Introducción a *Active Directory*

El Directorio Activo (*Active Directory* – AD) es una base de datos distribuida que permite almacenar información relativa a los recursos de una red con el fin de facilitar su localización y administración. Microsoft *Active Directory* es la implementación más reciente de Servicios de Directorio para Windows. Las cuestiones básicas relacionadas con un centro de servicios de directorio giran alrededor de la información que se puede almacenar en la base de datos, cómo se almacena, cómo se puede consultar información específica y qué se puede hacer con los resultados. *Active Directory* se compone del propio servicio de directorio junto con un servicio secundario que permite el acceso a la base de datos y admite las convenciones de denominación X.500.

Los Servicios de Dominio de *Active Directory* (AD DS) almacenan datos y administran la comunicación entre usuarios y dominios, incluidos los procesos de inicio de sesión de usuarios, autenticación y búsquedas en el directorio. Un controlador de dominio de Active Directory es un servidor que ejecuta AD DS

1.- ¿Por qué implementar un Dominio en una red?

Los dominios y los grupos de trabajo representan diferentes formas de organizar equipos y, en general, todos los recursos de una red. La diferencia principal entre estas dos opciones es la forma de administrar los equipos y otros recursos de las redes. Eso sí, todos los equipos que ejecutan Windows en una red deben ser, obligatoriamente, parte de un grupo de trabajo o de un dominio.

- En un grupo de trabajo:

- Todos los equipos se encuentran en el mismo nivel, ninguno tiene el control sobre otro.
- Cada equipo dispone de un conjunto de cuentas de usuario. Para iniciar sesión en un equipo del grupo de trabajo, se debe disponer de una cuenta en dicho equipo.
- Normalmente, no hay más que unos veinte equipos.
- Un grupo de trabajo no está protegido con contraseña.
- Todos los equipos deben encontrarse en la misma red local o subred.

- En un dominio:

- Es obligatorio tener uno o más equipos son servidores. Los administradores de red utilizan los servidores para controlar la seguridad y los permisos de todos los equipos del dominio. Así resulta más sencillo efectuar cambios, ya que éstos se aplican automáticamente a todos los equipos. Los usuarios de dominio deben proporcionar una contraseña o algún otro tipo de credencial cada vez que accedan al dominio.
- Si se dispone de una cuenta de usuario en el dominio, se puede iniciar sesión en cualquier equipo del dominio, sin necesidad de disponer de una cuenta en dicho equipo.
- Probablemente solo se podrán hacer cambios limitados a la configuración de un equipo, porque los administradores de red, con frecuencia, desean garantizan un nivel de homogeneidad entre los equipos.
- Un dominio puede incluir miles de equipos.
- Los equipos pueden encontrarse en diferentes redes locales.

2.- Estructura Lógica vs Estructura Física de *Active Directory*

Active Directory separa la estructura lógica de la estructura física real. Veamos qué elementos componen cada una de ellas y cómo los administradores se aprovechan de estos dos tipos de estructuras para diseñar la red más adecuada para cada situación.

2.1.- Estructura Lógica

La estructura lógica de *Active Directory* se compone de elementos intangibles como **objetos**, **dominios**, **árboles** y **bosques**. Este espacio lógico permite a los Administradores abstraerse de la Estructura Física que, básicamente la componen los **controladores de dominio** y los **sitios**, que veremos en el siguiente punto.

Esta separación entre estructura física y lógica nos permitirá una mejor organización de los elementos que componen la red en función de la naturaleza de los objetos y de la función organizativa de la empresa.

Ahora, en este punto, nos centraremos en explorar la utilización de los dominios y los bosques (y los árboles correspondientes) para que éstos jueguen el rol de punto central de gestión del resto de objetos del *Active Directory*. De este modo, todos los datos y los servicios ofrecidos, grabados dentro de los Servicios de Dominio de *Active Directory* podrán ser localizados en cualquier punto de la red por los usuarios y, a su vez, por las aplicaciones empresariales vinculadas.

2.1.1.- Los objetos del *Active Directory*

El bloque de construcción básico de *Active Directory* es el **objeto**, un conjunto de **atributos** y **métodos** diferenciado que representa un recurso de la red, un usuario, un grupo, etc.

→ Los objetos son instancias de una **clase** de elementos concretos.

→ Los usuarios, grupos y equipos son ejemplos de clases de objeto diferentes.

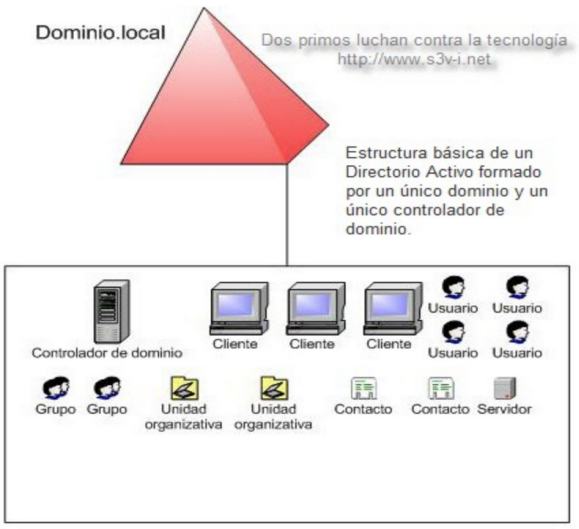
→ Los **atributos** del objeto son características de objetos del directorio. Ejemplos de atributos para un objeto usuario serían : dysplayname, compañía, departamento, email, móvil, nombre, iniciales, etc .

