

TEMA 6

El Directorio Activo en Windows Server 2016

1. Introducción al Directorio Activo

En este tema veremos qué es el Directorio Activo, cómo se instala y una configuración básica del **Active Directory o Servicios de Dominio de Active Directory (AD DS)**, nosotros lo llamaremos **Directorio Activo** porque está ampliamente utilizado este nombre.

1.1. Definición

En una red de Microsoft Windows Server 2016 (también en 2012-2000), el **servicio de Directorio Activo** proporciona:

1. **la estructura**
2. **las funciones para organizar, administrar y controlar el acceso a los recursos de red.**

El Directorio Activo proporciona también la **capacidad de centralizar la administración de la red** de Windows Server 2016.

Esta capacidad significa que almacena en un único sitio la información sobre los recursos de nuestra empresa: información de usuarios, grupos e impresoras. Esto permite que desde una sola ubicación y con la consola administrativa tengamos la capacidad de controlar el Directorio completamente.

El Directorio Activo es el servicio de directorio de una red de Windows Server 2016 que **almacena información sobre los recursos de la red y permite que los mismos resulten accesibles a los usuarios y a las aplicaciones.**

Los servicios de directorio proporcionan una manera coherente de nombrar, describir, localizar, tener acceso, administrar y asegurar la información relativa a los recursos de red.

1.2. La funcionalidad

El Directorio Activo proporciona funcionalidad de servicio de directorio, como medio para organizar, administrar y controlar centralmente el acceso a los recursos de red.

Así mismo hace que la topología física de red y los protocolos pasen desapercibidos, de manera que **un usuario de una red pueda tener acceso a cualquier recurso sin saber dónde está el mismo o cómo está conectado físicamente a la red.**

El Directorio Activo está organizado en secciones que permiten el almacenamiento de una gran cantidad de objetos. Como resultado, **es posible ampliar** el Directorio Activo a medida que crece una organización (modular), permitiendo que una organización que tenga un único servidor con unos cuantos centenares de objetos crezca hasta tener miles de servidores y millones de objetos.

Un servidor que ejecuta Windows Server 2016 almacena:

- la configuración del sistema
- la información de las aplicaciones
- la información acerca de la ubicación de los perfiles de usuario.

En combinación con las directivas de grupo, el Directorio Activo **permite a los administradores controlar escritorios distribuidos, servicios de red y aplicaciones desde una ubicación central**, al tiempo que utiliza una interfaz de administración coherente.

Además, el Directorio Activo proporciona un control centralizado del acceso a los recursos de red, al permitir que los usuarios sólo inicien sesión una sola vez para obtener pleno acceso a los recursos mediante el Directorio Activo.

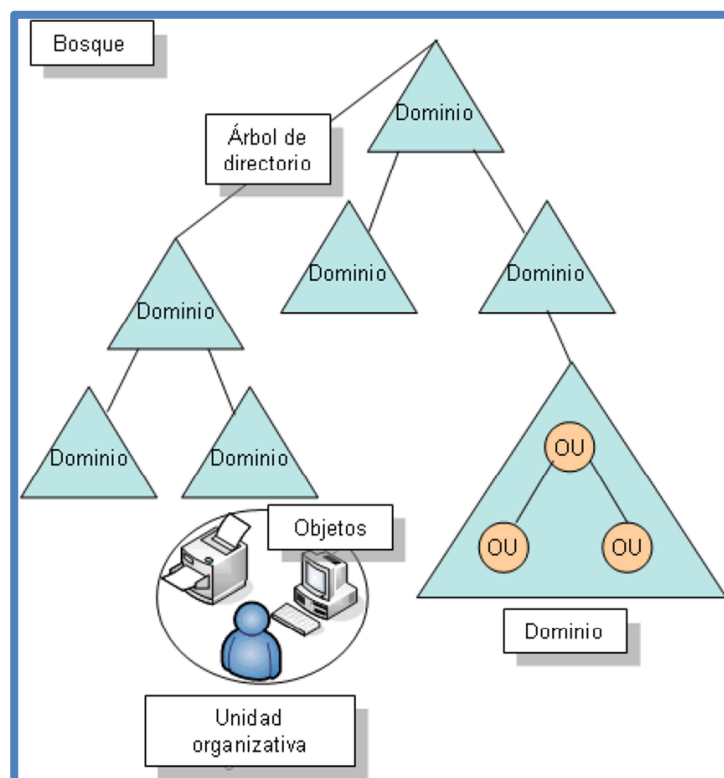
1.3. Estructura Lógica del Directorio Activo

El Directorio Activo proporciona el almacenamiento seguro de la información sobre objetos en su estructura jerárquica lógica.

