CCN
centro criptológico nacional

Guía de Seguridad de las TIC

IMPLEMENTACIÓN DE SEGURIDAD EN SERVIDOR DE FICHEROS SOBRE MICROSOFT WINDOWS SERVER 2016

NOVIEMBRE 2018

MINISTERIO DE DEFENSA

Edita:

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC,
ou=sello electrónico, serialNumber=S2800155J,
o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO
CRIPTOLOGICO NACIONAL, c=ES
2018.11.29 15:32:13 +01'00'

NIPO: 083-19-035-6
Fecha de Edición: noviembre de 2018

Sidertia Solutions S.L. ha participado en la realización y modificación del presente documento y sus anexos.

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de Enero, actualizado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

noviembre de 2018

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como CERT Gubernamental Nacional español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo a esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

2. INTRODUCCIÓN

Este documento forma parte del conjunto de normas desarrolladas por el Centro Criptológico Nacional para entornos basados en los productos y sistemas operativos de Microsoft (CCN STIC 500), siendo de aplicación para la Administración pública en el cumplimiento del Esquema Nacional de Seguridad (ENS) y de obligado cumplimiento para los sistemas que manejen información clasificada nacional.

La serie CCN STIC 500 se ha diseñado de manera incremental. Así, dependiendo del sistema, se aplicarán consecutivamente varias de estas guías. En este sentido se deberán aplicar las guías correspondientes dependiendo del entorno que se esté asegurando.

Por ejemplo, en el caso de un entorno que le sea de aplicación el ENS, para un servidor miembro de un dominio con Microsoft Windows Server 2012 R2, en el que se instale Microsoft Exchange Server 2013, deberán aplicarse las siguientes guías:

a) Guía CCN-STIC-870A en el servidor miembro con Windows Server 2012 R2.

b) Guía CCN-STIC-873 Internet Information Services (IIS) 8.5.

c) Guía CCN-STIC-880 Microsoft Exchange Server 2013 en Windows 2012 R2.

Por ejemplo, en el caso de un entorno de red clasificada, para un servidor con Microsoft Windows Server 2012 R2, en el que se instale Microsoft Exchange Server 2013, deberán aplicarse las siguientes guías:

a) Guía CCN-STIC-560A en el servidor miembro con Windows Server 2012 R2.

b) Guía CCN-STIC-563 Internet Information Services (IIS) 8.5.

c) Guía CCN-STIC-552 Microsoft Exchange Server 2013 en Windows 2012 R2.

Nota: Estas guías están pensadas y diseñadas para entornos de máxima seguridad donde no existirá conexión con redes no seguras como puede ser Internet.

3. OBJETO

El propósito de este documento consiste en proporcionar los procedimientos para implementación, establecer la configuración y realizar tareas de administración maximizando las condiciones de seguridad del servidor de ficheros de Microsoft Windows Server 2016 en un servidor miembro de una infraestructura de dominio.

La configuración que se aplica a través de la presente guía se ha diseñado para ser lo más restrictiva posible, minimizando la superficie de ataque y por lo tanto los riesgos que pudieran existir. En algunos casos y dependiendo de la funcionalidad requerida del servidor, podría ser necesario modificar la configuración, que aquí se plantea, para permitir que el equipo proporcione servicios adicionales.

No obstante, se tiene en consideración que los ámbitos de aplicación son muy variados y por lo tanto dependerán de su aplicación, las peculiaridades y funcionalidades de los servicios prestados por las diferentes organizaciones. Por lo tanto, las plantillas y normas de seguridad se han generado definiendo unas pautas generales de seguridad que permitan el cumplimiento de los mínimos establecidos en el ENS y las condiciones de seguridad necesarias en un entorno clasificado.

En el caso de la aplicación de seguridad sobre un entorno perteneciente a una red clasificada, se establece la máxima seguridad posible teniendo en consideración la guía CCN-STIC-301 – Requisitos STIC. Si su sistema requiere de otra configuración menos restrictiva, y está autorizado para ello, consulte el apartado “APLICACIÓN DE NIVELES DE CLASIFICACIÓN” del “ANEXO B” de la guía codificada como CCN-STIC-570A para realizar los pasos adecuados.

Esta guía asume que el servidor de ficheros se va a implementar sobre un equipo con un sistema operativo Windows Server 2016 Standard de 64 Bits, donde se ha seguido el proceso de implantación definido en la guía CCN-STIC-570A.

Cumpliendo con estos requisitos previos, puede iniciar la instalación del servidor de ficheros basado en Microsoft Windows Server 2016 Standard.

Así mismo, no se contempla en esta guía la instalación del servicio de archivos y almacenamiento en clúster, ni se han aplicado características de alta disponibilidad o protección ante fallos del servicio.

4. ALCANCE

La guía se ha elaborado para proporcionar información específica para realizar una implementación del servidor de ficheros de Microsoft Windows Server 2016 en una configuración restrictiva de seguridad. Se incluyen, además, operaciones básicas de administración como la compartición de recursos, asignación de ACL, implementación de políticas y delegación de la administración, entre otros aspectos, además de aquellas acciones que deben ser llevadas a cabo para el adecuado mantenimiento del servicio.

El escenario en el cual está basada la presente guía tiene las siguientes características técnicas:

a) Un único bosque de Directorio Activo.

b) Un único dominio dentro del bosque de Directorio Activo.

c) Nivel funcional del bosque y del dominio en Windows Server 2016 Standard.

d) Un controlador de dominio basado en Windows Server 2016 Standard.

e) Un servidor miembro del dominio basado en Windows Server 2016 Standard.

f) No se contemplan mecanismos de alta disponibilidad ni balanceo de carga en el escenario planteado.

Este documento incluye:

a) **Mecanismos para la aplicación de configuraciones.** Se incorporan mecanismos para la implementación de forma automática de las configuraciones de seguridad susceptibles de ello.

b) **Mecanismos para la creación de cuentas necesarias para la funcionalidad de la solución.** Tanto los procesos de implementación como de instalación requieren de cuentas específicas; se ha automatizado el proceso de creación de dichas cuentas.

c) **Descripción de la seguridad en el servicio de archivos y almacenamiento.** Completa la descripción de los mecanismos de seguridad, autenticación y autorización utilizados en el servicio de archivos y almacenamiento de Windows Server 2016, así como las medidas para reforzar dicha seguridad.

d) **Guía paso a paso.** Va a permitir implantar y establecer las configuraciones de seguridad de un servidor de ficheros de Windows Server 2016.

e) **Guía de administración.** Va a permitir realizar tareas de administración en el entorno de seguridad establecido.

f) **Lista de comprobación.** Permitirá verificar el grado de cumplimiento de un servidor con respecto a las condiciones de seguridad que se establecen en esta guía.

5. DESCRIPCIÓN DEL USO DE ESTA GUÍA

Para entender esta guía, es conveniente explicar el proceso de aplicación de seguridad que describe y los recursos que proporciona. Este proceso constará de los siguientes pasos:

a) Antes de comenzar a aplicar la guía, además de los requisitos para la instalación del servicio de archivos y almacenamiento, será necesario cumplir los requisitos definidos para Windows Server 2016.

b) Si el entorno que el que está aplicando seguridad pertenece a una red clasificada, se deberá realizar la securización del sistema antes de instalar el rol de servidor de ficheros, será necesario aplicar la guía de seguridad codificada como CCN-STIC-570A y a continuación se deberá instalar y configurar el rol de servidor de ficheros de Windows Server 2016 tal y como se describe en la presente guía.

c) En aquellos sistemas que les sea de aplicación el ENS estas medidas deberán adaptarse a las necesidades de cada organización.

5.1 AVISOS IMPORTANTES A LOS USUARIOS DE ESTA GUÍA

Los contenidos de esta guía son de aplicación a equipos tipo puesto servidor con Sistema Operativo Windows Server 2016, en castellano, con el objetivo de reducir la superficie de exposición a ataques posibles con una instalación por defecto, manteniendo los principios de máxima seguridad, mínima exposición y servicios y mínimos privilegios que emanan de la CCN-STIC-301. En el caso de llevar a cabo la aplicación de esta guía sobre el Sistema Operativo con una configuración de idioma diferente al castellano, es posible que deba incorporar nuevos recursos y/o realizar ciertas modificaciones sobre los recursos que se adjuntan con este documento para permitir la correcta aplicación y uso del documento.

La guía ha sido probada y verificada con la versión de Windows Server 2016 Standard, con los parámetros por defecto de instalación y aplicando la guía CCN-STIC-570A para su configuración. No se ha verificado en otros tipos de instalaciones como pudiera ser Windows Server 2016 Datacenter. No obstante, y teniendo en consideración las funcionalidades de ambas versiones de sistema operativo servidor, podría llegar a implementarse la siguiente guía sobre la versión Datacenter. La presente guía no será funcional con la versión Windows Server 2016 Essentials.

Esta guía se ha diseñado para reducir la superficie de exposición de los equipos servidores que cuenten con una implementación de rol de servidor de ficheros en un entorno de dominio de Active Directory.

La guía de seguridad ha sido elaborada utilizando un laboratorio basado en una plataforma de virtualización tipo Hyper-V de Windows Server 2016 con las siguientes características técnicas:

a) Servidor Dell PowerEdgeTM T320:

   i. Intel Pentium Xeon Quad Core.

   ii. HDD 80 GB.

   iii. 32 GB de RAM.

   iv. Interfaz de Red 1 GB.

Esta guía de seguridad no funcionará con hardware que no cumpla con los requisitos de seguridad mínimos de Windows Server 2016. Esto quiere decir que se requieren equipos con procesadores Intel o AMD de 64 bits (x64), con más de 2048 MB de memoria RAM.

Así mismo, hay que tener en cuenta que el rol de servidor de ficheros requiere, para un entorno de producción, un mínimo de 2 GB de memoria RAM para funcionar adecuadamente, aunque se recomiendan 4 GB. Oficialmente no se indica ningún requerimiento adicional.

Se espera, por tanto, que el rendimiento de Windows Server 2016 pueda exceder dichos límites. Es por ello que se recomienda al menos disponer de 4 GB de memoria RAM en entornos en producción.

Por otro lado, es importarte remarcar que no existe ningún requisito de hardware o software especial para ejecutar Servicios de archivos y almacenamiento.

La guía ha sido desarrollada con el objetivo de dotar a la infraestructura de la seguridad máxima en caso de redes clasificadas y la seguridad mínima siguiendo las normas descritas en el ENS. Es posible que algunas de las funcionalidades esperadas hayan sido desactivadas y por lo tanto pueda ser necesario aplicar acciones adicionales para habilitar servicios o características deseadas en Microsoft Windows Server 2016.

Para garantizar la seguridad de los servidores, deberán instalarse las actualizaciones recomendadas por el fabricante, disponibles a través del servicio de Windows Update. Las actualizaciones por lo general se liberan los segundos martes de cada mes, no obstante, hay que tener presente que determinadas actualizaciones por su criticidad pueden ser liberadas en cualquier momento.

Dependiendo de la naturaleza de estas actualizaciones, el lector podrá encontrarse con algunas diferencias respecto a lo descrito en esta guía. Esto viene motivado por los cambios que en ocasiones se realizan para las distintas actualizaciones de seguridad.

Antes de aplicar esta guía en producción, deberá asegurarse de haber probado en un entorno aislado y controlado donde se han aplicado los test y cambios en la configuración, que se ajustan a los criterios específicos de cada organización.

El espíritu de estas guías no está dirigido a reemplazar políticas consolidadas y probadas de las organizaciones sino a servir como la línea base de seguridad, que deberá ser adaptada a las necesidades propias de cada organización.

5.2 ESTRUCTURA DE LA GUÍA

Esta guía dispone de una estructura que diferencia la implementación del servidor de ficheros sobre Microsoft Windows Server 2016 dependiendo del entorno sobre el que vaya a ser aplicado, así como una diferenciación de la versión a utilizar.

La guía dispone de las siguientes configuraciones divididas en dos grandes anexos, los cuales se definen a continuación:

a) Anexo A: En este anexo se define la configuración necesaria para adaptar los sistemas Microsoft Windows Server 2016 en sus versiones Standard y Datacenter con rol de servidor de ficheros a las necesidades requeridas por el Esquema Nacional de Seguridad (ENS).

b) Anexo B: En este anexo se define la configuración necesaria para adaptar los sistemas Microsoft Windows Server 2016 en sus versiones Standard y Datacenter a las necesidades requeridas en los entornos clasificados donde se quiera instalar el rol de servidor de ficheros.

