

2

Unidad

Controladores de dominios en redes Windows



Y estudiaremos:

- Las características que identifican a los sistemas en red, como Windows Server.
- El procedimiento para iniciar y detener sesión en un equipo con Windows Server.
- El concepto de dominio, así como características y estructura del mismo.
- El procedimiento para instalar y desinstalar controladores de dominio.
- Los objetos y herramientas de administración que se utilizan en los controladores de dominio.

En esta unidad aprenderemos a:

- Manejar Windows Server y sus diferentes versiones.
- Iniciar y detener el equipo Windows Server.
- Familiarizarte con el concepto de dominio y conocer algunas de sus características.
- Entender la estructura física de un dominio.
- Instalar y desinstalar un controlador de dominio.
- Identificar los objetos que se manejan en un controlador de dominio.
- Utilizar herramientas de administración de un controlador de dominio.

**Web**

Busca en la web las diferentes versiones de Windows Server y compáralas.

**Recuerda**

Al símbolo del sistema podemos acceder pulsando *Iniciar > Ejecutar* e introduciendo dentro del cuadro de texto **cmd** y por último *Aceptar*.

**Vocabulario**

Windows PowerShell. Es un shell de línea de comandos y un lenguaje de scripting basado en tareas especialmente diseñado para la administración del sistema.

**Claves y consejos**

Si al instalar algún tipo de software o hardware el sistema no arranca correctamente, podemos iniciarla en modo seguro de tal forma que podamos deshacer la operación que está causando el problema.

**Actividades**

1. ¿Todas las versiones de Windows pueden trabajar en varias plataformas hardware?
2. ¿Cuál es la característica que determina la portabilidad de estos SO?

1. Un primer contacto con Windows Server

Windows 2008 R2 Server (en adelante Windows Server) es un SO de entorno servidor de los más extendidos en la actualidad. Se trata de 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 ellas son capaces de gestionar dos o más procesadores gracias al modelo de gestión que incorporan, el denominado Multiproceso Simétrico (**SMP**, Symmetric Multi-Processing). Hay distribuciones de Windows Server que se pueden utilizar en cluster (varios equipos funcionan como uno solo).

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

Windows Server se diseñó originalmente para trabajar con arquitecturas Intel, AMD, Alpha, Mips, PowerPC, etc. De ello se deduce la portabilidad del sistema y la gestión de multiplataformas hardware a través de la abstracción del hardware que hace el núcleo del SO.

En cuanto a la interfaz gráfica, Windows Server utiliza las mismas características que las versiones de sobremesa equivalentes, que en el caso de 2008 R2 Server es Windows 7. En general, la interfaz gráfica está basada en Explorer.

En el escritorio de las versiones de Windows Server, al igual que en las versiones de sobremesa, podemos encontrar iconos, ventanas y las diferentes barras y líneas de menús de forma casi idéntica a como se muestran en las versiones de sobremesa.

También se puede interactuar con el SO a través del **intérprete de comandos** de la misma forma que en las versiones de sobremesa. Además, en esta versión de Windows Server se incorpora la interfaz de texto **Windows PowerShell**

1.1. Inicio del sistema Windows Server

Lo primero que debemos tener en cuenta es que un SO servidor no se suele apagar. Normalmente son sistemas que, una vez instalados, se mantienen encendidos ininterrumpidamente, ya que suelen dar servicios a empresas u organizaciones de forma local o remota.

Puntualmente los SO servidores se pueden apagar por necesidades de mantenimiento del hardware o del software, pero en la mayoría de los casos se procura mantenerlos encendidos.

El hecho de que permanezcan encendidos durante semanas, meses o años no es un problema, siempre y cuando estén ubicados en salas informáticas que cumplan los requisitos de seguridad y refrigeración correctos.

Una vez instalado el SO, tal y como se indicó en la unidad anterior, veremos de qué forma podemos iniciar y detener el sistema dependiendo de las necesidades que tengamos en cada momento.

En todas las versiones de Windows Server, a excepción de la versión 2012 (Windows 8 Server), el botón *Iniciar* se encuentra en la parte izquierda de la barra de tareas. Este botón toma diferentes aspectos dependiendo de la versión del SO, pero es prácticamente el mismo que en las versiones Windows XP, Vista y 7. Las versiones de Windows 8 son totalmente diferentes, por lo que en el documento del CEO correspondiente a esta unidad podemos ver sus particularidades.

Si pulsamos el botón de *Iniciar*, podemos acceder a los programas y opciones de configuración de Windows. También podemos apagar el sistema, cerrar la sesión de trabajo, buscar archivos, etc. Recomendamos repasar lo visto en el curso anterior respecto de la interfaz gráfica de Windows 7.

Las opciones habituales que aparecen pulsando el botón *Iniciar*, dependiendo de la versión del SO, son prácticamente las mismas que en las versiones de sobremesa, a excepción de algunas opciones que trataremos con detalle más adelante.

Al igual que en Windows XP, Vista y 7, la forma normal de iniciar el sistema es pulsando el botón de encendido del equipo. Tras pulsar la combinación de teclas **Ctrl+Alt+Supr**, aparecerá la pantalla de **login** y en este caso introducimos el nombre del único usuario que puede iniciar sesión en el equipo, así como su contraseña. Este usuario será el administrador.

Debemos hacer una observación, y es que en caso de trabajar con Windows Server solamente se nos pedirá contraseña, ya que se asume como usuario a la única persona que hasta la fecha existe en el sistema: el administrador.

Si la última vez que utilizamos el equipo lo cerramos correctamente, el equipo se volverá a encender de forma correcta.

Puede ocurrir que a veces el sistema no se cierre de forma adecuada. Algunas de las causas son: un bloqueo del equipo, un corte del fluido de corriente eléctrica, una instalación de software no verificado, un virus, etc.

En este caso nos puede aparecer una pantalla en modo texto con varias opciones que nos permitirá iniciar el sistema de una u otra forma, dependiendo de lo que queramos hacer. Esta misma pantalla en la que se muestran las diferentes formas de iniciar la carga del SO puede obtenerse si durante el proceso de arranque, antes de que aparezca la primera pantalla de carga del SO, pulsamos repetidamente la tecla **F8**. Veamos estas opciones en la Tabla 2.1:

Si iniciamos el equipo con la opción	Conseguiremos
Reparar el equipo	Cargar una pequeña interfaz de trabajo para que, entre otras cosas, se nos permita restaurar una imagen del equipo, además de recuperar puntos de restauración.
Modo seguro	Iniciar el SO utilizando el conjunto mínimo de controladores de dispositivos y servicios necesarios para iniciar Windows.
Modo seguro con funciones de red	Iniciar el SO utilizando el conjunto mínimo de controladores de dispositivos y servicios necesarios para iniciar Windows, además de los controladores que necesita para cargar las funciones de red.
Modo seguro con símbolo del sistema	Iniciar el SO con una consola de trabajo en entorno texto: <i>Cmd.exe</i> .
Habilitar el registro de arranque	Generar un fichero de registro de la secuencia de carga de los controladores del SO cuando el equipo se inicia con cualquiera de las opciones de modo seguro, excepto <i>La última configuración buena conocida</i> . El texto del registro de inicio se guarda en el archivo <i>Ntbtlog.txt</i> en la carpeta <i>%SystemRoot%</i> .
Habilitar vídeo de baja resolución (640x480)	Iniciar el SO habilitando el modo de resolución más baja. Es como <i>Habilitar modo VGA</i> normal.
La última configuración buena conocida	Iniciar Windows utilizando todo lo que se cargó la última vez, ya que el equipo entonces se inició y cerró correctamente.
Modo de restauración de servicios de directorio	Iniciar el SO en modo de recuperación para controladores de dominio basados en Windows. Este modo realiza una reparación del servicio de directorio.
Modo de depuración	Iniciar el SO en modo de depuración en Windows decidiendo qué controladores se cargan y cuáles no.
Deshabilitar el reinicio automático en caso de error del sistema	Que Windows no se reinicie automáticamente en caso de que haya un error. Seleccionaremos esta opción únicamente en caso de que Windows quede atrapado en un bucle en el que el sistema genere un error, intente reiniciarse y vuelva a generar el error reiteradamente.
Deshabilitar el uso obligatorio de controladores firmados	Que se carguen los controladores exclusivos de los fabricantes de hardware. De esta forma se pueden utilizar controladores genéricos para evitar posibles errores de compatibilidad con los controladores firmados u originales.
Iniciar Windows normalmente	Iniciar Windows en su modo normal.

