

Conectar clientes Windows 11 y Ubuntu a un Active Directory (AD)

2022

Conectar clientes Windows 11 y Ubuntu a un Active Directory (AD) 2022 implica dos procesos diferentes. El de Windows es nativo y directo, mientras que Ubuntu requiere la instalación y configuración de algunos paquetes.

Aquí tienes los pasos para ambos.

Requisitos Previos (¡Importante!)

Antes de empezar, asegúrate de cumplir con lo siguiente:

1. **Servidor AD Funcional:** Tu Controlador de Dominio (DC) con Windows Server 2022 debe estar instalado, configurado y operativo.
 2. **Nombre de Dominio:** Debes conocer el nombre completo de tu dominio (ej. `miempresa.local`).
 3. **Credenciales:** Necesitas un usuario y contraseña de AD con permisos para unir equipos al dominio (como el `Administrador` del dominio).
 4. **Red y DNS:** Este es el paso **más crítico**. Tanto el cliente Windows 11 como el de Ubuntu **deben** usar la dirección IP de tu Controlador de Dominio (el servidor AD 2022) como su **servidor DNS principal**.
 - Sin la resolución DNS correcta, los clientes *nunca* encontrarán el dominio.
-



1. Conectar Cliente Windows 11

Este proceso es sencillo. Asegúrate de que tu edición de Windows 11 **no sea "Home"**, ya que esta edición no puede unirse a un dominio de Active Directory. Necesitas **Windows 11 Pro, Enterprise o Education**.

1. **Verificar DNS:**
 - Ve a `Configuración > Red e Internet`.
 - Selecciona tu adaptador (Ethernet o Wi-Fi) y ve a sus propiedades.
 - En `Asignación de servidor DNS`, haz clic en `Editar`.
 - Configúalo en `Manual`, activa `IPv4` e ingresa la dirección IP de tu Controlador de Dominio en `DNS preferido`.
 - Guarda y reinicia la conexión si es necesario.

2. Unir al Dominio:

- Abre el menú Inicio, escribe `sysdm.cpl` y presiona Enter. Esto abrirá las "Propiedades del sistema".
- Ve a la pestaña **Nombre de equipo**.
- Haz clic en el botón **Cambiar...**
- En la sección "Miembro de", selecciona **Dominio**.
- Escribe el nombre completo de tu dominio (ej. `miempresa.local`).
- Haz clic en **Aceptar**.

3. Autenticar:

- Aparecerá una ventana pidiendo credenciales.
- Ingresa el nombre de usuario (ej. `Administrador`) y la contraseña de tu cuenta de AD con permisos para unir equipos.
- *Nota: Si el nombre de usuario "Administrador" es ambiguo, usa el formato `DOMINIO\usuario` (ej. `MIEMPRESA\Administrador`).*

4. Reiniciar:

- Si todo sale bien, recibirás un mensaje de bienvenida al dominio.
 - El sistema te pedirá reiniciar el equipo. Hazlo para aplicar los cambios.
 - Despues de reiniciar, podrás iniciar sesión con tus credenciales de dominio (ej. `MIEMPRESA\tu_usuario`).
-



2. Conectar Cliente Ubuntu (Método Moderno con `realmd`)

Usaremos `realmd` y `sssd`, que es el método estándar y más sencillo para integrar Ubuntu con AD.

1. Verificar DNS y Hora:

- **DNS:** Asegúrate de que `/etc/resolv.conf` apunte a tu DC, o configúralo a través del gestor de red (Netplan o NetworkManager GUI). Tu Ubuntu *debe* poder resolver el nombre del dominio.
- Puedes probarlo con: `ping miempresa.local` (reemplaza con tu dominio).

Hora: La hora del cliente Ubuntu y del servidor AD deben estar sincronizadas. Kerberos (el protocolo de autenticación de AD) es muy sensible a diferencias de tiempo. Instala un cliente NTP:

Bash

```
sudo apt update
```

```
sudo apt install ntp
```

2. Instalar Paquetes Necesarios:

Abre una terminal e instala los paquetes que gestionarán la conexión y la autenticación.

Bash

```
sudo apt update
```

```
sudo apt install realmd sssd sssd-tools libnss-sss libpam-sss adcli samba-common-bin  
krb5-user
```

○

- Durante la instalación de **krb5-user**, es posible que te pida un "Reino (realm) de Kerberos predeterminado". Escribe el nombre de tu dominio **en mayúsculas** (ej. **MIEMPRESA.LOCAL**).

3. Descubrir el Dominio (Opcional pero recomendado):

Este comando verifica que Ubuntu pueda encontrar tu dominio AD usando el DNS.

Bash

```
realm discover miempresa.local
```

- Deberías ver una salida que lista tu dominio, el tipo (**active-directory**) y el software necesario.

4. Unir al Dominio:

Ejecuta el siguiente comando para unirte. Reemplaza **Administrador** con tu usuario de AD con permisos y **miempresa.local** con tu dominio.

Bash

```
sudo realm join -U Administrador miempresa.local
```

- Te pedirá la contraseña del usuario **Administrador** de AD. Ingrésala.
- Si todo va bien, no devolverá ningún error.

5. Verificar la Unión:

Para confirmar que te has unido, usa:

Bash

```
realm list
```

- Deberías ver tu dominio listado.

Prueba a resolver un usuario de AD:

Bash

```
id usuario_de_ad@miempresa.local
```

- Deberías ver la información (UID, GID) de ese usuario.

6. Configurar Creación de Carpetas Personales (Home):

- Por defecto, cuando un usuario de AD inicia sesión por primera vez, Ubuntu no crea su carpeta **/home/usuario**. Debemos habilitarlo.

Edita el archivo de configuración de PAM (Pluggable Authentication Modules):

Bash

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

Añade la siguiente línea justo *antes* de la línea `session required pam_unix.so`:

```
session required pam_mkhomedir.so skel=/etc/skel/ umask=0022
```

- Guarda el archivo (Ctrl+O) y sal (Ctrl+X).

7. (Opcional) Dar Permisos `sudo` a Usuarios o Grupos de AD:

- Si quieres que ciertos usuarios o grupos de AD tengan privilegios `sudo` en el equipo Ubuntu, debes añadirlos al archivo `sudoers`.

La forma más segura es crear un nuevo archivo en `/etc/sudoers.d/`:

Bash

```
sudo nano /etc/sudoers.d/dominio_admins
```

Para dar `sudo` a un usuario específico:

```
usuario_de_ad@miempresa.local ALL=(ALL:ALL) ALL
```

Para dar `sudo` a un grupo de AD (recomendado):

```
%grupo_de_ad@miempresa.local ALL=(ALL:ALL) ALL
```

*Nota: El `%` indica que es un grupo. Si el nombre del grupo tiene espacios, usa comillas:

```
"%Grupo con Espacios@miempresa.local".
```

Después de estos pasos, deberías poder ver el "dominio" en la pantalla de inicio de sesión de Ubuntu (GDM) o simplemente iniciar sesión usando el formato `usuario@miempresa.local` con su contraseña de AD.