Cabe remarcar que en sus respectivos anexos se dotará de la información necesaria y concreta para cada tipo de implementación.

De manera adicional, en cada una de las carpetas “Scripts” que se adjuntan a los documentos, existe un directorio que almacena un informe en formato HTML con cada objeto de directiva de grupo (GPO) o directiva de grupo local (GPL) que se aplica.

6. SERVIDOR DE FICHEROS EN WINDOWS SERVER 2016

Un servidor de ficheros es un tipo de servidor que almacena y distribuye diferentes tipos de archivos informáticos entre los usuarios de una red de ordenadores. Su función es proporcionar una ubicación central en la red y permitir el acceso remoto a los usuarios desde otros equipos a los archivos que almacena y comparte o sobre los que tiene acceso.

El rol Servicios de archivos y almacenamiento de Microsoft Windows Server 2016 permite configurar y administrar uno o más servidores de ficheros, los cuales proporcionan ubicaciones centrales en la red para almacenar archivos y compartirlos con usuarios de la red.

A modo de aplicación, dentro de una organización, si los usuarios de la red necesitan tener acceso a los mismos archivos y aplicaciones, o si la administración centralizada de archivos y copias de seguridad es importante en la organización, se deberá configurar un servidor como servidor de ficheros.

Por otro lado, los administradores pueden hacer uso del rol Servicios de archivos y almacenamiento para configurar y administrar varios servidores de ficheros y sus capacidades de almacenamiento correspondientes con la herramienta “Administrador del servidor” o “Windows PowerShell”.

En Windows Server 2016 se implementan algunas mejoras sobre las funcionalidades que ya se incorporaron en Windows Server 2012 R2 y se añaden otras nuevas, las cuales se describen a continuación:

a) Espacios de almacenamiento directo. Esta función permite la creación de almacenamiento altamente disponible y escalable con servidores de almacenamiento local. Reduce el tiempo de implementación y administración de los sistemas de almacenamiento que son declarados por software y permite el uso de dispositivos de disco SSD con conexiones SATA y discos NVME. Anteriormente no estaban disponibles para espacios de almacenamiento de clúster con discos compartidos. Espacios de almacenamiento directo utiliza la red como capa de almacenamiento, aprovechando SMB3 y SMB directo(RDMA) para el almacenamiento eficiente de CPU.

b) Réplica de almacenamiento (SR) es una nueva funcionalidad en Windows Server 2016 que permite la replicación sincrónica independiente del almacenamiento y a nivel de bloque entre servidores o clústeres para la recuperación ante desastres, así como la extensión de un clúster de conmutación por error entre sitios. La replicación sincrónica permite el reflejo de datos en sitios físicos con volúmenes coherentes frente a bloqueos para asegurar que no se produce absolutamente ninguna pérdida de datos en el nivel de sistema de archivos. La replicación asincrónica permite la extensión de sitios más allá del área metropolitana con la posibilidad de pérdida de datos.

c) Calidad de servicio de almacenamiento, se puede utilizar para inspeccionar de forma central el rendimiento del almacenamiento de punto a punto y crear directivas de administración mediante Hyper-V y clústeres de CSV. Ahora se puede crear directivas de calidad de servicio de almacenamiento(QoS) en un clúster de CSV y asignarlas en uno o varios discos de máquinas virtuales de Hyper-V.

d) Mejoras referentes a la desduplicación de datos:

   i. Compatibilidad con volúmenes grandes. Ahora se admiten volúmenes de hasta 64TB para la desduplicación de datos.

   ii. Compatibilidad con archivos de gran tamaño. En Windows 2016 los archivos de hasta 1TB son totalmente compatibles para la desduplicacion de datos.

   iii. Compatibilidad con Nano Server.

   iv. Compatibilidad con copia de seguridad simplificada.

   v. Compatibilidad con las actualizaciones progresivas de sistema operativo de clúster.

e) En Windows 10 y Windows Server 2016, las conexiones de cliente a los recursos compartidos de archivos SYSVOL y NETLOGON predeterminados de Active Directory Domain Services en controladores de dominio ahora requieren firma SMB y autenticación mutua (como Kerberos). Este cambio reduce la probabilidad de ataques de tipo "Man in the middle". Si alguna de los dos requisitos (firma SMB y autentificación) no está disponible, no se aplicarán las directivas de grupo y los scripts basados en dominio.

f) Carpetas de trabajo. Se han mejorado las notificaciones cuando se realizan cambios en los archivos. En Windows Server 2012 R2, cuando se realizaban cambios en las carpetas de trabajo del servidor, se producía un retardo de hasta 10 minutos para que los clientes vieran reflejado el cambio. Con Windows Server 2016, el servidor de carpetas de trabajo notifica inmediatamente a los clientes de Windows 10 y los cambios del archivo se sincronizan inmediatamente.

g) El sistema de archivos resistentes (ReFS) fue implementado en Windows Server 2012 R2 y en Windows Server 2016 se han introducido las siguientes mejoras:

i. Aumento del rendimiento y tamaño máximo del volumen (4,7 ZB (zettabytes)).

ii. Se incorpora la clonación de bloques, mejorando el rendimiento de las operaciones de máquina virtual.

iii. Nueva herramienta de escaneo que permite la recuperación de almacenamiento perdido y recuperar datos de información corrompida.

Nota: Toda la información de las novedades de almacenamiento en Windows Server 2016 pueden ser consultadas a través del siguiente enlace:
https://docs.microsoft.com/es-es/windows-server/storage/whats-new-in-storage

Cuando se instala Windows Server 2016, el programa de instalación implementa por defecto el rol “Servicios de archivos y almacenamiento.

Para usar el “Administrador de recursos del servidor de archivos” en Windows Server 2016, se debe instalar el rol “Servicios de archivos y almacenamiento” en el equipo donde desea usar la administración de ficheros.

El equipo debe estar unido a un dominio de Active Directory como un servidor miembro. Si desea autenticar los clientes o publicar una carpeta compartida en Active Directory, el servidor de ficheros se debe unir a un dominio. Si no necesita realizar ninguna de estas tareas, no es necesario unir el servidor de ficheros a un dominio.

Todo el espacio disponible en el disco debe estar asignado. Puede utilizar Administración de discos o DiskPart.exe (línea de comandos) para crear una nueva partición a partir del espacio no asignado.

Todos los volúmenes de disco existentes deberían utilizar el sistema de archivos NTFS o cualquier otro que permita la aplicación de ACL’s. Los volúmenes FAT32 no son seguros y no admiten compresión de archivos y carpetas, cuotas de disco, cifrado de archivos ni permisos de archivo individuales.

Por defecto el programa de instalación da a todos los sistemas de ficheros el formato NTFS, por lo que normalmente no será necesario indicarlo explícitamente. Si los equipos disponen de BIOS UEFI, también son válidas las particiones con sistemas de archivos EFI.

El Firewall de Windows debe estar habilitado y debe permitir las comunicaciones para el acceso a los archivos. Debido a la implementación de otras guías es posible que el sistema esté securizado y no permita el uso de las características del servidor de ficheros.

Si el Firewall de Windows está habilitado, debe seleccionar “Compartir archivos e impresoras” en la ficha “Excepciones de Firewall de Windows”, a fin de que la función de servidor de ficheros funcione correctamente.

En la siguiente tabla se enumera la información de la que se debe disponer antes de agregar la función de servidor de archivos.

Antes de agregar una función de servidor de archivo	Descripción
Determine si desea configurar cuotas de disco.	– Utilice cuotas de disco para realizar un seguimiento y controlar el uso del espacio en disco para volúmenes NTFS por volumen. – Las cuotas impiden que los usuarios utilicen más espacio en disco del asignado, ya que registran un suceso cuando un usuario supera un límite de espacio en disco especificado.
Determine si desea utilizar el Servicio de Index Server.	– El Servicio de Index Server crea índices de los contenidos y propiedades de documentos en el disco duro local y en las unidades de red compartidas. Dichos índices permiten a los usuarios realizar búsquedas de forma más rápida y sencilla. – El Servicio de Index Server ralentiza el servidor, por lo que se recomienda utilizarlo únicamente si los usuarios buscan con frecuencia el contenido de los archivos del servidor.
Identifique las carpetas que desea compartir en el equipo y especifique un nombre de carpeta y una descripción.	– Los usuarios ven los recursos compartidos en este servidor de ficheros en función del nombre de archivo. Se recomienda crear nombres compartidos que se puedan recordar fácilmente y que sean representativos del contenido de la carpeta. Por ejemplo, se ofrece a cada uno de los usuarios 2 gigabytes (GB) para almacenar información privada en el servidor de ficheros. – Se puede asignar a la carpeta de nivel superior del servidor de ficheros el nombre Carpetas personales y, a continuación, nombrar cada una de las subcarpetas en función del nombre de dominio del usuario.
Determine el tipo de permisos que desea asignar a las carpetas.	– Asigne los permisos más restrictivos, siempre que permitan a los usuarios realizar las tareas necesarias. – El control de acceso en el sistema de archivos NTFS proporciona más seguridad que los permisos de recurso compartido independientes.

Requisitos de seguridad:

a) Para administrar un servidor de ficheros remoto, debe ser miembro del grupo “Admins. del dominio”, o del grupo local “Administradores” en el servidor de ficheros remoto. Estas credenciales no son necesarias para supervisar los servidores de ficheros remotos, aunque algunas funciones estarán deshabilitadas.

b) Para usar la consola “Administrador de recursos del servidor de archivos” (fsrm.msc) con la directiva de grupo, debe ser miembro del grupo local “Administradores” y tener acceso de escritura a los objetos de directiva de grupo (GPO) en el dominio de Servicios de dominio de Active Directory (AD DS) o la unidad organizativa donde desea implementar las conexiones con los servidores de ficheros.

c) Se recomienda a los administradores que usen una cuenta con permisos restrictivos para realizar tareas rutinarias no administrativas, y usar una cuenta con más permisos sólo cuando realicen tareas administrativas específicas.

6.1 COMPARTICIÓN DE RECURSOS

Un recurso compartido (fichero, directorio, etc.) permite a un usuario acceder a dicho recurso sin necesidad de que el usuario este en la ubicación actual del recurso. Normalmente este recurso es compartido a través de la red de manera que dicho usuario pueda hacer uso de éste.

Desde el punto de vista del servidor de ficheros compartir un recurso implica que los usuarios no tengan la necesidad de poseer el recurso en la propia máquina, de tal manera que todos los archivos necesarios estén de manera centralizada en un único servidor de ficheros para todos los usuarios.

6.2 PERMISOS DE ACCESO

Cada contenedor u objeto (recurso) de la red tiene información de control de acceso adjunta. Esta información se denomina descriptor de seguridad y controla el tipo de acceso permitido a usuarios y grupos. El descriptor de seguridad se crea automáticamente junto con el contenedor u objeto que se crea. Un ejemplo típico de objeto con un descriptor de seguridad es un archivo.

Los permisos se definen en el descriptor de seguridad de un objeto. Se asocian o asignan a usuarios y grupos específicos. Por ejemplo, para el archivo “Fichero.txt”, el grupo de cuentas predefinidas de administrador podría tener asignados permisos para leer, escribir y eliminar, mientras que el grupo de operadores de copia de seguridad sólo permisos para leer y escribir.

Cada asignación de permisos a un usuario o grupo se representa en el sistema como una entrada de control de acceso (ACE). Al conjunto completo de entradas de permiso de un descriptor de seguridad se le denomina conjunto de permisos o lista de control de acceso (ACL). De esta forma, para un archivo denominado “Fichero.txt”, el conjunto de permisos incluye dos entradas de permiso (ACL) según el ejemplo anterior:

a) Para el grupo de cuentas predefinidas de administrador.

b) Para el grupo de operadores de copia de seguridad.

Cuando se es miembro de un grupo de seguridad que está asociado a un objeto, se tiene cierta capacidad para administrar los permisos de ese objeto. En el caso de los objetos que se poseen (propietario del recurso), el control es total. Puede utilizar distintos métodos, como Servicios de dominio de Active Directory (AD DS), Directivas de grupo o listas de control de acceso (ACL), para administrar distintos tipos de objetos.

Existen dos tipos de permisos: permisos explícitos y permisos heredados.

a) Los permisos explícitos son aquellos que se establecen de forma predeterminada en los objetos cuando son creados por primera vez o aquellos que el usuario establece en éstos. También se denominan permisos explícitos a aquellos que el usuario otorga a objetos ubicados dentro de otro objeto.

b) Los permisos heredados son los que se propagan a un objeto desde un objeto que los contiene. Los permisos heredados facilitan la tarea de administrar permisos y aseguran su coherencia entre todos los objetos de un contenedor determinado.

