

## **Resumen sobre Cuentas de Usuario en Windows Server**

Las cuentas de usuario en un dominio de Windows Server son esenciales para gestionar la autenticación, el acceso a los recursos y la auditoría de actividades en la red. Estas cuentas pueden ser de dos tipos: cuentas de dominio, válidas en toda la red, o cuentas locales, específicas de cada máquina.

### **Cuentas Predefinidas en Windows Server:**

- **Administrador:** Tiene todos los derechos y permisos.
- **Invitado:** Tiene derechos limitados.

En redes de Windows, se puede operar en un **Grupo de Trabajo** o en un **Dominio**. En un **Grupo de Trabajo** se gestionan cuentas de usuario y recursos de manera descentralizada, mientras que en un **Dominio**, las cuentas y permisos son gestionados centralmente por un servidor llamado **Controlador de Dominio**.

### **Comparativa: Grupo de Trabajo vs. Dominio**

- **Grupo de Trabajo:** Mejor para redes pequeñas y con menos seguridad. Cada computadora administra su propia base de datos de usuarios.
- **Dominio:** Más seguro, ideal para redes grandes, centraliza la administración mediante **Active Directory** y permite una gestión eficiente de usuarios, contraseñas y permisos.

## **Denominación de Cuentas en Active Directory**

Las cuentas de usuario en un dominio se identifican con un nombre principal de seguridad (principal name), como `usuario@dominio.com`.

### **Opciones de Cuentas**

Al crear una cuenta, se pueden establecer restricciones como:

- **Horas de inicio de sesión:** Restringir los accesos a ciertas horas del día.
- **Iniciar sesión en:** Limitar el acceso a ciertas máquinas.
- **Caducidad de la cuenta:** Establecer fechas de expiración.

### **Contraseñas**

Las contraseñas deben ser seguras, y Windows Server impone requisitos de complejidad. Se recomienda cambiar las contraseñas regularmente y usar contraseñas difíciles de adivinar, pero fáciles de recordar para los usuarios. Tiene una longitud de al menos seis caracteres.

## **¿Qué es un Sistema Operativo en Red?**

Son aquellos sistemas que mantienen a dos o más equipos unidos a través de algún medio de comunicación (físico o no)

## Estructura Cliente-Servidor:

**Servidor:** Es un pc que comparte todos los recursos, con el resto de PC, conectados a él.

**Clientes:** Son los diferentes PC que se conectan para utilizar los recursos.

**Árbol:** Es un conjunto de dominios, los cuales dependen de una raíz común y están organizados en una determinada jerarquía, también llamada DNS común. Esta estructura permite identificar unos dominios de otros.

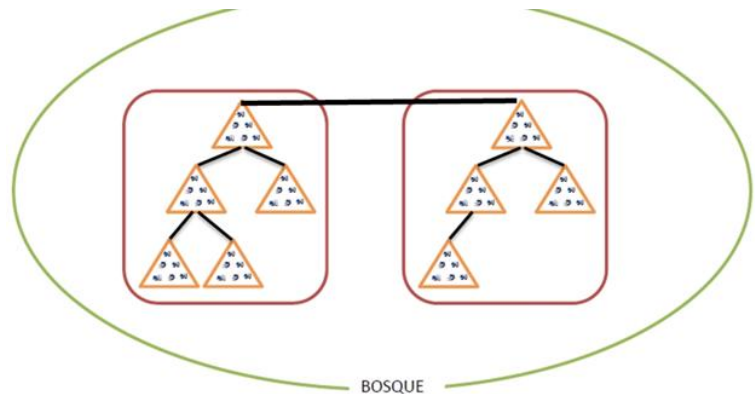
**Bosque:** Un bosque es la suma de todos los dominios existentes contenidos en él.

Árbol: Cada sección de la biblioteca (ciencia, historia, literatura) sería un dominio dentro de un árbol. Todos los libros en esa sección comparten un tema común.

Bosque: La biblioteca completa sería un bosque.

Diferentes secciones (árboles) pueden tener temas muy

diferentes, pero todos los libros están bajo el mismo techo (la biblioteca).



- No se pueden mover dominios de Active Directory entre bosques.
- Sólo se puede eliminar un dominio de un bosque si este no tiene dominios hijo.
- Después de haber creado el dominio raíz de un árbol, no se pueden añadir al bosque dominios con un nombre de dominio de nivel superior.
- No se puede crear un dominio padre de un dominio existente.

## Creación de Cuentas de Usuario

Para crear cuentas de usuario en Active Directory:

1. **Abrir Usuarios y Equipos de Active Directory.**
2. Crear el usuario en el contenedor adecuado (OU).
3. Definir el nombre de usuario, contraseña, y otras opciones (como la caducidad de la contraseña).

## **Administración de Cuentas de Usuario**

El proceso de gestión de cuentas incluye tareas como:

- **Copiar:** Crear nuevas cuentas con configuraciones similares.
- **Agregar miembros a un grupo:** Organizar usuarios en grupos.
- **Deshabilitar o habilitar cuentas:** Administrar cuentas temporalmente inactivas.
- **Restablecer contraseñas:** Cambiar contraseñas olvidadas.
- **Mover cuentas:** Reubicar usuarios entre diferentes unidades organizativas.
- **Eliminar:** Eliminar cuentas de usuario (recomendable deshabilitar antes de eliminar).
- **Cambiar nombre:** Modificar el nombre del usuario, sin alterar el SID (identificador de seguridad).

La administración eficaz de las cuentas de usuario en un dominio facilita el control y la seguridad en grandes redes corporativas.

## **Resumen de Propiedades y Administración de Cuentas de Usuario del Dominio**

### **Propiedades de las Cuentas de Usuario del Dominio:**

#### **Pestaña General:**

- **Nombre:** Nombre completo del usuario.
- **Iniciales:** Iniciales del usuario.
- **Apellidos:** Apellidos del usuario.
- **Nombre para mostrar:** Nombre descriptivo utilizado en aplicaciones.
- **Descripción:** Breve descripción del usuario.
- **Oficina y Número de teléfono:** Información de contacto y ubicación.
- **Correo electrónico:** Dirección de correo del usuario.
- **Página Web:** Dirección URL de la página del usuario.

#### **Pestaña Dirección:**

- **Dirección física:** Domicilio del usuario.

#### **Pestaña Cuenta:**

- **Nombre de inicio de sesión:** Identificador único del usuario en la red.
- **Restricciones de inicio de sesión:** Definir cuándo y dónde puede iniciar sesión el usuario.
- **Caducidad de cuenta y contraseña:** Opciones para caducar cuentas y contraseñas.
- **Desbloquear cuenta:** Reestablecer el acceso si la cuenta fue bloqueada por intentos incorrectos.
- **Cuenta deshabilitada:** Desactivar la cuenta temporalmente.

#### **Pestaña Perfil:**

- **Ruta de acceso al perfil:** Especifica dónde se almacenan los archivos y configuraciones del usuario.
- **Archivos de comandos de inicio de sesión:** Configura scripts que se ejecutan al iniciar sesión.
- **Directorio principal:** Ruta al directorio del usuario, puede ser local o de red.

#### **Pestaña Teléfonos:**

- Números de teléfono adicionales (móvil, localizador, etc.).

#### **Pestaña Organización:**

- Información sobre la organización del usuario, como título, departamento y supervisores.

#### **Pestaña Miembro de:**

- Grupos a los que pertenece el usuario.

#### **Pestañas Adicionales:**

- Entorno, Sesiones, Control remoto, y Servicios de Terminal Server, que configuran el acceso remoto y otros perfiles específicos.

#### **Creación de Unidades Organizativas (OU):**

1. Se expande el nodo del dominio y se selecciona "Nuevo" → "Unidad Organizativa".
2. Asignar nombre a la OU (ej. "gente") y confirmar con "OK".
3. Se pueden agregar OUs como "clientes", "grupos", "administradores", y "servidores".
4. Descripción y detalles adicionales pueden agregarse en las propiedades de cada OU.

En este sentido, es importante conocer que en el Directorio Activo existen contenedores que no son en realidad unidades organizativas (por ejemplo, "Users" o "Computers"), y que en estos contenedores no es posible definir directivas.

Sin embargo, un objeto no puede copiarse, ya que su nombre distinguido es su clave primaria en la base de datos del directorio (debe ser único).

#### **Proceso de Creación de Usuarios:**

1. **Iniciar el proceso:** Hacer clic derecho en "Nuevo" → "Usuario".

2. **Rellenar la información:** En el cuadro de diálogo "Nuevo Objeto – Usuario", introducir datos como nombre, apellidos, y nombre de usuario.
3. **Contraseña:** Al pulsar "Siguiente", se solicita ingresar la contraseña del usuario y activar la casilla "El usuario debe cambiar la contraseña al siguiente inicio de sesión".
4. **Configuración adicional:** Una vez creado el usuario, se puede acceder a sus propiedades con clic derecho → "Propiedades" para modificar otras configuraciones.

## Modificación de Directivas de Seguridad:

- **Política de contraseñas:** Windows Server requiere contraseñas complejas y con características específicas. Para permitir la creación de usuarios sin contraseña, se debe modificar la **Directiva de Contraseña:**
  1. Acceder a "Herramientas administrativas" → "Administración de directivas de grupo".
  2. Editar la política "Default Domain Policy" y deshabilitar la opción "Las contraseñas deben cumplir los requisitos de complejidad".
  3. Configurar las políticas de **historial de contraseñas, longitud mínima, vigencia máxima y vigencia mínima** a 0.
  4. Recargar las políticas para aplicar los cambios.

Esto permite crear usuarios sin contraseña, útil en casos específicos como alumnos de infantil, pero no es necesario en todos los casos.

## Creación de un Nuevo Usuario:

1. **Acceder a Active Directory:** Abrir "Usuarios y equipos de Active Directory".
2. **Nuevo usuario:** Clic derecho en "Usuarios" → "Nuevo" → "Usuario", luego rellenar los datos del usuario.
3. **Contraseña:** Asignar una contraseña, activar "La contraseña nunca caduca" y desactivar "El usuario debe cambiar la contraseña al iniciar sesión".
4. **Finalizar:** Hacer clic en "Finalizar" para crear el usuario.

## Ejemplo de Usuarios Creación:

- Crear usuarios como "1ESOA01", "1ESOA02", "2ESOD07", "3ESOC14" con contraseñas que cumplen los requisitos de seguridad, como **Micentro2012** o **Micentro2009**.

Una vez completado el proceso, los nuevos usuarios se mostrarán en la carpeta "Users" de Active Directory.

## Unión de un equipo Windows 10 a un controlador de dominio

Este procedimiento detalla los pasos para conectar una máquina con **Windows 10** a un **controlador de dominio de Windows Server**:

## 1. Requisitos previos

Antes de comenzar el proceso de unión de un equipo Windows 10 a un dominio, se deben cumplir ciertos requisitos básicos:

- **Controlador de dominio:** Debes tener un servidor **Windows Server 2012, 2016 o 2022** configurado como **controlador de dominio**. Este servidor debe de disponer un **de Active Directory** que gestionará las credenciales y políticas de seguridad de todos los dispositivos que se unan al dominio.
- **Máquina con Windows 10:** Se debe contar con un dispositivo que tenga instalado **Windows 10** (puede ser físico o virtual). Esta será la máquina que se unirá al dominio. Ambos deben de estar en la misma red en VirtualBox.

## 2. Verificación de comunicación entre las máquinas

Una vez que ambos equipos están configurados, realizaremos un ping para verificar que tienen conexión entre ellos y que pueden conectarse a través de la red.

```
ping <IP_DEL_SERVIDOR>
```

## 3. Configuración de red en el equipo Windows 10

Importante que el **Windows 10** esté correctamente configurado para reconocer el servidor como su servidor DNS, ya que el **Active Directory** se gestiona a través del DNS.

- **Windows Server** debe tener una **dirección IP estática**, ya que actúa como el servidor DNS principal.
- En **Windows 10**, la configuración **DNS** debe apuntar a la IP del servidor de dominio (Windows Server). Esto garantizará que todas las solicitudes de resolución de nombres en la red apunten al servidor del dominio.
  - Accede a las **Propiedades del adaptador de red**.
  - En **Protocolo de Internet versión 4 (TCP/IPv4)**, configura el **DNS preferido** con la dirección IP del servidor de dominio y asegúrate que estén en la misma subred.

