ACTIVE DIRECTORY. GESTIÓN DE DOMINIOS.

CASO PRÁCTICO

CARMINFO S.L. está progresando. Como Fernando terminó su fase de prácticas y ha decidido seguir estudiando, Carmen ha notado que necesitaba a alguien más para abarcar todo el trabajo y ha contratado a Laura. En la oficina en la que CARMINFO S.L. tiene su sede, hay cinco equipos conectados en red:

a) Un servidor con Ubuntu Server
b) Un servidor con Windows Server 2008 R2
c) El equipo de Carmen, con Windows 7
d) El equipo de Laura, también con Windows 7
e) Un equipo adicional con Windows 7, al que está conectada una impresora.

LAURA: Carmen, empezamos a tener un número significativo de equipos, ¿verdad?

CARMEN: Sí, es cierto. Pero me preocupa que este sistema empiece a convertirse en un caos. Por ejemplo, ¿no te parece que sería bueno poder utilizar tu nombre de usuario y tu contraseña independientemente del equipo en el que inicies sesión?

LAURA: Sí. Y también estaría bien no tener que usar el disco USB cada vez que nos tenemos que pasar un documento. Por no hablar del rollo de la impresora. A ver si la ponemos compartida en red o algo.

CARMEN: Sí. Y hay que sacar más partido a los servidores, que nos han salido caros. Por todo eso, estoy pensando en organizar nuestros equipos en un dominio. ¿Qué opinas?

LAURA: Cuéntame más...

1. Qué es Active Directory.

Active Directory significa "directorio activo" (a partir de ahora, podemos referirnos a este concepto con sus siglas en inglés, AD). Es el término que usa Microsoft para referirse a su implementación de servicio de directorio en una red de ordenadores. Ésa es la definición, pero, ¿qué es un servicio de directorio? Pues bien, un **servicio de directorio** es una aplicación o un conjunto de aplicaciones que entre otras cosas :

- ✓ Almacena y organiza la información sobre los usuarios y usuarias de una red de ordenadores.
- ✓ Organiza los recursos de red.
- ✓ Permite a los administradores y administradoras gestionar el acceso de usuarios a los recursos sobre dicha red.

Analiza la frase anterior: ya sabes lo que es una aplicación. Ahora bien, ¿a qué se refiere con "usuarios y usuarias de una red de ordenadores"? Los usuarios y usuarias de una red de ordenadores son, sencillamente, las personas que utilizan dicha red. En CARMINFO S.L. se trata de Carmen y de Laura. Pero para que las personas puedan usar la red, hay que crear cuentas de usuario.

También tienes que tener claro qué son los **recursos** de red. Los recursos que maneja un servicio de directorio son, principalmente:

- ➔ Impresoras.
- ➔ Carpetas
- ➔ Archivos compartidos en red.
- ➔ Equipos.

¿Y quiénes son los administradores y administradoras de la red? Los administradores son usuarios que tienen más poder para gestionar los recursos que el resto de los usuarios.

Resumiendo, puedes concluir que AD es un conjunto de aplicaciones, creado por Microsoft, que sirve para que las personas que utilizan una red puedan acceder a los equipos, carpetas compartidas e impresoras de la misma, de la forma en que los administradores de la red lo hayan dispuesto.

A.D. es un servicio de directorio extensible y escalable que permite administrar eficientemente los recursos de red y ayuda a monitorizar y localizar estos servicios.

- Un servicio de directorio es un lugar donde se centraliza información sobre los recursos de una organización.
- Un directorio es una base de datos optimizada para lectura, navegación y búsqueda.
- Los servicios de directorio son almacenes de información acerca de entidades de red (aplicaciones, usuarios, archivos, impresoras.) proporcionan una manera consistente de nombrar, describir, localizar, acceder, administrar y asegurar la información acerca de los recursos almacenados.

¿Cómo hace esto AD? AD maneja una base de datos que contiene información sobre todos estos elementos que hemos ido nombrando y que forman parte de la red. Estos elementos son los **objetos de AD** y algunos de ellos son los usuarios, los equipos y las impresoras. Hay otros tipos de objetos, de los que hablaremos en su momento.
A.D. permite un único punto de administración para todos los recursos públicos (ficheros, dispositivos, periféricos, bases de datos, usuarios, etc.) El administrador da acceso a los recursos definidos.

El aspecto que más llama la atención cuando se accede por primera vez a una red con AD es que se puede acceder a varios equipos *utilizando la misma cuenta de usuario*. El motivo es que, en AD, los usuarios ya no son propios de cada equipo (locales) sino que residen en la base de datos. Cuando un usuario quiere iniciar sesión en un equipo, AD consulta su base de datos para saber si ese usuario puede iniciar sesión en ese equipo. De esta forma, manejando la información de su base de datos, AD permite que el acceso a los recursos sea el que los administradores y administradoras han configurado.

PARA SABER MÁS:
Si te interesa profundizar en el conocimiento de lo que es un servicio de directorio y también en conocer otros servicios de directorio que no sean Active Directory, consulta el siguiente enlace.

Texto enlace: Servicio de directorio en Wikipedia.
URL: http://es.wikipedia.org/wiki/Servicio_de_directorio
Título: Más información sobre lo que es un servicio de directorio.

2. Qué es un dominio.

CASO PRÁCTICO
Carmen ha decidido instalar un servicio de directorio en su organización.

Podría utilizar como servicio de directorio la tecnología de Novell Netware, o bien LDAP (*Lightweight Directory Access Protocol* - en español Protocolo Ligero de Acceso a Directorios) sobre Linux, o también Active Directory de Microsoft. Como ya ha adquirido una licencia de Windows Server 2008 R2, va a utilizar Active Directory. Así podrá amortizar su inversión. Por otro lado, tiene varios conocidos que trabajan con ello, a los que podría recurrir en caso de surgirle dudas.

Le ha pedido a Laura que ponga en marcha el servicio de directorio. La pobre Laura está un poco asustada, porque sólo ha realizado estas tareas haciendo prácticas en el instituto en el que estudiaba. Teme haber olvidado muchas cosas.

Por eso, antes de empezar, decide repasar conceptos. Mientras se documentaba, se ha encontrado con el concepto de "dominio". Así que decide que antes de seguir adelante, debe comprender bien en qué consiste un dominio.

DESTACADO
Un **dominio** es una agrupación lógica de objetos de Active Directory que permite la administración centralizada de dichos objetos.

En la base de datos de AD el dominio en sí también es un objeto, que estará relacionado jerárquicamente con los objetos del dominio en una relación padre-hijos. El dominio será el objeto padre de todos los objetos que contiene.

1.1.- Nombrar al dominio.

Supongamos un caso como el de CARMINFO S. L. Los objetos de AD serán los cuatro equipos, la impresora y los objetos, grupos, etc. que Carmen y Laura decidan crear. En la siguiente imagen puedes ver algunos objetos agrupados dentro de una pirámide. Esta pirámide representa el **dominio** en el que estarán agrupados estos objetos.

Es importante que conozcas la forma de nombrar los objetos en un dominio de Active Directory.

¿Cómo se nombran los dominios?
Cada dominio lleva asociado un nombre que lo identifica y que se escribe siguiendo las convenciones de los nombres DNS (Domain Name System, Sistema de Nombres de Dominio). Los nombres que utilizas cuando navegas por Internet para referirte a los sitios Web, son nombres DNS. Así no te será complicado entender los nombres de dominio. Un nombre DNS consiste en **dos o más partes**, llamadas etiquetas, separadas por puntos. Por ejemplo, *norte.carminfosl.com*.

