

Sistemas Operativos en Red

UD 06. Dominios con Windows Server



Consejería d'Educació,
Investigació, Cultura i Esport

I.E.S. SERRA PERENXISA



Fons Social Europeu

L'FSE inverteix en el teu futur

Autor: Sergi García

Actualizado Octubre 2023



Licencia



Reconocimiento - No comercial - CompartirIgual (BY-NC-SA): No se permite un uso comercial de la obra original ni de las posibles obras derivadas, la distribución de las cuales se ha de hacer con una licencia igual a la que regula la obra original.

Nomenclatura

A lo largo de este tema se utilizarán diferentes símbolos para distinguir elementos importantes dentro del contenido. Estos símbolos son:

Importante

Atención

Interesante

ÍNDICE

| | |
|---|-----------|
| 1. Introducción | 4 |
| 2. ¿Qué es Windows Server? | 4 |
| 3. Instalación de Windows Server | 4 |
| 4. Post Instalación de Windows Server | 5 |
| 4.1 Directivas de seguridad locales | 5 |
| 4.2 Roles en Windows Server | 6 |
| 4.3 Administración de discos y sistemas RAID en Windows Server | 7 |
| 5. Directorio activo y dominios | 8 |
| 5.1 Directorio activo (Active Directory) | 8 |
| 5.2 Dominio | 9 |
| 5.3 Controlador de dominio | 9 |
| 5.4 Árbol de dominios | 9 |
| 5.5 Bosque | 10 |
| 5.6 Unidad organizativa | 10 |
| 5.7 Relaciones de confianza | 10 |
| 5.8 Directivas de grupo GPO | 11 |
| 6. Gestión de dominios: Creación y despliegue | 11 |
| 6.1 Instalación de un servidor Windows Server 2022 | 11 |
| 6.2 Creación de un dominio: interfaz gráfica | 12 |
| 6.3 Creación de un dominio: PowerShell | 12 |
| 6.4 Introduciendo clientes Windows en un dominio: interfaz gráfica | 14 |
| 6.5 Introduciendo clientes Windows en un dominio: PowerShell | 14 |
| 6.6 Añadir clientes GNU/Linux al dominio | 15 |
| 7. Gestión de dominios: Gestión de usuarios, grupos y unidades organizativas | 15 |
| 7.1 Usuarios y grupos locales de una máquina | 15 |

| | |
|--|-----------|
| 7.2 Cuentas de usuario del dominio | 15 |
| 7.3 Grupos del dominio | 16 |
| 7.4 ¿Cuándo usar cada uno de los tipos de grupos de seguridad? | 16 |
| 7.5 Gestión de usuarios: interfaz gráfica | 17 |
| 7.6 Gestión de usuarios: PowerShell | 18 |
| 7.7 Gestión de grupos: interfaz gráfica | 18 |
| 7.8 Gestión de grupos: PowerShell | 19 |
| 7.9 Gestión de unidades organizativas: interfaz gráfica | 19 |
| 7.10 Gestión de unidades organizativas: PowerShell | 20 |
| 8. GPO (Group Policy Objects) | 20 |
| 8.1 ¿Dónde se aplican las GPO? | 21 |
| 8.2 Gestión de GPOs: interfaz gráfica | 21 |
| 8.3 Gestión de GPOs: PowerShell | 22 |
| 9. Recomendaciones de seguridad al administrar Windows Server | 22 |
| 10. Materiales de apoyo/ampliación | 23 |
| 11. Bibliografía | 23 |

UNIDAD 06. DOMINIOS CON WINDOWS SERVER

1. INTRODUCCIÓN

En el desarrollo de esta unidad trataremos la gestión de servidores con entornos Microsoft. Para ello realizaremos un resumen de los conceptos necesarios para la administración de este tipo de servidores (Directorio activo, dominios, usuarios, servicios, etc.) y explicaremos a grandes rasgos las principales operaciones a realizar.

2. ¿QUÉ ES WINDOWS SERVER?

Windows Server es un sistema operativo desarrollado por Microsoft que está diseñado específicamente para ser utilizado en servidores. A diferencia de los sistemas operativos de escritorio, como Windows 10, Windows Server se centra en brindar servicios y funciones avanzadas para administrar redes, almacenamiento, aplicaciones empresariales y otros recursos de una organización.

Windows Server ha evolucionado desde sus primeras versiones, donde eran conocidos como Windows NT, hasta la actual versión estable Windows Server 2022, la cual tiene soporte hasta el 14 de octubre de 2031. Para más información de versiones de Windows Server y soporte temporal de cada versión, podéis visitar [Windows Server release information | Microsoft Learn](#).

3. INSTALACIÓN DE WINDOWS SERVER

La instalación de Windows Server no se diferencia mucho de la instalación de otros sistemas Windows que ya han sido tratados a lo largo de este y otros módulos.

Algunos de los pasos clave a realizar son:

1. **Iniciar la Instalación:** inserta el medio de instalación y reinicia el servidor. El proceso de instalación se iniciará desde el medio.
 - a. Asegúrate de seleccionar la edición adecuada de Windows Server 2022 durante el proceso de instalación.
2. **Seleccionar el Idioma y la Distribución del Teclado.**
3. **Seleccionar el Tipo de Instalación:** Puedes elegir entre una instalación personalizada o una actualización, según tus necesidades.
 - a. **Para una instalación nueva, selecciona "Personalizada".**
4. **Particionar el Disco Duro:** en la instalación personalizada, puedes crear particiones en el disco duro y seleccionar dónde se instalará Windows Server. También puedes formatear y particionar unidades adicionales según sea necesario.
 - a. No está recomendado instalar más de un sistema operativo donde instales un Windows Server. Aun así, si en ese mismo computador vas a instalar otros sistemas operativos, recuerda dejar espacio libre particionado.
5. **Configurar Opciones de Red y Región.**
6. **Crear una Contraseña del Administrador.**
7. **Finalizar la Instalación:** una vez completada, el servidor se reiniciará y estarás listo para comenzar la configuración inicial y la administración del servidor.
8. **Realizar Configuraciones Post-Instalación:** después de la instalación, deberás configurar roles y características, aplicar actualizaciones, y establecer políticas de seguridad según las necesidades de tu entorno.

4. POST INSTALACIÓN DE WINDOWS SERVER

A continuación mencionamos algunos pasos a tener en cuenta en la post instalación de Windows Server.

4.1 Directivas de seguridad locales

Las directivas de seguridad locales en Windows Server son configuraciones específicas que se aplican al sistema operativo a nivel local para mejorar la seguridad y el control. Estas directivas permiten a los administradores establecer reglas y restricciones que afectan a la seguridad y el comportamiento del sistema. Estas solo pueden ser modificadas con usuarios con permiso de administrador.

! Atención: existe diversas formas de acceder al editor de directivas de seguridad locales, pero una de las más prácticas es presionar “Win + R” y escribir “secpol.msc” y pulsar intro.

A continuación, se proporciona un resumen de las directivas de seguridad locales en Windows Server:

- **Directivas de Contraseña:**
 - Establecer reglas para contraseñas, como longitud mínima y complejidad.
 - Definir políticas de bloqueo de cuentas después de varios intentos fallidos de inicio de sesión.
 - Configurar la duración máxima de las contraseñas y la historia de contraseñas anteriores.
- **Directivas de Bloqueo de Cuenta:**
 - Controlar cuántos intentos fallidos de inicio de sesión se permiten antes de bloquear una cuenta.
 - Establecer la duración del bloqueo de la cuenta.
- **Directivas de Auditoría:**
 - Determinar qué eventos del sistema se registran y qué eventos se ignoran.
 - Configurar la ruta de los registros de eventos de seguridad.
- **Directivas de Control de Acceso a Objetos:**
 - Definir permisos y restricciones de acceso a archivos, carpetas y recursos del sistema.
 - Controlar quién tiene acceso y qué tipo de acceso tienen los usuarios y grupos.
- **Directivas de Bloqueo de Programas:**
 - Restringir la ejecución de ciertos programas o scripts no autorizados.
 - Evitar que se ejecuten aplicaciones no deseadas o potencialmente peligrosas.
- **Directivas de Política de Seguridad Local:**
 - Configurar opciones de seguridad generales, como el nivel de seguridad de contraseñas o el modo de inicio de sesión interactivo.
 - Establecer directivas de seguridad específicas para el sistema.
- **Directivas de Seguridad de Red:**
 - Controlar la comunicación de red, incluyendo reglas de firewall, seguridad de IPsec y configuración de autenticación de red.
- **Directivas de Autenticación:**
 - Definir las opciones de autenticación, como autenticación de contraseña, autenticación de tarjeta inteligente o autenticación de huella digital.
- **Directivas de Control de Servicios:**
 - Administrar los servicios y controlar quién puede iniciar, detener o pausar servicios específicos.

