CCN
centro criptológico nacional

Guía de Seguridad de las TIC

IMPLEMENTACIÓN DE SEGURIDAD NEXTCLOUD

NOVIEMBRE 2019

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES

NIPO: 083-19-272-3
Fecha de Edición: noviembre de 2019
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.

julio de 2019

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 Linux (CCN STIC 600), 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.

3. OBJETO

El propósito de este documento consiste en proporcionar los procedimientos para la implementación, establecer la configuración y realizar tareas de administración maximizando las condiciones de seguridad del servidor de alojamiento de archivos Nextcloud en un servidor independiente CentOS 7.4 Linux.

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 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.

Esta guía asume que el servidor de ficheros se va a implementar sobre un equipo con un sistema operativo CentOS 7.4 Linux, donde se ha seguido el proceso de implantación definido en la guía CCN-STIC-619 Anexo A.

Cumpliendo con estos requisitos previos, puede iniciar la instalación del servidor de alojamiento de archivos Nextcloud.

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 alojamiento de archivos Nextcloud 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:

a) Un servidor independiente basado en CentOS 7.4 Linux.

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

Este documento incluye:

a) **Descripción de versiones.** Para todos aquellos operadores que tengan experiencia en versiones previas, se proporciona la información sobre las diferentes opciones y versiones de las que dispone el sistema.

b) **Descripción de las nuevas funcionalidades.** Para todos aquellos operadores que tengan experiencia en las versiones anteriores de Nextcloud, se incluyen las nuevas características del producto.

c) **Funcionalidades de seguridad local adicionales.** Completa descripción de aquellas características y servicios que, no encontrándose definidos por defecto, agregan seguridad adicional al servidor de alojamiento de archivos Nextcloud.

d) **Mecanismos para la implementación de la solución.** Se incorporan mecanismos para la implementación de la solución de forma automatizada.

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

f) **Guía paso a paso.** Va a permitir implantar y establecer las configuraciones de seguridad en un servidor de alojamiento de archivos Nextcloud.

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

h) **Configuración de cifrado de archivos.** Establece los mecanismos para la configuración del cifrado que aporta el propio Nextcloud.

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 servidor de alojamiento de archivo, será necesario cumplir los requisitos definidos para CentOS 7.4 Linux.

b) 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 CentOS 7.4 Linux 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.

Para los entornos de ENS se podrá utilizar la versión de CentOS 7.4 x86_64 Everything (build 1708), con la opción de instalación deseada, que más se adapte a las necesidades de cada organización.

La guía ha sido desarrollada y probada en entorno de uso de servicios Linux con la versión de CenOS 7.4 Linux x86_64 Everything (build 1708).

La guía de seguridad ha sido elaborada utilizando un laboratorio basado en una plataforma de virtualización tipo Hyper-V sobre Windows Server 2012 R2 Datacenter con las siguientes características técnicas:

a) Servidor Dell PowerEdge™ T320:

   i. Intel Pentium Xeon CPU E5 2430 2.20GHz.

   ii. HDD 1 TB.

   iii. 64 GB de RAM.

   iv. Interfaz de Red 1 Gbit/s.

Esta guía de seguridad no funcionará con hardware que no cumpla con los requisitos de seguridad mínimos de CentOS 7. Esto quiere decir que se requieren equipos con procesadores Intel o AMD de 64 o 32 bits (x64 o i386), con más de 1 GB de memoria RAM ambas versiones.

Se aconseja, no obstante, por seguridad y rendimiento, la implementación de versiones de 64 bits frente a las de 32 bits.

A partir de la versión 7, CentOS solo admite completamente la arquitectura x86-64, mientras que las siguientes arquitecturas no son compatibles:

a) IA-32 en todas las variantes, tuvo soporte temporalmente en CentOS 7.0.

b) IA-32 sin extensión de dirección física (PAE), no compatible desde CentOS 6

c) IA-64 (arquitectura Intel Itanium), fue compatible con CentOS 3 y 4

d) PowerPC de 32 bits (Apple Macintosh y PowerMac con procesador PowerPC G3 o G4), el soporte beta estaba disponible en CentOS 4

e) IBM Mainframe (eServer zSeries y S / 390), no compatible desde CentOS 5

f) Alpha, el soporte estaba disponible en CentOS 4

g) El soporte SPARC, beta estaba disponible en CentOS 4

Nota: Puede comprobar los requisitos del sistema de CentOS en el siguiente enlace https://wiki.centos.org/es/About/Product.

La guía ha sido desarrollada con el objetivo de dotar a las infraestructuras con la seguridad adecuada dependiendo del entorno sobre el que se aplique. Es posible que algunas de las funcionalidades esperadas hayan sido desactivadas y, por lo tanto, pueda ser necesario aplicar acciones adicionales para habilitar servicios, demonios o características deseadas.

Para garantizar la seguridad de los puestos de trabajo, deberán instalarse las actualizaciones recomendadas por el fabricante, disponibles a través del servicio “yum update --security “. Las actualizaciones por lo general están disponibles en los servidores espejo (servidores que replican los propios de RED-HAT), en las siguientes 72 horas después de su publicación por el equipo de RED-HAT. Normalmente estos paquetes están disponibles en 24 horas, no obstante, hay que tener presente que determinadas actualizaciones por su criticidad pueden ser liberadas en cualquier momento. Se deberá tener en cuenta la implementación de las actualizaciones tanto para el sistema operativo como para los diferentes servicios instalados. Deberá tener en consideración que CentOS está basado en RED-HAT y ofrecen diferentes tiempos de implementación de actualizaciones. En líneas posteriores de la presente guía se tratarán las consideraciones oportunas.

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 el hecho de haber probado su configuración y comportamiento en un entorno aislado y controlado, en el cual se habrán aplicado las pruebas y posteriores cambios en la configuración que se ajusten a los criterios específicos de cada organización.

Si estuviera aplicando la presente configuración de seguridad en un sistema ya configurado con una versión previa de esta guía, tenga en cuenta los cambios personalizados que hubiera realizado. La aplicación nuevamente de la seguridad a través de los paso a paso correspondientes, puede implicar que tenga que ajustar de nuevo los valores que ya hubiera personalizado.

El espíritu de estas guías no está dirigido a remplazar políticas consolidadas y probadas de las organizaciones sino a servir como línea base de seguridad. Esta línea 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 alojamiento de archivos Nextcloud 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 aunadas en un mismo anexo, el cual se define a continuación:

a) Anexo A: En este anexo se define la configuración necesaria para adaptar un servidor de alojamiento de archivos Nextcloud a las necesidades requeridas por el Esquema Nacional de Seguridad (ENS).

6. SERVIDOR DE ALOJAMIENTO DE ARCHIVOS

Un servidor de alojamiento de archivos 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 servidor de alojamiento de archivos Nextcloud permite configurar y administrar un servidor de ficheros, el cual proporciona una ubicación central 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 alojamiento de archivos.

En Nextcloud 15 se implementan algunas mejoras sobre las funcionalidades que ya se incorporaron en versiones anteriores y se añaden otras nuevas, las cuales se describen a continuación:

a) Después de su solución de comunicaciones en Nextcloud 13 y de mejorar la gestión y administración en Nextcloud 14, Nextcloud 15 llega con una red social integrada. Basada en el estándar ActivityPub, lo que han denominado como Nextcloud Social es una red social distribuida y federada, pero más limitada. Nextcloud Social funciona de manera descentraliza destinada a su uso en organizaciones y puede conectarse con nodos de Mastodon, todo con el objetivo de “facilitar la comunicación interna y la colaboración”.

b) La seguridad sigue siendo una preocupación clave para los usuarios de Nextcloud. Para mejorar la protección de los servidores de Nextcloud, esta versión permite a los administradores controlar y aplicar la autenticación de dos factores globalmente o en una base de grupo por grupo. Además, incluye códigos de una sola vez para administradores de sistemas, que se utilizarán cuando el segundo factor no esté disponible.

   Para reforzar aún más Nextcloud, esta versión incluye reglas CSP (Política de seguridad de contenido) más estrictas que brindan una protección aún más profunda contra las vulnerabilidades de las secuencias de comandos entre sitios. La tercera generación de Tokens de aplicaciones mejora el manejo en el cambio de contraseñas externas. Esto reduce la cantidad de veces que los usuarios tienen que volver a autorizar sus aplicaciones cliente, ya que los clientes pueden volver a autorizarse automáticamente, siempre que uno de los inicios de sesión de los usuarios sea válido.

c) Colaboración con la integración de aplicaciones móviles para Online Office, Talk en la barra lateral del archivo. Una nueva barra lateral, que integra las versiones de Nextcloud como revisiones de documentos, permite llamadas de audio / video y chat durante las sesiones de edición, que permite compartir y comentar más fácilmente.

   Mejoras en el diseño, como mejores iconos y colores en las barras de herramientas, compatibilidad con HiDPI y representación de miniaturas en la aplicación Archivos. Una experiencia móvil mejor y más rápida, haciendo que la edición de documentos en línea, en tiempo real y colaborativa esté disponible para los usuarios de Nextcloud en cualquier lugar.

d) Nextcloud ha tenido durante mucho tiempo capacidades de flujo de trabajo básicas, lo que permite escribir aplicaciones personalizadas que ejecutarían operaciones en archivos cuando se cumplan ciertas condiciones. Esta versión presenta dos de estas aplicaciones: “Convertidor de documentos a PDF” y “Scripts externos”. Ambos hacen lo que el nombre sugiere, permitiendo a los administradores definir ciertas reglas que deben aplicarse para permitir que los documentos se conviertan a PDF o se ejecuten a través de un script. Conozca más detalles en esta entrada de blog.

e) La versión 1.2 de la aplicación de búsqueda de texto completo basada en Elastic Search ahora está disponible con Nextcloud 15. No solo indexa los archivos y permite a los usuarios buscar en su contenido, sino que también ofrece a los autores de las aplicaciones capacidad de escribir un tipo de complemento que le permite indexar datos de la aplicación. Así se puede buscar marcadores, elementos del calendario, contactos, música o cualquier otra cosa. Incluso hay un complemento de OCR que puede extraer texto de las imágenes. Todo eso funciona en el mismo cuadro de búsqueda que está disponible en cada aplicación, si la aplicación es compatible con la aplicación “Búsqueda de texto completo”.

