Introducción al Directorio Activo con Windows Server

Windows Server.

Windows Server (2003/2008/2012/2016/2019) es un SO de entorno servidor de los más extendidos en la actualidad. Es un SO con interfaz gráfica, multitarea, multiusuario y que trabaja en tiempo real/compartido.

Las versiones básicas de Windows Server son multitarea real, puesto que todas son capaces de gestionar dos o más procesadores gracias al Multiproceso Simétrico (SMP).

Hay versiones más avanzadas que pueden gestionar hasta 16 procesadores.

Todas las versiones de Windows Server soportan programas o aplicaciones DOS (8 bits) y aplicaciones Windows de 16 y 32 bits (y la mayoría de las versiones soportan las de 64 bits).

Windows Server se diseñó para trabajar con múltiples arquitecturas, por lo que tiene una gran portabilidad.

La interfaz gráfica es como la de las versiones de sobremesa (XP, 7, 10...).

Windows 2003 Server se parece más a XP, Windows 2008 Server a 7, Windows Server 2012 y 2016 se parecen a W10.

También podemos interactuar con el SO por una CLI (shell o intérprete de comandos).

Inicio del sistema Windows Server.

Un SO servidor no se suele apagar. Normalmente, una vez instalados, se mantienen encendidos ininterrumpidamente, ya que suelen dar servicios a empresas u organizaciones y siempre deben estar disponibles.

Puntualmente los SO servidores se pueden apagar por necesidades de mantenimiento del hardware o del software

El botón “Inicio” suele encontrarse en la parte izquierda de la barra de tareas. Las opciones habituales que aparecen son prácticamente las mismas que en las versiones de sobremesa (la posición, aspecto y opciones del botón “Inicio” dependen de la versión).

Tras iniciar el sistema y pulsar la combinación de teclas Ctrl+Alt+Supr, aparecerá la pantalla de login, donde introducimos el nombre de un usuario que puede iniciar sesión en el equipo, así como su contraseña.

Si la última vez que se usó el equipo se cerró correctamente, se volverá a iniciar sin problemas. Pero a veces no cierra de forma correcta por causas hardware (bloqueo del sistema, corte de corriente...) o software (instalación un programa problemático, virus...).

Cuando no cerró correctamente, en el siguiente inicio, aparece un menú en modo texto muy similar a las versiones de sobremesa.

También se puede iniciar este menú manualmente pulsando F8 durante el inicio del sistema.

Apagado del sistema Windows Server.

Para apagar o reiniciar el equipo usaremos el botón “Inicio”. Se mostrará una pantalla en la que tenemos que indicar si se ha planeado o no el apagado, e indicar por qué apagamos el equipo, añadiendo una breve descripción (toda la información es registrada por el sistema).

Si el equipo se apaga inesperadamente, durante el siguiente inicio de sesión habrá que indicar esta información para que la registre (“Rastreador de eventos de apagado”). 2.- Servicio de directorio y dominio.

Servicio de directorio y de dominio

Los administradores de redes saben que la forma más eficiente de aprovechar el potencial de los equipos con Windows Server es mediante la creación de “dominios”.

Un dominio es un conjunto de elementos (ordenadores, usuarios, directorios, archivos, periféricos...), cuya información administrativa y de seguridad se almacena de forma centralizada, facilitando así la labor del administrador.

Windows Server utiliza el concepto de Directorio Activo (AD, Active Directory) para gestionar estos dominios.

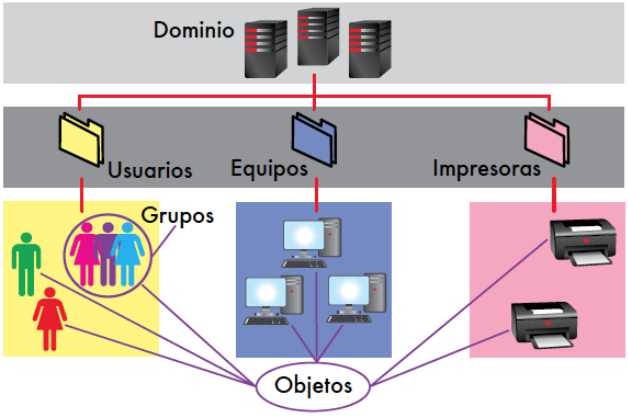
El Directorio Activo es un servicio de directorio de una red Windows Server, que guarda en una base de datos toda la información sobre los recursos de la red y permite el acceso de los usuarios a dichos recursos y a determinadas aplicaciones. De esta forma, consigue gestionar de forma centralizada el acceso a los recursos de la red.

