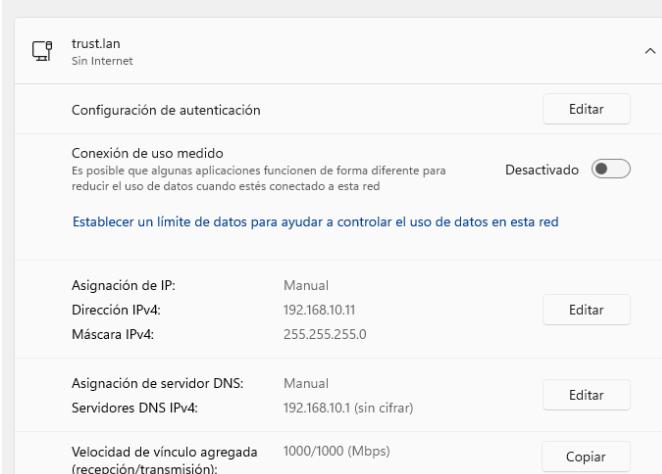
C:\Users\Administrador>nslookup uoc.edu
Servidor:  DC-TRUST-01.trust.lan
Address:  192.168.10.1

Respuesta no autoritativa:
Nombre:  uoc.edu
Addresses:  99.83.131.89
           75.2.63.131
```

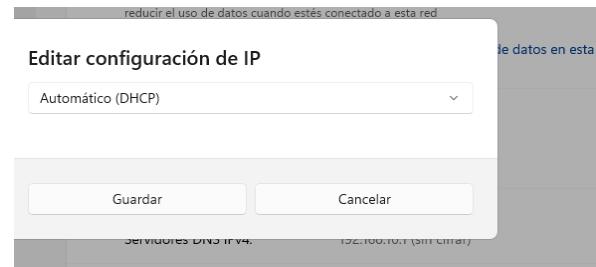
### *Mostrar el correcto funcionamiento de DHCP*

Si vamos a nuestra máquina Windows 11, como hemos visto anteriormente nosotros configuramos manualmente los parámetros y asignamos la IP 192.168.10.11

#### Red e Internet > Ethernet



Si pulsamos en editar y los asignamos automáticamente.



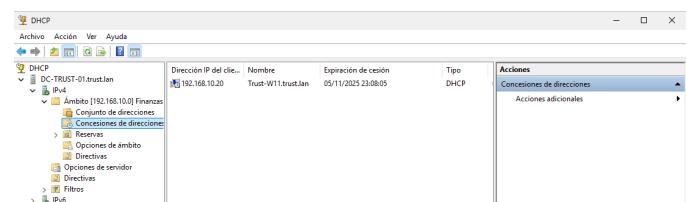
En el cmd ejecutamos un ifconfig

Y podemos observar que se ha añadido la IP 192.168.10.20 que es la primera del ámbito de Finanzas que habíamos configurado anteriormente.

Además en el servidor se registra la dirección junto con el hostname