Nota: Toda la información de las novedades de Nextcloud 15 pueden verse en el manual de administración en el siguiente enlace:
https://docs.nextcloud.com/server/15/admin_manual/release_notes.html

En caso de ser necesario autenticar los clientes o publicar una carpeta compartida en Active Directory, el equipo debe estar unido a un dominio de Active Directory como un servidor miembro. Si no existe la necesidad de realizar ninguna de estas tareas, no es necesario unir el servidor de alojamiento de archivos a un dominio.

Nextcloud se instala con una aplicación LDAP para permitir que los usuarios de LDAP (incluido Active Directory) aparezcan en sus listas de usuarios de Nextcloud. Estos usuarios se autenticarán en Nextcloud con sus credenciales de LDAP, por lo que no tendrá que crear cuentas de usuario de Nextcloud separadas para ellos. Se podrán administrar los miembros, cuotas y permisos de uso compartido de Nextcloud como cualquier otro usuario de Nextcloud.

Nextcloud usa todo el espacio disponible dentro de la partición o directorio que se defina en la instalación, usualmente se instala en "/var/www/html/nextcloud". Si está definida, se instalará dentro de la partición "/var", siendo recomendable separar en distintas particiones otros subdirectorios que cuelgan de "/var" por razones operativas, como "/var/www" para tener separados del resto del sistema los distintos sitios web alojados en un servidor web, el "/var/lib/mysql" para aislar las bases de datos de posibles saturaciones que se den en "/var", /var/log para aislar específicamente los ficheros de log, etc. El motivo de esto es evitar una de las incidencias más frecuentes que es la falta de espacio en un sistema de ficheros. Si el sistema tiene una única partición y ésta se llena completamente, las aplicaciones no podrán seguir escribiendo datos a disco, por lo que pueden producirse todo tipo de situaciones con resultados imprevisibles, desde corrupción de datos por no poderse volcar el contenido de las cachés a disco, aplicaciones que dejan de funcionar por no poder escribir sobre ficheros temporales necesarios para su funcionamiento, o directamente el colapso de todo el sistema por no poder seguir funcionando correctamente el sistema operativo .

Por todo esto, es conveniente añadir puntos de montaje externos o adicionales para el alojamiento de archivos de los distintos usuarios.

Todos los volúmenes de disco existentes deberían utilizar el sistema de archivos XFS 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 CentOS 7.4 Linux dota a todos los sistemas de ficheros el formato XFS, 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 CentOS 7.4 Linux 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 ya disponga de aplicación de seguridad y no permita el uso de las características del servidor de alojamiento de archivos.

Si el Firewalld está habilitado, debe seleccionar las excepciones necesarias, a fin de que el servidor de alojamiento de ficheros y el conjunto de servicios LAMP (Linux, Apache, MySQL y PHP) funcionen correctamente.

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

Antes de configurar el servidor de alojamiento de archivos	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 XFS por volumen. – Adicionalmente puede agregar cuotas internamente en el propio servidor Nextcloud. – 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.
Configure correctamente repositorios.	– Configure los repositorios necesarios para la instalación del servidor LAMP y de Nextcloud. – Puede necesitar librerías adicionales para cada uno de los servicios, escoja repositorio confiables recomendados por CentOS.
Particiones y puntos de montaje.	– Si tiene posibilidad de separar las particiones y redimensionar por LVM, separe el servidor Nextcloud del resto de particiones del sistema.
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. – Configure correctamente los permisos, grupos, propietarios y acciones permitidas para la partición que aloje el servidor Nextcloud y todas sus subcarpetas.

Requisitos de seguridad:

a) 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.

b) Siempre se debe mantener actualizado el sistema y aplicar los parches, soluciones de seguridad y actualizaciones de kernel más recientes y tan pronto se encuentre encuentren disponibles.

c) El demonio cron tiene una característica incluida en la cual se puede especificar los usuarios que pueden y no pueden ejecutar tareas programadas. Esto se controla con el uso de los archivos llamados /etc/cron.allow y /etc/cron.deny. Para bloquear a un usuario, basta con añadir su nombre de usuario en el archivo cron.deny y para permitir un usuario que ejecute tareas, se añade su nombre en el archivo cron.allow. Si se desea deshabilitar a todos los usuarios del uso de tareas, se añade la palabra ALL a una línea del archivo cron.deny.

d) El módulo SELinux (Security Enhanced Linux o Seguridad Mejorada de Linux, en español) es un mecanismo de seguridad y control de acceso que se incluye en el kernel. Deshabilitar esta característica, significa quitar los mecanismos de seguridad del sistema. Se recomienda su utilización y su correcta configuración incluso si el equipo está conectado a Internet y provee servicios públicos.

e) Si no se utiliza ningún protocolo de IPv6 en el sistema, entonces de debería deshabilitar, puesto que ninguna de las aplicaciones, políticas y protocolos de IPv6 se requieren.

f) Si el sistema posee una cantidad considerable usuarios, es muy importante recolectar información de la actividad y procesos de cada usuario, para después poder analizar esa información en caso de problemas de rendimiento o seguridad.

6.1 COMPARTICIÓN DE RECURSOS

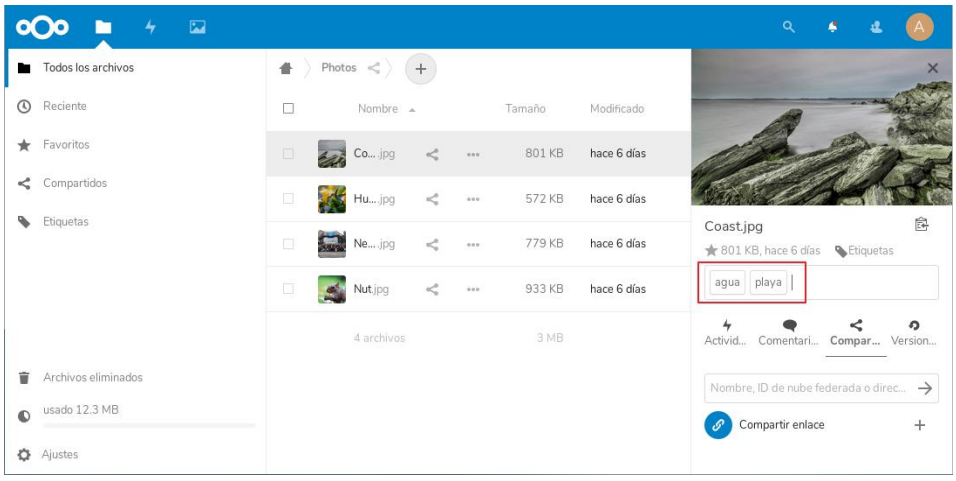
Un recurso compartido (fichero, directorio, etc.) permite a un usuario acceder a dicho recurso sin necesidad de que el usuario este en la ubicación actual del recurso. Normalmente este recurso es compartido a través de la red de manera que dicho usuario pueda hacer uso de éste.

Desde el punto de vista del servidor de alojamiento de archivos 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.

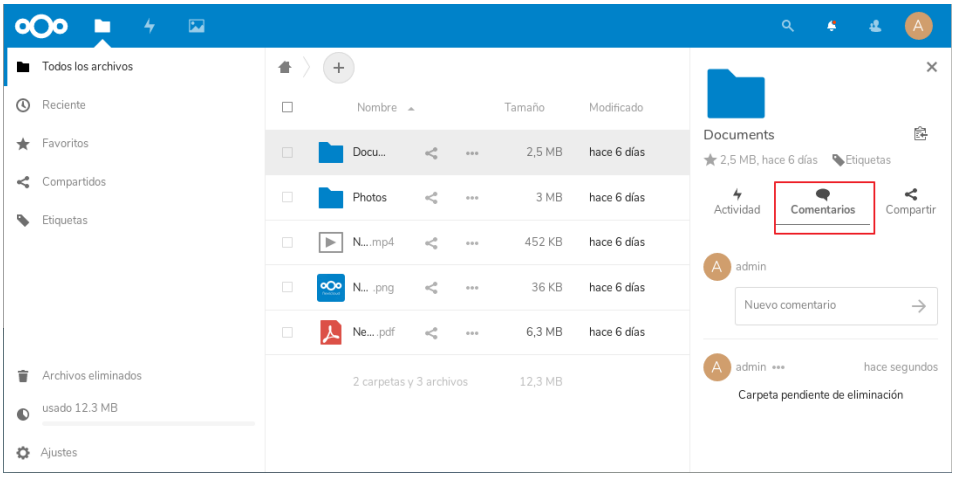
6.1.1 ACCESO A LOS DOCUMENTOS DESDE NEXTCLOUD WEB

Puede acceder a sus archivos de Nextcloud con la interfaz web de Nextcloud y crear, previsualizar, editar, eliminar, compartir y volver a compartir archivos. El administrador de Nextcloud tiene la opción de deshabilitar estas funciones.

Puede asignar etiquetas a los archivos. Para crear etiquetas, abra un archivo en la vista Detalles. A continuación, escriba sus etiquetas. Para ingresar más de una etiqueta, presione la tecla de retorno después de crear cada etiqueta. Todas las etiquetas son etiquetas del sistema y son compartidas por todos los usuarios en su servidor de Nextcloud.



Utilice la vista Detalles para agregar y leer comentarios en cualquier archivo o carpeta. Los comentarios son visibles para todos los que tienen acceso al archivo.



Se pueden ver vídeos que se alojen en Nextcloud con la aplicación de reproducción de vídeo, simplemente pulsando en él. La calidad de este dependerá del navegador web que se utilice y el formato del vídeo.

Nota: Si el administrador de Nextcloud no ha desactivado la opción de reproducción y aun así no se puede ver el vídeo se puede tratar de un error del navegador.