Tabla 2.1. Opciones de carga del SO.



Actividades

3. ¿Se puede iniciar Windows Server en modo seguro?
4. Si suspendemos el equipo y se corta el suministro de corriente eléctrica, ¿qué ocurre en el sistema?



Importante

Estos SO tienen en ejecución una serie de servicios y procesos que si dejan de estar disponibles en la red pueden provocar que el resto de equipos clientes o servidores dejen de funcionar correctamente. Esta es la razón por la que en dichos casos se considera que el apagado o reinicio del equipo es una operación sobre la que hay que actuar con cautela.



Recuerda

Si suspendemos el sistema, debemos asegurarnos de que el equipo tenga siempre suministro eléctrico, ya que de otra forma, toda la información de la sesión como archivos abiertos procesos, desaparecerá.

1.2. Apagado del sistema Windows Server

Cada vez que vamos a apagar el equipo se mostrará una pantalla en la que tenemos que indicar si se ha planeado o no el apagado y seleccionar además por qué apagamos el equipo, añadiendo por último una breve descripción de por qué estamos realizando tal acción (Fig. 2.1).

Es importante tener en cuenta que si por cualquier circunstancia el equipo se apaga inesperadamente, en el siguiente inicio de sesión y una vez cargado el SO se mostrará una pantalla denominada *Rastreador de eventos de apagado* (Fig. 2.2). En ella tenemos que anotar las causas que creemos que han provocado el apagón inesperado del equipo.

La mayor diferencia respecto de las versiones Windows de sobremesa es que ahora, al apagar el sistema, se nos solicita información de la causa del apagado o reinicio del equipo, puesto que, como hemos explicado, es poco habitual que un SO servidor se apague.



Fig. 2.1. Opciones de apagado.

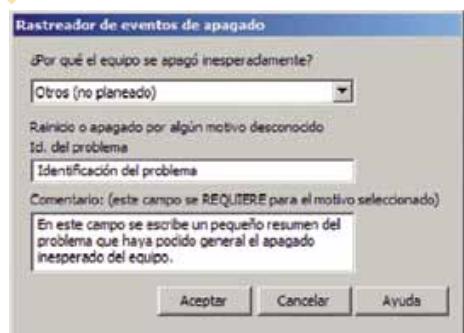


Fig. 2.2. Rastreador de eventos de apagado.



Caso práctico 1

Instalar VMware Tools e iniciar y apagar el Sistema Windows Server analizando las opciones y anotando lo que ocurre en cada una de las posibles situaciones

1. Iniciamos el sistema de forma normal, sin pulsar la tecla **F8** durante el inicio del mismo. Tras pulsar la combinación de teclas **Ctrl+Alt+Supr** y cuando aparezca la pantalla de **login**, introducimos el nombre de usuario y contraseña con los que realizamos la instalación del equipo: el administrador.
2. Realizamos la instalación de VMware Tools, tal y como se puede ver en el documento del CEO correspondiente a esta unidad. Una vez instaladas, se mostrará un mensaje emergente en el que se nos indica si queremos o no reiniciar el equipo. Indicaremos que no.
3. Una vez iniciado el equipo y terminada la instalación de VMware Tools, pulsamos en el botón *Inicio* y en el

ícono . Elegimos la opción *Reiniciar*, tal y como se muestra en la pantalla de la Figura 2.1. En esta pantalla seleccionamos la opción *Sistema operativo: reconfiguración (planeada)* que se muestra en la caja de texto *Opción*. Añadimos un comentario indicando lo que hemos hecho y pulsamos *Aceptar*.

4. Una vez reiniciado el equipo, lo apagaremos bruscamente. Analizaremos lo que sucede cuando iniciamos sesión de nuevo.
5. Para terminar, reiniciamos el equipo siguiendo la misma secuencia que hemos explicado, pero al iniciarlo lo haremos en *Modo seguro* para analizar la diferencia. Por último, reiniciamos el equipo y lo iniciamos normalmente.

El resto de opciones de apagado se gestionan igual que en los sistemas de sobremesa.

● 2. Servicio de directorio y dominio

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 y un grupo de trabajo.

De esta forma y por el momento nuestro equipo 2008 R2 Server, 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 **características** que lo diferencie del resto. Veamos el esquema de la Figura 2.3.

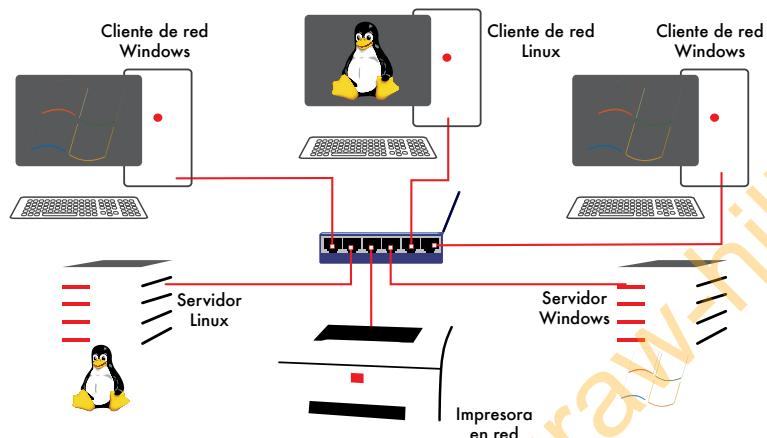


Fig. 2.3. Esquema de red sin servidor.

Es ahora el momento de hacer que este SO se convierta en un servidor de red, con funcionalidad para loguear usuarios y poder gestionar de forma centralizada los recursos de la infraestructura de red.

Normalmente los administradores de redes tienen claro que la forma más eficiente de aprovechar el potencial de los equipos con Windows Server es mediante la creación de los llamados **dominios**. En estos dominios se almacena de forma centralizada información administrativa (cuentas de usuarios, impresoras, directorios, etc.) y de seguridad, facilitando así la labor del administrador. Windows Server utiliza el concepto de **Directorio Activo (AD, Active Directory)** como almacén de datos (objetos) para implementar este tipo de configuración.

El Directorio Activo, de ahora en adelante **DA**, es el **servicio de directorio** de una red con Windows 2000, 2003, 2008, 2008 R2 o 2012 Server.

El DA es un servicio de red 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 se convierte en un modelo para organizar, controlar y administrar de forma centralizada el acceso a los recursos de la red.

Como veremos más adelante, cuando instalamos un DA en uno o varios equipos Windows Server de nuestra red, convertimos a dichos equipos en servidores o, más correctamente, en los denominados **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, por lo tanto, una herramienta fundamental de administración de toda la infraestructura informática de una empresa u organización con dominio.



Vocabulario

Directorio Activo o Active Directory. Es el servicio de directorio de una red con Windows 2000, 2003, 2008, 2008 R2 o 2012 Server. Determina la utilización de recursos de red de forma centralizada.

Dominio. Es una agrupación de equipos y usuarios que facilita la administración de los equipos y cuentas de usuario.



Actividades

5. ¿Es lo mismo un dominio que el Directorio Activo o Active Directory?
6. ¿Un grupo se considera unidad organizativa?



Claves y consejos

AD DS (Servicios de dominio de Active Directory) proporciona una base de datos distribuida que almacena y administra información acerca de los recursos de red y datos específicos de algunas aplicaciones.

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 o desplegar programas en múltiples ordenadores. En general, el DA almacena información sobre una organización en una base de datos central.

La estructura de un DA (Fig. 2.4) 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 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.** Forman una representación de un recurso de red, como pueden ser usuarios, impresoras, ordenadores, unidades de almacenamiento, etc.

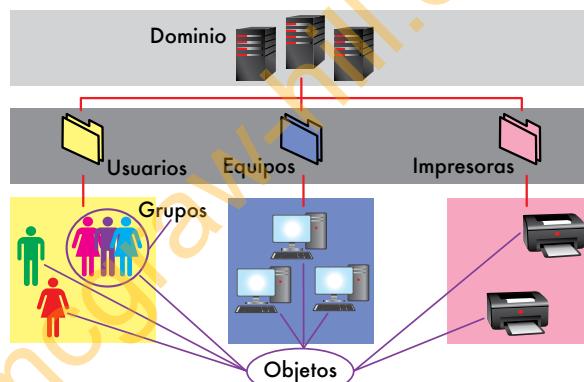


Fig. 2.4. Estructura de DA.