```
C:\Users\Administrador>ipconfig
Configuración IP de Windows

Adaptador de Ethernet LAN:
  Sufijo DNS específico para la conexión. . . : trust.lan
  Vínculo: dirección IPv6 local. . . : fe80::c68f:3843:fd67:f0d6%7
  Dirección IPv4. . . . . : 192.168.10.20
  Máscara de subred . . . . . : 255.255.255.0
  Puerta de enlace predeterminada . . . . . : 192.168.10.1
```



5. Instalar herramientas de administración remota para configurar el/los servidores. La configuración de este servicio, sólo permitirá acceder desde un rango de direcciones IP determinado y tan sólo a un usuario específico. Crear un vídeo tutorial en el cual se demuestre la instalación y configuración de herramientas de administración remota.

## A. Explicar el proceso de instalación del Escritorio remoto

*Habilitar Escritorio Remoto en el servidor:*

- Para permitir que una computadora acepte conexiones RDP, se debe habilitar la opción de Escritorio Remoto en la configuración.
- Ir a Configuración > Sistema > Escritorio remoto.
- Activar la opción de Habilitar Escritorio remoto.

*Conectar desde el cliente:*

- En la máquina que actuará como cliente, abrir la aplicación Conexión a Escritorio Remoto (Remote Desktop Connection).
- Introducir el nombre o la dirección IP de la computadora a la que se quiere conectar.
- Ingresar las credenciales (nombre de usuario y contraseña) de la cuenta que tiene permisos para acceder al equipo remoto.

*Opciones avanzadas:*

- RDP permite ajustar la calidad de la conexión, el tamaño de pantalla, o redirigir recursos locales como carpetas, impresoras y más para que se puedan usar en el equipo remoto.

En nuestro caso vamos a instalar **RDP multisesión**. Es una característica que permite que múltiples usuarios se conecten simultáneamente a una misma máquina (generalmente un servidor) a través de **Remote Desktop Protocol (RDP)**, cada uno con su propia sesión de escritorio independiente. Esta funcionalidad es comúnmente utilizada en sistemas operativos de servidor, como **Windows Server**, donde varios usuarios pueden acceder de forma remota al servidor, pero cada uno trabaja en su propio entorno sin interferir con las actividades de otros usuarios.

