**Administración y monitorización de procesos, red, memoria, sistemas de archivos, servicios (impresión, etc.), usuarios, grupos y permisos.**

Administración de los recursos.

Permite realizar tres conjuntos de tareas para administrar los recursos de almacenamiento en servidores locales o remotos:

Administración de cuotas. Establece un límite de espacio máximo o de advertencia en un volumen o en un árbol de carpetas. Permite crear y aplicar plantillas de cuotas con propiedades de cuota estándar.

Administración del filtrado de archivos. Define reglas de filtrado que supervisan o bloquean los intentos de guardar determinados tipos de archivos en un volumen o un árbol de carpetas por parte de los usuarios. Permite crear y aplicar plantillas de filtrado con exclusiones de archivos estándar.

Administración de informes de almacenamiento. Genera informes integrados que permiten llevar un seguimiento del uso de cuotas, de las actividades de filtrado de archivos y de los patrones de uso del almacenamiento.

También puede aplicar directivas de cuotas y de filtrado de archivos cuando se aprovisiona una carpeta compartida o por medio de una interfaz de línea de comandos.

Administración de las cuentas de usuario y de equipo.

Las cuentas de usuario y las cuentas de equipo de Active Directory representan una entidad física como una persona o un equipo. Las cuentas de usuario también se pueden utilizar como cuentas de servicio dedicadas para algunas aplicaciones.

Las cuentas de usuario y de equipo (así como los grupos) se denominan también principales de seguridad. Los principales de seguridad son objetos de directorio a los que se asigna automáticamente identificadores de seguridad (SID), que se utilizan para tener acceso a los recursos del dominio. Una cuenta de usuario o de equipo se utiliza para:

Autenticar la identidad de un usuario o equipo.

Una cuenta de usuario permite que un usuario inicie una sesión en equipos y dominios con una identidad que puede ser autenticada por el dominio. Para obtener información acerca de la autenticación, vea Control de acceso en Active Directory. Cada usuario que se conecta a la red debe tener su propia cuenta de usuario y su propia contraseña única. Para aumentar la seguridad, debe evitar que varios usuarios compartan una misma cuenta.

Autorizar o denegar el acceso a los recursos del dominio.

Después de que el usuario haya sido autenticado, se le autoriza o deniega el acceso a los recursos del dominio según los permisos explícitos asignados a dicho usuario en el recurso.