Dominios en Windows Server

1. Introducción al concepto de directorio y dominio

En el sentido más amplio, un directorio no es más que una lista detallada de objetos. Por ejemplo, una guía de teléfonos es un tipo de directorio que guarda información sobre personas, empresas y otras entidades. De cada uno de los elementos representados, se almacena su nombre, dirección y número de teléfono.

En muchos sentidos, *Active Directory Domain Services* (*AD DS*) es muy parecido a una guía telefónica, aunque resulta más flexible. Se basa en el concepto de dominio que introdujo *Windows NT* con el fin de facilitar la administración. Sin embargo, ahora el objetivo es crear una estructura dinámica y fácilmente accesible, a través de la que se puede almacenar la información de toda la organización, tanto relativa a la estructura del propio directorio como de su administración, y acceder a ella de forma centralizada.

Active Directory está basado en una serie de estándares establecidos por la Unión Internacional de Telecomunicaciones (UIT) llamados X.500.

El protocolo LDAP se creó como una versión ligera de X.500

AD DS puede almacenar información sobre la organización, sitios, ordenadores, usuarios, objetos compartidos y cualquier otra cosa que pueda formar parte de la infraestructura de red. A diferencia de los elementos de una guía telefónica, los elementos almacenados en un *Directorio Activo* pueden ser diferentes unos de otros (usuarios, grupos, políticas de acceso, permisos, asignación de recursos, etc), por lo que la información concreta que se almacena variará según la naturaleza del objeto. Toda esta información se guarda en una base de datos jerárquica.

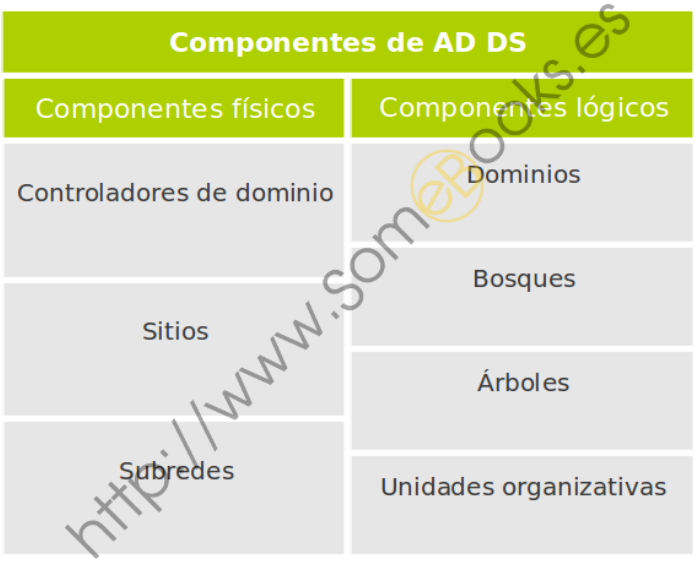
El motor de esta base de datos es el mismo que incorpora *Microsoft Exchange Server* y permite la replicación de controladores de dominio. Es decir, se puede enviar la información contenida en la base de datos a diferentes controladores de dominio a través de la red. De esta forma, un usuario creado en un determinado controlador de dominio, podría iniciar sesión en cualquier cliente unido a otro controlador de dominio diferente sin ninguna complicación.

Además de administrar políticas que serán válidas en toda la organización, *Active Directory*permite realizar operaciones como la instalación de programas, de forma simultánea y centralizada, en multitud de clientes o aplicar actualizaciones críticas en toda la organización.

Cuando utilizamos *Active Directory*, tenemos a nuestra disposición herramientas de administración para establecer *políticas de grupo*, para incluir unos grupos dentro de otros en diferentes niveles, un acceso sencillo al árbol de usuarios, ordenadores, impresoras y contactos, etc.

Obviamente, podemos utilizar *Windows Server* sin usar *Active Directory*, pero estaremos prescindiendo de un amplio conjunto de capacidades.