Característica	RDP (Una sola sesión)	RDP Multisesión
Usuarios simultáneos	Solo un usuario puede conectarse a la vez	Múltiples usuarios pueden conectarse simultáneamente
Entorno operativo	Windows 10/11 Pro, Home (versiones cliente)	Windows Server, Azure Virtual Desktop (entornos multisesión)
Sesiones independientes	No, solo una sesión activa por equipo	Sí, cada usuario tiene una sesión independiente
Uso común	Acceso remoto para un usuario a un escritorio personal	Acceso remoto para múltiples usuarios a un servidor compartido
Recursos compartidos	Solo un usuario utiliza los recursos del sistema	Los recursos del servidor son compartidos entre los usuarios

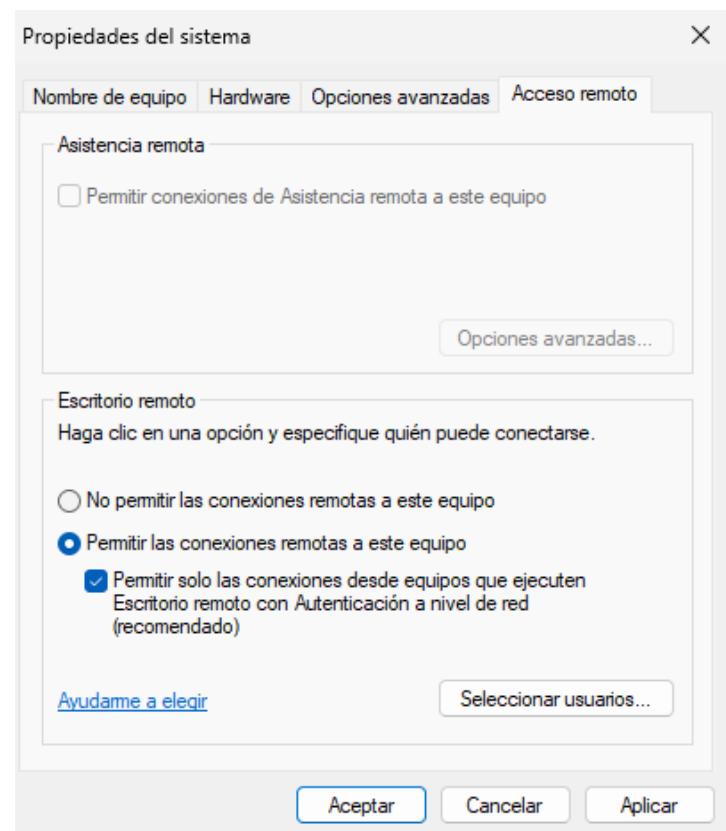
## B. Configurar RSAT y mostrar el proceso de instalación y acceso.

En nuestro Windows Server 2025, pulsamos en Servidor local > Escritorio remoto



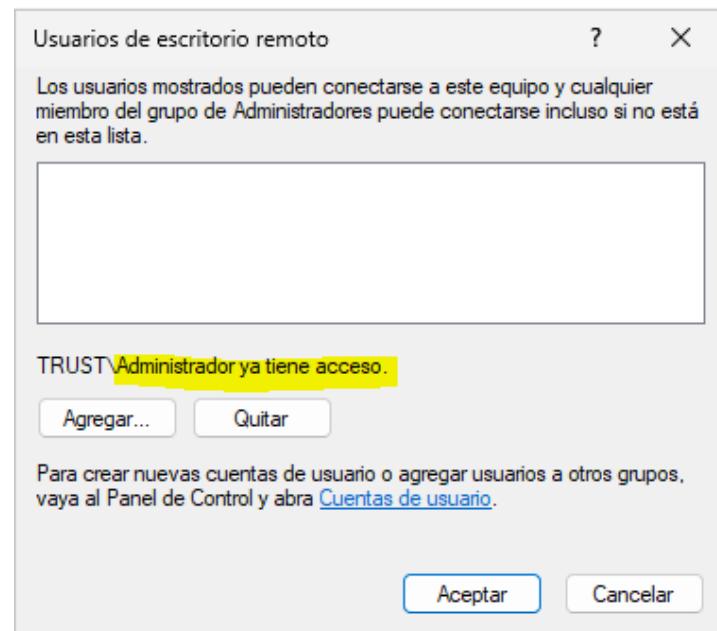
Marcamos la opción de Permitir las conexiones desde equipos que ejecuten Escritorio remoto con Autenticación a nivel de red.

Pulsamos en Seleccionar usuarios.



Como vemos Administrador ya tiene acceso. En futuros productos deshabilitamos el usuario Administrador, debemos asegurarnos de agregar la cuenta que utilizaremos como administrador del dominio (ruben.vicente)

Aquí podemos agregar o quitar permisos para el escritorio remoto.



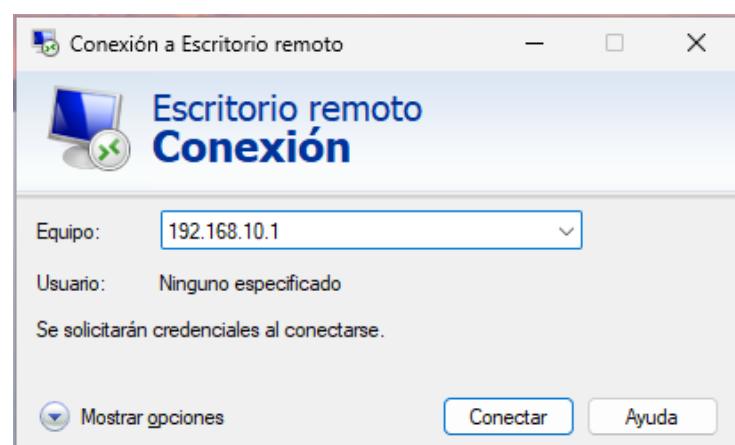
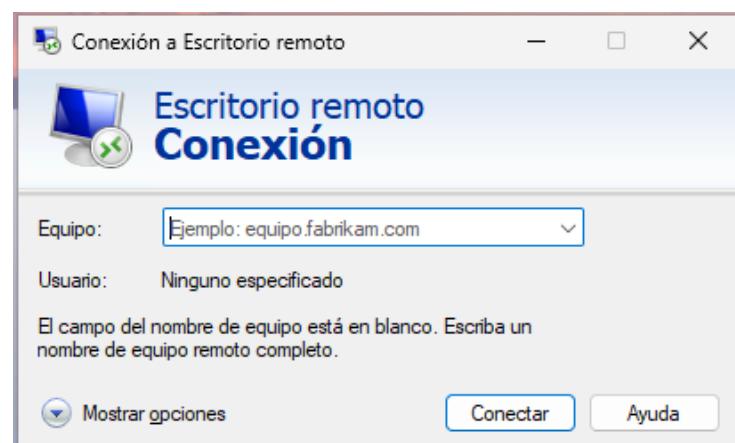
Ya tenemos el Escritorio Remoto Habilitado.

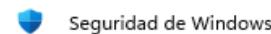


- c. Mostrar y comentar qué ficheros son necesarios para su correcto funcionamiento.
- d. Detallar la configuración establecida y el contenido de los ficheros.

## E. Mostrar el funcionamiento y la conexión remota a la máquina.

En nuestra máquina Windows 11





## Escribir las credenciales

Estas credenciales se usarán para conectarse a 192.168.10.1.

Nombre de usuario

Contraseña

Dominio:

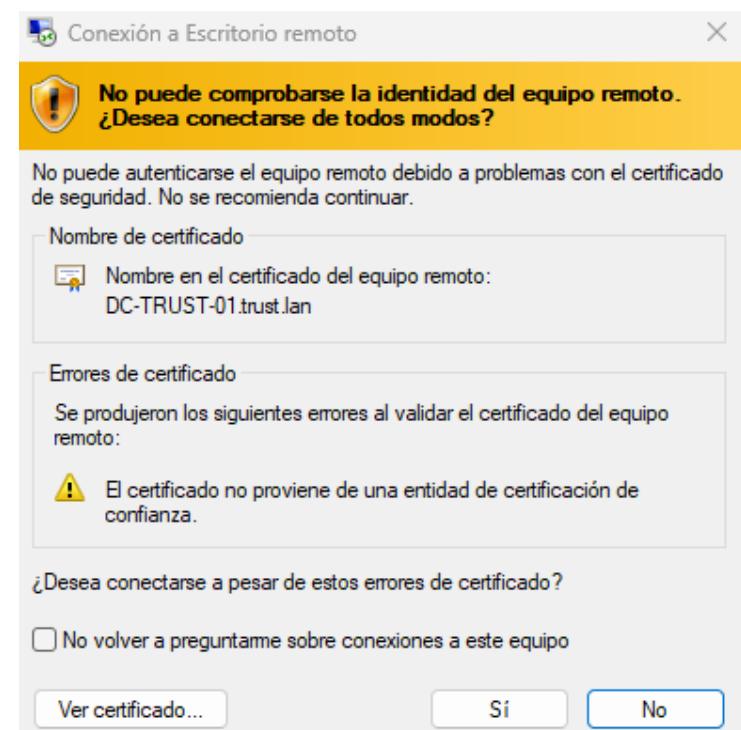
Recordar cuenta

Aceptar

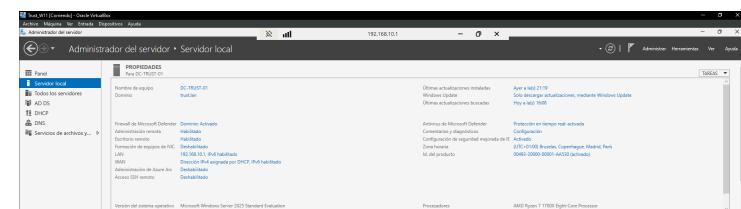
Cancelar