→ Los **métodos** del objeto se pueden considerar como 'el pedido' a un objeto para que realice una tarea determinada, o la vía para enviar un mensaje a dicho objeto y que éste reaccione acorde a dicho mensaje. Ejemplos de métodos para un objeto usuario serían : cambio de contraseña, habilitar/deshabilitar, bloquear/desbloquear, etc .

En el nivel más bajo, algunos objetos representan entidades individuales de la red, como un usuario o un equipo. Estos objetos de denominan **hoja** y no pueden contener otros objetos en su interior. Sin embargo, para facilitar la administración y simplificar la organización del *Active Directory*, se pueden colocar objetos hoja dentro de otros objetos denominados **objetos contenedor**. Decir que, estos objetos contenedor también van a poder contener otros contenedores de forma anidada, o jerárquica, formando una estructura de tipo árbol idéntica a la que tenemos en un sistema de archivos, donde los contenedores serían los directorios y las hojas serían los archivos.

El tipo más común de objeto contenedor es la **Unidad Organizativa** (OU, *Organizational Unit*). Vamos a poder utilizar OUs para organizar objetos de un **dominio** en algún tipo de agrupación lógica administrativa. En general, la elección del esquema de OUs para un dominio será teniendo en cuenta: la delegación del control de los objetos existentes en su interior, la futura aplicación directivas de grupo (GPO - *Group Policy Object*) a los objetos internos a dicha OU o, simplemente, por mera organización de los recursos y objetos de la red (dominio).

Todos los objetos de la red, ya sean hojas o contenedores, sólo pueden existir dentro de un único dominio. Los dominios se usan para agrupar objetos relacionados con el fin de reflejar la red de una organización. Cada dominio que se crea almacena información acerca de los objetos que contiene, únicamente. El número de objetos en un dominio puede llegar a ser hasta de varios billones de objetos, por lo que el hecho de montar más de un dominio para gestionar los recursos de una única empresa tendrá que estar muy justificado, siendo el motivo más común la ubicación física de los objetos y que la comunicación entre ellos y el controlador de dominio sea lenta (ubicación física).



Dentro de *Active Directory*, un dominio también se puede denominar **partición**. Así, cada dominio representa un límite de seguridad y, el acceso a los objetos dentro de cada dominio, se controla mediante **entradas de control de acceso** (ACE, *Access Control Entries*) contenidas en **listas de control de acceso** (ACL, *Access Control Lists*). Estas opciones de seguridad no cruzan los límites de los dominios.

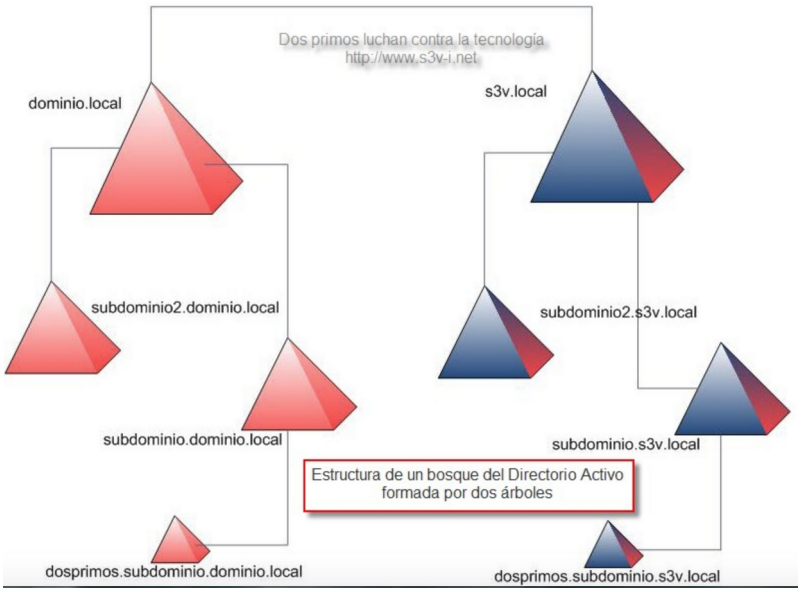
Nota.- *Active Directory* está íntimamente ligado a los servicios DNS (*Domain Name Server*). DNS es el protocolo estándar de resolución de nombres definido por la IETF. Este protocolo permite a los equipos cliente registrarse y resolver los nombres de otros equipos. Una vez resuelto el nombre (nombre → IP), va a ser posible acceder al equipo al igual que a sus recursos. DNS está, por definición, constituido por tres componentes principales :

- El espacio de nombres de dominio (*Domain Namespace*), que comprende los registros de los recursos asociados a este espacio.
- Los servidores de nombres DNS (DNS *Name Servers*).
- Los clientes DNS (DNS *Resolvers* o DNR).

Cuando se agrupan dominios relacionados entre sí, para permitir el uso compartido de los recursos globales, se crean agrupaciones denominadas **árboles de dominios (*tree*)** y **bosque de dominios (*forest*)**.