En cuanto a la estructura del servicio de directorio, lo primero que debemos saber es que existen dos tipos de componentes en *Active Directory*: los *componentes físicos* y los *componentes lógicos*. Veámoslos representados en la siguiente tabla:



Por otro lado, *Active Directory* resulta útil tanto en redes pequeñas como en instalaciones con millones de elementos relacionados.

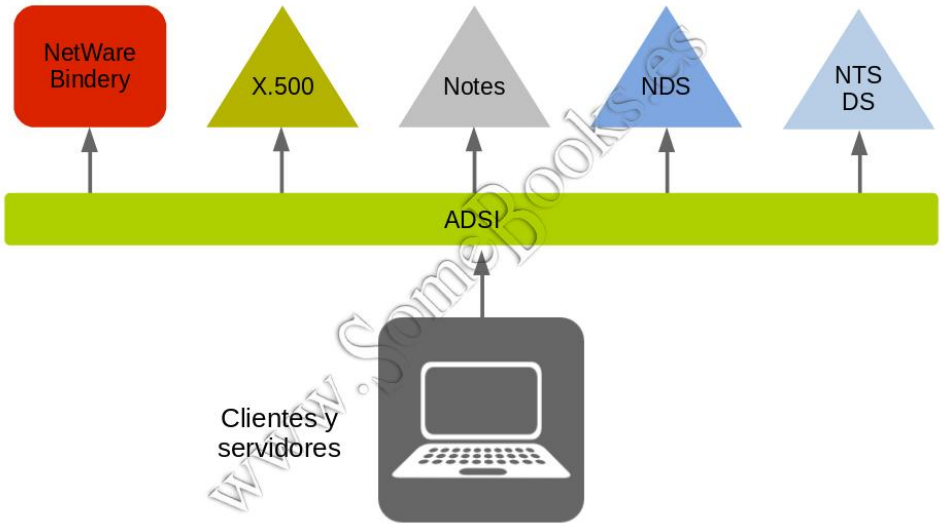
2. Conceptos básicos en una estructura de Directorio Activo

Una vez que disponemos de una idea global del concepto de directorio y de lo que son los dominios, es conveniente que hagamos un repaso de la terminología que vamos a emplear cuando hablemos de *Active Directory Domain Services*. Esto es lo que haremos a continuación:

Directorio

Como ya hemos mencionado antes, un *Directorio* es un repositorio único para la información relativa a los usuarios y recursos de una organización. *Active Directory* es un tipo de directorio y contiene información sobre las propiedades y la ubicación de los diferentes tipos de recursos dentro de la red. Usándolo, tanto los usuarios como los administradores pueden encontrarlos con facilidad.

Una de las ventajas que ofrece *Active Directory* es que puede utilizar *LDAP* (*Lightweight Directory Access Protocol*, en español, *Protocolo Ligero de Acceso a Directorios*), un protocolo de acceso estándar que permitirá la consulta de información contenida en el directorio. Sin embargo, también puede utilizar *ADSI* (*Active Directory Services Interface*, en español, *Interfaces de Servicio de Active Directory*), un conjunto de herramientas ofrecidas por *Microsoft*, que tienen una interfaz orientada a objetos y que permiten el acceso a características de *Active Directory Domain Services* que no están soportadas por *LDAP*.



Dominio

Un *Dominio* es una colección de objetos dentro del directorio que forman un subconjunto administrativo. Pueden existir diferentes dominios dentro de un bosque, cada uno de ellos con su propia colección de objetos y *unidades organizativas*.

Para poner nombre a los dominios se utiliza el protocolo *DNS*. Por este motivo, *Active Directory*necesita al menos un *servidor DNS* instalado en la red. Más adelante, en este mismo apartado, definiremos los conceptos de *bosque* y *unidad organizativa*.

Objeto

La palabra *Objeto* se utiliza como nombre genérico para referirnos a cualquiera de los componentes que forman parte del directorio, como una impresora o una carpeta compartida, pero también un usuario, un grupo, etc. Incluso podemos utilizar la palabra *objeto* para referirnos a una *unidad organizativa*.

Cada objeto dispondrá de una serie de características específicas (según la clase a la que pertenezca) y un nombre que permitirá identificarlo de forma precisa.