- A la etiqueta ubicada más a la derecha se le llama dominio de nivel superior. En el ejemplo *carminfosl**.com*** sería la etiqueta **".com".**

- Cada etiqueta a la izquierda especifica una subdivisión. En este caso, la etiqueta "carminfosl" es una subdivisión de ".com", y "norte" es una subdivisión de "**carminfo**".

Además del nombre en formato DNS, los dominios tienen un nombre corto, llamado nombre NetBIOS (NetBIOS es un protocolo de red utilizado por Microsoft para redes locales). Es necesario que tengan este nombre para ser compatibles con sistemas anteriores a Windows Server 2000.

- ➔ Un ejemplo de nombre DNS completo sería ***carminfosl.com***
- ➔ **U**n ejemplo de nombre NetBIOS sería *CARMINFOSL*.

DESTACADO
Muchas veces crearás dominios para uso interno. En ese caso, no es necesario que el nombre que les pongas al dominio sea visible en Internet. Es decir, no hace falta que sea un nombre de verdad. Cuando practiques creando dominios, estarás en esa situación. En ese caso, utiliza un sufijo que no se utilice en Internet, por ejemplo, ".mio". Muchas veces se utiliza ".local", pero este sufijo puede darte problemas con máquinas Linux.

Tipo de nombre	Descripción	Ejemplo
El dominio raíz	Es la parte superior del árbol, que representa un nivel sin nombre; a veces, se muestra como dos comillas vacías (""), que indican un valor nulo. Cuando se utiliza en un nombre de dominio DNS, empieza con un punto (.) para designar que el nombre se encuentra en la raíz o en el nivel más alto de la jerarquía del dominio. En este caso, el nombre de dominio DNS se considera completo e indica una ubicación exacta en el árbol de nombres. Los nombres indicados de esta forma se llaman nombres de dominio completos (FQDN, *Fully Qualified Domain Names*)	**Un sólo punto (.) o un punto usado al final del nombre, como "ejemplo.microsoft.com.".**
Dominio de nivel superior	Un nombre de dos o tres letras que se utilizan para indicar un país o región, o el tipo de organización que usa un nombre.	".com", que indica un nombre registrado para usos comerciales o empresariales en Internet.
Dominio de segundo nivel 	Nombres de longitud variable registrados que un individuo u organización utiliza en Internet. Estos nombres siempre se basan en un dominio de nivel superior apropiado, según el tipo de organización o ubicación geográfica donde se utiliza el nombre.	"microsoft.com.", que es el nombre de dominio de segundo nivel registrado para Microsoft por el registrador de nombres de dominio DNS de Internet.

Subdominio	Nombres adicionales que puede crear una organización y se derivan del nombre de dominio registrado de segundo nivel. Incluyen los nombres agregados para desarrollar el árbol de nombres de DNS en una organización y que la dividen en departamentos o ubicaciones geográficas.	"ejemplo.microsoft.com.", que es un subdominio ficticio asignado por Microsoft para utilizarlo en nombres de ejemplo de documentación.
Nombre de recurso o de host	Nombres que representan una hoja en el árbol DNS de nombres e identifican un recurso específico. Normalmente, la etiqueta de la izquierda de un nombre de dominio DNS identifica un equipo específico en la red.	"host-a.ejemplo.microsoft.com.", donde la primera etiqueta ("host-a") es el nombre de host DNS de un equipo específico en la red. 

Un dominio es simplemente un subárbol del espacio de nombres. El nombre de un dominio es el nombre del nodo raíz correspondiente. Un dominio agrupa un conjunto de hosts y/o subdominios que se relacionan de acuerdo a cierto criterio, ya sea geográfico u organizacional. En el DNS cada dominio es administrado por una organización o empresa determinada. Ésta puede decidir dividir el o los dominios que administra en subdominios, así como asignar la administración de éstos a otras entidades. Cada dominio puede contener tanto subdominios como hosts independientes, al igual que un directorio posee subdirectorios y ficheros a la vez. El DNS en la actualidad sigue ciertos patrones en cuanto a su organización. Ésta se basa en niveles de acuerdo a la posición del dominio. El nivel superior o primer nivel lo forman aquellos dominios descendientes del dominio raíz. Los fundamentales se listan a continuación:

?? ***Com***: Agrupa a organizaciones comerciales. Ejemplos: *ibm.com*, *yahoo.com*, *redhat.com*, etc.
?? ***Edu***: Reune a organizaciones de propósitos educacionales. Ejemplos: *berkeley.edu*, *cornell.edu*, etc.
?? ***Net***: Agrupa a organizaciones dedicadas al desarrollo de las redes. Ejemplos *rpmfind.net*, *nic.net*, *computing.net*, etc.
?? ***Org***: Reune a organizaciones no comerciales. Ejemplos: *linuxdoc.org*, *ibiblio.org*, *linux.org*, *insflug.org*, etc.
?? ***Gov***: Agrupa a organizaciones gubernamentales. Ejemplo: *nasa.gov*, *nsf.gov*, etc.
Como parte del espacio de nombres de dominio también existen dominios de primer nivel que designan zonas geográficas. Sus nombres representan a todos los países a través de dos letras. Ejemplos: *es* para España, *au* para Australia, *de* para Alemania, etc. Para ver a todos los dominios geográficos de primer nivel puede consultarse *http://www.iana.org/cctld/cctld-whois.htm*. Puede ocurrir que los dominios geográficos de primer nivel contengan a su vez algunos de los dominios organizativos de primer nivel. Ejemplos: *edu.au*, *org.uk*, etc.

1.2.- Nombrar usuarios y equipos.

¿Cómo se nombran las cuentas de usuario?
Cuando el administrador o administradora del dominio crea un usuario, tiene que ponerle un "nombre de inicio de sesión" al usuario. Por ejemplo, se puede crear el usuario *carmen* en el dominio *carminfosl.com*.

Para nombrar a esa cuenta de usuario, Active Directory utiliza el **UPN** (User Primary Name – Nombre principal de usuario) que consiste en el nombre de inicio de sesión, seguido del signo '@' y del nombre del dominio en el que se ha creado la cuenta de usuario. En el ejemplo, el UPN del usuario *carmen* del dominio *carminfosl.com* sería carmen@carminfosl.com. Como puedes ver, es muy similar a una cuenta de correo electrónico. A continuación tienes la oportunidad de verlo de cerca.

Texto enlace: Nombres de objetos de Active Directory.
URL: SOR02_CONT_R05_NombresAD.swf

¿Cómo se nombran los equipos?
Es sorprendente ver cómo muy pocas organizaciones se toman su tiempo a la hora de poner nombres a sus equipos en función de su tarea a realizar. Si se ponen nombres de personas, en vez de la función que va atener el equipo puede hacer complicado a los usuarios e incluso para el resto de administradores encontrar los recursos que necesiten. Te has de decidir por un esquema de nomenclatura que sea significativo tanto para los administradores como para los usuarios. Para ayudar a los usuarios debes decidir un esquema de nombres que ayude a identificar lo que hace cada equipo y su ubicación. Por ejemplo, puedes utilizar como nombre del primer servidor del departamento de ingeniería IngServer01. Los nombres identifican tanto a equipos como a servidores y especifican los departamentos donde se encuentran. Los nombres de los equipos deben ser sencillos de recordar y fáciles de trabajar con ellos.
Los nombres de los equipos tienen que ser únicos en el dominio.
Todos los equipos, pertenezcan o no a un dominio, tienen un nombre. Este nombre lo puedes conocer entrando en la configuración avanzada del sistema (si estás en Windows 7, Windows Server) o en las propiedades de **Mi PC** (si estás en Windows XP). También puedes ejecutar el comando **hostname** (que significa "nombre de equipo") en el símbolo del sistema.