Cuando instalemos un DA en uno o varios equipos Windows Server, convertimos a dichos equipos en "controladores de dominio" (Domain Controllers).

El resto de los equipos de la red podrán actuar como clientes del dominio, y tendrán acceso a la información almacenada en los controladores de dominio (cuentas de usuario, grupo, equipo, etc.).

Una de las ventajas fundamentales del DA es separar la estructura lógica de la organización (dominios) de la estructura física (topología de red).

La estructura de un DA se basa en los siguientes conceptos:



Dominio: Estructura fundamental. Agrupa todos los objetos que se administran de forma estructural y jerárquica.

Unidad organizativa (UO): Es la unidad jerárquica inferior al dominio y que puede estar compuesta por una serie de objetos y/o por otras UO. Las unidades organizativas son contenedores del Directorio Activo.

Grupos: Conjunto de objetos del mismo tipo que se utilizan fundamentalmente para la asignación de derechos de acceso a los recursos. Normalmente son de usuarios.

Objetos: Son una representación de un recurso de red, como pueden ser usuarios, impresoras, ordenadores, unidades de almacenamiento, etc.

El Directorio Activo de Windows Server.

Cada dominio de Windows Server queda identificado unívocamente mediante un nombre DNS (Ej: midominio225.es).

Cada equipo perteneciente al dominio tendrá un nombre de tipo DNS, que está formado por un nombre NetBios y un sufijo que será el nombre DNS del domino (Ej.: servidor1.midominio225.es).

El DA utiliza los nombres y servicios DNS para tres funciones principales:

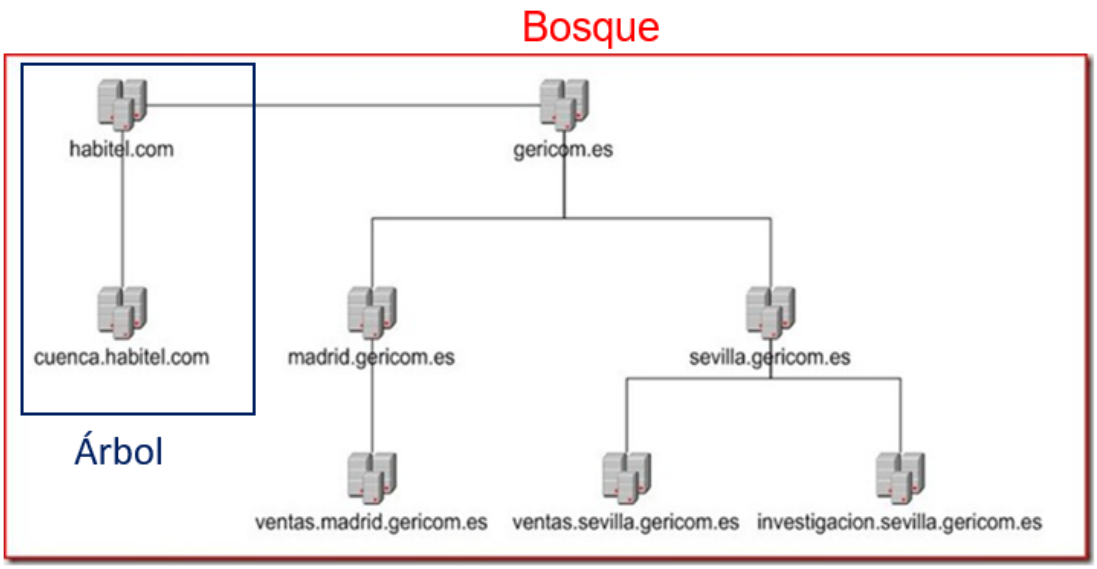
- Resolución de nombres: convierte nombres DNS en direcciones IP.
- Definición del espacio de nombres: los nombres del dominio y sus objetos son de tipo DNS.
- Búsqueda de los componentes de DA: busca los objetos del dominio (controladores, servidores, equipos...) por su nombre DNS.

Algunos términos utilizados habitualmente en DA son:

Espacio de nombres: es un área delimitada (dominio, subdominio, árbol, bosque) donde el nombre de cualquiera de sus objetos tiene el mismo sufijo (Ej.: **equipo1.dominio.es** y **equipo2.dominio.es**).

Resolución de nombres: proceso de traducción de un nombre DNS al objeto o información que representa.

Controlador de dominio: es un equipo cuyo S.O. es un Windows Server, y que tiene el servicio de D.A. instalado.