En *Active Directory* el **bosque (*forest*)** es una colección de uno o más dominios que comparten una misma **estructura lógica**, **catálogo global**, **esquema** y **configuración**. Un bosque permite combinar así divisiones diferentes en una organización o, incluso, pueden agruparse organizaciones distintas. Tener en cuenta que, todo dominio debe pertenecer a un bosque.

Un árbol de dominios (*tree*) es una colección de uno o más dominios que comparten un espacio de nombre contiguo. Aunque un árbol se puede componer de un único dominio, se pueden combinar varios dentro del mismo espacio de nombres en una estructura jerárquica. Cada árbol también se representa por un espacio de nombres contiguo. Por ejemplo, si el dominio raíz de una compañía es "empresa.com" y crea dominios diferentes para las divisiones de ventas y soporte, los nombres de dominio serían "ventas.empresa.com" y "soporte.empresa.com". A estos dominios se les denomina secundarios. Cada dominio genera automáticamente relaciones de confianza con sus subdominios. Como comentamos hace un momento, cuando se realiza una relación de confianza entre varios dominios con distinto espacio de nombres, se realiza una agrupación denominada **bosque (*forest*)**, por ejemplo, empresa1.com y empresa2.com.



Los dominios de un mismo bosque se conectan de forma transparente a través de **relaciones de confianza de dos sentidos** con seguridad basada en el protocolo **Kerberos**. Estas confianzas son permanentes, y no se pueden eliminar. Estas confianzas también son transitivas, es decir, si el dominio A confía en el dominio B y el dominio B confía en el dominio C, entonces el dominio A confía en el dominio C.

Todos los dominios dentro de un bosque comparten una definición formal de todos los tipos de objetos denominada **esquema**. Además, dentro de un bosque determinado, todos los dominios comparten el **catálogo global**. El catálogo global es un conjunto parcial de atributos que se replica a todos los controladores de dominio del bosque.

Otra ventaja de *Active Directory* es que se va a poder desinstalar de un equipo sin necesidad de tener que reinstalar todo el sistema operativo del servidor. Decir que, se denomina **servidor independiente** a un equipo servidor que no pertenece a ningún Dominio y **servidor miembro** a un equipo servidor que pertenece a un Dominio pero que no es controlador de dicho Dominio. Si un servidor miembro de un Dominio existente queremos que sea también **controlador de dominio** hay que realizar una acción que se denomina **promocionarlo a servidor de dominio.**

2.1.2.- Estructura física

Los **controladores de dominio** y los **sitios** son los dos componentes básicos que tienen que ver con la estructura física de Active Directory.

Windows 2012 R2 (y posteriores) NO tiene controladores de dominio principal (PDC, *Primary Domain Controller*) y controladores de dominio de reserva (BDC, *Backup Domain Controller*). **Todos los servidores que participan en la administración de la red en un entorno Windows 2022 se consideran controladores de dominio iguales.** Cada controlador de dominio (DC) almacena una copia duplicada de la base de datos del directorio, siendo el proceso de replicación es automático entre los controladores del dominio.

En las redes empresariales que abarcan varias ubicaciones geográficas, las implicaciones del diseño y la estructura de una red de área ancha son extremadamente importantes, pues la replicación de la base de datos del directorio requiere una comunicación rápida entre todos los controladores de dominio del bosque. Así, **un sitio de *Active Directory*** representa la topología física de la red en el directorio. Un sitio podría ser definido como un conjunto de subredes bien conectadas.

Mediante la configuración de sitios de *Active Directory* es posible optimizar los procesos de replicación, autenticación y localización de servicios en la red. Saber que, la cantidad de sitios no tiene relación con la de dominios; un sitio podría abarcar varios dominios (dentro de un mismo bosque) así como se podrían utilizar múltiples sitios para un único dominio. El sitio tiene relación con la estructura física mientras que el dominio con la estructura lógica.

Resumiendo.- Si en una empresa tenemos dos o más sedes separadas por una línea no muy rápida, tendremos que montar un dominio en cada sede o crear un único dominio indicando que cada sede es un sitio distinto de dicho dominio. Así conseguiremos que las replicaciones entre servidores tengan el mínimo tráfico posible.

3.- Componentes principales del *Active Directory*

Active Directory puede soportar prácticamente un número ilimitado de funciones y capacidades en una red de empresa, desde operaciones a pequeña escala hasta operaciones a gran escala multidominio.

Para crear el *Active Directory*, Microsoft tomó los conceptos de **X.500** y **LDAP**, y los moldeó con una serie de nuevos componentes para llegar a su estructura final. Así, *Active Directory* abarca los siguientes conceptos principalmente :

- Espacio de nombres
- Objetos
- Contenedor
- Esquema
- Catálogo Global
- Partición

3.1.- Espacio de nombres

Un espacio de nombres (*Namespaces*) es un área designada que tiene límites específicos donde se puede resolver un nombre lógico asignado a cada **objeto** del Active Directory. El uso principal de un espacio de nombres es organizar las descripciones de los recursos para permitir a los usuarios localizarlos por sus características o propiedades (**atributos** de los objetos). La base de datos del directorio para un espacio de nombres determinado se puede usar con el fin de localizar un objeto sin conocer su nombre. Si un usuario sabe el nombre de un recurso, puede consultar información útil acerca de ese objeto.