## 4. Creación de un usuario en el servidor de dominio

En el servidor con **Windows Server**, antes de unir el equipo, debes asegurarte de que haya un usuario creado en **Active Directory** que tenga privilegios para agregar equipos al dominio.

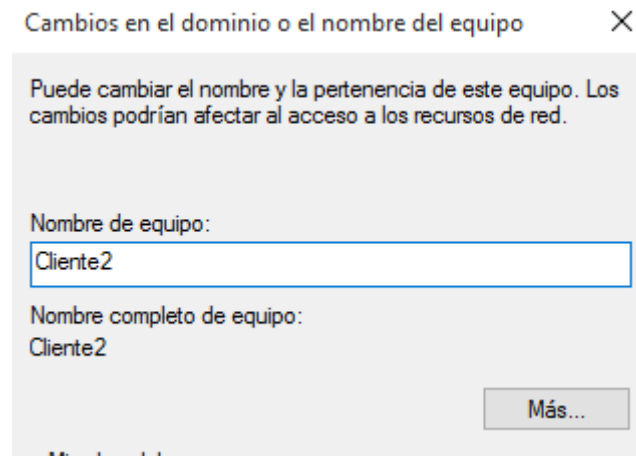
- Abre la herramienta **Usuarios y equipos de Active Directory** en el servidor.
- Crea un **nuevo usuario de dominio** si aún no tienes uno adecuado.
  - Este usuario debe tener privilegios administrativos en el dominio o pertenecer al grupo **Administradores de dominio** para poder agregar dispositivos a la red.

## 5. Unir el equipo Windows 10 al dominio

Ahora, en la máquina **Windows 10**, sigue estos pasos para agregar el equipo al dominio:

- **En propiedades del sistema, Cambiar** en la sección **Nombre de equipo, dominio y grupo de trabajo del equipo**.

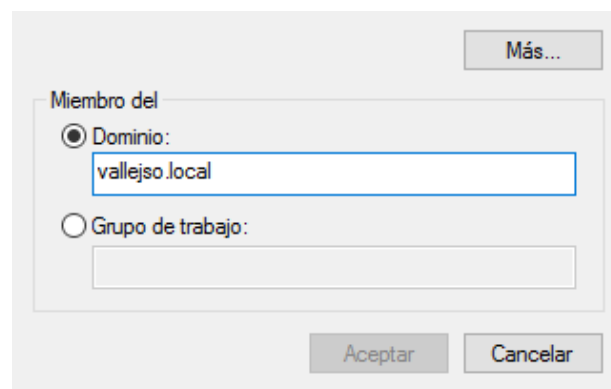
1. **Cambiamos el nombre del equipo:**



reiniciamos la maquina

2. **Unirse al dominio:**

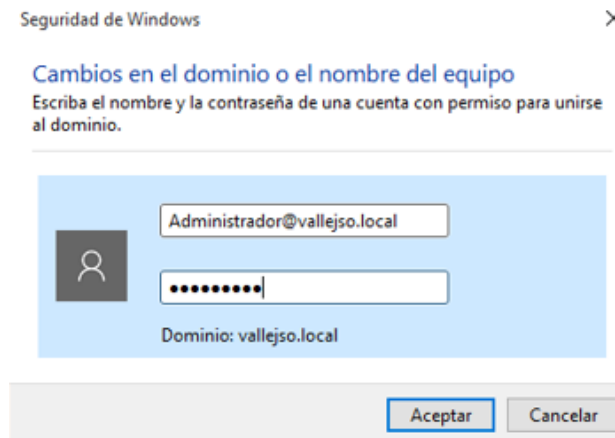
- En la ventana **Propiedades del sistema**, selecciona **Miembro de dominio** e ingresa el nombre del dominio.



Previamente desactivamos el firewall.

3. **Autenticación en el dominio:**

- Indica un usuario que pertenezca al grupo **Administradores de dominio**.



## 6. Confirmación de unión al dominio

La ventana mostrará algo como "Se unió correctamente al dominio".

## 7. Inicio de sesión en el dominio

Después de reiniciar el equipo:

1. **Pantalla de inicio de sesión:**
  - Presiona **Ctrl + Alt + Supr** para llegar a la pantalla de inicio de sesión.
  - Haz clic en **Cambiar de usuario** y luego en **Otro usuario**.
2. **Iniciar sesión con una cuenta de dominio:**
  - Introduce el nombre de usuario en el formato **usuario@dominio**, por ejemplo, **alonso@ajpdsoft**.
  - Ingresa la **contraseña** del usuario de **Active Directory** que has creado en el servidor.

Nota: Recuerda que las credenciales del usuario son gestionadas por el servidor de dominio, no por el equipo local. Esto significa que el equipo local no almacenará la contraseña; en su lugar, validará el inicio de sesión a través del controlador de dominio.

## 8. Verificación en el servidor de dominio

Para confirmar que el equipo se ha unido correctamente al dominio, puedes verificar la existencia del equipo en **Active Directory**:

- Abre la herramienta **Usuarios y equipos de Active Directory**.
- En el panel izquierdo, selecciona **Computadoras**. Aquí deberías ver el equipo con el nombre que le hayas asignado al equipo con **Windows 10**.



Resumen:

- 1.Red Interna
- 2.Misma subred
3. Desactivar el firewall
- 4.Cambiar el nombre (reiniciar)
5. Hacer ping
- 6.Unir al dominio

¿Qué pasa si no va?

Volver a revisar lo anterior o:

- 1.Comprobar el SID (sysprep) o la MAC.

## Introducción a DSADD

La principal de **DSADD** es permitir la creación de objetos en el directorio de AD, lo que es esencial para la gestión de usuarios, grupos, equipos y otras entidades dentro de la infraestructura de TI. **DSADD** se puede utilizar para automatizar la creación de objetos, lo que es muy útil cuando se manejan grandes cantidades de datos o usuarios, como en un entorno educativo o empresarial.

## Comandos Principales de DSADD

- **dsadd user:** Añade un único usuario en el directorio.
- **dsadd group:** Añade un único grupo en el directorio.
- **dsadd ou:** Agrega una unidad organizativa (OU) al directorio.
- **dsadd computer:** Añade un único equipo en el directorio.
- **dsadd quota:** Añade una especificación de cuota a una partición de directorio.

Los comandos de **DSADD** permiten la gestión directa desde la línea de comandos, facilitando tareas como la creación masiva de usuarios o la organización de los objetos dentro de AD.

## Sintaxis del Comando DSADD

Para utilizar **dsadd**, se debe ejecutar el comando desde un símbolo del sistema elevado (con privilegios de administrador). La sintaxis básica es:

```
dsadd <tipo de objeto> <nombre distintivo>
```

Donde:

- **<tipo de objeto>:** Puede ser **user**, **group**, **ou**, **computer**, etc.

- **<nombre distintivo (DN):** Especifica la ubicación del objeto dentro de AD, utilizando la nomenclatura **Distinguished Name (DN)**, que incluye el nombre de la unidad organizativa (OU) y el dominio.

## Ejemplos de Uso de DSADD

### 1. Crear una Unidad Organizativa (OU)

Para crear una nueva unidad organizativa en el directorio, se utiliza el siguiente comando:

```
dsadd ou "ou=Aulas,dc=ana,dc=local"
```

Este comando crea una OU llamada "Aulas" en el dominio **ana.local**.

### 2. Crear un Usuario

Para agregar un nuevo usuario llamado "Laura" en la unidad organizativa "Segundo", el comando sería:

```
dsadd user "cn=Laura,ou=Aulas,ou=Segundo,dc=ana,dc=local"
```

Este comando crea el usuario **Laura** dentro de la estructura de unidades organizativas **Aulas** y **Segundo**.

### 3. Habilitar una Cuenta de Usuario

Por defecto, las cuentas de usuario creadas con **dsadd** están deshabilitadas. Para habilitar la cuenta y asignar una contraseña, se puede agregar el parámetro **-pwd** seguido de la contraseña:

```
dsadd user "cn=Laura,ou=Aulas,ou=Segundo,dc=ana,dc=local" -pwd P@ssword
```

Este comando habilita la cuenta y asigna la contraseña **P@ssword** a la cuenta de **Laura**.

## Automatización de la Creación de Usuarios con Archivos por Lotes

En situaciones donde se necesite crear múltiples usuarios de forma automatizada, **DSADD** puede integrarse en scripts o archivos por lotes. Esto es útil cuando hay que crear cuentas de usuarios para un gran número de empleados o estudiantes.

Para ello, podemos crear un archivo de texto con los nombres y contraseñas de los usuarios y usar un script de **batch** (por ejemplo, un archivo .cmd o .bat) para procesar esta información y crear las cuentas automáticamente.

### Ejemplo de Script en Batch

### Alumnos.txt:

```
Carlos;Alcazar;alcazar.carlos;P@ssword1
Miguel;Bautista;bautista.miguel;P@ssword2
Juan Carlos;Bohoyo;bohoyo.jcarlos;P@ssword3
```

### Alta-Alumnos.cmd:

```
FOR /F "tokens=1,2,3,4 delims=;" %%A IN (alumnos.txt) DO (
    dsadd user "cn=%%A %%B,ou=alumnos,dc=inclan,dc=local" -pwd %%D
)
```

For /L?

Este script leerá el archivo **alumnos.txt**, que contiene los datos de los usuarios, y ejecutará el comando **dsadd** para crear cada cuenta de usuario con su correspondiente contraseña.

## Otras Herramientas de Administración de AD

Además de **DSADD**, existen otros comandos útiles para la gestión de objetos en Active Directory:

- **DSRM** (Remove): Elimina objetos en el directorio.

```
dsrm "cn=Laura,ou=Aulas,ou=Segundo,dc=ana,dc=local"
```

- **DSMOD** (Modify): Modifica atributos de los objetos existentes.

```
dsmod user "cn=Laura,ou=Aulas,ou=Segundo,dc=ana,dc=local" -pwd
"NuevaContraseña"
```

- **DSMOVE** (Move): Mueve objetos dentro de AD.

```
dsmove "cn=Laura,ou=Aulas,ou=Segundo,dc=ana,dc=local"
"ou=Profesores,dc=ana,dc=local"
```

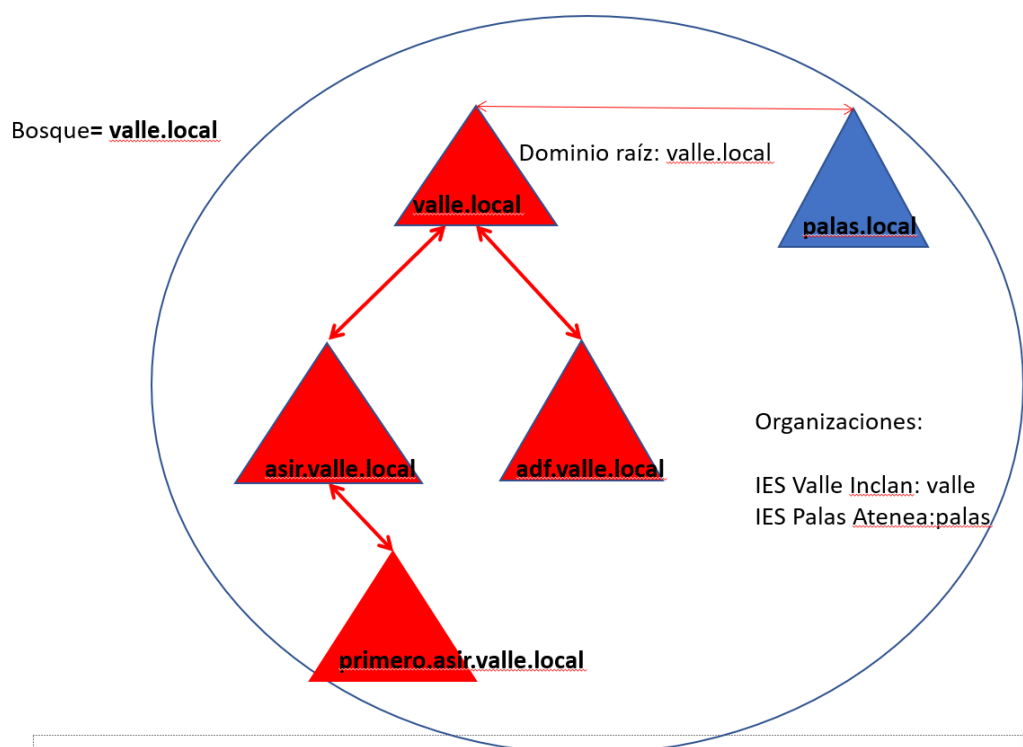
- **DSQUERY** (Query): Realiza consultas para buscar objetos en AD.

```
dsquery user -name "Laura*"
```

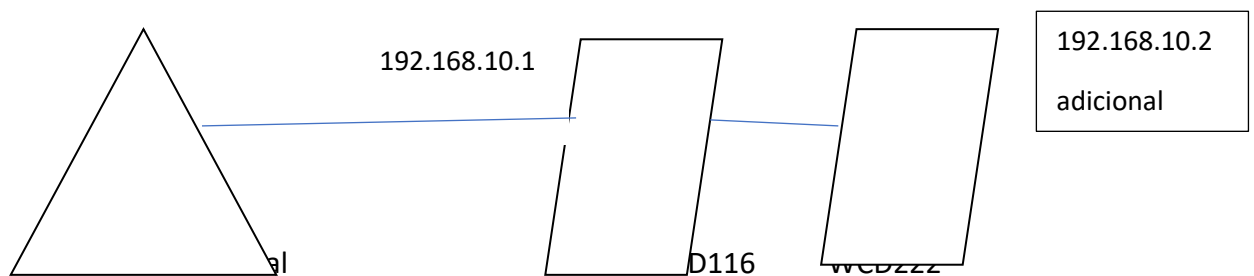
- **DSGET** (Get): Obtiene atributos de objetos en AD.

```
dsget user "cn=Laura,ou=Aulas,ou=Segundo,dc=ana,dc=local"
```

Pipeline (busca un objeto y añádelo a un grupo).