2.1. El Directorio Activo de Windows Server

Importante

Los dominios de Windows Server utilizan los nombres DNS para identificar a los equipos en la red. El nombre DNS siempre estará representado por un sufijo (.com, .es, .org, etc.) y el nombre propio del dominio.

Cada dominio de Windows Server queda identificado únicamente mediante un nombre **DNS**, tal y como nos muestra la Figura 2.5: mcgrawhill.es.

Cada equipo Windows Server 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 y 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.

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

1. **Resolución de nombres:** DNS permite realizar la resolución de nombres al convertir los nombres de host (nombres de equipo) a direcciones IP.
2. **Definición del espacio de nombres:** el DA utiliza las convenciones de nomenclatura de DNS para asignarles nombre a los dominios.
3. **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.

Recuerda

Cuando instalamos el primer controlador de dominio en un equipo con Windows Server, estamos declarando la raíz del dominio, el árbol y el bosque del nuevo dominio.

La terminología utilizada en un DA cambia radicalmente respecto de las versiones de NT 4.0 Server, denominación que determinó en su momento la estructura de dominios de redes Microsoft. Algunos términos de los utilizados habitualmente en DA son los siguientes:

1. **Espacio de nombres.** Directorio Activo usa las convenciones de nomenclatura de DNS para asignar nombre a los dominios. Los nombres de dominio pueden o están formados por dos o más palabras separadas por puntos gracias a una estructura jerárquica denominada **espacio de nombres** (Name space) y ciertas reglas. Sirvan como ejemplo los nombres que aparecen en la Figura 2.5.
2. **Resolución de nombres.** Domain Name Server o **DNS** permite realizar la resolución de nombres al convertir los nombres de hosts a direcciones IP y viceversa.
3. **Controlador de dominio.** Servidor Windows Server con DA instalado. En el equipo se almacena, mantiene y gestiona la base de datos de usuarios y recursos de la red.
4. **Nombre de dominio.** Son las denominaciones asignadas a los ordenadores de la red. En nuestro caso llamaremos a nuestro dominio mcgrawhill.es, que será el dominio raíz.
5. **Árbol de dominio.** Es el conjunto de dominios formado por el nombre de dominio raíz mcgrawhill.es y el resto de dominios cuyos nombres constituyen un espacio contiguo con el nombre raíz. Véanse en la Figura 2.5 los diferentes nombres del árbol de dominios, como compras.mcgrawhill.es o ventas.mcgrawhill.es.
6. **Bosque de árboles de dominios.** Es el conjunto de árboles de dominio.



Actividades

7. Pon un ejemplo de un nombre completo de dominio.
8. ¿Es lo mismo un bosque que un árbol?



Recuerda

La funcionalidad de un servicio de directorio es que «permite organizar, administrar y controlar desde un punto los recursos de red».

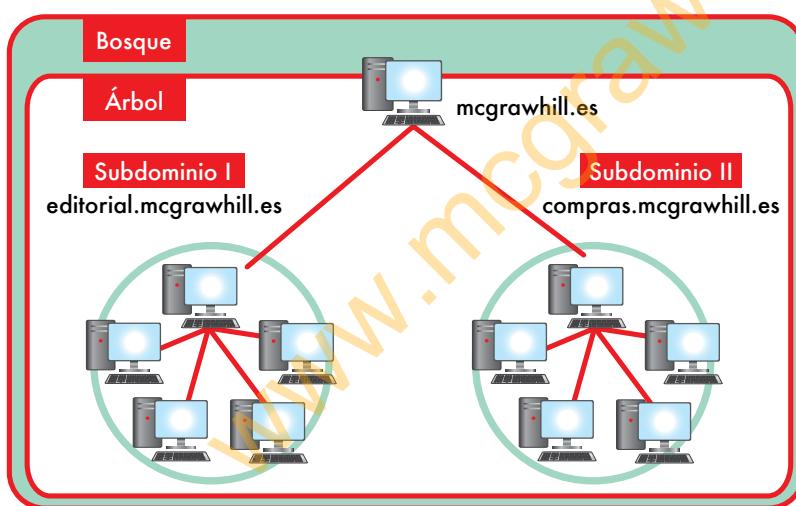


Fig. 2.5. Estructura jerárquica de dominios. Árbol único en el bosque.

● 2.2. Estructura física de un dominio en Windows Server. Requisitos

La apuesta fundamental de Microsoft fue desprenderte de la interfaz NetBios que viene desde los «antiguos sistemas», aunque la sigue utilizando por razones de compatibilidad. En la actualidad, la 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.

DA permite que los usuarios tengan un único inicio de sesión independientemente del ordenador en el que se sienten. A partir de loguearse al 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.



Importante

La menor unidad constructiva para poder utilizar **DA** es el dominio, que podemos definir como un «conjunto arbitrario de recursos de red bajo una administración común».

Para crear un dominio en primer lugar deberemos tener instalada cualquier versión del SO Windows Server en el equipo. El resto de requisitos son:

- 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.

Recordemos que Windows Server recién instalado no es en sí mismo un servidor de casi nada. Tendremos que añadir roles para hacer que el equipo vaya desempeñando en la empresa el papel deseado. Recordemos que en la instalación prácticamente no hicimos nada especial, salvo indicar el nombre de equipo, el número de conexiones concurrentes y poco más.

● 2.3. Especificaciones de dominio en Windows Server

En primer lugar, y siempre 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.** En este caso, tendremos un ordenador principal, que controle todo el sistema, teniendo o no dominios hijos delegados o subdominios (Figura 2.5). El dominio principal siempre tendrá un nombre similar a dominioprincipal.com, por ejemplo, y el resto de dominios hijos, si es que los tenemos, tendrán denominaciones similares a subdominio1.dominioprincipal.com, subdominio2.dominioprincipal.com, etc.
- **Necesitamos más de un dominio.** Este caso es similar al anterior, con la única diferencia de que contaremos con dos controladores principales de dominio, como por ejemplo, dominioprincipal1.com y dominioprincipal2.com, con sus correspondientes subdominios y controladores adicionales. Como se puede apreciar en la Figura 2.6, tenemos dos dominios independientes, cada uno con su estructura jerárquica.

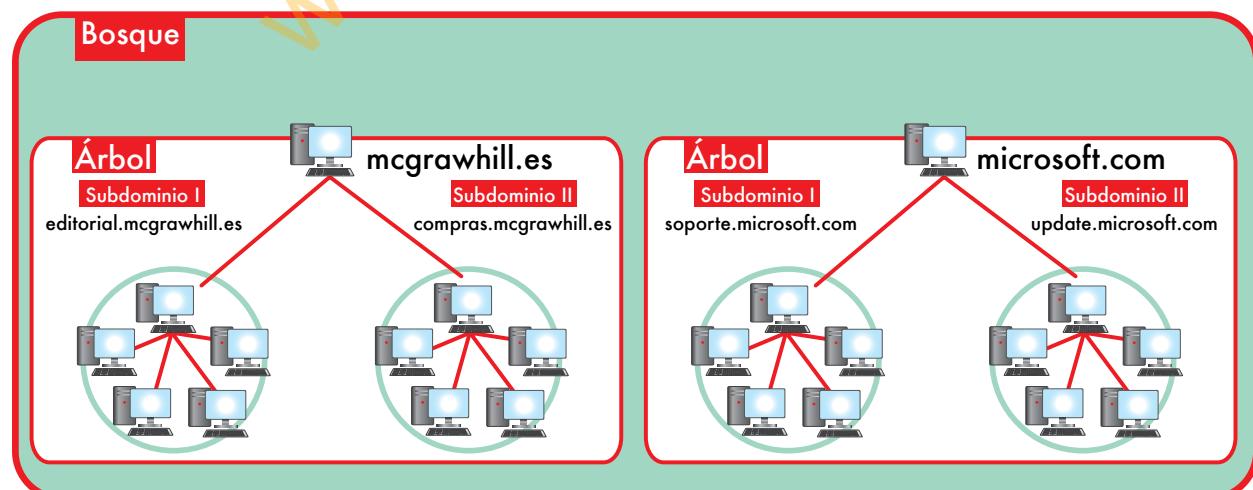


Fig. 2.6. Árboles de dominios en el mismo bosque.

