# Administración de dominios (Implantación de sistemas operativos)

## Estructura cliente-servidor

La estructura cliente-servidor es un modelo de arquitectura de red que organiza las tareas y las cargas de trabajo entre los proveedores de recursos o servicios, llamados servidores, y los solicitantes de servicios, conocidos como clientes. Este modelo es fundamental en la informática y las redes, y se utiliza en una variedad de aplicaciones, desde servicios web hasta bases de datos y sistemas de comunicación. A continuación, se detalla de manera extensa la estructura cliente-servidor, sus componentes, funcionamiento, ventajas, desventajas y ejemplos prácticos.

## Definición y conceptos básicos

En el modelo cliente-servidor, la funcionalidad de la aplicación se divide entre dos entidades principales:

1. **Cliente**: Es el componente que solicita servicios o recursos. Los clientes son generalmente dispositivos de usuario final, como computadoras, teléfonos inteligentes o tablets, que interactúan con los servidores para realizar tareas específicas.
2. **Servidor**: Es el componente que provee servicios o recursos a los clientes. Los servidores pueden ser sistemas de hardware o software que responden a las solicitudes de los clientes y les proporcionan los datos o servicios requeridos.

## Funcionamiento del modelo cliente-servidor

El funcionamiento básico del modelo cliente-servidor se puede describir en los siguientes pasos:

1. **Solicitud del cliente**: El cliente inicia una solicitud para un recurso o servicio. Esto podría ser una petición de una página web, el acceso a una base de datos, o la solicitud de una operación en una aplicación.
2. **Procesamiento del servidor**: El servidor recibe la solicitud del cliente, la procesa, y genera una respuesta. Este procesamiento puede incluir la consulta a bases de datos, la ejecución de cálculos, o la recuperación de archivos.
3. **Respuesta del servidor**: El servidor envía la respuesta al cliente. Esta respuesta puede ser una página web renderizada, datos en formato JSON, resultados de una consulta, o cualquier otro tipo de recurso solicitado.

## Componentes del modelo cliente-servidor

El modelo cliente-servidor puede incluir varios componentes adicionales que ayudan en la comunicación y procesamiento de solicitudes:

1. **Middleware**: Software intermediario que facilita la comunicación y gestión de datos entre los clientes y servidores. Ejemplos comunes incluyen servidores web, servidores de aplicaciones y servicios de mensajería.
2. **Protocolos de comunicación**: Reglas y estándares que gobiernan el intercambio de datos entre clientes y servidores. Ejemplos incluyen HTTP/HTTPS para la web, FTP para transferencia de archivos, y SQL para bases de datos.
3. **Bases de datos**: Sistemas que almacenan y gestionan datos

que pueden ser solicitados por clientes. Los servidores de bases de datos son cruciales en muchas aplicaciones cliente-servidor.
4. **Caché**: Sistemas que almacenan temporalmente los datos frecuentemente solicitados para mejorar el rendimiento y reducir la carga en los servidores.

## Ventajas del modelo cliente-servidor

El modelo cliente-servidor ofrece varias ventajas:

1. **Centralización**: Los recursos y servicios están centralizados en servidores, lo que facilita la administración, mantenimiento y seguridad.
2. **Escalabilidad**: Es posible escalar los servidores para manejar un mayor número de solicitudes mediante la adición de hardware o la implementación de balanceadores de carga.
3. **Mantenimiento sencillo**: Las actualizaciones y mejoras se pueden implementar en el servidor sin necesidad de modificar los clientes, siempre que los clientes sigan utilizando la misma interfaz de comunicación.
4. **Seguridad**: La centralización permite un control más riguroso sobre el acceso a los datos y servicios, facilitando la implementación de políticas de seguridad.

## Desventajas del modelo cliente-servidor

A pesar de sus ventajas, el modelo cliente-servidor también presenta ciertas desventajas:

1. **Costos de infraestructura**: La implementación y mantenimiento de servidores robustos y seguros puede ser costosa.
2. **Punto único de falla**: Si el servidor central falla, todos los clientes dependientes de él también se verán

afectados. La redundancia y los sistemas de respaldo son cruciales para mitigar este riesgo.
3. **Latencia**: La comunicación entre clientes y servidores puede introducir latencia, especialmente si los servidores están ubicados geográficamente lejos de los clientes.

---

## Ejemplos

### Carpetas compartidas

Las carpetas compartidas son una aplicación concreta del modelo cliente-servidor, especialmente en el ámbito de la gestión de archivos y la colaboración en red. En este sistema, un servidor de archivos actúa como el núcleo central donde se almacenan las carpetas y archivos que se compartirán entre los usuarios. Este servidor no solo almacena los datos, sino que también gestiona los permisos de acceso, asegurando que solo los usuarios autorizados puedan acceder o modificar los archivos.

Cuando un usuario quiere acceder a una carpeta compartida, utiliza su dispositivo, que actúa como cliente, para enviar una solicitud al servidor. El servidor procesa esta solicitud, verificando las credenciales del usuario y los permisos asociados a la carpeta solicitada. Si el acceso está permitido, el servidor envía los datos necesarios al cliente, permitiendo al usuario ver, modificar o añadir archivos en la carpeta compartida.

Este sistema ofrece múltiples beneficios. Uno de los más importantes es la centralización de los datos, lo que facilita la administración y el respaldo de la información. Además, la colaboración se vuelve más eficiente, ya que varios usuarios pueden trabajar en los mismos archivos simultáneamente, con la certeza de que siempre estarán accediendo a la versión más

reciente del documento.

Otro beneficio significativo es la capacidad de establecer permisos detallados. Los administradores pueden definir quién puede ver, editar o eliminar archivos, lo que mejora la seguridad y asegura que solo las personas adecuadas tengan acceso a la información sensible.