**PRACTICAS    Añadir controlador de dominio adicional(7).**



1. Creamos un clon de Windows 2022 con las gest-aditions instaladas.
2. Para que veáis que podemos integrar controladores de dominio distintos uno con 2016 y otro con 2022 siempre que el nivel funcional del bosque y del dominio nos lo permitan.

### 3. Arrancamos y le llamamos 2022- CD222

1. Red → red interna
2. Cambiar nombre del equipo
3. Dirección IP fija y en la misma subred que el Controlador de dominio principal.
4. Servidor DNS preferido ponemos la IP del controlador de dominio principal CD1.
5. Desactivar el Firewall en las dos máquinas.
6. primero miramos si hay conexión física entre estas dos máquinas. Con ping ip, en los dos sentidos y si todo esta correcto continuamos, si nos da algún problema paramos y resolvemos los problemas. Siempre tiene que responder el ping.
7. No es necesario que sea un miembro del dominio para convertirlo en un C.D pero si lo hacemos ya nos aseguramos que tenemos conectividad lógica con el dominio.  
Administrador @valle.local  
En dominio  
Vallexxx.local → se unió correctamente al dominio
8. Tenemos que tener el controlador de dominio principal CD1 corriendo.

### 4. Arrancamos la máquina CD222

- Agregar Roles → Instalar servicio de dominio del Active Directory
- Ejecutamos dcpromo, que a partir de 2012 en adelante es ejecutar la

#### Banderita.

- a) Bosque Existente
- b) Agregar un C.D a un dominio existente  
Nombre de dominio= vallexxx.local  
Establecer credenciales alternativas → con administrador @vallexxx.local.
- c) Seleccione un dominio para este controlador de dominio vallexxx.local
- d) En que sitio vas a ubicar este controlador. El nombre del sitio (site) suele ser igual o parecido al edificio físico donde se encuentra o la zona física.

## **ANTES DE CONTINUAR VAMOS A CAMBIAR EL NOMBRE DEL SITE QUE TENEMOS ACTUALMENTE EN DC1**

Nos vamos a CD1 y nos vamos a Herramientas → sitios y servicios del Active Directory.

Ahora nosotros aquí tenemos un site que se crea por defecto, y cuyo nombre se le da al instalar el CD1, y tenemos un solo site con un solo servidor CD1 y tiene un nombre predeterminado

Nombre → Default-First-Site-Name y aquí le cambiamos el nombre a site Madrid-risa.

Nos posicionamos encima del site y botón derecho, y modificamos el nombre.

Ahora nos regresamos al CD2

- e) Damos marcha atrás.
- f) Después continuamos y veremos que ya nos aparece el nombre de site que nosotros hemos modificado antes.
- g) Mejor poner otro servidor DNS (un 2 DNS en el mismo dominio) para que este Controlador de dominio también tenga su propio DNS.

Es mejor que tenga un segundo servidor DNS y van a replicar los datos entre los dos DNS cada 15 minutos, los cambios que tengan y de esa manera en cualquier momento podemos apagar un equipo y lo lógico es que los clientes tuvieran como serdir DNS principal al CD1 y como servidor DNS secundario del CD2.

- h) Catalogo Global—Si
- i) Como replican los datos del dominio a este equipo, a través de la red, desde un C.D.  
Replicar los datos a través de la red
- j) Cogemos un servidor que este en la red en nuestro site.
- k) Contraseña en modo restauración servicio directorio. Esto es para cuando se tiene problemas con los servicios de directorio si nos da error ... Reiniciamos y al reiniciar F8 Modo seguro y modo restauración de los servicios de Directorio.

### **5. Reiniciamos la máquina CD222.**

6. Cuando arranque CD2, miramos la configuración Ip de la máquina.

A pesar de que nosotros le hemos dicho que tenga un DNS propio, en la configuración de este CD2 nos aparece

Servidor DNS preferido la IP del DC1, pero hay que modificarlo aunque 2016 hay veces que lo hace automáticamente y dejarlo:

DNS preferido: 127.0.0.1 o su IP

DNS alternativo en blanco.

**Ahora nosotros tenemos un dominio con dos controladores de dominio** distintos y con 2 DNS. Esto lo podemos aprovechar a la hora de instalar los clientes... De tal forma que si en un momento dado uno no está disponible automáticamente los clientes puedan utilizar el otro, y así también podemos balancear la carga.

Si tenemos 2 C.D con DNS propio si estamos trabajando ejemplo en un instituto donde tenemos 12 clases, pues entonces repartimos un poco la carga, a la vez que nos aseguramos que los clientes tengan siempre conectividad física.

Los clientes correspondientes a 6 clases en su configuración IP tendrían puesto:

DNS preferido DC1

DNS secundario DC2

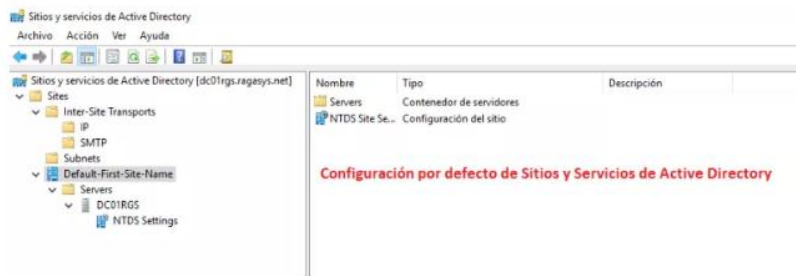
Los clientes de las otras 6 clases restantes en su configuración IP tendrían lo contrario:

DNS preferido DC2

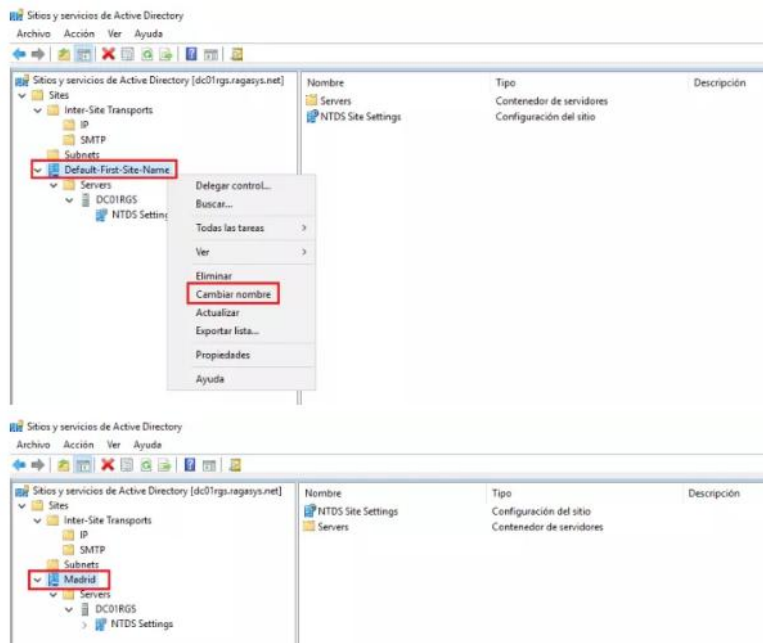
DNS secundario DC1

Normalmente un equipo siempre utiliza el DNS preferido, da igual que en un momento le hagamos una consulta que no sepa resolver, sino conoce la respuesta no va a ir a preguntarle al DNS secundario sino que va a ir a preguntar a los nodos superiores (o desinencias raíz) no al secundario. **El DNS secundario solo se utiliza si el primario no funciona por la causa que fuera.**

7. Ahora ya nos vamos al DC1 y nos vamos a usuarios y equipos del Active Directory. En la parte de Domains Controllers ya tiene que aparecer el DC2 como segundo controlador de dominio
8. Ahora vamos a ver el DNS del DC2 tienen que tener sus zonas y en el DC1 también.  
DC2 Aquí botón derecho propiedades en la pestaña Reenviadores, tengo como reenviador la IP del DC1, significa que este cuando no sepa resolver un registro porque no pertenezca al dominio valle, local, este le pasa el marrón al DC1 para que DC1 resuelva, si lo conoce lo resuelve y le da la respuesta, pero sino lo conoce como en su caso DC1 no tiene ningún reenviador, lo que hace es utilizar la sugerencia RAIZ, que son servidores DNS de Internet y le pasaría el marrón a ellos.  
Ipconfig /flushdns---→ borra la cache de resolución DNS.
9. Mirar sitios y servicios del Active Directory.



- La primera configuración que vamos a realizar será renombrar el "Default-First-Site-Name" como "Madrid", ya que nuestro controlador de dominio principal está ubicado geográficamente en las oficinas de Madrid, así tendremos nuestro primer Site listo para asignarle las subredes correspondientes:



**10. Objetos NTDS Setting.** Lo que ocurre en los controladores de dominio tenemos unos objetos donde se configura la replicación de datos = NTDS Setting del DC1. Este objeto lo que dice es que este controlador de dominio va a replicar los datos desde el servidor DC2, y en el DC2 tendremos su análogo, otro objeto similar que nos dice que la replicación de datos se hace desde el DC1. De esta manera podemos configurar como se va a hacer la replicación de datos entre los distintos controladores de los distintos dominios y de los distintos sites para ir haciendo caminos que permitan que toda la información esté en todos los sites.

Normalmente en un site todos los controladores de dominio replican con todos los controladores de dominio replican con todos y además cada cierto tiempo definido.

- Ningún controlador de dominio es el maestro.
- Todos los C.D. son iguales y contienen una copia de la B.D., del directorio
- Los controladores de dominio replican los cambios entre ellos.



- Cualquier controlador de dominio puede procesar los cambios del directorio y replicarlos.
- Los controladores de dominio replican inmediatamente ciertas actualizaciones urgentes, por ejemplo la eliminación de una cuenta de usuario.
- Establecer varios controladores de dominio dentro de un dominio permite tolerancia a fallos
- Todos tienen asignada las mismas tareas salvo: Servidor de cabeza de puente, y la función del maestro de operaciones.

Botón derecho propiedades y cambiar programación aquí se le dice cada cuanto tiempo va a replicar y puede replicar hasta 4 veces en una hora, según necesidades.

También desde aquí podemos replicar ahora en el momento concreto que queramos.

NTDS site -> Botón derecho y replicar ahora directamente en este momento.

Ipconfig /flushdns---> borramos la cache de resolución DNS, y así si hacemos un ping, forzamos siempre a la búsqueda contra el servidor DNS.

## 11. CREAR OBJETOS EN EL DOMINIO

- Crear objetos en el DC1 mediante la herramienta gráfica.  
Cada controlador de dominio tiene un rango de SID y utiliza su rango y de esa manera sus identificadores son únicos en el dominio.  
¿Qué hacer para que el SID nos aparezca, en las propiedades del usuario?  
Ver->Características avanzadas,  
Para que nos muestre la ficha de Editor de atributos, en propiedades, aquí buscamos el objeto SID object sid.  
Quien se encarga de gestionar los rangos de los SID, -> el maestro de RID

Cuando se agrega un nuevo controlador al dominio, se podrá en contacto con el RID para asignarle un nuevo rango, cada controlador de dominio tiene un rango de SID y así los identificadores son únicos en el dominio.