- **Directivas de BitLocker:**
 - Configurar la encriptación de disco completo con BitLocker y definir políticas relacionadas con la administración de claves.
- **Directivas de Seguridad Avanzada:**
 - Configurar características de seguridad avanzada, como Control de Cuentas de Usuario (UAC), directivas de ejecución de aplicaciones y control de inicio de sesión.

Las directivas de seguridad locales son esenciales para establecer y mantener un entorno seguro en un servidor Windows Server 2022. Los administradores deben revisar y ajustar estas directivas según los requisitos de seguridad de su organización y las mejores prácticas de seguridad.

4.2 Roles en Windows Server

Los roles en Windows Server son conjuntos predefinidos de funcionalidades y servicios que se pueden instalar y configurar en un servidor para cumplir con una función específica. Estos roles permiten a los administradores de sistemas adaptar un servidor Windows para satisfacer las necesidades y requisitos particulares de una organización.

No vamos a trabajar con todos los roles. Aquí, con fin putamente informativo, indicamos un resumen de los roles más importantes en Windows Server:

- **Roles de Servidor:**
 - **Servidor de archivos:** Proporciona servicios de almacenamiento y permite compartir archivos y carpetas en la red.
 - **Servidor web (IIS):** Permite alojar sitios web y aplicaciones web en el servidor.
 - **Servidor DNS:** Gestiona la resolución de nombres de dominio en la red.
 - **Servidor DHCP:** Proporciona configuraciones de red automáticas a dispositivos en la red.
 - **Servidor de impresión:** Facilita la administración de impresoras y tareas de impresión en la red.
- **Roles de Infraestructura:**
 - **Servidor de control de dominio (Active Directory):** Administra la autenticación y la administración centralizada de usuarios, grupos y recursos en una red.
 - **Servidor de certificados:** Facilita la administración y emisión de certificados digitales.
 - **Servidor de directivas de acceso en red (NPS):** Permite la autenticación de usuarios y dispositivos en la red.
 - **Servidor de administración de derechos:** Gestiona la administración de derechos digitales para proteger contenido.
 - **Servidor de proxy inverso:** Protege la red al actuar como intermediario entre los usuarios y los servidores internos.
- **Roles de Aplicación:**
 - **Servidor de base de datos (SQL Server):** Proporciona servicios de gestión de bases de datos.
 - **Servidor de aplicaciones:** Aloja aplicaciones empresariales personalizadas.
 - **Servidor de virtualización (Hyper-V):** Permite la virtualización de servidores y recursos.
- **Roles de Almacenamiento y Archivo:**
 - **Servidor de archivos y almacenamiento:** Proporciona funciones de almacenamiento y compartición de archivos avanzadas.
 - **Servidor de copia de seguridad:** Administra y automatiza las copias de seguridad de datos.

- **Roles de Administración y Monitorización:**
 - **Servidor de administración central:** Facilita la administración centralizada de múltiples servidores.
 - **Servidor de supervisión:** Controla y registra el rendimiento y la disponibilidad de recursos y servicios.
- **Roles de Red y Acceso Remoto:**
 - **Servidor VPN:** Proporciona acceso seguro a la red para usuarios remotos.
 - **Servidor de equilibrio de carga:** Distribuye el tráfico de red entre varios servidores para mejorar la disponibilidad y el rendimiento.

4.3 Administración de discos y sistemas RAID en Windows Server

El Administrador de Discos en Windows Server es una herramienta que permite a los administradores de sistemas gestionar y administrar los discos y volúmenes en un servidor. Permite realizar una variedad de tareas relacionadas con el almacenamiento, incluyendo la configuración de sistemas RAID y la gestión de cuotas de disco.

Administrador de Discos en Windows Server:

- **Administración de Discos Básicos y Dinámicos:** El Administrador de Discos permite a los administradores convertir discos básicos en discos dinámicos, lo que permite características avanzadas como la expansión de volúmenes y la administración de espejos.
- **Creación y Formateo de Particiones:** Los administradores pueden crear nuevas particiones en discos, formatear particiones con sistemas de archivos como NTFS y FAT, y asignar letras de unidad a las particiones.
- **Administración de Volúmenes:** Es posible crear volúmenes simples, volúmenes espejo, volúmenes RAID-5 y volúmenes RAID-0, y administrar su tamaño y estado.
- **Gestión de Letras de Unidad y Puntos de Montaje:** Se pueden asignar letras de unidad a particiones o usar puntos de montaje para acceder a volúmenes en rutas específicas.
- **Reparación de Volúmenes:** El Administrador de Discos puede ayudar a detectar y solucionar problemas en volúmenes, como la marca de un volumen como activo o reparar volúmenes espejo después de una falla de disco.

Cuotas de Disco en Windows Server:

- **Cuotas de Disco:** Las cuotas de disco son límites que se aplican a la cantidad de espacio en disco que los usuarios o grupos pueden consumir en un volumen específico.
- **Gestión de Cuotas:** Con las cuotas de disco habilitadas, los administradores pueden supervisar y controlar el uso del espacio en disco por parte de los usuarios y grupos. Esto es útil para evitar que un usuario agote todo el espacio de almacenamiento en un servidor.
- **Notificación y Control:** Cuando un usuario se acerca al límite de su cuota de disco, se pueden configurar notificaciones para informar al usuario y a los administradores. Además, se pueden establecer políticas para impedir que un usuario exceda su cuota asignada.

Sistemas RAID en Windows Server:

Redundant Array of Independent Disks (RAID) es una tecnología que combina múltiples discos duros en una sola unidad lógica con el objetivo de mejorar el rendimiento y/o la redundancia de los datos almacenados. Los niveles de RAID son configuraciones específicas que se utilizan para combinar múltiples discos duros en un solo conjunto con el objetivo de mejorar el rendimiento, la redundancia de datos o ambas cosas.

En Windows Server, puedes configurar diferentes tipos de RAID para satisfacer las necesidades de tu entorno. Aquí te explico los tipos de RAID más comunes admitidos por Windows Server:

- **RAID 0 (Striping):**
 - Rendimiento: Alto.
 - Redundancia: Ninguna.
 - En RAID 0, los datos se dividen en fragmentos y se escriben en múltiples discos en paralelo. Esto mejora significativamente el rendimiento de lectura y escritura, ya que se pueden acceder a los datos simultáneamente desde varios discos. Sin embargo, no se ofrece redundancia, lo que significa que la pérdida de un solo disco resulta en la pérdida de todos los datos en el conjunto.
- **RAID 1 (Mirroring):**
 - Rendimiento: Moderado (lectura), igual que el disco más lento (escritura).
 - Redundancia: Alta.
 - RAID 1 utiliza dos discos o más para duplicar los datos. Cada dato se escribe en dos discos diferentes, lo que proporciona una copia idéntica (espejo) de los datos en caso de fallo de uno de los discos. Ofrece alta redundancia, pero el costo es una capacidad de almacenamiento efectiva reducida a la mitad.
- **RAID 5 (Striping con Paridad):**
 - Rendimiento: Moderado (lectura y escritura).
 - Redundancia: Moderada.
 - RAID 5 divide los datos en fragmentos y los distribuye en varios discos, al igual que RAID 0. Sin embargo, también calcula y almacena información de paridad distribuida en los discos. Esto permite la recuperación de datos en caso de fallo de uno de los discos. RAID 5 proporciona un equilibrio entre rendimiento y redundancia y es adecuado para entornos donde se necesita cierta protección de datos sin sacrificar demasiada capacidad.
- **RAID 10 (Combinación de Mirroring y Striping):**
 - Rendimiento: Alto (lectura y escritura).
 - Redundancia: Alta.
 - RAID 10 combina los beneficios de RAID 1 y RAID 0. Los datos se dividen en fragmentos y se escriben en múltiples discos en paralelo, como en RAID 0, pero cada disco tiene un espejo en otro disco, como en RAID 1. Esto ofrece un alto rendimiento y alta redundancia, pero también consume más espacio en disco debido a la duplicación de datos.