Introducimos nuestras credenciales de Administrador y como vemos aparece una advertencia debida a que nos está indicando que detrás de trust.lan no existe una unidad certificadora.

Pulsamos en si, puesto que nos queremos conectar de todos modos.



Como vemos estamos dentro del servidor desde Trust\_W11. Pero nuestra sesión anterior dentro del servidor nos ha echado.



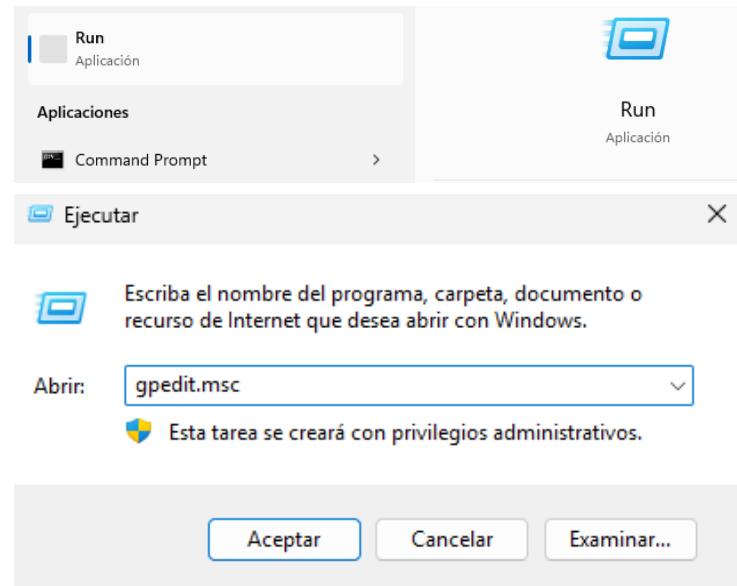
Sucederá lo mismo en al revés.



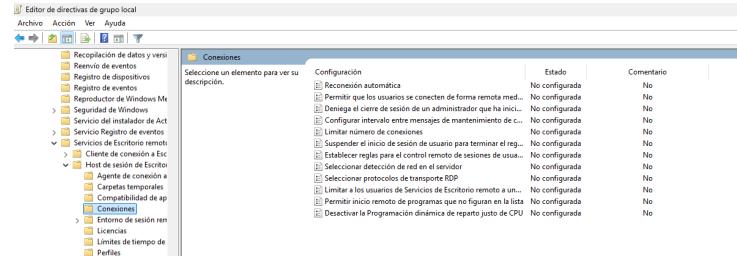
## Configuración de RDP (Escritorio Remoto) Multi-sesión

Para permitir múltiples sesiones de Escritorio Remoto (RDP) en Windows Server, las Políticas de Grupo Local juegan un papel clave en ajustar las configuraciones de seguridad y acceso remoto. Para habilitar el acceso de varios usuarios al mismo tiempo debemos realizarlo a través de la siguiente política.

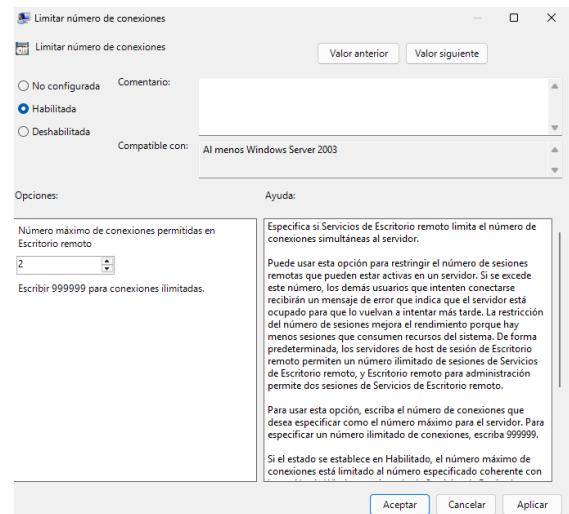
Abre el Ejecutar de Windows y escribe gpedit.msc para abrir la consola del "Editor de políticas de grupo local"



Dentro de "Configuración del equipo", "Plantillas administrativas", "Componentes de Windows", "Servicios de Escritorio remoto", "Escritorio remoto Host de sesión" y dentro de "Conexiones"



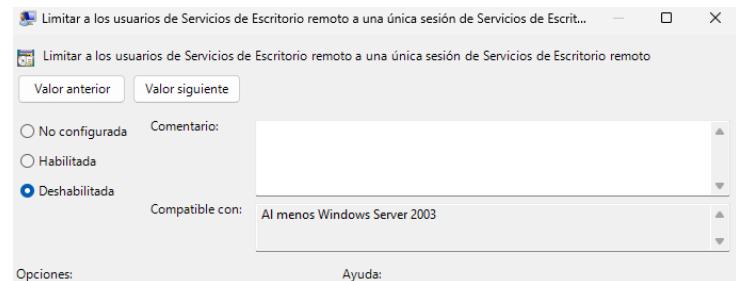
Doble clic en "Limitar el número de conexiones" del mismo apartado, lo habilitamos y establece el número máximo de conexiones de escritorio remoto en 2.



Ahora, doble clic en la política "Limitar a los usuarios del Servicio de Escritorio remoto a una sola sesión de Servicios de Escritorio remoto", marca la casilla deshabilitada, aplica los cambios y cierra la ventana.

Esto nos permite que los usuarios puedan establecer un número ilimitado de conexiones remotas simultáneamente.

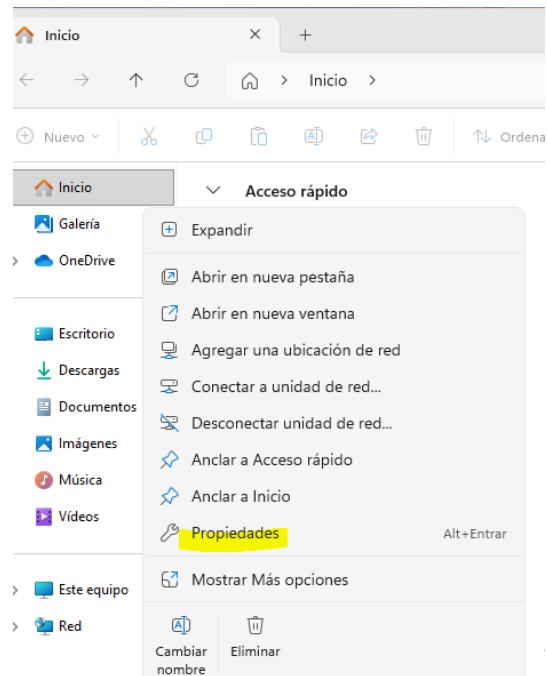
Así debería de quedarnos.



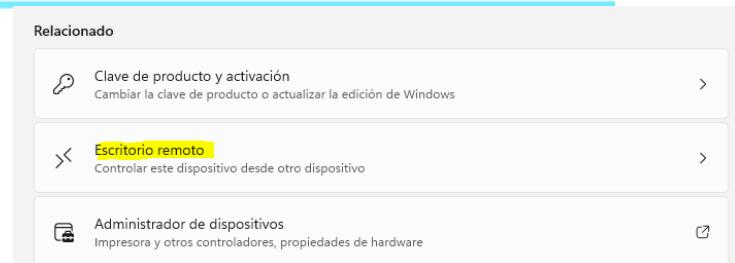
Configuración	Estado	Comentario
Reconexión automática	No configurada	No
Permitir que los usuarios se conecten de forma remota med...	No configurada	No
Deniega el cierre de sesión de un administrador que ha inici...	No configurada	No
Configurar intervalo entre mensajes de mantenimiento de c...	No configurada	No