Árbol: conjunto de uno o más dominios que comparten un espacio de nombres contiguo. Si hay varios, se organizan en estructura de árbol jerárquico.

El primer dominio creado es la **raíz** del árbol.

Cuando se agregan dominios a un árbol, serán dominios secundarios, hijos, o subdominios.

Los dominios secundarios suelen representar entidades geográficas, departamentos, u otras divisiones de la organización.

Bosque: grupo de árboles que no comparten un espacio de nombres contiguo, y que se conectan a través de relaciones de confianza.

Un dominio único constituye un árbol (de un solo dominio) y, a su vez, un bosque (de un solo árbol).

Un bosque tiene un único dominio raíz, que será el primer dominio creado por la organización.

Estructura física de un dominio en Windows Server. Requisitos.

Anteriormente se utilizaba la interfaz NetBios, pero ahora se utiliza el sistema de "espacio de nombres DNS" (NetBios se incluye por compatibilidad).

El servicio de DA permite que los usuarios tengan un único inicio de sesión independientemente del ordenador en el que se sienten. Desde allí, podrán acceder a los recursos de la red para los que esté autorizado.

Requisitos para crear un dominio:

Instalar cualquier versión de Windows Server. El equipo donde se instale tendrá un nombre único (distinto del resto) en la red. El nombre de equipo y dominio no pueden coincidir.

TCP/IP instalado y configurado manualmente y no de forma automática con DHCP.

Instalar y configurar el servicio de DNS. Durante el proceso de instalación de DA el SO se encarga de instalarlo y configurarlo adecuadamente de forma automática (no es necesario hacerlo previamente).

Tener espacio libre en disco y por lo menos una partición debe estar en formato NTFS, no necesariamente donde esté instalado el SO.

Que el usuario Administrador del equipo tenga contraseña.

Si sólo instalamos Windows Server, ni siquiera se puede considerar un servidor (es un "standalone"); si tiene instalado algún servicio conseguimos un "servidor independiente"; y sólo cuando instalamos DA conseguimos que se convierta en "controlador de dominio".

Especificaciones de dominio en Windows Server.

Antes de empezar a instalar DA en nuestra organización, tendremos que realizar una planificación de la estructura de dominios que deseamos tener:

Necesitamos un solo dominio o árbol: En este caso, tendremos un ordenador principal que controle todo el sistema, teniendo o no dominios hijos delegados o subdominios. El dominio principal tendrá un nombre como "dominioprincipal.com", y el resto de dominios hijos, tendrán nombres como "subdominio1.dominioprincipal.com", "subdominio2.dominioprincipal.com", etc.

Necesitamos varios dominios o árboles: Contaremos con dos controladores principales de dominio, por ejemplo dominioprinipal1.com y dominioprincipal2.com, con sus correspondientes subdominios y controladores adicionales.

La estructura jerárquica de dominios se crea «de arriba hacia abajo», es decir, primero debemos crear el dominio raíz del árbol y posteriormente el resto de subdominios. La unión de todos los árboles forma el bosque.

El primer controlador de dominio instalado en la organización es el dominio raíz del bosque, el cual contiene la configuración y el esquema del bosque (compartido por todos los dominios de la organización).

Después podemos agregar más dominios para que crezca ese árbol o para crear nuevos árboles en ese bosque.

Instalación y desinstalación del Directorio Activo.

Consideraciones previas a la instalación del Directorio Activo.

Antes de instalar DA nos tendremos que fijar en:

Si queremos que el equipo donde instalemos y configuremos DA sea en el único servidor o controlador de dominio de la red, o queremos que haya más servidores o controladores de dominio.

Necesitaremos saber el nombre del equipo donde instalaremos DA.

Al instalar el SO, el equipo pertenecerá a un grupo de trabajo, pero esto ya no tendrá importancia después de instalar DA (pertenecerá a un dominio).

Revisar la configuración TCP/IP de red, que debe ser configuración manual:

- IP: dirección única de esa red (ej.: 192.168.1.1).
- Máscara: la correspondiente a ese tipo de red (ej.: 255.255.255.0).
- Puerta de enlace: dirección del **router** o proxy que da acceso al exterior (Internet).
- Servidor DNS: su propia dirección (127.0.0.1).

Ojo!! Hay que poner la máquina virtual en “adaptador puente” y procurar activar la detección de redes y el uso compartido de archivos en el “Centro de redes y recursos compartidos”.

Identificación del equipo: podemos elegirlo, pero no puede estar repetido en la red y debe ser significativo para que identifique bien al controlador de dominio.