Además, si el equipo forma parte de un dominio de Active Directory, tiene un nombre DNS completo. A este nombre DNS completo de un equipo se le llama **FQDN** (Fully Qualifyed Domain Name – Nombre de Dominio Completamente Cualificado). Este nombre no es más que una unión entre el nombre de equipo (el que obtienes con **hostname**, o mirando en la configuración del sistema) y el nombre del dominio al que está unido el equipo, separadas ambas partes por un punto (.).

Por ejemplo, un equipo que pertenezca al dominio *carminfosl.com* y cuyo nombre de equipo es PC-Carmen, tendrá por nombre *PC-Carmen.carminfosl.com.* Si en CARMINFO S.L. tienen un servidor de páginas web, pueden ponerle de nombre ***www*** y así su nombre FQDN sería www.carminfosl.com.

Nombre de un equipo perteneciente a un dominio su Nombre de Dominio Completamente Cualificado es:
nombre_de_**equipo.**nombre_del_**dominio**

Si la red de nuestra organización debe conectarse a Internet, tendrás que obtener un nombre de dominio público que nos proporcione un organismo de registro o utilizar un servicio similar al que proporciona tu proveedor de servicios de Internet. Debido a que muchos nombres de dominio ya se han registrado, deberas contar con un grupo bastante amplio de alternativas a la hora de registrar tu organización. Después de obtener el nombre de dominio, se ha de configurar el albergue DNS del dominio. Esto se hace indicando las direcciones de dos o más servidores DNS que gestionarán los servicios DNS del dominio. Normalmente, estos servidores DNS pertencen a nuestro proveedor de servicios de Internet.

PARA SABER MÁS

Tienes toda la información sobre nomenclatura de objetos en Active Directory en esta dirección de la biblioteca TechNet de Microsoft.

Texto enlace: Nomenclatura de objetos en Active Directory en Microsoft TechNet.
URL: http://technet.microsoft.com/es-es/library/cc739093(WS.10).aspx
Título: Información de Microsoft TechNet sobre la nomenclatura en Active Directory.

Y en la siguiente presentación, puedes encontrar un resumen de las características más importantes de Active Directory:

Texto enlace: Introducción al servicio de directorio de Microsoft Active Directory.
URL: http://www.redeschile.net/files/microsoft/8.-%20Introduccion%20a%20las%20infraestructuras%20de%20Active%20Directory.ppt
Título: Introducción al servicio de directorio de Microsoft Active Directory.

2.- Instalar Active Directory y crear un dominio nuevo.

CASO PRÁCTICO
Laura se dispone a instalar Active Directory y crear el dominio que le ha encargado Carmen.

En primer lugar, tiene que pensar un nombre para el dominio. Carmen le cuenta que ha comprado el nombre de dominio en Internet *carminfosl.com*, por lo que Laura ya no tiene dudas: ése será el nombre del dominio de Active Directory.

Laura sabe que si se equivoca en algún paso tendrá que deshacer el dominio y volverlo a crear. Para evitar realizar intentos fallidos en el servidor, ha pensado que lo mejor será probar primero en una máquina virtual. Así, si se equivoca, no dejará ningún rastro en el servidor definitivo.

Como no es un proceso que lleve más de media hora, decide realizar el ensayo en la máquina virtual y, si le da tiempo, dejarlo instalado en el servidor real antes de marcharse a casa.

Siguiendo los pasos de un manual, tiene claro que va a ejecutar el comando ***dcpromo*** y completar una serie de pasos, tras los cuales el equipo se convertirá en un **controlador de dominio**.

Para crear un dominio, tienes que instalar Active Directory en un equipo. Al realizar esta acción convertirás dicho equipo en un **controlador de dominio**. Para que exista un dominio tiene que existir, al menos, un controlador de dominio que lo sustente.

Controlador de dominio: Equipo con Windows Server 2008 que mantiene la base de datos de A.D.
Servidor miembro: equipo que forma parte del dominio haciendo uso de los servidores del mismo. Necesita autentificarse en el dominio (mediante un controlador de dominio) para poder usar los recursos.

2.1 Instalación de los servicios de dominio de AD.

A la vista de la historia de Laura y del título de este apartado, puedes intuir que para configurar Active Directory necesitas instalar los "servicios de dominio de Active Directory". El equipo en el que realices esta instalación se convertirá en un equipo especial para la red: un **controlador de dominio**.

En realidad, no se trata de una instalación sin más. Para que puedas instalar AD y crear un dominio, el equipo que va a ser el controlador de dominio tiene que cumplir ciertos requisitos, siendo los más importantes los siguientes:

- Debe tener como sistema operativo Windows Server: Windows 2000 Server, Windows Server 2003, Windows Server 2008 o Windows Server 2008 R2.
- Debe contar con al menos un volumen de almacenamiento formateado con NTFS (NT File System, Sistema de Ficheros NT).
- Hay que acceder al equipo con una cuenta de usuario con credenciales administrativas: la propia cuenta Administrador o una cuenta cualquiera que pertenezca al grupo Administradores.
- Aunque en Server 2008 R2 no es imprescindible, es muy recomendable que el equipo tenga una dirección IP estática.

A continuación puedes ver un vídeo en el que se completa el proceso de instalación de AD y se crea un dominio.

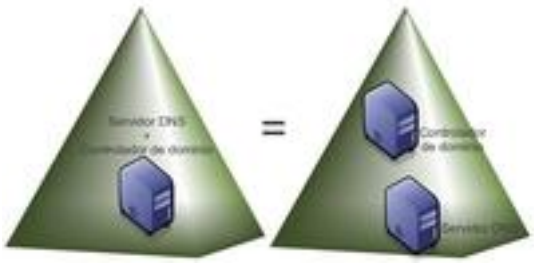
Texto enlace: Proceso de instalación de AD.
URL: SOR02_CONT_R07_InstalacionActiveDirectory.avi
Título: Instalación de AD y configuración del primer dominio.

Como puedes observar, para iniciar el asistente de instalación de los servicios de dominio de AD, ejecutamos el comando **dcpromo**. El asistente realiza varias preguntas importantes. En un ejemplo como el de Laura en el caso práctico, en el apartado "elegir una configuración de implementación", debes optar por la opción "**crear un dominio nuevo en un bosque nuevo".** Puesto que el dominio que se está creando no depende de ningún otro dominio que ya exista. Un poco más adelante conocerás el significado de las otras opciones que aparecen en esta pantalla. Otra pregunta que el asistente plantea es el **nivel funcional**. En el apartado 6 aprenderás en qué consiste esta característica.

Un dato imprescindible es el **nombre del dominio.** El nombre del dominio creado por Laura en el caso práctico es *carminfosl.com*. En el apartado anterior aprendiste que los dominios utilizan el sistema de nombres DNS. Esto tiene la siguiente consecuencia: para que un dominio funcione, los ordenadores que pertenecen a él deben ser capaces de traducir los nombres DNS del dominio a las direcciones IP correspondientes asociadas a dichos nombres. Por ejemplo, *PC-Carmen.carminfosl.com* o www.carminfosl.com Este proceso de traducción se llama **"resolver un nombre"**.