## RESUMEN: MAESTROS DE OPERACIONES (FSMO)

En los sistemas **Windows Server**, los roles FSMO (Flexible Single Master Operations) son funciones críticas asignadas a controladores de dominio (DC) específicos para

garantizar que ciertas operaciones sean únicas y evitar conflictos de replicación en Active Directory.

## 1. ¿Qué son los roles FSMO?

- **FSMO (Flexible Single Master Operations):** Permiten tareas críticas que no son prácticas con múltiples maestros.
- **Replicación de Maestro Único:** Designa un DC único para realizar ciertos cambios, evitando conflictos de replicación.

## 2. Tipos de roles FSMO

Se dividen en:

- **Roles que abarcan todo el bosque (2):**
  - Maestro de Esquema.
  - Maestro de Nombres de Dominio.
- **Roles que abarcan todo el dominio (3):**
  - Emulador de PDC.
  - Maestro RID.
  - Maestro de Infraestructura.

### Roles que abarcan todo el bosque (únicos por bosque):

1. **Maestro de Esquema:**
  - Controla actualizaciones al esquema de Active Directory (definiciones de objetos y atributos).
  - Útil para cambios globales como añadir un nuevo tipo de objeto.
  - **Comando para consultar:**  
`dsquery server -hasfsmo schema`
2. **Maestro de Nombres de Dominio:**
  - Controla la adición o eliminación de dominios en el bosque.
  - Imprescindible para modificaciones estructurales en Active Directory.
  - **Comando para consultar:**  
`dsquery server -hasfsmo name`

### Roles que abarcan todo el dominio (únicos por dominio):

1. **Emulador de PDC:**
  - Simula el comportamiento de un controlador principal de dominio en entornos antiguos.
  - Procesa solicitudes de sincronización de hora y actualizaciones de contraseñas.
  - **Comando para consultar:**  
`dsquery server -hasfsmo pdc`

## 2. Maestro RID:

- Asigna rangos de identificadores relativos (RID) para crear SIDs únicos para cuentas y grupos.
- Evita que se repitan identificadores en el dominio.
- **Comando para consultar:**  
`dsquery server -hasfsmo rid`

## 3. Maestro de Infraestructura:

- Actualiza referencias cruzadas entre objetos cuando se mueven entre dominios.
- Esencial en entornos con múltiples dominios.
- **Comando para consultar:**  
`dsquery server -hasfsmo infr`

## Administración de roles FSMO:

### 1. Comandos para ver roles FSMO:

- Ver roles en el bosque y dominio:  
`netdom query fsmo`
- Para dominios específicos:  
`netdom query /domain:<nombre_dominio> fsmo`

### 2. Transferir roles FSMO:

- **Roles del bosque:**
  - **Cambiar Maestro de Esquema:**  
Usa la consola **Esquema de Active Directory**.  
Comando previo para habilitarla:  
`regsvr32 schmmgmt.dll`
  - **Cambiar Maestro de Nombres de Dominio:**  
Usa la consola **Dominios y Confianzas de Active Directory**.
- **Roles del dominio:**
  - **Cambiar Emulador de PDC, Maestro RID y Maestro de Infraestructura:**  
Usa la consola **Usuarios y Equipos de Active Directory**.  
Haz clic derecho sobre el dominio > "Maestro de Operaciones".

## NTDSUTIL

Herramienta de línea de comandos que proporciona facilidades de administración para los servicios de dominio de Active Directory (AD). Puede utilizar los comandos ntdsutil para realizar el mantenimiento de la base de datos del AD.

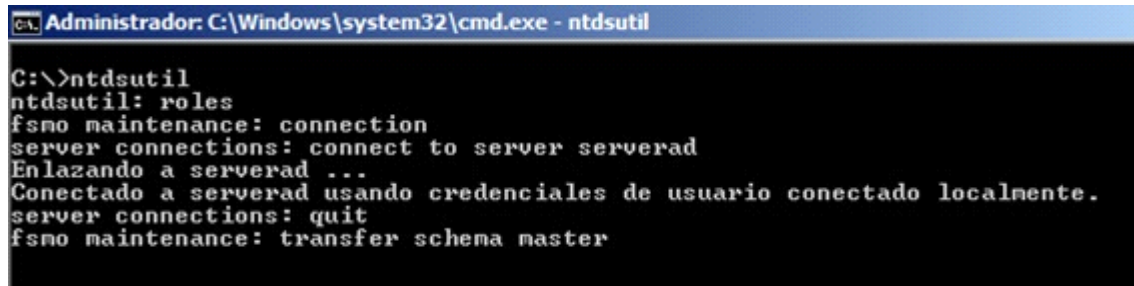
Son unos pasos muy sencillos a seguir y que nos facilitara cambiar nuestro maestro de esquema a un nuevo Domain Controller.

Nota: Tenemos que realizar los siguientes pasos desde el servidor que queramos que sea maestro de esquema.

- Abrimos la ventana de comandos
- Escribimos: `ntdsutil`
- En el símbolo del sistema de ntdsutil, escribimos: `roles`
- En el símbolo del sistema de fsmo maintenance, escribimos: `connection`

- En el símbolo del sistema de server connections, escribimos: **connect to server** "nombre del **controladorDeDominio**"

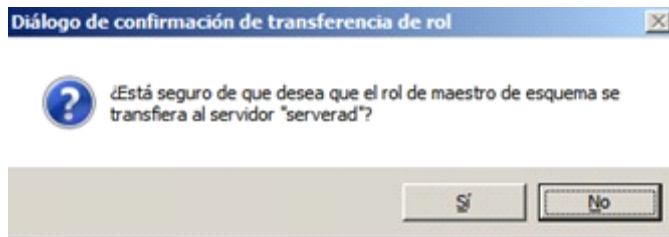
1) Transferimos el maestro de esquemas



```

C:\>ntdsutil
ntdsutil: roles
fsmo maintenance: connection
server connections: connect to server serverad
Enlazando a serverad ...
Conectado a serverad usando credenciales de usuario conectado localmente.
server connections: quit
fsmo maintenance: transfer schema master
  
```

- Confirmamos el mensaje que nos sale.



- Transferir el maestro de Nombres de dominio. : **transfer naming master**
- Transferir el maestro de Infraestructuras: **transfer infrastructure master**
- Transferir el Emulador de PDC: **transfer PDC**
- Transferir el Maestro de RID: **transfer RID master**

## Tipos de perfiles de usuario

### 1. Perfiles locales:

- **Características:**
  - Se almacenan en el disco duro donde el usuario inicia sesión.
  - Solo accesibles desde la máquina donde fueron creados.
  - Se crea la primera vez que el usuario inicia sesión en un equipo.
- **Configuración:** Opción predeterminada en dominios si no se especifica otro tipo de perfil.
- 

### 2. Perfiles temporales:

- **Características:**
  - Se crean si hay un error al cargar el perfil de usuario.
  - No guardan configuraciones ni documentos.
  - Se eliminan al cerrar la sesión.
- **Uso común:** Diagnósticos o usuarios con permisos muy limitados.

### 3. Perfiles móviles:

- **Características:**
  - Se almacenan en una carpeta de red (habitualmente compartida en el controlador de dominio).
  - El usuario puede acceder a su perfil desde cualquier equipo del dominio.
  - Durante la sesión, el perfil móvil se copia localmente para evitar sobrecarga en la red.
  - Al cerrar sesión, el perfil actualizado se sincroniza de nuevo con el servidor.
- **Problemas posibles:**
  - Si el servidor no está disponible al cerrar sesión, pueden generarse conflictos entre el perfil local y el móvil.
  - Combinación automática de archivos y configuraciones al iniciar sesión (puede causar comportamientos "extraños").
- **Configuración:**
  - Crear una carpeta compartida en el servidor (p. ej.: \\servidor\perfiles).
  - Configurar permisos adecuados.
  - Usar la variable %username% para crear carpetas personalizadas por usuario.

### 4. Perfiles obligatorios:

- **Características:**
  - Basados en perfiles móviles, pero los usuarios no pueden realizar cambios permanentes.
  - Al cerrar sesión, el perfil siempre vuelve al estado inicial (sin cambios).
  - Ideal para bibliotecas, cibercafés o entornos controlados.
- **Configuración:**
  - Renombrar el archivo NTUSER.DAT del perfil a NTUSER.MAN.
  - Requiere tomar posesión administrativa de la carpeta del perfil y ajustar permisos.

## Pasos para crear un perfil móvil:

### 1. Preparación en el servidor:

- Crear una carpeta en el servidor para almacenar los perfiles, p. ej., C:\Perfiles.
- Configurar la carpeta como **compartida**:
  - Nombre de recurso compartido: Perfiles\$ (el símbolo \$ oculta la carpeta en la red).
  - Permisos: Dar **Control Total** al grupo "Usuarios del dominio".
- Asegurar permisos de **seguridad** para que solo el propietario y el sistema tengan acceso.

### 2. Configuración en Active Directory:

- En las propiedades del usuario, ir a la pestaña **Perfil**.
- En la sección "Ruta de acceso al perfil", introducir la ruta compartida, p. ej.:

\\servidor\Perfiles\%username%

<b>Tipo de perfil</b>	<b>Ventajas</b>	<b>Desventajas</b>
<b>Local</b>	Fácil de configurar, sin dependencias de red.	No sincroniza entre equipos, copias de seguridad complicadas.
<b>Temporal</b>	Ideal para diagnósticos o acceso limitado.	No guarda configuraciones ni documentos.
<b>Móvil</b>	Acceso desde cualquier equipo del dominio, sincronización centralizada.	Posibles conflictos, requiere red funcional y configuraciones de permisos adecuadas.
<b>Obligatorio</b>	Estado inmutable, ideal para entornos públicos o compartidos.	Sin personalización, requiere más configuración administrativa.

### 3. Iniciar sesión con el usuario:

- Al iniciar sesión por primera vez, se crea automáticamente la carpeta correspondiente al usuario en la ruta compartida.
- Si no se carga el perfil móvil, eliminar el perfil local desde **Propiedades del sistema > Opciones avanzadas > Perfiles de usuario**.

## Errores comunes y soluciones:

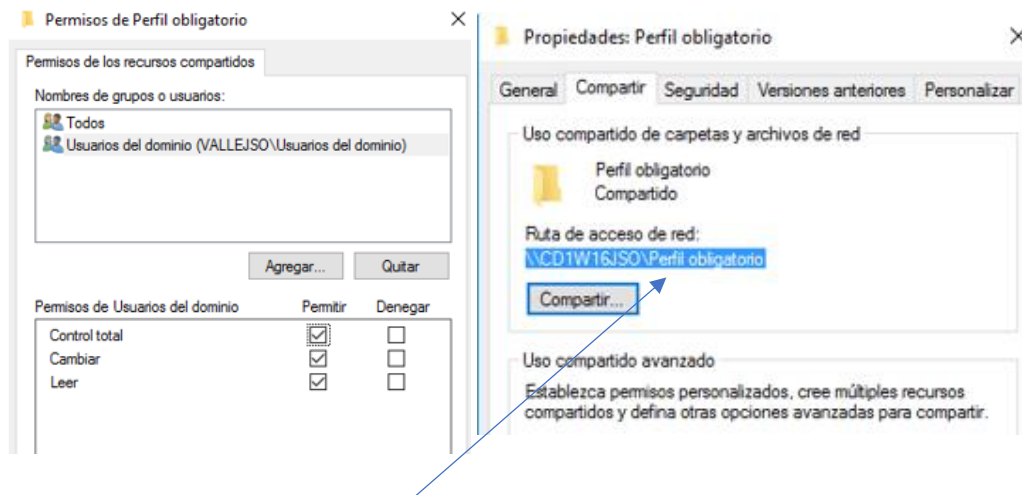
- Error al abrir sesión: "No encuentra el perfil móvil".**
  - **Causa:** La ruta del perfil no existe o el usuario no tiene permisos de acceso.
  - **Solución:** Verificar la ruta y los permisos.
- Error al cerrar sesión: "No puede grabar el perfil".**
  - **Causa:** El usuario no tiene permisos de escritura en la carpeta compartida.
  - **Solución:** Ajustar los permisos en la carpeta del perfil.
- Conflictos entre perfiles local y móvil.**
  - **Causa:** Desconexión del servidor al cerrar sesión.
  - **Solución:** Resolver manualmente los conflictos o limitar los perfiles móviles a usuarios únicos.