Sin embargo, las carpetas compartidas también presentan ciertos desafíos. La dependencia de un servidor central significa que, si este servidor falla, el acceso a las carpetas compartidas se interrumpe para todos los usuarios. Por lo tanto, es crucial implementar redundancias y copias de seguridad para minimizar el riesgo de pérdida de datos o interrupciones del servicio. Además, la gestión de permisos puede volverse compleja en organizaciones grandes, requiriendo un sistema bien planificado para evitar errores y garantizar la seguridad.

En términos prácticos, las carpetas compartidas se utilizan en una amplia variedad de contextos. En el entorno empresarial, permiten a los equipos de trabajo colaborar en proyectos, compartir documentos y centralizar la información del proyecto. En el ámbito educativo, facilitan el intercambio de materiales entre profesores y estudiantes, y en el hogar, pueden utilizarse para compartir fotos, videos y otros archivos personales entre los miembros de la familia.

Un ejemplo común de uso de carpetas compartidas es a través de servicios de almacenamiento en la nube como Google Drive, Dropbox o OneDrive. Estos servicios proporcionan interfaces fáciles de usar para que los clientes accedan a carpetas compartidas desde cualquier lugar con conexión a Internet. Los servidores de estos servicios gestionan las solicitudes de los clientes, asegurando que los datos se transmitan de manera segura y eficiente.

- https://www.jesusninoc.com/02/11/ejercicios-de-powershel

l-obtener-informacion-sobre-los-dispositivos-de-almacenamiento/

- https://www.jesusninoc.com/06/14/conectarse-a-una-carpeta-compartida-con-powershell/
- https://www.jesusninoc.com/04/30/ejercicios-de-powershell-crear-una-carpeta-compartida-mapearla-y-utilizarla/
- https://www.jesusninoc.com/03/17/ejercicios-de-powershell-mapear-varias-unidades-que-se-encuentran-en-un-fichero/
- https://www.jesusninoc.com/02/16/ejercicios-de-powershell-mapear-varios-recursos-unidades-creando-tambien-las-carpetas-y-compartiendo-leyendo-de-un-fichero-el-nombre-el-mismo-nombre-para-todas-las-operaciones-de-la-carpeta-que/

**Pruebas de concepto**

- https://www.jesusninoc.com/02/19/ejercicios-de-powershell-enviar-el-codigo-de-una-pagina-web-mediante-udp-entre-un-cliente-y-un-servidor-despues-de-realizar-una-comprobacion-del-nombre-de-usuario/
- https://www.jesusninoc.com/05/22/sistema-que-permite-almacenar-en-un-fichero-los-credenciales-de-usuario-de-windows-haciendo-una-peticion-a-un-servidor-web-mediante-el-metodo-post-despues-obtener-el-password-en-texto-plano/
- https://www.jesusninoc.com/02/19/ejercicios-de-powershell-uso-y-manipulacion-de-credenciales/
- https://www.jesusninoc.com/02/19/ejercicios-de-powershell-enviar-credenciales-entre-un-cliente-y-un-servidor-por-udp/
- https://www.jesusninoc.com/02/19/ejercicios-de-powershell-enviar-credenciales-entre-un-cliente-y-un-servidor-por-udp-y-ejecutar-una-aplicacion-en-el-servidor-con-dichos-credenciales/

---

### Ejercicios

- https://www.jesusninoc.com/02/16/ejercicios-de-powershell-crear-recursos-unidades-con-new-psdrive-de-para-varias-carpetas-compartidas-leyendo-de-un-fichero-las-rutas-compartidas-y-los-nombres-de-los-recursos-que-se-van-a-crear/
- https://www.jesusninoc.com/02/16/ejercicios-de-powershell-mapear-varios-recursos-unidades-creando-tambien-las-carpetas-y-compartiendo-leyendo-de-un-fichero-el-nombre-el-mismo-nombre-para-todas-las-operaciones-de-la-carpeta-que/

---

### Más información

- https://www.jesusninoc.com/07/11/11-gestion-del-directorio-activo-nivel-intermedio/

---

# Protocolo LDAP

El Protocolo de Acceso Ligero a Directorios (LDAP, por sus siglas en inglés) es un estándar abierto para el acceso y mantenimiento de servicios de directorio distribuido sobre una red IP. LDAP es ampliamente utilizado para autenticar usuarios y acceder a información en un entorno de red, proporcionando una forma eficiente y estandarizada de manejar la autenticación, la autorización y la búsqueda de información en sistemas distribuidos.

# Origen y evolución del LDAP

LDAP fue desarrollado en la década de 1990 como una versión simplificada del Protocolo de Acceso a Directorios X.500, que era complejo y requería una gran cantidad de recursos. LDAP se diseñó para ser más ligero y fácil de implementar, lo que llevó a su rápida adopción en la industria. Su diseño permite que los clientes accedan a los datos almacenados en servidores de directorio de manera rápida y eficiente, facilitando la administración de identidades y recursos en redes grandes y heterogéneas.

# Funcionamiento de LDAP

El funcionamiento de LDAP se basa en un modelo cliente-servidor, donde los clientes envían solicitudes de acceso a los datos y los servidores responden a esas solicitudes. Aquí se describen los componentes y procesos clave involucrados:

## Componentes

1. **Cliente LDAP**: Una aplicación o dispositivo que envía solicitudes al servidor LDAP para obtener información o autenticar usuarios.
2. **Servidor LDAP**: Un sistema que almacena la información del directorio y responde a las solicitudes del cliente. Este servidor puede manejar millones de entradas y es altamente optimizado para búsquedas rápidas y eficientes.
3. **Directorio LDAP**: Una base de datos especializada que almacena información estructurada en una jerarquía de objetos, como usuarios, grupos, computadoras y otros recursos de red.

## Operaciones básicas

1. **Bind**: Autentica al cliente con el servidor LDAP. Es el

primer paso en cualquier comunicación LDAP, estableciendo la identidad del cliente.
2. **Search**: Permite al cliente buscar entradas en el directorio que coincidan con ciertos criterios.
3. **Compare**: Verifica si una entrada específica contiene un atributo con un valor determinado.
4. **Modify**: Permite al cliente modificar los atributos de una entrada existente.
5. **Add**: Agrega una nueva entrada al directorio.
6. **Delete**: Elimina una entrada del directorio.
7. **Unbind**: Termina la sesión LDAP.