Además de estos tipos comunes, existen otras configuraciones de RAID, como RAID 6, RAID 50 y RAID 60, que ofrecen diferentes niveles de rendimiento y redundancia para satisfacer necesidades específicas.

La elección del tipo de RAID dependerá de tus necesidades de rendimiento y tolerancia a fallos. Es importante seleccionar el nivel de RAID adecuado para garantizar que tus datos estén protegidos y tu sistema funcione de manera eficiente en un entorno de Windows Server.

5. DIRECTORIO ACTIVO Y DOMINIOS

5.1 Directorio activo (Active Directory)

El Directorio Activo (Active Directory) es una base de datos jerárquica organizada, establecida en uno o varios servidores, que se utiliza para almacenar información sobre diferentes objetos. Su propósito principal es centralizar diversas operaciones de red, como inicio de sesión desde equipos dentro de una organización, implementación de políticas, despliegue de aplicaciones, entre otras.

En concreto, el directorio activo es una implementación específica del protocolo LDAP (Lightweight Directory Access Protocol) que almacena los objetos existentes en su sistema. Cualquier objeto dentro de este sistema, debe pertenecer a un dominio. Para saber más del protocolo LDAP https://es.wikipedia.org/wiki/Protocolo_ligero_de_acceso_a_directorios

Los objetos básicos que permite almacenar el Directorio activo son:

- Usuarios
- Grupos
- Equipos
- Impresoras
- Unidades organizativas


El uso de Directorio activo permite el acceso a múltiples recursos con un solo inicio de sesión, evitando así tener que recordar credenciales para distintos elementos.

De manera avanzada, podrían añadirse nuevos objetos modificando el esquema del directorio, aunque esta operación no es habitual ni la realizaremos durante el curso

5.2 Dominio

Un dominio en el Directorio Activo es un conjunto de objetos relacionados entre sí, organizados de manera jerárquica. El dominio actúa como un contenedor que almacena y gestiona la información de los objetos asociados dentro del Directorio Activo. Es una estructura fundamental en la administración de redes, ya que proporciona un contexto lógico y seguro para gestionar usuarios, equipos, grupos y otros recursos dentro de una organización.

Dentro de un dominio, tanto los recursos locales (como archivos y carpetas) como ciertos elementos del dominio (como impresoras compartidas) cuentan con listas de control de acceso (ACL, por sus siglas en inglés). Cada ACL almacena un conjunto de entradas de control de acceso (ACE, por sus siglas en inglés), que determinan si se concede o deniega un permiso a usuarios individuales o grupos de seguridad. De esta manera, se establece un control preciso sobre los derechos de acceso a recursos específicos dentro del dominio.

 **Importante:** las “ACL” están compuestas por distintas “ACE”. Mediante estas “ACE” indican quién puede o no acceder a un recurso del sistema.

5.3 Controlador de dominio

Un controlador de dominio es un servidor que alberga la base de datos de objetos asociada a un dominio y replica esta información en otros controladores de dominio adicionales.

Los controladores de dominio desempeñan un papel fundamental al autenticar y autorizar a los objetos dentro de su ámbito de control. Actúan como una autoridad centralizada para verificar la identidad de usuarios, equipos y otros recursos en el dominio, garantizando así la seguridad y el acceso adecuado a los recursos de la red.

Estos controladores de dominio trabajan en conjunto para mantener la coherencia y la sincronización de la base de datos de objetos del dominio, asegurando que los cambios realizados en un controlador se reflejen en los demás. Esto garantiza la disponibilidad y la redundancia de la información dentro del dominio, mejorando la fiabilidad y la escalabilidad del entorno de red.

5.4 Árbol de dominios

Un árbol de dominios es una estructura jerárquica de dominios interrelacionados, organizados generalmente mediante un sistema de nombres de dominio (DNS), que comparten una raíz común. Esta arquitectura se implementa con el propósito de fragmentar la estructura del

Directorio Activo y lograr un mejor rendimiento al asignar responsabilidades a diferentes dominios dentro del Directorio Activo.

Al dividir la estructura en árbol de dominios, se pueden delegar tareas de administración y gestión a nivel de dominio, lo que proporciona una mayor flexibilidad y escalabilidad. Cada dominio dentro del árbol puede tener su propio conjunto de controladores de dominio y objetos asociados, lo que permite una distribución eficiente de la carga y una gestión más efectiva de los recursos de red en sistemas corporativos grandes.

Además, el uso de un sistema DNS para organizar los dominios dentro del árbol proporciona una resolución de nombres eficiente y facilita la navegación y la comunicación entre los distintos dominios y sus objetos.

5.5 Bosque

Un bosque en el contexto del Directorio Activo es un conjunto de árboles de dominios interconectados. En un bosque, al menos un dominio primario está asociado, y este dominio en particular almacena el esquema del bosque.

El concepto de bosque en el Directorio Activo es fundamental para establecer una estructura lógica y de confianza en una red empresarial. Los árboles de dominios dentro del bosque están conectados mediante relaciones de confianza, lo que permite la colaboración y el intercambio de recursos entre los dominios.

! Atención: durante las actividades de este curso, trabajaremos únicamente con un único bosque.

5.6 Unidad organizativa

Una Unidad Organizativa (OU, por sus siglas en inglés) es un objeto utilizado para agrupar otros objetos dentro de un dominio de manera jerárquica. Las Unidades Organizativas tienen como propósito crear una estructura lógica que represente la organización, lo cual facilita las tareas de administración.

Las Unidades Organizativas permiten organizar y gestionar de manera eficiente los objetos del Directorio Activo, como usuarios, equipos, grupos y otros recursos. Al establecer una estructura jerárquica mediante las OU, es posible reflejar la estructura de la organización, lo que facilita la aplicación de políticas, permisos y configuraciones específicas a grupos de objetos relacionados.

5.7 Relaciones de confianza


Las relaciones de confianza son fundamentales en el Directorio Activo y se establecen entre bosques, árboles y dominios para autenticar usuarios de un dominio en otro dominio. El objetivo principal es permitir que un usuario de un dominio, llamémoslo A, pueda acceder y autenticarse en otro dominio, denominado B.

Cuando el dominio A confía en el dominio B, al intentar un usuario de B identificarse en el dominio A, el dominio A solicitará a B que valide las credenciales del usuario y, en caso de éxito, se le concederá el acceso.

Es importante destacar que las relaciones de confianza son unidireccionales. Esto significa que si el dominio A confía en el dominio B, no implica automáticamente que B confíe en A. Si se desea establecer una confianza bidireccional, debe especificarse explícitamente.

Además, es importante tener en cuenta que las relaciones de confianza no son necesariamente transitivas. Para que sean transitivas, es necesario indicarlo explícitamente. Esto significa que si el dominio A confía en el dominio B y el dominio B confía en el dominio C, no implica automáticamente que el dominio A confíe en el dominio C. Debe establecerse explícitamente una relación de confianza entre A y C para lograr la transitividad.

Al crear dominios dentro de un mismo bosque, se generan automáticamente relaciones de confianza bidireccionales y transitivas entre los dominios de ese bosque. Sin embargo, estas relaciones pueden modificarse posteriormente según los requerimientos específicos de la organización.

 **Importante:** las relaciones de confianza en el Directorio Activo permiten autenticar usuarios de un dominio en otro dominio. Recuerda que estas relaciones son unidireccionales y no necesariamente transitivas.