De forma predeterminada, los objetos de un contenedor heredan los permisos desde ese contenedor cuando se crean los objetos. Por ejemplo, cuando crea el directorio “Nueva carpeta”, todas las subcarpetas y archivos creados en el directorio “Nueva carpeta” heredan de forma automática los permisos de la carpeta. De esta manera, el directorio “Nueva carpeta” tiene permisos explícitos, mientras que los subdirectorios y los archivos poseen permisos heredados.

Es importante también conocer cómo se aplican los permisos heredados:

a) Cuando la casilla “Aplicar estos permisos a objetos y/o contenedores sólo dentro de este contenedor” está desactivada.

Aplicar en	Permisos a la carpeta actual	Permisos a las subcarpetas de la carpeta actual	Permisos a los archivos de la carpeta actual	Permisos a todas las subcarpetas subsiguientes	Permisos a los archivos de todas las subcarpetas subsiguientes
Sólo esta carpeta	X				
Esta carpeta, subcarpetas y archivos	X	X	X	X	X
Esta carpeta y sus subcarpetas	X	X		X	
Esta carpeta y sus archivos	X		X		X
Sólo subcarpetas y archivos		X	X	X	X
Sólo subcarpetas		X		X	
Sólo archivos			X		X

b) Cuando la casilla “Aplicar estos permisos a objetos y/o contenedores sólo dentro de este contenedor” está activada

Aplicar en	Permisos a la carpeta actual	Permisos a las subcarpetas de la carpeta actual	Permisos a los archivos de la carpeta actual	Permisos a todas las subcarpetas subsiguientes	Permisos a los archivos de todas las subcarpetas subsiguientes
Sólo esta carpeta	X				
Esta carpeta, subcarpetas y archivos	X	X	X		
Esta carpeta y sus subcarpetas	X	X			
Esta carpeta y sus archivos	X		X		
Sólo subcarpetas y archivos		X	X		
Sólo subcarpetas		X			
Sólo archivos			X		

Todos los objetos que se encuentran en un volumen NTFS tienen un propietario. El propietario controla el modo en que se establecen los permisos en el objeto y a quién se conceden.

De forma predeterminada, el propietario es la entidad que creó el objeto. El propietario siempre puede cambiar los permisos de un objeto, incluso cuando se le deniega el acceso al objeto. Al tomar posesión de un objeto el usuario se convierte en el propietario de este.

La posesión de un objeto puede ser tomada por:

a) Un administrador. De manera predeterminada, al grupo “Administradores” se le concede el derecho de usuario “Tomar posesión” de archivos y otros objetos.

b) Cualquier usuario o grupo que tenga el permiso “Tomar posesión” en el objeto.

c) Un usuario que tenga el derecho de usuario “Restaurar archivos y directorios”.

La propiedad se puede transferir de las siguientes formas:

a) El propietario actual puede conceder el permiso “Tomar posesión” a otro usuario si ese usuario es miembro de un grupo definido en el testigo de acceso del propietario actual. El usuario debe tomar posesión realmente para completar la transferencia.

b) Un administrador puede tomar posesión.

c) Los usuarios que tengan el derecho de usuario “Restaurar archivos y directorios” pueden hacer doble clic en “Otros usuarios y grupos” y seleccionar cualquier usuario o grupo al que deseen asignar la propiedad.

En un servidor de ficheros, el acceso a una carpeta puede estar determinado por dos conjuntos de entradas de permisos.

a) Los permisos de recurso compartido definidos en una carpeta. También denominados permisos FAT.

b) Los permisos NTFS definidos en la carpeta, también conocidos como permisos locales o de seguridad. Estos permisos también pueden ser asignados sobre ficheros.

Los permisos de recursos administrativos compartidos, tales como Admin$ o C$, son utilizados para administrar equipos de forma remota. Esto puede emplearse tanto en sistemas de ficheros FAT, FAT32 o NTFS.

Los permisos de recurso compartido y los permisos NTFS son independientes, es decir, ninguno modifica al otro. Los permisos de acceso final en una carpeta compartida se determinan teniendo en cuenta las entradas de permiso de recurso compartido y de permiso NTFS. En un término final se aplicarán siempre los permisos más restrictivos. Por ejemplo, si una carpeta tiene permisos de recurso compartido de “Control Total”, mientras que en los permisos NTFS posee las características de “Leer y ejecutar” los usuarios que accedan a ese recurso solo podrán “Leer y ejecutar”.

A modo de recomendación a continuación se definen una serie de permisos a conceder en función del tipo de carpeta que se esté compartiendo:

Tipo de recurso	Descripción	Permisos FAT (permisos de recurso compartido)	Permisos NTFS (permisos locales)
Carpeta pública	Carpeta accesible a todos los usuarios.	Permiso "Cambiar" al grupo Usuarios.	Permiso "Modificar" al grupo Usuarios.
Carpeta privada	Carpeta con información que solo debe ser vista por los administradores.	Permiso "Cambiar" al grupo Usuarios. Permiso "Control Total" al grupo Administradores.	Permiso "Escribir" al grupo de usuarios que se aplica a "Sólo esta carpeta". (Esta opción está disponible en la página Opciones avanzadas). * Permiso "Control total" al grupo Administradores.
Carpeta de aplicaciones	Carpeta que contiene aplicaciones para ejecutar a través de la red.	Permiso "Leer" al grupo Usuarios.	Permisos "Leer, Leer y ejecutar y Mostrar el contenido de la carpeta" al grupo Usuarios
Carpeta personal	Carpeta individual de cada usuario.	Permiso "Control total" en su carpeta correspondiente.	Permiso "Control total" en su carpeta correspondiente.

Nota: Si cada usuario necesita tener determinados permisos para los archivos que deja, es posible crear una entrada de permiso para el identificador de seguridad conocido (SID) Creator Owner y aplicarla a "Sólo subcarpetas y archivos". Por ejemplo, puede conceder los permisos Leer y Escribir al SID de Creator Owner en la carpeta privada y aplicarlos a todas las subcarpetas y archivos. De este modo, el usuario que ha dejado o creado el archivo (Creator Owner) tiene la capacidad para leer y escribir en el archivo. Después, Creator Owner puede tener acceso al archivo mediante la ubicación de red: \\NombreServidor\RecursoCompartido\NombreFichero.

Además, es necesario tener en consideración las siguientes casuísticas:

a) Conceder a un usuario el permiso NTFS “Control total” en una carpeta permite a ese usuario tomar posesión (hacerse propietario) de la carpeta a menos que esté restringido de alguna forma. Se deber tener especial cuidado al conceder el permiso “Control total”.

b) Si se desea administrar el acceso a carpetas exclusivamente mediante permisos NTFS, es necesario establecer los permisos de recurso compartido en “Control total” para el grupo “Todos”.

c) Los permisos NTFS influyen sobre el acceso tanto local como remoto además de aplicarse con independencia del protocolo. Por el contrario, los permisos de recurso compartido (FAT) sólo se aplican a recursos compartidos de red. No restringen el acceso a ningún usuario local ni a ningún usuario de Terminal Server del equipo en el que tenga establecidos permisos de recurso compartido. Por lo tanto, no ofrecen privacidad entre usuarios de un equipo que utilizan varios usuarios, ni en un servidor de Terminal Server al que tienen acceso varios usuarios.

d) De forma predeterminada, el grupo “Todos” no incluye el grupo “Anónimo”, por lo que los permisos que se aplican al grupo “Todos” no afectan al grupo “Anónimo”.

Nota: En la medida de lo posible no deberán aplicarse permisos al grupo “Todos”. En vez de esto se otorgarán permisos al grupo “Usuario autenticados” o al grupo o grupos de usuarios que exclusivamente deban ser receptores del permiso.

Los permisos efectivos son definidos como la suma de los permisos que se adquieren por el usuario que se es y por los grupos a los que pertenece dicho usuario, teniendo en cuenta que siempre se aplican los permisos más restrictivos. Por ejemplo, si sobre un archivo se le aplica el permiso “Control Total” en el grupo “Usuarios” (grupo al que se supone que pertenece el usuario) y al usuario que puede acceder a dicho archivo solo se le aplica el permiso de “Leer” los permisos efectivos serán los de “Control Total”, ya que estos se suman. Por el contrario, si sobre el grupo “Usuarios” al que pertenece el usuario se asigna sobre ese archivo el permiso “Control Total” pero al usuario en particular sobre el archivo no se le permite “Escribir”, podrá realizar cualquier acción menos escribir.

Los siguientes factores se utilizan para determinar los permisos efectivos:

a) Pertenencia a grupos globales.

b) Pertenencia a grupos locales.

c) Pertenencia a grupos universales.

d) Permisos locales.

e) Privilegios locales.

Los siguientes identificadores de seguridad (SID) conocidos no se utilizan para determinar los permisos efectivos:

a) Inicio de sesión anónimo.

b) Lote, Grupo de creador.

c) Acceso telefónico.

d) Controladores de dominio empresariales.

e) Interactivo.

f) Red.

g) Proxy.

h) Restringido.

i) Remoto.

j) Servicio.

k) Sistema.

l) Usuario de Terminal Server.

m) Otra organización.

n) Esta organización

Además, los permisos de recurso compartido no son parte del cálculo de permisos efectivos. El acceso a los recursos compartidos se puede denegar a través de los permisos de recurso compartido incluso cuando el acceso se permite mediante permisos NTFS.

Los siguientes factores no se usan con el fin de determinar permisos efectivos para objetos a los que se tiene acceso remoto:

a) Pertenencia a grupos locales.

b) Privilegios locales.

c) Permisos de recurso compartido.

Los permisos efectivos se basan en una evaluación local de la pertenencia al grupo del usuario, los privilegios de usuario y los permisos. Si el recurso que se consulta se encuentra en un equipo remoto, los permisos efectivos que se muestran no incluirán los permisos concedidos o denegados al usuario a través del uso de un grupo local en el equipo remoto.

Existen Permisos especiales (permisos avanzados) que permiten agregar acciones adicionales a los permisos locales o NTFS. Estos permisos son descritos a continuación además de incluir como se aplican dependiendo de los permisos locales que posea el recurso.

Cada uno de los permisos locales (NTFS) se compone de un grupo lógico de permisos especiales que se enumeran y definen a continuación. No todos los permisos especiales se aplicarán a todos los objetos.

Permiso	Descripción
Recorrer carpeta / Ejecutar archivo	El permiso "Recorrer carpeta" permite o deniega el movimiento por las carpetas para llegar a otros archivos o directorios, incluso si el usuario no tiene permisos para las carpetas recorridas. Este permiso sólo surte efecto si no se otorga al grupo o usuario el derecho de usuario "Omitir comprobación de recorrido" en la Consola de administración de directivas de grupo. De forma predeterminada, el grupo "Todos" tiene el derecho de usuario "Omitir comprobación de recorrido". (Sólo afecta a carpetas). El permiso "Ejecutar archivo" permite o deniega la ejecución de archivos de programa. (Sólo afecta a los archivos). Al configurar el permiso "Recorrer carpeta" en una carpeta no se define de manera automática el permiso "Ejecutar archivo" en todos los archivos de esa carpeta.
Listar carpeta / Leer datos	El permiso "Listar carpeta" permite o deniega ver nombres de archivos y subcarpetas de la carpeta. Este permiso sólo afecta al contenido de esa carpeta, con independencia de si la carpeta en la que se configura el permiso aparecerá en la lista. (Sólo afecta a carpetas). El permiso "Leer datos" permite o deniega la vista de datos en archivos. (Sólo afecta a los archivos).
Leer atributos	Permite o deniega la vista de los atributos de un archivo o carpeta, como sólo lectura y oculto. Los atributos se definen mediante NTFS.
Atributos extendidos de lectura	Permite o deniega la vista de atributos extendidos de un archivo o carpeta. Los atributos extendidos se definen mediante programas y pueden variar según el programa.
Crear archivos / Escribir datos	El permiso "Crear archivos" permite o deniega la creación de archivos dentro de la carpeta. (Sólo afecta a carpetas). El permiso "Escribir datos" permite o deniega la realización de cambios en el archivo y la sobrescritura del contenido existente. (Sólo afecta a los archivos).
Crear carpetas o agregar datos	El permiso "Crear carpetas" permite o deniega la creación de carpetas dentro de la carpeta. (Sólo afecta a carpetas). El permiso "Agregar datos" permite o deniega la realización de cambios al final del archivo, pero no el cambio, eliminación ni sobrescritura de los datos existentes. (Sólo afecta a los archivos).