## Beneficios de LDAP

1. **Estandarización**: LDAP es un estándar abierto, lo que asegura interoperabilidad entre diferentes sistemas y aplicaciones.
2. **Escalabilidad**: LDAP está diseñado para manejar grandes volúmenes de consultas y datos, lo que lo hace adecuado para organizaciones grandes.
3. **Flexibilidad**: Permite la integración con diversos sistemas y aplicaciones, incluyendo sistemas operativos, aplicaciones web y servicios de red.
4. **Seguridad**: Soporta métodos de autenticación y cifrado que aseguran la privacidad y la integridad de los datos transmitidos.

## Desafíos y consideraciones

A pesar de sus ventajas, LDAP presenta algunos desafíos y consideraciones que deben tenerse en cuenta:

1. **Complejidad de configuración**: Configurar y mantener un servidor LDAP puede ser complejo, especialmente en entornos grandes o heterogéneos.

2. **Gestión de seguridad**: Es crucial asegurar que las políticas de seguridad sean rigurosas para proteger la información sensible almacenada en el directorio.
3. **Dependencia de la red**: Dado que LDAP opera sobre redes IP, la latencia y la disponibilidad de la red pueden afectar su rendimiento.

## Aplicaciones prácticas

LDAP se utiliza en una amplia variedad de aplicaciones y entornos. En las empresas, es comúnmente utilizado para la autenticación de usuarios en sistemas de inicio de sesión único (SSO), donde los usuarios pueden acceder a múltiples servicios con una sola autenticación. También se emplea para gestionar y organizar información de recursos de red, como computadoras y dispositivos, en sistemas de administración de redes.

En aplicaciones web, LDAP puede integrarse con servidores web y aplicaciones para proporcionar autenticación centralizada y control de acceso. Por ejemplo, muchos sistemas de gestión de contenido y portales web utilizan LDAP para manejar cuentas de usuario y permisos de acceso.

## Ejemplos de implementaciones de LDAP

Algunas implementaciones populares de LDAP incluyen:

1. **OpenLDAP**: Una implementación de código abierto muy utilizada en sistemas Linux y Unix.
2. **Microsoft Active Directory**: Un servicio de directorio que utiliza LDAP para gestionar identidades y recursos en entornos Windows.
3. **Apache Directory Server**: Un servidor LDAP de código abierto desarrollado por la Apache Software Foundation.

---

### Ejercicios

- https://www.jesusninoc.com/2018/05/16/utilizar-un-filtro-ldap-para-localizar-un-usuario/

---

### Más información

- https://www.jesusninoc.com/07/11/11-gestion-del-directorio-activo-nivel-intermedio/

---

# Concepto de dominio. Subdominios. Requisitos necesarios para montar un dominio

Un dominio es una forma de identificar y organizar recursos y servicios en una red, generalmente en Internet. Un dominio representa una dirección única que los usuarios pueden utilizar para acceder a un sitio web o a servicios específicos de una organización. El Sistema de Nombres de Dominio (DNS) es el encargado de traducir estos nombres de dominio en direcciones IP que las computadoras utilizan para localizarse y comunicarse entre sí en la red.

Por ejemplo, en el dominio «example.com»:

- «example» es el nombre del dominio.
- «.com» es el dominio de nivel superior (TLD, por sus siglas en inglés).

Un subdominio es una subdivisión de un dominio principal. Los subdominios permiten organizar y gestionar diferentes secciones o servicios de un sitio web bajo un mismo dominio principal. Los subdominios heredan parte del nombre del dominio principal y añaden una parte adicional para especificar un área particular. Por ejemplo, en «blog.example.com»:

- «blog» es el subdominio.
- «example.com» es el dominio principal.

Los subdominios son útiles para separar servicios distintos dentro de una misma organización, como «mail.example.com» para correo electrónico y «shop.example.com» para una tienda en línea.

## Dominios en Active Directory

En el contexto de Active Directory (AD), un dominio es una colección estructurada de objetos como usuarios, grupos y dispositivos, que comparten una base de datos de directorio y una política de seguridad común. Un dominio en Active Directory proporciona un marco centralizado para la administración y control de estos objetos, facilitando la implementación de políticas de seguridad y la gestión de recursos en una red corporativa.

## Subdominios en Active Directory

Un subdominio en Active Directory es un dominio secundario que se deriva de un dominio principal (o raíz). Los subdominios permiten una estructura jerárquica y segmentada de la red, donde cada subdominio puede representar una unidad organizativa diferente, como departamentos, ubicaciones geográficas o divisiones específicas de la empresa. Cada subdominio puede tener su propia base de datos de directorio y políticas, pero sigue siendo parte del dominio principal,

permitiendo así una administración centralizada y coherente.

Por ejemplo, en una organización con el dominio principal «empresa.com», se pueden crear subdominios como «ventas.empresa.com» y «soporte.empresa.com» para gestionar mejor las necesidades específicas de cada departamento.

## Requisitos necesarios para montar un dominio en Active Directory

Configurar un dominio en Active Directory implica varios pasos y requisitos específicos. A continuación se detallan los elementos necesarios para implementar y gestionar un dominio AD:

1. **Preparación del entorno de red**:
    - **Evaluación de la infraestructura**: Asegúrese de que su infraestructura de red cumpla con los requisitos para implementar Active Directory, incluyendo hardware adecuado, topología de red y configuraciones de seguridad.
    - **Sistema operativo**: Debe contar con servidores que ejecuten una versión compatible de Windows Server (como Windows Server 2016, 2019 o 2022).