Como podemos apreciar en la Figura 2.6, la estructura jerárquica de dominios se crea «de arriba hacia abajo», es decir, primero debemos crear el **dominio raíz** del árbol, como por ejemplo, mcgrawhill.es, y posteriormente el resto de subdominios, como editorial.mcgrawhill.es y compras.mcgrawhill.es. Todo en su conjunto forma el bosque.

Cuando se instala el primer controlador de dominio en la organización, se crea lo que se denomina el dominio raíz del bosque, el cual contiene la configuración y el esquema del bosque (compartido por todos los dominios de la organización). Más adelante podemos agregar dominios como subdominios de dicha raíz (**árbol de dominios**) o bien crear otros dominios «hermanos» de la raíz (**bosque de dominios**), debajo del cual podemos crear subdominios, y así sucesivamente.

3. Instalación y desinstalación de DA

Una vez instalado el software del SO en el equipo, tenemos que concederle funcionalidad. Para ello podremos agregar o eliminar características o funciones que hagan que el equipo Windows Server deje de ser un servidor independiente o standalone y se convierta en un verdadero servidor de red.

3.1. Consideraciones previas a la instalación de DA

Para instalar DA en nuestra organización, tenemos que partir de la base de qué es lo que queremos o necesitamos:

- Que donde instalaremos y configuremos DA sea en el único servidor o controlador de dominio de la red.
- Que haya más servidores o controladores de dominio en la red, además del nuestro en el que tengamos instalado DA.
- Para realizar cualquiera de estas dos operaciones, tendremos que saber cómo hemos identificado el ordenador en el que instalaremos DA.
- Tendremos muy en cuenta el nombre del equipo antes de instalar DA.
- Además, tras haber instalado el SO el equipo pertenecerá a un grupo de trabajo, nombre que no tiene mayor importancia si lo que queremos hacer es instalar DA.



Claves y consejos

Si queremos que nuestra red sea «más ligera», podemos añadir controladores de dominio adicionales, de reserva y jerarquizados al controlador principal para que este, como único controlador del dominio, se libere de parte de la carga de trabajo en momentos puntuales.



Caso práctico 2

Revisar la configuración del equipo Windows 2008 R2 Server para instalar DA. Revisar la instalación realizada en el caso práctico de la Unidad 1 y personalizar el escritorio

Como podemos observar, tras el proceso de instalación nuestro equipo Windows Server nos pide que introduzcamos un nombre de usuario y contraseña para poder iniciar sesión. En el caso concreto de Windows 2008 R2 Server, solamente se nos solicitará la contraseña del único usuario que puede iniciar sesión en el sistema: el administrador.

Iniciada la sesión en el equipo, tendremos que realizar determinados ajustes en el mismo antes de proceder a la instalación de DA.

Vamos a suponer que la empresa PEQUE S.A., con la que trabajamos todo el curso anterior, quiere instalar un domi-

nio con un equipo Windows 2008 R2 Server para centralizar toda la administración de su red e infraestructura informática.

La instalación de los equipos Windows 2008 R2 Server ya se realizó en la Unidad 1. El enunciado del Caso práctico 1 decía lo siguiente: «Preparar una máquina virtual para proceder a instalar el SO Windows 2008 R2 Server. Los requisitos hardware mínimos para esta instalación en máquina virtual serán 512 MB de RAM y un disco duro de 40 GB. Seguiremos el manual de VMware que encontrarás en el documento del CEO correspondiente a esta unidad.»

Tras terminar la instalación del SO Windows 2008 R2 Server e iniciar el equipo por primera vez, FAZER S.L. se propone configurar este equipo para posteriormente instalar los servicios de directorio.

(Continúa)



Caso práctico 2

(Continuación)

Haremos configurado los siguientes parámetros desde la ventana de *Tareas de configuración inicial*:

- **Zona horaria:** UTC+01:00) Bruselas, Copenhague, Madrid, París.
- **Funciones de red.** Asignaremos la IP 192.168.1.50+X/24, donde X es el número de equipo en el aula. Como puerta de enlace indicamos la dirección del router o de otro equipo que nos diga el profesor. Como DNS indicamos 127.0.0.1 como preferida. De esta configuración hablaremos un poco más adelante.
- **Nombre del equipo.** El nombre será SERVERXXR2, donde XX es el número del equipo en el aula (01, 02..., 15).
- **Actualizaciones automáticas.** Pulsamos en *Cambiar Configuración de la zona adecuada* y seleccionamos la opción *Descargar actualizaciones, pero permitirme elegir si deseo instalarlas*.
- **El resto de opciones las iremos configurando más adelante.**

Esto mismo podemos hacerlo por otro camino, que es el habitual. Veamos cómo:

1. Identificación de red del equipo.

- Haremos clic con el botón derecho del ratón en el ícono de Red > Propiedades o en Inicio > Red > Propiedades.
- En el ícono que representa el adaptador del área de notificación, botón derecho Abrir el centro de redes y recursos compartidos o en el panel de control con vista de ícono hacemos clic en Centro de redes y recursos.
- En cualquiera de los cuatro casos anteriores llegamos a la misma pantalla, en la que se muestra información de red del equipo Server.
- Haremos clic en Cambiar la configuración del adaptador.
- Se muestran las conexiones de red. Elegimos la nuestra y con el botón derecho del ratón seleccionamos Propiedades > Protocolo de Internet versión [TCP/IP 4] > Propiedades.
- Introducimos los datos de identificación de red del equipo.

2. Identificación del equipo. Para configurar esta opción iremos a:

- Inicio > Equipo > Propiedades > Cambiar configuración o
- Inicio > Panel de control > Sistema > Cambiar configuración.
- Hacemos clic en la pestaña Nombre de equipo y pulsamos en el botón Cambiar.
- En el cuadro de diálogo que aparece, en la caja de texto Nombre de equipo, introducimos la identificación propuesta en el ejercicio. También podemos comprobar que por defecto nuestro equipo se encuentra en el grupo de trabajo WORKGROUP, lo que no nos tiene que preocupar por ahora.

3. Credenciales del administrador de red. Es totalmente necesario que el administrador de este equipo tenga una contraseña determinada que cumpla los requisitos de seguridad (ocho caracteres con mayúsculas, minúsculas y números). Esta contraseña será la misma posteriormente para los administradores locales de cada equipo cliente y que integraremos en el dominio. Para gestionar la contraseña del usuario Administrador, iremos a:

- Inicio > Herramientas Administrativas > Administración de equipos o
- Inicio > Equipo > Administrar o
- Inicio > Panel de control > Herramientas administrativas > Administración de equipos.
- En la pantalla que aparezca seleccionamos el grupo Usuarios y grupos locales y la unidad organizativa Usuarios, y con el botón derecho del ratón sobre el usuario Administrador seleccionamos Establecer contraseña.
- Asignaremos una contraseña, por ejemplo, 1234Abcd o algo similar.

Terminada la configuración, reiniciamos cada uno de los equipos del aula. Exploramos la red de forma similar a como lo hacíamos en XP/7 y comprobamos que todos los equipos aparecen en pantalla. Si alguno no aparece, comprobamos las credenciales de red o la configuración de VMware para la red.

3.2. Instalación de Servicios de dominio de DA

En este epígrafe vamos a ver el proceso a seguir para instalar los servicios de directorio en un controlador principal de dominio en una red en la que solamente habrá un servidor Windows 2008 R2 Server, el cual tiene instalados todos los servicios necesarios para nuestra organización.



Caso práctico 3

Configurar el equipo Windows 2008 R2 Server como un controlador de dominio

Ya sabemos que la empresa PEQUE S.A., asesorada por FAZER S.L., desea montar una infraestructura de dominio único para toda su infraestructura.

Se realizará en primer lugar el procedimiento de instalación de los Servicios de dominio de Active Directory en el equipo con Windows 2008 R2.

En primer lugar, para empezar a trabajar de forma sencilla, marcamos la casilla de verificación que deshabilita la pantalla de *Tareas de configuración inicial* para que no se muestre cada vez que se enciende el equipo.

Realmente lo que vamos a hacer a continuación es darle un «rol» al equipo Windows 2008 R2 Server. En concreto este «rol» es el de controlador de dominio, y para ello tenemos que instalar los servicios de directorio o, lo que es lo mismo, instalar y configurar el Directorio Activo (DA) en el equipo recién instalado.