Nextcloud puede mostrar vistas previas de archivos de imagen, de audio o de texto si se encuentra habilitado por administrador de servidor. Pasando el cursor por encima de estos archivos se pueden llevar a cabo diferentes funciones:

a) **Favoritos**: Pulsando los tres puntos que se encuentran en la línea del archivo se puede añadir a favoritos, para resaltarlo.

b) **Compartir**: Se puede compartir cualquier archivo pulsando el botón de compartir, introduciendo el nombre o dirección de correo de la persona a la que se desea compartir el archivo. Una vez compartido el archivo con un usuario, se puede escoger que funciones se podrá llevar a cabo. Entre ellas se encuentran la de Editar, que incluirá la opción de Crear, Cambiar o Eliminar archivos, Compartir (con un tercer usuario) o Establecer una fecha de caducidad. También se puede dejar de compartirlo con ese usuario pulsando sobre “Dejar de compartir”.

c) **Desplegable**: Además de lo explicado anteriormente y de la misma manera que se incluye un archivo como Favorito, se puede pulsar en los tres puntos para poder Renombrar el archivo, Mover o copiarlo en otra carpeta, Descargarlo o Eliminarlo.

Nota: La opción **Abrir en ONLYOFFICE** está solo disponible para previsualizar archivos PDF o similares.

d) **Detalles**: En detalles se puede ver información general sobre un archivo, actividades, comentarios, ajustes de compartir y revisiones.

e) **Archivos ocultos:** En la parte inferior izquierda se encuentra el botón de Ajustes, mediante el cual se puede mostrar u ocultar archivos ocultos. Este tipo de archivos ocultos se llaman Dotfiles, porque incluyen un punto "**.**" delante de su nombre (que se puede incorporar renombrándolo). Cuando se realice esta acción, el nombre del archivo aparecerá en gris. En este momento ya se podrá ocultar y mostrarlo según necesidad. Esto va a permitir mantener una interfaz mucho más ordenada.

f) **Previsualización**: Se puede también previsualizar los archivos que se tienen en el servidor Nextcloud con doble clic, siempre que el administrador del sistema lo haya habilitado.

g) **Navegación en Nextcloud:** Navegar a través de las carpetas de Nextcloud es tan sencillo como pulsar aquella que se desea abrir y trabajar con ella utilizando la flecha de atrás del navegador para volver a la anterior ventana. Además, Nextcloud incluye una barra de navegación para proporcionar una rápida navegación.

h) **Iconos de compartir**: Si un archivo o carpeta está compartido con uno o más usuarios aparecerá el botón de compartir visto anteriormente. Si por el contrario el archivo esta compartido mediante un enlace, aparecerá marcado con un icono parecido al de una cadena.

i) **Crear o subir archivos y directorios**: Para subir o crear nuevos archivos y carpetas se pulsará el botón representado un "**+**". También se pueden subir archivos arrastrándolos directamente en la página.

j) **Seleccionar archivos y carpetas:** Se pueden seleccionar uno o más archivos y carpetas pulsando en los recuadros del lado de su nombre. Esto nos permitirá realizar acciones en masa como Mover o copiar, Descargar o Eliminar. También se pueden seleccionar todos mediante el recuadro situado encima de todos los archivos.

k) **Filtración de la vista de archivos:** Mediante la barra situada a la izquierda de los archivos se pueden buscar de manera más rápida los archivos. Que se ordenarán de manera automática según la información que se introduzca en el archivo.

l) **Mover archivos:** Se puede mover archivos y carpetas manteniendo pulsado sobre el archivo y arrastrándolo donde se desea mover.

m) **Cambio en la fecha de caducidad de archivos compartidos:** Se puede introducir una fecha de caducidad tanto en archivos locales como en archivos públicos compartidos.

n) **Crear o conectar a un enlace compartido de federación:** El uso compartido de la nube federada permite montar archivos compartidos de servidores Nextcloud remotos y administrarlos como un recurso compartido local.

6.1.2 ACCESO A LOS DOCUMENTOS DESDE WEBDAV

Nextcloud es totalmente compatible con el protocolo WebDAV, y puede conectarse y sincronizarse con los archivos de Nextcloud a través de WebDAV.

Para no tener que descargar la aplicación de Nextcloud Desktop se puede conectar el ordenador al servidor de Nextcloud a través de WebDAV. WebDAV es una extensión de protocolo de transferencia de hipertexto (HTTP) que facilita la creación, lectura y edición de archivos en servidores web. Con él se puede acceder a recursos compartidos de Nextcloud en Linux, MacOS y Windows de la misma manera que cualquier recurso de red remoto, y mantenerse sincronizado.

a) Configuración de WebDAV en MacOS:

   i. Primeramente, pulse en Ir en el apartado de Conectar al servidor.

   ii. Se abrirá una ventana en la que se especificará la dirección del servidor Nextcloud.

   iii. Finalmente pulse Conectar

b) Configuración de WebDAV en Windows: Si se usa la implementación nativa de Windows, se puede asignar Nextcloud a una nueva unidad. La asignación a una unidad permite navegar por los archivos almacenados en un servidor Nextcloud de la misma manera que lo harían los archivos almacenados en una unidad de red mapeada.

   El uso de esta función requiere conectividad de red. Si se desea almacenar sus archivos sin internet, se usará Nextcloud Desktop para sincronizar todos los archivos en su Nextcloud con uno o más directorios del disco duro local.

   i. Abrir un símbolo del sistema en Windows.

   ii. Ingresar la siguiente línea en el símbolo del sistema para asignar a la unidad Z del ordenador:

```
net use Z: https://server/remote.php/dav/files/USERNAME/ /user:usuario contraseña
```

c) Asignación de unidades con Windows Explorer:

   i. Migrar al equipo en el Explorador de Windows.

   ii. Pulsar botón derecho en Entrada del equipo y seleccionar “Asignar unidad de red…” desde el menú desplegable.

   iii. Elegir una unidad de red local a la que desea asignar Nextcloud.

   iv. Especificar la dirección de la instancia de Nextcloud, seguido de **/remote.php/dav/files/USERNAME/.**

   v. Pulsar en Finalizar.

d) Accediendo a archivos usando cURL: Como WebDAV es una extensión de HTTP, cURL se puede usar para crear secuencias de comandos de las operaciones de archivos.

   i. Para crear una carpeta con la fecha actual como nombre:

```
$ curl -u usuario:contraseña -X MKCOL
  “https://example.com/nextcloud/remote.php/dav/files/USUARIO/$(date ‘+%d-%b-%Y’)“
```

ii. Para cargar un archivo error.log en ese directorio:

```
$ curl -u usuario:contraseña -T error.log
  "https://example.com/nextcloud/remote.php/dav/files/USUARIO/$(date '+%d-%b-%Y')/error.log"
```

iii. Para mover un archivo:

```
$ curl -u usuario:contraseña -X MOVE –header 'Destination:
  https://example.com/nextcloud/remote.php/dav/files/USERNAME/target.jpg'
  https://example.com/nextcloud/remote.php/dav/files/USERNAME/source.jpg
```

6.2 PERMISOS DE ACCESO

En Unix/Linux todos los archivos pertenecen obligatoriamente a un usuario y a un grupo. Cuando un usuario crea un nuevo archivo, el propietario del archivo será el usuario que lo ha creado y el grupo del archivo será el grupo principal de dicho usuario.

En los Sistemas Unix/Linux, la gestión de los permisos que los usuarios y los grupos de usuarios tienen sobre los archivos y las carpetas, se realiza mediante un sencillo esquema de tres tipos de permisos que son:

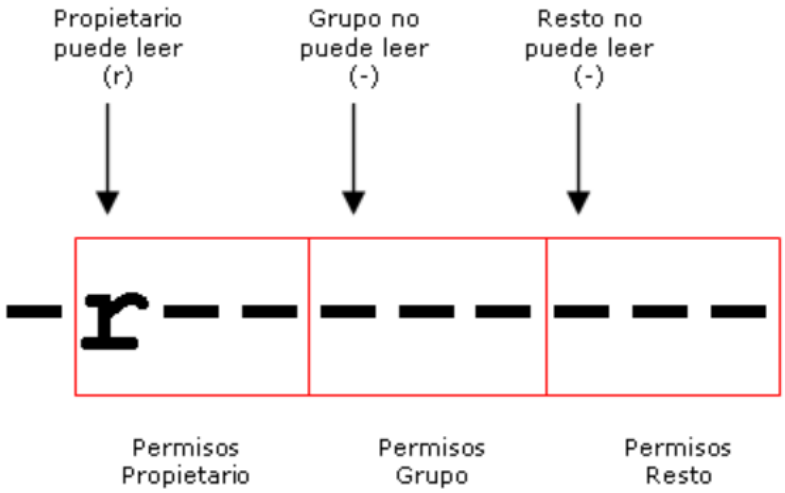
a) Permiso de lectura

b) Permiso de escritura

c) Permiso de ejecución

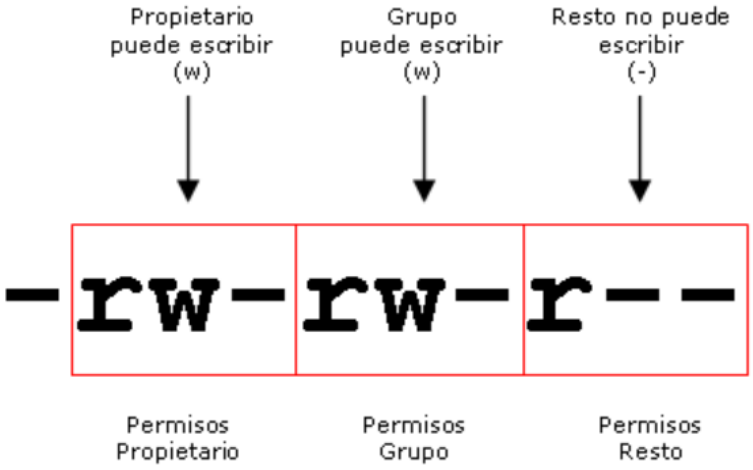
El significado de estos permisos difiere si se tienen sobre archivos o sobre carpetas. A continuación, se muestran los distintos significados para cada uno de los casos:

a) **Permiso de lectura:** Cuando un usuario tiene permiso de lectura de un archivo significa que puede leerlo o visualizarlo, bien sea con una aplicación o mediante comandos. Si el usuario no tiene permiso de lectura, no podrá ver el contenido del archivo.