2. **Configuración del servidor DNS**:
    - **DNS integrado con Active Directory**: Active Directory depende de DNS para resolver nombres de dominio y localizar recursos. Configure el servidor DNS para que sea compatible con Active Directory.
    - **Zonas y registros DNS**: Cree las zonas y registros DNS necesarios para el dominio, incluyendo registros A, SRV y otros registros de servicio necesarios para la localización y autenticación de controladores de dominio.

3. **Instalación de Active Directory**:
    - **Promover el servidor a Controlador de Dominio**: Utilice el asistente de instalación de Active Directory Domain Services (AD DS) para promover su servidor a controlador de dominio. Esto incluye la creación de la base de datos de directorio y la configuración de las políticas de seguridad iniciales.
    - **Configuración de la forest y el dominio**: Defina la estructura de la forest y el dominio. La forest es la estructura más alta en Active Directory y puede contener múltiples dominios.

4. **Administración de usuarios y grupos**:
    - **Creación de cuentas de usuario y grupos**: Configure cuentas de usuario y grupos dentro del dominio para facilitar la gestión de permisos y accesos.
    - **Unidades organizativas (OU)**: Organice usuarios y recursos en unidades organizativas para aplicar políticas específicas y simplificar la administración.

5. **Implementación de políticas de grupo (GPO)**:
    - **Configuración de GPOs**: Utilice las Políticas de Grupo para aplicar configuraciones y políticas de seguridad a usuarios y equipos en el dominio. Las GPOs pueden aplicarse a nivel de dominio, OU o grupo.

6. **Configuración de servicios adicionales**:
    - **Autenticación y seguridad**: Configure servicios de autenticación y políticas de seguridad adicionales, como Kerberos, NTLM, y políticas de contraseñas.
    - **Replicación de controladores de dominio**: Configure la replicación entre múltiples controladores de

dominio para garantizar la redundancia y la alta disponibilidad de Active Directory.

7. **Mantenimiento y monitoreo**:
    - **Monitoreo y auditoría**: Implemente soluciones de monitoreo y auditoría para supervisar la actividad en Active Directory y detectar posibles problemas de seguridad o de rendimiento.
    - **Respaldo y recuperación**: Establezca procedimientos de respaldo y recuperación para la base de datos de Active Directory y otros componentes críticos.

---

**Más información**

- https://www.jesusninoc.com/07/11/11-gestion-del-directorio-activo-nivel-intermedio/

---

# Administración de cuentas. Cuentas predeterminadas

La administración de cuentas en Active Directory (AD) es un componente esencial para la gestión de identidades y accesos dentro de una red corporativa. Las cuentas de usuario, grupo y máquina son los principales objetos administrados en AD, y su correcta configuración y administración aseguran el control y la seguridad en el acceso a los recursos de la red.

# Tipos de cuentas en Active Directory

En Active Directory, existen varios tipos de cuentas que son gestionadas para diferentes propósitos:

1. **Cuentas de usuario**: Representan a individuos que necesitan acceso a los recursos de la red. Estas cuentas permiten la autenticación y la autorización de los usuarios en el dominio.
2. **Cuentas de grupo**: Agrupan cuentas de usuario para facilitar la administración de permisos y políticas. Los grupos pueden ser de dos tipos: grupos de seguridad (para control de acceso) y grupos de distribución (para listas de distribución de correo).
3. **Cuentas de máquina**: Representan a dispositivos como computadoras y servidores que son miembros del dominio. Estas cuentas permiten la autenticación de dispositivos y la aplicación de políticas de grupo a nivel de máquina.

# Administración de cuentas de usuario

La administración de cuentas de usuario implica varias tareas esenciales para mantener la seguridad y eficiencia en la red. Estas tareas incluyen la creación, modificación, y eliminación de cuentas, así como la implementación de políticas de contraseñas y la gestión de permisos.

## Creación de cuentas de usuario

Para crear una cuenta de usuario en Active Directory, se utiliza la herramienta «Usuarios y equipos de Active Directory» (ADUC). Durante la creación, se deben especificar varios atributos, como:

- **Nombre de usuario**: Un identificador único para el usuario.

- **Contraseña**: Una clave secreta que el usuario utilizará para autenticarse.
- **Información de contacto**: Detalles como el nombre completo, número de teléfono y dirección de correo electrónico.
- **Organización**: Información sobre la posición del usuario dentro de la organización, como el departamento y el cargo.

### Modificación de cuentas de usuario

Las cuentas de usuario pueden ser modificadas para actualizar la información del perfil, cambiar contraseñas, y ajustar permisos y membresías de grupos. Es crucial mantener la información de contacto y de organización actualizadas para asegurar una administración precisa de los usuarios y la aplicación correcta de políticas.

### Eliminación de cuentas de usuario

Eliminar cuentas de usuario inactivas o innecesarias es importante para mantener la seguridad. Esto previene el acceso no autorizado y reduce la carga administrativa. Antes de eliminar una cuenta, es buena práctica deshabilitarla temporalmente y verificar que el usuario ya no necesita acceso a los recursos de la red.

## Cuentas predeterminadas en Active Directory

Active Directory viene con varias cuentas predeterminadas que son creadas durante la instalación del dominio. Estas cuentas tienen roles específicos y permisos asociados que son fundamentales para el funcionamiento y la administración del dominio.

### Cuentas de usuario predeterminadas

1. **Administrador**: Esta es la cuenta de administrador predeterminada con permisos completos en el dominio. Es crucial para la configuración inicial y la administración continua de Active Directory.
2. **Invitado (Guest)**: Esta cuenta está deshabilitada por defecto y tiene permisos limitados. Puede ser habilitada para proporcionar acceso temporal a usuarios externos o invitados.

### Cuentas de grupo predeterminadas

1. **Administradores del dominio (Domain Admins)**: Grupo que tiene permisos administrativos completos en el dominio.
2. **Usuarios del dominio (Domain Users)**: Grupo al que se añaden automáticamente todas las cuentas de usuario creadas en el dominio.
3. **Usuarios avanzados (Power Users)**: Grupo con permisos adicionales para administrar ciertos aspectos del sistema, pero con menos privilegios que los administradores.
4. **Usuarios del escritorio remoto (Remote Desktop Users)**: Grupo que permite a los usuarios conectarse remotamente a los servidores y estaciones de trabajo en el dominio.
5. **Operadores de cuentas (Account Operators)**: Grupo que tiene permisos para crear, modificar y eliminar cuentas de usuario y de grupo.