5.8 Directivas de grupo GPO

Las Directivas de Grupo son un conjunto de configuraciones que se pueden aplicar a objetos dentro de un dominio con el fin de implementar ajustes específicos. Estas directivas permiten modificar una variedad de funcionalidades destacadas, entre las cuales se encuentran:

- **Comandos de inicio de sesión:** las Directivas de Grupo brindan la capacidad de controlar y personalizar los comandos de inicio de sesión en los equipos del dominio. Esto incluye configuraciones como scripts de inicio, configuración de políticas de seguridad y acciones a ejecutar durante el inicio de sesión de un usuario.
- **Directivas de seguridad de cuentas de usuario:** mediante las Directivas de Grupo, es posible establecer configuraciones de seguridad para las cuentas de usuario en el dominio. Esto incluye la imposición de políticas de contraseñas, bloqueo de cuentas después de un número determinado de intentos fallidos, restricciones de inicio de sesión, entre otras medidas de seguridad.
- **Distribución de software a equipos clientes:** las Directivas de Grupo permiten la distribución y administración centralizada de software en los equipos clientes del dominio. Esto facilita la instalación, actualización y desinstalación de aplicaciones de forma automática y controlada en los equipos del dominio.

Estas funcionalidades son solo algunos ejemplos de las muchas posibilidades que las Directivas de Grupo ofrecen para personalizar y gestionar la configuración en un entorno de dominio. Al utilizar estas directivas de manera efectiva, se pueden mantener configuraciones consistentes, establecer políticas de seguridad y simplificar la administración de la red en toda la organización.

6. GESTIÓN DE DOMINIOS: CREACIÓN Y DESPLIEGUE

6.1 Instalación de un servidor Windows Server 2022

Durante la instalación de un servidor Windows Server 2022, se siguen varios pasos para seleccionar la versión adecuada y configurar diversos aspectos utilizando el asistente de instalación. Algunos de los elementos que se configuran durante este proceso incluyen la partición del disco, la configuración de fecha y hora, la creación de una contraseña para la cuenta de administrador, entre otros.

- El primer paso es seleccionar la versión específica de Windows Server 2022 que se desea instalar, asegurándose de elegir la edición adecuada según las necesidades y requisitos del servidor.
- Luego, se procede a configurar el particionado del disco, lo que implica seleccionar el disco o partición en el cual se instalará el sistema operativo y definir su tamaño y formato.
- Después, se establece la configuración de fecha y hora para garantizar la sincronización adecuada del servidor con la red y otros dispositivos.
- En este punto, se crea una contraseña para la cuenta de administrador, que proporcionará acceso completo al servidor. Es fundamental elegir una contraseña segura y recordarla adecuadamente para garantizar la seguridad del sistema.

Además de estos aspectos mencionados, el asistente de instalación también permite configurar otras opciones, como la configuración regional, las actualizaciones automáticas, los ajustes de red y la configuración de roles y características adicionales según las necesidades específicas del servidor.

6.2 Creación de un dominio: interfaz gráfica

Antes de crear un dominio, es común revisar y ajustar la configuración de red de acuerdo a nuestras necesidades. Por lo general, los servidores controladores de dominio se configuran con una dirección IP fija.

Una vez todo listo, daremos los siguientes pasos (que pueden ser ligeramente distintos según la versión):

- Para crear un dominio, debemos utilizar la herramienta "Administrador del servidor" en el ordenador que deseamos utilizar como controlador de dominio. Desde allí, accederemos a la opción "Agregar roles y características".
- Aparecerá un asistente en el cual seleccionaremos si queremos realizar una "Instalación basada en características o en roles". Luego, de la lista de servidores disponibles, elegiremos el servidor destinado a ser el controlador de dominio.
- Una vez hecho esto, podremos seleccionar los roles que deseamos instalar en nuestro sistema. En este caso, elegiremos "Servicios de dominio de Active Directory", y al instalarlo, se nos indicará que se instalarán algunas características requeridas para este rol.
- Generalmente, nuestro servidor también requerirá que instalemos otros roles para el correcto funcionamiento del dominio, como el rol de "Servidor DNS" o el rol de "Servidor DHCP".
- La creación del dominio incluirá los siguientes pasos:
 - Elegir si queremos unirlo a un bosque existente, crear un nuevo bosque o si este controlador será un controlador adicional de dominio.
 - Especificar el nombre del dominio.
 - Seleccionar el nivel de funcionalidad del dominio, lo cual determina la compatibilidad con otras versiones de Windows Server 20XX.
 - Decidir si deseamos que nuestro servidor también funcione como servidor DNS del dominio (generalmente recomendado).
 - Establecer una contraseña para la cuenta de administrador del dominio.
- Después de instalar el software y reiniciar el servidor, se mostrarán notificaciones de configuración que debemos atender. En ellas, seleccionaremos la opción "Promover este servidor a controlador de dominio".

! Atención: durante el proceso de promoción, se nos ofrecerá la opción de "Ver script", que nos mostrará un script PowerShell con todas las acciones realizadas hasta ese momento, lo cual puede resultar útil para la automatización de procesos.

6.3 Creación de un dominio: PowerShell

Al igual que cuando creamos un dominio mediante interfaz gráfica, antes de crear un dominio usando PowerShell, es común revisar y ajustar la configuración de red de acuerdo a nuestras necesidades. Por lo general, los servidores controladores de dominio se configuran con una dirección IP fija.

! Atención: es recomendable realizar la creación del dominio (y la mayoría de operaciones en Windows Server) mediante PowerShell, ya que tenemos mayor control de que está sucediendo y

también facilita la replicación y la automatización.

Dado que un Windows Server que va a hacer de controlador de dominio, utiliza generalmente IP fija, vamos a repasar los comandos PowerShell necesarios para gestionar esto.

Gestión de IP Fija con PowerShell (si procede)

En primer lugar, podemos obtener la lista de adaptadores de red con el comando

```
Get-NetAdapter
```

Con ello, por ejemplo, podemos consultar la IP de una interfaz de red con:

```
(Get-NetIPAddress -InterfaceAlias "NombreInterfaz").IPAddress
```

Si, por ejemplo, quisiéramos establecer una IP Fija, podríamos con:

```
New-NetIPAddress -InterfaceAlias "NombreInterfaz" -IPAddress "DirecciónIP"  
-PrefixLength "LongitudPrefijo" -DefaultGateway "PuertaDeEnlace"
```

Donde reemplazaríamos "NombreInterfaz" con el nombre de la interfaz obtenido en el paso anterior, "DirecciónIP" con la dirección IP que desees asignar, "LongitudPrefijo" con la longitud del prefijo de la máscara de subred (por ejemplo, 24 para una máscara de subred /24), y "PuertaDeEnlace" con la dirección IP de la puerta de enlace predeterminada.

Promoviendo Windows Server a controlador de dominio

Una vez configurada adecuadamente la red, promoveremos Windows Server a controlador de dominio. En primer lugar, instalaremos la función de "Servicios de dominio de Active Directory" en un servidor Windows Server. Esta función es necesaria para convertir el servidor en un controlador de dominio. Lo haremos con el comando:

```
Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools
```

Tras ello, promoveremos el servidor a controlador de dominio. Suponiendo que queramos crear un dominio llamado "serra.com" con nombre Netbios "SERRA", utilizaremos el siguiente comando:

```
Install-ADDSForest -DomainName "serra.com" -DomainNetbiosName "SERRA" -DomainMode  
"WinThreshold" -ForestMode "WinThreshold" -InstallDNS -Force
```

El comando **Install-ADDSForest** se utiliza para configurar un nuevo bosque de dominio en un servidor Windows Server y establecerlo como el primer controlador de dominio en ese dominio. El comando además establece el nombre del dominio, el modo de dominio y bosque, instalando el servicio DNS y forzando la ejecución sin solicitar confirmación adicional. Veamos la explicación de cada parámetro utilizado en el comando:

- **DomainName "serra.com"**: Especifica el nombre del dominio que se creará. En este caso, el dominio se llamará "serra.com". Reemplaza "serra.com" con el nombre de dominio deseado.
- **DomainNetbiosName "SERRA"**: Establece el nombre NetBIOS del dominio. El nombre NetBIOS es un nombre de 15 caracteres que se utiliza para identificar el dominio en entornos antiguos de Windows. En este caso, el nombre NetBIOS del dominio será "SERRA". Puedes cambiarlo según tus preferencias, pero ten en cuenta que debe cumplir con las restricciones de nombres NetBIOS.
- **DomainMode "WinThreshold"**: Especifica el modo de dominio. El valor "WinThreshold" se refiere a Windows Server 2016 y versiones posteriores. Esto indica que el dominio funcionará en el nivel funcional de dominio compatible con Windows Server 2016. Si

deseas utilizar otro nivel funcional, puedes elegir un valor adecuado para tu entorno.