El permiso de lectura se simboliza con la letra 'r' del inglés 'read'.

b) **Permiso de escritura:** Cuando un usuario tiene permiso de escritura sobre un archivo significa que puede modificar su contenido, e incluso borrarlo. También le da derecho a cambiar los permisos del archivo mediante el comando "**chmod**" así como cambiar su propietario y el grupo propietario mediante el comando "**chown**". Si el usuario no tiene permiso de escritura, no podrá modificar el contenido del archivo.

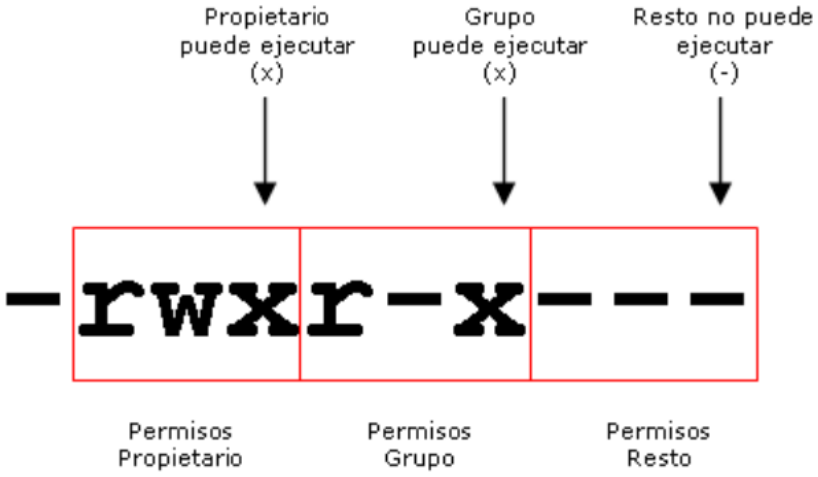


El permiso de escritura se simboliza con la letra 'w' del inglés 'write'.

c) **Permiso de ejecución:** Cuando un usuario tiene permiso de ejecución de un archivo significa que puede ejecutarlo. Si el usuario no dispone de permiso de ejecución, no podrá ejecutarlo, aunque sea una aplicación.

Los únicos archivos ejecutables son las aplicaciones y los archivos de comandos (scripts). Si se trata de ejecutar un archivo no ejecutable, dará errores.

Cuando un usuario tiene permiso de ejecución sobre una carpeta, significa que puede entrar en ella, bien sea con el comando 'cd' o con un explorador de archivos como "Konqueror". Si no dispone del permiso de ejecución significa que no puede ir a dicha carpeta.



El permiso de ejecución se simboliza con la letra 'x' del inglés 'eXecute'.

6.2.1 PERMISOS DE ARCHIVO

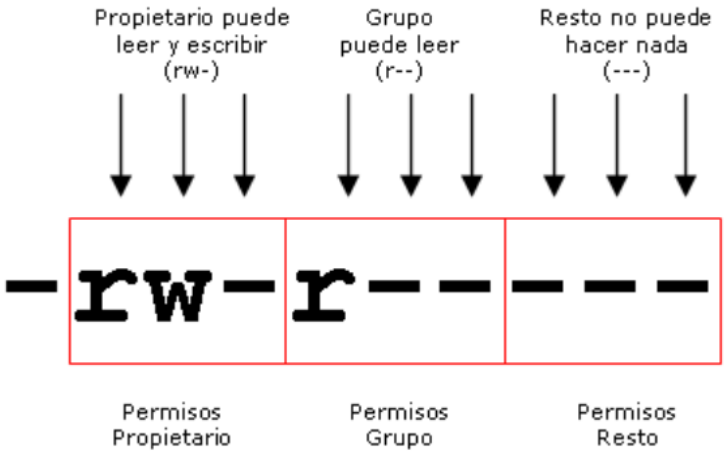
Los permisos solamente pueden ser otorgados a tres tipos o grupos de usuarios:

a) Al usuario propietario del archivo

b) Al grupo propietario del archivo

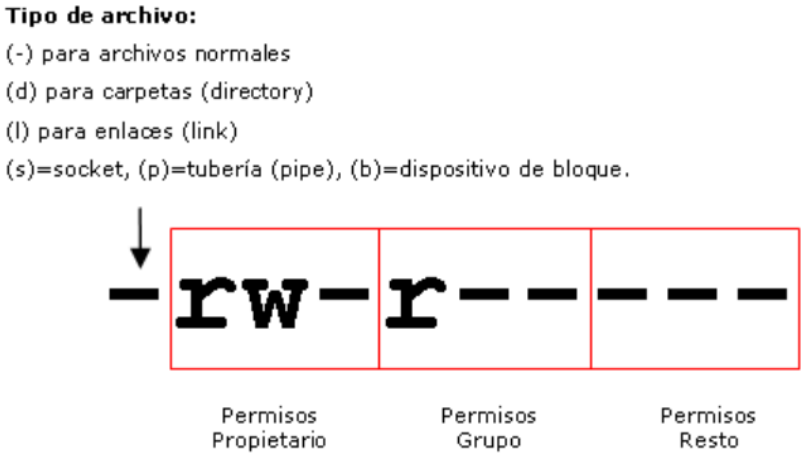
c) Al resto de usuarios del sistema (todos menos el propietario)

Se pueden dar permisos de lectura, escritura, ejecución o combinación de ambos al usuario propietario del archivo, al grupo propietario del archivo o al resto de usuarios del sistema. En Unix/Linux no existe la posibilidad de asignar permisos a usuarios concretos ni a grupos concretos, tan solo se puede asignar permisos al usuario propietario, al grupo propietario o al resto de usuarios.



Para poder cambiar permisos sobre un archivo, es necesario poseer el permiso de escritura sobre el mismo. El usuario root puede modificar los permisos de cualquier archivo ya que tiene acceso total sin restricciones a la administración del sistema.

Cuando se muestran los permisos de un archivo o directorio el primer carácter indica de qué tipo de archivo se trata. Si es un guión '-' significa que se trata de un archivo normal, la letra 'd' significa que se trata de una carpeta (directory), la letra 'l' significa que se trata de un enlace (link). Otros valores son s, p, b que se refieren a sockets, tuberías (pipe) y dispositivos de bloque respectivamente.



Como anteriormente se menciona, los 9 caracteres siguientes simbolizan los permisos del usuario propietario (3 caracteres), los permisos del grupo propietario (3 caracteres) y los permisos del resto de usuarios (3 caracteres). Vienen codificados con las letras r, w y x que se refieren a los permisos de lectura, escritura y ejecución. Si en lugar de aparecer dichas letras aparecen guiones significa que se carece de dicho permiso.

Para cambiar los permisos de un archivo o una carpeta es necesario disponer del permiso de escritura (w) sobre dicho archivo o carpeta. Para hacerlo, se utiliza el comando "**chmod**". La sintaxis del comando chmod es la siguiente:

```
$ chmod [opciones] permiso nombre_archivo_o_carpeta
```

Los permisos se pueden representar de dos formas. La primera es mediante las iniciales de a quién va dirigido el permiso (usuario=u, grupo=g, resto=o (other)), seguido de un signo + si se quiere añadir permiso o un signo - si se quiere quitar y seguido del tipo de permiso (lectura=r, escritura=w y ejecución=x).

La segunda forma de representar los permisos es mediante un código numérico cuya transformación al binario representaría la activación o desactivación de los permisos. El código numérico está compuesto por tres cifras entre 0 y 7. La primera de ellas representaría los permisos del usuario propietario, la segunda los del grupo propietario y la tercera los del resto de usuarios.

En binario, las combinaciones representan el tipo de permisos. El bit más a la derecha (menos significativo) se refiere al permiso de ejecución (1=activar y 0=desactivar). El bit central se refiere al permiso de escritura y el bit más a la izquierda se refiere al permiso de lectura. La siguiente tabla muestra las 8 combinaciones posibles:

Código	Binario	Permisos efectivos
0	0 0 0	- - -
1	0 0 1	- - x
2	0 1 0	- w -
3	0 1 1	- w x
4	1 0 0	r - -
5	1 0 1	r - x
6	1 1 0	r w -
7	1 1 1	r w x

6.2.2 BITS SUID Y SGID

El bit SUID es una extensión del permiso de ejecución. Se utiliza en escasas ocasiones y sirve para que cuando un usuario ejecute una aplicación, ésta se ejecute con permisos del usuario propietario en lugar de hacerlo con los del usuario que ejecuta la aplicación, es decir, es equivalente a que sea ejecutada por el propietario.

Para activar el bit SUID, se puede ejecutar el comando "**chmod u+s nombre_archivo**" o sumar 4000 al número en octal si se utiliza dicho sistema. También se puede hacer lo mismo para el grupo, es el denominado bit SGID sumando 2000 al número en octal. Activar los bits SUID o SGID puede ocasionar problemas de seguridad sobre todo si el propietario es root.

Si se aplica el bit SGID a una carpeta, todas las subcarpetas y archivos creados dentro de dicha carpeta tendrán como grupo propietario el grupo propietario de la carpeta en lugar del grupo

primario del usuario que ha creado el archivo. Es una ventaja cuando varias personas pertenecientes a un mismo grupo trabajan juntas con archivos almacenados en una misma carpeta. Si se otorgan permisos de lectura y escritura al grupo, los archivos podrán ser modificados por todos los miembros del grupo y cuando cualquiera de ellos cree un archivo, éste pertenecerá al grupo.