## Buenas prácticas para la administración de cuentas en Active Directory

1. **Políticas de contraseñas**: Implemente políticas estrictas de contraseñas que incluyan requisitos de complejidad, caducidad y reutilización limitada.

2. **Auditoría y monitoreo**: Realice auditorías regulares y monitoree el uso de cuentas para detectar actividades sospechosas o no autorizadas.
3. **Delegación de administración**: Use la delegación de control para asignar responsabilidades administrativas a diferentes niveles, asegurando que los permisos se otorguen según el principio de mínimo privilegio.
4. **Mantenimiento de cuentas**: Revise periódicamente las cuentas de usuario para deshabilitar o eliminar aquellas que ya no sean necesarias, y actualice la información de las cuentas activas.
5. **Uso de grupos**: Aproveche los grupos de seguridad para administrar permisos de acceso de manera más eficiente, en lugar de asignar permisos directamente a las cuentas individuales.

---

**Más información**

- https://www.jesusninoc.com/07/11/11-gestion-del-directorio-activo-nivel-intermedio/

---

# Contraseñas. Bloqueos de cuenta

Las contraseñas y los bloqueos de cuenta son elementos críticos en la seguridad de cualquier sistema basado en Active Directory (AD). Las contraseñas actúan como la primera línea de defensa contra el acceso no autorizado, mientras que los bloqueos de cuenta son una medida preventiva para proteger las cuentas de usuario contra ataques de fuerza bruta y otros intentos de acceso malintencionado.

En el contexto de Active Directory, las contraseñas deben cumplir con ciertas políticas que aseguren su complejidad y efectividad. Las políticas de contraseñas incluyen requisitos como longitud mínima, complejidad (incluir una combinación de letras mayúsculas, minúsculas, números y caracteres especiales), y caducidad (requiriendo a los usuarios cambiar sus contraseñas periódicamente). Estas políticas ayudan a minimizar la probabilidad de que las contraseñas sean adivinadas o descifradas por atacantes.

Además de los requisitos de complejidad, la gestión de contraseñas también implica la configuración de políticas de reutilización, que previenen que los usuarios reutilicen contraseñas antiguas dentro de un número específico de cambios. Esto es importante para asegurar que las contraseñas nuevas no sean similares a las anteriores, manteniendo así la robustez de la seguridad.

El bloqueo de cuentas es una medida de seguridad diseñada para proteger las cuentas de usuario de intentos de acceso no autorizados repetidos, como los ataques de fuerza bruta. En Active Directory, se puede configurar una política de bloqueo de cuentas que determina el número de intentos fallidos de inicio de sesión permitidos antes de que la cuenta sea bloqueada. Por ejemplo, si un usuario ingresa una contraseña incorrecta cinco veces consecutivas, su cuenta puede ser bloqueada temporalmente para prevenir accesos malintencionados.

La política de bloqueo de cuentas también especifica la duración del bloqueo, es decir, cuánto tiempo permanecerá bloqueada una cuenta antes de que se desbloquee automáticamente. Esta duración puede ser configurada según las necesidades de seguridad de la organización. En algunos casos, se puede requerir la intervención de un administrador para desbloquear la cuenta, lo cual añade una capa adicional de seguridad al proceso.

El manejo efectivo de contraseñas y bloqueos de cuenta es fundamental para mantener la seguridad en un entorno de Active Directory. Las organizaciones deben equilibrar la necesidad de seguridad con la conveniencia para los usuarios. Políticas de contraseñas demasiado estrictas pueden llevar a usuarios a prácticas inseguras, como escribir sus contraseñas en lugares no seguros. De igual manera, bloqueos de cuenta muy frecuentes pueden resultar en una experiencia de usuario frustrante.

Para mitigar estos problemas, las organizaciones pueden implementar mecanismos de autenticación multifactor (MFA), que añaden una capa adicional de seguridad al requerir que los usuarios proporcionen más de una forma de verificación, como un código enviado a un dispositivo móvil además de la contraseña. Esto reduce la dependencia exclusiva en las contraseñas y aumenta significativamente la seguridad.

---

**Más información**

- https://www.jesusninoc.com/07/11/11-gestion-del-directorio-activo-nivel-intermedio/

---

# Cuentas de usuarios y equipos

Las cuentas de usuarios y equipos son fundamentales para la administración y seguridad de una red corporativa. Estas cuentas permiten gestionar el acceso a recursos y servicios, aplicando políticas de seguridad y control de permisos en un entorno centralizado.

Las **cuentas de usuario** en Active Directory representan individuos que necesitan acceder a recursos de la red, como

aplicaciones, archivos y servicios. Cada cuenta de usuario contiene información esencial como el nombre de usuario, la contraseña, y atributos adicionales como el nombre completo, la dirección de correo electrónico y el departamento al que pertenece el usuario. La administración de estas cuentas implica la creación, modificación, y eliminación de cuentas, así como la aplicación de políticas de seguridad, como la longitud y complejidad de las contraseñas y la configuración de permisos y roles.

Al crear una cuenta de usuario, se define un identificador único y una contraseña inicial. Es común que los administradores requieran que los usuarios cambien su contraseña en el primer inicio de sesión para asegurar que solo el usuario conoce su clave. Además, las cuentas de usuario pueden ser miembros de grupos de seguridad, lo que facilita la asignación de permisos y políticas a múltiples usuarios simultáneamente.

Las **cuentas de equipo** representan dispositivos, como computadoras y servidores, que forman parte del dominio de Active Directory. Estas cuentas permiten que los dispositivos se autentiquen y se comuniquen de manera segura dentro de la red. Cada cuenta de equipo también tiene un nombre único y una contraseña, aunque estas contraseñas se manejan automáticamente por el sistema y se actualizan periódicamente sin intervención manual.