Los **objetos** de Active Directory representan:

- **usuarios**
- **recursos** (por ejemplo, ordenadores e impresoras)

A su vez algunos objetos pueden ser "contenedores" de otros objetos, por ejemplo, un grupo de usuarios o unidades administrativas, bajo un nombre "Informática" están todos los usuarios de ese departamento.

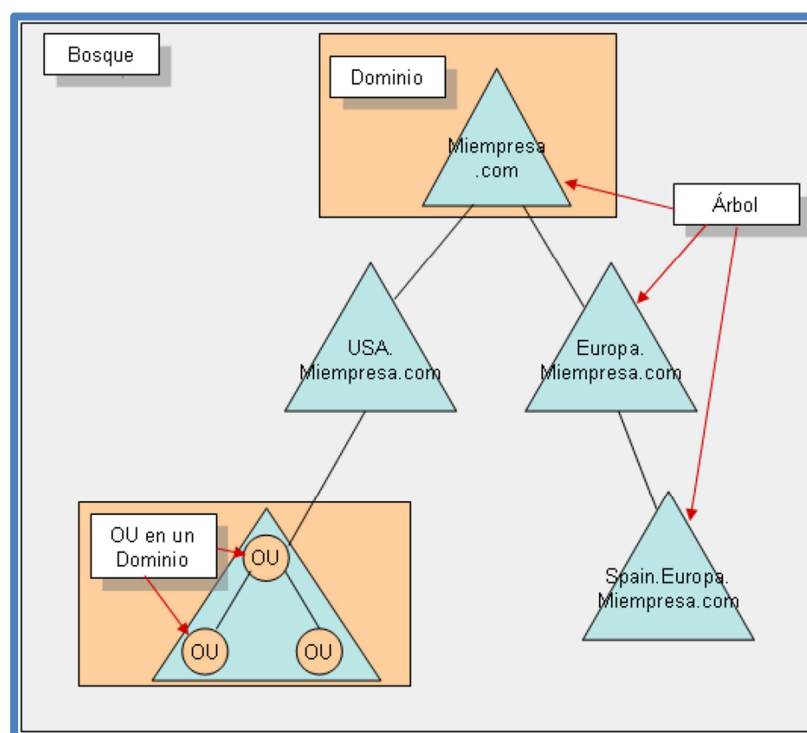


La **estructura lógica de Active Directory** incluye los siguientes componentes:

- **Objetos.** Son los componentes básicos de la estructura lógica (usuarios y recursos).
- **Clases de objetos.** Son las plantillas o los modelos para los tipos de objetos que se pueden crear en Active Directory. Cada clase de objeto es definida por un grupo de atributos, los cuales definen los valores posibles que se pueden asociar a un objeto. Cada objeto tiene una combinación única de los valores de atributos. Por ejemplo {usuarios}, {equipos}, {impresoras}, etc.
- **Unidades organizativas.** Podemos utilizar estos objetos contenedores para organizar otros objetos con propósitos administrativos, por ejemplo, dividir nuestra empresa en departamentos. Organizando éstos es más fácil localizar y administrar objetos. También podemos delegar la autoridad para administrar estas unidades organizativas de manera que podemos tener administradores de cada una de ellas.
- **Dominios.** Son las unidades funcionales clave de la estructura lógica de Active Directory, son colecciones de los objetos administrativos definidos, que comparten en una base de datos común del directorio, políticas de la seguridad y relaciones de confianza con otros dominios. Los dominios proporcionan las tres funciones siguientes:
 - ✓ Un límite administrativo para los objetos
 - ✓ Medios de administrar la seguridad para los recursos compartidos
 - ✓ Una unidad de réplica para los objetos
- **Árbol de dominios.** Son dominios agrupados en estructuras jerárquicas. Cuando se agrega un segundo dominio a un árbol, se convierte en hijo del dominio raíz. El dominio al cual un "dominio hijo" se une se llama "dominio padre". El dominio hijo a su vez puede tener sus propios hijos, combinándose con el nombre de su padre para formar su propio y único nombre, Domain Name System (DNS). Por ejemplo "ventas.miempresa.com" "ventas" sería un dominio hijo del principal "miempresa.com"
- **Bosque.** Un bosque es una instancia completa del Directorio Activo y consta en uno o más árboles. En un solo árbol de dos niveles, lo recomendado para la mayoría de las organizaciones, todos los dominios hijos se hacen "hijos" del dominio raíz del bosque para formar un árbol contiguo. El primer dominio en el bosque se llama Dominio raíz del bosque y el nombre de ese dominio se refiere al bosque, por ejemplo, miempresa.com. Por defecto, la información en Active Directory se comparte solamente dentro del bosque. De esta manera, la seguridad del bosque estará contenida en una sola instancia de Active Directory. Así que la mayoría de las veces nuestra organización será de un sólo dominio (miempresa.com) dentro de un solo bosque.