## Ventajas y desventajas de cada tipo de perfil

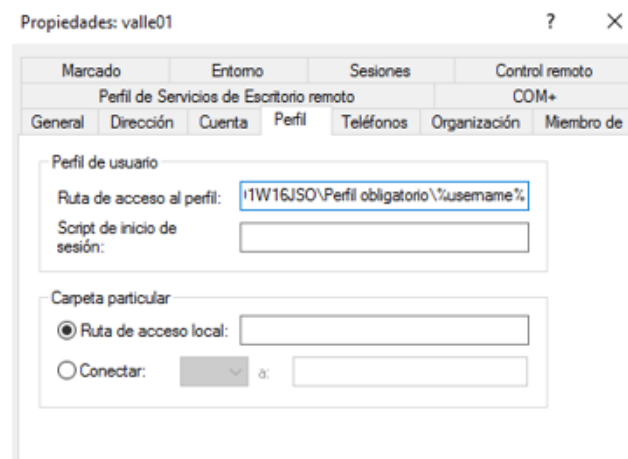
### PASOS PARA CREAR UN PERFIL OBLIGATORIO

Sobre una carpeta de perfil sólo tiene permisos el usuario propietario del perfil.

- 1) Creamos una carpeta que compartiremos con los permisos de compartir y NTFS a Usuarios del dominio con control total.



- 2) Creamos un usuario "Cliente" en una unidad organizativa, y en su perfil añadimos la ruta de acceso de la carpeta en la pestaña "Perfil" y la variable %username%:



- 3) Preparamos el perfil como si fuera a ser un perfil móvil.
- 4) Nos vamos al Windows10, "el cliente conectado al dominio" y nos conectamos con el usuario Cliente. Una vez conectados preparamos el perfil móvil como deseamos, con el fondo de pantalla y una carpeta como queramos. Salimos del sistema windows10.
- 5) Entramos otra vez en Windos10 (nos conectamos otra vez con el usuario Obligatorio) Después nos vamos a \\CD1xxx.  
Seleccionamos el equipo del controlador de dominio CD1. Después buscamos la carpeta que tenemos compartida para los perfiles obligatorios, y dentro tenemos la carpeta Obligatorio.v5. Nos situamos sobre la carpeta botón derecho, propiedades, seguridad, Editar, Agregar y agregamos al usuario Administrador con control total y aceptamos.
- 6) Ahora cerramos sesión en el equipo cliente Windows10.
- 7) Nos vamos al equipo CD1 y modificamos la carpeta poniendo el fichero NTUSER.DAT, lo modificamos como NTUSER.MAN

- 8) Ya tenemos un usuario obligatorio
- 9) Nos conectamos otra vez en el cliente Windows10, "el cliente conectado al dominio" y nos conectamos con el usuario Cliente, y ahora el perfil tiene que ser perfil obligatorio.

En el caso de que no se cambie a perfil obligatorio acceder con otro usuario > borrar el perfil (con permisos de administrador) > y volver a iniciar sesión para que sea oficialmente perfil obligatorio.

## 1. Grupos de Usuarios

Un grupo en Active Directory es una colección de cuentas de usuario, equipos, contactos u otros grupos, que se administra como una única entidad. Su objetivo principal es simplificar la asignación de permisos y derechos.

- **Ventajas:**
  - **Simplificar la administración:** Permisos aplicados al grupo afectan a todos sus miembros.
  - **Delegación:** Se pueden asignar derechos una vez al grupo y agregar o eliminar usuarios según sea necesario.
  - **Listas de distribución:** Usadas para enviar correos a varios usuarios mediante grupos de distribución.
- **Ejemplo de nombre completo:** Para un grupo llamado "smr" en el dominio `rlopezs30.local`, su nombre completo sería `smr@rlopezs30.local`.

### 1.1 Grupos Integrados en Active Directory

Active Directory proporciona grupos integrados con derechos predefinidos para realizar tareas específicas.

- **Contenedores Builtin y Users:**

Permiten simplificar la asignación de derechos y permisos a otras cuentas o grupos

- **Builtin:** Grupos con ámbito **local integrado**. No se pueden cambiar su tipo ni ámbito.
  - **Users:** Incluye grupos con ámbitos **global** y **local de dominio**, que pueden moverse dentro del dominio.
- Tanto los grupos del contenedor Builtin, como los del contenedor Users, pueden cambiarse libremente de contenedor, siempre que se mantengan dentro del mismo dominio.

## 2. Tipos de Grupos

Existen dos tipos principales de grupos en Active Directory:



1. **Grupos de distribución:**

- Usados para listas de correo electrónico, no tienen SID y no pueden asignar permisos de seguridad.

2. **Grupos de seguridad:**

- Utilizados para asignar permisos a recursos compartidos y establecer restricciones.
- Permiten asignar:
  - Derechos de usuario (acciones dentro del dominio).
  - Permisos para recursos (acceso a archivos o carpetas).

### 3. Ámbitos de los Grupos

El **ámbito** determina el alcance del grupo dentro de la red y qué permisos puede tener.

- **Local de dominio:**

- Permisos efectivos solo en el dominio donde se crea el grupo.
- Ideal para controlar recursos dentro de un único dominio.

- **Global:**

- Solo permite incluir cuentas y grupos globales del mismo dominio.
- Los permisos aplican en cualquier dominio del bosque.

- **Universal:**

- Permite incluir usuarios y grupos de diferentes dominios.
- Ideal para redes con múltiples dominios en el bosque.

### 4. Cuándo Usar Cada Tipo de Grupo

1. **Grupos locales de dominio:**

- Útiles para recursos específicos de un dominio.

•**Ejemplo de uso:** si tenemos un recurso específico en un dominio y queremos conceder permisos a un grupo de usuarios dentro de ese dominio, podemos utilizar un grupo local de dominio. De esta forma, para cada recurso compartido (impresora, directorio compartido, etc.) se crean tantos grupos locales como configuraciones de permisos se necesiten. Por ejemplo, control total sobre un directorio o de solo lectura:

GL\_ControlTotalDocumentos y GL\_LecturaDocumentos. Se configuran los permisos con estos dos grupos locales y, por último, tan solo tendremos que añadir los grupos globales o usuarios del dominio individuales a cada uno de los grupos en función de los permisos que queramos darles.

- Ejemplo: Controlar accesos diferenciados (lectura o escritura) a carpetas compartidas.

2. **Grupos globales:**

- Usados para organizar usuarios con necesidades similares de acceso en cualquier dominio del bosque.

•**Ejemplo de uso:** podemos agrupar usuarios con una función similar y otorgar permiso para acceder a un recurso, como una impresora o una carpeta compartida y archivos, que está disponible en el dominio local o en otro dominio del mismo bosque.

### 3. Grupos universales:

- Ideales para recursos que abarcan varios dominios.

•**Ejemplo de uso:** si tenemos varios dominios en un bosque y necesitamos otorgar permisos, a usuarios de diferentes dominios, para acceder a recursos, en todo el bosque, puedes utilizar un grupo universal para gestionar esos permisos. Cuidado con su uso ya que carga mucho el tráfico de la red y consumiendo muchos recursos.

¿y si necesitamos que estos 5 usuarios impriman en una impresora situada en otro dominio del bosque?

Para ello, en lugar de añadir los usuarios a un grupo local de dominio, lo conveniente es colocar las cinco cuentas de usuario en un grupo con ámbito global y agregar este grupo global como miembro del grupo local de dominio que da permisos sobre las impresoras. De este modo, conseguiremos que a nuestros usuarios se les pueda asignar permisos en cualquier dominio del bosque.

Si lo asignamos como Dominio Local, podremos usar el plotter siempre que esté dentro de nuestro dominio local. Sin embargo, si en otro dominio del bosque se instala un nuevo plotter, ellos no podrán ver el grupo NEC\_PLOTTER puesto que dicho grupo “no sale” de nuestro dominio de ninguna forma.

Si lo asignamos como Global, el grupo NEC\_PLOTTER si sería visible en los otros dominios, pero pongamos que de repente nos avisan que el usuario LUISJOSE (que no es de nuestro dominio, sino de otro dominio del bosque) necesita permisos para usar nuestro plotter... no podremos incluir al usuario LUISJOSE en el grupo NEC\_PLOTTER, ya que un grupo Global solo permite que introduzcamos a usuarios de nuestro propio dominio.

Si lo asignamos como Universal, no tendríamos ningún problema, ya que este tipo de grupos no tiene prácticamente ningún tipo de limitación, sin embargo, dichos grupos influyen negativamente en el funcionamiento de nuestro dominio, ya que “consumen” muchos recursos de nuestro directorio activo.

Una solución “elegante” sería crear NEC\_PLOTTER como grupo local, y darle permisos sobre nuestro plotter. A continuación, creamos

un grupo global NEC\_PLOTTERg y le añadimos como miembro a nuestro grupo local NEC\_PLOTTER. De esta forma, un dominio de nuestro bosque podrá añadir a sus recursos a nuestro grupo NEC\_PLOTTERg y así asignarles permisos a nuestros usuarios. Del mismo modo, si necesito añadir a un usuario LUISJOSE de otro dominio a nuestro plotter, lo puedo introducir en el grupo local NEC\_PLOTTER.

## 5. Administración de Cuentas de Grupo

Las acciones más comunes incluyen:

- Crear, modificar, agregar y eliminar miembros.
- Anidar grupos (un grupo como miembro de otro).
- Eliminar grupos según necesidades de reestructuración.

### 5.1 Crear Grupos

Se realiza desde la herramienta *Usuarios y Equipos de Active Directory*. Se define:

- **Nombre del grupo:** Único en el dominio, con un SID asignado automáticamente.
- **Tipo y ámbito del grupo.**

### 5.2 Modificar Propiedades

Desde la pestaña **Propiedades**, se pueden cambiar:

- **Nombre, descripción, correo.**
- **Ámbito y tipo del grupo.**
- **Miembros y relaciones de pertenencia.**

### 5.3 Gestión de Miembros

- **Agregar miembros:** Desde la pestaña "Miembros", se seleccionan usuarios, equipos o grupos.
- **Eliminar miembros:** Los usuarios eliminados del grupo pierden los permisos asociados al grupo.
- **Anidar grupos:** Permite estructurar jerárquicamente los permisos y simplificar la administración.

### 5.4 Eliminar Grupos

Eliminar un grupo no afecta a sus miembros, pero se pierden los permisos asignados al grupo

## . Creación y gestión de grupos con DSADD

- **Comando para crear un grupo:**

```
dsadd group "GroupDn" [atributos]
```

- **GroupDn:** Nombre distinguido del grupo.
- Ejemplo:

```
dsadd group "CN=VIKINGOS, CN=USERS, DC=BIXO, DC=COM"
```

- **Atributos útiles:**

- **-secgrp [yes|no]:** Define si el grupo es de seguridad o distribución.
- **-scope [L|G|U]:** Define el ámbito (Local, Global, Universal).
- **-desc descripción:** Descripción del grupo.
- **-members MemberDn:** Añade miembros al grupo.