Permiso	Descripción
Atributos de escritura	Permite o deniega el cambio de los atributos de un archivo o de una carpeta, como sólo lectura y oculto. Los atributos se definen mediante NTFS. El permiso “Atributos de escritura” no implica la creación o eliminación de archivos o carpetas, sólo incluye el permiso para realizar cambios en los atributos de un archivo o una carpeta.
Atributos extendidos de escritura	Permite o deniega el cambio de los atributos extendidos de un archivo o carpeta. Los atributos extendidos se definen mediante programas y pueden variar según el programa. El permiso “Atributos extendidos” de escritura no implica la creación o eliminación de archivos o carpetas, sólo incluye el permiso para realizar cambios en los atributos de un archivo o una carpeta.
Eliminar subcarpetas y archivos	Permite o deniega la eliminación de subcarpetas y archivos, incluso si no se ha otorgado el permiso “Eliminar” en la subcarpeta o archivo.
Eliminar	Permite o deniega la eliminación del archivo o de la carpeta. Si no ha obtenido el permiso “Eliminar” en un archivo o carpeta, podrá eliminarlo si se le ha otorgado el permiso “Eliminar subcarpetas y archivos” en la carpeta principal.
Permisos de lectura	Permite o deniega la lectura de los permisos del archivo o carpeta, como “Control total”, “Leer” y “Escribir”.
Cambiar permisos	Permite o deniega el cambio de los permisos del archivo o carpeta, como “Control total”, “Leer” y “Escribir”.
Tomar posesión	Permite o deniega la toma de posesión del archivo o de la carpeta. El propietario de un archivo o de una carpeta siempre puede cambiar los permisos, independientemente de los permisos existentes.
Sincronizar	Permite o deniega a diferentes subprocesos que esperen al identificador de archivo o carpeta y que se sincronicen con otro subproceso que pueda enviarle señales. Este permiso sólo se aplica a programas multiproceso y de varios subprocesos.

En la siguiente tabla se muestran las limitaciones de acceso para cada conjunto de permisos NTFS especiales.

Permisos especiales	Control total	Modificar	Leer y Ejecutar	Mostrar el contenido de la carpeta (sólo en carpetas)	Lectura	Escritura
Recorrer carpeta / Ejecutar archivo	X	X	X	X		
Listar carpeta / Leer datos	X	X	X	X	X	
Atributos de lectura	X	X	X	X	X	
Atributos extendidos de lectura	X	X	X	X	X	
Crear archivos / Escribir datos	X	X				X
Crear carpetas / Anexar datos	X	X				X
Atributos de escritura	X	X				X
Atributos extendidos de escritura	X	X				X
Eliminar subcarpetas y archivos	X					
Eliminar	X	X				
Permisos de lectura	X	X	X	X	X	X
Cambiar permisos	X					
Tomar posesión	X					
Sincronizar	X	X	X	X	X	X

Es importante además tener en consideración los siguientes factores:

a) Aunque los permisos “Mostrar el contenido de la carpeta” y “Leer y ejecutar” parecen tener los mismos permisos especiales, se heredan de forma diferente. El permiso “Mostrar contenido de carpeta” lo heredan las carpetas y no lo heredan los archivos, y debería aparecer sólo cuando se ven los permisos de carpeta. El permiso “Leer y ejecutar” lo heredan los archivos y las carpetas, y siempre está presente cuando se ven los permisos de archivo o carpeta.

b) En esta versión de Windows, el grupo “Todos” no incluye el grupo “Inicio de sesión anónimo” de forma predeterminada, por lo que los permisos que se aplican al grupo “Todos” no afectan al grupo “Inicio de sesión anónimo”.

c) Los servidores de archivos de Windows Server 2016 proporcionan una interfaz de usuario donde los administradores pueden ver los permisos vigentes de los usuarios en archivos o carpetas, solucionar problemas de acceso y conceder acceso, según sea necesario.

6.3 AUDITORIA DE SEGURIDAD DE ACCESO A OBJETOS

La auditoría de seguridad es una de las herramientas más eficaces para mantener la seguridad de una organización.

Uno de los principales objetivos de las auditorías de seguridad es el cumplimiento de las normas. Como parte de la gestión de un sistema de seguridad, la trazabilidad recoge una de las dimensiones fundamentales para poder evaluar incidencias de seguridad. Los registros de eventos que proporciona el servidor de ficheros, permitirán que una organización trace dicha incidencia en aspectos fundamentales tales como el cuándo, quién y/o desde dónde.

Las auditorías de seguridad ayudan a detectar comportamientos anómalos, a identificar y mitigar brechas en las directivas de seguridad y a impedir el comportamiento irresponsable mediante la creación de un registro de la actividad del usuario que puede utilizarse para un análisis forense.

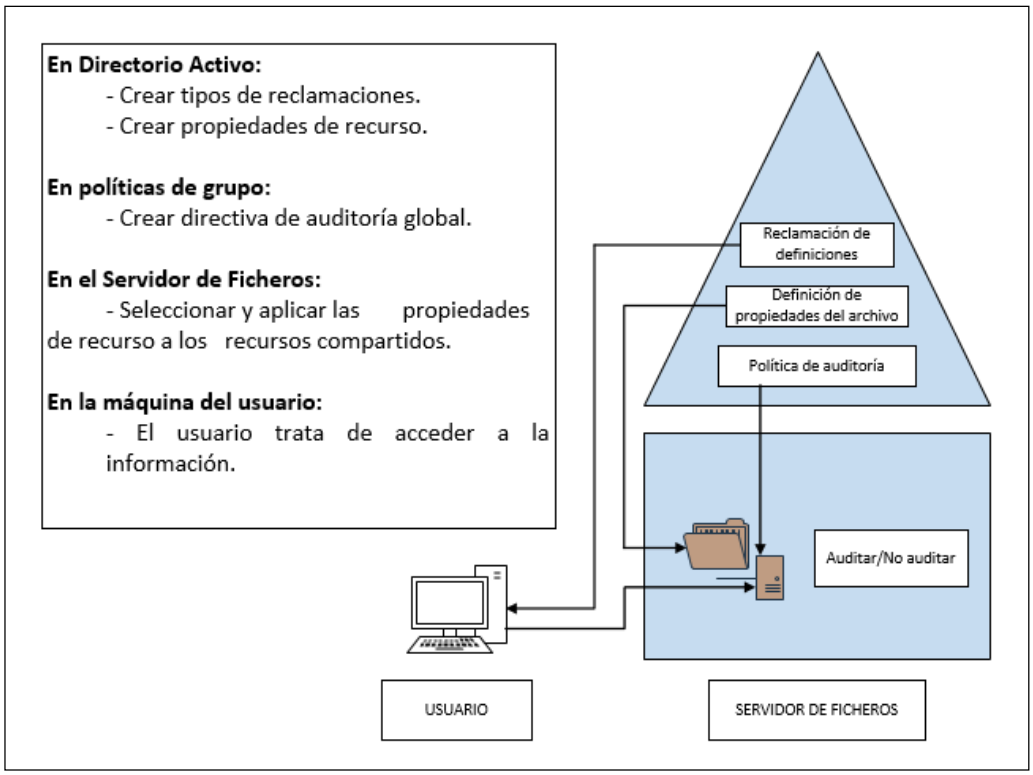
Auditar el acceso a objetos permite identificar que usuario ha obtenido acceso a un objeto como, por ejemplo, un archivo, una carpeta, una clave de Registro, una impresora, etc., que tiene su propia lista de control de acceso.

Con Windows Server 2016, es posible crear directivas de auditoría utilizando notificaciones y propiedades de recursos. Esto genera directivas de auditoría más avanzadas, más concretas y más fáciles de administrar.

Un elemento a considerar para la auditoría podría ser el siguiente ejemplo. La necesidad de auditar a todos los que no tienen permiso sobre una carpeta crítica e intentan obtener acceso a un documento clasificado. La auditoría debería contemplar el recoger toda la actividad de los usuarios, para todos los accesos bien en la carpeta o en el documento concreto.

Windows Server 2016 mejora los eventos de acceso a datos existentes con notificaciones de usuario, equipo y recursos. Estos eventos se generan por servidor. Para proporcionar una vista completa de los eventos de la organización, Microsoft está trabajando con asociados que proporcionan herramientas de recopilación y análisis de eventos, como los Servicios de recopilación de auditorías de System Center Operations Manager.

La siguiente figura muestra un ejemplo de auditoria de seguridad central:



Configurar y utilizar auditorías de seguridad suele implicar los siguientes pasos generales:

a) Identificar el conjunto correcto de datos y usuarios que se deben supervisar.

b) Crear y aplicar las directivas de auditoría apropiadas.

c) Recopilar y analizar los eventos de auditoría.

d) Administrar y supervisar las directivas que se crearon.

7. ALMACENAMIENTO

Las unidades de almacenamiento son todos aquellos dispositivos, internos o externos, que almacenan la información de un sistema dado, de manera temporal o permanente.

Espacios de almacenamiento es un subsistema de almacenamiento que se incluye en Windows y que le permite agrupar discos estándar (como discos Serial ATA o Serial Attached SCSI) en uno o varios grupos de almacenamiento, y después crear discos virtuales conocidos como “Espacios de almacenamiento” desde la funcionalidad disponible en los Grupos de almacenamiento.

Espacios de almacenamiento ofrece resistentes funciones de virtualización de almacenamiento para implementaciones físicas o virtuales críticas. Con los espacios de almacenamiento, la pila de almacenamiento de Windows se ha mejorado fundamentalmente para incorporar dos nuevas abstracciones:

a) Grupos de almacenamiento. Conjunto de discos físicos que permiten agregar discos, ampliar la capacidad de una forma flexible y delegar la administración.

b) Espacios de almacenamiento. Discos virtuales creados a partir de espacio libre en un grupo de almacenamiento. Los espacios de almacenamiento tienen atributos tales como nivel de resistencia, capas de almacenamiento, aprovisionamiento fijo y control administrativo preciso.

La Desduplicación de datos permite reducir la cantidad de bloques de datos duplicados en almacenamiento, pudiendo almacenar en una capacidad de almacenamiento determinada muchos más datos de lo que permitían las versiones anteriores que usaban almacenamiento de instancia única (SIS) o la compresión del sistema de archivos NTFS.

7.1 ESPACIOS DE ALMACENAMIENTO

Los Espacios de almacenamiento permiten disponer de soluciones de almacenamiento rentables, de alta disponibilidad, escalables y flexibles para implementaciones físicas o virtuales. Espacios de almacenamiento ofrece una sofisticada funcionalidad de virtualización de almacenamiento que permite a los clientes usar almacenamiento estándar para implementaciones multinodo escalables o implementaciones de un solo servidor.

Después de agrupar los discos físicos en Grupos de almacenamiento, puede crear discos virtuales desde la capacidad disponible sin tener que administrar individualmente cada disco físico. Con esta agregación de discos se logra un uso más eficaz de la capacidad en disco, se agrega almacenamiento fácilmente sin impacto para los usuarios y se delega la administración del almacenamiento a quien se desee. En Windows Server 2016, puede usar grupos de almacenamiento con Espacios de almacenamiento o con subsistemas de almacenamiento que no sean de Microsoft, incluidos los subsistemas que usan el estándar SMI-S.

Los Espacios de almacenamiento y los Grupos de almacenamiento reducen los costos de administración, ya que los administradores dedican menos tiempo a aprovisionar el almacenamiento. También simplifican las tareas de administración, de modo que los administradores que no están especializados en almacenamiento pueden configurar y administrar almacenamiento resistente y de alta disponibilidad. Espacios de almacenamiento también supone un ahorro de costos de hardware, gracias al uso de discos estándar del sector para el almacenamiento resistente con alta disponibilidad.

Con los Grupos de almacenamiento, en lugar de administrar cada disco de manera individual, se agregan discos físicos a uno o más grupos y, a continuación, se crean discos virtuales a partir de la capacidad disponible (Espacios de almacenamiento). Tras ello, se crean volúmenes en los discos virtuales, como si fueran discos físicos. Cuando la capacidad disponible en el grupo empieza a ser escasa, basta con crear más Espacios de almacenamiento o añadir más discos físicos al Grupo de almacenamiento.

Los discos virtuales también proporcionan aprovisionamiento dinámico, lo que significa que la capacidad del grupo se usa solo en función del tamaño de los archivos que se copian en los discos virtuales, y no del tamaño del disco virtual que cree. Por ejemplo, un disco virtual de 10 TB podría consumir 100 MB de capacidad del grupo si todavía no se han copiado muchos archivos en el disco.