- **-ForestMode "WinThreshold":** Indica el modo de bosque. Al igual que el parámetro -DomainMode, el valor "WinThreshold" establece el nivel funcional del bosque compatible con Windows Server 2016. Puedes ajustar este valor según tus necesidades y la compatibilidad requerida con otras versiones de Windows.
- **-InstallDNS:** Este parámetro indica que se debe instalar el servicio DNS (Domain Name System) en el controlador de dominio. DNS es esencial para la resolución de nombres en una infraestructura de dominio y se recomienda instalarlo junto con el controlador de dominio.
- **-Force:** Este parámetro permite forzar la ejecución del comando sin solicitar confirmación adicional. Úsalo con precaución, ya que evita que se realicen verificaciones adicionales antes de la instalación del dominio.

! **Atención:** utiliza este comando y otros que afecten a Windows sabiendo que esta haciendo y revisando previamente a ejecutarlo que todo sea correcto.

6.4 Introduciendo clientes Windows en un dominio: interfaz gráfica

Los clientes de un dominio suelen ser sistemas operativos como Windows Server 20xx (actuando como clientes), Windows 7, 8, 10 o 11. Para agregar un cliente al dominio, el cliente debe tener acceso de red al servidor. Luego, debemos modificar la configuración DNS del cliente para que utilice un servidor DNS capaz de resolver los nombres asociados al dominio al que desea unirse.

! **Atención:** generalmente, colocarás como IP del servidor DNS, la IP de Windows Server.

Después de configurar el DNS, se cambia el modo de trabajo del cliente de "Workstation" a "Dominio", indicando el nombre del dominio al que desea unirse.

Es importante mencionar que se deben ingresar las credenciales de un usuario del dominio que pertenezca al grupo "Administradores de controladores del dominio" para permitir la inclusión del cliente en el dominio. Para evitar confusiones con usuarios locales, se recomienda ingresar el identificador completo del usuario en el formato "NombreDominio\UsuarioAdmin" al momento de proporcionar las credenciales. **Si las credenciales son válidas y el proceso es exitoso, se deberá reiniciar el equipo para completar la unión al dominio.**

6.5 Introduciendo clientes Windows en un dominio: PowerShell

Igual que cuando añadimos un cliente desde interfaz gráfica, para agregar un cliente al dominio, el cliente debe tener acceso de red al servidor y utilizar un servidor DNS capaz de resolver los nombres asociados al dominio al que desea unirse.

Ya vimos como cambiar la IP con PowerShell en el apartado donde configuramos el servidor Windows Server. Si, además, queremos cambiar el servidor DNS de una interfaz, podemos usar el comando:

```
Set-DnsClientServerAddress -InterfaceAlias "NombreInterfaz" -ServerAddresses  
"ServidorDNS1", "ServidorDNS2"
```

Donde "ServidorDNS1" y "ServidorDNS2" son las IPs de los servidores DNS.

! **Atención:** generalmente, colocarás como IP del servidor DNS, la IP de Windows Server.

Tras ello, procedemos a unir al cliente al dominio usando el comando Add-Computer. Este comando permite unir un equipo cliente a un dominio específico. Un ejemplo de uso:

```
Add-Computer -DomainName "NombreDominio" -Credential "NombreDominio\UsuarioAdmin"
```


Donde:

- **DomainName "NombreDominio":** Especifica el nombre del dominio al que se desea unir el cliente. Reemplaza "NombreDominio" con el nombre del dominio correspondiente.
- **Credential "NombreDominio\UsuarioAdmin":** Indica las credenciales de un usuario del dominio que tenga los privilegios necesarios para unir el cliente al dominio. Reemplaza "NombreDominio" con el nombre del dominio y "UsuarioAdmin" con el nombre de usuario del administrador del dominio.

Una vez que se ejecuta el comando, el equipo cliente intentará unirse al dominio especificado utilizando las credenciales proporcionadas. **Si las credenciales son válidas y el proceso es exitoso, se deberá reiniciar el equipo para completar la unión al dominio.**

6.6 Añadir clientes GNU/Linux al dominio

Dado que la autenticación en Active Directory de Windows Server utiliza Kerberos y LDAP para establecer la autenticación y la comunicación con el dominio, es posible agregar clientes GNU/Linux a dominios Windows. Para ello, además de una configuración de red adecuada y una resolución de DNS correcta, existen varias herramientas disponibles que facilitan la unión de clientes Linux a un dominio Windows.

Una de las más populares es **SSSD (System Security Services Daemon)**. Su web oficial es <https://sssd.io/>. Esta herramienta proporciona un conjunto de servicios para integrar sistemas Linux con servicios de directorio, como Active Directory.


7. GESTIÓN DE DOMINIOS: GESTIÓN DE USUARIOS, GRUPOS Y UNIDADES ORGANIZATIVAS

7.1 Usuarios y grupos locales de una máquina

Los usuarios y grupos locales en una máquina **son aquellos que existen únicamente en esa máquina específica, ya sea que esté unida a un dominio o no.** Sin embargo, es importante destacar que en un entorno de dominio, el enfoque principal es utilizar usuarios y grupos del dominio para administrar y asignar permisos en toda la red.

En el caso de las máquinas unidas a un dominio, **se tiene la flexibilidad de agregar cuentas y grupos del dominio a los grupos locales de esa máquina.** Es decir, si tenemos el grupo local "GrupoLocal", podemos agregarle como miembro tanto un grupo del dominio llamado "GrupoDominio" como un usuario del dominio llamado "UsuarioDominio". Esto facilita las tareas administrativas al permitir que los permisos y accesos se administren de manera centralizada a través del dominio.

Al añadir cuentas y grupos del dominio a los grupos locales de una máquina, se puede otorgar acceso a recursos específicos de la máquina a usuarios y grupos del dominio. Esto simplifica la gestión de permisos, ya que no es necesario crear usuarios y grupos locales en cada máquina individualmente.

 **Importante:** al agregar cuentas y grupos del dominio a los grupos locales de una máquina, se deben considerar las configuraciones de seguridad y las políticas establecidas en el dominio. Esto garantiza que se respeten las restricciones y políticas de seguridad del dominio al otorgar permisos a usuarios y grupos en las máquinas locales.

7.2 Cuentas de usuario del dominio

Una cuenta de usuario es un objeto utilizado para identificar y autenticar a un usuario en un dominio. Es importante destacar que una cuenta de usuario no siempre está asociada a una persona física, ya que también puede estar vinculada a otros propósitos, como la ejecución de un programa o servicio específico.

Los objetos de las cuentas de usuario son fundamentales para permitir la autenticación de un usuario y, con base en su identidad, otorgar o denegar acceso a los recursos del dominio. Estas cuentas se utilizan para administrar y controlar los permisos de los usuarios en la red.

En la instalación de Windows Server 2022, se crean algunas cuentas por defecto, como la cuenta de “Administrador”.

! **Atención:** es importante revisar y gestionar adecuadamente las configuraciones y permisos de estas cuentas, según las necesidades y políticas de seguridad específicas de cada organización.

