4.1. Introducción

Este capítulo introduce los conceptos fundamentales sobre dominios Windows Server 2008, que permiten unificar y centralizar la administración de conjuntos de sistemas Windows servidores y clientes en organizaciones de cualquier tamaño.

En concreto, se explicarán los denominados Servicios de Dominio del Directorio Activo (*Active Directory Domain Services*), que en conjunto permiten implantar dominios en una organizción, así como la administración de los mismos, incluyendo los principales objetos que pueden definirse en el dominio, la compartición de recursos entre sistemas de la organización y la delegación de tareas administrativas dentro de un dominio.

4.2. El Directorio Activo

4.2.1. Servicios de Dominio del Directorio Activo

Hoy en día, los ordenadores existentes en cualquier organización se encuentran formando parte de redes de ordenadores, de forma que pueden intercambiar información. Desde el punto de vista de la administración de sistemas, la mejor forma de aprovechar esta característica es la creación de un *dominio* de sistemas, en donde la información administrativa y de seguridad se encuentra *centralizada* en uno o varios servidores, facilitando así la labor del administrador. Windows Server 2008 utiliza el concepto de **directorio** para implementar dominios de sistemas Windows, que pueden incluir sistemas servidores (como Windows 2000, Windows Server 2003 o Windows Server 2008) y clientes (como Windows XP, Windows Vista o Windows 7).

En el ámbito de las redes de ordenadores, el concepto de *directorio* (o almacén de datos) se define como una estructura jerárquica que almacena información sobre objetos existentes en la red (o más ampliamente, en la organización). Normalmente, un directorio se implementa mediante una base de datos optimizada para operaciones de lectura, que soporta búsquedas de grandes volúmenes de información y con capacidades de exploración. Existen varios estándares de la industria que especifican cómo debe definirse un servicio de directorio, destacando entre ellos el *Directory Access Protocol*, así como una versión simplificada y más utilizada del mismo, denominada *Lightweight Directory Access Protocol*, o LDAP.

Active Directory Domain Services (AD DS), o Servicios de Dominio del Directorio Activo, es el nombre que recibe el conjunto de elementos que globalmente constituyen el servicio directorio en dominios Windows Server 2008 (por simplificar, en adelante nos referiremos a este servicio como Directorio Activo, tal como se le denominaba en versiones previas de Windows Server). En esencia, este servicio almacena

información acerca de los recursos disponibles en el dominio y permite el acceso controlado de los usuarios y aplicaciones a dichos recursos, de forma que se convierte en un medio de organizar, controlar y *administrar* centralizadamente el acceso a los recursos de la red.

Como veremos, al instalar el Directorio Activo en sistemas Windows Server 2008 de nuestra red, convertimos a dichos sistemas en los servidores del dominio, o más correctamente, en los denominados *Controladores de Dominio* (*Domain Controllers*, o "DCs"). El resto de los equipos de la red pueden convertirse entonces en los clientes de dicho servicio de directorio, también denominados *miembros* del dominio, con lo que pueden consultar toda la información almacenada en los DCs. Como veremos, esta información incluye elementos típicamente centralizados en dominios de muchos tipos de sistemas, como cuentas de usuario, grupo, ordenador, etc., así como otras características propias de sistemas Windows Server, como directivas de usuario o equipo, relaciones de confianza, aspectos sobre la replicación de datos entre servidores, etc. De esta forma, el Directorio Activo se convierte en una herramienta fundamental de administración de toda la organización.

Una de las ventajas fundamentales del Directorio Activo a la hora de administrar dominios es que conceptualmente separa la estructura *lógica* de la organización (dominios) de su estructura *física* (topología de red). Ello permite, por una parte, independizar la estructuración de dominios de la organización de la topología de la red o redes que interconectan los sistemas; y, por otra parte, permite administrar la estructura física explícitamente cuando es necesario, de forma independiente de la administración de los dominios. Más adelante en este capítulo se exponen ambas estructuras detalladamente.

4.2.2. Estándares relacionados

A partir de la versión Windows 2000, Windows Server ha basado la implementación del Directorio Activo, una serie de protocolos y estándares existentes, lo cual ha permitido obtener un servicio de directorio no sólo robusto y escalable, sino también interoperable con otros servicios de directorio. Entre estos estándares, podemos destacar los siguientes:

- DHCP (*Dynamic Host Configuration Protocol*). Protocolo de configuración dinámica de ordenadores, que permite la administración desatendida de características de red.
- DNS (*Domain Name System*). Servicio de nombres de dominio que permite la administración de los nombres de ordenadores. Este servicio constituye el mecanismo de asignación y resolución de nombres (traducción de nombres simbólicos a direcciones IP) en Internet.