Esta operación puede hacerse desde *Inicio > Herramientas Administrativas > Administrador del Servidor* o desde *Inicio > Panel de control > Herramientas Administrativas > Administrador del Servidor*.

Se mostrará una consola llamada *Administrador del Servidor*, que nos permitirá otorgar el rol deseado al equipo; es decir, nos permitirá instalar los servicios de directorio en el equipo Windows 2008 R2 Server.

Procedemos de forma similar a como lo hicimos instalando las características, pero en este caso lo que instalamos será un nuevo rol. En concreto ahora, en la raíz de la consola *Administrador del Servidor* haremos clic en *Agregar roles*.

En el *Asistente para agregar roles* seguiremos los siguientes pasos:

1. Antes de empezar. Se nos informa de todo lo que previamente tenemos que haber configurado e instalado en el equipo antes de instalar el rol. Verificamos que:

- El administrador tenga una contraseña que cumpla los requisitos de complejidad mínimos.
- Que el equipo tenga asignada una dirección IP fija (no por DHCP con máscara de subred adecuada).
- Que el servidor principal de DNS sea el mismo. En este caso como *Servidor DNS preferido* en la configuración del adaptador pondremos 127.0.0.1.
- Que el equipo tenga instaladas las actualizaciones de seguridad que hayan salido hasta la fecha.
- Pulsaremos *Siguiente*.

2. Seleccionar roles de servidor. Hacemos clic en la casilla de verificación, *Servicios de Dominio de Active Directory*. Pulsamos *Siguiente*. A continuación se nos muestra una pantalla informativa de lo que es este servicio, pero en la que no tenemos que indicar nada. Pulsaremos *Siguiente*.

3. Confirmar selecciones de instalación. Si lo que tenemos en pantalla es lo que deseamos, simplemente pulsamos en *Instalar*.

4. Progreso y resultado. Observamos lo que se está instalando y si la instalación se ha realizado de manera correcta, se nos indicará en la última pantalla. Pulsaremos *Siguiente*.

Realizada esta operación, si nos vamos a la raíz de la consola de *Administrador del Servidor* y pulsamos en *Roles > Servicios de Dominio de Active Directory*, veremos que tenemos instalados los servicios de DA, pero el equipo aún no es un controlador de dominio.

Los servicios que acabamos de instalar no confieren al equipo la funcionalidad de controlador de dominio, pero permiten realizar multitud de configuraciones una vez que el equipo lo sea.

Los **Servicios de dominio de Active Directory (AD DS)**, entre otras cosas:

- Almacenan información acerca de los usuarios, equipos y otros recursos de una red.
- Permiten a los administradores administrar esta información de manera segura.
- Facilitan el uso compartido de los recursos.
- Permiten la colaboración entre usuarios del dominio.

Aunque su instalación no es estrictamente obligada, recomendamos hacerla, especialmente si el equipo forma parte de una red de una organización de tamaño medio.



Actividades

12. Para crear una nueva estructura de dominio, ¿qué pasos tenemos que seguir?
13. ¿Se puede instalar un controlador de dominio adicional a un controlador de dominio principal?
14. ¿Y un controlador de dominio adicional para un bosque?

3.3. Promover el equipo Windows Server a controlador de dominio

Terminado de instalar el AD DS, procedemos a la promoción del equipo a controlador de dominio. Para ello tenemos que comprobar que los requisitos previos expuestos en el punto anterior se siguen cumpliendo. Veamos con un caso práctico cómo se realiza la promoción.

Si operásemos con Sistemas Windows 2000/2003/2008/2012 Server, el procedimiento es prácticamente el mismo. Eso sí, tendremos muy claro lo que es el nivel de funcionalidad, y sobre todo si en nuestra red hay o no más servidores ya instalados, e incluso si posteriormente vamos a realizar ampliaciones de la infraestructura del dominio.



Caso práctico 4

Configurar el equipo Windows 2008 R2 Server como un controlador de dominio

Después de haber instalado AD DS promovemos el equipo a controlador de dominio.

1. Ejecutamos el programa que nos guía en el proceso de promoción del equipo a controlador de dominio. Lo hacemos desde *Inicio > Ejecutar* y tecleamos **dcpromo.exe**.
2. En la primera pantalla que se muestra hacemos clic en *Siguiente* y entonces nos aparecerá una pantalla de advertencia en la que se nos informa de la compatibilidad del SO respecto de la instalación de AD. Pulsamos *Siguiente* y se mostrará entonces la primera pantalla de configuración (Fig. 2.7).

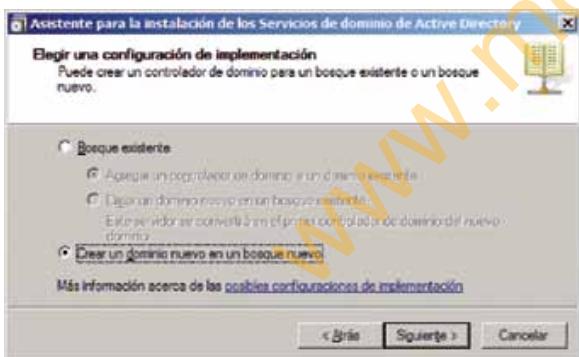


Fig. 2.7. Pantalla inicial de instalación de DA.

3. En esta pantalla, seleccionamos la opción de *Crear un dominio nuevo en un bosque nuevo*. Es lógico si tenemos en cuenta que de momento no disponemos de nada. Lo primero es crear la estructura de dominio raíz, el árbol al que pertenecerá el dominio y el bosque en el que se integrará. Pulsamos *Siguiente*.
4. En la siguiente pantalla que aparece, como la de la Figura 2.8, tenemos que introducir el nombre completo de nuestro dominio raíz, que es el primero del bosque.

Asimismo, el nombre que indiquemos será el nombre del bosque, que determinará el **espacio de nombres** para la gestión que realicemos desde este momento con el dominio. Este nombre completo tiene que ser un nombre DNS con sufijo incluido

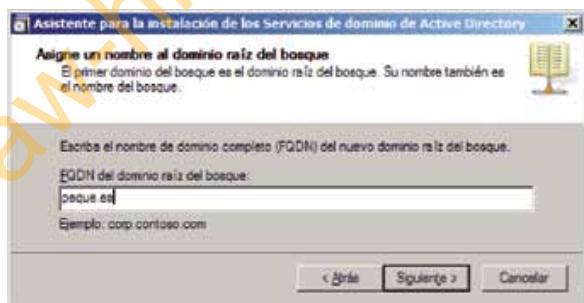


Fig. 2.8. Identificación del dominio.

5. Introducimos, en nuestro caso, el nombre **peque.es**. Pulsamos *Siguiente*.
6. Tras comprobar el nombre, en la siguiente pantalla se nos solicita el *Nivel funcional del bosque*. Aquí introducimos de qué forma vamos a integrar nuestro dominio con otros dominios de la red. Seleccionaremos Windows 2000/2003/2008 Server, dependiendo del equipo servidor que tenga instalado DA de menor rango en esta categoría de sistemas.

Si, por ejemplo, la empresa PEQUE ya tuviera un equipo con DA en un dominio con Windows 2000 Server y otro con Windows 2003 Server, tendríamos que elegir Windows 2000 como nivel de funcionalidad. Es decir, siempre se selecciona como nivel de funcionalidad el del equipo de menor rango en esta escala, siendo 2000 el mínimo y 2008 el máximo, independientemente del tipo de dominio del resto de equipos de la red.

En nuestro caso, aunque solamente vamos a contar con dominio maestro único con Windows 2008 Server,

(Continúa)



Caso práctico 4

(Continuación)

seleccionamos el nivel de funcionalidad de Windows 2008. Elegimos este nivel, ya que puede ser que contemos con dominios de otras versiones anteriores a 2008 Server. En realidad, a efectos de configuración, notaremos pocos cambios. Sin embargo, esto sí que afecta al **catálogo global** o base de datos que se genera con DA, ya que el SO, sin que nosotros tengamos que hacer nada, amplía la funcionalidad a todas las versiones de Server.

Cada nivel de funcionalidad superior incluye características de los niveles anteriores además de otras nuevas. Por esta razón al seleccionar el nivel de funcionalidad de Windows 2008 seleccionamos *Nivel de funcionalidad Windows 2008 R2 Server* y pulsamos *Siguiente*.