6.3 AUDITORIA DE SEGURIDAD

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

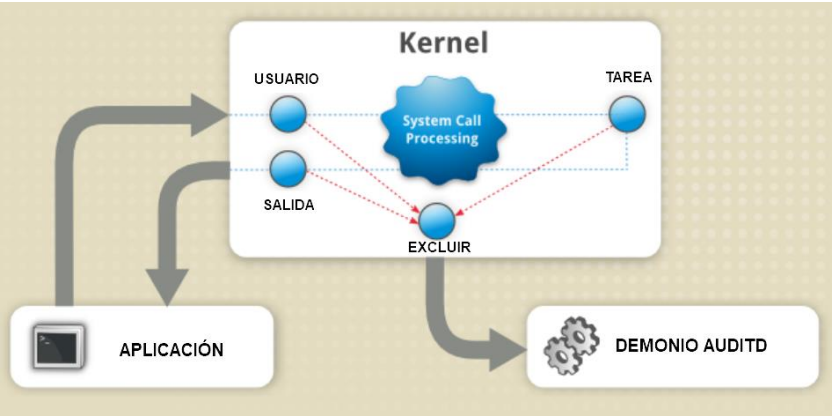
Uno de los principales objetivos de las auditorías de seguridad es el cumplimiento de las normas. Como parte de la gestión de un sistema de seguridad, la trazabilidad recoge una de las dimensiones fundamentales para poder evaluar incidencias de seguridad. Los registros de eventos que proporciona el servidor 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 impresora, etc.

Con CenOS 7 Linux, es posible crear directivas de auditoría utilizando la herramienta audit. Auditd genera directivas de auditoría más avanzadas, más concretas y más fáciles de administrar.

El sistema de auditoría consta de dos partes principales: las aplicaciones y utilidades del espacio de usuario y el procesamiento de llamadas del sistema del lado del kernel. El componente del kernel recibe llamadas del sistema desde las aplicaciones de espacio de usuario y las filtra a través de uno de los tres filtros: usuario, tarea o salir. Una vez que una llamada del sistema pasa a través de uno de estos filtros, se envía a través del filtro de exclusión, que, en función de la configuración de la regla de auditoría, lo envía al daemon de auditoría para su posterior procesamiento.



El demonio de auditoría del espacio de usuario recopila la información del kernel y crea las entradas del archivo de registro en un archivo de logs. Otras utilidades de Audit en el espacio de usuario interactúan con el daemon de auditoría, el componente de auditoría del kernel o los archivos de registro de auditoría:

a) **audisp**: el demonio de "audit dispatcher" interactúa con el demonio de audit y envía eventos a otras aplicaciones para su posterior procesamiento. El propósito de este demonio es proporcionar un mecanismo de complemento para que los programas analíticos en tiempo real puedan interactuar con los eventos de auditoría.

b) **auditctl**: la utilidad de control de auditoría interactúa con el componente de auditoría del kernel para controlar una serie de configuraciones y parámetros del proceso de generación de eventos.

Las utilidades de auditoría restantes toman el contenido de los archivos de registro de auditoría como entrada y generan una salida en función de los requisitos del usuario. Por ejemplo, la utilidad aureport genera un informe de todos los eventos registrados.

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.

Además del propio sistema operativo, Nextcloud respalda con aplicaciones de Información del servidor, Actividades y Auditoría.

Nextcloud registra los datos en el archivo "nextcloud.log" provisto en la raíz de su directorio de datos. Opcionalmente, puede grabar una auditoría completa en un archivo de registro de auditoría separado. Las herramientas de prevención de pérdida de datos y de administración de dispositivos móviles pueden usar esto, ya que la información del agente de usuario está disponible junto con los registros extensos de usuario, IP y fecha / hora.

Los registros de auditoría proporcionados incluyen información de sesión de usuario, manejo de archivos, administración de usuarios, uso compartido y otras acciones.

7. NEXTCLOUD

Se trata de un proyecto de software libre creado inicialmente por el mismo creador de OwnCloud, Frank Karlitschek, con el objetivo de que los usuarios recuperen el control sobre sus datos. El objetivo del producto es proporcionar a las organizaciones y a los particulares un control sobre su información y datos, facilitando la sincronización y el intercambio de ficheros entre dispositivos. Además, incorpora otras herramientas que permiten comunicarse por audio y vídeo vía WebRTC de manera segura.

Entre sus principales características y ventajas es posible encontrar:

a) **Archivos accesibles desde cualquier lugar**: Con su sencilla interfaz web permite compartir ficheros con otros usuarios, crear y enviar vínculos públicos protegidos por contraseña, permitir que otros carguen archivos en su nube e incluso recibir notificaciones de actividad por teléfono o correo. Incluye también clientes para dispositivos móviles y de escritorio.

b) **Seguridad**: Desde el proyecto se garantiza que siguen las mejores prácticas de la industria respecto a la seguridad, implementando una amplia variedad de protocolos y aplicando de manera continua actualizaciones que corrigen posibles bugs de seguridad. De hecho, en las

últimas versiones han incluido tecnologías como SAML 2.0 para garantizar la autentificación de segundo factor.

c) **Gestionar el flujo de trabajo:** Los administradores de sistema podrán controlar y dirigir el flujo de datos entre los usuarios o entre los servidores. El etiquetado de archivos basado en reglas y la respuesta a estas etiquetas, así como otros indicadores como la ubicación física, el grupo de usuarios, las propiedades del archivo y el tipo de solicitud permitirán denegar específicamente el acceso, la conversación, la eliminación o la retención de datos. En dichas restricciones se pueden incluir ciertas zonas geográficas o grupos en concreto.

d) **Supervisa la actividad del servidor:** Nextcloud puede llegar a escalar hasta millones de usuarios, por lo que es muy importante revisar en todo momento el estado de los servidores. Para ello se brinda una serie de monitores que permiten supervisar su estado y rendimiento. Todo ello incluido en la interfaz web de usuario, además de una API. La App "Nextcloud Activity" ofrece a los usuarios una visión clara de lo que está pasando con sus ficheros en todo momento. Rastrea las modificaciones de archivos, descargas de acciones y cambios en comentarios o etiquetas. Todo ello se puede notificar mediante correo electrónico o incluso vía feed RSS.

e) **Clientes para dispositivos móviles o de escritorio:** Se tienen disponibles clientes en la mayoría de plataformas, entre las que se encuentran Android, iOS y PC. Esto permite sincronizar y compartir los ficheros de una manera segura a través de una conexión cifrada. Los clientes móviles cuentan con la carga automática de imágenes y vídeos. Dichos clientes permiten manejar diferentes cuentas a la vez, mostrando todas las actividades que ocurren en el servidor y notificar los nuevos elementos.

f) **Almacenamiento externo:** Nextcloud permite acceder a los ficheros de terceros, productos privativos como Amazon, Google y Dropbox (siempre que se quiera asumir el riesgo y bajo propia responsabilidad del usuario). Incluso se puede acceder a ellos mediante protocolos como NFS o FTP. Su aplicación de cifrado puede funcionar sobre datos en reposo tanto para el almacenamiento local como el remoto, protegiendo así los datos almacenados en redes fuera de nuestra infraestructura. Las claves pueden ser manejadas desde un servidor externo de claves o almacenadas localmente

g) **Calendario y agenda de contactos:** pudiéndose sincronizar utilizando los clientes de escritorio o el dispositivo móvil. Permite sincronizar calendarios mediante "CalDAV" o "CardDAV Sync".

h) **Llamadas de audio y vídeo seguras:** Nextcloud utiliza su propio chat privado y seguro. Su propio servicio de videoconferencia es accesible a través de navegadores y aplicaciones dedicadas en ordenadores o computadoras, dispositivos móviles y clientes de escritorio, siempre cifrados de extremo a extremo, además de mensajes de texto y compartición de ficheros. Todo ello garantizado mediante las tecnologías de Spreed.ME y WebRTC y facilitado por una interfaz fácil de usar.

i) **Collabora Online:** suite de oficina en línea, que está basada en el popular producto LibreOffice y que soporta la mayoría de formatos de documento, hojas de cálculo y presentaciones.

7.1 INSTALACIÓN

Para asegurarse de que el sistema funcionará sin errores, emplee siempre hardware certificado. El proceso de certificación de hardware es continuo y la base de datos correspondiente se actualiza con regularidad.

Nota: Consulte el formulario de búsqueda de hardware certificado en:
https://wiki.centos.org/hardware

Para una correcta instalación del servidor de alojamiento de archivos Nextcloud, se necesitan varios servicios adicionales, estos servicios se conocen comúnmente como LAMP.

LAMP no es un programa en concreto, sino que es una sigla formada por las iniciales de 4 tipos de software: Linux, Apache, MySQL y PHP.

Para un mejor rendimiento, estabilidad y funcionalidad, existen las siguientes recomendaciones para la ejecución de un servidor Nextcloud. El servidor de Nextcloud no es compatible con Windows y MacOS.

Requerimientos	Opciones
Sistema Operativo	– Ubuntu 18.04 LTS (recomendado) – RHEL 7 (recomendado) – Debian 8 (Jessie), 9 (Stretch) – SUSE Linux Enterprise Server 12 con SP3 – openSUSE Leap 42.1+ – CentOS 7
Bases de Datos	– MySQL o MariaDB 5.5+ (recomendado) – Oracle Database 11g – PostgreSQL 9/10 – SQLite (Solo recomendado para pruebas e instancias mínimas)
Servidor Web	– Apache 2.4 con mod_php o php-fpm (recomendado) – nginx con php-fpm
PHP Runtime	– 7.0 – 7.1 – 7.2 – 7.3
Memoria RAM	– Mínimo 128MB – Recomendado 512MB

Requerimientos	Opciones
Cliente de Escritorio	– Windows 7+ – MacOS Lion (10.7) + (64-bit) – Linux (CentOS 6.5+, Ubuntu 14.04+, Fedora 21+, openSUSE 13, SUSE Linux Enterprise 11 SP3+, Debian 8 (Jessie)+, Red Hat Enterprise Linux 7).
Aplicaciones móviles	– iOS 10.x+ – Android 4.x+
Navegador Web	– Microsoft Internet Explorer 11 – Microsoft Edge – Mozilla Firefox – Google Chrome/Chromium – Apple Safari

Nota: Si desea utilizar Nextcloud Talk, debe usar Mozilla Firefox 52+ o Google Chrome / Chromium 49+ para tener una experiencia completa con las video llamadas y el uso compartido de pantallas. Google Chrome / Chromium requiere un complemento adicional para compartir la pantalla.