### Ejemplo: Crear grupos específicos

1. Crear un grupo global para el departamento desarrollo:

```
dsadd group "CN=desarrollo,OU=grupos,DC=aic,DC=local" -secgrp  
yes -scope g -desc "Grupo Global de desarrollo" -members  
"CN=desarrollo01,OU=desarrollo,OU=usuarios,DC=aic,DC=local"
```

2. Crear un grupo local de dominio y añadir otros grupos como miembros:

```
dsadd group  
"CN=ACL_desarrollo_modificar,OU=grupos,DC=aic,DC=local" -secgrp  
yes -scope l -desc "Grupo Local para desarrollo" -members  
"CN=desarrollo,OU=grupos,DC=aic,DC=local"  
"CN=direccion,OU=grupos,DC=aic,DC=local"
```

## Gestión avanzada de grupos

1. **Eliminar grupos:**

```
dsrm "GroupDn"
```

Ejemplo:

```
dsrm "CN=VIKINGOS, CN=USERS, DC=BIXO, DC=COM"
```

2. **Añadir miembros a un grupo existente:**

```
dsmod group "GroupDn" -addmbr "MemberDn"
```

Ejemplo:

```
dsmod group "CN=grupol,OU=grupos,DC=vallexxx,DC=local" -addmbr  
"CN=usuariol,OU=usuarios,DC=vallexxx,DC=local"
```

### 3. Eliminar miembros de un grupo:

```
dsmod group "GroupDn" -rmmbr "MemberDn"
```

Ejemplo:

```
dsmod group "CN=grupol,OU=grupos,DC=vallexxx,DC=local" -rmmbr  
"CN=usuariol,OU=usuarios,DC=vallexxx,DC=local"
```

### 4. Cambiar el tipo de un grupo existente:

```
dsmod group "GroupDn" -secgrp [yes|no] -scope [L|G|U]
```

### 5. Mover o renombrar grupos:

- Cambiar el nombre:

```
dsmove "GroupDn" -newname "NewName"
```

- Mover entre unidades organizativas:

```
dsmove "GroupDn" -newparent "NewOU"
```

- Mover y cambiar nombre:

```
dsmove "GroupDn" -newname "NewName" -newparent "NewOU"
```

---

## Consultas útiles

#### 1. Mostrar todos los grupos del dominio:

```
dsquery group "dc=dominio,dc=local"
```

#### 2. Mostrar los miembros de un grupo:

```
dsget group "GroupDn" -members
```

#### 3. Listar grupos que comiencen con un nombre específico:

```
dsquery group domain root -name "Nombre*"
```

**Ejemplo práctico:** Crear un grupo llamado NUEVO, añadir 4 usuarios, y luego quitar dos usuarios del grupo:

#### 1. Crear grupo:

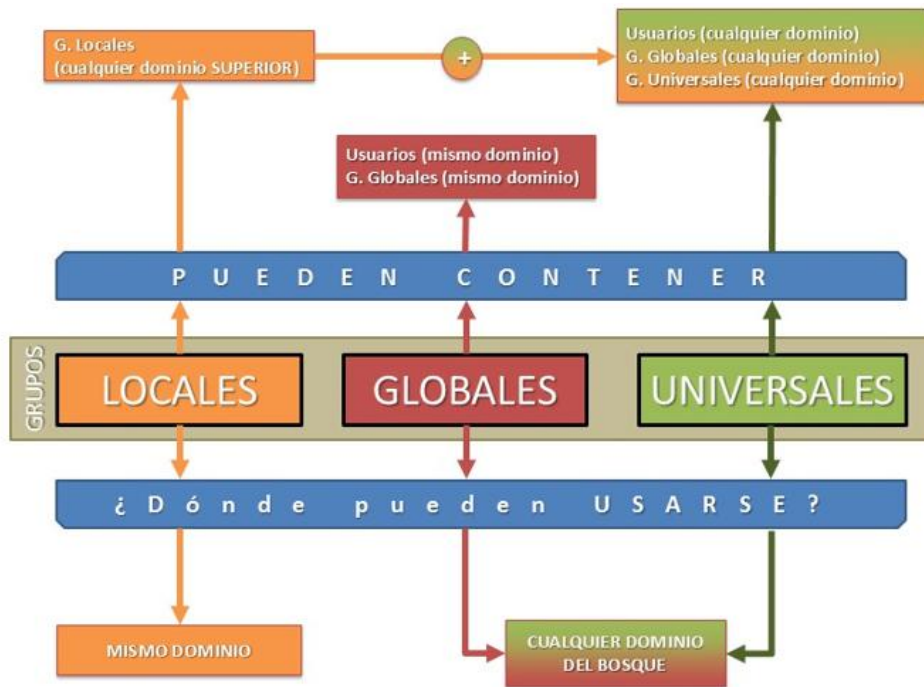
```
dsadd group "CN=NUEVO,OU=grupos,DC=vallexxx,DC=local"
```

## 2. Añadir usuarios:

```
dsmod group "CN=NUEVO,OU=grupos,DC=vallexxx,DC=local" -addmbr  
"CN=user1,OU=usuarios,DC=vallexxx,DC=local"  
"CN=user2,OU=usuarios,DC=vallexxx,DC=local"
```

## 3. Quitar usuarios:

```
dsmod group "CN=NUEVO,OU=grupos,DC=vallexxx,DC=local" -rmmbr  
"CN=user1,OU=usuarios,DC=vallexxx,DC=local"
```



Ámbito de grupo	Contenido: El grupo puede incluir como miembros:	Visibilidad: Al grupo se le pueden asignar permisos en:
Dominio Local	Las cuentas del cualquier dominio del bosque. Grupos globales de cualquier dominio. Grupos Universales de cualquier dominio. Grupos locales de dominio, pero solo del dominio local.	Solo en el dominio local.
Global	Las cuentas del dominio local. Los grupos globales del dominio local.	Cualquier dominio del bosque.
Universal	Las cuentas de cualquier dominio del bosque. Los grupos globales de cualquier dominio del bosque. Los grupos universales de cualquier dominio del bosque.	Cualquier dominio del bosque.

## Cómo Compartir Recursos entre Controladores de Dominio y Subdominios

### Escenario

- **Dominio principal:** vallexxx.local
  - Controladores de dominio:
    - Windows 2008 (DC1)
    - Windows 2012 (DC2)
  - **Grupo Universal:** "Nivel 1 Universal"
- **Subdominio:** asir.vallexxx.local
  - Dirección IP: 192.168.0.3
  - **Grupo Global:** "Nivel Acceso 1"

El objetivo es permitir que un usuario del subdominio asir.vallexxx.local acceda a un archivo almacenado en el controlador de dominio vallexxx.local.

**Nota:** Es necesario que el subdominio tenga una máquina cliente Windows conectada para realizar las pruebas.

### Pasos para Configurar el Acceso

### 1. Crear la carpeta y el recurso en el dominio principal

- En el controlador de dominio **vallexxx.local**, crear una carpeta llamada **TUTORIAL** en la raíz de la unidad **C:** y dentro incluir un archivo.

**Ejemplo:** **C:\TUTORIAL\archivo.txt**

### 2. Crear usuarios y grupo en el subdominio

- En el subdominio **asir.vallexxx.local**, realizar las siguientes acciones:
  - Crear usuarios como **Manuel, David, Carmen Navarro y Ana Herrero**.
  - Crear un grupo de tipo **Global** llamado **"Nivel Acceso 1"**.
  - Agregar a los usuarios **Carmen Navarro y Ana Herrero** como miembros del grupo **"Nivel Acceso 1"**.

#### Opciones para crear el grupo:

- **Opción A:** Acceder directamente al subdominio **asir.vallexxx.local** y crear el grupo desde allí.
- **Opción B:** Desde el controlador de dominio **vallexxx.local**, usar la herramienta **Dominios y Confianzas** para administrar el subdominio y crear el grupo remotamente.

### 3. Crear un grupo en el dominio principal

- En el dominio **vallexxx.local**, crear un grupo en el controlador de dominio:
  - **Inicial intento con un grupo Global:**
    - Intentar crear un grupo Global llamado **"Nivel 1 Global"** y agregarle el grupo **"Nivel Acceso 1"** del subdominio.
    - **Error esperado:** No será posible agregar el grupo del subdominio porque los grupos Globales solo admiten miembros del mismo dominio.
  - **Solución:** Crear un grupo **Universal** llamado **"Nivel 1 Universal"** en lugar de un grupo Global.
    - Los grupos Universales permiten incluir grupos y usuarios de diferentes dominios dentro del bosque.
    - Agregar al grupo **"Nivel 1 Universal"** el grupo **"Nivel Acceso 1"** del subdominio **asir.vallexxx.local**.

### 4. Compartir la carpeta TUTORIAL

- En el controlador de dominio **vallexxx.local**, compartir la carpeta **TUTORIAL**:
  - Botón derecho sobre la carpeta → **Propiedades** → **Compartir**.
  - Agregar el grupo **"Nivel 1 Universal"** con permisos de solo lectura.

### 5. Probar el acceso desde el cliente en el subdominio



- En una máquina cliente con Windows 10, conectada al subdominio `asir.vallexxx.local`, iniciar sesión con un usuario que sea miembro del grupo "*Nivel Acceso 1*" (por ejemplo, **Carmen Navarro**).
- **Actualizar directivas de grupo** en los controladores de dominio y el cliente:
  - Ejecutar el comando:
 

```
gpupdate /force
```
- Reiniciar la máquina cliente y verificar que el usuario puede acceder al archivo compartido en `\\vallexxx.local\TUTORIAL`.

## Notas Importantes

- **Uso de Grupos Universales:**  
Los grupos Universales deben utilizarse con cuidado, ya que pueden generar tráfico adicional en la red al replicarse entre todos los controladores de dominio del bosque.

## Alternativa

- En lugar de usar un grupo Universal en el dominio principal, puedes optar por usar un grupo **Local de Dominio**:
  - Crear un grupo Local de Dominio en `vallexxx.local` llamado "*Nivel 1 Local*".
  - Agregar al grupo "*Nivel Acceso 1*" del subdominio como miembro del grupo "*Nivel 1 Local*".
  - Compartir la carpeta **TUTORIAL** con permisos para el grupo "*Nivel 1 Local*".

Esta alternativa reduce el impacto en la red, pero el grupo Local de Dominio solo estará disponible dentro de `vallexxx.local` y no en otros dominios o subdominios.

## 1. Permisos y Derechos

- **Derechos y permisos:** Los derechos son atributos que permiten realizar acciones sobre el sistema, mientras que los permisos se asignan a usuarios o grupos sobre recursos específicos.
- **SAT (Security Access Token):** Al conectar un usuario, se le asigna un token de acceso que incluye su SID (identificador de seguridad), el de los grupos a los que pertenece y sus derechos.
- **ACLs:** Las Listas de Control de Acceso (ACLs) son responsables de gestionar los permisos en los recursos. Existen dos tipos principales:
  - **DACL:** Controla los permisos de acceso (permitidos o denegados).
  - **SACL:** Especifica las acciones que deben ser auditadas.
- **Herencia de ACLs:** Los recursos pueden heredar ACLs de otros recursos para simplificar la administración.

## 2. Gestión de Recursos Compartidos

- **Protocolo SMB:** Este protocolo permite compartir recursos como archivos e impresoras entre sistemas. Samba, una alternativa gratuita, ha hecho posible que sistemas Linux y otros usen SMB.
- **Configuración de la red en Windows:** Para compartir recursos, los equipos deben estar en el mismo grupo de trabajo o dominio, y deben tener direcciones IP, máscara de red y servidores DNS configurados correctamente.
- **Carpetas compartidas:** Cuando se comparte una carpeta, todos sus archivos y subdirectorios también se comparten. Los nombres de los recursos no necesitan coincidir con los nombres originales, y si un recurso termina en \$, será oculto en las búsquedas.

### 3. Acceso a Recursos Compartidos

- **Conexión a carpetas compartidas:** Para acceder a recursos compartidos, se puede usar la ruta directa del recurso (\\Servidor\RecursoCompartido) o buscarlo a través de la red.
- **Administración de conexiones:** A través de herramientas como "Administración de equipos" o comandos como `net share`, se pueden ver, gestionar y terminar las conexiones activas a los recursos compartidos.
- **Recursos especiales:** Algunos recursos como `ADMIN$`, `IPC$` y `NETLOGON` son creados por defecto para la administración y seguridad del sistema, y no permiten modificar sus permisos, aunque pueden ser eliminados.

### 4. Recursos Compartidos Especiales

- **Tipos de recursos especiales:**
  - **ADMIN\$:** Usado por el sistema para la administración remota.
  - **IPC\$:** Para la comunicación entre procesos.
  - **NETLOGON:** Para la validación de cuentas en un dominio.
  - **SYSVOL:** Contiene los datos de Active Directory.
  - **PRINT\$ y FAX\$:** Usados para compartir impresoras y servicios de fax.

### 5. Permisos de Recursos Compartidos

- **Permisos:** Se pueden configurar para controlar el acceso a carpetas compartidas. Los permisos básicos incluyen:
  - **Sin acceso:** No tiene permisos.
  - **Leer:** Permite ver y abrir archivos.
  - **Cambiar:** Permite leer y modificar archivos.
  - **Control total:** Permite leer, cambiar y modificar permisos.
- Los permisos de acceso compartido se combinan con los permisos NTFS (sistema de archivos) para determinar el nivel de acceso real.

### 6. Conexión a Unidades de Red

- **Desde el explorador de Windows:** Se puede mapear una unidad de red y asignarle una letra, con la opción de hacer la conexión permanente o solo temporal.
- **Comandos de red:** El comando `net use` permite conectar, desconectar y administrar unidades de red desde la línea de comandos.