Nota: Un bosque comparte un espacio de nombres contiguo: usa.miempresa.com<->europa.miempresa.com.

Veamos algunas recomendaciones para la creación de la estructura.



Cuanto más Bosques, Árboles y Dominios tengamos más complejo será administrarlo llegando a unos niveles de complejidad insoportables así que debemos diseñar bien nuestra estructura de red.

Algunas recomendaciones:

- Tengo una empresa de **hasta 50 equipos** en una sola oficina, aunque sean varias plantas, el caso es que es que es una unidad conectada por switches y demás.
En este caso un sólo bosque con un sólo árbol y un sólo dominio, es decir la estructura más sencilla funcionará perfectamente: "miempresa.com"
- Tengo **más de 100 equipos** y algunos de ellos están conectados por VPN (redes virtuales), es decir, a través de Internet con la planta principal.
En este caso seguimos recomendando la anterior, todo una estructura lógica de un solo bosque árbol-dominio: "miempresa.com"
- Tengo **dos empresas grandes con el mismo tamaño** en equipos y separadas por una conexión "lenta": Internet, Frame Relay,... En ese caso para independizar las dos administraciones ya que se necesitará más de un administrador lo suyo es un solo bosque, pero con un árbol de dos dominios: "norte.miempresa.com" y "sur.miempresa.com"

La idea es evitar en lo posible la creación de bosques porque aumentan mucho la complejidad y administración. Tienen sentido por ejemplo en una gran empresa multinacional donde cada país representaría una rama de un bosque. En ese caso si es necesario el bosque.

1.4. Estructura física de Active Directory

En contraste con la estructura lógica y los requisitos administrativos, la **estructura física del Directorio Activo optimiza el tráfico de la red**.

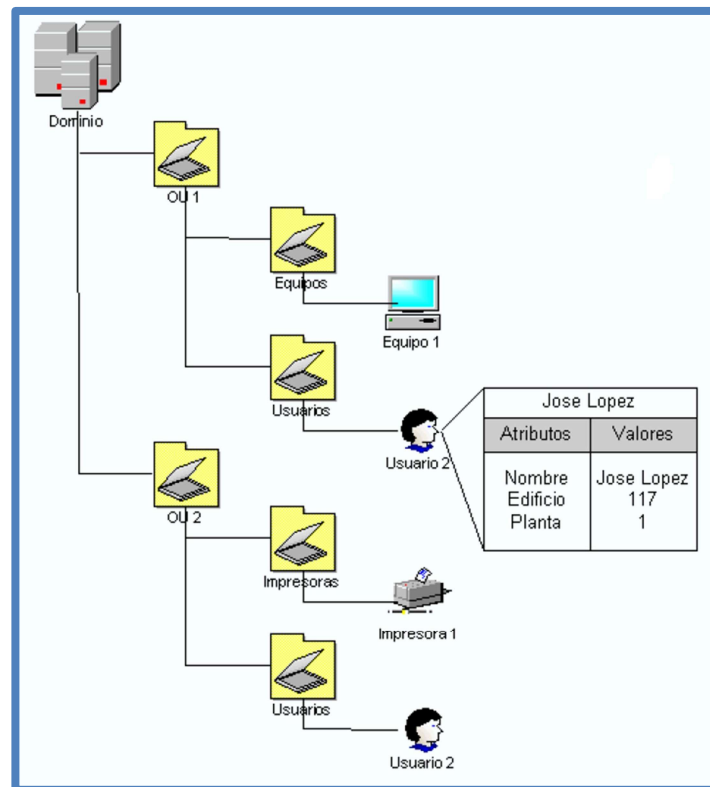
Estas van a ser las partes en las que se divide internamente el Directorio Activo y las que deberán estar perfectamente ensambladas para crear la estructura de red. En nuestro caso, que tendremos redes muy sencillas sólo utilizaremos una parte de toda esta estructura de red.