Una cuestión importante que hay que tener en cuenta es que el diseño del espacio de nombres determina, a la larga, el grado de utilidad que la base de datos representará para los usuarios a medida que crezca. Los algoritmos de ordenación y búsqueda no pueden vencer los inconvenientes de un diseño lógico inadecuado.

En lo que se refiere a la lógica, *Active Directory* de Windows es, simplemente, otro espacio de nombres. En *Active Directory* se almacenan dos tipos principales de información:

- La ubicación lógica del objeto.
- Una lista de **atributos** acerca del objeto.

3.2.- Objetos

El dominio está compuesto de **objetos**, éstos tienen atributos asignados, como un número de teléfono, ubicación de oficina, etc., y se pueden usar para localizar objetos en la base de datos del directorio. El uso de atributos para la búsqueda es incluso más importante cuando el esquema de *Active Directory* se extiende, es decir, se modifica. Cuando se agregan objetos, clases de objetos o atributos de esos objetos a la base de datos del directorio, su estructura determina su utilidad para los usuarios del directorio.

3.3.- Contenedores

Otro conjunto de elementos utilizados en el AD son los **Contenedores (*container*),** que son objetos que están diseñados para almacenar otros objetos del directorio. **Bosques (*forests*), árboles (*trees*), dominios (*domains*) y unidades organizativas (OU - *organizational unit*)** son todos los tipos de contenedores.

3.4.- Esquema

Se define el **Esquema del *Active Directory*** como el conjunto de clases de objetos, y sus atributos, que pueden ser creados en el *Active Directory*. Por ejemplo, a partir de la clase Usuario se pueden crear objetos cuenta de usuario que tiene ciertos atributos como contraseña, grupos a los que pertenece, carpeta personal, carpeta del perfil móvil, etc.

El esquema del AD es extensible, es decir, se pueden definir nuevas clases o atributos a las ya existentes. Así y todo, la modificación del esquema es "peligroso". Modificaciones inadecuadas pueden dañar o deshabilitar los controladores de dominio. Sólo los usuarios pertenecientes al grupo "*Schema Admins*" pueden realizar estas modificaciones.

3.5.- Catálogo Global

Un concepto interesante es el **Catálogo Global** (*global catalog*), se trata de la base de datos que contiene todos los objetos que pertenecen al bosque. AD construye el catálogo global replicando la información entre todos los controladores de dominio existentes en el bosque.

El servidor de catálogo global es un controlador de dominio que almacena una copia completa de todos los objetos del directorio de su dominio y una copia parcial, de solo lectura, de todos los objetos del resto de dominios del bosque.

Las copias parciales de solo lectura de los objetos que componen el catálogo global se describen como "parciales" porque incluyen un conjunto limitado de atributos: los atributos que requieren el esquema junto con los atributos que se usan con mayor frecuencia en operaciones de búsqueda de usuarios. Estos atributos se marcan para su inclusión en el conjunto de atributos parciales (PAS) como parte de sus definiciones de esquema. El almacenamiento de los atributos buscados con más frecuencia de todos los objetos del dominio del catálogo global hace que las búsquedas sean más eficaces para los usuarios sin afectar al rendimiento de la red con referencias innecesarias a controladores de dominio y sin requerir que un servidor de catálogo global almacene grandes cantidades de datos que no son necesarios.

Haciendo una analogía con las guías de teléfono antiguas, el catálogo global vendría a ser como las páginas amarillas, que nos facilitan la localización de distintos elementos cambiando el color de ciertos elementos, etc.

El catálogo global es el servicio que permite la resolución de muchas consultas comunes originadas desde cualquier parte del bosque. Por ejemplo, toda la información perteneciente a los "grupos universales", incluyendo sus miembros, se encuentra allí.

Por defecto, A*ctive Directory* almacena el catálogo global en el primer controlador de dominio de un nuevo bosque. Es posible mover o copiar el catálogo global a otro controlador de dominio.

3.6.- Partición

Active Directory está dividido en **particiones** (no las de los HDs), que permiten que redes muy grandes sean más manejables. Las particiones existentes son las siguientes:

- ***Domain partition.*** Esta partición contiene información sobre todos los objetos como usuarios, grupos, equipos y OUs de un dominio. Esta información es replicada a todos los controladores de dominio existentes en el interior del dominio, y un subconjunto de esta información es replicada en los servidores de catálogo global existentes en el bosque.
- ***Schema partition.*** Esta partición contiene definiciones de todos los objetos y sus atributos. Las reglas para la creación y el trabajo con ellos también se guardan ahí. Esta partición es replicada en todos los controladores de dominio del bosque.
- ***Configuration partition.*** Esta partición contiene información sobre la estructura del Active Directory en el bosque, incluyendo dominios, sitios y servicios. También es replicada a todos los controladores de dominio del bosque.
- ***Application partition.*** Esta partición contiene datos que ciertas aplicaciones necesitan que sean replicados por todo el bosque. Dependiendo de la aplicación la información se replicará a todos o a algunos controladores de dominio.

4.- Nomenclatura estándar de X.500 y LDAP.

Enlace interesante.

Iniciado con X.500 y ampliado por LDAP se trata de una serie de estándares que definen el modo de indicar la dirección exacta de los objetos en el interior del directorio.