## 7. Publicación en Active Directory

- **Publicar recursos:** Al publicar un recurso compartido en Active Directory, se facilita su localización por otros equipos del dominio.
- **Acceso mediante GPO:** Las políticas de grupo permiten automatizar la publicación y gestión de recursos en la red.

## 8. Seguridad en los Recursos Compartidos

- **Auditoría y control de acceso:** Es importante habilitar la auditoría para monitorizar los intentos de acceso a recursos compartidos y asegurar que solo los usuarios autorizados tengan acceso.
- **Automatización y scripts:** Utilizar scripts y políticas de grupo para automatizar la configuración de permisos y el acceso a recursos.

## 9. Mantenimiento y Monitorización

- **Revisión de permisos:** Es crucial realizar auditorías periódicas para garantizar que los permisos estén correctamente configurados.
- **Comprobación de accesibilidad:** Verificar regularmente que los recursos compartidos sean accesibles desde todos los dispositivos.
- **Monitorización de uso:** Controlar el acceso y la utilización de los recursos para evitar problemas de rendimiento o seguridad.
- avanzadas de gestión de permisos.

## 10. Actividad: Creación y Configuración de Recursos Compartidos

En este apartado se detalla cómo realizar ciertas configuraciones prácticas relacionadas con los recursos compartidos:

- **Crear carpetas compartidas en Windows Server 2022:** Se debe crear dos carpetas denominadas "CarpetaCompartida" y "CarpetaCompartida2" en el escritorio del servidor y luego configurarlas para ser compartidas en la red.
  - **Asignación de letras de unidad:**
    - Para "CarpetaCompartida", se asigna la letra **Z:**, pero no se configura para que se conecte automáticamente al iniciar sesión.
    - Para "CarpetaCompartida2", se asigna la letra **X:** y se configura para que se conecte automáticamente al iniciar sesión.
  - **Verificación:** Después de cerrar sesión y volver a iniciar, se verifica si las unidades **X** y **Z** están disponibles.
  - **Publicación en Active Directory:** Además de compartir los recursos, es posible publicarlos en el Directorio Activo para facilitar su búsqueda y acceso dentro de un dominio. Esto se puede hacer desde las opciones de "Usuarios y Equipos de AD" o mediante la creación de un nuevo recurso compartido dentro de una Unidad Organizativa (OU).
- 

## 11. Actividad: Compartición Simple de Recursos en un Controlador de Dominio

Se explica cómo compartir carpetas en un servidor de dominio para facilitar el acceso a los usuarios dentro del dominio:

1. **Compartir carpetas:** Se crean las carpetas **basesdedatos**, **plantillasword**, y **copiasseguridad** en el controlador de dominio.
  2. **Configuración de uso compartido:**
    - Se activan las opciones de uso compartido desde el "Centro de redes y recursos compartidos", lo que permite compartir archivos e impresoras y activar la detección de redes.
  3. **Permisos de acceso:**
    - Para la carpeta **basesdedatos**, se asigna al usuario **Luisa Jiménez** permisos de solo lectura.
    - Para la carpeta **copiasseguridad**, se asigna al usuario **Luis Roldán** permisos de lectura y escritura.
- 

## 12. Configuración de Permisos y Seguridad en Recursos Compartidos

Los permisos de los recursos compartidos deben gestionarse cuidadosamente para garantizar la seguridad y el control sobre el acceso. Algunos puntos clave incluyen:

- **Comprobación de permisos:** Los permisos del recurso compartido deben ser revisados primero, y luego los permisos NTFS (que se configuran desde la pestaña de "Seguridad") se aplican. El sistema aplica el permiso más restrictivo para determinar el acceso final.
  - **Tipos de permisos:**
    - **Sin acceso:** No tiene permisos.
    - **Leer:** Permite ver los archivos, pero no modificarlos.
    - **Cambiar:** Permite leer, modificar, y eliminar archivos.
    - **Control total:** Permite realizar cualquier acción, incluyendo cambiar permisos y tomar posesión de archivos.
- 

## 13. Configuración de Recursos en Redes de Dominio

El compartir recursos dentro de un dominio y configurarlos adecuadamente es crucial para asegurar que los usuarios y equipos de la red tengan acceso adecuado y controlado. Las siguientes configuraciones se detallan:

- **Activación del uso compartido:** Asegúrate de que las carpetas y archivos estén correctamente configurados en el servidor para ser accesibles por los clientes del dominio.
  - **Publicación en Directorio Activo:** Para que los recursos sean fácilmente localizables en un dominio, se recomienda publicar los recursos en Active Directory, lo que hace que los recursos sean visibles para los usuarios y dispositivos dentro del dominio de manera centralizada.
-

## 14. Conclusión: Mejores Prácticas en la Gestión de Recursos Compartidos

Es importante seguir una serie de buenas prácticas para asegurar que los recursos compartidos sean administrados de forma eficiente y segura:

- **Monitorear y auditar recursos:** Configura auditorías para rastrear el acceso a los recursos compartidos, lo que te permitirá identificar accesos no autorizados o actividades sospechosas.
- **Configurar adecuadamente los permisos:** Asegúrate de aplicar los permisos más restrictivos que sean necesarios, combinando permisos de recursos compartidos y permisos NTFS.
- **Mantener la seguridad:** Los recursos como carpetas compartidas deben estar configurados para que solo usuarios autorizados tengan acceso a ellos. Además, es importante revisar periódicamente la configuración de la red y los permisos.
- **Documentación y respaldo:** Mantén un registro detallado de los recursos compartidos y sus configuraciones. Esto facilitará la administración y recuperación de datos en caso de problemas.

## 15. Gestión de Accesos y Recursos Compartidos en Redes Complejas

En entornos más grandes, como redes de dominios, se gestionan no solo los recursos compartidos, sino también los accesos y las auditorías de los mismos de forma centralizada a través de servidores y herramientas de administración de redes.

### 15.1 Accesos a Recursos Compartidos a través de la Red

Los recursos compartidos, como carpetas y unidades, son accesibles desde otros equipos en la red, pero el acceso está determinado por varios factores:

1. **Permisos de acceso:** Estos permisos deben ser correctamente configurados para asegurar que solo los usuarios o grupos autorizados puedan acceder a los recursos. Los permisos pueden ser de lectura, escritura o control total.
2. **Comprobación de accesibilidad:** Asegurarse de que los recursos compartidos son visibles y accesibles a través de la red es un paso crucial. Esto se realiza configurando adecuadamente la detección de redes y el uso compartido de archivos e impresoras en el sistema operativo.
3. **Comprobación de permisos NTFS:** Cuando se usan sistemas de archivos como NTFS, los permisos del sistema de archivos también deben ser tomados en cuenta. Aunque los permisos de red (compartidos) se aplican primero, si un usuario no tiene acceso a nivel de NTFS, no podrá acceder al archivo o carpeta, independientemente de los permisos de red.

### 15.2 Configuración de Unidades de Red

Para facilitar el acceso, es posible asignar letras de unidades a recursos compartidos. En este contexto, se mencionan varias formas de conectarse a una unidad de red:

1. **Conexión manual:** El usuario puede conectarse manualmente a un recurso compartido a través de la barra de direcciones del explorador de archivos o

mediante comandos en la consola de Windows (cmd). Un ejemplo sería usar \\servidor\carpetaCompartida.

2. **Conexión automática:** Se pueden establecer conexiones automáticas a unidades de red al inicio de la sesión de un usuario, lo que facilita el acceso recurrente a las carpetas o archivos compartidos.
3. **Comandos net use:** El comando net use es utilizado para conectar unidades de red, permitir su desconexión y verificar conexiones existentes.

---

## 16. Recursos Compartidos Especiales

Windows crea ciertos recursos compartidos ocultos que se utilizan para fines administrativos del sistema. Estos recursos, aunque no son visibles para los usuarios normales, son importantes para la gestión del sistema y la red.

1. **ADMIN\$:** Este recurso está relacionado con la administración remota del sistema. Se utiliza para gestionar el sistema de forma remota y acceder al directorio de sistema en Windows.
2. **IPC\$:** El recurso IPC (Inter-Process Communication) se utiliza para la comunicación entre procesos en la red, lo que permite que las máquinas se comuniquen y envíen comandos a otras.
3. **Netlogon y SYSVOL:** Son recursos vitales en un dominio. **NETLOGON** se usa para la validación de cuentas en dominios, y **SYSVOL** es un recurso que contiene scripts y políticas de seguridad para los controladores de dominio de Active Directory.
4. **Impresoras y FAX:** Los recursos **PRINT\$** y **FAX\$** están relacionados con la gestión de impresoras y faxes en una red de dominio. Los controladores de impresoras y las configuraciones de fax se distribuyen a los clientes desde estos recursos compartidos.

---

## 17. Monitoreo y Auditoría de Recursos Compartidos

Es importante monitorear el acceso a los recursos compartidos para garantizar que los permisos se apliquen correctamente y que no haya accesos no autorizados.

1. **Sesiones activas:** Se puede visualizar qué usuarios están actualmente conectados a los recursos compartidos y qué archivos están abiertos. Desde el panel de administración de equipos, se pueden ver detalles como el número de conexiones y la duración de la sesión.
  2. **Cierre de sesiones:** En caso de que se necesite liberar recursos o gestionar el acceso de usuarios, es posible terminar sesiones individuales o incluso todas las sesiones activas en el sistema.
  3. **Archivos abiertos:** También es posible consultar qué archivos están actualmente en uso, quién los está utilizando y desde qué equipo. Esto permite gestionar recursos y solucionar problemas de acceso o bloqueo de archivos.
-

## 18. Publicación de Recursos en Active Directory

Para mejorar la visibilidad y el acceso a los recursos dentro de un dominio, es recomendable publicar recursos compartidos en Active Directory.

1. **Publicación de recursos:** Esto hace que los recursos compartidos sean fácilmente descubribles por otros usuarios dentro de la misma red o dominio, sin tener que conocer la ruta exacta al recurso.
  2. **Búsqueda en el Directorio Activo:** Los usuarios pueden buscar recursos compartidos a través de Active Directory utilizando herramientas estándar del sistema, lo que simplifica la localización de recursos en redes grandes.
- 

## 19. Configuración y Gestión de Permisos de Recursos Compartidos

La configuración correcta de los permisos de los recursos compartidos es clave para garantizar que solo los usuarios o grupos autorizados tengan acceso a los datos.

1. **Tipos de permisos:** Los permisos para recursos compartidos pueden ser:
    - **Leer:** Permite visualizar y abrir archivos, pero no modificarlos.
    - **Cambiar:** Además de leer, permite modificar, agregar y eliminar archivos y carpetas.
    - **Control total:** Incluye leer, cambiar y la capacidad de modificar los permisos de archivos y carpetas.
  2. **Interacción con NTFS:** Los permisos de un recurso compartido se combinan con los permisos NTFS. Si un usuario tiene permisos de solo lectura a nivel de NTFS, pero control total en el recurso compartido, el acceso final será limitado por el permiso más restrictivo, es decir, el permiso NTFS.
- 

## 20. Actividades Finales: Prácticas de Gestión de Recursos

Al final del documento se proponen actividades prácticas que refuerzan la comprensión y la aplicación de lo aprendido:

- **Compartición de recursos en un dominio:** Se requiere compartir carpetas específicas en un controlador de dominio y asignar permisos específicos a los usuarios.
- **Comprobación de accesibilidad:** Los administradores deben asegurarse de que las carpetas compartidas sean accesibles desde equipos clientes en la red.
- **Gestión de permisos:** Los administradores deben configurar y ajustar los permisos de los recursos compartidos para asegurarse de que sean adecuados para las necesidades de los usuarios.

## Políticas de Grupo en Windows

Las políticas de grupo son una herramienta fundamental en entornos Windows que permite configurar y administrar de forma centralizada varios aspectos de los equipos y usuarios de un dominio. Estas configuraciones incluyen, entre otras cosas:

- Modificaciones del registro.
- Políticas de seguridad.
- Instalación de software.
- Ejecución de scripts.
- Redirección de carpetas locales hacia recursos en red.

## Políticas Locales vs. Políticas de Grupo

- **Políticas Locales:** Son configuraciones aplicadas individualmente en un equipo y se gestionan con la consola `gpedit.msc` o `secpol.msc`.
- **Políticas de Grupo (GPO):** Permiten la gestión centralizada en entornos con Directorio Activo, facilitando la administración en dominios Windows Server.