- En la nueva pantalla que aparece, tenemos que marcar la casilla *Servidor DNS* como opciones adicionales a instalar en el dominio. Si no marcamos esta casilla, no se realizará la resolución de nombres, es decir, no se podrán asociar los nombres de los equipos con sus direcciones IP y, por lo tanto, no podremos unir clientes al dominio.

Puede que aparezca una pantalla de advertencia indicando un mensaje muy extenso. Esto simplemente es una advertencia que nos dice que si queremos hacer que este equipo forme parte de una infraestructura Server ya establecida, tenemos que configurar el servicio de DNS, de tal forma que se delegue este servicio en el equipo que ya se configuró como servidor principal. En nuestro caso, como lo que estamos haciendo es instalar el primer y único controlador de dominio de la red, no tendremos que hacer nada. Pulsamos *Sí*.

Puede ocurrir que al pulsar *Siguiente* aparezca una pantalla como la de la Figura 2.9.

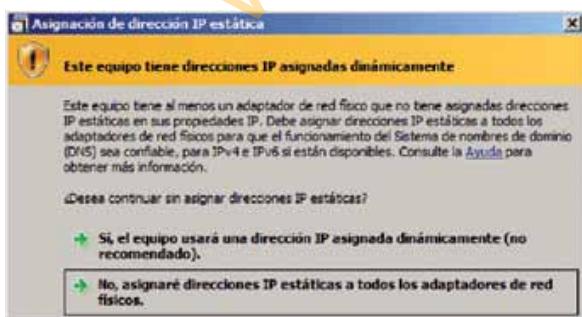


Fig. 2.9. Dirección IP estática.

Si aparece esta pantalla, es debido a que la dirección IP de nuestro adaptador de red no está bien con-

figurada o simplemente no lo está. Seleccionamos la segunda opción: *No, asignaré direcciones IP estáticas a todos los adaptadores de red físicos*. También puede ocurrir que no hayamos desmarcado la casilla de TCP/IP versión 6 en la configuración del adaptador de red, de tal forma que el equipo nos solicite una IP para este tipo de conexión. Si es así, desmarcaremos esta casilla de las propiedades del adaptador de red.

- En la nueva pantalla que aparece, como la de la Figura 2.10, indicamos la ubicación de los archivos que conforman la base de datos con la que trabajará DA. Podemos modificar el destino de estos archivos, pero no su nombre. Eso sí, es estrictamente necesario que el destino de estos archivos sea una carpeta local en una partición o disco con sistema de archivos **NTFS**. Normalmente dejaremos la ubicación por defecto.
- Al pulsar *Siguiente* se muestra la pantalla en la que se nos solicita la contraseña que se requerirá para la administración de determinados componentes de DA. Introducimos la contraseña deseada y pulsamos *Siguiente*.

Recomendamos introducir la misma contraseña que tiene el usuario *Administrador* del equipo para evitar algunos problemas de acceso que se puedan producir por no coincidir las contraseñas.

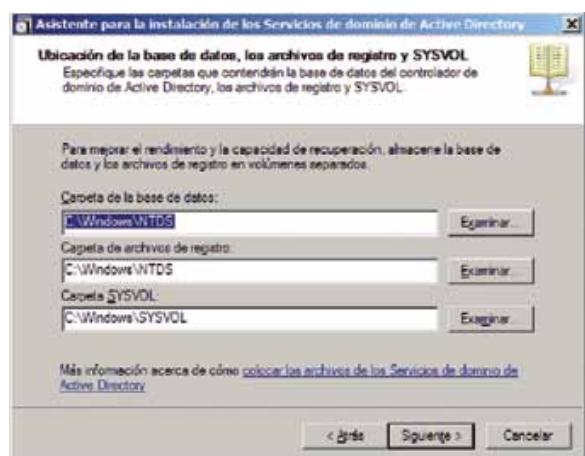


Fig. 2.10. Ubicación de archivos de base de datos de DA.

- Pulsamos *Siguiente* y aparece una pantalla resumen con lo que vamos a realizar. Pulsamos de nuevo *Siguiente* y comienza el periodo de promoción a controlador de dominio de nuestro equipo. Podemos seguir

(Continúa)



Caso práctico 4

(Continuación)



Fig. 2.11. Finalización de promoción de DA.

este proceso, que tardará más o menos tiempo, a través de la información que se va mostrando en la pantalla similar a la de la Figura 2.11.

Pasados algunos minutos, a veces bastante y dependiendo del hardware de nuestro equipo, terminará el proceso de promoción.

11. Reiniciamos el equipo y ya tenemos preparado nuestro sistema como un controlador de dominio de DA para gestionar de forma centralizada los recursos de red.



Vocabulario

FQDN (Fully Qualified Domain Name). Es un nombre completo que incluye el nombre NetBios del equipo y el nombre DNS del dominio asociado a ese equipo.

3.4. Eliminación de un controlador de dominio

Ya hemos visto cómo se hace para que un equipo con Windows 2008 R2 Server se convierta en controlador de dominio y ejecute los servicios de DA.

Por cualquier circunstancia, podemos querer desinstalar la estructura de dominio de nuestra organización bien para modificarla o simplemente para eliminarla.

Eso sí, si decidimos desinstalar DA de nuestro equipo, perderemos toda la configuración realizada hasta el momento, como cuentas de usuario, grupos, equipos, etc. Es decir, los objetos creados hasta el momento se eliminarán, ya que la base de datos y el catálogo global que almacena toda la información desaparecerán.

Es en este punto donde toma gran importancia el proceso de planificación en la instalación de un dominio con DA, ya que el planificar mal o rápidamente este tipo de infraestructuras, o sin contar con todo el personal de la organización, puede provocar que tarde o temprano el diseño elegido no cubra las necesidades para las que se diseñó, con lo que entonces habrá que proceder a la desinstalación y nueva instalación de la infraestructura con el problema logístico y organizativo que esto conlleva.

Veamos cómo se elimina DA de un controlador de dominio.

Cuando se instaló el dominio, hicimos que un equipo de la infraestructura fuera el que tuviera instalado los servicios de Directorio Activo y, por lo tanto, el único que contiene el denominado **catálogo global**. Este catálogo incluye todos los objetos del dominio: usuarios, equipos, recursos compartidos, impresoras, etc.

Si eliminamos DA teniendo en cuenta esta circunstancia, ocurrirá que se perderá todo el catálogo global, y el equipo en que se instaló DA pasará a ser un servidor independiente o **stand alone**, es decir, el equipo tendrá la misma estructura que inmediatamente después de la instalación del SO.

Si el equipo del que eliminamos DA es un equipo que se añadió como equipo de reserva o equipo de seguridad al dominio, el eliminar DA de este equipo no implica la eliminación del catálogo global, ya que dicho catálogo está replicado en todos los equipos de la red. Solamente al eliminar el último controlador de dominio de la infraestructura, que lógicamente será el primer equipo en el que se instaló DA, se destruye definitivamente la base de datos de objetos de DA.



Caso práctico 5

En primer lugar, eliminar DA del controlador de dominio y hacer que el equipo Windows 2008 R2 Server sea un servidor independiente en el que no se ejecutan los servicios de directorio. Terminaremos el caso práctico volviendo a promover el equipo Windows 2008 R2 Server a controlador de dominio con las mismas credenciales que tenía inicialmente

Lo primero es indicar que una cosa es despromover el dominio y otra eliminar los AD DS (Servicios de dominio de Directorio Activo). Si hacemos que el equipo deje de ser un controlador de dominio, estaremos impidiendo que en él puedan gestionarse (loguearse) fundamentalmente usuarios del dominio. Eliminaremos la base de datos de recursos compartidos, recursos de red, etc.

Si eliminamos además AD DS, estaremos impidiendo que este equipo pueda administrar otros dominios o subdominios de la red de forma sencilla y eficaz.

De forma similar a como realizábamos la promoción llevaremos a cabo la despromoción.

1. Iniciamos sesión como Administrador del equipo y desde *Inicio > Ejecutar* ejecutamos el comando `dcpromo`. Se nos muestra una pantalla de inicio del asistente de configuración de DA. Pulsamos *Siguiente* y aparece la advertencia de la Figura 2.12.



Fig. 2.12. Eliminación de Active Directory.

2. Esta indica que este controlador es un servidor de catálogo global, es decir, que es el controlador principal del dominio y que se utiliza para que los usuarios se validen a él. Este mensaje indica la peligrosidad del proceso.