Esta función la realiza un **servidor DNS**, que es un equipo que almacena tablas para hacer corresponder nombres DNS con direcciones IP.

Por lo tanto, para que un dominio funcione, tiene que haber un servidor DNS que resuelva sus nombres. Cuando estamos creando el dominio desde cero, tal como hemos visto en el vídeo o como hizo Laura en el caso práctico, aún no existe ningún servidor DNS que conozca el nombre del dominio. Por eso, el asistente de instalación de los servicios de dominio de AD nos da la opción de instalar también un servidor DNS.



Simplemente aceptamos esa sugerencia y el propio asistente hará todo el trabajo de configuración. Eso significa que el equipo se convierte no sólo en controlador de dominio, sino también en servidor DNS.

2.2 Cómo incorporar un equipo al dominio.

CASO PRÁCTICO

En CARMINFO S.L. Existen tres ordenadores, aparte de los dos servidores. Estos tres equipos ejecutan Windows 7. En uno de ellos suele trabajar Carmen y en otro Laura, aunque a veces necesitan iniciar sesión en el ordenador de la otra, para acceder a algún archivo. El tercer equipo se adquirió con vistas a servir de equipo de respaldo, por si alguno de los otros dos se estropea.

La idea de Carmen es poder acceder a recursos que se encuentren centralizados en el servidor de Windows Server 2008 R2, como será la impresora, carpetas compartidas, etc. Y sobre todo, quiere que se pueda acceder siempre con la misma cuenta de usuario, independientemente de en qué equipo se siente cada una.

Para que todo esto sea posible, tienen que unir los tres equipos con Windows 7 al dominio. Cuando hagan ésto, podrán definir usuarios en Active Directory y utilizarlos. En concreto, Carmen utilizará el usuario *cmartinez* (por Carmen Martínez) y Laura utilizará el usuario *lgarcia* (por Laura García).

Cuando unimos un equipo al dominio, el objetivo que perseguimos es poder iniciar sesión en dicho equipo utilizando los usuarios que se han definido en Active Directory. En lugar de utilizar los usuarios locales que se definieron previamente en el equipo. En el caso práctico, Carmen y Laura aún no han creado usuarios en AD, pero ya existe uno que se crea por defecto: **el usuario Administrador.**

En el siguiente vídeo puedes ver el proceso que hay que seguir para unir un equipo con con S.O Windows 7 a un dominio. Además, verás cómo el usuario Administrador del dominio inicia sesión en el equipo recién incorporado.

Como puedes observar, el proceso es similar al de cambiar el nombre del equipo, pero marcando "miembro de dominio", y escribiendo el nombre del mismo.

Texto enlace: Proceso de incorporación de un equipo a un dominio.
URL: SOR02_CONT_R11_IncorporacionADominio.avi
Título: Presentación que ilustra el proceso de incorporación de un equipo con Windows 7 a un dominio.

Para que la operación tenga éxito, es muy importante:

1. En la configuración TCP/IP del equipo que vamos a unir al dominio, hemos de establecer como servidor DNS preferido, la dirección IP del equipo que funciona como servidor DNS en el dominio. Como viste en el apartado anterior, el servidor DNS puede ser el propio controlador de dominio.
2. Hay que utilizar una cuenta perteneciente al grupo **Administradores del dominio,** no basta con ser Administrador del equipo local.

2.3 Configurar un controlador de dominio de respaldo.

CASO PRÁCTICO

Carlos, que también es informático, le cuenta a su amiga Carmen que en su trabajo han tenido un problema importante: se produjo una subida de tensión y quedó dañado el controlador de dominio de la organización.

La base de datos de Active Directory se perdió y ahora no pueden iniciar sesión en los ordenadores con los usuarios y contraseñas que usaban siempre.
Tampoco tienen acceso a las impresoras ni a los archivos compartidos en red. Como no tenían copia de seguridad y el disco duro quedó físicamente dañado, tienen que volver a definir todos los usuarios, permisos, recursos, etc. del dominio.

Carmen quiere evitar que esto suceda en CARMINFO S.L., así que, ha adquirido otro ordenador, ha instalado en él Windows Server 2008 R2 y está decidida a instalar un *controlador de dominio de respaldo*.

¿Qué harías tú en el lugar del informático encargado del dominio en la empresa de Carlos? Si tu respuesta es no volver a ir al trabajo por pura vergüenza, no estás muy desencaminado. En primer lugar, deberían haber programado copias de seguridad de los sistemas. Pero además, existe una forma muy sencilla de respaldar los datos del dominio, que cualquier informático debe conocer. Eso es lo que vas a aprender en este apartado.

En el controlador de dominio reside la base de datos de Active Directory, que, como ya sabes, almacena información sobre los equipos, usuarios, grupos, impresoras, etc. que pertenecen al dominio. ¿Cómo podemos proteger esa base de datos de un posible fallo físico del disco duro en el que reside?
Aparte de las copias de seguridad tradicionales, existe una forma de hacer una copia de seguridad de la base de datos de AD. Una vez que ya se tiene creado el dominio, existe la posibilidad de agregar controladores de dominio adicionales. Éstos son equipos con Windows Server, en los que también configuramos AD y que se comunican con el controlador de dominio principal para replicar la base de datos de AD. Esta replicación se realiza de forma automática.

Si por cualquier causa el primer controlador de dominio falla, los controladores de dominio adicionales que hayas configurado se hacen cargo de todas las tareas. Además, el hecho de tener varios controladores de dominio equilibra la carga de la red cuando se accede a la información de AD.

En el siguiente vídeo puedes ver el proceso de creación de un controlador de dominio de respaldo. Como puedes comprobar, el comando para iniciar el proceso es el mismo de siempre: **dcpromo**. Lo que ahora cambia es la respuesta a la pregunta del apartado "elegir una configuración de implementación". Ahora hay que contestar: "**Agregar** un controlador de dominio a un dominio existente".

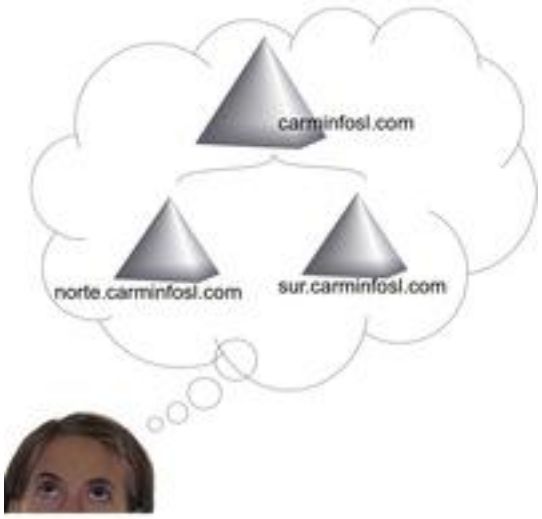
Texto enlace: Proceso de adición de un controlador de dominio de respaldo.
URL: SOR02_CONT_R14_ControladorDominioRespaldo.avi
Título: Vídeo sobre el proceso de adición de un controlador de dominio de respaldo.