7.1.1 INTERFAZ WEB

Se puede acceder al servidor Nextcloud utilizando cualquier navegador web compatible. Solo se necesita ingresar la URL del servidor de Nextcloud (por ejemplo, cloud.example.com) e ingresar el nombre de usuario y contraseña.

Para obtener la mejor experiencia con la interfaz web de Nextcloud, se recomienda que utilice la versión más reciente y compatible de un navegador de esta lista:

a) Microsoft Internet Explorer

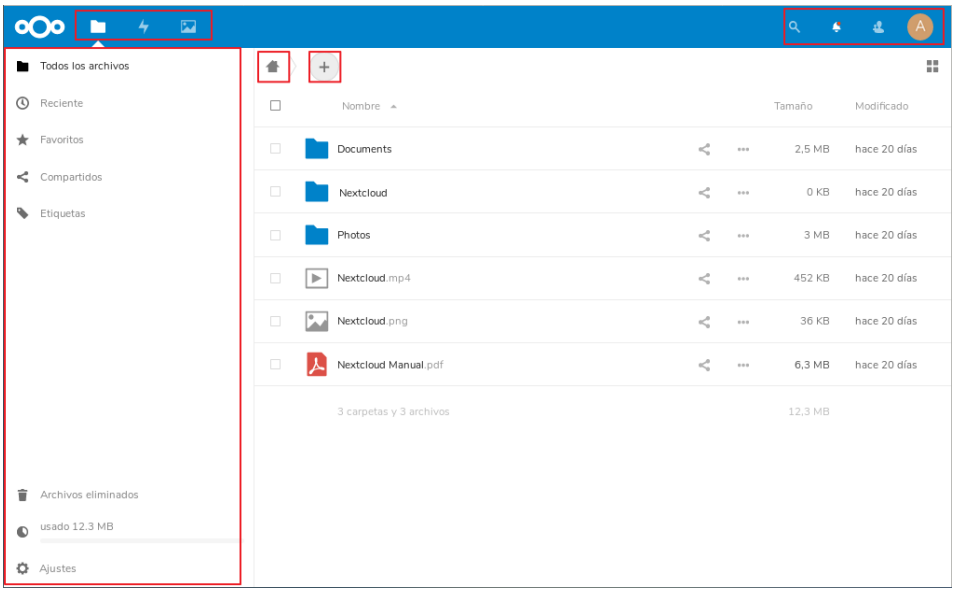
b) Microsoft Edge

c) Mozilla Firefox

d) Google Chrome / Chromium

e) Apple Safari

La interfaz de usuario de Nextcloud contiene los siguientes campos y funciones:



a) **Menú de selección de aplicaciones:** Ubicado en la esquina superior izquierda, encontrará todas las aplicaciones que están disponibles en su instancia de Nextcloud. Al hacer clic en el icono de una aplicación, se le redirigirá a la aplicación.

b) **Campo de información de aplicaciones:** Ubicado en la barra lateral izquierda, proporciona filtros y tareas asociadas con la aplicación seleccionada. Por ejemplo, cuando está utilizando las aplicaciones de Archivos, tiene un conjunto especial de filtros para encontrar rápidamente sus archivos, como los archivos que ha compartido con usted y los que ha compartido con otros. Verás diferentes elementos para otras aplicaciones.

c) **Vista de aplicación:** El campo central, en la interfaz de usuario de Nextcloud. Este campo muestra el contenido o las funciones del usuario de la aplicación seleccionada.

d) **Barra de navegación:** Ubicada en la ventana de visualización principal (la vista de la aplicación), esta barra proporciona un tipo de navegación que le permite migrar a niveles más altos de la jerarquía de carpetas hasta el nivel raíz (inicio).

e) **Botón Nuevo:** Ubicado en la barra de navegación, el botón Nuevo le permite crear nuevos archivos, nuevas carpetas o cargar archivos.

f) **Campo de búsqueda:** haga clic en la lupa en la esquina superior derecha para buscar archivos.

g) **Menú Contactos:** le ofrece de una descripción general de sus contactos y usuarios en su servidor. Dependiendo de los detalles proporcionados y las aplicaciones disponibles, puede iniciar directamente una video llamada con ellos o enviar correos electrónicos.

h) **Botón de la galería**: Se ve como cuatro pequeños cuadros, y le lleva directamente a su galería de imágenes.

i) **Menú de configuración:** haga clic en la imagen de su perfil, ubicada a la derecha del campo de búsqueda, para abrir el menú desplegable de configuración. Su página de Configuración proporciona las siguientes configuraciones y características:

i. Enlaces para descargar aplicaciones de escritorio y móviles.
ii. Uso del servidor y disponibilidad de espacio.
iii. Gestión de contraseñas
iv. Nombre, correo electrónico y configuración de imagen de perfil
v. Administrar navegadores y dispositivos conectados
vi. Membresías de grupo
vii. Ajustes de idioma de la interfaz
viii. Gestionar notificaciones
ix. ID de nube federada y botones para compartir redes sociales
x. Administrador de certificados SSL / TLS para almacenamientos externos.
xi. Sus configuraciones de dos factores
xii. Información de la versión de Nextcloud

7.2 SEGURIDAD INICIAL

Para asegurar de forma correcta cualquier herramienta en Linux, es recomendable seguir una serie de pautas de configuración desde el inicio. Por ello, se tendrán en cuenta configuraciones iniciales de instalación tales como el particionado, el sistema de archivos a utilizar o la complejidad de contraseñas entre otros.

Las contraseñas son las llaves del sistema. Deben ser lo más seguras posibles para evitar inicios de sesión no autorizados, que es el primer paso hacia problemas de seguridad mayores. El uso de contraseñas lo suficientemente fuertes como para amortizar un ataque es un paso decisivo y a la vez sencillo que ahorrará muchos problemas en el futuro.

7.2.1 CONFIGURACIÓN DE CONTRASEÑAS

Muchas contraseñas utilizadas por usuarios son bastante fáciles de adivinar. Nextcloud 15 proporciona diferentes maneras de proveer autentificación al sistema. En cualquier situación en la cual se elija una contraseña como parte de un esquema de autentificación, la seguridad de ese esquema estará por lo menos parcialmente a la merced de la complejidad de la contraseña elegida.

Una contraseña segura tiene que tener al menos estas características:

a) Tener una longitud mínima de 8 caracteres.
b) Mayúsculas y minúsculas alternadas.
c) Tantos signos de puntuación y números como sea posible.
d) Evitar palabras o frases comunes que puedan figurar en cualquier diccionario.

e) No tener relación evidente con datos personales del usuario: Nombre, fecha de nacimiento, etc.

Otro factor a tener en cuenta es la **caducidad de contraseñas**. Dentro de las tareas frecuentes que se realizan tanto en Linux como en el propio servidor Nextcloud, se encuentra la de administrador de cuentas de usuario, tanto en su creación y edición, como en establecimiento o modificación de la caducidad y el vencimiento de las contraseñas de los usuarios, siendo política de seguridad modificar regularmente la misma.

Para esto, puede ser útil el comando **chage** para el cambio de contraseña en el sistema operativo local, el cual es usado para modificar la información de caducidad de la contraseña de un usuario específica, permite ver la información de antigüedad de la cuenta de un usuario o cambiar el número de días entre los cambios de contraseña y la fecha de la última contraseña. Del mismo modo, el servidor de alojamiento de archivos Nextcloud, proporciona sus propios mecanismos de caducidad y complejidad de contraseñas para los usuarios propios del servidor.

En esta guía se configurará de manera permanente una caducidad de contraseña para nuevos usuarios y modificará la política de seguridad de los usuarios ya existentes para que cumplan estos requisitos de seguridad establecidos. Las recomendaciones de configuración en cuanto a la caducidad de las contraseñas serán las siguientes:

a) El periodo máximo durante el que se puede mantener una contraseña será de 60 días.

b) La longitud mínima de la contraseña será de 8 caracteres.

c) El período mínimo durante el que se debe mantener una contraseña será de 15 días.

d) El período durante el que el sistema avisará de una futura caducidad de la contraseña será de 15 días.

7.2.2 PARTICIONADO Y SISTEMA DE ARCHIVOS

Como recomendación previa a la instalación y configuración del servidor de alojamiento de archivos, se debe establecer la cantidad y tamaño de las particiones, así como el sistema de archivos a utilizar. Aunque estos factores dependen en gran medida del uso que se vaya a hacer del sistema, se van a dar una serie de recomendaciones para ayudar a su correcta elección.

Para realizar una correcta elección del sistema de archivos hay que tener en cuenta los tipos de archivos más comunes que existen en Linux.

Se optará por elegir **XFS** como sistema de archivos recomendado.

Sistema de archivos	Sistema operativo	Descripción
FAT	Heredado	Sistema de archivos heredado que se ha adoptado universalmente. **FAT12**, **FAT16** y **FAT32**.
Ext2	Linux	El segundo Filesystem: Sigla de "Extended Graphics Array" utilizado por muchas distribuciones Linux.
Ext3	Linux	El tercero Filesystem: Se añadió registro diario (journaling), utilizado por muchas distribuciones Linux.
Ext4	Linux	El cuarto Filesystem: utilizado por muchas distribuciones Linux. “**Extiende los límites de almacenamiento**.”

Sistema de archivos	Sistema operativo	Descripción
JFS	Linux	Journaled File System: fue introducido por IBM y aún se admite, pero ha sido sustituido por Ext4.
XFS	Linux/Red-HAT	Sistema de archivos de 64 Bits, actualmente opción por defecto en Red Hat.
ReiserFS	Linux/SUSE	Se trataba de un formato de archivo que estaba en uso en varias distribuciones, pero ha sido reemplazado por Ext3.
Btrfs	Linux/SUSE	CentOS/Red-Hat tienen soporte para este sistema de archivos, **SUSE ofrece este sistema por defecto**, recomendándolo para particiones críticas del sistema.