Limitar número de conexiones	Habilitada	No
Suspender el inicio de sesión de usuario para terminar el reg...	No configurada	No
Establecer reglas para el control remoto de sesiones de usu...	No configurada	No
Seleccionar detección de red en el servidor	No configurada	No
Seleccionar protocolos de transporte RDP	No configurada	No
Limitar a los usuarios de Servicios de Escritorio remoto a un...	Deshabilitada	No
Permitir inicio remoto de programas que no figuran en la lista	No configurada	No
Desactivar la Programación dinámica de reparto justo de CPU	No configurada	No

## Configurar Escritorio remoto para la máquina de Windows 11

En nuestro equipo de Windows 11 > Propiedades



Pulsamos en Escritorio Remoto

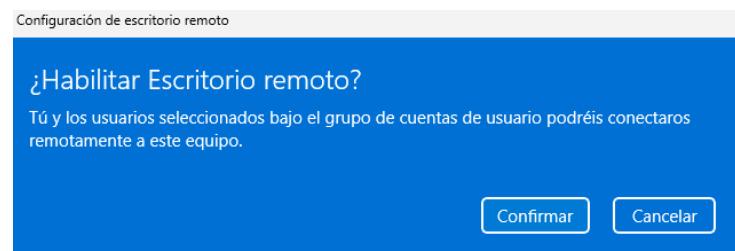


Lo activamos

Sistema > Escritorio remoto



Pulsamos en confirmar.



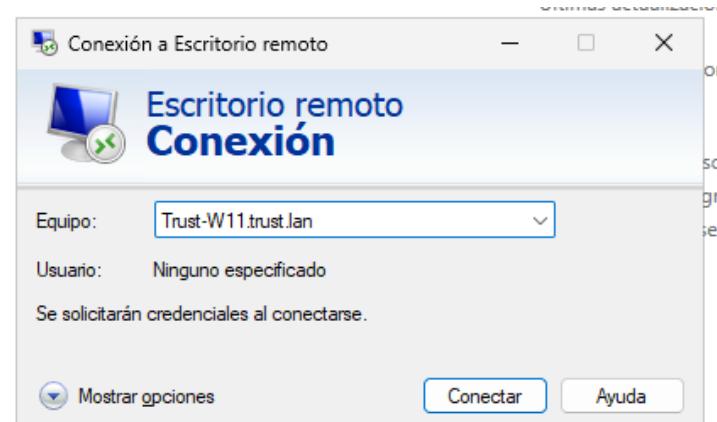
## F. Comprobar el correcto funcionamiento del nuevo sistema informático y el servicio de directorio.

Ya hemos visto que desde el equipo Windows 11 nos podemos conectar a Windows Server 2025. Ahora lo que vamos a ver es si podemos desde otro equipo, en este caso desde el servidor podemos acceder al dispositivo Trust-W11, que es nuestro equipo Windows 11.

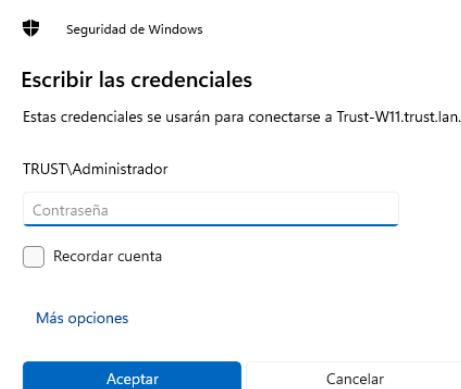
Abrimos el escritorio remoto dentro de nuestro servidor.



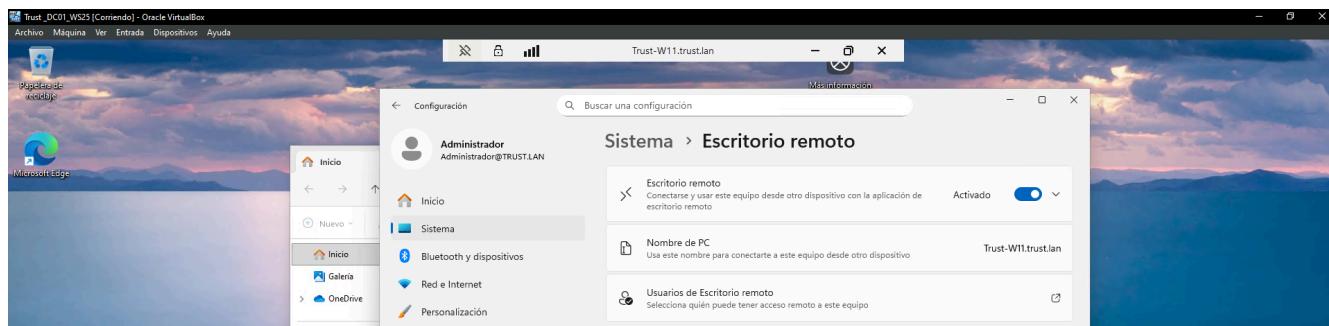
Añadimos el equipo al que deseamos conectarnos, en nuestro caso el Trust-W11.trust.lan



Ingresamos nuestras credenciales.



Y como vemos podemos acceder desde nuestro Trust\_DC01\_WS25, que es la máquina virtual de nuestro Windows Server 2025



## Bibliografía

- Clockwork Computer. (2024, septiembre 15). **Windows 11** *Instalación desde cero en VirtualBox [Video]*. YouTube. <https://www.youtube.com/watch?v=gj4KcnhaO6k>
- Clockwork Computer. (s. f.). *Clockwork Computer* [Blog]. Recuperado de <https://clockworkcomputerip.blogspot.com/>

## Anexo

### Instalación de Ubuntu Desktop y unirlo al dominio.

En nuestro Ubuntu Desktop instalamos todos los paquetes necesarios.

#### Instalar NTPDATE