Como veremos más adelante, las características específicas de cada tipo de objeto quedarán definidas en el *Esquema* de la base de datos.

En general, los objetos se organizan en tres categorías:

- Definición de *usuario*:

  Desde un punto de vista informático, un usuario es un conjunto de *permisos* y de *privilegios* sobre determinados recursos.

  En este sentido, un usuario no tiene que ser, necesariamente, una persona.

  Usuarios: identificados a través de un nombre (y, casi siempre, una contraseña), que pueden organizarse en grupos, para simplificar la administración.

- *Recursos*: que son los diferentes elementos a los que pueden acceder, o no, los usuarios según sus *privilegios*. Por ejemplo, carpetas compartidas, impresoras, etc.
- *Servicios*: que son las diferentes *funciones* a las que los usuarios pueden tener acceso. Por ejemplo, el correo electrónico.

Cuando instalamos *Active Directory* en un ordenador con *Windows Server*, convertimos a ese ordenador en un *Controlador de dominio*.

Existen objetos que pueden contener a su vez otros objetos, como es el caso de los *grupos de usuarios* y de las *unidades organizativas*.

Controlador de dominio

Un *Controlador de dominio* (*domain controller*) contiene la base de datos de objetos del directorio para un determinado dominio, incluida la información relativa a la seguridad. Además, será responsable de la autenticación de objetos dentro de su ámbito de control (facilitarán la apertura y el cierre de sesión, las búsquedas en el directorio, etc.).

En un dominio dado, puede haber varios controladores de dominio asociados, de modo que cada uno de ellos represente un rol diferente dentro del directorio. Sin embargo, a todos los efectos, todos los controladores de dominio, dentro del mismo dominio, tendrán la misma importancia.

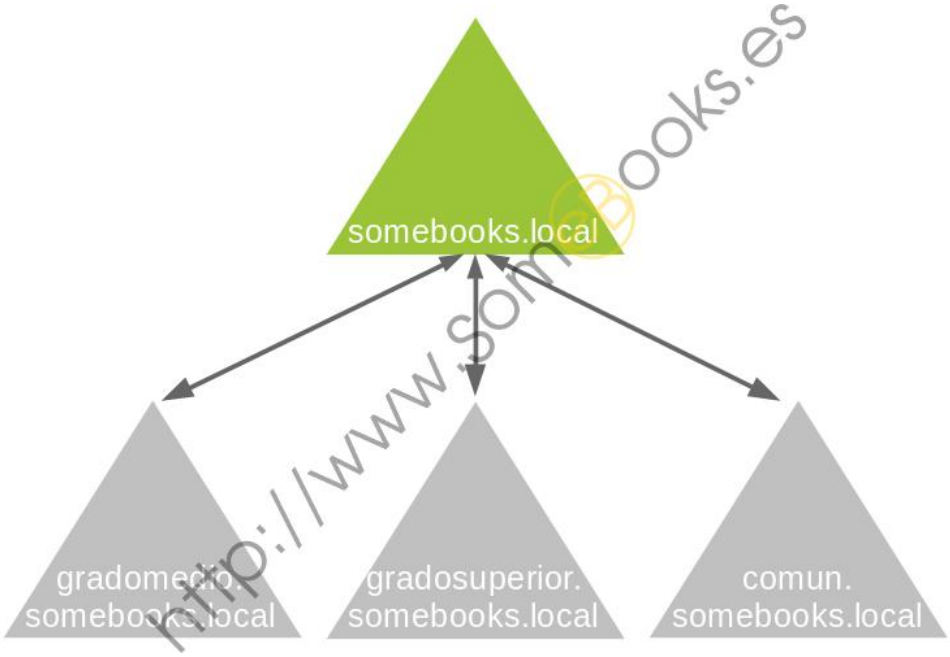
Árboles

Un *Árbol* es simplemente una colección de dominios que dependen de una raíz común y se encuentran organizados como una determinada jerarquía. Dicha jerarquía también quedará representada por un *espacio de nombres DNS* común.