7.3 Grupos del dominio


Los grupos en el Directorio Activo son conjuntos de objetos que se administran como una única entidad, y su propósito principal es simplificar las tareas administrativas. Existen dos tipos de grupos en el Directorio Activo:

- **Grupos de distribución:** estos grupos se utilizan principalmente para la mensajería y funciones similares. Se crean para facilitar el envío de mensajes a un conjunto de usuarios.
- **Grupos de seguridad:** estos grupos son fundamentales en la administración del Directorio Activo y son aquellos que usaremos habitualmente durante el módulo. Estos que permiten definir el acceso a recursos mediante listas de control de acceso (ACLs). Los grupos de seguridad se utilizan para asignar permisos y controlar el acceso a objetos y recursos en el dominio.

Dentro de los grupos de seguridad, encontramos diferentes tipos de grupos según su alcance:

- **Grupos locales de dominio:** Estos grupos pueden contener cuentas de cualquier dominio, grupos globales de cualquier dominio, grupos universales de cualquier dominio y grupos locales de dominio del mismo dominio que el grupo local de dominio primario. Los permisos de estos grupos se aplican únicamente en el dominio al que pertenecen y su replicación se limita a ese dominio.
- **Grupos globales:** Estos grupos pueden contener cuentas y grupos globales del mismo dominio que el grupo global primario. Los permisos asignados a los grupos globales se extienden a cualquier dominio dentro del bosque al que pertenecen. La replicación de estos grupos se limita a su propio dominio.
- **Grupos universales:** Estos grupos pueden contener cuentas y grupos globales y universales de cualquier dominio dentro del bosque donde resida el grupo universal. Los permisos asignados a los grupos universales se aplican en cualquier dominio del bosque. Sin embargo, su replicación se extiende a todo el árbol del bosque, lo que puede generar un mayor tráfico de replicación. Por lo tanto, se recomienda su uso en redes con múltiples dominios donde sea necesario compartir recursos y permisos en todo el bosque.

Si quieres entender mejor como funcionan los grupos en Windows Server 2022, recomendamos <https://learn.microsoft.com/es-es/windows-server/identity/ad-ds/manage/understand-security-groups>

 **Importante:** utilizar el tipo de grupo adecuado según el alcance necesario nos permitirá lograr un mejor rendimiento y eficiencia en el Directorio Activo.

7.4 ¿Cuándo usar cada uno de los tipos de grupos de seguridad?

Es importante comprender las diferencias y usos adecuados de los diferentes tipos de grupos en el Directorio Activo para lograr una administración eficiente de permisos y accesos a recursos en el dominio. Aquí hay una explicación más detallada sobre cuándo utilizar cada tipo de grupo:

- **Grupos locales de dominio:**
 - **Uso recomendado:** Los grupos locales de dominio son ideales cuando se necesitan

asignar permisos y controlar el acceso a recursos dentro del mismo dominio.

- **Alcance limitado:** Estos grupos solo se aplican al dominio específico en el que se crean y su replicación se limita a ese dominio.
- **Ejemplo de uso:** Si tienes un recurso específico en un dominio y deseas conceder permisos a un grupo de usuarios dentro de ese dominio, puedes utilizar un grupo local de dominio.
- **Grupos globales:**
 - **Uso recomendado:** Los grupos globales son útiles cuando se requiere asignar permisos y controlar el acceso a recursos en diferentes dominios dentro del mismo bosque.
 - **Alcance extendido:** Los permisos asignados a los grupos globales se aplican a cualquier dominio dentro del bosque al que pertenecen.
 - **Ejemplo de uso:** Si tienes varios dominios en un bosque y deseas otorgar acceso a un recurso compartido a usuarios de diferentes dominios, puedes utilizar un grupo global para agrupar a esos usuarios.
- **Grupos universales:**
 - **Uso recomendado:** Los grupos universales son beneficiosos cuando se necesita compartir permisos y controlar el acceso a recursos en todo el bosque, especialmente en entornos con múltiples dominios.
 - **Alcance amplio:** Los permisos asignados a los grupos universales se aplican a cualquier dominio dentro del bosque y su replicación abarca todo el árbol del bosque.
 - **Ejemplo de uso:** Si tienes varios dominios en un bosque y necesitas otorgar permisos a usuarios de diferentes dominios para acceder a recursos en todo el bosque, puedes utilizar un grupo universal para gestionar esos permisos.

Es importante tener en cuenta que la elección del tipo de grupo adecuado depende del alcance necesario y las necesidades específicas de administración de permisos y accesos en tu entorno. Al seleccionar el tipo de grupo correcto, se logra un mejor rendimiento y eficiencia en la administración del Directorio Activo, asegurando que los usuarios adecuados tengan acceso a los recursos necesarios dentro del dominio.

! **Atención:** durante el curso, lo más habitual será utilizar grupos locales de dominio y en alguna ocasión grupos globales.

7.5 Gestión de usuarios: interfaz gráfica

Para gestionar usuarios en el Directorio Activo, puedes acceder a la herramienta "Usuarios y equipos de Active Directory" desde la ventana "Administrador del servidor".

En la sección "Users" de esta herramienta, podrás crear usuarios en el dominio. Al crear un usuario, se te solicitará proporcionar información como:

- **Nombre de inicio de sesión:** Es el nombre único que identificará al usuario en el dominio.
- **Contraseña:** Debes establecer una contraseña segura para el usuario.
- **Opciones marcables:** Aquí podrás seleccionar opciones adicionales, como "Debe cambiar la contraseña al siguiente inicio de sesión", "El usuario no puede cambiar la contraseña", "La contraseña nunca expira" o "Cuenta deshabilitada".

Una vez creada la cuenta, si haces clic con el botón derecho del ratón y seleccionas "Propiedades", accederás a más opciones de configuración para la cuenta. Algunas opciones destacadas incluyen:

- **Cambio de contraseña:** Permite cambiar la contraseña actual del usuario.
- **Horas de inicio de sesión:** Aquí puedes especificar las horas durante las cuales se permite el inicio de sesión con esta cuenta.

- **Equipos desde los que se puede iniciar sesión:** Puedes controlar desde qué equipos o estaciones de trabajo se permite al usuario iniciar sesión.
- **Visualización / Modificación de los grupos:** Esta opción te permite ver y modificar los grupos a los que pertenece el usuario, lo que influye en los permisos y accesos que tiene dentro del dominio.

7.6 Gestión de usuarios: PowerShell

La administración de usuarios en el Directorio Activo también se puede realizar de manera eficiente mediante PowerShell. A continuación, te mostraré cómo llevar a cabo algunas tareas comunes utilizando comandos de PowerShell:

Crear un usuario:

Puedes utilizar el comando `New-ADUser` para crear un nuevo usuario en el dominio. Por ejemplo:

```
New-ADUser -Name "NombreUsuario" -SamAccountName "SamAccountName" -UserPrincipalName "usuario@dominio.com" -Enabled $true -PasswordNeverExpires $true
```

Establecer una contraseña para un usuario:

Puedes utilizar el comando `Set-ADAccountPassword` para establecer una nueva contraseña para un usuario. Por ejemplo:

```
Set-ADAccountPassword -Identity "NombreUsuario" -NewPassword (ConvertTo-SecureString -AsPlainText "NuevaContraseña" -Force)
```

Cambiar opciones de cuenta de usuario:

Puedes utilizar el comando `Set-ADUser` para cambiar las opciones de cuenta de un usuario. Por ejemplo:

```
Set-ADUser -Identity "NombreUsuario" -ChangePasswordAtLogon $true -CannotChangePassword $true -Enabled $false
```

Obtener información de un usuario:

Puedes utilizar el comando `Get-ADUser` para obtener información detallada sobre un usuario en el dominio. Por ejemplo:

```
Get-ADUser -Identity "NombreUsuario"
```

Estos son solo algunos ejemplos de cómo administrar usuarios en el Directorio Activo utilizando PowerShell. PowerShell proporciona una amplia gama de cmdlets específicos para la administración del Directorio Activo, lo que te permite automatizar tareas, aplicar configuraciones avanzadas y gestionar eficientemente las cuentas de usuario en el dominio.