Igual que en el apartado anterior, se tienen que cumplir los siguientes requisitos:

1. En la **configuración TCP/IP** del controlador de dominio de respaldo, has de establecer como servidor DNS preferido, la dirección IP del equipo que funciona como servidor DNS en el dominio.
2. Hay que utilizar las credenciales de **Administrador del dominio**.

3.- Dominios, árboles y bosques.

CASO PRÁCTICO



La compañía de publicidad GARABATO tiene oficinas repartidas por diferentes ciudades de España. Han contratado a CARMINFO S.L. Para realizar algunas de las tareas de la administración informática de la oficina de Santander.

En la toma de contacto con la red informática de GARABATO, Carmen y Laura pueden comprobar que es posible acceder a archivos, impresoras, etc. de todas las oficinas de la empresa, a pesar de estar repartidas por una gran extensión geográfica.

LAURA: ¿Has visto, Carmen? Desde aquí pueden ver los usuarios de toda España. ¿Cómo lo hacen?

CARMEN: ¿Te has fijado en que la red tiene varios dominios?

LAURA: Yo sólo veo *garabato.com*.

CARMEN: No, fíjate bien. Tienen *garabato.com*, y también *santander.garabato.com*, *sevilla.garabato.com*, *valencia.garabato.com*... Cada uno de esos nombres es un dominio. Están relacionados entre sí. Por eso, se pueden ver desde aquí los usuarios de todos ellos.

LAURA: Ah. ¿Y cómo se relacionan entre sí esos dominios?

CARMEN: En este caso, están formando un **árbol**. Otro tipo de relación formaría un **bosque**. Cuando volvamos a CARMINFO te lo explico tranquilamente. Además, yo tengo en mente algo parecido...

2.4 Jerarquías en Active Directory.

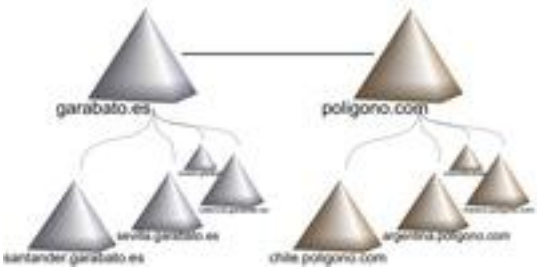
Hasta ahora has aprendido a crear un dominio, que es una agrupación de diferentes recursos unidos por un nombre de dominio y cuya información reside en Active Directory.

Varios dominios pueden relacionarse entre sí jerárquicamente, como en una relación de padre-hijo. En el ejemplo de la empresa GARABATO, puedes comprobar que hay un dominio principal, cuyo nombre DNS es *garabato.es*. Ese dominio principal tiene varios dominios secundarios, o dominios "hijos". En la figura se representan cuatro. Como puedes observar, los nombres de estos dominios se forman anteponiendo una etiqueta (por ejemplo, "santander") al nombre del dominio "padre" ("garabato.es"). Cada dominio hijo es un dominio con todas sus características y debe cumplir con los mismos requisitos (servidor DNS y controlador de dominio).

Cuando se organizan los dominios como en la empresa GARABATO, se dice que tenemos un ***árbol.***
Un árbol es una agrupación jerárquica de *dominios*, que además comparten el mismo espacio de nombres DNS. El dominio situado en la parte más alta de la jerarquía es el ***dominio raíz.*** El dominio raíz es siempre el primero que se establece cuando se crea un nuevo árbol de dominios.

A su vez, los árboles pueden establecer relaciones con otros árboles. Sin embargo, estas relaciones no son jerárquicas, sino de igual a igual. La relación que se establece entre dos árboles se llama "**relación de confianza bidireccional**". Cuando varios árboles se relacionan de esta forma, constituyen un ***bosque***.

Piensa en un conglomerado de empresas que pertenezca al mismo grupo. Por ejemplo, imagina que la empresa GARABATO pertenece a un grupo de empresas en el que también figura una editorial llamada POLÍGONO. GARABATO y POLÍGONO mantendrán árboles diferentes, con espacios de nombres DNS separados. Pero se puede establecer entre los dos árboles una relación de confianza, formando un bosque como el de la figura.



La ventaja de esta estructura es que se puede conceder permisos de acceso sobre los recursos de un dominio a los usuarios de todo el bosque. Por ejemplo, se puede conceder acceso a un usuario de *valencia.garabato.es* para que imprima en una impresora situada en el edificio central de POLIGONO. La impresora pertenecerá a *poligono.com*.

Con estas prestaciones **¿Quién necesita FAX?**

DESTACADO
El primer dominio que se crea en un bosque se denomina *dominio raíz del bosque.*

PARA SABER MÁS
En este enlace puedes encontrar toda la información de la biblioteca TechNet de Microsoft sobre Active Directory en general.

Texto enlace: Active Directory en Microsoft TechNet.
URL: http://technet.microsoft.com/es-es/library/cc782657(WS.10).aspx
Título: Información de Microsoft TechNet sobre Active Directory.

2.5 Cómo agregar un dominio a un árbol ya existente.

CASO PRÁCTICO

Después de lo que han visto en GARABATO, Laura y Carmen quieren experimentar con dominios, árboles y bosques en CARMINFO. Como CARMINFO es todavía una empresa joven y no tienen presupuesto para más servidores, deciden utilizar máquinas virtuales para hacer las pruebas.

Empezarán agregando un dominio secundario al árbol *carminfosl.com*, que ya está creado y funcionando. Soñando con una futura ampliación de la empresa, deciden llamar a este dominio secundario *sur.carminfosl.com*.

El proceso de creación de un dominio secundario es muy similar al de creación del dominio raíz. En el apartado 3, aprendiste a crear un dominio completamente nuevo, es decir, aprendiste a crear el dominio raíz de un bosque.

Para configurar un equipo como controlador de un dominio secundario de un árbol ya existente, aparte de contar con acceso de administrador local al equipo, también es necesario que tengas acceso a una cuenta del grupo "Administradores de organización". Lo más sencillo es controlar la cuenta de Administrador en el *dominio raíz*. Esta cuenta pertenece a dicho grupo. En el caso práctico, para crear *sur.carminfosl.com*, habrá que acceder con el usuario Administrador de *carminfosl.com*.

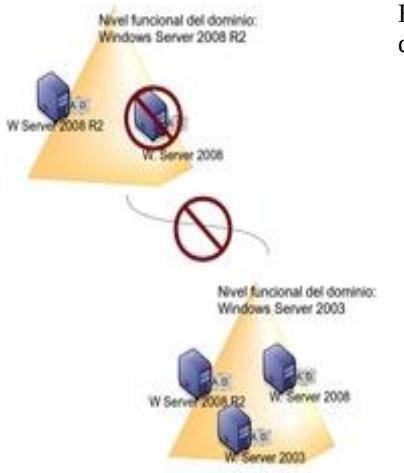
También es necesario controlar la configuración TCP/IP. Ya sabes que es conveniente que los controladores de dominio tengan una IP estática. Además, para que el equipo reconozca el espacio de nombres DNS del dominio,

en la configuración TCP/IP debes establecer como servidor DNS preferido la IP del servidor DNS del dominio raíz. Por supuesto, el dominio principal debe estar en funcionamiento y debe existir conectividad con él.

A continuación puedes ver un vídeo en el que se completa el proceso de instalación de AD y se crea el dominio secundario.

Texto enlace: Proceso de creación de un dominio secundario.
URL: SOR02_CONT_R18_CreacionDominioSecundario.avi
Título: Vídeo que ilustra el proceso de creación de un dominio nuevo en un árbol existente.