- SNTP (*Simple Network Time Protocol*). Protocolo simple de tiempo de red, que permite disponer de un servicio de sincronización de tiempo entre sistemas conectados por red.
- LDAP (*Lightweight Directory Access Protocol*). Protocolo ligero (o compacto) de acceso a directorio. Este es el protocolo mediante el cual las aplicaciones acceden para leer o modificar la información existente en la base de datos del directorio.
- Kerberos V5. Protocolo utilizado para la autenticación de usuarios y máquinas..
- Certificados X.509. Estándar que permite distribuir información a través de la red de una forma segura.

De entre todos ellos, es imprescindible que el administrador conozca en detalle la relación entre el Directorio Activo y DNS. A continuación se exponen los aspectos fundamentales de esta relación.

4.2.3. El Directorio Activo y DNS

Tanto el Directorio Activo como DNS establecen espacios de nombres. Podemos entender un espacio de nombres como un área delimitada en la cual un nombre puede ser resuelto. La resolución de nombres es el proceso de traducción de un nombre en un objeto o información que lo representa. Por ejemplo, el sistema de ficheros NTFS puede ser considerado un espacio de nombres en cual un nombre de fichero puede ser resuelto en el fichero propiamente dicho.

DNS es el sistema de nombres de facto para redes basadas en el protocolo TCP/IP y además, es el servicio de nombres que se usa para localizar ordenadores en Internet. Inclusive sin considerar dominios, Windows Server 2008 utiliza principalmente DNS para localizar a otros ordenadores en la red. A continuación se expone la relación que existe entre DNS y los dominios Windows Server 2008.

Cada dominio Windows Server 2008 se identifica unívocamente mediante un nombre de dominio DNS (por ejemplo, `miempresa.com`). Por otro lado, cada ordenador basado en Windows Server que forma parte de un dominio tiene un nombre DNS cuyo sufijo es precisamente el nombre DNS de dicho dominio (siguiendo con el ejemplo, un ordendor de dicho dominio podría denominarse `pc0100.miempresa.com`). De esta forma, los dominios y ordenadores que se representan como objetos en Active Directory, són también nodos en DNS. Por tanto resulta fácil confundir ambos espacios de nombres, ya que comparten idénticos nombres de dominio. La diferencia es que aunque comparten la misma estructura, almacenan información diferente: DNS almacena zonas y registros de recursos y el Directorio Activo almacena dominios y objetos de dominio.

Como conclusión diremos que Directorio Activo *utiliza* DNS para tres funciones principales:

1. **Resolución de nombres**: DNS es el mecanismo por defecto de resolución de nombres en dominios Windows Server 2008, permitiendo localizar por nombre a los ordenadores de la red (al traducir nombres a direcciones IP).

2. **Definición del espacio de nombres**: el Directorio Activo utiliza las convenciones de nomenclatura de DNS para asignar nombres a los dominios. Es decir, los dominios Windows Server 2008 se nombran necesariamente mediante nombres de dominio DNS.

3. **Búsqueda de los componentes físicos de AD**: para iniciar una sesión de red o realizar consultas al Directorio Activo, los sistemas Windows miembros de un dominio deben encontrar primero a alguno de los DCs del dominio, y para ello realizan consultas DNS. Por tanto, debe existir un servidor DNS disponible que incluya la información necesaria para responder estas consultas. En particular, esta información se almacena en DNS mediante registros de recursos SRV que especifican el servidor (o servidores) del dominio que proporcionan los servicios de directorio correspondientes (LDAP, Kerberos, catálogo global, etc.).

4.2.4. Estructura lógica

La estructura lógica del Directorio Activo se centra en la administración de los *recursos* de la organización, independientemente de la ubicación física de dichos recursos, y de la topología de las redes subyacentes. Como veremos, la estructura lógica de la organización se basa en el concepto de *dominio*, o unidad mínima de directorio, que internamente contiene información sobre los recursos (usuarios, grupos, ordenadores, directivas, etc.) existentes en dicho dominio. Dentro de un dominio es posible subdividir lógicamente el directorio mediante el uso de *unidades organizativas*, que permiten una administración independiente sin la necesidad de crear múltiples dominios. Sin embargo, si la organización necesita estructurarse en varios dominios, también puede hacerlo, mediante los conceptos de *árbol* y *bosque*; ambos son jerarquías de dominios a distintos niveles, en función de si los dominios comparten o no un espacio de nombres común. A continuación se presentan todos estos conceptos de forma más detallada.