7.7 Gestión de grupos: interfaz gráfica

Para administrar grupos en el Directorio Activo, puedes acceder a la herramienta "Usuarios y equipos de Active Directory" desde la ventana "Administrador del servidor".

En la sección "Users" de esta herramienta, podrás crear grupos en el dominio. Al crear un grupo, se te solicitará proporcionar información como:

- **Nombre:** es el nombre único que identificará al grupo en el dominio.
- **Tipo del grupo:** debes especificar si el grupo es de distribución o de seguridad. Los grupos de distribución se utilizan principalmente para funciones como la mensajería, mientras que los grupos de seguridad se utilizan para administrar permisos y controlar el acceso a recursos. Durante el curso, **normalmente utilizaremos grupos de seguridad**.
- **Ámbito:** Aquí deberás seleccionar el ámbito del grupo, que puede ser local, global o universal.

Una vez creado el grupo, si haces clic con el botón derecho del ratón y seleccionas "Propiedades", accederás a más opciones de configuración para el grupo. Algunas opciones destacadas incluyen:

- **Miembros:** Esta opción te permite agregar miembros al grupo, ya sean cuentas de usuario u otros grupos. Puedes seleccionar los usuarios o grupos relevantes y agregarlos al grupo en esta sección.
- **Miembro de:** Aquí se muestra una lista de los grupos de los cuales el grupo actual es miembro. Esto te permite visualizar y administrar las relaciones de pertenencia entre los grupos.

7.8 Gestión de grupos: PowerShell

La administración de grupos en el Directorio Activo también se puede realizar de manera eficiente mediante PowerShell. A continuación, te mostraré cómo llevar a cabo algunas tareas comunes utilizando comandos de PowerShell:

Crear un grupo:

Puedes utilizar el comando New-ADGroup para crear un nuevo grupo en el dominio. Por ejemplo:

```
New-ADGroup -Name "NombreGrupo" -GroupScope Global -GroupCategory Security
```

Agregar miembros a un grupo:

Puedes utilizar el comando Add-ADGroupMember para agregar miembros a un grupo existente. Por ejemplo:

```
Add-ADGroupMember -Identity "NombreGrupo" -Members "Usuario1", "Usuario2"
```

Obtener información de un grupo:

Puedes utilizar el comando Get-ADGroup para obtener información detallada sobre un grupo en el dominio. Por ejemplo:

```
Get-ADGroup -Identity "NombreGrupo"
```

Modificar propiedades de un grupo:

Puedes utilizar el comando Set-ADGroup para modificar las propiedades de un grupo existente. Por ejemplo:

```
Set-ADGroup -Identity "NombreGrupo" -Description "Nueva descripción del grupo"
```

Estos son solo algunos ejemplos de cómo administrar grupos en el Directorio Activo utilizando PowerShell, pero existen muchas más posibilidades.

7.9 Gestión de unidades organizativas: interfaz gráfica

Para administrar unidades organizativas en el Directorio Activo, puedes acceder a la herramienta "Usuarios y equipos de Active Directory" desde la ventana "Administrador del servidor".

En la sección "Users" de esta herramienta, podrás crear unidades organizativas dentro de las cuales puedes organizar y administrar objetos y otras unidades organizativas. Para crear una unidad organizativa, sigue estos pasos:

- Haz clic con el botón derecho del ratón en la ubicación donde deseas crear la unidad organizativa, ya sea en el nivel raíz o dentro de otra unidad organizativa existente.
- Selecciona "Nueva" y luego elige "Unidad Organizativa" en el menú desplegable.
- Asigna un nombre significativo a la unidad organizativa y haz clic en "Aceptar" para crearla.

Una vez creada la unidad organizativa, puedes comenzar a organizar los objetos y otras unidades organizativas dentro de ella. Para hacerlo, simplemente arrastra y suelta los objetos desde la sección "Users" o desde otras unidades organizativas.

Además de la creación y organización de unidades organizativas, la herramienta "Usuarios y equipos de Active Directory" también te permite acceder a varias opciones de configuración y administración de unidades organizativas. Al hacer clic con el botón derecho del ratón en una unidad organizativa y seleccionar "Propiedades", podrás acceder a opciones como:

- **Seguridad:** Permite configurar los permisos y los niveles de acceso para la unidad organizativa.
- **Políticas de grupo:** Permite aplicar políticas específicas a la unidad organizativa y a los objetos contenidos en ella.
- **Ubicación:** Muestra la ruta completa de la unidad organizativa dentro de la estructura del Directorio Activo.

7.10 Gestión de unidades organizativas: PowerShell

La administración de unidades organizativas en el Directorio Activo también se puede realizar de manera eficiente mediante PowerShell. A continuación, algunos ejemplos:

Crear una unidad organizativa:

Puedes utilizar el comando `New-ADOrganizationalUnit` para crear una nueva unidad organizativa en el dominio. Por ejemplo:

```
New-ADOrganizationalUnit -Name "NombreUnidadOrganizativa" -Path  
"OU=UnidadesOrganizativas,DC=dominio,DC=com"
```

Mover objetos a una unidad organizativa:

Puedes utilizar el comando `Move-ADObject` para mover objetos, como usuarios, grupos o equipos, a una unidad organizativa específica. Por ejemplo:

```
Move-ADObject -Identity "CN=Usuario1,OU=UnidadesOrganizativas,DC=dominio,DC=com"  
-TargetPath "OU=NuevaUnidadOrganizativa,DC=dominio,DC=com"
```

Obtener información de una unidad organizativa:

Puedes utilizar el comando `Get-ADOrganizationalUnit` para obtener información detallada sobre una unidad organizativa en el dominio. Por ejemplo:

```
Get-ADOrganizationalUnit -Identity "OU=UnidadesOrganizativas,DC=dominio,DC=com"
```

Modificar propiedades de una unidad organizativa:


Puedes utilizar el comando `Set-ADOrganizationalUnit` para modificar las propiedades de una unidad organizativa existente. Por ejemplo:

```
Set-ADOrganizationalUnit -Identity "OU=UnidadesOrganizativas,DC=dominio,DC=com"  
-Description "Nueva descripción de la unidad organizativa"
```

Estos son solo algunos ejemplos de cómo administrar unidades organizativas en el Directorio Activo utilizando PowerShell, pero existen muchas más posibilidades.

8. GPO (GROUP POLICY OBJECTS)

Las GPO, o "Group Policy Objects" en inglés, son un conjunto de reglas y configuraciones de política de seguridad que se utilizan en sistemas operativos Windows para administrar y controlar la configuración de usuarios y computadoras en una red. Estas políticas permiten a los administradores de sistemas establecer y aplicar políticas de seguridad, configuración y comportamiento en múltiples dispositivos y usuarios de manera centralizada, generalmente un servidor con el servicio de Active Directory.

 **Importante:** cabe destacar que las GPO se pueden respaldar y restaurar, lo que facilita la recuperación de configuraciones de políticas en caso de errores o pérdida de datos.

8.1 ¿Dónde se aplican las GPO?

Las GPO contienen una serie de configuraciones de políticas que se pueden aplicar a diferentes objetos, como usuarios, grupos de usuarios, computadoras o grupos de computadoras. Estas configuraciones pueden afectar el comportamiento del sistema operativo y las aplicaciones en esos objetos. Al aplicar las GPO, además, deben tenerse en cuenta los siguientes aspectos:

- **Herencia y Prioridad:** Las GPO se aplican a través de una estructura jerárquica. Las políticas pueden heredarse de niveles superiores, como el dominio o la unidad organizativa (OU), y luego se pueden aplicar o anular en niveles inferiores. Las GPO también tienen una prioridad que determina cuál tiene la última palabra en caso de conflictos.
- **Aplicación Selectiva:** Las GPO pueden aplicarse selectivamente a objetos específicos, lo que permite una gran flexibilidad en la administración. Por ejemplo, se pueden aplicar políticas diferentes a diferentes grupos de usuarios o computadoras dentro de la red.