Como en nuestro caso el controlador es único, en un bosque único, y no existen otros bosques, podremos realizar la operación. Pero si nuestro dominio contase con algún otro bosque, con controladores adicionales de dominio o con subdominios, no podríamos eliminarlo. En este caso tendríamos que ir eliminando los controladores de dominio jerárquicamente de menor a mayor jerarquía.

Teniendo esto claro, pulsamos *Aceptar* y aparece una pantalla como la de la Figura 2.13.

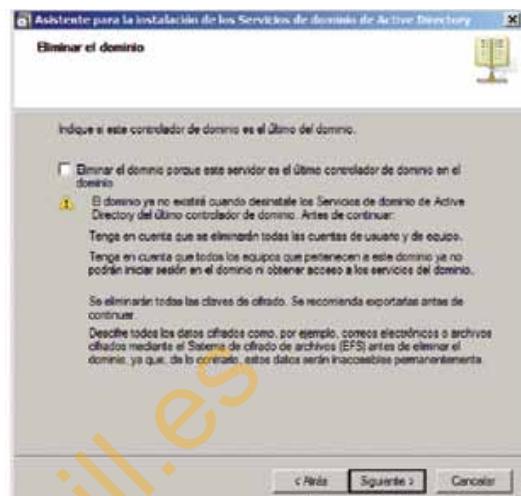


Fig. 2.13. Eliminar el dominio.

3. En esta pantalla se nos indica que marquemos la casilla de verificación, siempre y cuando sea el último controlador del dominio. En nuestro caso, como es el único, evidentemente es el último, pero recordemos que si hubiera otros subdominios o controladores adicionales, no marcaríamos esta casilla para desinstalarlos.
4. Marcada la casilla, pulsamos *Siguiente* y aparece una pantalla dandonos información sobre las particiones en las que se ha replicado la base de datos de DA. Pulsamos *Siguiente* y sale una nueva pantalla en la que indicaremos si queremos eliminar o no toda la información que las particiones de la base de datos contienen. Es conveniente eliminarlas, siempre y cuando, como es nuestro caso, el objetivo sea eliminar completamente los servicios de directorio del equipo Windows Server.
5. Una vez marcada la casilla *Eliminar todas las particiones*, pulsamos en *Siguiente*. Puede ocurrir que a continuación se muestre otra pantalla en la que se nos pregunte si queremos eliminar la configuración del servicio de DNS, que en su momento se configuró para poder utilizar los servicios de directorio.
6. Marcamos la casilla de verificación que indica esta circunstancia y pulsamos *Siguiente*. Si se nos solicita, que es lo normal, introducimos las contraseñas del usuario *Administrador* del equipo que utilizamos para la creación de DA.
7. Pulsamos *Siguiente* en las pantallas posteriores y el proceso de despromoción comienza. Pasados unos minutos, cuando finalice, tendremos que reiniciar el equipo o marcar la casilla *Reiniciar al completar* de la última pantalla que aparece.

Una vez despromovido, lo volveremos a promover a controlador de dominio con las mismas credenciales.



Vocabulario

Objetos en DA. Representan las entidades que pueden administrarse en una red de ordenadores.

4. Gestión de dominios Windows Server

El Directorio Activo, tal como ya hemos visto, es en realidad una base de datos jerárquica de objetos, que representan las entidades que pueden administrarse en una red de ordenadores, en nuestro caso, en un dominio de sistemas Windows 2008 R2 Server.

De esta forma, en general en todas las versiones de Windows Server, la gestión de un dominio puede realizarse de forma centralizada desde cualquier equipo que pertenezca al dominio, ya que solamente es necesario administrar en sí mismo el Directorio Activo. Cuando nos referimos a «administrar», estamos hablando de crear, gestionar y configurar adecuadamente los objetos del directorio que representan a las entidades o recursos que existen en el dominio (recursos como usuarios, grupos, equipos, etc.).

4.1. Objetos que administra un dominio

Veamos cuáles son los objetos que pueden manejarse en un dominio Windows Server y que se muestran en la Figura 2.14.

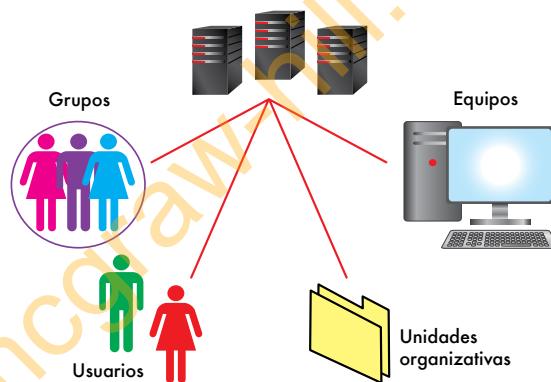


Fig. 2.14. Objetos del Directorio Activo.

A. Usuarios globales

Cuando tenemos instalado un controlador de dominio con Windows Server, se crean en el sistema cuentas de usuario y de grupo globales (users).

Las cuentas y grupos locales del equipo desaparecen, ya que ahora en el controlador de dominio solamente se gestionan cuentas de usuario y grupo globales. Estas cuentas globales sirven para:

- Identificar y autenticar a las personas (usuarios) que podrán acceder al sistema, es decir, loguearse al controlador de dominio.
- Administrar y gestionar los permisos y privilegios que servirán para controlar el acceso que los usuarios hacen a los recursos del sistema.

Supongamos que trabajamos en un grupo de trabajo, es decir, sin dominio. Si una persona (usuario) quiere trabajar en varios equipos, necesita disponer de una cuenta local de usuario dada de alta en cada uno de ellos. Esta cuestión queda solucionada al trabajar en un dominio, ya que el usuario es de dominio y no local, lo cual le proporciona la posibilidad de iniciar sesión en cualquier equipo del dominio.

En un controlador de dominio con Windows Server, se pueden crear cuentas de **usuario global**. El término «global» debe interpretarse como global al dominio. Los datos de una cuenta de usuario global se almacenan en el Directorio Activo y por tanto en su base de datos, y son conocidos por todos los ordenadores del dominio (en realidad, por todos los ordenadores de bosque).

Más adelante veremos de qué forma integramos los equipos clientes en el dominio para que esta funcionalidad se pueda utilizar.

Las cuentas de usuario globales representan una cuenta única de usuario que se puede utilizar desde cualquier ordenador integrado en el dominio. En este caso, cuando una persona se conecta a cualquiera de dichos ordenadores haciendo uso de su cuenta de usuario global, el ordenador en cuestión realiza una consulta al Directorio Activo, que valida las credenciales del usuario, y el resultado de la validación es enviado al ordenador cliente, que concede o rechaza la conexión.

No es incompatible que los equipos que actúan como clientes de un dominio, además de conocer a los usuarios globales del dominio, puedan tener también sus propios usuarios locales. En este caso, dichos usuarios son únicamente visibles en el ordenador en el que han sido creados. Cuando una persona desea entrar en el sistema utilizando una cuenta local, dicha cuenta se valida contra la base de datos local de ese ordenador. A este usuario local jamás se le podrán asignar permisos de acceso a recursos del dominio, puesto que allí no tiene cuenta.

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.

En el controlador de dominio pueden crearse diferentes tipos de grupos de usuarios: grupos de distribución y grupos de seguridad.

La gestión de usuarios y grupos la veremos detenidamente en la siguiente unidad. Ahora solamente nos interesa saber que los grupos son otro tipo de objetos gestionados por DA y que implementan una agrupación de usuarios para conceder o no permisos de utilización de recursos del dominio.

C. Equipos

La misma base de datos del Directorio Activo de un dominio que conserva toda la información relativa a cuentas de usuarios y grupos globales almacena asimismo información relativa a los equipos (computers) que forman parte del dominio.

Se almacena el nombre del ordenador, así como un identificador único y privado que lo identifica únicamente y que solamente conoce el controlador de dominio. Gracias a esta identificación única, a cada equipo (objeto en general) se pueden asignar permisos y derechos. Objetos como usuarios, grupos y equipos quedan identificados cada uno de ellos por un número o identificación en el equipo.

D. Unidades organizativas

Como ya hemos visto, las «unidades organizativas» también son conocidas como UO (Organization Units). Son objetos del directorio que a su vez pueden contener otros objetos. El uso fundamental de las UO es delegar la administración de sus objetos a otros usuarios distintos del administrador del dominio y personalizar el comportamiento de los usuarios y/o equipos mediante la aplicación de directivas.