La creación de cuentas de equipo se realiza típicamente durante el proceso de «unirse al dominio», donde un dispositivo es configurado para ser parte del dominio de Active Directory. Una vez que el dispositivo es parte del dominio, puede ser gestionado centralizadamente, permitiendo a los administradores aplicar políticas de grupo, actualizaciones de software y configuraciones de seguridad de manera uniforme.

## Administración de cuentas de usuarios

La administración de cuentas de usuarios implica varias tareas críticas:

1. **Creación de cuentas**: Utilizando herramientas como «Usuarios y equipos de Active Directory» (ADUC), los administradores pueden crear nuevas cuentas de usuario, especificando detalles como el nombre de usuario, la contraseña inicial, y los atributos del perfil.
2. **Modificación de cuentas**: Los administradores pueden actualizar la información del perfil del usuario, cambiar contraseñas, y ajustar permisos y roles según sea necesario.
3. **Desactivación y eliminación de cuentas**: Las cuentas de usuario que ya no son necesarias deben ser desactivadas o eliminadas para mantener la seguridad de la red. La desactivación es una medida temporal que puede ser revertida, mientras que la eliminación es permanente.
4. **Aplicación de políticas de seguridad**: A través de las Políticas de Grupo (GPO), los administradores pueden imponer requisitos de contraseñas, configuraciones de seguridad, y otros parámetros que se aplicarán automáticamente a las cuentas de usuario.

## Administración de cuentas de equipos

La administración de cuentas de equipos también es esencial para el mantenimiento de una red segura y bien gestionada:

1. **Unirse al dominio**: Cuando un equipo se une al dominio de Active Directory, se crea automáticamente una cuenta de equipo. Este proceso puede ser realizado por un administrador o por un usuario autorizado.
2. **Aplicación de políticas de grupo**: Las Políticas de Grupo permiten a los administradores configurar y gestionar

las políticas de seguridad y configuración que se aplican a los equipos en el dominio, asegurando una administración consistente.
3. **Gestión de equipos**: A través de la consola ADUC, los administradores pueden ver y gestionar las cuentas de equipo, incluyendo la actualización de información y la desactivación o eliminación de equipos que ya no son utilizados.

## Importancia de la gestión eficiente

Una gestión eficiente de las cuentas de usuario y equipo en Active Directory es crucial para mantener la seguridad y la operatividad de una red corporativa. La administración centralizada de estas cuentas permite a los administradores aplicar políticas de seguridad de manera uniforme, controlar el acceso a recursos, y mantener un registro actualizado de los usuarios y dispositivos que forman parte del dominio. Además, una gestión adecuada minimiza los riesgos de accesos no autorizados y garantiza que solo los usuarios y dispositivos autorizados puedan interactuar con los recursos de la red.

---

### Ejemplos

- https://www.jesusninoc.com/2016/07/02/list-local-users/
- https://www.jesusninoc.com/04/12/ejercicios-de-powershell-seleccionar-usuarios-que-empiezan-por-una-letra-con-una-expresion-regular/

---

**Ejercicios**

- https://www.jesusninoc.com/02/22/ejercicios-de-powershell-crea-un-usuario-en-un-directorio-activo/
- https://www.jesusninoc.com/02/22/ejercicios-de-powershell-crear-una-ou-unidad-organizativa-en-un-directorio-activo/
- https://www.jesusninoc.com/05/16/utilizar-un-filtro-ldap-para-localizar-un-usuario/
- https://www.jesusninoc.com/07/05/utilizar-un-filtro-ldap-para-verificar-la-hora-del-ultimo-inicio-de-sesion-de-los-usuarios-del-active-directory/

---

**Más información**

- https://www.jesusninoc.com/07/11/11-gestion-del-directorio-activo-nivel-intermedio/

---

# Perfiles móviles y obligatorios

Los perfiles móviles y obligatorios son dos métodos para gestionar las configuraciones y datos de usuario en una red corporativa, facilitando la administración centralizada y mejorando la experiencia del usuario.

Un perfil móvil es un perfil de usuario que se almacena en un servidor central y se descarga en cualquier computadora que el usuario utilice dentro del dominio. Este tipo de perfil permite que los usuarios mantengan un entorno de trabajo consistente y personalizado, independientemente del dispositivo desde el cual inicien sesión. Al iniciar sesión,

el perfil del usuario, que incluye configuraciones personales, archivos y preferencias, se carga en la computadora en uso. Al cerrar la sesión, los cambios realizados se sincronizan de vuelta al servidor central, asegurando que las actualizaciones se mantengan disponibles en la próxima sesión desde cualquier dispositivo.

La principal ventaja de los perfiles móviles es la portabilidad, ya que los usuarios pueden trabajar desde diferentes dispositivos sin perder su configuración personal. Sin embargo, el primer inicio de sesión en un nuevo dispositivo puede llevar tiempo debido a la necesidad de descargar el perfil completo. Además, una red confiable y rápida es crucial para una buena experiencia de usuario, dado que la sincronización del perfil depende de la conectividad.

Por otro lado, un perfil obligatorio es un perfil que se define y controla estrictamente por los administradores y no permite cambios permanentes por parte del usuario. Este tipo de perfil es útil en entornos donde es crucial mantener configuraciones uniformes y restringir la personalización, como en aulas, quioscos de información o estaciones de trabajo compartidas. Cualquier cambio realizado por el usuario durante la sesión se descarta al cerrar sesión, y el perfil vuelve a su estado original la próxima vez que el usuario inicie sesión. Esto asegura que todas las configuraciones y políticas sean consistentes y cumplan con los requisitos organizacionales.

El uso de perfiles obligatorios ofrece una seguridad y control significativos, ya que los administradores tienen control total sobre la configuración del entorno de usuario. Esto reduce los problemas técnicos y mantiene una configuración estable. Sin embargo, la falta de personalización puede ser frustrante para los usuarios que requieren un entorno adaptado a sus necesidades.