De esta forma, sabremos que los dominios **somebooks.es** e **informatica.somebooks.es** forman parte del mismo árbol, mientras que **sliceoflinux.com** y **somebooks.es** no.

El objetivo de crear este tipo de estructura es fragmentar los datos del *Directorio Activo*, replicando sólo las partes necesarias y ahorrando ancho de banda en la red.

Si un determinado usuario es creado dentro de un dominio, éste será reconocido automáticamente en todos los dominios que dependan jerárquicamente del dominio al que pertenece.



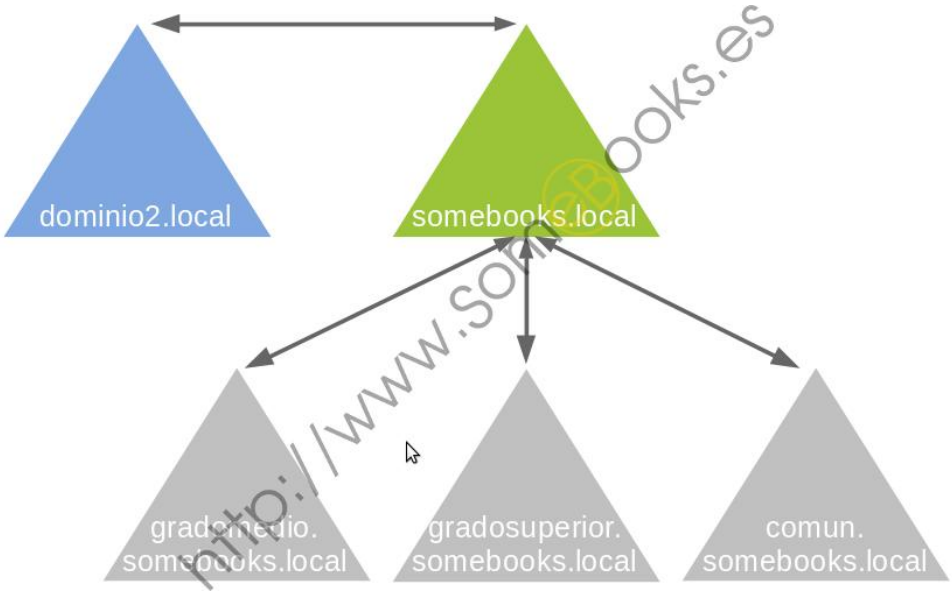
Bosque

El *Bosque* es el mayor contenedor lógico dentro de *Active Directory*, abarcando a todos los dominios dentro de su ámbito. Los dominios están interconectados por *Relaciones de confianza* transitivas que se construyen automáticamente (consultar más adelante el concepto de *Relación de confianza*). De esta forma, todos los dominios de un bosque confían automáticamente unos en otros y los diferentes árboles podrán compartir sus recursos.

Como ya hemos dicho, los dominios pueden estar organizados jerárquicamente en un árbol que comparte un *espacio de nombres DNS* común. A su vez, diferentes árboles pueden estar integrados en un bosque. Al tratarse de árboles diferentes, no compartirán el mismo espacio de nombres.

De forma predeterminada, un bosque contiene al menos un dominio, que será el *dominio raíz del bosque*. En otras palabras: cuando instalamos el primer dominio en un ordenador de nuestra red que previamente dispone de *Windows Server*, además del propio dominio, estamos creando la raíz de un nuevo árbol y también la raíz de un nuevo bosque.