Los elementos de la estructura física del Directorio Activo son:

- **Controladores de Dominio.** Son servidores ejecutando Windows Server y el Directorio Activo. Cada controlador de dominio realiza funciones de almacenamiento y replicación y sólo pueden contener un dominio. Para asegurar una disponibilidad continua del Directorio Activo, cada dominio debe tener más de un controlador de dominio. Esto asegura que podamos seguir trabajando en caso de error en el controlador principal.
- **Sitios del Directorio Activo.** Los sitios son grupos de equipos conectados, por ejemplo, las distintas plantas o delegaciones de una empresa y pertenecen al dominio principal creado en el anterior punto.
En contraste con la agrupación lógica que hemos visto antes de forma jerárquica, se incluye ahora el concepto de *Site* para agrupar recursos dentro de un bosque de acuerdo con su ubicación física o subred. Un sitio puede contener objetos de más de un dominio o árbol dentro del bosque y árboles individuales pueden contener más de un sitio. La utilización de sitios permite controlar la replicación de datos de las bases de datos del Directorio Activo y aplicar distintas directivas dependiendo solo de su ubicación física.
Normalmente definiremos un único "site" a todos los recursos que estén en nuestra red local.
- **Catálogo Global.** El catálogo global es una parte de información del dominio creado con el propósito de habilitar a controladores de dominio de otros dominios del mismo bosque a localizar recursos de cualquier dominio. Por ejemplo, los usuarios que estén buscando recursos como ficheros, carpetas o impresoras de otro dominio lo harán en el catálogo global para así buscar no solo en su dominio sino en la base de datos completa de un bosque. El catálogo global también nos va a permitir iniciar una sesión en otro dominio que no sea el nuestro poniendo simplemente el "nombre principal de usuario" (UPN) que es el nombre construido en forma de email: usuario@dominio.com.

2. Servicios de directorio

Un **servicio de directorio** es un **depósito estructurado de información sobre personas y recursos** en una organización. En una red Windows Server 2016, el servicio de directorio es el Directorio Activo.



Un servicio de directorio fundamentalmente:

- **Permite a usuarios y aplicaciones tener acceso a la información sobre objetos.**

Esta información se almacena en forma de propiedades, por ejemplo, el nombre de un usuario es una propiedad del objeto "usuario".

Buscaremos objetos basándonos en su clase, atributo, valor del atributo, localización dentro de la estructura del Directorio Activo, o con cualquier combinación de estos valores.

- **Hace transparentes la topología y los protocolos físicos de la red.**

El "maestro de infraestructura" se encarga de configurar la disposición de los controladores de dominio, después todo se maneja como un único sitio lógico.

De esta manera, un usuario en una red puede tener acceso a cualquier recurso, por ejemplo, a una impresora, sin saber dónde está el recurso o dónde está conectado físicamente con la red y permite el almacenamiento de gran cantidad de objetos.

Dado que se organiza en particiones, el Directorio Activo puede ampliarse a la vez que crece la organización.

Por ejemplo, un directorio puede ampliarse de un solo servidor con algunos objetos a millares de servidores y millones de objetos.




2.1. El Esquema

El esquema del Directorio Activo contiene las definiciones de todos los objetos, como, por ejemplo, usuarios, equipos e impresoras almacenados en él.

Es decir, cuando creamos un usuario le ponemos distintos parámetros o atributos: nombre, teléfonos, departamento, todos estos son valores del esquema.

En un controlador de dominio hay solamente un esquema para todo el bosque, de esta manera, todos los objetos que se crean en el directorio cumplen con las mismas reglas.

El esquema tiene dos tipos de definiciones: *Clases de objetos y atributos*:

Objetos	Atributos propiedades
	Nombre Departamento Contraseña
	Nombre Ubicación
	Nombre Ubicación

En la programación orientada a objetos se define la clase como una plantilla para crear objetos. Es decir, para crear un botón en un formulario de Windows utilizaremos la clase "Botón".