El asistente realiza varias preguntas importantes. Para asignar un dominio secundario a un árbol ya existente, en el apartado "elegir una configuración de implementación", debes optar por la opción **"crear un dominio nuevo en un bosque existente".**



Hasta ahora, no se ha abordado el tema del ***nivel funcional.*** El nivel funcional de un dominio determina su compatibilidad con versiones anteriores:

- Si el nivel funcional del bosque es **X**, sólo se pueden conectar a este bosque dominios con nivel funcional X o más moderno que **X.**
- Si el nivel funcional de un dominio es **Y**, sólo se pueden configurar como controladores de este dominio equipos con sistema operativo **Y** o más moderno.
- Si el nivel funcional del bosque es Windows **Server 2003,** sólo podrás unir dominios con nivel funcional Windows Server 2003, Windows Server 2008 o Windows Server 2008 R2.
- Si seleccionas como nivel funcional de un dominio "Windows **Server 2008**", todos los controladores de dominio que configures tendrán que tener como sistema operativo Windows Server 2008 o Windows Server 2008 R2.

2.6 6.3.- Cómo agregar un árbol nuevo a un bosque.

CASO PRÁCTICO
En su fantasía de construir el árbol de dominios de una gran empresa, Laura reivindica su propio espacio: quiere que se tenga en cuenta su futura empresa: LAURINFO S. L.

CARMEN: ¿Ya quieres dejar CARMINFO?

LAURA: Bueno... Podríamos asociarnos. Compartir información, recursos, impresoras... Pero yo quiero tener mi propio árbol: *laurinfosl.com*.

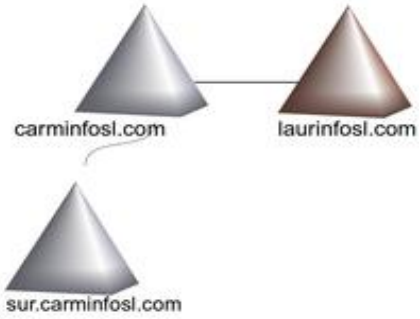
CARMEN: Laura, que sólo estamos haciendo pruebas con máquinas virtuales.

LAURA: Ya lo sé, pero soñar es gratis. Además, así probamos cómo crear un bosque: uno que incluya *carminfosl.com* y *laurinfosl.com*.

CARMEN: Vale, me has convencido.

A veces se desea compartir recursos entre dominios que no comparten espacio de nombres DNS. En este caso, los dominios pertenecen a árboles diferentes y lo que hay que hacer es establecer una *relación de* ***confianza bidireccional.***

Esto es lo que en el apartado 6 sucedía con *garabato.es* y *poligono.com.* En el caso práctico, el diagrama completo del bosque quedaría como el de la siguiente figura.



Para crear *laurinfosl.com* y hacerle formar parte del bosque ya existente (*carminfosl.com*), deberías iniciar el asistente de instalación de los servicios de dominio de AD, ejecutando el proceso **dcpromo.** En esta ocasión**,**

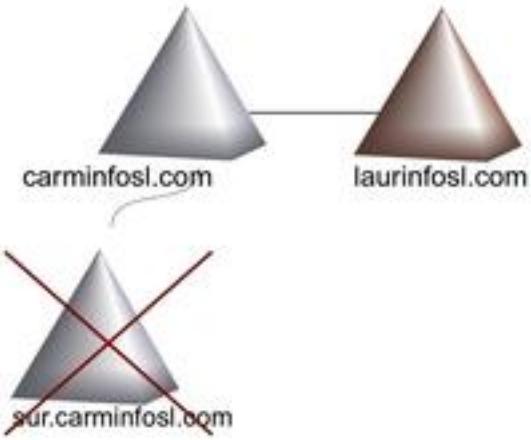
- ✓ marcarías la opción **"Usar la instalación en modo avanzado**".
- ✓ En el apartado "elegir una configuración de **implementación**", tendrías que marcar "**Bosque existente**".
- ✓ Después, "crear un dominio **nuevo** en un b**osque existente**"
- ✓ Marcar la casilla de verificación de "c**rear una raíz de árbol** de dominio nueva en lugar de un nuevo dominio secundario".

En el siguiente vídeo puedes ver todo el proceso.

Texto enlace: Creación de un árbol nuevo en un bosque existente.
URL: SOR02_CONT_R22_NuevoArbolBosqueExistente.avi
Título: Vídeo que ilustra el proceso de creación de un árbol nuevo en un bosque existente.

2.7 Cómo eliminar un dominio.

CASO PRÁCTICO



Una vez satisfecha su curiosidad sobre cómo crear dominios, árboles y bosques, Laura y Carmen ya no necesitan para nada los dominios adicionales que crearon.

LAURA: Como ya no usamos *sur.carminfosl.com* ni *laurinfosl.com*, ¿por qué no borramos directamente las máquinas virtuales en las que los creamos?

CARMEN: No, Laura, no hay que hacer eso. El dominio *carminfosl.com* no lo vamos a borrar. Si borramos "a lo bruto" dominios que estén relacionados con él, va a seguir pensando que existen y contendrá información incoherente.

LAURA: Entonces habrá que borrarlos siguiendo el procedimiento indicado. Así, el "superviviente" tendrá la información actualizada.

El proceso de eliminación de un dominio consiste en desinstalar los servicios de Active Directory de todos los controladores de dominio que pertenezcan al dominio. Cuando se desinstala AD del último controlador de dominio que queda, el dominio queda eliminado. Todos los datos de la base de datos de AD se pierden, así que esta operación debe realizarse con precaución. Puede parecerte sencillo, y lo es, pero hay que respetar ciertas reglas. Si no es así, te pueden surgir problemas difíciles de solventar.

1. Antes de eliminar un dominio, tienes que hacer cambios en los equipos miembros del dominio. En concreto, tienes que hacer que sean miembros de un grupo de trabajo, en lugar de miembros del dominio. Este paso no puede realizarse en los controladores.
2. Para eliminar un dominio hay que ser miembro del grupo "Administradores del dominio" (en el *dominio raíz del bosque*) o del grupo "Administradores de organización".
3. Cuando en el dominio existen varios controladores, hay que repetir el procedimiento en cada controlador.
4. Si el dominio tiene dominios secundarios, no se puede eliminar. Por ejemplo, si *sur.carminfosl.com* sigue existiendo, no puedes eliminar *carminfosl.com*. Tendías que eliminar primero el dominio secundario.

5. Si estás eliminando el último dominio de un bosque, al eliminar el dominio vas a eliminar también el bosque, con toda su información asociada.

El procedimiento que has de seguir para eliminar un dominio se inicia ejecutando **dcpromo** en un controlador de dominio. En el siguiente vídeo puedes ver el proceso completo.

Texto enlace: Eliminación de un dominio.
URL: SOR02_CONT_R24_EliminacionDominio.avi
Título: Presentación que ilustra el proceso de eliminación de un dominio.

2.8 Características de Active Directory

• Escalabilidad : Puede crecer y soportar un elevado número de objetos.
• Integración con el DNS
- Los nombres de dominio son nombres DNS y tienen que estar registrados en él.
- AD usa DNS como servicio de nombres y de localización.
- Es necesario instalar DNS antes de poder instalar AD.