## Conceptos Clave de las GPO

1. **Objeto de Política de Grupo (GPO):**
  - Es un contenedor que almacena configuraciones de políticas para equipos y usuarios.
  - Se puede vincular a **sitios, dominios y Unidades Organizativas (UO)** en el Directorio Activo.
2. **Herencia de GPO:**
  - Las políticas aplicadas en un dominio se heredan por todas las Unidades Organizativas (UO) de ese dominio.
  - Modificar la *Default Domain Policy* afecta a todos los equipos y usuarios del dominio.
3. **Jerarquía de configuración en GPO:**
  - **Configuración del equipo:** Configuraciones que se aplican a nivel de equipo (independientemente del usuario).
  - **Configuración del usuario:** Configuraciones que se aplican al usuario, independientemente del equipo donde inicie sesión.

## GPO Predeterminadas

1. **Default Domain Policy:**
  - Se aplica a todo el dominio y afecta a todos los equipos y usuarios.
  - Ejemplo de políticas aplicadas:
    - Contraseñas complejas y con una longitud mínima de 7 caracteres.
    - Historial de contraseñas: no permite reutilizar las últimas 24 contraseñas.
    - Vigencia máxima de la contraseña: 42 días.
    - Vigencia mínima de la contraseña: 1 día.
2. **Default Domain Controllers Policy:**
  - Se aplica exclusivamente a los controladores de dominio.

## Modificar una GPO



1. Accede a **Herramientas > Administración de Directivas de Grupo**.
2. Edita la GPO correspondiente (por ejemplo, *Default Domain Policy*).
3. Realiza los cambios necesarios:
  - Ejemplo: Modificar la vigencia mínima de la contraseña de 1 día a 0.
4. Guarda los cambios y verifica las configuraciones aplicadas con la opción "Mostrar todos los valores".

## Aplicación de GPO

1. Las GPO se aplican en función del inicio:
  - **Políticas de equipo:** Se aplican al arrancar el equipo.
  - **Políticas de usuario:** Se aplican al iniciar sesión.
2. Reevaluación periódica:
  - Usuarios y equipos: Cada 90 minutos (con un retraso aleatorio de 30 minutos).
  - Servidores de dominio: Cada 5 minutos.

Para un usuario si le afecta una GPO por defecto y otra del grupo al que pertenece, prevalecerá la del grupo.

### Forzar la Aplicación Inmediata:

- Utilizar el comando:

```
gpupdate /force
```

- Reiniciar el equipo o esperar el tiempo predefinido.

## Ejemplo Práctico: Contraseñas

1. Configuración inicial en *Default Domain Policy*:
  - **Contraseñas complejas:** Habilitado.
  - **Historial de contraseñas:** 24 contraseñas recordadas.
  - **Longitud mínima:** 7 caracteres.
  - **Vigencia mínima:** 1 día.
  - **Vigencia máxima:** 42 días.
2. Modificación:
  - Cambiar la vigencia mínima a 0 días.
  - Guardar los cambios y ejecutar `gpupdate /force`.
3. Resultado:
  - El usuario puede cambiar su contraseña inmediatamente, sin esperar el día mínimo.

## Consideraciones Finales

- **Cuidado al modificar GPO globales:** Cambios en políticas como *Default Domain Policy* afectan a todo el dominio.
- **Impacto en el rendimiento:** El uso excesivo de GPO complejas o innecesarias puede aumentar la carga en la red y el tiempo de inicio de sesión.

## Ejemplo Práctico: Contraseñas

1. Configuración inicial en *Default Domain Policy*:
  - **Contraseñas complejas**: Habilitado.
  - **Historial de contraseñas**: 24 contraseñas recordadas.
  - **Longitud mínima**: 7 caracteres.
  - **Vigencia mínima**: 1 día.
  - **Vigencia máxima**: 42 días.
2. Modificación:
  - Cambiar la vigencia mínima a 0 días.
  - Guardar los cambios y ejecutar `gpupdate /force`.
3. Resultado:
  - El usuario puede cambiar su contraseña inmediatamente, sin esperar el día mínimo.

## Consideraciones Finales

- **Cuidado al modificar GPO globales**: Cambios en políticas como *Default Domain Policy* afectan a todo el dominio.
- **Impacto en el rendimiento**: El uso excesivo de GPO complejas o innecesarias puede aumentar la carga en la red y el tiempo de inicio de sesión.

## Resumen: Redirección de Carpetas y Gestión de GPOs

### Directivas de Grupo: Conceptos Básicos

- Las **Directivas de Grupo (GPOs)** se gestionan desde *Herramientas > Administración de Directivas de Grupo*.
- Existen dos tipos de directivas:
  - **Directivas de equipo**: se aplican al iniciar el equipo.
  - **Directivas de usuario**: se aplican al iniciar sesión.
- En cada dominio, encontramos dos GPOs predefinidas:
  - **Default Domain Policy**: se aplica a todo el dominio, incluyendo sus unidades organizativas (U.O.).
  - **Default Domain Controllers Policy**: afecta exclusivamente a los controladores de dominio (U.O. Domain Controllers).

### Configuración de Contraseñas en GPO

Ejemplo de políticas configuradas en la Default Domain Policy:

- Almacenar contraseñas usando cifrado reversible: **Deshabilitado**.
- Historial de contraseñas: **24 contraseñas recordadas**.
- Complejidad de contraseña: **Habilitada**.
- Longitud mínima: **7 caracteres**.
- Vigencia máxima: **42 días**.
- Vigencia mínima: **1 día**.

## Modificación de Políticas

1. Acceder a la GPO deseada (*Editar*).
2. Cambiar valores en *Configuración de equipo > Directivas > Configuración de Windows > Configuración de seguridad > Directivas de cuenta > Directivas de contraseña*.
3. Ejemplo: Modificar la vigencia mínima de contraseña de 1 a 0 días para permitir cambios múltiples diarios.
4. Aplicar cambios mediante `gpupdate` desde CMD o esperar la sincronización automática.

## Redirección de Carpetas (Documentos)

Permite centralizar los documentos de los usuarios en una carpeta compartida en el servidor. Esto facilita la seguridad, el acceso desde múltiples dispositivos y la sincronización local para uso sin conexión.

### Pasos para Configurar la Redirección:

1. **Crear y compartir una carpeta en el servidor:**
  - o Ejemplo: `C:\Documentos_Usuarios`.
  - o Compartir con permisos de "Control Total" para el grupo objetivo (ej., **GrupoAlumnos**).
  - o Configurar seguridad eliminando permisos heredados y dejando solo Administradores, Sistema y el grupo creado.
2. **Crear un grupo de seguridad global/local:**
  - o Ejemplo: `GrupoAlumnos`.
  - o Usar comandos:
    - `dsquery` para listar usuarios de una U.O.
    - `dsadd` para crear el grupo.
    - `dsmod` para agregar usuarios al grupo.
3. **Crear y configurar la GPO:**
  - o Ir a *Configuración de Usuario > Configuración de Windows > Redirección de Carpetas > Documentos*.
  - o En **Propiedades**:
    - Configuración: Básico (redirigir todas las carpetas a la misma ubicación).
    - Ruta de acceso raíz: Ejemplo `\\Servidor\Documentos_Usuarios`.
    - Opciones adicionales:
      - **Mover contenido existente:** Copia datos locales a la carpeta de red.
      - **Derechos exclusivos del usuario:** Solo el usuario puede acceder a su carpeta.
      - Configurar acciones para cuando se elimine la GPO (dejar datos en red o devolverlos al local).
4. **Vincular la GPO a la U.O. correspondiente.**
5. **Probar funcionalidad:**
  - o Validar desde un cliente (ej., Windows 10).
  - o Confirmar la creación automática de carpetas por usuario.

- Verificar sincronización local y en red al desconectar y reconectar el equipo.

### Mensajes al Usuario al Iniciar Sesión

1. Crear una GPO vinculada a la U.O. objetivo.
2. En *Configuración de Usuario > Plantillas Administrativas > Sistema > Inicio de Sesión*:
  - Habilitar la opción "*Ejecutar estos programas al iniciar sesión*".
  - Añadir la ruta del archivo (ej., un mensaje en un archivo .txt compartido en red).

### Imagen Corporativa como Fondo de Pantalla

1. Crear o seleccionar la imagen corporativa.
2. Guardarla en una carpeta compartida del servidor con permisos restringidos.
3. Configurar una GPO:
  - *Configuración de Usuario > Plantillas Administrativas > Escritorio > Tapiz del Escritorio*.
  - Establecer la ruta de la imagen.
4. Vincular la GPO a la U.O. de toda la empresa.

### Prioridad en la Aplicación de GPOs

- **Orden de prioridad:** Equipo local < Sitio < Dominio < U.O.
- Las GPOs se suman, y solo se anulan si son contradictorias. La política **más restrictiva** prevalece.

Este enfoque asegura una gestión eficiente y segura de los usuarios y recursos dentro del dominio.

### Resumen: Cuotas de Disco 1

Las cuotas de disco permiten controlar y gestionar el uso del espacio en volúmenes NTFS. Estas configuraciones son útiles para evitar el uso excesivo de espacio en disco por parte de los usuarios.

#### Características principales:

- **Control del uso del espacio:**
  - Se puede especificar un **límite de cuota**. Si un usuario lo excede, no podrá usar más espacio y se registrará un evento en el visor de eventos.
  - Se puede establecer un **nivel de advertencia**, generando un evento cuando un usuario lo alcance.
- **Archivos comprimidos:**
  - Se contabilizan según su tamaño original (sin comprimir).

## Configuración de cuotas:

1. **Desde las Directivas de Grupo:**
    - Ubicación:
      - Configuración de equipo > Plantillas administrativas > Sistema > Cuotas de disco.
  2. **En propiedades de una unidad:**
    - Desde las propiedades del volumen NTFS en la pestaña **Cuotas**, donde se pueden habilitar, definir límites y exportarlas a otros volúmenes.
- 

## Actividad: Configurar cuotas de disco

- *Unidad C:).*
  - Selecciona **Propiedades** > pestaña **Cuotas**.
  - Si no están activadas, selecciona **Habilitar la gestión de cuotas**.
2. **Establecer límite general:**
    - Define un límite general de 2 GB para todos los usuarios:
      - Marca la opción **Denegar espacio en disco a los usuarios que excedan el límite**.
      - Establece el límite de **2 GB** y un nivel de advertencia opcional (por ejemplo, 1.8 GB).
  3. **Configurar cuota personalizada para un usuario:**
    - En la pestaña **Cuotas**, haz clic en **Entradas de cuota**.
    - Selecciona **Nuevo** o busca el usuario específico (por ejemplo, *Luisa Jiménez*).
    - Define para este usuario:
      - **Límite: 5 GB.**
      - **Nivel de advertencia: 4 GB.**

## Cuotas de Disco 2

Las **cuotas de disco** son límites establecidos por los administradores para controlar el uso del espacio en los sistemas de archivos, limitando la cantidad de datos que los usuarios pueden almacenar. Son especialmente útiles en entornos como servidores

## Configuración de Cuotas:

1. **Habilitar Cuotas:**
  - Se habilitan desde las **propiedades del volumen NTFS**, donde se activa la opción de "Habilitar administración de cuota".
  - Es posible **configurar límites** (espacio máximo permitido) y **niveles de advertencia** para los usuarios.
  - Las opciones incluyen la posibilidad de **denegar el acceso a más espacio cuando se supera el límite**.
2. **Cuotas por Usuario:**

- Las cuotas pueden configurarse de manera **individual**, permitiendo que cada usuario tenga un límite distinto de almacenamiento.
  - Es posible definir **alertas de advertencia** cuando se alcanza un cierto porcentaje de uso del espacio, y limitar el uso tras exceder el límite.
3. **Herramientas y Gestión:**
- Windows Server incluye herramientas para gestionar las cuotas, como el **Administrador de recursos del servidor de archivos**, que permite crear, modificar y monitorear cuotas a nivel de carpeta y usuario.
  - Las alertas pueden configurarse para **notificar al administrador** cuando un usuario alcance un umbral de uso.

**Prácticas recomendadas:**

- Dejar **espacio libre adicional** en los discos para personalizar cuotas y gestionar metadatos de NTFS.
- **Ajustar las cuotas** según el tipo de usuario y las necesidades de almacenamiento.
- Utilizar **informes y alertas** para detectar problemas de espacio antes de que afecten al sistema.

Gpedit.msc: modificación de políticas de grupo

Fsmgmt.msc: carpetas compartidas

Secpol.msc políticas de seguridad

Gpmc.msc: administrar las directivas de grupo