Esta clase le dice al programa de qué partes se compone el botón y como debe crearlo. Una vez creado ya existe el objeto "botón" en el formulario y se puede utilizar, **las clases son pues, las plantillas para crear los objetos**.

Esos botones que creamos tienen además una serie de propiedades: color, tamaño, que identifican su aspecto, a estos valores se les llama atributos o propiedades.

Un ejemplo de clase son los usuarios, los ordenadores y las impresoras que describen los objetos posibles que se pueden crear en el directorio.

Cada objeto tiene una colección de atributos. Cada atributo se define solamente una vez y se puede utilizar en muchos objetos.

Por ejemplo, el atributo de la descripción se utiliza en muchos objetos: equipos, usuarios, ... pero se define solamente una vez en el esquema para asegurar consistencia.

2.2. El Catálogo Global

El catálogo global es un contenedor de información de los atributos de todos los objetos del Directorio Activo.

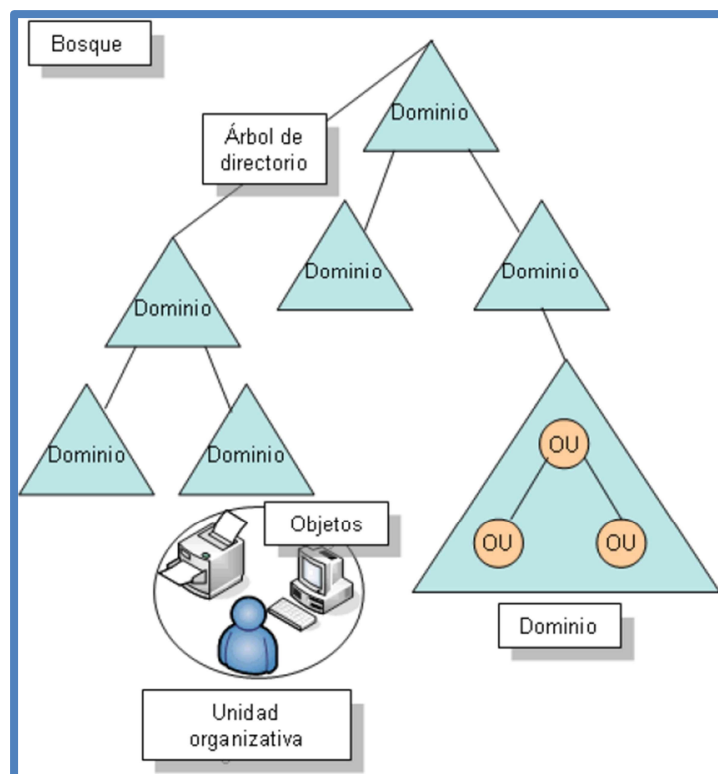
Los miembros del grupo "**Administradores del esquema**" pueden cambiar los atributos que se almacenan en el Catálogo Global, dependiendo de los requisitos de la organización.

El catálogo global contiene:

1. Los atributos que se utilizan con más frecuencia en las consultas, por ejemplo, nombre, apellidos, nombre de usuario, ...
2. La información que necesaria para determinar la localización de cualquier objeto en el directorio.
3. Un subconjunto por defecto de los atributos para cada tipo de objeto.
4. Los permisos de acceso para cada objeto y atributos, almacenados en el Catálogo Global. Si buscamos un objeto y no tenemos los permisos apropiados para acceder a él, el objeto no aparecerá en los resultados de la búsqueda. Los permisos de acceso aseguran que los usuarios puedan encontrar solamente los objetos a los que se les han asignado el acceso.