```
sudo apt-get install ntpdate
```

```
sudo ntpdate -q trust.lan
```

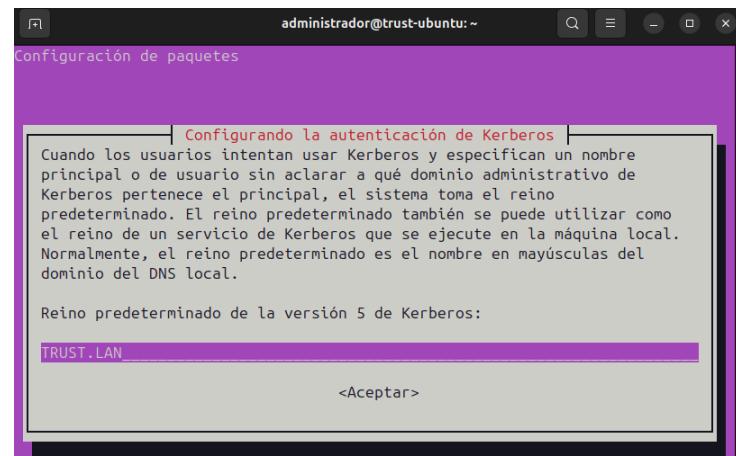
```
sudo ntpdate trust.lan
```

```
administrador@trust-ubuntu:~$ sudo apt-get install ntpdate
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:

[REDACTED]
```

#### Instalar paquetes necesarios

```
sudo apt-get install samba krb5-config krb5-user
winbind libpam-winbind libnss-winbind
```



Comprobar autenticación en el servidor de Kerberos mediante el administrador de usuarios  
kinit Administrador@TRUST.LAN

```
administrador@trust-ubuntu:~$ kinit Administrador@TRUST.LAN
Password for Administrador@TRUST.LAN:
Warning: Your password will expire in less than one hour on mar 14 sep 2100 04:48:05
[REDACTED]
administrador@trust-ubuntu:~$ klist
Ticket cache: FILE:/tmp/krb5cc_1000
Default principal: Administrador@TRUST.LAN

Valid starting       Expires             Service principal
29/10/25 23:36:02  30/10/25 09:36:02  krbtgt/TRUST.LAN@TRUST.LAN
renew until 30/10/25 23:35:54
```

Mover archivo smb.conf y crear copia de seguridad  
sudo mv /etc/samba/smb.conf  
/etc/samba/smb.conf.initial

```
root@trust-ubuntu:/home/administrador# nano /etc/samba/smb.conf
[global]
workgroup = TRUST
realm = TRUST.LAN
netbios name = trust-ubuntu
security = ADS
dns forwarder = 192.168.10.1

[REDACTED]
```

sudo nano /etc/samba/smb.conf

```
root@trust-ubuntu:/home/administrador# sudo systemctl restart smbd nmbd
root@trust-ubuntu:/home/administrador# sudo systemctl enable smbd nmbd
Synchronizing state of smbd.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable smbd
Synchronizing state of nmbd.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable nmbd
root@trust-ubuntu:/home/administrador#
```

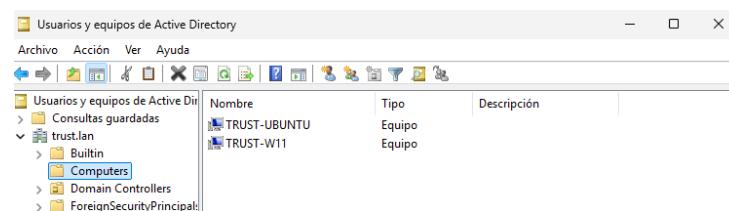
Reiniciar todos los daemons de samba  
sudo systemctl restart smbd nmbd

Habilitar los servicios de samba  
sudo systemctl enable smbd nmbd

Unir Ubuntu Desktop a SAMBA AD DC  
 sudo net ads join -U Administrador

Vemos como en Usuarios y equipos de Active Directory aparece nuestro equipo TRUST-UBUNTU

```
root@trust-ubuntu:/home/administrador# sudo net ads join -U Administrador
Password for [TRUST\Administrador]:*
Using short domain name -- TRUST
Joined 'TRUST-UBUNTU' to dns domain 'trust.lan'
No DNS domain configured for trust-ubuntu. Unable to perform DNS Update.
DNS update failed: NT_STATUS_INVALID_PARAMETER
root@trust-ubuntu:/home/administrador#
```



sudo nano /etc/nsswitch.conf

```
GNU nano 7.2                               /etc/nsswitch.conf *
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the 'glibc-doc-reference' and 'info' packages installed, try:
# 'info libc "Name Service Switch"' for information about this file.
#
passwd:      compat winbind
group:       compat winbind
shadow:      compat winbindn
gshadow:     files systemd

hosts:       files dns
networks:    files

protocols:   db files
services:    db files sss
ethers:      db files
rpc:         db files

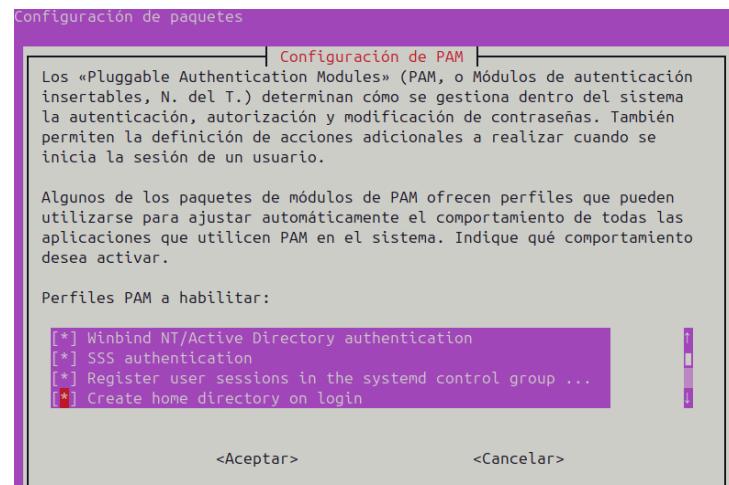
netgroup:    nis sss
automount:   sss
```

Reinic平 servicio winbind  
 sudo systemctl restart winbind