Nota: Se recomienda usar discos duros virtuales de tamaño fijo para las máquinas virtuales que se ejecutan en un entorno de producción. Dado que al crear un disco duro virtual de tamaño fijo se asigna una cantidad de espacio fija en el almacenamiento físico subyacente, puede asegurarse de que haya espacio de almacenamiento suficiente para todos los discos duros virtuales que cree. Esto le ayudará a evitar quedarse sin espacio de almacenamiento, como puede ocurrir al usar discos duros virtuales de expansión dinámica, que van aumentando de tamaño a medida que se van escribiendo datos en ellos.

A continuación, se exponen las características más importantes de las que disponen los Espacios de almacenamiento:

a) Capas de almacenamiento: permite crear discos virtuales compuestos por dos capas de almacenamiento:
   i. Capa de la unidad de estado sólido para datos con acceso frecuente.
   ii. Capa de la unidad de disco duro para datos con acceso menos frecuente.

   Esta funcionalidad mueve automáticamente los datos con acceso frecuente a un almacenamiento más rápido (unidad de estado sólido o SSD) y los datos con acceso infrecuente a un almacenamiento más lento (disco duro o HD).

   Las Capas de almacenamiento combinan los mejores atributos de las unidades de estado sólido y las unidades de disco duro. Aumentan el rendimiento de los datos más usados ("activos") al moverlos a unidades de estado sólido sin sacrificar la capacidad de almacenar grandes cantidades de datos en los económicos discos duros.

   Los siguientes aspectos funcionan de manera diferente con las Capas de almacenamiento:
   i. Para crear un Espacio de almacenamiento con Capas de almacenamiento, el Grupo de almacenamiento debe tener una cantidad suficiente de discos duros y unidades de estado sólido para admitir la distribución de almacenamiento seleccionado y los discos duros deben tener suficiente espacio libre.
   ii. Al crear un Espacio de almacenamiento mediante el Asistente para nuevo disco virtual, puede especificar que desea crear el disco virtual con capas de almacenamiento.
   iii. Para crear un Espacio de almacenamiento con Capas de almacenamiento, el disco virtual debe usar un aprovisionamiento fijo y el número de columnas debe ser idéntico en ambas capas (un reflejo bidireccional de cuatro columnas con Capas de almacenamiento requeriría ocho unidades de estado sólido y ocho unidades de disco duro).
   iv. Los volúmenes que se creen en discos virtuales que usen Capas de almacenamiento deben tener el mismo tamaño que el disco virtual.

b) Caché con reescritura: los Espacios de almacenamiento puede usar las unidades de estado sólido existentes en el Grupo de almacenamiento para crear una caché con reescritura tolerante a caídas del suministro eléctrico y que almacene en búfer pequeñas operaciones de escritura aleatorias en unidades de estado sólido antes de escribirlas posteriormente en las unidades de disco duro.

A menudo, las pequeñas operaciones de escritura aleatorias dominan las cargas de trabajo habituales de las organizaciones y pueden influir en el rendimiento de otras transferencias de datos que se estén realizando. Con el uso de unidades de estado sólido (que son excelentes para el acceso aleatorio) para una caché con reescritura, los Espacios de almacenamiento pueden reducir la latencia de las operaciones de escritura aleatorias y reducir enormemente la influencia en el rendimiento de otras transferencias de datos.

La Caché con reescritura es transparente para los administradores y los usuarios y se crea en todos los discos virtuales nuevos si hay suficiente cantidad de unidades de estado sólido en el Grupo de almacenamiento, según lo determinen los siguientes requisitos del espacio de almacenamiento asociado:

i. Los espacios simples requieren una unidad de estado sólido.

ii. Los espacios reflejados bidireccionales y los espacios de paridad única requieren dos unidades de estado sólido.

iii. Los espacios reflejados tridireccionales y los espacios de paridad dual requieren tres unidades de estado sólido.

La Caché con reescritura funciona con todos los tipos de espacios de almacenamiento, incluidos los que tienen Capas de almacenamiento.

De manera predeterminada, los Espacios de almacenamiento recién creados usan automáticamente una Caché con reescritura de 1 GB cuando el Grupo de almacenamiento contiene suficientes discos físicos con Tipo de medio establecido en SSD o Uso establecido en Diario para admitir la configuración de resistencia especificada. Si no hay suficientes discos físicos con esta configuración, el tamaño de la caché con reescritura se establece en 0, excepto en los espacios de paridad, en los que se establece en 32 MB.

c) Paridad dual: permite almacenar dos copias de la información de paridad en un espacio de paridad, lo que protege frente a dos errores de disco simultáneos.

La paridad dual permite mantener un alto nivel de resistencia al usar un espacio de paridad con gran cantidad de discos o cada vez que necesite protegerse contra dos errores de disco simultáneos.

El tipo de resistencia de paridad dual es una opción al crear discos virtuales en el Administrador del servidor

d) Ahora, Espacios de almacenamiento incluye la capacidad de volver a generar automáticamente espacios de almacenamiento a partir del espacio libre en el grupo de almacenamiento en lugar de usar reservas activas.

Se tarda menos en volver a generar los espacios de almacenamiento, ya que varios discos del grupo pueden aceptar los datos que se almacenaban en el disco que ha sufrido el error en lugar de esperar a que una sola reserva activa escriba todos los datos. Además, ya no es necesario disponer de unidades de reserva activa y el espacio libre en el grupo de almacenamiento puede proporcionar capacidad y rendimiento adicionales al grupo.

Cuando se produce un error en un disco físico, en lugar de escribir una copia de los datos que se encontraban en el disco que ha sufrido el error en una única reserva activa, los datos se copian en varios discos físicos del grupo para lograr el nivel anterior de resistencia. Los administradores ya no necesitan asignar discos físicos como reservas activas en el grupo de almacenamiento.

e) Arquitectura multiempresa. La administración de grupos de almacenamiento puede controlarse mediante listas de control de acceso (ACL) y puede delegarse en función de cada grupo. De esta manera, es posible admitir escenarios de hospedaje que requieran el aislamiento de inquilinos (empresas). Los espacios de almacenamiento cumplen con el conocido modelo de seguridad de Windows; por lo tanto, pueden integrarse completamente con los Servicios de dominio de Active Directory.

La tecnología Espacios de almacenamiento tiene los siguientes requisitos:

a) Está soportado en los siguientes sistemas operativos: Windows Server 2016, Windows Server 2012 R2, Windows Server 2012 o Windows 10.

b) Discos conectados serie ATA (SATA) o SCSI conectados en serie (SAS), de manera opcional, en un contenedor de un grupo de discos (JBOD).

c) Los adaptadores RAID, si se usan, deben tener todas las funciones deshabilitadas y no deben interferir con los dispositivos conectados, incluidos los servicios de contenedor que proporciona un JBOD.

Existen tres tipos diferentes de espacios de almacenamiento, denominados almacenamiento resistente (tipos de resistencia), con características únicas que los hacen más o menos indicados para almacenar diferentes tipos de archivos. Estos espacios son los siguientes:

a) Los espacios simples: están diseñados para aumentar el rendimiento, pero no guardan varias copias de los archivos por lo que no los protegen en caso de errores de la unidad. Son más indicados para datos temporales (como archivos de representación de vídeo), archivos temporales de editores de imagen y archivos de objeto de compilador intermedios. Los espacios simples requieren al menos una unidad.

b) Los espacios de espejo: están diseñados para aumentar el rendimiento y guardar más de una copia de los archivos para protegerlos contra errores de la unidad. Los espacios de reflejo doble realizan dos copias de los archivos y pueden tolerar errores en una unidad, mientras que los espacios de reflejo triple pueden tolerar errores en dos unidades. Están indicados para almacenar una amplia variedad de datos, desde un recurso compartido de archivos de uso general a una biblioteca de VHD. Cuando un espacio de reflejo se formatea con el Sistema de archivos resistente (ReFS), Windows mantiene automáticamente la integridad de los datos, lo que hace que los archivos sean aún más resistentes ante errores de la unidad. Los espacios de reflejo doble necesitan al menos dos unidades, y los espacios de reflejo triple necesitan al menos cinco.

c) Los espacios de paridad están diseñados para aumentar la eficiencia del almacenamiento y guardar más de una copia de los archivos para protegerlos en caso de errores de la unidad. Los espacios de paridad están indicados para el archivo de datos y medios de streaming, como música y vídeos. Este diseño de almacenamiento requiere al menos tres unidades para protegerte en caso de error de una unidad, y al menos siete unidades para protegerte en caso de error de dos unidades.

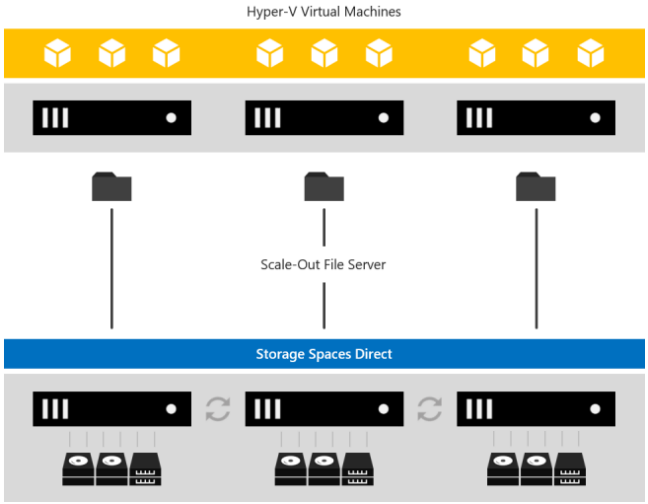
7.1.1 ESPACIOS DE ALMACENAMIENTO DIRECTO

Espacios de almacenamiento directo presenta una memoria caché del lado del servidor integrada para maximizar el rendimiento del almacenamiento. Se trata de una caché de lectura y escritura grande, persistente y en tiempo real. La memoria caché se configura automáticamente cuando se habilita espacios de almacenamiento directo. En la mayoría de los casos, no se necesita administración manual. El funcionamiento de la memoria caché depende de los tipos de unidades presentes.

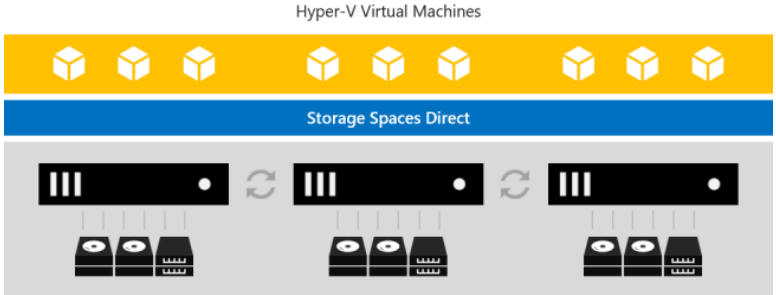
Espacios de almacenamiento directos se incluye en Windows Server 2016 Datacenter y en las versiones preliminares de Windows Server.

Para implementar esta funcionalidad se puede realizar mediante dos métodos, Convergido e Hyperconvergido.

a) Despliegue Convergido: consiste en separar los servidores de Hyper-V de otros que tengan activada esta característica. Para comunicarse a través de la red utilizaran los recursos compartidos de archivos SMB3. Es utilizada para implementaciones a gran escala como Hyper-V IaaS.



b) Despliegue Hiperconvergido: ejecuta las máquinas virtuales Hyper-V o las bases de datos de SQL Server directamente en los servidores que proporcionan el almacenamiento, almacenando sus archivos en los volúmenes locales. Esto elimina la necesidad de configurar el acceso y los permisos del servidor de archivos, y reduce los costos de hardware para las pequeñas y medianas empresas o las implementaciones remotas de oficinas / sucursales.



7.1.2 RÉPLICA DE ALMACENAMIENTO

La característica de réplica de almacenamiento ofrece nuevas funciones de preparación y recuperación ante desastres en Windows Server 2016 Datacenter Edition. Es una tecnología de que permite la replicación de volúmenes entre servidores o clústeres para la recuperación ante desastres. También permite crear clústeres de conmutación por error ampliados que abarcan dos sitios y que tienen todos los nodos sincronizados.