Recuerda

Los usuarios que se gestionan en DA son usuarios globales, reconocidos por todos los equipos que forman parte de un dominio. Los usuarios locales se gestionan exclusivamente en cada equipo, pertenezcan o no a un dominio.



¿Sabías que...?

Las unidades organizativas son contenedores de Active Directory en los que se pueden colocar usuarios, grupos, equipos y otras unidades organizativas.



Actividades

15. ¿Qué tipos de objetos se manejan normalmente en DA?
16. ¿De qué forma se reconoce cada objeto en el sistema?
17. ¿Qué tipos de usuarios podemos administrar desde la herramienta Administración de equipos?
18. ¿Es necesario configurar el servicio DNS para dar de alta un controlador de dominio en Windows Server?

4.2. Herramientas básicas de administración de dominios

Una vez instalado DA y configurado el controlador de dominio, disponemos de una serie de herramientas para administrar la base de datos, objetos y recursos que serán gestionados por el dominio. Veamos cuáles son estas herramientas:



Caso práctico 6

Utilización e identificación de herramientas para la gestión del Directorio Activo

Para conocer y utilizar las herramientas que sirven para la gestión del DA en un servidor Windows Server, tenemos que ejecutar *Inicio > Panel de control > Herramientas Administrativas*. También podemos ejecutar *Inicio > Herramientas Administrativas* (Fig. 2.15).

1. Administración de equipos. Con esta herramienta administraremos y configuraremos opciones básicas del controlador de dominio. Podemos administrar usuarios y grupos locales, espacio de almacenamiento en disco, recursos compartidos, etc. Como esta herramienta la vamos a utilizar de forma habitual, de momento no haremos un análisis detallado de la misma. Cuando integramos un equipo en un dominio, esta herramienta tiene menos utilidad, ya que entre otras cosas desaparece la gestión de usuarios y grupos locales, puesto que pasan a gestionarse desde una de las opciones que veremos a continuación.

Cuando ejecutamos esta herramienta, vemos una pantalla como la de la Figura 2.16.

Las opciones que se presentan son las siguientes:

- **Herramientas del sistema:**

- *Programador de tareas.* Su funcionamiento es prácticamente el mismo que en Windows Vista/7/8, por lo que repasaremos cómo lo hicimos con esta versión del sistema para proceder de la misma forma en Windows 2008 Server.
- *Visor de eventos.* En esta opción, podemos analizar un histórico de los sucesos que han ocurrido en nuestro sistema, como errores de inicio o cierre del equipo, interrupción de servicios, acceso a recursos del equipo, etc.
- *Carpetas compartidas.* Nos muestra en una sola ventana todos los recursos compartidos desde este equipo. Esta opción es muy interesante, ya que a veces es difícil localizar las carpetas compartidas en todas sus ubicaciones.
- *Rendimiento.* Podemos analizar los recursos consumidos por el equipo en cuanto a CPU, disco, red y memoria. El resto de opciones son objeto de admi-

nistración más avanzada, que en nuestro caso no veremos.

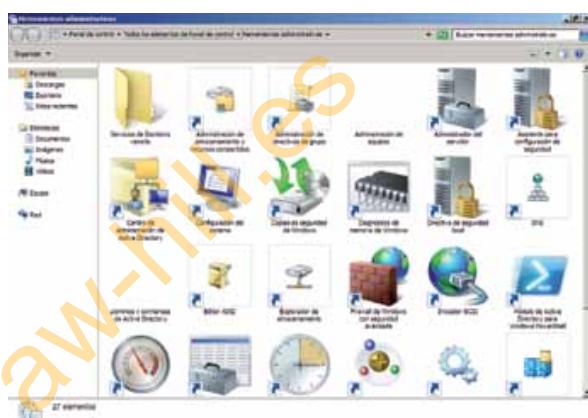


Fig. 2.15. Herramientas administrativas.

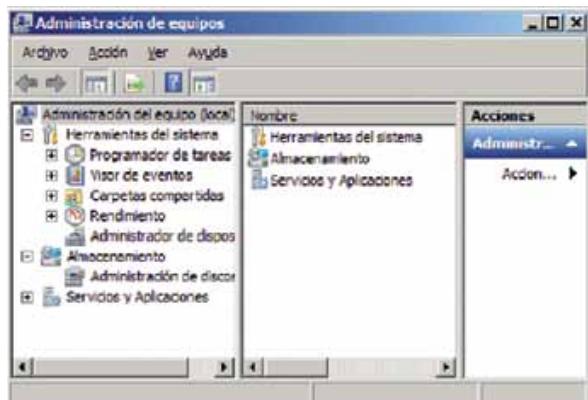


Fig. 2.16. Administración de equipos.

- *Administrador de dispositivos.* Podemos gestionar el hardware de nuestro equipo igual que lo hacíamos en las versiones Windows de sobremesa. Podemos desinstalar o deshabilitar dispositivos, así como ver los recursos que consume o solucionar problemas específicos, como actualización de controladores. El procedimiento es el mismo que en versiones Windows Vista/7/8 o XP.

(Continúa)



Caso práctico 6

(Continuación)

- **Almacenamiento.** Concretamente en *Almacenamiento de disco* podemos gestionar los discos duros y/o volúmenes de nuestro sistema de forma muy similar a como se hacía en las versiones de sobremesa. Este punto lo trataremos más adelante.
- **Servicios y aplicaciones.** Aquí gestionamos precisamente eso, los servicios que se están ejecutando en nuestro equipo. Esta opción también la trataremos más adelante.
- 2. **DNS.** Desde aquí administraremos este servicio, que nos permite asociar nombres de equipo o host con direcciones IP. Durante el proceso de instalación de DA se instala y configura automáticamente este servicio, por lo que de momento no es necesario realizar ninguna operación sobre el mismo.
- 3. **Dominiros y confianzas de Active Directory.** Con esta herramienta podemos configurar algo muy importante: «las relaciones de confianza». Las relaciones de confianza se configuran cuando en una organización existen dos o más dominios diferentes y deseamos unificar la administración de toda la organización desde cualquiera de los controladores de dominio existentes. Con este tipo de relaciones varios dominios se administran como si fueran uno solo.
- 4. **Usuarios y equipos de Active Directory.** Desde esta herramienta podemos administrar usuarios globales, grupos y equipos del dominio, entre otras cosas. A diferencia de la herramienta *Administración de equipos*, que se utiliza para la gestión de usuarios, grupos y recursos locales, con esta otra herramienta se gestionan los objetos del dominio.

Al ejecutar esta herramienta, vemos una pantalla como la de la Figura 2.17.



Fig. 2.17. Usuarios y equipos de Active Directory.

Con esta herramienta podemos manejar la mayoría de los **objetos** que vamos a tratar en este curso. Gestionaremos usuarios, grupos, controladores de dominio, equipos, unidades organizativas, etc.

Como podemos apreciar en la Figura 2.17, está directamente seleccionada la opción de *Users* y podemos apreciar en la parte derecha la lista de usuarios predefinidos que existen en el dominio.

En la siguiente unidad veremos detalladamente la gestión de este tipo de objetos.

El resto de herramientas no las trataremos de momento, pero a lo largo del libro iremos utilizando alguna más.

Respecto de *Usuarios y equipos de Active Directory*, se ha de recordar que es una herramienta que se instala cuando se crea el dominio, algo que se produce cuando instalamos los servicios de DA en el primer equipo de la infraestructura.

Por ello al realizar esta instalación los usuarios locales del equipo en el que hemos instalado DA dejarán de existir inmediatamente; no podremos gestionar usuarios locales.

Ahora los usuarios que se gestionen serán usuarios del dominio, pudiendo identificarse al dominio desde cualquier equipo que añadamos, incluyendo el propio controlador de dominio, que, por cierto, es una operación poco habitual.

Si en nuestra infraestructura tuviéramos más de un controlador de dominio, es decir, si contáramos con un controlador de dominio principal y uno de reserva o de seguridad, la gestión y administración de usuarios equipos, grupos, etc., podrían hacerse desde cualquiera de estos equipos con la herramienta *Usuarios y equipos de Active Directory*, independientemente del servidor desde el que estuviésemos trabajando.

Debemos tener muy presente que los usuarios locales solamente existen en equipos Windows 2008 R2 Server no promovidos a controladores de dominio. Una vez promovidos, los usuarios locales no existen; solamente existen usuarios del domino.