```
root@trust-ubuntu:/home/administrador# sudo systemctl restart winbind
root@trust-ubuntu:/home/administrador# wbinfo -u
administrador
invitado
```

Listar usuarios y grupos del dominio.  
 wbinfo -u

Configurar pam-auth-update para autenticarnos con cuentas de dominio y que se creen automáticamente los directorios.  
 sudo pam-auth-update



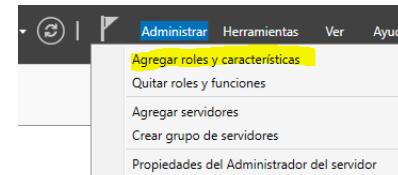
Editar el archivo /etc/pam.d/common-account para crear automáticamente directorios.  
nano /etc/pam.d/common-account

```
GNU nano 7.2          /etc/pam.d/common-account *
# only deny service to users whose accounts are expired in /etc/shadow.
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.
#
# here are the per-package modules (the "Primary" block)
account [success=2 new_authtok_reqd=done default=ignore]      pam_unix.so
account [success=1 new_authtok_reqd=done default=ignore]      pam_winbind.so
# here's the fallback if no module succeeds
account requisite          pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
account required          pam_permit.so
# and here are more per-package modules (the "Additional" block)
account sufficient        pam_localuser.so
account [default=bad success=ok user_unknown=ignore]      pam_sss.so
# end of pam-auth-update config
session    required      pam_mkhomedir.so   skel=/etc/skel/   umask=0022
```

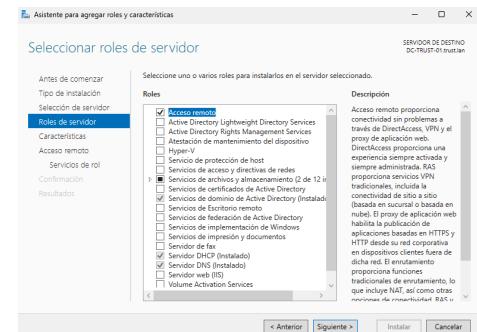
## SNAT en Windows Server 2025

SNAT (Source Network Address Translation) es una técnica de NAT (Network Address Translation) que se utiliza para cambiar la dirección IP de origen en los paquetes que salen de una red interna hacia una red externa (Internet). El propósito principal de SNAT es permitir que los dispositivos de una red privada, que utilizan direcciones IP privadas (no enrutable en Internet), puedan acceder a una red pública (como Internet) utilizando una dirección IP pública.

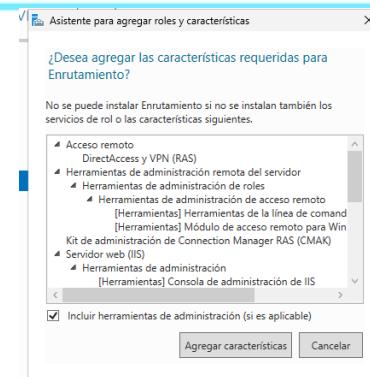
Agregamos roles y características



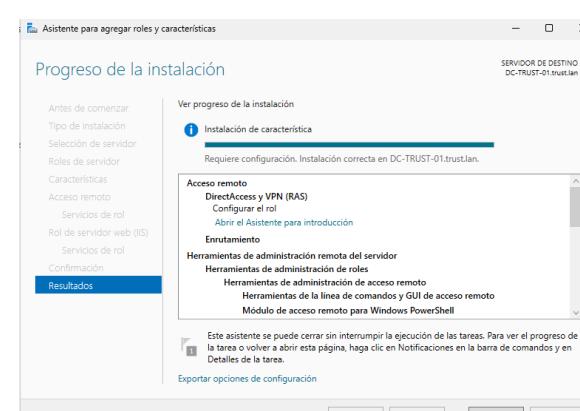
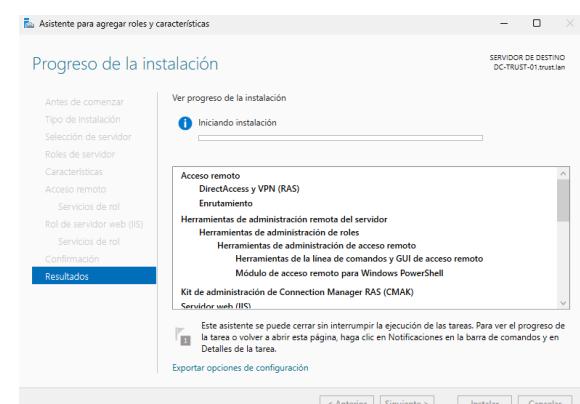
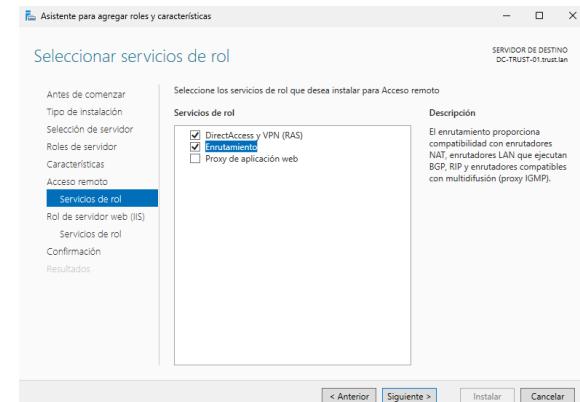
Seguimos el instalador y seleccionamos Acceso remoto

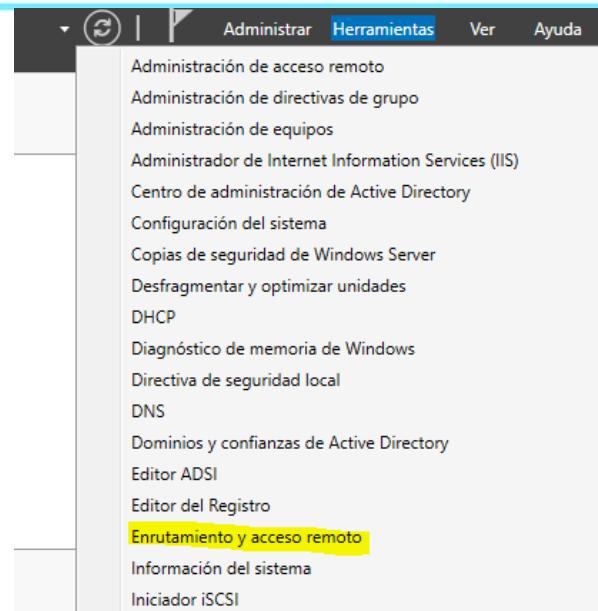


Agregamos las características.

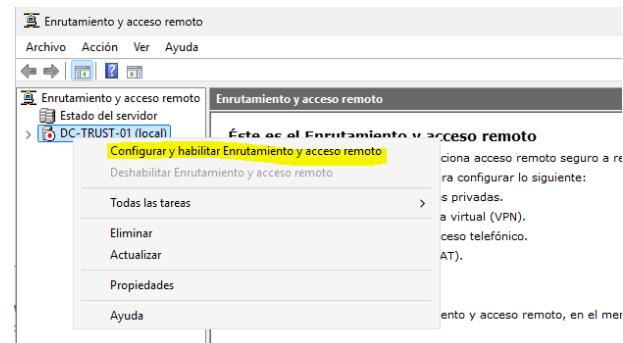


Marcamos Enrutamiento

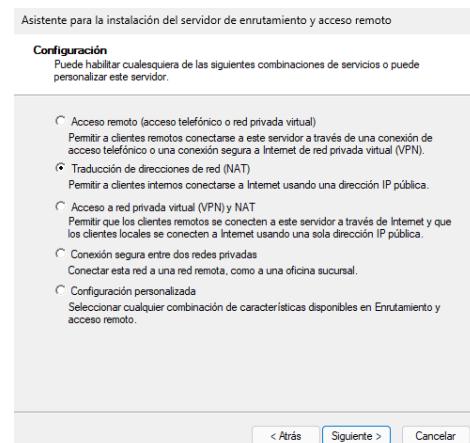




Click derecho en nuestro dominio > Configurar Enrutamiento y acceso remoto.



Seleccionamos Traducción de direcciones de red (NAT)



Seleccionamos la interfaz pública para conectarnos a internet en nuestro caso WAN

Asistente para la instalación del servidor de enrutamiento y acceso remoto

#### Conexión a Internet NAT

Puede seleccionar una interfaz existente o crear una nueva interfaz de marcado a petición para equipos clientes a fin de conectarse a Internet.

- Utilizar esta interfaz pública para conectarse a Internet:

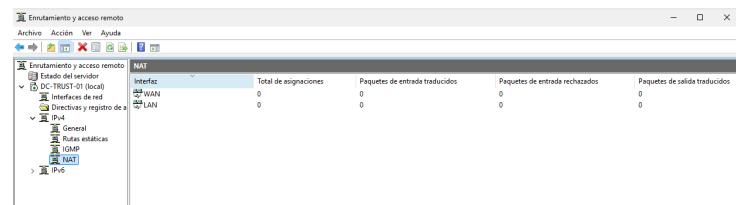
Interfaces de red:

Nombre	Descripción	Dirección IP
LAN	Intel(R) PRO/1000 MT...	192.168.10.1
LAN2	Intel(R) PRO/1000 MT...	192.168.20.1
WAN	Intel(R) PRO/1000 MT...	10.0.2.15 (DHCP)

- Crear una conexión a Internet de marcado a petición

Una interfaz de marcado a petición se activa cuando un cliente usa Internet. Seleccione esta opción si el servidor se conecta con un módem o usando el protocolo punto a punto a través de Ethernet. El Asistente para interfaz de marcado a petición se iniciará al final de este asistente.

< Atrás      Siguiente >      Cancelar



En nuestra máquina Windows 11 añadimos la puerta de enlace y realizamos un ping a google