Como el *Active Directory* emplea LDAP como el protocolo para acceder a los objetos en el directorio, es muy importante conocer su funcionamiento para poder aprovechar todas las posibilidades que nos brinda el *Active Directory*.

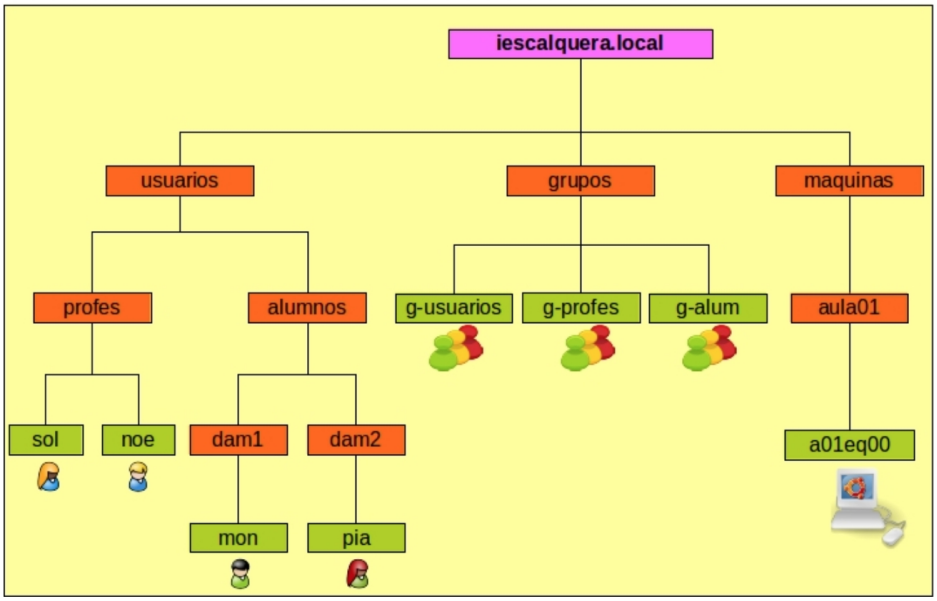
Las rutas de acceso incluyen los **Nombres Distinguidos (*Distinguished Names* – DN)** y los **Nombres Distinguidos Relativos (*Relative* DN – RDN).** También nos deberían ser familiares los **Nombres Principales de Usuario (*User Principal Names* - UPN)** y los **Identificadores Únicos Globales (*Globally Unique Identifiers* – GUID).**

4.1.- Distinguished Names - DN.

Cada uno de los objetos existentes en LDAP es identificado por su DN que define la dirección completa desde la cima del árbol LDAP hasta el propio objeto. Para lograr esto, en X.500 se definieron una serie de abreviaciones. La especificación completa de los DN, incluyendo su sintaxis y la lista completa de abreviaturas, está dada en la RFC 1779. Los más comunes son los siguientes:

- CN = *Common Name*
- OU = *Organizational Unit*
- DC = *Domain Component*
- O = *Organization Name*
- C = *Country Name*

Dos objetos distintos no pueden tener nunca el mismo DN. Para especificar el DN hay que incluir el nombre del objeto en sí y todos los contenedores hasta llegar a los mas alto del árbol.



4.2.- Relative Distinguished Names – RDN

El RDN es el atributo que distingue el objeto en sí.

Veamos un ejemplo:

DN: CN=sol,OU=Profes,OU=Usuarios,DC=iescalquera,DC=local

RDN: CN=sol

4.3.- User Principal Names

Además de los DN y RDN descritos anteriormente, AD también utiliza el concepto de UPN. El UPN es un atajo para que los usuarios puedan iniciar sesión o enviar un mail. Por ejemplo, para el DN visto anteriormente, el UPN sería: sol@profes.usuarios.iescalquera.local

4.4.- Globally Unique Identifiers

Todos los objetos guardados en el AD también tienen un único identificador llamado GUID, el cual es un número hexadecimal de 128 bits asignado cuando el objeto es creado. El GUID es creado en un atributo llamado "objectGUID", que existe en todos los objetos de AD. A diferencia de DN o RDN, este identificador nunca cambia aunque se mueva o renombre el objeto.

Por ejemplo, si tenemos un usuario, lo eliminamos y, luego, creamos otro usuario con los mismos atributos que el anteriormente eliminado, este nuevo usuario tendrá el atributo "objectGUID" distinto que el anterior. Los dos objetos serán distintos.

4.5.- Identificadores de seguridad

El identificador de seguridad (SID) es un valor que identifica de forma única una entidad de seguridad principal como un usuario, grupo, servicio o equipo en el interior del AD. No existen dos objetos en un bosque que tengan el mismo SID. El SID de un objeto sí puede cambiar en determinadas circunstancias, por ejemplo si ese objeto se mueve de un dominio a otro en un bosque.

Al igual que el GUID, si eliminamos un objeto y lo volvemos a crear con las mismas propiedades, ese objeto tendrá distinto SID.

Enlace objectGUID vs SID.