A continuación, Se muestra una organización de las particiones como ejemplo, siendo viables alternativas en función de los usos del sistema.

Partición	Tamaño
/	120 GiB xfs
/boot	500 MiB xfs
/boot/efi	Default MiB vfat
/var	50 GiB xfs
/tmp	25 GiB xfs
/var/log	35 GiB xfs
/home	200 GiB xfs
/var/log/audit	15 GiB xfs
/var/www	50 GiB xfs
swap	½ Memoria RAM Equipo

Durante la instalación o posteriormente se recomienda cifrar las particiones aumentando la seguridad de la misma e impidiendo que personal no autorizado pueda acceder a datos críticos.

7.2.3 CONFIGURACIÓN INICIAL

Por defecto el servidor de alojamiento Nextcloud, crea ciertas configuraciones para facilitar el acceso al usuario, habilitando la mayor parte de funcionalidades y aumentando la velocidad de instalación del mismo. Estas configuraciones en muchas ocasiones pueden ser motivo de posibles brechas de seguridad.

Para evitar brechas innecesarias, se configurarán ciertos parámetros de manera correcta:

a) **http/https:** Las siglas **HTTP**, acrónimo de Hypertext Transfer Protocol, es un protocolo de transferencia de hipertexto. El protocolo HTTP ha sido desarrollado por la World Wide Web Consortium y la Internet Engineering Task Force. Se finalizó en 1999 con el objetivo de definir y poder estandarizar la sintaxis y la semántica de los intercambios de información que se llevan a cabo entre los distintos equipos que componen una red.

Durante muchos años el protocolo HTTP ha sido el más utilizado en la Red. Desde que comenzó su desarrollo en 1989, se han lanzado diferentes versiones más avanzadas que han sabido adaptarse a las necesidades y al avance tecnológico del momento:

i. HTTP/0.9: La primera versión del protocolo HTTP, denominada así a posteriori para poder identificarlas de las siguientes versiones. Este protocolo no utiliza cabeceras HTTP por lo que solamente podían transferirse archivos en HTML. Además, no existían los códigos de estado HTTP.

ii. HTTP/1.0: Mucho más flexible que la versión anterior tanto para navegadores como para los servidores web. Permite los métodos de petición GET, HEAD y POST y todavía es utilizada hoy en día en algunos servidores proxy.

iii. HTTP/1.1: Publicada en 1997 y añade bastantes mejoras con relación a la versión anterior. En esta versión ya se pueden realizar múltiples peticiones a la vez por parte de un cliente, la conexión puede ser reutilizada y se añadieron mejoras en la gestión de caché.

iv. HTTP/2: Pretende implantarse como un estándar en la web. Aunque no modifica semánticamente el protocolo anterior, sí incluye muchas mejoras que benefician tanto a usuarios como a cualquier persona que tenga una web. Por ejemplo, HTTP/2 incluye compresión, necesita menos recursos, lo que implica una menor latencia, el servidor puede responder a varias peticiones al mismo tiempo… En definitiva, mejoras que tienen como objetivo una Web más rápida y segura.

En cambio, **HTTPS** utiliza una combinación de dos protocolos (HTTP+SSL/TLS) que hace que cualquier tipo de información que se transmita en la red sea cifrada y nadie pueda acceder a ella, únicamente navegador y servidor web. Y para ello es necesario que el servidor web tenga instalado un Certificado SSL.

La información que se transmite bajo el protocolo HTTP es susceptible de ser interceptada por usuarios no autorizados, pudiendo poner en peligro los datos se la organización y la privacidad de sus usuarios. En cambio, tener un certificado SSL y que funcione bajo el protocolo HTTPS servirá para asegurar a los usuarios que la web es legítima y que es seguro navegar en ella.

b) **Autenticación LDAP:** Nextcloud se instala con una aplicación LDAP para permitir que los usuarios de LDAP (incluido Active Directory) aparezcan en sus listas de usuarios de Nextcloud. Estos usuarios se autenticarán en Nextcloud con sus credenciales de LDAP, por lo que no tendrá que crear cuentas de usuario de Nextcloud separadas para ellos. Administrarás sus membresías, cuotas y permisos de uso compartido de Nextcloud como cualquier otro usuario de Nextcloud.

Nota: El módulo PHP LDAP es requerido; Este módulo se define como php-ldap en la mayoría de las distribuciones.

La aplicación LDAP soporta:

i. Soporte de grupo LDAP

ii. Intercambio de archivos con usuarios y grupos de Nextcloud

iii. Acceso vía WebDAV y Nextcloud Desktop Client

iv. Versiones, almacenamiento externo y todas las demás funciones de Nextcloud

v. Conectividad perfecta con Active Directory, sin necesidad de configuración adicional

vi. Soporte para grupos primarios en Active Directory

vii. Detección automática de atributos LDAP como el DN base, el correo electrónico y el número de puerto del servidor LDAP

viii. Solo acceso de lectura a su LDAP (no se admite la edición o eliminación de usuarios en su LDAP)

ix. Opcional: permitir a los usuarios cambiar su contraseña LDAP desde Nextcloud

c) **SELinux:** Cuando se tiene SELinux habilitado en la distribución de Linux, puede tener problemas de permisos después de una nueva instalación de Nextcloud y ver los errores de permisos denegados en sus registros de Nextcloud.

Se proveerán de comandos específicos para la puesta en marcha del servidor de alojamiento de archivos sin mermar la seguridad deshabilitando SELinux.

d) **PHP-FPM:** PHP-FPM (FastCGI Process Manager) es la implementación alternativa de PHP FastCGI con características adicionales que altamente útiles para sitios web de mayor tráfico. Entre sus características están:

i. Manejo avanzado para detener/arrancar procesos de forma fácil.

ii. Posibilidad de iniciar hilos de procesos con diferentes uid/gid/chroot/environment, escuchar en diferentes puertos y usar distintos php.ini.

iii. Modo seguro

iv. Registro stdout y stderr.

v. Reinicio de emergencia en caso de destrucción accidental del caché opcode.

vi. Soporte acelerado de subidas.

vii. “slowlog”, scripts de registro de procesos (no sólo sus nombres, sin sus backtraces también, usando ptrace y similares para leer procesos execute_data remotos) que son inusualmente lentos.

viii. fastcgi_finish_request() – Función especial para detener y descargar todos los datos mientras continúa haciendo algún proceso más largo (conversión de vídeos, procesamiento de estadísticas, etc.).

ix. Creación dinámica/estático de hilos.

x. Información básica del status SAPI (similar al mod_status de Apache).

xi. Basado en archivos de configuración php.ini.

e) **GRUB.** GNU Grand Unified Boot loader (GRUB) es un gestor de arranque múltiple desarrollado inicialmente para el sistema GNU Hurd. El gestor de arranque grub tiene varias funciones, pero sin duda su misión principal es seleccionar qué sistema operativo instalado o kernel cargar en el momento de arranque del sistema. Permite también que el usuario transmita argumentos al kernel. Por estos motivos Grub solo tiene que ser accesible por root y mediante contraseña, aplicando los pasos de esta guía que se describirán posteriormente conseguiremos:

   i. Bloquear el acceso a la línea de comandos del Grub.

   ii. Bloquear la posibilidad de edición de las entradas del Grub.

   iii. Bloquear la posibilidad de ejecución de todas las entradas del Grub.

f) **Contraseña segura para Root.** Cuando se habla de root, se refiere a la cuenta superusuario en Linux, aquella que posee todos los privilegios y permisos para realizar acciones sobre el sistema. Para ciertas acciones que afectan al sistema de archivos, se requiere tener acceso root. Sin embargo, se debe tener un conocimiento sobre las acciones que se realizan, ya que una acción realizada de manera errónea podría ocasionar daños importantes en el sistema. Para evitar el uso de instrucciones con privilegios de superusuario la cuenta root tiene que estar dotada con una contraseña segura que evite que cualquier usuario malintencionado pueda comprometer de algún modo el sistema.

g) **Usuarios UID 0.** En el fichero /etc/passwd/ existe un campo UID por cada usuario, que corresponde al identificador de cada usuario. Algunas distribuciones de Linux por defecto, crean varios usuarios con UID 0 que corresponde al identificador de superusuario. Si existen varios superusuarios en el sistema la probabilidad de vulnerar el mismo es mayor, por este motivo se deben limitar los usuarios con UID 0 únicamente a root, siendo el único usuario habilitado para tener control total sobre el sistema.

h) **Cuentas sin contraseñas.** En Linux existe la opción de configurar una cuenta de usuario sin contraseña, aunque ese usuario no pertenezca a los denominados “sudores” (administradores). En el sistema no debe de haber ningún usuario sin contraseña, esto supondría una vulnerabilidad, ya que cualquier usuario podría acceder a información sensible sin necesidad de estar autorizado para ello.

7.2.4 ELEMENTOS INNECESARIOS DEL SISTEMA

En este punto es necesario tratar siempre de deshabilitar todos aquellos elementos del sistema que no sean necesarios, minimizando la superficie de posibles ataques al mismo.

7.2.4.1 APLICACIONES INNECESARIAS

Una de las características del software libre es su carácter colaborativo. De esta manera existen cientos de miles de librerías disponibles, que permiten a los desarrolladores crear una aplicación sin tener que empezar de cero. Disponiendo de componentes de diferentes tamaños con un objetivo o funcionalidad específica y que permiten hacer la aplicación más robusta.

De esta característica se nutren las distribuciones Linux y sus herramientas. Para que esas aplicaciones se ejecuten correctamente, se necesita que estén instalados el resto de paquetes. De esta forma, cuando se instala una aplicación, también se instalan aquellos paquetes necesarios para su funcionamiento.