4.2.4.1. Dominios

La unidad principal de la estructura lógica del Directorio Activo es el dominio. Un dominio es un conjunto de ordenadores, o equipos, que comparten una base de datos de directorio común. En un dominio tiene que existir uno o varios sistemas Win-

dows Server 2008 que actúen como DCs (es decir, con el rol AD DS instalado), y pueden existir además un número indeterminado de sistemas clientes o miembros del dominio. Como hemos visto, cada dominio se identifica unívocamente por un nombre de dominio DNS, que debe ser el sufijo DNS principal de todos los ordenadores miembros del dominio, incluyendo el o los controladores.

El uso de dominios permite conseguir los siguientes objetivos:

- **Delimitar la seguridad**. Un dominio Windows Server 2008 define un límite de seguridad. Las directivas de seguridad, los derechos administrativos y las listas de control de acceso (*Access Control Lists*, ACLs) no se comparten por defecto entre dominios. Es decir, aunque en una organización pueden existir múltiples dominios interrelacionados, cada uno presenta una configuración de seguridad independiente.

- **Replicar información**. Como veremos más adelante, la información sobre los objetos que existen en un dominio se almacena en una de las *particiones* que contiene la base de datos del directorio (en particular, la denominada partición del dominio). Cada partición constituye lo que se conoce como una unidad de replicación, o conjunto concreto de equipos (DCs) que mantienen una copia idéntica de la partición mediante replicación. Active Directory utiliza un modelo de replicación multimaestro, lo cual significa que cualquier DC admite cambios en la información de su partición, y es capaz de replicarlos luego al resto de DCs que constituyen su unidad de replicación. En particular, la unidad de replicación de la partición de dominio de un dominio concreto está constituida por los DCs de dicho dominio, pero no de otros.

- **Aplicar Políticas (o Directivas) de Grupo**. Un dominio define un posible ámbito para las políticas. Al aplicar un objeto de política de grupo (GPO) en un dominio, este establece comportamientos específicos a los ordenadores (equipos) y usuarios del dominio bajo su ámbito. Por defecto, estas políticas se aplican siempre dentro de un mismo dominio y no entre dominios.

- **Delegar permisos administrativos**. En dominios Windows Server 2008 se puede realizar una delegación personalizada de los derechos administrativos a usuarios o grupos concretos dentro del Directorio Activo, tanto a nivel del dominio completo como de unidades organizativas (OUs) individuales. Esto reduce la necesidad de tener varios administradores con amplios permisos administrativos. Ya que un dominio representa un límite de seguridad, los permisos administrativos delegados también se limitan al dominio.

4.2.4.2. Múltiples dominios en la misma organización

Existen muchos casos, especialmente en organizaciones grandes, en los que es interesante que una misma organización disponga de varios dominios (por ejemplo, para reflejar una distribución geográfica o departamental, distintas empresas, etc.). El Directorio Activo permite almacenar y organizar la información de directorio de varios dominios de forma que, aunque la administración de cada uno sea independiente, dicha información esté disponible para todos los dominios. Como se explica a continuación, el conjunto de dominios de una organización pertenece a una estructura lógica denominada bosque, que puede estar formado por uno o varios dominios, distribuidos en uno o varios árboles de dominios.

La estructura de dominios de una organización se basa en los nombres de sus dominios. Puesto que en Windows Server, estos nombres se basan en el estándar DNS, los dominios se crean en una estructura de arbol invertida, con la raíz en la parte superior. Sin embargo, aunque la estructura se basa en los nombres, la vinculación entre dominios se establece explícitamente mediante las denominadas relaciones de confianza, que se describen más adelante.

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 (compartidos 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" del dominio inicial (es decir, ampliando el número de árboles del **bosque de dominios**), debajo del cual podemos crear subdominios, y así sucesivamente.

Arbol Un árbol es un conjunto de uno o más dominios dentro de un bosque que comparten un espacio de nombres contiguo, es decir, comparten un sufijo de DNS común. Como hemos dicho, si en una organización existe más de un dominio, estos se disponen en una o varias estructuras de árbol jerárquicas.

El primer dominio que se crea en una organización es el dominio raíz del bosque, y crea el propio bosque y el primer árbol del mismo. Cuando se agrega un dominio a un árbol existente, éste pasa a ser un dominio secundario (o hijo) de alguno de los dominios existentes, que pasa a ser su dominio padre. Los dominios secundarios pueden representar entidades geográficas (valencia, madrid, barcelona), entidades administrativas dentro de la organización (departamento de ventas, departamento de desarrollo ...), u otras delimitaciones específicas de una organización, según sus necesidades.