2.3. Nombres distinguidos y nombres distinguidos relativos

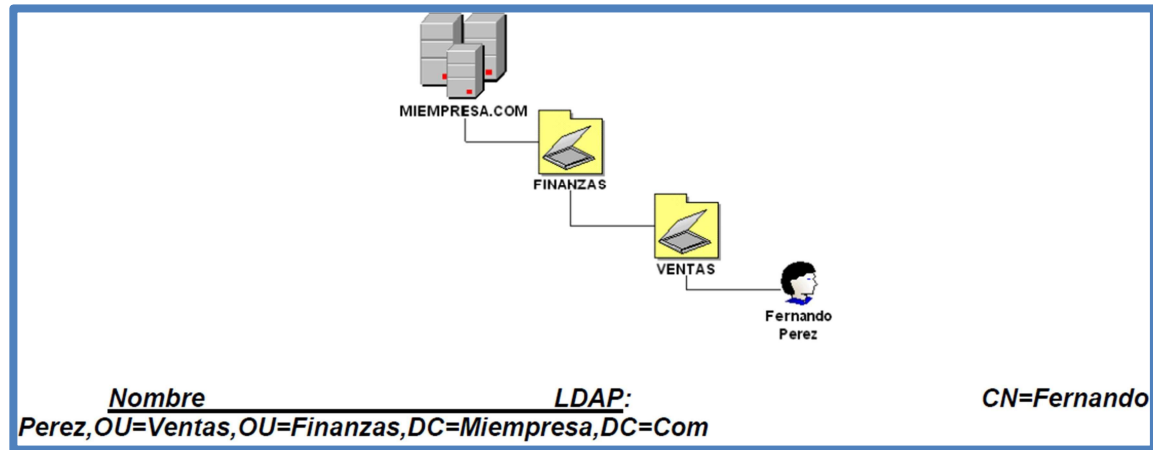
Sabemos que estamos trabajando con una estructura jerárquica cuando estamos con el Directorio Activo; hay una raíz principal y de ahí se expanden otros objetos como unidades organizativas, usuarios, equipos, ...



Existe **un servicio estándar que se encarga de ponerle nomenclatura a estos objetos y así poder consultarlos y trabajar con ellos de forma normalizada.**

Este servicio se llama **LDAP** (*Lightweight Directory Access Protocol, Protocolo Ligero de Acceso a Directorios*).

Por ejemplo, fíjate en el gráfico y su nombre al interpretarlo en el árbol:



Así que **LDAP es el servicio que utiliza internamente el Directorio Activo para poder consultar su catálogo.**

Este servicio utiliza un nombre que representa objetos en el Directorio Activo que mantiene la estructura jerárquica del sistema de dominios.

Esta representación se llama "**Nombre Distinguido**" del objeto e identifica el **dominio donde se localiza el objeto** y la **trayectoria completa** para alcanzar el objeto. Este nombre distinguido es único en el bosque del directorio activo.

El "**nombre distinguido relativo**" de un objeto identifica únicamente **el objeto en su contenedor**. Dos objetos en el mismo contenedor no pueden tener el mismo nombre. Y el nombre distinguido relativo siempre es el primer componente del nombre distinguido.

Por ejemplo, si un usuario se llama "José Rodríguez" de la Unidad Organizativa "Informática" del dominio "miempresa.com"... el nombre distinguido de cada elemento de la estructura lógica sería:

CN=Jose Rodriguez,OU=Informática,DC=miempresa,DC=com

y su **nombre distinguido relativo** sería: **CN=Jose Rodriguez**




- **CN** es el **Common Name** (Nombre principal o común) del objeto en su contenedor.
- **OU** es la **Organizational Unit** (Unidad organizativa) que contiene el objeto. Puede haber más de un valor de OU si el objeto está en una Unidad Organizativa anidada dentro de más niveles.
- **DC** es el **Domain Component** (el dominio), por ejemplo .com. o .msft. Hay siempre al menos dos Domain Components: miempresa.com

Los "domain components" de los nombres distinguidos están basados en el sistema de nombres de dominio (DNS).

2.4. Herramientas del Active Directory

Windows Server 2016 proporciona varios complementos para las consolas MMC y herramientas de línea de comandos para administrar el Directorio Activo.

La tabla siguiente describe los complementos administrativos que más utilizaremos en la administración del Directorio Activo, que están en la consola MMC o en el menú **Herramientas del Administrador del Servidor**. Usaremos únicamente el primero.

Complemento	Descripción	Menú
Usuarios y equipos de Active Directory	Administra y publica la información en el directorio, sin duda será la más utilizaremos ya que será donde administremos cuentas de usuarios, equipos, grupos. Podremos añadir equipos al dominio, administrar políticas, en fin, el centro de nuestro directorio.	 Usuarios y equipos de Active Dire
Dominios y confianzas de Active Directory	Administra las relaciones de confianza entre dominios y bosques. Poco uso porque es para estructuras muy complejas.	 Dominios y confianzas de Active Di
Sitios y servicios de Active Directory	Administra las réplicas del directorio. Imprescindible si tenemos varias localizaciones que administrar.	 Sitios y servicios de Active Direct