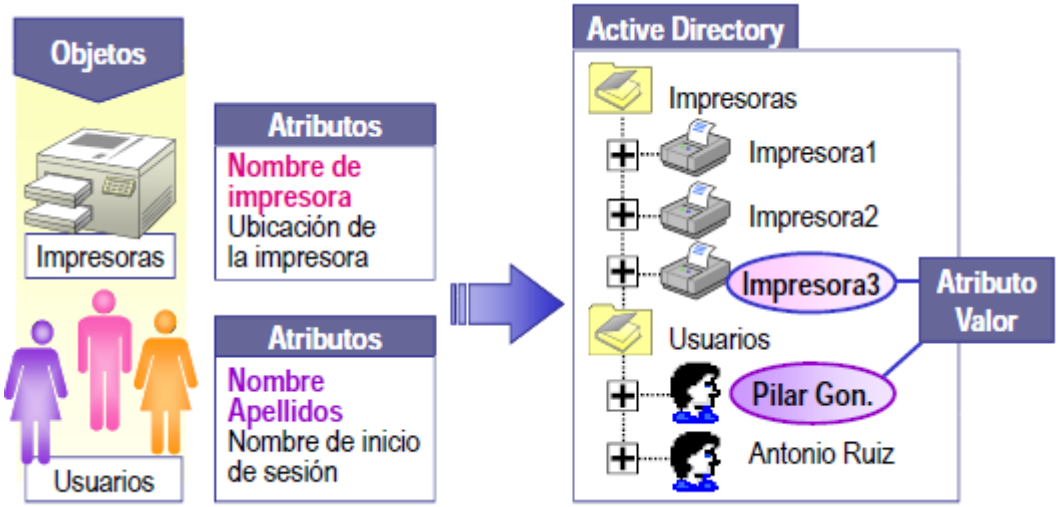
• Extensible: Permite personalizar las clases y objetos que están definidas dentro de AD según las necesidades propias.
• Seguridad: Incorpora las características de seguridad de W2008-Server, p.e., se puede controlar el acceso a cada objeto.
• Multimaestro
- No distingue entre controladores de dominio primarios o secundarios.
- Cualquier controlador de dominio puede procesar cambios del directorio.
- Las actualizaciones o modificaciones realizadas en un controlador se replican al resto, siendo todos "iguales".

• Flexible
- Permite reflejar la organización lógica y física de la empresa u organización donde se instala.
- Permite que varios dominios se conecten en una estructura de árbol o de bosque.

• Sigue el estándar LDAP (Lightweight Directory Access Protocol)

2.9 Organización de AD

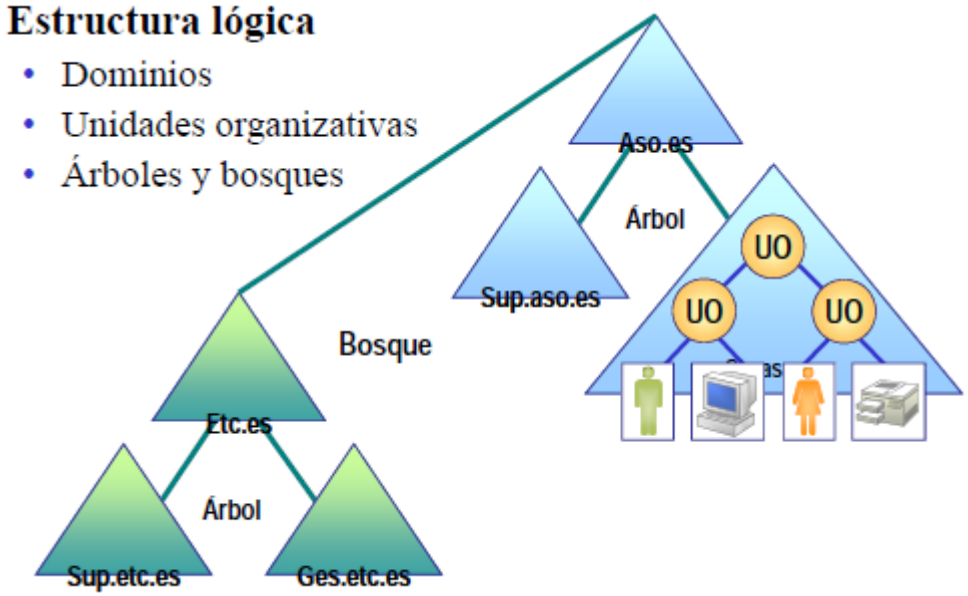
• Objetos de Active Directory
– Active Directory almacena información sobre los recursos de red y proporciona los servicios que permiten que la información se encuentre disponible y sea útil
– Esta información la pone a disposición de los administradores y los usuarios de la red
• P.e., almacena información sobre las cuentas de usuario (nombres, contraseñas, nº de teléfono, etc.) y permite que otros usuarios autorizados de la misma red tengan acceso a esa información
– Los recursos almacenados se denominan objetos y pueden ser: usuarios, impresoras, servidores, bases de datos, grupos, equipos y directivas o políticas de seguridad
– Un objeto es diferenciado por su nombre y representa un recurso de red
– Un objeto tiene un conjunto de atributos que lo definen y son sus características (para un usuario su nombre, apellidos, e-mail, ...)



Atributos
• Los objetos representan los recursos de red
• Los atributos definen la información relativa a un objeto
• Estructura lógica
– Active Directory organiza los recursos mediante una estructura lógica, lo que permite localizar un recurso por su nombre y no por su localización física (que se hace transparente a los usuarios)
– Dominio
• Colección de equipos que comparten la base de datos del Active Directory y que se administran de forma conjunta
– Los controladores de dominio, almacenan una copia de la base de datos y permiten gestionarla y administrarla. También controlan el acceso a la red, a la BD del directorio y a los recursos compartidos
– Los servidores miembros usan los servicios y recursos
• El dominio es la unidad central de la estructura lógica de AD
• Un dominio se crea al generar el primer controlador del dominio

• Un dominio representa:
  – El límite para la autenticación
  – El límite para la replicación de la base de datos
  – El límite para las políticas o directivas
• El nombre del dominio debe ser único y ha de estar registrado en el DNS
– El DNS es la base de la infraestructura del Active Directory ya que permite que los servidores miembros localicen a los controladores de dominio
• Un dominio puede estar en varias subredes
• En una red pueden existir varios dominios
• Mantiene su ACL (lista de control de acceso) con todos los permisos para los recursos del dominio, controlando los usuarios que pueden acceder al mismo y el tipo de acceso • Los elementos de la base de datos del directorio (cuentas de usuarios, grupos, equipos y recursos compartidos, como impresoras y carpetas) los usarán todos los equipos del dominio
• Todos los recursos (u objetos) de la red existen en un dominio y cada dominio almacena información exclusivamente de los objetos que contiene
– Unidades organizativas
• Los recursos del dominio se organizan en Unidades Organizativas (OU, Organizational Units), que son contenedores (como directorios) que permiten ordenar los recursos u objetos dentro de un dominio
• Contienen agrupaciones lógicas de recursos, como archivos, impresoras, cuentas, aplicaciones y otros recursos del dominio
• Son como subgrupos dentro del dominio que reflejan, normalmente, la estructura funcional o de negocios de una organización
• Sólo pueden contener objetos del dominio al que están asociados
• Crean vistas del directorio más pequeñas y manejables
• Se puede delegar la autoridad sobre las mismas, para manejar con más facilidad el acceso a los recursos administrativos
– A nivel de Administración permiten
  – Agrupar objetos con los mismos requerimientos
  – Delegación de tareas de una unidad organizativa
  – A nivel de políticas (directivas) de grupo permiten
  – Establecer una configuración distinta a una unidad organizativa
  – Establecer detalles de seguridad distintos a una unidad organizativa
– Ejemplo de unidades organizativas
• Usuarios (unidad organizativa)
• Profesores (unidad organizativa)
• AdministraciónSistemasOperativos (uo)
Pilar, Álvaro, José (usuarios)
• Arquitectura (uo)
Javier, Manolo, Antonio, Gregorio (usuarios)
• Redes (uo)
Juan, Óscar, Félix (usuarios)