La réplica es admitida de forma síncrona y asíncrona:

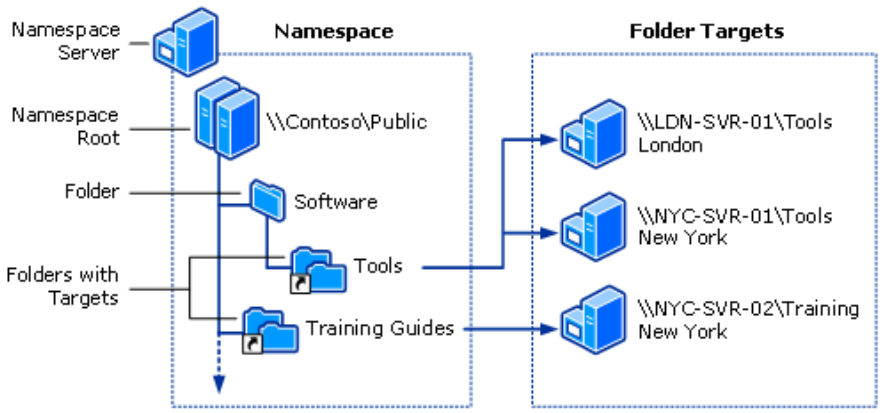
a) La replicación síncrona refleja los datos en lugar de red de baja latencia con volúmenes frente a bloqueos de forma que se asegure que no hay ninguna pérdida de datos a nivel de sistema de archivos durante un error.

b) La replicación asíncrona refleja los datos para redes con latencias superiores, sin embargo, no se garantiza que ambos lugares tengan copias idénticas de datos en el momento del error.

A diferencia de otros productos, Réplica de almacenamiento incorpora tecnología puntera en el ámbito de la seguridad. Esto incluye la firma de paquetes, el cifrado completo de datos de AES-128-GCM, la compatibilidad con la aceleración del cifrado de Intel AES-NI y la prevención de ataque de tipo "Man in the middle" mediante la integridad por autenticación previa. Además, Réplica de almacenamiento utiliza Kerberos AES256 para toda la autenticación entre los nodos.

7.1.3 ESPACIOS DE NOMBRES DFS

Espacios de nombres DFS es un rol de Windows Server que permite agrupar las carpetas compartidas ubicadas en distintos servidores en uno o varios espacios de nombres con una estructura lógica. De esta forma se permite a los usuarios una vista virtual de las carpetas compartidas, donde una única ruta de acceso conduce a los archivos ubicados en varios servidores, tal y como se muestra en la siguiente imagen:



7.1.4 REFS

El Sistema de archivos resistente (ReFS) fue introducido por primera vez en Windows Server 2012, está diseñado para maximizar la disponibilidad de los datos, escalar de manera eficiente a conjuntos de datos de gran tamaño en diversas cargas de trabajo y proporciona la integridad de los datos por medio de la resistencia a los daños. Esta característica intenta solucionar un creciente conjunto de escenarios de almacenamiento y establecer una base para futuras innovaciones.

Este sistema de archivos presenta las siguientes ventajas:

a) Resistencia: Se pueden detectar daños con precisión y también solucionarlos mientras está en línea, ayudando a proporcionar mayor integridad y disponibilidad de los datos.

b) Rendimiento: Presenta nuevas características para cargas de trabajo

   i. Paridad acelerada por reflejos: La paridad acelerada por reflejos ofrece alto rendimiento, así como una capacidad de almacenamiento eficiente para los datos.

   ii. Operaciones de VM con aceleración: ReFS presenta nuevas funcionalidades especialmente dirigidas a mejorar el rendimiento de las cargas de trabajo virtualizadas como el bloque de clonación y el VDL disperso.

   iii. Tamaños variables de clúster: ReFS admite tamaños de clúster de entre 4KB y 64 KB

c) Escalabilidad: está diseñado para admitir grandes grupos de datos sin que tenga un impacto negativo en el rendimiento, consiguiendo una mayor escalabilidad que sistemas anteriores.

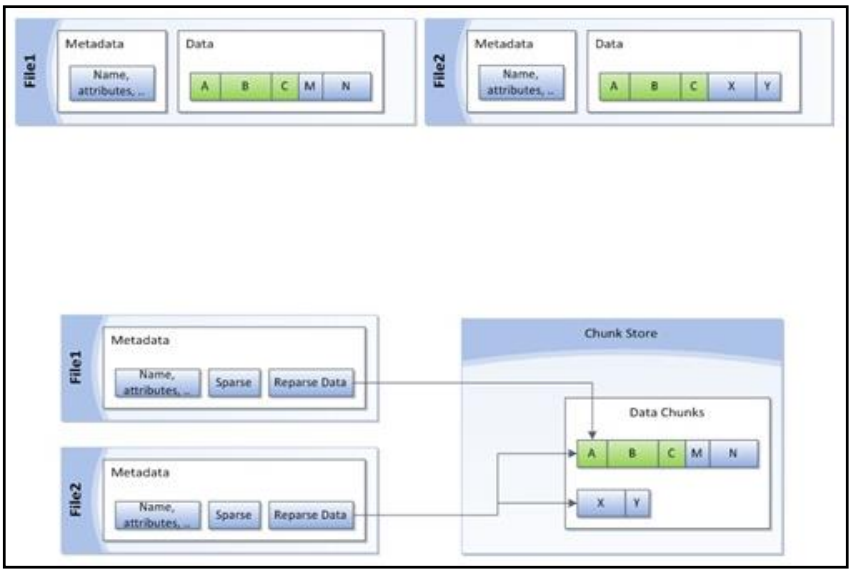
7.2 DESDUPLICACIÓN DE DATOS

Nota: Según el fabricante se recomienda que se instale la actualización "KB4025334" del 18 de julio de 2017 al usar Desduplicación de datos con Windows Server 2016, que contiene un conjunto de correcciones importantes de confiabilidad. Para más información consulte el siguiente enlace: https://support.microsoft.com/kb/4025334

La desduplicación de datos implica detectar y eliminar la duplicación en los datos sin comprometer su fidelidad o integridad. El objetivo es almacenar más datos en menos espacio al segmentar archivos en pequeños fragmentos de tamaño variable (32–128 KB), identificar fragmentos duplicados y mantener una sola copia de cada fragmento.

Las copias redundantes de los fragmentos se reemplazan por una referencia a la copia única. Los fragmentos se comprimen y se organizan en archivos de contenedor especiales de la carpeta de información de volumen del sistema.

El resultado es una transformación en disco de cada archivo, como se muestra en la siguiente imagen:



Después de la desduplicación, los archivos ya no se almacenan como secuencias de datos independientes y se reemplazan por rutas internas que apuntan a bloques de datos que se almacenan en un almacén de fragmentos común. Dado que estos archivos comparten bloques, esos bloques solo se almacenan una vez, lo que reduce el espacio en disco necesario para almacenar todos los archivos. Durante el acceso a los archivos, los bloques correctos se ensamblan de manera transparente para proporcionar los datos sin llamar a la aplicación y sin que el usuario tenga conocimiento de la transformación en disco en el archivo. Esto permite a los administradores aplicar la desduplicación a archivos sin tener que preocuparse por cualquier cambio en el comportamiento de las aplicaciones o el impacto de los usuarios sobre esos archivos.

Después de habilitar un volumen para desduplicación y de optimizar los datos, el volumen contiene lo siguiente:

a) Archivos sin optimizar. Por ejemplo, entre los archivos sin optimizar se podrían encontrar archivos que no cumplen la opción de directiva de antigüedad de archivo, archivos de estado del sistema, secuencias de datos alternas, archivos cifrados, archivos con atributos extendidos, archivos menores de 32 KB, otros archivos de punto de repetición de análisis o archivos que otras aplicaciones están usando (el límite de "en uso" se elimina en Windows Server 2012 R2).

b) Archivos optimizados. Archivos que se almacenan como puntos de repetición de análisis y que contienen punteros a un mapa de los fragmentos correspondientes en el almacén de fragmentos que es necesario restaurar cuando se solicite el archivo.

c) Almacén de fragmentos. Ubicación de los datos de archivos optimizados.

d) Espacio libre adicional. Los archivos optimizados y el almacén de fragmentos ocupan mucho menos espacio que antes de la optimización.

Para abordar el crecimiento del almacenamiento de datos en la organización, los administradores consolidan servidores y hacen de la escalabilidad, de la capacidad y de la optimización de los datos sus principales objetivos. La desduplicación de datos proporciona formas prácticas de lograr estos objetivos, entre ellas:

a) Optimización de la capacidad. La desduplicación de datos almacena más datos en menos espacio físico. Logra más eficacia de almacenamiento que la que ofrecían características como la compresión NTFS o Almacenamiento de instancia única (SIS). La desduplicación de datos usa la compresión y fragmentación de tamaño variable en subarchivos, lo que reporta una relación de optimización del almacenamiento de 2:1 en los servidores de archivos generales, y de hasta 20:1 en los datos de virtualización.

b) Escalabilidad y rendimiento. La desduplicación de datos es sumamente escalable, eficiente en cuanto a uso de recursos y no intrusiva. Se puede ejecutar en varios volúmenes simultáneamente sin afectar a otras cargas de trabajo en el servidor. El escaso impacto que tiene en las cargas de trabajo del servidor se consigue limitando los recursos de CPU y memoria que se consumen. Si el servidor se carga con mucho trabajo, la desduplicación puede detenerse por completo. Además, los administradores tienen la posibilidad de ejecutar los trabajos de desduplicación de datos en cualquier momento, programar cuándo se ejecutará la desduplicación de datos y establecer directivas de selección de archivos.

c) Confiabilidad e integridad de los datos. Cuando se aplica la desduplicación de datos, se mantiene la integridad de los datos. La desduplicación de datos usa la suma de comprobación, la coherencia y la validación de identidad a fin de asegurar la integridad de los datos. Para todos los metadatos y los datos a los que se haga referencia con más frecuencia, la desduplicación de datos mantiene la redundancia para garantizar que los datos puedan recuperarse en caso de corrupción de datos.

d) Eficacia de ancho de banda con BranchCache. A través de la integración con BranchCache, se aplican las mismas técnicas de optimización a los datos que se transfieren a través de la WAN a una sucursal. El resultado son tiempos de descarga de archivos más rápidos y consumo reducido de banda ancha.

e) Administración de optimización con herramientas conocidas. La desduplicación de datos tiene una funcionalidad de optimización integrada en el Administrador de servidores.

Para aprovechar las ventajas de la desduplicación de datos, el entorno debe cumplir los siguientes requisitos:

a) Servidor: un equipo o una máquina virtual de Windows Server 2016 con al menos un volumen de datos.

b) (Opcional) Otro equipo o máquina virtual que ejecute Windows Server 2016 y que esté conectado al servidor a través de la red.

Es importante además que, si la desduplicación de datos se realiza en cargas de trabajo de VDI o de copia de seguridad virtualizada, todos los archivos VHD deben cumplir los siguientes requisitos:

a) Estar almacenados en un servidor de archivos que ejecuta Windows Server 2016, y el nodo de almacenamiento y el nodo de cálculo estar ejecutándose en distintos servidores.

b) Estar almacenados en almacenamiento local en una configuración hiperconvergente limitada específica.

Desduplicación de datos en Windows Server 2016 se ha optimizado con las siguientes novedades:

a) Admite datos de tamaños de volúmenes de hasta 64TB.

b) Los archivos de hasta 1 TB son totalmente compatibles.

c) Se ha agregado un nuevo tipo de uso predeterminado (Copia de seguridad) para una implementación fluida de Desduplicación de datos para aplicaciones virtualizadas de copia de seguridad.

d) Ahora es totalmente compatible con la nueva característica Actualización gradual de sistema operativo de clúster de Windows Server 2016.

e) Como nuevas características destacan la compatibilidad con la nueva opción de implementación de Windows Server 2016, Nano Server, copias de seguridad simplificada y actualizaciones graduales de sistema operativo en clúster.

8. GESTIÓN DE ARCHIVOS

El Administrador de recursos del servidor de archivos, que se usó por primera vez con el sistema operativo Windows Server 2003 R2, es un conjunto de herramientas del sistema operativo Windows Server 2016 que permite a los administradores aplicar límites de almacenamiento a volúmenes y carpetas, impedir a los usuarios que guarden tipos de archivos concretos en el servidor y generar informes completos de almacenamiento. El Administrador de recursos del servidor de archivos no solamente ayuda a los administradores a controlar y supervisar de una manera eficaz los recursos de almacenamiento existentes desde un lugar centralizado, sino que también les ayuda a planear e implementar cambios futuros en la infraestructura de almacenamiento.

El “Administrador de recursos del servidor de archivos” proporciona un conjunto de características que permite administrar y clasificar los datos almacenados en los servidores de ficheros.

