Windows Active Directory

/via: https://deephacking.tech/que-es-active-directory/

origen

```
Active Directory tuvo sus inicios a principios de los años 90, en un contexto donde Microsoft estaba bajo investigación por prácticas monopólicas en el mercado de los sistemas operativos para ordenadores personales. Para diversificar su enfoque y reducir su dependencia de los consumidores finales, Microsoft decidió expandirse hacia el mercado empresarial. Con una fuerte presencia ya establecida gracias a Windows y Office, la compañía buscó crear una solución que facilitara la gestión de datos y recursos en grandes organizaciones. Así nació Active Directory, una herramienta diseñada para integrarse con Windows Server, presentando una estructura jerárquica y escalable.

El primer paso de Active Directory se dio con el lanzamiento de Windows 2000 Server. Antes de esto, la configuración de los usuarios en redes empresariales se almacenaba en una base de datos SAM en el controlador de dominio (servidor central) de la red, utilizando el protocolo Netlogon para la autenticación de usuarios. Sin embargo, la creciente complejidad de las redes empresariales reveló una serie de limitaciones del formato SAM cuando de escalabilidad se refería, esto llevó a una transición hacia Active Directory con Windows 2000, que además introdujo el protocolo de autenticación Kerberos.

Active Directory ofrece ventajas significativas respecto a la antigua base de datos SAM, siendo más extensible y permitiendo almacenar datos adicionales en la configuración de usuarios, como por ejemplo el nivel de seguridad, que puede ser utilizado por aplicaciones para gestionar el acceso a recursos. Todos estos datos se almacenan localmente en un controlador de dominio y son accesibles mediante el protocolo LDAP, que funciona sobre TCP/IP en el puerto 389.

En resumen, después de todo este tostón se puede decir que Active Directory ha ido evolucionando hasta convertirse en lo que es hoy en día, una herramienta esencial para casi todas las empresas IT del mundo.

Sabiendo ya qué es Active Directory ahora toca ver algunas de sus características principales para poder entender como funciona y se estructura.
```

objeto

- todo es un objeto (recursos de red: usuarios, ordenadores...), con propiedades
- GUID = Global Unique Identifier
    - identificador único en el AD
    - DN = Distinguised Name
        - ruta jerarquica que muestra ubicación en el arbol AD
    - SID = Security Identifier
        - identificador único para tareas de seguridad

dominios

- 1 AD, varios dominios, varios DC (Domain Controler) por cada dominio
- cada dominio posee un nombre DNS: `%USERDNSDOMAIN%`
- que tiene asociado un nombre NETBIOS (el que se usa para hacer login)

arbol y bosques

- dominios y subdominios = arbol
- conjunto de árboles = bosque
- no se utiliza el concepto de **arbol** (en general) y se suele hablar de dominios y bosques
- comunicación entre los diferentes dominios/subdominios del mismo arbol
- relación de confianza entre los arboles de un bosque

modos funcionales

- dependiendo de la versión de Windows Server, opearemos a un modo funcional u otro.
    - relación de características según el modo funcional: https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-adts/564dc969-6db3-49b3-891a-f2f8d0a68a7f

OUs (Unidades organizativas)

- objetos contenedores para ayudar a organizar la información
- permite aplicar políticas, restricciones o accesos al conjunto de objetos de una OU

contenedores

- simiar a una OU, pero:
    - no objetos adminisrtativos → no delegar permisos de adminisrtación. más simples.
    - agrupar objetos que no requieres aplicar políticas
    - no heredan ni aplican las directivas de grupo (GPO)
    - ejemplos: Users, Computers, Builtin...

GPO

- colección políticas (configuraciones y reglas)
- aplicables a nivel de dominio o de OU, usuario o grupo
- herencia

DC

- servidores centrales que tiene la BDD del AD
- autenticación y autorización
- replicación datos en AD
- intervalo por defecto 3h

LDAP y Kerberos

- protocolos fundamentales
- LDAP = Lightweight Directory Access Protocol
  - acceder y administrar información del AD
  - puerto 389
  - versión segura LDAPS, puerto 636
- Kerberos
  - autenticación
  - tickets:
    - usuari accede a recurso de la red, envía solicitud a Kerberos
    - Kerberos le devuelve un ticket
    - Este ticket se puede presentar a otros servicios/recursos para autenticar, sin tener que enviar las crendeciales
    - https://deephacking.tech/humilde-intento-de-explicar-kerberos/