Credenciales del administrador de red: es imprescindible que el Administrador del equipo tenga una contraseña que cumpla los requisitos de seguridad (al menos 8 caracteres que incluyan mayúscula, minúscula y número).

Instalación de Servicios de dominio de DA.

Es imprescindible instalar estos servicios de dominio como paso previo.

Se encuentra en “Agregar Roles o características”.

Gracias a estos servicios, se almacena la información de los recursos del dominio, y se facilita la administración del mismo y la compartición de los recursos.

Promover (promocionar) el equipo Windows Server a controlador de dominio.

La instalación del DA también se denomina “promoción”.

También se puede utilizar el comando “dcpromo” (si se ejecuta desde el principio, también instala los “Servicios de dominio de DA”).

Elegir el tipo de controlador de dominio:

- Nuevo bosque (dominio raíz de la organización).
- Nuevo árbol dentro del bosque.
- Dominio secundario o subdominio.
- Controlador de dominio adicional.

Introducir nombre del dominio, subdominio, etc.

Nivel funcional del bosque: indicamos el sistema más antiguo de todos los controladores de dominio del bosque para que haya compatibilidad entre todos.

Si no está instalado el servidor DNS (que es imprescindible), aparecerá una pantalla donde podemos indicar que lo instale ahora.

Puede aparecer una pantalla que indique que hay algún adaptador de red que tiene asignadas direcciones IP dinámicamente. Puede deberse a que:

- Olvidamos poner una configuración IPv4 estática.
- Tenemos activado el protocolo IPv6 (debemos desactivarlo).

En todo caso, en esta pantalla indicaremos que asignaré direcciones IP estáticas en todos los adaptadores.

Elegir ubicación del Directorio Activo (c:\windows\NTDS) y de la copia de seguridad del dominio en el servidor (c:\windows\SYSVOL). Es modificable su ubicación pero no el nombre final de los directorios, y siempre deben estar en una partición NTFS.

Introducir la contraseña del Administrador (para poder gestionar algunos componentes del DA).

Ofrece un resumen de las acciones que realizará y finalmente instala DA.

Reiniciar el equipo y comprobar que ya es controlador de dominio.

Eliminación de un controlador de dominio.

Si decidimos desinstalar DA (despromocionar) perderemos toda la configuración realizada hasta el momento, como cuentas de usuario, grupos, equipos, etc., ya que se borra la base de datos y el catálogo global del dominio que estaba guardado en ese equipo (que deja de ser controlador de dominio).

Si existen más controladores de dominio en ese dominio, la base de datos y el catálogo global no se pierde, ya que está duplicado en cada controlador de dominio.

Ojo: al igual que pasaba al instalarlo, no es lo mismo despromocionar (o despromover) un controlador de dominio que desinstalar los servicios de dominio de DA:

Despromocionar: se elimina la base de datos del dominio y, por tanto, los clientes no se pueden conectar al dominio a través de ese equipo.

Desinstalar servicios: ese equipo no podrá administrar otros dominios y subdominios de la red (de forma sencilla).

Para despromover, volvemos a ejecutar “dcpromo” (mensaje de advertencia).¿Este controlador de dominio es el último que queda o hay más?

Si es el último, hay que marcar la casilla de verificación. Si quedan otros controladores adicionales o existen subdominios de éste, no se marca.

Hay que eliminar los controladores de dominio en orden inverso a como se crearon: no se pueden borrar dominios sin borrar antes sus subdominios, ni el dominio raíz sin borrar antes todo el árbol.

Solamente al eliminar el último controlador de dominio de la infraestructura, que será el primer equipo en el que se instaló DA, se destruye definitivamente la base de datos de objetos de DA.

También pregunta si queremos borrar las particiones donde se ha replicado la

base de datos del dominio (normalmente se borran).

Puede que nos pregunte si queremos desinstalar el servidor DNS. Responderemos según nuestras necesidades.

Introducir la contraseña del Administrador y reiniciar el equipo.

Recordar que los servicios de dominio de DA siguen instalados.

Si este procedimiento falla o nos da un error, podemos intentar con el comando “dcpromo /forceremoval”.

Gestión de dominios Windows Server.

Cuando un equipo con Windows Server es controlador de dominio, puede gestionar el dominio de forma centralizada, ya que dispone de una base de datos jerárquica con todos los objetos del mismo, que pueden ser creados, configurados, eliminados...

Objetos que administra un dominio.

A.- Usuarios globales.