Ejemplo:

```
# Seleccionamos todas las propiedades del usuario "usuario1"
PS> $usuario1 = get-aduser -Identity usuario1 -Properties *
# Mostramos su ObjectGUID
PS> $usuario1.ObjectGUID.Guid
846d19a4-6062-4632-805d-d3872cb7ce67
# Mostramos su SID
PS> $usuario1.sid.Value
S-1-5-21-2537797745-3889458602-117915915-1108
```

4.6.- Active Directory Canonical Names

Es la versión del DN que muestra el *Active Directory*. Por ejemplo, en el DN visto anteriormente el *Active Directory Canonical Name* sería:

iescalquera.local/usuarios/profes/sol

5.- Componentes lógicos del *Active Directory*

En la creación de la estructura jerárquica de la base de datos de *Active Directory*, Microsoft facilitó la localización de recursos tales como carpetas e impresoras por su nombre en lugar de por la ubicación física. Estos bloques lógicos incluyen, tal y como ya nombramos antes, dominios, árboles, bosques y OUs.

Como el dominio es la unidad básica sobre la que se construye el *Active Directory*, lo introduciremos antes que los bosques y los árboles (donde los dominios se encuentran) y las UOs, que son contenedores que existentes en su interior.

5.1.- Dominios

El dominio representa el núcleo de la estructura de red. El dominio es un agrupamiento de ordenadores que comparten un directorio y unas normas de seguridad comunes.

Aunque un dominio es una unidad en sí misma que no necesita ningún otro dominio para su perfecto funcionamiento, en *Active Directory*, se pueden tener una serie de dominios organizados en "árboles" y "bosques", con relaciones de confianza entre ellos. Así y todo, en un dominio Windows 2016 el número de objetos puede llegar a ser de millones.

El archivo donde se guarda la base de datos del AD que define el dominio es **ntds.dit**. Cada dominio tiene su propio archivo ntds.dit, que está replicado en todos los controladores de dominio (*multimaster replication*).

Algunos beneficios de utilizar múltiples dominios son los siguientes :

- Los dominios pueden ser considerados como límites de seguridad. En otras palabras, los administradores de cada dominio pueden definir ACLs que determinan los derechos de acceso y los permisos sobre los objetos de su dominio.
- También, cada administrador tiene la autoridad de configurar las políticas de seguridad sólo sobre los objetos de su dominio (*Group Policies*).
- Una compañía multinacional podrá elegir entre hacer un gran dominio o un dominio específico en cada país. Para así adaptarse mejor a las normas de cada país en concreto.

5.2.- Árboles

Un árbol es un grupo de dominios que comparte un espacio de nombres contiguo. En otras palabras, un árbol consiste en un dominio padre que tiene un conjunto de dominios hijos cuyos nombres reflejan el del padre.

Por ejemplo, un dominio padre llamado **empresa.com** puede tener de dominios hijo **productos.empresa.com**, **oficinas.empresa.com**, etc. El número de hijos puede seguir creciendo **america.productos.empresa.com**…

Todos los dominios en un árbol están vinculados tú a tú, con relaciones de confianza transitivas; en otras palabras, las cuentas en un mismo dominio pueden acceder a los recursos de otro dominio y viceversa.

5.3.- Bosques

Un bosque consiste en un grupo de árboles que no comparten un espacio de nombres contiguo.

Por defecto, existe relación de confianza transitiva entre los dominios principales de cada árbol que pertenece a un bosque.

Saber que, todos los dominios en un bosque comparten un esquema común y el catálogo global. En un bosque, un dominio tiene que ser el dominio raíz del bosque (*forest root domain*). El dominio raíz es siempre el primer dominio creado cuando se creó el bosque.

5.4.- Unidades organizativas

Una unidad organizativa (OU) es un subgrupo lógico de un dominio. Se emplean para dividir los recursos que pertenecen a un grupo, sección, departamento, etc. en el interior de una compañía y así poder aplicar distintas Directivas de Grupo sólo a esos recursos.

La idea es crear una jerarquía de Unidades Organizativas que nos permitan una configuración adaptada a nuestras necesidades.

También son utilizadas para delegar el control de actividades administrativas a ciertos usuarios. Se introducen los recursos en una OU sobre los que queremos delegar el control a un usuario.

Se pueden introducir en una OU: Otras OUs, Grupos, Usuarios, equipos, impresoras, etc. El mínimo elemento sobre el que podemos aplicar una directiva de grupo es una OU.

Una división típica en OUs dentro de un dominio son Usuarios y Equipos, y dentro de equipos, por ejemplo, servidores miembros, controladores de dominio, equipos clientes, etc.

6.- Componentes físicos del *Active Directory*

En contraste con el agrupamiento local del *Active Directory* en bosques, árboles, dominios y OUs, Microsoft también incluye varios componentes físicos como sitios, controladores de dominio, servidores del catálogo global y maestros de operaciones.

6.1.- Sitios

El concepto de sitio permite agrupar juntos recursos en el interior de un bosque de acuerdo con la localización física y las subredes. Así, un sitio es un conjunto de una o más subredes IP que están conectadas por una red de alta velocidad (como una red de área local).

El empleo de sitios nos permite controlar la replicación de los datos en el interior de la base de datos de *Active Directory*. También permite aplicar políticas de grupo distintas o delegar el control administrativo de cierto conjunto de objetos existentes en una localización física. Se deberían configurar varios sitios sólo si están separados por un enlace de baja velocidad, si esa no es la situación, no se recomiendan.

6.2.- Controladores de dominio

Cualquier servidor en el que se instaló el *Active Directory* es un controlador de dominio (DC). Todos estos servidores permiten la autenticación de los usuarios en el dominio donde se encuentren y, también, permiten la administración de *Active Directory*.