```
c:\users\Administrador>ipconfig
Configuración IP de Windows

Adaptador de Ethernet LAN:

        Sufijo DNS específico para la conexión. . . :
        Vínculo: dirección IPv6 local. . . : fe80::c68f:3843:fd67:f0d6%7
        Dirección IPv4. . . . . : 192.168.10.11
        Máscara de subred. . . . . : 255.255.255.0
        Puerta de enlace predeterminada. . . . . : 192.168.10.1

C:\Users\Administrador>ping 8.8.8.8

Haciendo ping a 8.8.8.8 con 32 bytes de datos:
Respueta desde 8.8.8.8: bytes=32 tiempo=20ms TTL=254
Respueta desde 8.8.8.8: bytes=32 tiempo=19ms TTL=254
Respueta desde 8.8.8.8: bytes=32 tiempo=20ms TTL=254
Respueta desde 8.8.8.8: bytes=32 tiempo=19ms TTL=254

Estadísticas de ping para 8.8.8.8:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 19ms, Máximo = 20ms, Media = 19ms
```

Podemos ver el tráfico de qué conexión privada se está enruteando a qué IP pública.

DC-TRUST-01 - Tabla de signación de sesiones de traducción de direcciones de red							
Protocolo	Local	Dirección privada	Dirección privada	Dirección pública	Puerto público	Puerto privado	Indice
TCP	Entrada externa	192.168.10.11	63.434	10.0.2.15	63.434	4.207.207.139	443
TCP	Entrada externa	192.168.10.11	63.434	10.0.2.15	63.434	4.207.247.139	443