Árboles de dominio
• Un árbol de dominio es una agrupación de uno o más dominios que comparten un espacio de nombres continuo



– aso.es (ppal), sup.aso.es, sis.aso.es, ges.aso.es (el resto secundarios)
• El nombre de dominio de un dominio secundario es el nombre relativo a ese dominio agregado al nombre del dominio ppal
• Los dominios dentro del árbol comparten el esquema común, el catálogo global y los datos de configuración (topología del directorio)
• Confianza: los dominios de un árbol están conectados por medio de relaciones de confianza
• Al crear un nuevo dominio ya forma un árbol: es el dominio principal de ese árbol

– Bosques de dominio

• Un bosque de dominio está compuesto por uno o más árboles de dominio distintos e independientes entre sí, que comparten información del directorio común
– aso.es, sup.aso.es, sis.aso.es, ges.aso.es
– etc.es, sup.etc.es, sis.etc.es, ges.etc.es
– redes.es, sup.redes.es, sis.redes.es, ges.redes.es
• Todos los árboles de un bosque comparten el esquema común, el catálogo global y los datos de configuración
• Los dominios en un bosque operan independientemente, pero el bosque permite la comunicación a lo largo de toda la organización
• El bosque tiene un único dominio raíz, llamado dominio raíz del bosque, que es el primer dominio creado en el mismo
• Los nombres de dominio dentro de un bosque pueden ser discontinuos o continuos en la jerarquía del DNS
– Continuos: están en el mismo árbol de dominio
– Discontinuos: forman varios árboles de dominio
• Por defecto, un único dominio ya forma un árbol y un bosque
– Se puede ampliar el árbol añadiendo un nuevo dominio con un – Se puede ampliar el bosque al añadir un nuevo dominio con un nombre discontinuo, que formará un nuevo árbol de dominio

Estructura lógica

• Dominios
• Unidades organizativas
• Árboles y bosques

Estructura física

– **Controlador de dominio**
• Un controlador de dominio es un equipo con W2008Server que almacena una copia del directorio del dominio (base de datos local del dominio)
• Puede haber varios controladores de dominio, cada uno de ellos tendrá una copia completa del directorio
• Cada controlador permite realizar cambios en el directorio, administrando los cambios y replicándolos a los otros controladores de dominio del mismo dominio
• Los controladores de dominio administran todas las facetas de las interacciones de los usuarios en un dominio (localización de objetos o validación de un intento de inicio de sesión, ...)

• La replicación se hace en intervalos de tiempo, pudiendo establecer la frecuencia a la que se producen las replicaciones entre controladores de dominio
• AD usa un modelo replicación multimaestro:
– Ningún controlador del dominio es el maestro
– Todos los controladores son "iguales" y contienen una copia de la BD del directorio. (En realidad todos los controladores son "casi iguales")
– Los controladores replican los cambios entre ellos
– Cualquier controlador de dominio puede procesar los cambios del directorio y replicarlos
• Los controladores de dominio replican inmediatamente ciertas actualizaciones urgentes, por ejemplo la eliminación de una cuenta de usuario
• Establecer varios controladores de dominio dentro de un dominio permite tener tolerancia a fallos
• Todos tienen asignadas las mismas tareas salvo:
– Servidor de cabeza de puente para replicar información del directorio con otros sitios
– Las funciones del maestro de operaciones
– Sitios
• Un sitio es una agrupación de equipos que están conectados físicamente por conexiones rápidas y de alta fiabilidad.
Habitualmente equipos conectados en una LAN
• La razón básica de crear sitios es aprovechar los mecanismos de comunicación "eficientes" (rápidos y fiables) entre sistemas bien comunicados
• Un sitio es básicamente una subred TCP/IP
• Son independientes de la estructuras lógica de dominio. No existe relación entre la estructura física de la red y la lógica del dominio:
– Un único dominio puede estar en varios sitios
– En un sitio puede haber varios dominios
• Importante no confundir sitio con dominio:
– Dominio: agrupación lógica de usuarios y equipos
– Sitio: agrupación física de equipos
Los equipos están asignados a sitios según su localización en la subred o en un conjunto de subredes
• Si la empresa tiene varias subredes que no tienen buena conexión entre sí o están en ubicaciones geográficas distintas, (p.e. una sucursal en Murcia y otra en Cartagena), hay que definir un sitio por cada subred
• Debe tener asociado, al menos, un controlador de dominio en cada sitio (para facilitar y acelerar el acceso a los datos del AD)
• La información de los sitios se usa para:
Validación de seguridad en los servidores miembros: el proceso de autenticación se hace en los controladores del dominio del sitio en el que está el servidor miembro (si es posible …)
La replicación de la información de directorio se hace con más frecuencia dentro de sitios que entre sitios (reduciendo el tráfico de la red)
• Un controlador del dominio será servidor de cabeza de puente:
realiza la réplica de datos hacia y desde un sitio, y envía los datos recibidos a los otros controladores del sitio

2.10 Espacio de nombres

Los nombres de AD son nombres registrados en el servidor de DNS, por lo que se pueden usar formatos de nombre estándar del tipo aso.es
Esto permite la estructuración jerárquica de AD
Nomenclaturas: 4 nomenclaturas para identificar objetos
• DN (Distinguished Name) (nombre completo)
Único para cada objeto
Contiene suficiente información para que un usuario recupere el objeto del directorio, incluyendo el nombre del dominio y la ruta
Se compone de varios atributos: el nombre del dominio al que pertenece (DC) y de las unidades organizativas en las que está (OU) y el nombre relativo del objeto (CN)
• RDN (Relative Distinguished Name) (nombre completo relativo)
Identifica unívocamente al objeto dentro su unidad organizativa
Es parte del DN
Podemos tener dos objetos con el mismo nombre si los objetos pertenecen a distintas Unidades Organizativas
• GUID (Globally Unique Name) (identificador global único)
Número de 128 bits, distinto para cada objeto, y que no cambia nunca
Es único y está formado por el Id de seguridad del dominio (prefijo) y un Id relativo único, (asignado por el maestro de operaciones)
• UPN (User Principal Name) (nombre principal de usuario)
Son nombres cortos y descriptivos del objeto
El nombre común del objeto se combina con el dominio para formar el UPN

Supongamos que tenemos el dominio aso.es y dentro de él la unidad organizativa users, dentro la unidad organizativa Profesores y dentro el usuario Pilar:

– El nombre completo o distinguished name para este usuario:

» CN=Pilar,OU=Profesores,OU=users,DC=aso,DC=es

– El nombre completo relativo o Relative Distinguished Name:

» Pilar

Si movemos el usuario Pilar a una nueva unidad organizativa llamada Investigadores:

– El nombre completo o distinguished name será:

» CN=Pilar,OU=Investigadores,DC=aso,DC=es

UPN: pilar@aso.es