Un controlador de dominio almacena la copia completa de todos los objetos del dominio, además del esquema e información relevante del bosque en el que se encuentre localizado el dominio.
Teniendo más de un DC en un dominio conseguimos:

- Tolerancia a fallos. Si un servidor de dominio cae, otro está activo para la autenticación, etc.
- Balanceo de cargas. Todos los DC participan igual en las actividades del dominio, distribuyendo así la carga a lo largo de varios servidores. Esta configuración optimiza la velocidad de las respuestas.

6.3.- Servidores del Catálogo Global

El catálogo global es el subconjunto de la información del dominio creado con el propósito de que otros controladores de dominio del mismo bosque consigan encontrar recursos de dicho dominio.

Por defecto, el primer controlador de dominio instalado en un nuevo dominio se convierte en servidor de catálogo global. También se pueden designar otros servidores de dominio como servidores de catálogo global.
El servidor de catálogo global realiza las siguientes funciones:

- Localiza objetos en el interior del bosque.
- Autentica usuarios por su UPN.
- Proporciona información a los miembros de grupos universales.

6.4.- Maestros de operaciones

Microsoft diseñó *Active Directory* de tal modo que se pueden realizar la mayor parte de las tareas de administración desde cualquier controlador de dominio. Sin embargo, existen ciertas tareas que sólo se pueden realizar desde controladores de dominio determinados, estos servidores son conocidos como Maestros de operaciones (*Operations masters* ó *Flexible Single-Master Operations* -FSMO).
Las funciones de las que hablamos son las siguientes:

- Maestro de esquema.
- Maestro de nombres de dominio.
- Emulador de PDC.
- Maestro de infraestructura.
- Maestro RID (*Relative Identifier*). Que asigna los SID a los objetos creados en su dominio.

7.- Nivel Funcional del Bosque y del Dominio

Los Niveles Funcionales determinan las capacidades que están disponibles del dominio o del bosque de Servicios de Dominio de *Active Directory* (AD DS). También determinan los sistemas operativos *Windows Server* que se pueden ejecutar en los controladores de dominio del dominio o del bosque.

Por otro lado, los niveles funcionales NO afectan a los sistemas operativos que se pueden ejecutar en las estaciones de trabajo y en los servidores miembros que están unidos al dominio o al bosque.

Cuando implementamos AD DS, mejor establecer los niveles funcionales del dominio y del bosque en el valor más alto que admita nuestro entorno. De este modo, se podrá emplear el mayor número posible de características de AD DS.

Por ejemplo, si estamos seguros de que nunca se agregará al dominio o al bosque controladores de dominio que ejecuten Windows Server 2008, mejor seleccionar el nivel funcional de Windows Server 2012 (o, del mismo modo Windows 2012 R2) durante el proceso de implementación. Por el contrario, si existe posibilidad de que se vaya a conservar o agregar algún controlador de dominio que ejecute Windows Server 2008, hay que seleccionar el nivel funcional de Windows Server 2008.

8.- Grupos de Seguridad de *Active Directory*. Alcance

Los Grupos se utilizan en AD para agrupar usuarios y así poder configurar distintas ACLs sobre objetos del AD.

Para poder configurar mejor esta "seguridad" tenemos en el AD varios tipos de grupos que tienen distinto "alcance".

El ámbito de un grupo determinado indica qué objetos puede contener ese grupo, limitando a objetos del mismo dominio o permitiendo objetos de otros dominios. También controla donde puede ser utilizado ese grupo, en el dominio o en cualquier dominio del bosque.

8.1.- Grupos Locales del Dominio

Los Grupos Locales del Dominio pueden tener en su interior los siguientes miembros:

- Usuarios
- Equipos
- Grupos Globales de cualquier Dominio del Bosque
- Grupos Universales
- Grupos Locales del mismo Dominio

Así, los grupos locales se emplean para asignar permisos a recursos en el mismo dominio al que pertenece ese grupo local.

8.2.- Grupos Globales

Los Grupos Globales pueden tener los siguientes miembros:

- Usuarios
- Equipos
- Otros Grupos Globales del mismo dominio

Se pueden emplear Grupos Globales para configurar permisos sobre recursos localizados en cualquier dominio de un bosque. Esto se puede conseguir añadiendo el grupo global como miembro de un grupo local que tenga los permisos requeridos.

Un grupo global puede ser miembro de otro grupo global sólo si los dos están en el mismo dominio.

8.3.- Grupos Universales

Los Grupos Universales pueden tener cualquiera de los siguientes tipos de miembros:

- Usuarios
- Equipos
- Grupos Globales de cualquier dominio del Bosque
- Outros Grupos Universales

Teniendo esto en cuenta, podemos configurar el acceso a objetos de un dominio del bosque empleando grupos locales haciendo que los universales sean miembro de ellos.

Se pueden emplear también grupos universales para configurar permisos a grupos y cuentas que, o bien abarcan varios dominios o todo el bosque.

Se usan los grupos con ámbito Universal para consolidar los grupos que abarcan varios dominios.