En ambos casos, la implementación de estos perfiles se realiza

a través de políticas de grupo en Active Directory. Para los perfiles móviles, los administradores configuran la ruta de perfil en las propiedades de la cuenta de usuario, especificando una ruta de red donde se almacenará el perfil. Para los perfiles obligatorios, los administradores configuran un perfil de usuario específico y lo marcan como obligatorio, cambiando el nombre del archivo de perfil NTUSER.DAT a NTUSER.MAN para asegurar que los cambios no se guarden permanentemente.

Tanto los perfiles móviles como los obligatorios tienen sus propios beneficios y desafíos, y la elección entre ellos depende de los requisitos operativos y de seguridad de la organización. Los perfiles móviles son ideales para entornos donde los usuarios necesitan movilidad y consistencia en sus configuraciones y datos personales, mientras que los perfiles obligatorios son adecuados para entornos que requieren un control estricto y una configuración uniforme. La correcta implementación y gestión de estos perfiles pueden mejorar significativamente la eficiencia y la seguridad de la red corporativa.

---

**Más información**

- https://www.jesusninoc.com/07/11/11-gestion-del-directorio-activo-nivel-intermedio/

---

# Carpetas personales

Las carpetas personales, también conocidas como carpetas redirigidas, son una funcionalidad que permite almacenar las carpetas de usuario en un servidor central en lugar de en el

disco duro local del usuario. Esto mejora la gestión de datos y la experiencia del usuario, proporcionando accesibilidad y seguridad.

Las carpetas personales se configuran para redirigir ciertos directorios de usuario, como «Documentos», «Escritorio» e «Imágenes», a una ubicación de red central. Esta redirección permite a los usuarios acceder a sus archivos y configuraciones desde cualquier computadora dentro del dominio, manteniendo una experiencia de usuario coherente. Esto es especialmente útil en entornos donde los usuarios cambian de estación de trabajo frecuentemente.

Almacenar archivos en un servidor central permite aplicar políticas de seguridad más estrictas y facilita el respaldo regular de datos, reduciendo el riesgo de pérdida de información. Además, los administradores pueden gestionar de manera centralizada las carpetas y archivos de los usuarios, aplicando políticas de grupo para controlar el acceso, las cuotas de almacenamiento y las configuraciones de seguridad. Mover el almacenamiento de datos a un servidor central también reduce la carga en los discos duros de las estaciones de trabajo individuales, mejorando su rendimiento y prolongando su vida útil.

La implementación de carpetas personales en Active Directory se realiza mediante la configuración de la redirección de carpetas utilizando las Políticas de Grupo (GPO). Primero, se crea una carpeta compartida en un servidor de archivos que será accesible para todos los usuarios y se configuran los permisos adecuados para asegurar que solo los usuarios autorizados puedan acceder y modificar sus datos. Luego, mediante la consola de administración de políticas de grupo (GPMC), se crea o edita una GPO que se aplicará a las unidades organizativas (OU) correspondientes a los usuarios. En la GPO, se especifican las carpetas que se van a redirigir y se define la ruta de red del servidor de archivos. Una vez configurada la GPO, se aplica a las OUs designadas y se verifica que las

carpetas de los usuarios se redirigen correctamente a la ubicación de red especificada.

Es recomendable habilitar la caché sin conexión para las carpetas redirigidas, permitiendo a los usuarios acceder a sus archivos incluso cuando no están conectados a la red, sincronizando los cambios automáticamente cuando se restablece la conexión. Además, implementar cuotas de almacenamiento en el servidor de archivos puede ayudar a gestionar el espacio en disco y prevenir el uso excesivo de recursos por parte de los usuarios. Los administradores deben monitorear regularmente el uso de las carpetas redirigidas y realizar mantenimiento preventivo, como la limpieza de archivos temporales y la gestión de permisos.

---

**Más información**

- https://www.jesusninoc.com/07/11/11-gestion-del-directorio-activo-nivel-intermedio/

---

# Plantillas de usuario. Variables de entorno

Las plantillas de usuario y las variables de entorno son herramientas esenciales que facilitan la gestión y personalización de las cuentas de usuario en una red corporativa. Estas herramientas permiten a los administradores aplicar configuraciones uniformes y específicas de manera eficiente.

# Plantillas de usuario

Las plantillas de usuario son perfiles predefinidos que los administradores pueden utilizar para crear nuevas cuentas de usuario de manera rápida y uniforme. Al emplear una plantilla, se asegura que todas las cuentas de usuario creadas a partir de ella tengan configuraciones y permisos consistentes, alineados con las políticas de la organización.

**Características de las plantillas de usuario**:

1. **Consistencia**: Garantizan que todos los usuarios tengan configuraciones uniformes, lo que facilita la administración y reduce errores.
2. **Eficiencia**: Aceleran el proceso de creación de cuentas, evitando la necesidad de configurar manualmente cada nueva cuenta.
3. **Personalización**: Permiten predefinir configuraciones específicas como grupos de pertenencia, permisos de acceso, políticas de seguridad y más.

**Implementación**: Para crear una plantilla de usuario, los administradores pueden configurar una cuenta de usuario con los ajustes deseados y luego utilizar esta cuenta como base para crear nuevas cuentas. Esta técnica se suele utilizar para roles específicos dentro de la organización, como cuentas de empleados nuevos, contratistas, o departamentos específicos.

# Variables de entorno

Las variables de entorno son parámetros que almacenan información sobre el entorno del sistema y el perfil del usuario. Estas variables se utilizan para configurar el entorno del usuario y las aplicaciones que se ejecutan en el sistema, proporcionando flexibilidad y personalización.