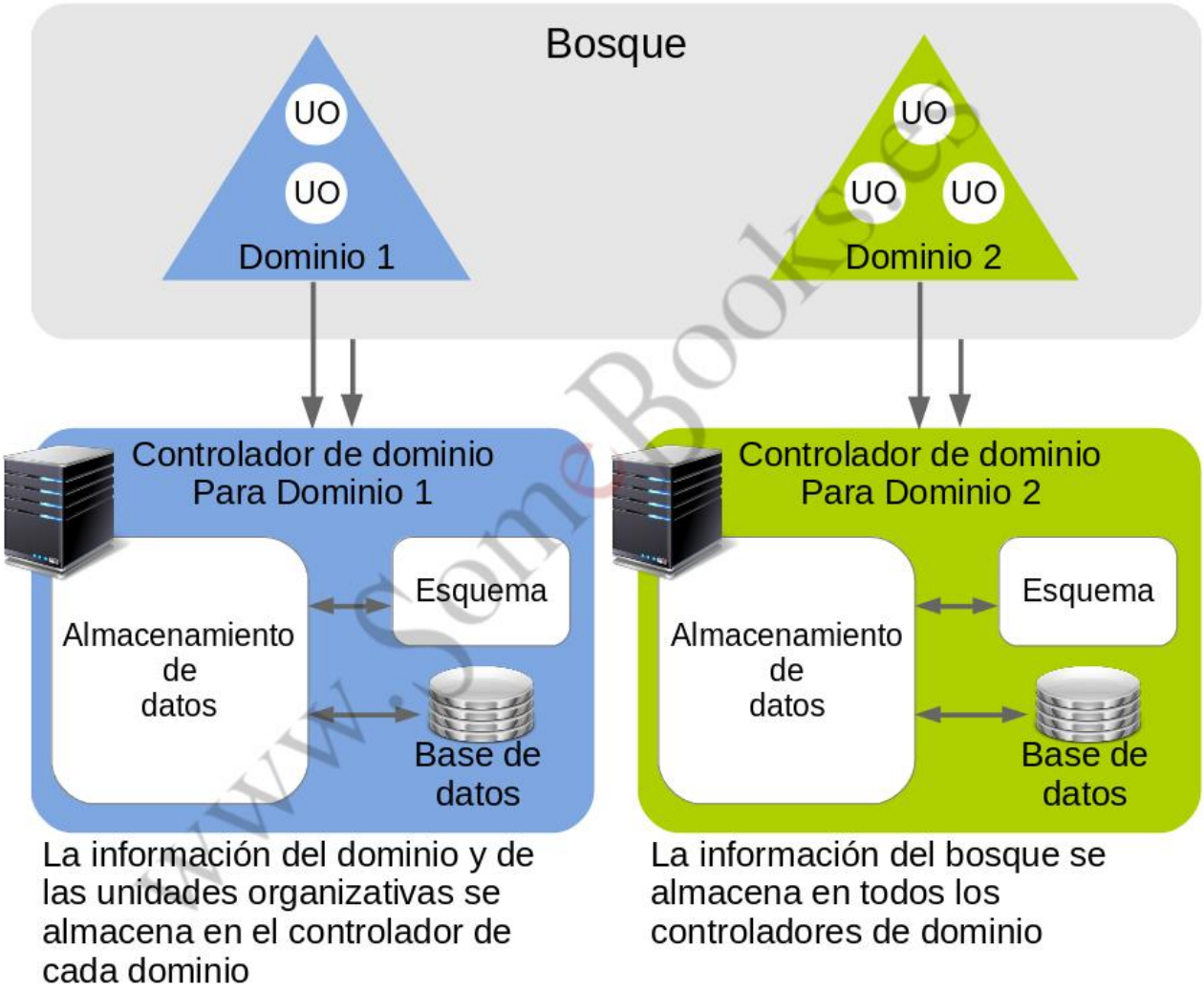
El *dominio raíz del bosque* contiene el *Esquema* del bosque, que se compartirá con el resto de dominios que formen parte de dicho bosque (consultar el concepto de *Esquema* más adelante).



Unidad Organizativa

Una *Unidad Organizativa* es un contenedor de objetos que permite organizarlos en subconjuntos, dentro del dominio, siguiendo una jerarquía. De este modo, podremos establecer una estructura lógica que represente de forma adecuada nuestra organización y simplifique la administración.

Otra gran ventaja de las unidades organizativas es que simplifican la delegación de autoridad (completa o parcial) sobre los objetos que contienen, a otros usuarios o grupos. Esta es otra forma de facilitar la administración en redes de grandes dimensiones.



Esquema

En *Active Directory Domain Services* se utiliza la palabra *Esquema* para referirse a la estructura de la base de datos. En este sentido, utilizaremos la palabra atributo para referirnos a cada uno de los tipos de información almacenada.