Un punto importante en el empleo de los grupos universales es que la pertenencia a ellos no debe cambiar a menudo, pues los grupos universales son almacenados en el catálogo global. Los cambios de usuarios y grupos pertenecientes a grupos universales son replicados a todos los servidores de catálogo global del bosque. Si estos cambios se realizan a menudo pueden consumir mucho ancho de banda.

8.4.- Anidamiento de grupos

Como discutimos antes, el anidamiento de grupos es el hecho de agregar un grupo como miembro de otro grupo. Por ejemplo, cuando hacemos un grupo global como miembro de un grupo universal, se dice que se hizo un anidamiento a un grupo universal.

El anidamiento de grupos reduce el número de veces que hay que asignar permisos a usuarios en diferentes dominios de un bosque. Por ejemplo, si tenemos múltiples dominios hijos en nuestro AD, y existen usuarios de cada dominio que necesitan acceder a una base de datos localizada en el dominio padre, el modo más sencillo de hacerlo sería el siguiente:

- Crear un grupo global en cada dominio que contenga todos los usuarios que necesitan acceder a la base de datos.
- Crear un grupo universal en el dominio padre. Y luego poner como miembros de este dominio los grupos globales antes creados.
- Agregar el grupo universal a un grupo local para asignarle los permisos necesarios para acceder a la base de datos.

En el caso que más nos vamos a encontrar, que es, un único dominio en un bosque, lo normal es emplear Grupos Globales de Seguridad anidados y, los permisos, directamente aplicados a estos Grupos Globales.

Por defecto existen un conjunto de grupos y usuarios en el dominio, estos objetos deben permanecer en los contenedores predeterminados y bajo el control del propietario del dominio:

- Administrador
- Invitado
- KRBTGT
- Administradores de Dominio
- Usuarios del Dominio
- Equipos del Dominio
- Editores de Certificados
- Administradores del Esquema
- Administradores de Empresa

9.- Diseño de la estructura de Unidades Organizativas

9.1.- Group Policy (Directivas de Grupo)

Aunque primero es diseñar la estructura de unidades organizativas para la delegación de administración, luego, lo normal, es crear niveles adicionales de unidades organizativas para fines de aplicar Directivas de Grupo.

Las Directivas de Grupo (GPO - *Group Policy Object*), tienen como misión agrupar la configuración de varios parámetros para poder aplicarlos de forma conjunta sobre cierto número de objetos del dominio (usuarios, equipos).

Con el Windows Server 2003, Microsoft introduce una consola de administración de directivas de grupo, denominada comúnmente GPMC (*Group Policy Management Console*), que nos facilita su administración y despliegue.

Las Directivas de Grupo pueden usar también Grupos de Seguridad para filtrar su alcance, es decir, para aplicar una configuración de directiva de grupo a un subconjunto de los objetos en una unidad organizativa sin crear una unidad organizativa secundaria.

Por ejemplo, se podría crear una configuración de directiva de grupo para aplicar solo a los usuarios que pertenecen al grupo G-Profesores, incluso si la unidad organizativa contiene todos los usuarios de ese Dominio. Para lograr esto, se debe aplicar la configuración de la Política de grupo a la unidad organizativa, luego crear el grupo G-Profesores y cambiar los permisos de la Política para que se apliquen solo a ese grupo.

Por el contrario, para delegar la administración de un subconjunto de una OU, se debe siempre crear una OU secundaria. Debido a que puede lograr un control preciso del alcance de la GPO con Grupos de Seguridad, la delegación de administración siempre tiene prioridad en el proceso de diseño de OU.

> **Nota:** Recuerda que no se puede aplicar la configuración de una Directiva de grupo a los contenedores predeterminados de ***Users*** y ***Computers***. Estas **NO SON unidades organizativas** y no se pueden colocar nuevas OUs en su interior, por lo que no se pueden usar para aplicar Directivas de grupo.

Se recomienda que acepte los valores predeterminados establecidos en la **Política Predeterminada de Dominio** y la **Política Predeterminada de Controladores de Dominio**, con la excepción de los siguientes puntos, que se deben personalizar para cumplir con los requisitos de seguridad requeridos:

- **Política Predeterminada de Dominio:**
  - Política de contraseñas
  - Política de bloqueo de cuenta
  - Política Kerberos
- **Política Predeterminada de Controladores de Dominio:**
  - Asignación de derechos de usuario

Otras configuraciones de Directiva de grupo (aquellas no relacionadas con la seguridad) no deben establecerse dentro de estas Configuraciones Predeterminadas de Directiva de Grupo; en su lugar, debe crearse Nuevos Objetos de Directiva de Grupo (GPO).

9.2.- Diseño de las OUs

El propietario del dominio es responsable de completar un diseño de OU para el dominio. El diseño debe contener:

- Un diagrama de la jerarquía de OUs.
- Una lista de OUs. Para cada OU:
- Su propósito.
- Una lista de usuarios o grupos que tienen control sobre la OU o los objetos que contiene.
- El tipo de control que tienen sobre la clase de objetos en la OU.

> **Nota:** Aunque el propietario de la OU tiene delegado el control sobre un subárbol de objetos, el propietario del dominio conserva el control total sobre todos los subárboles.

Cuando una computadora se une a un dominio de *Active Directory*, si no existe una cuenta para esa computadora, se creará una en el contenedor de *Computers*. Para evitar esto, cree previamente la cuenta de la computadora en la unidad organizativa adecuada.