8.2 Gestión de GPOs: interfaz gráfica

Para administrar las Directivas de Grupo (GPO) en el Directorio Activo, puedes utilizar la herramienta "Editor de administración de directivas de grupo" (GPMC) a través de una interfaz gráfica. A continuación, te mostraré cómo llevar a cabo algunas tareas comunes utilizando la interfaz gráfica del GPMC.

En primer lugar, deberás abrir el "Editor de administración de directivas de grupo". Puedes hacerlo accediendo a, "Inicio", allí en "Herramientas administrativas" y allí en "Editor de administración de directivas de grupo". Una vez en el editor, algunas de las acciones que se pueden realizar son:

- **Crear una nueva GPO:**
 - Haz clic con el botón derecho del ratón en la carpeta "Directivas de grupo de bosque" o "Directivas de grupo de dominio" en la jerarquía de navegación.
 - Selecciona "Crear GPO en este dominio y vincularlo aquí".
 - Asigna un nombre descriptivo a la nueva GPO y haz clic en "Aceptar".
- **Configurar una GPO:**
 - Una vez creada la GPO, puedes configurarla según tus necesidades. Para ello, haz clic con el botón derecho del ratón en la GPO y selecciona "Editar". Se abrirá el "Editor de administración de directivas de grupo" donde podrás definir las políticas y configuraciones que deseas aplicar.
- **Vincular una GPO a un contenedor:**
 - Para aplicar una GPO a un contenedor específico, como un dominio, una unidad organizativa o un sitio.
 - En la jerarquía de navegación del GPMC, selecciona el contenedor donde deseas vincular la GPO.
 - Haz clic con el botón derecho del ratón y elige "Vincular una GPO existente".
 - Selecciona la GPO que deseas vincular y haz clic en "Aceptar".
- **Administrar las configuraciones de una GPO:**
 - Al editar una GPO, podrás acceder a diferentes categorías de configuración, como "Configuración de usuario" y "Configuración de equipo". Estas categorías te permiten definir las políticas específicas que se aplicarán a los usuarios y equipos dentro del ámbito de la GPO.
- **Aplicar una GPO:**
 - Después de configurar una GPO, puedes aplicarla en el dominio o en un contenedor específico seleccionando la GPO y haciendo clic con el botón derecho del ratón en

"Aplicar" o utilizando la opción "Forzar actualización de directivas" para que los cambios se apliquen de inmediato.

8.3 Gestión de GPOs: PowerShell

La administración de las Directivas de Grupo (GPO) en el Directorio Activo también se puede realizar de manera eficiente mediante PowerShell. A continuación, algunos ejemplos cómo llevar a cabo algunas tareas comunes utilizando comandos de PowerShell:

Crear una nueva GPO:

Puedes utilizar el comando New-GPO para crear una nueva GPO en el Directorio Activo. Por ejemplo:

```
New-GPO -Name "NombreGPO"
```

Configurar una GPO:

Una vez creada la GPO, puedes configurarla según tus necesidades utilizando el comando Set-GPRegistryValue, Set-GPRegistryValue, Set-GPPermission, entre otros. Por ejemplo, para establecer una configuración de registro en la GPO:

```
Set-GPRegistryValue -Name "NombreGPO" -Key "HKEY_CURRENT_USER\Software\Ejemplo"  
-ValueName "EjemploConfig" -Value 1
```

Vincular una GPO a un contenedor:

Puedes utilizar el comando New-GPLink para vincular una GPO a un contenedor específico, como un dominio, una unidad organizativa o un sitio. Por ejemplo:

```
New-GPLink -Name "NombreGPO" -Target "OU=UnidadOrganizativa,DC=dominio,DC=com"
```

Obtener información de una GPO:

Puedes utilizar el comando Get-GPO para obtener información detallada sobre una GPO en el Directorio Activo. Por ejemplo:

```
Get-GPO -Name "NombreGPO"
```

Aplicar una GPO:

Después de configurar una GPO, puedes aplicarla utilizando el comando Invoke-GPUUpdate. Por ejemplo, para aplicar la GPO en un equipo remoto:

```
Invoke-GPUUpdate -Computer "NombreEquipo" -Force
```

Estos son algunos ejemplos de como gestionar las distintas GPOs usando PowerShell.

9. RECOMENDACIONES DE SEGURIDAD AL ADMINISTRAR WINDOWS SERVER

La administración de la seguridad en Windows Server es una tarea crítica para garantizar la protección de los datos y la continuidad de los servicios en un entorno empresarial.

A continuación, damos algunas sugerencias genéricas que deben ser tenidas en cuenta al administrar un servidor Windows Server:

- **Actualizaciones y Parches:** Mantén el sistema operativo y todas las aplicaciones actualizadas con los últimos parches de seguridad. Configura las actualizaciones automáticas o implementa un proceso regular de parcheo.
- **Firewall:** Habilita y configura el Firewall de Windows para bloquear tráfico no deseado y limitar la exposición de servicios no esenciales a la red.
- **Seguridad Física:** Asegúrate de que los servidores estén físicamente protegidos en un lugar seguro y que solo el personal autorizado tenga acceso físico a ellos.

- **Políticas de Contraseña:** Establece políticas de contraseñas fuertes que incluyan longitudes mínimas, complejidad y cambios regulares de contraseñas. Considera el uso de autenticación multifactor (MFA) cuando sea posible.
- **Control de Acceso:** Configura permisos y derechos de acceso adecuados para que solo los usuarios y grupos autorizados puedan acceder a recursos y carpetas compartidas.
- **Auditoría de Seguridad:** Habilita y configura la auditoría de seguridad para realizar un seguimiento de los eventos importantes, como inicios de sesión fallidos, acceso a archivos y cambios en la configuración.
- **Directivas de Grupo (GPO):** Utiliza GPO para aplicar políticas de seguridad en toda la red, incluyendo restricciones de ejecución de aplicaciones, políticas de contraseñas y restricciones de acceso a dispositivos.
- **Cifrado de Datos:** Implementa el cifrado de datos para proteger información confidencial, especialmente en unidades y comunicaciones sensibles.
- **Respaldo y Recuperación:** Establece un plan de respaldo y recuperación eficaz para proteger los datos contra pérdida o daño. Prueba regularmente la recuperación de datos.
- **Detección y Prevención de Intrusiones:** Utiliza herramientas y software de detección y prevención de intrusos (IDS/IPS) para identificar y bloquear actividades sospechosas en la red. Algunos de los software de este tipo más conocidos son:
 - <https://www.snort.org/>
 - <https://suricata.io/>
 - <https://securityonionsolutions.com/>
- **Acceso Remoto Seguro:** Limita y asegura el acceso remoto al servidor. Considera el uso de conexiones VPN y, cuando sea posible, restringe el acceso a direcciones IP específicas.
- **Monitoreo de Seguridad:** Implementa soluciones de monitoreo y análisis de registros para detectar eventos de seguridad y comportamientos anómalos.

10. MATERIALES DE APOYO/AMPLIACIÓN

Para los procesos descritos, puedes utilizar como material de apoyo el libro gratuito y con licencia libre “Sistemas Operativos en Red, 2ª edición” de SomeBooks.es. El libro está disponible en la siguiente dirección <http://somebooks.es/sistemas-operativos-red-2a-edicion/>

En concreto, para esta unidad, pueden ser útiles los capítulos:

- Capítulo 2: Instalación de Windows Server
- Capítulo 3: Tareas administrativas en Windows Server
- Capítulo 6: Dominios en Windows Server

11. BIBLIOGRAFÍA

[1] “Sistemas Operativos en Red, 2ª edición” de SomeBooks. El libro está disponible en la siguiente dirección <http://somebooks.es/sistemas-operativos-red-2a-edicion/>

[2] Mastering Windows Server 2022 - Fourth Edition, Jordan Krause

[3] Introducción a Windows Server 2022

<https://learn.microsoft.com/es-es/windows-server/get-started/get-started-with-windows-server>

[4] Grupos en Windows Server 2022

<https://learn.microsoft.com/es-es/windows-server/identity/ad-ds/manage/understand-security-gr>

[oups](#)