También suele emplearse una terminología *orientada a objetos*, donde la palabra *Clase* se referirá a un determinado tipo de objetos (con unas propiedades determinadas), mientras que un objeto determinado recibe el nombre de *instancia*. Por ejemplo, podríamos pensar que la clase usuario es una plantilla que definirá a cada uno de los usuarios (que serán instancias de la clase usuario).

Sitio

Un *Sitio* es un grupo de ordenadores que se encuentran relacionados, de una forma lógica, con una localización geográfica particular.

En realidad, pueden encontrarse físicamente en ese lugar o, como mínimo, estar conectados, mediante un enlace permanente, con el ancho de banda adecuado.

En otras palabras, un controlador de dominio puede estar en la misma zona geográfica de los clientes a los que ofrece sus servicios o puede encontrarse en el otro extremo del planeta (siempre que estén unidos por una conexión adecuada). Pero en cualquier caso, todos juntos formarán el mismo *sitio*.

Relaciones de confianza

En el contexto de *Active Directory*, las *Relaciones de confianza* son un método de comunicación seguro entre dominios, árboles y bosques. Las relaciones de confianza permiten a los usuarios de un dominio del *Directorio Activo* autenticarse en otro dominio del directorio.

Existen dos tipos de relaciones de confianza: *unidireccionales* y *bidireccionales*. Además, las relaciones de confianza pueden ser *transitivas* (A confía en B y B confía en C, luego A confía en C).

Maestro de Operaciones

Cada cuenta creada en el dominio recibe un *SID* (*Security ID*) único que no se reutiliza. El *SID* está formado por tres partes:

- Un identificador asignado por *ISO* para dominios *Microsoft*
- Un identificador del dominio (compartido por todas las cuentas del dominio)
- Un número asignado de forma secuencial, a partir de 1000, llamado *RID* (*Relative Identifier*)

Como hemos dicho al principio de este capítulo, cuando disponemos de varios *controladores de dominio* en un mismo dominio, se puede replicar la información contenida en la base de datos a los diferentes *controladores* a través de la red con el objetivo de descentralizar diferentes operaciones (por ejemplo, la autenticación de usuarios) y agilizar su funcionamiento.

Sin embargo, existe un conjunto especializado de tareas que deben estar centralizadas en un *controlador de dominio* específico para evitar inconsistencias. Este *controlador de dominio*"*especial*" recibe el nombre de *Maestro de Operaciones* o *FSMO* (de *Flexible Single Master Operations*).

Para entender la situación, vamos a poner un ejemplo: Supongamos que el *administrador* de un *controlador de dominio* realiza una modificación en el esquema del dominio al mismo tiempo que, un segundo administrador, desde un controlador distinto, realiza una modificación que resulta incompatible con la primera. Como podrás imaginar, cuando se produzca la replicación de la base de datos, estaremos en un aprieto.

Pues bien, para evitar este tipo de situaciones, sólo uno de los controladores del dominio podrá realizar este tipo de cambios.

Las acciones (también llamadas roles) que sólo pueden realizarse desde el Maestro de operaciones son sólo cinco y se incluyen en la siguiente tabla:

Roles FSMO		
Rol FSMO	Ubicación	Acciones
Maestro de esquema (Schema Master)	Único en el bosque	Administra los cambios en el esquema del directorio.
Maestro de nomenclatura de dominios (Domain Naming Master)	Único en el bosque	• Inscribe a los dominios en el bosque. • Administra la nomenclatura del dominio.
Maestro RID (RID Master)	Único en el dominio	Distribuye rangos de RID a los controladores de dominio para crear los SID
Maestro de infraestructura (Infrastructure Master)	Único en el dominio	Administra los movimientos de objetos de un dominio a otro.
Maestro Controlador Principal de Dominio (PDC Emulator)	Único en el dominio	• Permite la compatibilidad con versiones anteriores (principalmente Windows NT). • Actúa como servidor de horario (Time Server) del Dominio. • Actúa como referente en los bloqueos de cuentas y cambios de contraseña.