Cuando tenemos instalado un controlador de dominio con Windows Server, se crean en el sistema cuentas de usuario (***users***) y de grupo globales. Las cuentas y grupos locales del equipo desaparecen. Estas cuentas globales sirven para:

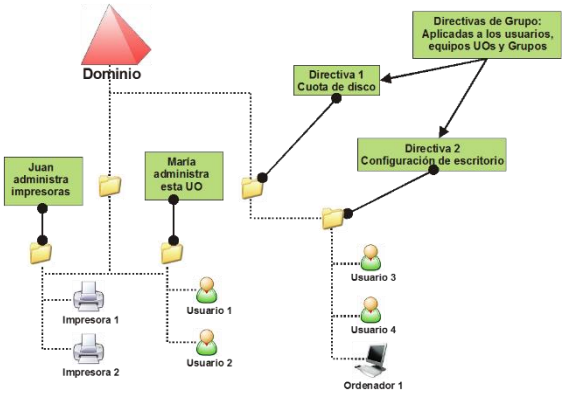
- Identificar y autentificar a las personas (usuarios) que podrán loguearse al dominio.
- Administrar y gestionar los permisos y privilegios que servirán para controlar el acceso de los usuarios a los recursos del sistema.

Las cuentas de usuario globales representan una cuenta única de usuario que se puede utilizar desde cualquier ordenador integrado en el dominio. La información de la cuenta se guarda en la base de datos del DA.

Los equipos clientes pueden tener, además de cuentas globales del dominio, sus propias cuentas locales.

B.- Grupos.

De forma similar a los usuarios globales, existen grupos (*groups*) que son almacenados en el Directorio Activo y que por tanto son visibles desde todos los ordenadores del dominio.



Sirven principalmente para agrupar usuarios u otros objetos, y poder conceder permisos sobre recursos a todos sus miembros a la vez en lugar de uno en uno.

Existen dos tipos de grupos: grupos de distribución y grupos de seguridad.

C.- Equipos.

La base de datos del DA también almacena información relativa a los equipos (computers) que forman parte del dominio.

Almacena el nombre del ordenador, así como un identificador único y privado, gracias al cual, a cada equipo se pueden asignar permisos y derechos (el resto de objetos también tienen este identificador).

D.- Unidades Organizativas.

Son objetos del DA que a su vez pueden contener otros objetos. Se usan para delegar la administración de sus objetos a otros usuarios distintos del administrador del dominio, y para personalizar el comportamiento de los usuarios y/o equipos mediante la aplicación de directivas.

Herramientas básicas de administración de dominios.

Al instalar DA, surgen algunas herramientas para administrar la base de datos, los objetos y los recursos del dominio.

Dichas herramientas se encuentran en las “Herramientas Administrativas”, y entre las más importantes están:

Administración de equipos: administra y configura opciones básicas del controlador de dominio como usuarios y grupos locales, espacio de almacenamiento, servicios y aplicaciones, y muchas otras herramientas (programador de tareas, visor de eventos, carpetas compartidas, administrador de dispositivos...). Esta herramienta también existe sin tener DA instalado, pero con menos funcionalidad.

DNS: permite administrar el servicio DNS, que sirve para asociar nombres de equipo o host con direcciones IP.

Dominios y confianzas de Active Directory: permite gestionar las “relaciones de confianza” entre dominios. Las relaciones de confianza se establecen cuando en una organización existen dos o más árboles diferentes y separados, y deseamos unificar la administración de toda la organización desde cualquiera de los controladores de dominio existentes en cualquiera de los árboles.

Usuarios y equipos de Active Directory: permite administrar usuarios y grupos globales, y equipos del dominio. Aquí no se manejan objetos locales como en la herramienta “Administración de equipos”.

Recordemos que cuando creamos un dominio, prácticamente desaparecen los usuarios locales (quedan para usarse cuando una máquina salga del dominio), ya que todas las cuentas pasan a ser globales.

Alternativas a Active Directory:

LDAP, la alternativa a Directorio Activo de Microsoft: LDAP (“*Lightweight Directory Access Protocol*”, «Protocolo Ligero de Acceso a Directorios») es un protocolo de tipo cliente-servidor para acceder a un servicio de directorio. Es gratuito y se puede usar tanto en Windows Server como en Linux Server.

Cuando se trata de utilizar un directorio para empresas medianas, a menudo se recurre al protocolo ligero LDAP.

En la nube: Azure Active **Directory** Domain Services (abreviado a **Azure** AD DS) es una herramienta que proporciona servicios de dominio administrados como, por ejemplo, unión a un dominio, directiva de grupo, LDAP o autenticación Kerberos/NTLM, que son totalmente compatibles con Windows Server Active **Directory.**