

3. Active directory

Convertir en servidor de red

Hasta el momento, y tras la instalación de Windows Server, lo único que hemos hecho ha sido identificar al equipo en una red asignándole:

- Un nombre
- Una dirección IP
- Un grupo de trabajo

De esta forma y por el momento nuestro equipo, salvando las diferencias, es como un equipo más de la red.

Hasta ahora, a pesar de poder ofrecer más servicios, no le hemos instalado ningún rol ni característica que lo diferencie del resto.

Funcionalidades necesarias

Es ahora el momento de hacer que este SO se convierta en un servidor de red, con funcionalidad para:

- Autenticación de usuarios
- Gestionar de forma centralizada los recursos de la infraestructura de red.

La forma más eficiente de realizar todo es mediante la creación de los llamados **dominios**.

En estos dominios se almacena de forma centralizada (facilitando así la labor del administrador)

- información administrativa (cuentas de usuarios, impresoras, directorios, etc.
- Información de seguridad, facilitando así la labor del administrador.

Active directory

WS utiliza el concepto de Directorio Activo (**Active Directory**) como almacén de datos (objetos).

El DA es un servicio de red que

- Guarda en una **base de datos** toda la información sobre los recursos de la red
- Permite el acceso de los usuarios a dichos recursos y a determinadas aplicaciones.

Active directory:

- Permite que los usuarios tengan un único inicio de sesión independientemente del ordenador en el que se sienten.
- A partir de iniciar sesión en el servidor podrán acceder a los recursos de red a los que cada uno de ellos esté autorizado.
- Hay que tener en cuenta que recursos de red pueden ser carpetas y archivos, equipos, los servicios del directorio, etc.

Se convierte en un modelo para organizar, controlar y administrar de forma centralizada el acceso a los recursos de la red.

Controladores de dominio

- Cuando instalemos un DA en uno o varios equipos Windows Server de nuestra red, convertimos a dichos equipos en **controladores de dominio** (Domain Controllers).
- El resto de los equipos de la red que no sean servidores pueden actuar como **clientes** del controlador de dominio y, por lo tanto, del dominio.
- Incluso pueden actuar como clientes los servidores que no se hayan convertido en controladores de dominio.
- Los clientes del dominio tienen acceso a la información almacenada en los controladores de dominio (cuentas de usuario, grupo, equipo, etc.).

El DA es una herramienta fundamental de administración de la infraestructura informática de una empresa u organización con dominio.

Requisitos para montar active directory

- Que el equipo Windows Server tenga un nombre único en la red representativo de un dominio. 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. Este servidor DNS puede ser el mismo en el que se instale DA, ya que durante el proceso de instalación de DA el SO se encarga de configurarlo adecuadamente de forma automática.
- Tener más de 250 MB de 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.

Ventajas de active directory

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

El DA permite a los administradores:

- Crear políticas a nivel de empresa
- Aplicar actualizaciones a una organización completa
- Desplegar programas en múltiples ordenadores.
- El DA almacena información sobre una organización en una base de datos central.

Conceptos de active directory

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

Dominio.

Estructura fundamental. Permite agrupar todos los objetos que se administran de forma estructural y jerárquica.

Unidad organizativa (UO)

Es la unidad jerárquica inferior al dominio. 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 usuarios)

Objetos.

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

Identificación de un dominio

- Cada dominio de WS queda identificado unívocamente mediante un nombre DNS: mcgrawhill.es.
- Cada equipo WS que forma parte de un dominio tiene un nombre que lo identifica dentro del dominio.
- Este nombre, que será de tipo DNS, también llamado FQDN (Fully Qualified Domain Name)

Constará de dos partes:

- Nombre NetBios del equipo + nombre DNS del dominio.

Por ejemplo, server.mcgrawhill.es. Recordemos que el nombre NetBios del equipo es el nombre que le hemos dado al equipo durante el proceso de instalación o el que se le asignó en las tareas iniciales nada más terminar la instalación del SO

Active directory y DNS

El DA utiliza los nombres y servicios DNS para 3 funciones principales:

Resolución de nombres

Convertir los nombres de host (nombres de equipo) a direcciones IP.

Definición del espacio de nombres

DA utiliza las convenciones de nomenclatura de DNS para asignarles nombre a los dominios.

Búsqueda de los componentes de DA

Para iniciar una sesión de red y utilizar los recursos de DA, el equipo que se conecta al dominio debe encontrar primero un controlador de dominio o servidor de catálogo global para procesar la autenticación de inicio de la sesión o la consulta.

NetBIOS y DNS

Microsoft se desprende de la interfaz NetBios que viene desde los «antiguos sistemas»

La sigue utilizando por razones de compatibilidad.

En la actualidad estructura de dominios de Windows Server se basa en un sistema jerárquico de nombres ampliamente aceptado, probado, normalizado: el espacio de nombres de DNS.

La forma en que Windows Server encuentra los servicios de red es a través del espacio de nombres de DNS y no a través de NetBios.