**Características de las variables de entorno**:

1. **Personalización del entorno**: Permiten a los administradores y aplicaciones configurar rutas de directorios, ubicaciones de archivos temporales, y otras configuraciones basadas en el entorno específico del usuario.
2. **Automatización**: Facilitan la automatización de scripts y procesos al proporcionar información sobre el entorno del sistema y del usuario.
3. **Flexibilidad**: Pueden ser modificadas temporalmente para la sesión actual o establecidas permanentemente para todas las sesiones del usuario.

**Uso común de variables de entorno**:

- **%USERPROFILE%**: La ruta del perfil del usuario.
- **%HOMEDRIVE% y %HOMEPATH%**: La unidad y la ruta del directorio principal del usuario.
- **%USERNAME%**: El nombre del usuario que ha iniciado sesión.
- **%COMPUTERNAME%**: El nombre del equipo en el que se está ejecutando la sesión.

**Implementación y configuración**: Los administradores pueden establecer variables de entorno globales que se aplican a todos los usuarios del sistema, o definir variables específicas para cuentas individuales o grupos de usuarios. Estas configuraciones se pueden realizar a través del Panel de Control de Windows o mediante Políticas de Grupo en Active Directory.

**Ejemplo de uso**: Un administrador podría utilizar una variable de entorno para definir la ubicación de un directorio de trabajo compartido, de manera que todas las aplicaciones y scripts se refieran a esta variable en lugar de una ruta de archivo fija. Esto facilita la gestión y la actualización de ubicaciones de recursos, ya que solo se necesita cambiar la

variable de entorno, y no cada referencia en los scripts y configuraciones.

---

**Más información**

- https://www.jesusninoc.com/07/11/11-gestion-del-directorio-activo-nivel-intermedio/

---

# Administración de grupos. Tipos. Estrategias de anidamiento. Grupos predeterminados

La administración de grupos es una función crítica que facilita la gestión de usuarios y recursos en una red corporativa. Los grupos permiten a los administradores aplicar permisos y configuraciones de manera eficiente a múltiples usuarios, mejorando la seguridad y simplificando la administración. Existen diferentes tipos de grupos en AD, y se pueden emplear diversas estrategias de anidamiento para organizar y gestionar estos grupos de manera eficaz. Además, hay ciertos grupos predeterminados que vienen preconfigurados con roles específicos.

## Tipos de grupos en Active Directory

Active Directory soporta dos tipos principales de grupos:

1. **Grupos de seguridad**: Utilizados para asignar permisos de acceso a recursos en la red, como archivos, carpetas y servicios. Los grupos de seguridad pueden ser utilizados en listas de control de acceso (ACL) para definir quién

tiene acceso a qué recursos.
2. **Grupos de distribución**: Utilizados principalmente para crear listas de distribución de correo electrónico en servicios como Microsoft Exchange. Los grupos de distribución no pueden ser utilizados para asignar permisos de seguridad.

Además de los tipos, los grupos en AD se clasifican según su ámbito:

1. **Grupos locales de dominio**: Pueden contener usuarios, grupos y equipos de cualquier dominio en el bosque, pero solo pueden asignar permisos dentro del dominio donde se crearon.
2. **Grupos globales**: Pueden contener usuarios y grupos de su propio dominio y pueden ser miembros de otros grupos en cualquier dominio del bosque. Se utilizan principalmente para organizar usuarios dentro de un dominio.
3. **Grupos universales**: Pueden contener usuarios, grupos y equipos de cualquier dominio en el bosque y pueden asignar permisos en cualquier dominio del bosque. Son útiles en entornos con múltiples dominios para asignar permisos de manera centralizada.

## Estrategias de anidamiento de grupos

El anidamiento de grupos es una práctica que implica la inclusión de un grupo dentro de otro grupo, facilitando una gestión más granular y flexible de permisos y roles. Aquí hay algunas estrategias comunes de anidamiento:

1. **A-G-DL-P (Accounts-Global-Domain Local-Permissions)**: Esta estrategia implica colocar cuentas de usuario en grupos globales, luego anidar esos grupos globales en grupos locales de dominio, y finalmente, asignar permisos a los grupos locales de dominio. Esto permite

una gestión eficiente de permisos y escalabilidad.
2. **A-G-U-DL-P (Accounts-Global-Universal-Domain Local-Permissions)**: Similar a la estrategia A-G-DL-P, pero incluye un nivel adicional de grupos universales. Las cuentas de usuario se colocan en grupos globales, que luego se incluyen en grupos universales, y estos, a su vez, se anidan en grupos locales de dominio. Finalmente, los permisos se asignan a los grupos locales de dominio. Esta estrategia es útil en entornos con múltiples dominios.

## Grupos predeterminados en Active Directory

Active Directory incluye varios grupos predeterminados con roles y permisos específicos para facilitar la administración de la red. Algunos de los grupos predeterminados más importantes son:

1. **Administradores (Administrators)**: Tienen control total sobre todos los objetos en el dominio y pueden realizar cualquier tarea administrativa.
2. **Usuarios (Users)**: Incluye todas las cuentas de usuario estándar. Los miembros de este grupo tienen permisos limitados.
3. **Operadores de cuenta (Account Operators)**: Tienen permisos para crear, modificar y eliminar cuentas de usuario y de grupo en el dominio.
4. **Operadores de copia de seguridad (Backup Operators)**: Tienen permisos para realizar operaciones de copia de seguridad y restauración en el dominio.
5. **Usuarios avanzados (Power Users)**: Tienen permisos adicionales para realizar ciertas tareas administrativas y de configuración en los sistemas locales.
6. **Operadores de impresión (Print Operators)**: Tienen permisos para gestionar impresoras y colas de impresión.

7. **Controladores de esquema (Schema Admins)**: Tienen permisos para modificar el esquema de Active Directory, que define la estructura de datos del directorio.
8. **Administradores de la empresa (Enterprise Admins)**: Tienen permisos administrativos en todo el bosque de Active Directory.
9. **Administradores de dominio (Domain Admins)**: Tienen permisos administrativos en su dominio específico.

---

## Más información

- https://www.jesusninoc.com/07/11/11-gestion-del-directorio-activo-nivel-intermedio/

---