El “Administrador de recursos del servidor de archivos” incluye las siguientes características:

a) **Infraestructura de clasificación de archivos:** la infraestructura de clasificación de archivos permite obtener una idea clara de los datos mediante la automatización de los procesos de clasificación con el fin de poder administrar los datos de manera más eficaz. Puede clasificar archivos y aplicar directivas según esta clasificación. Entre las directivas de ejemplo está el control de acceso dinámico para restringir el acceso a archivos, el cifrado de archivos y la expiración de archivos. Los archivos pueden clasificarse de manera automática mediante reglas de clasificación de archivos o de forma manual, modificando las propiedades de un archivo o carpeta que se haya seleccionado.

b) **Tareas de administración de archivos:** las tareas de administración de archivos permiten aplicar una acción o directiva condicional en los archivos según su clasificación. Entre las condiciones de una tarea de administración de archivos están la ubicación del archivo, las propiedades de clasificación, la fecha en que se creó el archivo, la fecha de la última modificación del archivo o la última vez que se accedió al archivo. Las acciones que una tarea de administración de archivos puede llevar a cabo incluyen la capacidad de expirar archivos, cifrar archivos o ejecutar un comando personalizado.

c) **Administración de cuotas:** las cuotas limitan el espacio permitido para un volumen o carpeta y se pueden aplicar automáticamente a las nuevas carpetas que se creen en un volumen. También puede definir plantillas de cuota que se apliquen a los nuevos volúmenes o carpetas.

d) **Administración del filtrado de archivos:** el filtrado de archivos ayuda a controlar los tipos de archivos que el usuario puede almacenar en un servidor de ficheros. Puede limitar la extensión que se puede almacenar en los archivos compartidos. Por ejemplo, puede crear un filtrado de archivos que no permita que se almacenen archivos con extensión MP3 en las carpetas compartidas personales en un servidor de ficheros.

e) **Informes de almacenamiento:** los informes de almacenamiento sirven para identificar las tendencias de uso del disco y el modo en que los datos están clasificados. También puede supervisar un grupo de usuarios en concreto para detectar los intentos de guardar archivos no autorizados.

Las características incluidas en el Administrador de recursos del servidor de archivos se pueden configurar y administrar mediante la consola MMC del Administrador de recursos del servidor de archivos.

El Administrador de recursos del servidor de archivos admite únicamente volúmenes que estén formateados con el sistema de archivos NTFS. El sistema de archivos resistente a errores no se admite.

A continuación, se reflejan los cambios realizados en el Administrador de recursos del servidor de archivos en relación a sus funcionalidades:

a) Borrar valores de propiedad de clasificación que ya no se aplican a un archivo actualizado: permite borrar valores de propiedad que ya no se aplican a un archivo actualizado durante la reevaluación de los valores de propiedad de clasificación existentes.

   i. Este cambio permite al Administrador de recursos del servidor de archivos eliminar de manera dinámica los valores de clasificación que ya no se aplican a un archivo. Por ejemplo, es posible que tenga un archivo que se haya clasificado como confidencial porque contenía una cadena concreta, como "Privado". Si la cadena se elimina, el archivo ya no se considera confidencial después de realizar una reevaluación.

b) Establecer valores máximos para informes de almacenamiento: permite configurar el número máximo de archivos por informe de almacenamiento y configurar los valores máximos de los parámetros predeterminados de informes de almacenamiento específicos. Al configurar los parámetros predeterminados de un informe, también puede configurar los siguientes valores máximos:

   i. Para el informe Archivos duplicados, puede especificar el número máximo de archivos en un grupo duplicado por informe y el número máximo de grupos de archivos duplicados por informe.

   ii. Para el informe Archivos por grupo de archivos, puede especificar el número máximo de grupos de archivos duplicados por informe y el número máximo de archivos en cualquier grupo de archivos por informe.

   iii. Para el informe Archivos por propietario, puede especificar el número máximo de propietarios por informe y el número máximo de archivos por propietario e informe.

   iv. Para los informes Archivos por propiedad y Carpetas por propiedad, puede especificar el número máximo de valores de propiedad por informe y el número máximo de archivos para cada valor de propiedad. Tenga en cuenta que, si establece los valores de uno de estos tipos de informe, afectará a ambos tipos.

c) Control de acceso dinámico: en Windows Server 2016, puede aplicar la gestión de datos en todos los servidores de archivos para controlar quién puede acceder a la información y auditar quién ha accedido a ella. El control de acceso dinámico permite:

   i. Clasificar los archivos automática o manualmente para identificar datos.

   ii. Controlar el acceso a los archivos aplicando directivas de acceso centrales.

   iii. Auditar el acceso a los archivos por medio de directivas de auditoría centrales de informes de cumplimiento y análisis forenses.

d) Las organizaciones pueden definir directivas centrales de acceso y auditoría en Active Directory y usarlas para controlar quién puede acceder a la información y realizar un seguimiento de quién accedió a la información almacenada en los servidores de archivos.

e) Clasificación automática: la clasificación automática mediante la infraestructura de clasificación de archivos se ha mejorado en Windows Server 2016 en los siguientes aspectos:

   i. Clasificación continua. Configure la infraestructura de clasificación de archivos para clasificar los archivos pocos segundos después de su creación o modificación en el servidor de ficheros, sin necesidad de esperar a que llegue el momento programado para que se efectúe la clasificación.

   ii. Clasificador de Windows PowerShell. Clasifique un archivo automáticamente con un script de Windows PowerShell que determine la clasificación del archivo. El clasificador de Windows PowerShell facilita la implementación de una lógica de clasificación personalizada específica para su organización. Por ejemplo, puede clasificar un archivo en función de quién lo creó o modificó por última vez.

   iii. Clasificador de contenido mejorado. Especifique cantidad mínima y máxima de repeticiones de una cadena o expresión regular. Por ejemplo, puede clasificar un archivo que contiene más de diez números de la seguridad social como un archivo que contiene información de identificación personal.

   iv. Espacio de nombres dinámico para reglas de clasificación. Especifique el tipo de información que contiene una carpeta, como datos de aplicación, datos de grupos o datos de usuario y, a continuación, configure reglas de clasificación basadas en el tipo de información en el que quiera aplicarlas.

f) Clasificación manual: en la pestaña Clasificación de las propiedades del archivo en Windows Server 2016, la infraestructura de clasificación de archivos agrega la posibilidad de clasificar archivos de forma manual. También puede clasificar las carpetas de modo que cualquier archivo agregado a la carpeta clasificada herede las clasificaciones de la carpeta principal.

g) La clasificación manual brinda a los usuarios y propietarios de contenido la posibilidad de clasificar sus archivos y carpetas usando la hoja de propiedades de ese archivo o carpeta.

h) Tareas de administración de archivos: en Windows Server 2016, las tareas de administración de archivos se han actualizado en los siguientes aspectos:

   i. Tarea de administración de archivos de Active Directory Rights Management Services. Cifre automáticamente cualquier archivo que tenga un protector AD RMS cuando se cumpla una condición especificada. Puede seleccionar una plantilla de directiva de derechos de AD RMS existente o especificar la directiva manualmente.

   ii. Tareas continuas de administración de archivos. Configure tareas de administración de archivos para que se ejecuten pocos segundos después crear o modificar esos archivos en un servidor de ficheros, cuando las propiedades de clasificación están definidas como condición en la tarea de administración de archivos.

Nota: Las tareas de administración de archivos no se pueden establecer como continuas si ha configurado una notificación o si hay asignada una programación fija.

iii. Espacio de nombres dinámico para tareas de administración de archivos. Especifique el tipo de información que contiene una carpeta, como datos de aplicación, datos de grupos o datos de usuario y, a continuación, configure tareas de administración de archivos basadas en el tipo de información en el que quiera que se realicen.

i) Asistencia de acceso denegado: la asistencia de acceso denegado permite personalizar el mensaje de error de acceso denegado que se muestra cuando un usuario que ejecuta Windows 8 no puede acceder a un archivo o carpeta en un servidor de ficheros. Puede configurar el mensaje de error de modo que el usuario pueda solicitar acceso al archivo directamente desde el cuadro de diálogo. También puede especificar el grupo de usuarios al que se envía la solicitud de acceso mediante el Administrador de recursos del servidor de archivos.

j) La asistencia para acceso denegado se puede configurar en la directiva del grupo o en la consola del Administrador de recursos del servidor de archivos, en cada servidor de ficheros. También puede personalizar el mensaje de error por cada servidor de ficheros o tener un mensaje de error independiente para cada recurso compartido de archivos en el servidor de ficheros.

k) La asistencia de acceso denegado ayuda a los usuarios a solucionar problemas de acceso para que puedan acceder a los archivos y carpetas que necesitan de manera más eficiente.

8.1 CUOTAS DE DISCO

Es posible utilizar el Administrador de recursos del servidor de archivos para crear una cuota para un volumen o carpeta y limitar así el espacio en disco que se le asigna. El límite de la cuota se aplica a todo el subárbol de carpetas.

Puede crear una cuota máxima o una cuota de advertencia:

a) Una cuota máxima impide a los usuarios guardar archivos una vez alcanzado el límite de espacio y genera notificaciones cuando el volumen de datos llega al umbral configurado.

b) La cuota de advertencia no impone un límite de cuota, pero genera todas las notificaciones configuradas.

Para determinar qué sucede cuando la cuota se acerca al límite, se puede configurar umbrales de notificación. Para cada umbral que se defina, puede enviar notificaciones por correo electrónico, registrar un evento, ejecutar un comando o script, o generar informes de almacenamiento. Por ejemplo, es posible que se desee enviar una notificación al administrador y al usuario que guardó el archivo cuando una carpeta alcance el 85 por ciento del límite de su cuota, y enviar otra notificación cuando se alcance el límite de la cuota. En algunos casos, podría desear ejecutar un script que aumente el límite de la cuota automáticamente cuando se alcance un umbral.

Al crear una cuota en un volumen o una carpeta, puede basar la cuota en una plantilla de cuota o usar propiedades personalizadas. Es recomendable que, siempre que sea posible, base una cuota en una plantilla de cuota. Una plantilla de cuota se puede volver a usar para crear cuotas adicionales y simplifica el mantenimiento continuo de la cuota.

El Administrador de recursos del servidor de archivos también puede generar cuotas automáticamente. Al configurar una cuota automática, puede aplicar una plantilla de cuota a un volumen o una carpeta principal. Se crea una cuota basada en la plantilla para cada una de las subcarpetas existentes y se genera una cuota automáticamente para cada subcarpeta nueva que se cree.

En la siguiente tabla se muestran las ventajas de usar las herramientas de administración de cuotas en el Administrador de recursos del servidor de archivos en lugar de usar cuotas de disco NTFS.

Características de las cuotas	Administrador de recursos del servidor de archivo	Cuotas de disco NTFS
Seguimiento de cuotas	Por carpeta o por volumen	Por usuario en un volumen
Cálculo de uso de disco	Espacio real en disco	Tamaño de archivo lógico
Mecanismos de notificación	Correo electrónico, informes personalizados, ejecución de comandos o scripts, registros de eventos	Registros de eventos únicamente

Las cuotas creadas en el Administrador de recursos del servidor de archivos son totalmente independientes de las cuotas de NTFS que pueda haber creado; estos sistemas no están diseñados para usarse simultáneamente. No obstante, para facilitar la migración desde cuotas de NTFS, el Administrador de recursos del servidor de archivos proporciona plantillas de cuotas que ayudan a volver a crear las propiedades de las cuotas de NTFS.