Los dominios que forman un árbol se vinculan mediante relaciones de confianza bidireccionales y transitivas. La relación padre-hijo entre dominios en un árbol de dominio es simplemente una relación de confianza. Sin embargo, los dominios siguen siendo independientes entre sí: los administradores de un dominio padre no son automáticamente administradores del dominio hijo y el conjunto de políticas de un dominio padre no se aplican automáticamente a los dominios hijo.

Por ejemplo, en la Universidad Politécnica de Valencia cuyo dominio actual de Active Directory es `upv.es` se crean dos nuevos departamentos: DSIC y DISCA. Con el fin de permitir la administración de los dominios por parte de los técnicos de los respectivos departamentos, se decide agregar dos nuevos dominios a su árbol de dominios existente en lugar de crear dos unidades organizativas en el dominio principal. Los dominios resultantes, `dsic.upv.es` y `disca.upv.es` forman un espacio de nombres contiguo, cuya raíz es `upv.es`. El administrador del dominio padre (`upv.es`) puede conceder permisos para recursos a cuentas de cualquiera de los tres dominios del árbol, pero por defecto no los puede administrar.

Bosque Un bosque se define como un grupo de árboles que no comparten un espacio de nombres contiguo, y que se conectan mediante relaciones de confianza bidireccionales y transitivas. A efectos prácticos, se debe recordar que sea cual sea la cantidad y estructuración de dominios de una organización, todos ellos constituyen un único bosque. Por lo tanto, aunque en la organización exista un único domnio, o varios dominios en un único árbol, dicho dominio o dicho árbol constituyen por sí mismos el bosque de la organización. En un bosque, todos los dominios comparten la misma configuración, el mismo esquema de directorio, y el mismo catálogo global (que se describe más adelante).

Añadir nuevos dominios a un bosque es fácil. Sin embargo, existen ciertas limitaciones que hemos de tener en cuenta al respecto:

- No se pueden mover dominios de Active Directory entre bosques.
- Sólo se puede eliminar un dominio de un bosque si este no tiene dominios hijo.
- Después de haber creado el dominio raíz de un árbol, no se pueden añadir al bosque dominios con un nombre de dominio de nivel superior.
- No se puede crear un dominio padre de un dominio existente.

En general, la estructuración de los dominios de una organización mediante un bosque con uno o varios árboles permite mantener convenciones de nombres de dominio tanto contiguos como discontiguos, lo cual puede ser útil en organizaciones con divisiones independendientes que quieren mantener sus propios nombres DNS.

Finalmente, debemos relacionar estos conceptos con el procedimiento para **crear un dominio**. Esto se hace mediante la ejecución de un asistente denominado **dcpromo.exe** en el sistema Windows Server 2008 que queramos *promocionar* a controlador de dominio. En concreto, este asistente nos permite elegir entre las siguientes opciones de instalación:

1. DC adicional de un dominio existente o DC para un dominio nuevo (creación de un dominio).

2. En el segundo caso, el dominio (nuevo) puede ser un dominio secundario de otro dominio existente (es decir, un subdominio en un árbol de dominios ya creado), o bien el dominio principal (raíz) de un nuevo árbol de dominios.

3. En este segundo caso, el dominio raíz puede ser de un bosque existente (agregamos una raíz nueva a un bosque) o de un nuevo bosque (creación del bosque). Por tanto, el primer dominio que creemos en una organización siempre será un dominio nuevo de un árbol nuevo de un bosque nuevo.

4.2.4.3. Niveles funcionales

A lo largo del tiempo, los sistemas Windows Server (y sus dominios) han evolucionado respecto a la funcionalidad que ofrecen. Esta evolución se refleja en los denominados *niveles funcionales*. Un nivel funcional, que puede estar definido a nivel de dominio o de bosque, establece simultáneamente una serie de características o funcionalidades disponibles en el dominio/bosque y la posibilidad de ser compatible con una versión previa de Windows Server a nivel de servidor (DC). Es decir, cuando situamos el nivel funcional del dominio/bosque en un valor determinado, podemos tener en dicho dominio DCs de cualquier versión de Windows Server que admita dicho nivel simultáneamente. Si elevamos el nivel funcional, ampliamos las posibilidades del dominio/bosque, pero a costa de no poder tener DCs de versiones previas de Windows que no sean compatibles con dicho nivel funcional. Una vez elevado el nivel funcional de un dominio/bosque, no puede volver a ponerse en el nivel previo.

A efectos prácticos, podemos entender los niveles funcionales como una forma