Active Directory

Juan M. Alberola

1. Introducción

Un componente fundamental de una estructura informática organizativa es el **Active Directory**, que nos permite gestionar las entidades y las relaciones dentro de la infraestructura. Con este servicio podremos gestionar los usuarios, sus credenciales y sus permisos. Además, también podremos gestionar los servidores, las estaciones de trabajo, los recursos, las aplicaciones, etc. Por tanto, debemos prestar mucha atención a la configuración de todo lo que definamos en el Active Directory porque de lo contrario, pondríamos en riesgo la seguridad del sistema.

2. Controlador de dominio

Un tema básico cuando hablamos de Active Directory es tener clara la diferencia entre los conceptos de grupo de trabajo y dominio. El **grupo de trabajo** nos permite definir un conjunto de ordenadores y recursos que tienen en común un nombre asignado. De esta forma, es muy fácil localizar los recursos del grupo si buscamos a través de el entorno gráfico de **Mis sitios de red**. Esta opción no añade nada más que una nomenclatura común, y la tenemos disponible por defecto cuando instalamos un equipo. Las políticas que definamos con esta configuración, sólo afectan al propio equipo, por lo que las denominamos **políticas de seguridad local**. Por tanto, tendríamos cuentas de usuario locales en cada uno de los equipos.

El concepto de **domino** sí que nos permite definir políticas a nivel de grupo de usuarios, equipos, aplicaciones, etc. de una forma global. Por tanto, en un entorno de producción organizativo, trabajaremos con dominios y no con grupos de trabajo. Esta política de seguridad común se gestiona desde un servidor que tenga el rol de Active Directory, y con ella podremos gestionar una serie considerable de aspectos como cuentas de usuario globales en la organización, cuentas de equipo, privilegios de acceso, etc. Al servidor que se encarga de dar soporte al dominio y gestionar la base de datos de toda la infraestructura, se le denomina **controlador de dominio**.

En un entorno productivo real, se recomienda que haya al menos dos servidores que sean controlador de dominio. A uno de ellos lo denominamos controlador de dominio **principal** y al otro **secundario**. El hecho de tener dos controladores de dominio permitirá que los clientes puedan iniciar sesión sin problemas si cae el controlador principal. A partir de esta configuración, las posibilidades son múltiples, como tener varios controladores de dominio secundarios en la misma organización, o gestionar varios dominios en la misma organización (por ejemplo, en sedes distintas). En este último caso, podemos utilizar el concepto

de **bosque** para referirnos al conjunto de dominios y controladores de dominio que pertenezcan a la misma infraestructura de red. A modo de ejemplo, podríamos tener un dominio llamado **florida.com**, otro **tics.florida.com**, y otro **administracion.florida.com**. Estos tres dominios estarían en el mismo bosque y serían gestionados por el mismo Active Directory. Si queremos añadir complejidad a nuestro sistema, también podemos hablar de varios **árboles** de dominios dentro de un bosque, cada uno de ellos gestionando un conjunto de dominios. No obstante, todos estos conceptos van más allá de los objetivos de esta asignatura.

Por tanto, a modo de resumen, podemos definir los siguientes pasos necesarios para gestionar los recursos de una manera centralizada en nuestro Active Directory:

1. Analizar y planificar las necesidades de nuestra organización.
2. Instalar los servidores que necesitemos.
3. Promocionar a controlador de dominio los servidores.
4. Unir al dominio los distintos equipos de nuestra organización.
5. Crear cuentas de usuario y asociarles privilegios y restricciones.
6. Definir recursos compartidos con los permisos adecuados.