Puede usar el Administrador de recursos del servidor de archivos en Windows Server 2016 para realizar las siguientes tareas:

a) Administrar cuotas:

   i. Crear, actualizar y obtener información de cuotas, que establecen un límite de espacio en un volumen o una carpeta.

   ii. Cuando el almacenamiento llega a un nivel predefinido, se envía un mensaje de correo electrónico a una lista de distribución, se registra un evento, se ejecuta un comando o script o bien se generan informes.

   iii. Establezca una cuota máxima para impedir que los usuarios superen un límite de almacenamiento o sencillamente para supervisar el almacenamiento en un volumen o una carpeta.

b) Generar cuotas automáticamente. Puede configurar el Administrador de recursos del servidor de archivos para que se aplique una cuota específica a todas las subcarpetas existentes y a cualquier subcarpeta nueva que se cree en un volumen o una carpeta. Por ejemplo, puede generar automáticamente cuotas estándar para los usuarios móviles o los usuarios nuevos de su organización.

c) Administrar filtros de archivos:

   i. Crear, actualizar y obtener información de los filtros de archivos, que controlan el tipo de los archivos que pueden guardar los usuarios.

   ii. Definir grupos de archivos que especifiquen las extensiones de archivo incluidas o excluidas en el filtrado personalizado.

   iii. Impedir activamente a los usuarios que guarden archivos no autorizados o sencillamente registrar los archivos de estos tipos que guarden los usuarios.

   iv. Crear reglas de excepciones de filtrado para carpetas determinadas.

   v. Cuando los usuarios intentan guardar archivos no autorizados, se desencadenan notificaciones por correo electrónico o de otro tipo.

d) Usar plantillas de cuotas y de filtrado de archivos:

   i. Reutilizar las reglas de administración de recursos en toda una organización, mediante la aplicación de límites de almacenamiento estándar o filtros de archivos a los volúmenes o carpetas nuevos.

   ii. Usar o modificar las plantillas integradas o crear plantillas nuevas para incorporar sus directivas del sistema.

   iii. Administrar las actualizaciones de cuotas o filtros de archivos desde una ubicación centralizada, mediante la actualización de las propiedades de las plantillas.

e) Ejecutar informes de almacenamiento:

   i. Elegir elementos de una extensa colección de informes incorporados y establecer parámetros de informes específicos para su entorno.

   ii. Programar informes periódicos para identificar las tendencias de uso de discos o las actividades de filtrado de archivos.

   iii. Generar instantáneamente informes a petición.

f) Administrar recursos remotos. Puede administrar recursos de almacenamiento en un servidor local o remoto mediante la ejecución del Administrador de recursos del servidor de archivos.

g) Realizar copia de seguridad y restauración de configuraciones de forma sencilla. La configuración del Administrador de recursos del servidor de archivos se guarda en la carpeta System Volume Information del directorio raíz del servidor y en cualquier volumen donde se apliquen cuotas o filtros de archivos. Para crear copias de seguridad y restaurar configuraciones del Administrador de recursos del servidor de archivos, puede usar una herramienta de copia de seguridad como Copias de seguridad de Windows Server.

El Administrador de recursos del servidor de archivos proporciona flexibilidad para crear, utilizar y administrar plantillas, tanto para cuotas como para filtros de archivos.

Una plantilla de cuota define un límite de espacio, el tipo de cuota (máxima o de advertencia) y un conjunto de notificaciones que se generarán cuando se acerque o supere el límite de la cuota.

Las plantillas de cuota simplifican la creación y el mantenimiento de cuotas:

a) Si usa una plantilla de cuota, puede aplicar un límite de almacenamiento estándar y un conjunto estándar de umbrales de notificación para muchos volúmenes y carpetas en los servidores de la organización.

b) Si basa las cuotas en una plantilla, puede actualizar automáticamente todas las cuotas basadas en una plantilla determinada mediante la edición de dicha plantilla. Esta característica simplifica el proceso de actualización de las propiedades de las cuotas proporcionando un punto central en el que los administradores de TI pueden realizar todos los cambios.

Por ejemplo, puede crear una plantilla de Cuota de usuario para aplicar un límite de 200 MB a la carpeta personal de cada usuario. Deberá crear para cada usuario una cuota basada en la plantilla Cuota de usuario y asignársela a la carpeta del usuario. Si posteriormente decide conceder a cada usuario espacio adicional en el servidor, sólo tiene que modificar el límite de espacio en la plantilla Cuota de usuario y elegir actualizar automáticamente cada cuota que se base en esa plantilla de cuota.

El Administrador de recursos del servidor de archivos proporciona varias plantillas de cuota. Por ejemplo:

a) Puede usar la plantilla Límite de 200 MB en informes a usuario para aplicar un límite máximo de 200 MB a la carpeta personal de cada usuario.

b) Para algunas carpetas, es posible que desee usar la plantilla Límite de 200 MB con extensión de 50 MB para aumentar automáticamente el límite de la cuota cuando se alcance un límite de cuota de 200 MB.

c) Otras plantillas predeterminadas están diseñadas para supervisar el uso del disco mediante cuotas de advertencia (por ejemplo, la plantilla Supervisar 200 GB de uso de volumen y la plantilla Supervisar 500 MB de recursos compartidos). Al usar estas plantillas, los usuarios pueden superar el límite de la cuota, pero cuando lo hacen se generan notificaciones de correo electrónico y del registro de eventos.

8.2 FILTRADO DE ARCHIVOS

Administración del filtrado de archivos: el filtrado de archivos ayuda a controlar los tipos de archivos que el usuario puede almacenar en un servidor de ficheros. Puede limitar las extensiones que se pueden almacenar en los archivos compartidos. Por ejemplo, puede crear un filtrado de archivos que no permita que se almacenen archivos con extensión MP3 en las carpetas compartidas personales en un servidor de ficheros.

En el nodo Administración del filtrado de archivos del complemento MMC del Administrador de recursos del servidor de archivos, puede realizar las siguientes tareas:

a) Crear filtros de archivos para controlar los tipos de archivos que los usuarios pueden guardar y generar notificaciones cuando los usuarios intenten guardar archivos no autorizados.

b) Definir plantillas de filtrado de archivos que puedan aplicarse a nuevos volúmenes o carpetas y que pueden utilizarse en toda una organización.

c) Crear excepciones de filtrado de archivos que amplíen la flexibilidad de las reglas de filtrado de archivos.

Es posible crear filtros de archivos para impedir que se guarden en un volumen o un árbol de carpetas los archivos que pertenezcan a grupos de archivos determinados. El filtro de archivos afecta a todas las carpetas de la ruta de acceso designada. Por ejemplo, se puede crear un filtro de archivos para impedir que los usuarios almacenen archivos de vídeo y audio en sus carpetas personales en el servidor.

De forma adicional se puede configurar el Administrador de recursos del servidor de archivos para que genere notificaciones por correo electrónico o de otro tipo cuando se produzca un evento de filtrado de archivos.

El filtro de archivos puede ser activo o pasivo:

a) El filtrado activo impide que los usuarios guarden tipos de archivo no autorizados en el servidor de ficheros.

b) El filtrado pasivo supervisa a los usuarios que guardan tipos de archivo específicos y genera las notificaciones configuradas, pero no les impide que guarden archivos.

El filtro de archivos no impide que los usuarios y las aplicaciones tengan acceso a los archivos que se guardaron en la ruta de acceso antes de que se creara el filtro de archivos, incluso si los archivos pertenecen a grupos de archivos bloqueados.

Para simplificar la administración de los filtros de archivos, es recomendable que se basen en plantillas de filtro de archivos. Las plantillas de filtro de archivos definen el tipo de filtrado que se debe realizar (activo o pasivo), un conjunto de grupos de archivos que se deben bloquear y un conjunto de notificaciones que se generarán cuando un usuario intente guardar un archivo no autorizado.

El Administrador de recursos del servidor de archivos proporciona varias plantillas de filtro de archivos por defecto, que sirven para bloquear archivos de audio y vídeo, ejecutables de imágenes y de correo electrónico, así como para satisfacer otras necesidades administrativas comunes.

Para lograr una mayor flexibilidad, es posible configurar una excepción al filtro de archivos en una subcarpeta de una ruta de acceso donde se haya creado un filtro de archivos. Cuando se coloca una excepción al filtro de archivos en una subcarpeta, permite que los usuarios guarden tipos de archivo que en otra situación se bloquearían con el filtro de archivos aplicado a la carpeta primaria.

Antes de empezar a trabajar con los filtros de archivos, es necesario comprender la función de los grupos de archivos. Los grupos de archivos se usan para definir un espacio de nombres para un filtro de archivos o una excepción al filtro de archivos, o bien para generar un informe de almacenamiento “Archivos por grupo de archivos”.

El grupo de archivos se compone de un conjunto de patrones de nombre de archivo que se agrupan en archivos incluidos y archivos excluidos:

a) Archivos incluidos: archivos que pertenecen al grupo.

b) Archivos excluidos: archivos que no pertenecen al grupo.

Por ejemplo, en el grupo de archivos “Archivos de audio”, podría incluir los siguientes patrones de nombre de archivo:

a) Archivos incluidos: *.mp*: incluye todos los archivos de audio creados en los formatos MPEG actuales y futuros (MP2, MP3, etc.).

b) Archivos excluidos: *.mpp: excluye los archivos creados en Microsoft Project (archivos .mpp), que, en caso contrario, se incluirían según la regla de inclusión anterior (*.mp*).

El Administrador de recursos del servidor de archivos proporciona varios grupos de archivos predeterminados que pueden verse en el Administración del filtrado de archivos al hacer clic en el nodo Grupos de archivos. Puede definir grupos de archivos adicionales o cambiar los archivos incluidos y excluidos. Los cambios que se realicen en un grupo de archivos afectarán a todos los filtros de archivos, plantillas e informes existentes a los que se haya agregado el grupo de archivos.

9. INFORMES DE ALMACENAMIENTO

El Administrador de recursos del servidor de archivos puede generar informes que permitirán comprender el uso de los diferentes archivos en el servidor de ficheros. Es posible usar los informes de almacenamiento para supervisar los patrones de uso de disco (por tipo de archivo o usuario), identificar archivos duplicados y latentes, realizar un seguimiento del uso de cuotas y auditar el filtrado de archivos.

Los informes de almacenamiento sirven para identificar las tendencias de uso del disco y el modo en que los datos están clasificados. También puede supervisar un grupo de usuarios en concreto para detectar los intentos de guardar archivos no autorizados.

En el nodo Administración de informes de almacenamiento del complemento MMC del Administrador de recursos del servidor de archivos, es posible realizar las siguientes tareas:

a) Programar informes de almacenamiento periódicos que permitan identificar las tendencias de uso de disco.

b) Realizar un seguimiento de los intentos de guardar archivos no autorizados para todos los usuarios o para un grupo de usuarios seleccionado.

c) Generar informes de almacenamiento inmediatamente.

Desde el nodo “Administración de informes de almacenamiento”, se pueden crear tareas de informes, que se usan para programar uno o varios informes periódicos, o bien generar informes a petición. En el caso de los informes a petición, al igual que en los programados, se recopilan los datos actuales antes de generarse el informe.

Además, se pueden generar informes automáticamente para informar cuando un usuario supera un umbral de cuota o intenta guardar un archivo no autorizado.

En la siguiente tabla se describe cada informe de almacenamiento disponible.

Informe	Descripción
Archivos duplicados	Enumera los archivos que presuntamente están duplicados (archivos con el mismo tamaño y hora de última modificación). Use este informe para identificar y reclamar el espacio en disco no aprovechado en archivos duplicados.
Auditoría de filtrado de archivos	Enumera eventos de filtrado de archivos que se hayan producido en el servidor de ficheros para un número específico de días. Use este informe para identificar los usuarios o las aplicaciones que infrinjan las directivas de filtrado.
Archivos por grupo de archivos	Enumera los archivos que pertenecen a los grupos de archivos especificados. Use este informe para identificar los patrones de uso de grupos de archivos, así como los grupos de archivos que ocupen gran cantidad de espacio en disco. Esto puede ayudar a determinar qué filtros de archivos debe configurar en el servidor.
Archivos por propietario	Enumera los archivos, agrupados por los usuarios a los que pertenecen. Use este informe para analizar los patrones de uso en el servidor e identificar los usuarios que usan gran cantidad de espacio en disco.
Archivos grandes	Enumera los archivos de un tamaño especificado o de mayor tamaño. Use este informe para identificar los archivos que consumen la mayor parte del espacio en disco en el servidor. Esto puede ayudarle a reclamar rápidamente gran cantidad de espacio en disco.
Archivos no usados recientemente	Enumera los archivos a los que no se ha tenido acceso durante un número especificado de días. Esto puede ayudarle a identificar los datos usados con poca frecuencia que se podrían archivar y quitar del servidor.
Archivos usados recientemente	Enumera los archivos a los que se ha tenido acceso en el plazo de un número especificado de días. Use este informe para identificar los datos usados con frecuencia que deben tener gran disponibilidad.
Uso de cuotas	Enumera las cuotas para las que el uso de cuotas es superior a un porcentaje especificado. Use este informe para identificar cuotas con niveles de uso elevados para poder tomar las medidas adecuadas.

Con la excepción del informe “Archivos duplicados”, todos los informes tienen parámetros configurables que determinan el contenido del informe. Los parámetros varían según el tipo del informe. En algunos casos, los parámetros de informe sirven para seleccionar los volúmenes y las carpetas para los que se va a generar un informe, para establecer un tamaño de archivo mínimo que incluir o para restringir el informe a los archivos de determinados usuarios.