Nextcloud por defecto posee ciertas aplicaciones que se deben revisar y eliminar si no son necesarias para la organización, y por el contrario instalar las que sean necesarias para garantizar la seguridad del servidor.

7.2.4.2 USUARIOS INNECESARIOS

Como se ha comentado anteriormente, por defecto el servidor de alojamiento de archivos crea configuraciones para facilitar el uso del mismo, una de esas configuraciones, son los usuarios predefinidos como admin, etc. Estos usuarios tienen permisos y configuraciones para ciertas partes del mismo. El tener usuarios predefinidos en el servidor, puede ser motivo de posibles brechas de seguridad.

Por esto, los usuarios tienen que ser los mínimos necesarios e indispensables, eliminando los que no sean necesarios y restringiendo ciertos permisos a los que por necesidad deban mantenerse.

7.3 SERVIDOR

7.3.1 ACTUALIZACIÓN DEL SERVIDOR

Las actualizaciones del servidor presentan mejoras sobre la propia herramienta de Nextcloud y a diversas aplicaciones que se ejecutan y son necesarias para la correcta funcionalidad del sistema y de la aplicación en sí, con la finalidad de mantener un funcionamiento óptimo y reparar, si fuese necesario, fallos, errores o vulnerabilidades que se pudieran presentar.

Todo servidor debe de estar actualizado, pero dependiendo de la criticidad del servidor que se deba actualizar, es posible que se necesite aislar del resto de sistemas o aislar su comunicación con redes externas e internet. Por este motivo ciertos sistemas necesitarán una actualización fuera de línea.

En esta guía se diferenciará la actualización por parte del fabricante de manera “online” y mediante parches y actualizaciones de manera “offline”.

7.3.1.1 ONLINE

Gracias al asistente de actualización del propio Nextcloud, el proceso de actualización se realizará de forma automática. El asistente de actualización de Nextcloud creará un punto de restauración en caso de que haya problemas durante la actualización. No obstante, antes de iniciar el proceso para actualizar Nextcloud es recomendable realizar una copia de seguridad de los siguientes elementos:

a) La base de datos de Nextcloud.

b) La carpeta de configuración.

c) La carpeta que contiene archivos y datos en el servidor.

7.3.1.2 OFFLINE

Para actualizar el servidor, se comenzará siempre haciendo una copia de seguridad nueva y deshabilitando todas las aplicaciones de terceros.

Posteriormente se realizarán los siguientes pasos:

a) Copia de seguridad de la base de datos, el directorio de datos y el archivo config.php de Nextcloud Server.

b) Descargar y descomprimir la última versión de Nextcloud Server desde "nextcloud.com/install/" en un directorio vacío fuera de su instalación actual.

c) Detener el servidor web (Apache, nginx).

d) Cambiar el nombre del directorio de Nextcloud actual, por ejemplo, nextcloud-old.

e) Al descomprimir el nuevo archivo, se crea un nuevo directorio nextcloud con sus nuevos archivos de servidor. Copiar este directorio y su contenido en la ubicación original de su antiguo servidor, por ejemplo / var / www /, para obtener una vez más la siguiente ruta / var / www / nextcloud.

f) Copiar el archivo config.php del antiguo directorio de Nextcloud al nuevo directorio de Nextcloud.

g) Si se mantienen los datos, copiar data/ en directorio nextcloud/, desde su versión anterior de Nextcloud a su nuevo directorio de nextcloud /.

h) Si se están utilizando aplicaciones de terceros, buscar en el nuevo directorio nextcloud/apps para ver si están allí. Si no, copiar desde del directorio de aplicaciones antiguas al nuevo. Se debe asegurar que los permisos de directorio de aplicaciones de terceros sean los mismos que para los demás.

i) Reiniciar el servidor web e iniciar la actualización desde la línea de comandos usando **occ**, por ejemplo:

```
$ sudo -u www-data php occ upgrade
```

j) La operación de actualización demora de unos minutos a unas pocas horas, dependiendo del tamaño de su instalación. Cuando termine, se mostrará un mensaje de éxito o un mensaje de error indicará dónde salió mal.

k) Por último, se debe iniciar sesión y comprobar en la parte inferior de la página de Administración el número de versión. Se deben revisar otras configuraciones específicas para asegurarse de su correcta aplicación. Posteriormente se deben revisar las aplicaciones principales para asegurarse de que estén habilitadas. Si es necesario se deben volver a habilitar aplicaciones de terceros.

7.3.2 ALMACENAMIENTO

En Linux, casi todo está representado por un archivo. Esto incluye hardware como unidades de almacenamiento, que se representan en el sistema como archivos en el directorio **/dev**.

Normalmente, los archivos que representan dispositivos de almacenamiento comienzan con sd o hd seguido de una letra. Por ejemplo, la primera unidad en un servidor suele ser algo así como **/dev/sda.**

Las particiones en estas unidades también tienen archivos dentro de **/dev**, representados al agregar el número de partición al final del nombre de la unidad. Por ejemplo, la primera partición en el disco del ejemplo anterior sería **/dev/sda1**.

Mientras que los archivos del dispositivo **/dev/sd*** y **/dev/hd*** representan la forma tradicional de referirse a unidades y particiones, existe una desventaja significativa al usar estos valores por sí mismos. El kernel de Linux decide qué dispositivo obtiene qué nombre en cada arranque, por lo que esto puede generar escenarios confusos en los que los dispositivos cambian los nodos del dispositivo.

Para evitar este problema, el directorio **/dev/disk** contiene subdirectorios correspondientes con formas diferentes y más persistentes para identificar discos y particiones en el sistema. Estos contienen enlaces simbólicos que se crean en el inicio de los archivos correctos **/dev/[s,h]da*.** Los enlaces se nombran de acuerdo con el rasgo de identificación del directorio (por ejemplo, mediante la etiqueta de partición en el directorio /dev/disk/by-partlabel). Estos enlaces siempre apuntan a los dispositivos correctos, por lo que pueden usarse como identificadores estáticos para espacios de almacenamiento.

7.3.3 ADMINISTRACIÓN Y MANTENIMIENTO

Tanto la Administración como el mantenimiento de servidores o equipos Linux es una tarea que necesita una vigilancia constante para asegurar la estabilidad del sistema.

El mantenimiento de servidores debe realizarse desde el primer momento en que estos comienzan a funcionar. Y es que, aunque en un primer momento parezca que el mantenimiento no es una tarea demasiado relevante, es importante sentar las bases para el medio y largo plazo, cuando el tráfico sea más elevado y los recursos almacenados en el servidor sean mayores.

7.3.3.1 AUTOMATIZACIÓN DE TAREAS

En un sistema cualquier tarea automatizada puede ser motivo de fallo de seguridad, por lo que hay que tener identificadas las tareas automatizadas que suceden en nuestro sistema, además de tener protegidos los programas y servicios que las crean.

La herramienta que se usa para automatizar procesos es **cron**. Esta herramienta no es más que un administrador regular de procesos en segundo plano (demonio) que ejecuta procesos o guiones a intervalos regulares (por ejemplo, cada minuto, día, semana o mes). Los procesos que deben ejecutarse y la hora en la que deben hacerlo se especifican en el fichero **Crontab**.

A demás existe el comando **“at”**. Esta herramienta permite programar tareas que se ejecutarán una única vez.

Para limitar la generación de tareas periódicas a usuarios que no estén autorizados (generalmente se considerará únicamente el usuario root como usuario autorizado para tal efecto) se crearán los ficheros **/etc/cron.allow** y **/etc/at.allow** en los que se incorporarán los nombres de los usuarios que pueden utilizar estos servicios.

Se puede establecer esto mismo mediante lista negra en lugar de lista blanca, si es así se crearán los ficheros **/etc/cron.deny** y **/etc/at.deny**, en los que aparecerán los nombres de los usuarios que no pueden utilizar los servicios de los planificadores de tareas.

Nota: Tanto en **CRON** como en **AT** los usuarios incluidos en los ficheros "**.allow**" tienen preferencia con respecto a los usuarios incluidos en el fichero "**.deny**".

7.3.3.2 LOGS DE SISTEMA

El encargado principal de recoger todos los logs para tener una visión global del sistema en Red-Hat/CentOS Linux 7 es la herramienta **Audit**.

El sistema **Audit** de Linux proporciona una forma de rastrear información relevante para la seguridad en su sistema. Según las reglas pre configuradas, **Audit** genera entradas de registro para registrar la mayor cantidad posible de información sobre los eventos que suceden en su sistema. Esta información es crucial en entornos de misión crítica para determinar quién viola las políticas de seguridad y cuáles son las acciones se han realizaron. La auditoría no proporciona seguridad adicional a su sistema; más bien, se puede usar para descubrir infracciones de las políticas de seguridad utilizadas en su sistema. Estas violaciones pueden evitarse con medidas de seguridad adicionales como SELinux.

Entre las partes del sistema que Audit es capaz de recoger información se encuentran las siguientes:

a) Fecha y hora, tipo y resultado de un evento.

b) Etiquetas más detalladas de sujetos y objetos.

c) Asociación de un evento con la identidad del usuario que activó el evento.

d) Todas las modificaciones a la configuración de auditoría e intentos de acceso a los archivos de registro de auditoría.

e) Todos los usos de los mecanismos de autenticación, como SSH, Kerberos y otros.

f) Cambios en cualquier base de datos confiable, como /etc/passwd.

g) Intentos de importación o exportación de información hacia o desde el sistema.

h) Incluir o excluir eventos en función de la identidad del usuario, las etiquetas de tema y objeto, y otros atributos.

i) Por la criticidad de los datos que contiene esta aplicación, se procederá a configurar los accesos a la misma de forma segura. A demás se hará hincapié en la creación de reglas que proporcionen la mayor información posible sobre lo que pueda ocurrir en el sistema.

Nextcloud ofrece ciertas aplicaciones de información, actividad y auditoria del servidor:

a) **Nextcloud Activity:** La aplicación Nextcloud Activity ofrece a los usuarios una visión clara de lo que está sucediendo con sus archivos. Proporciona a los usuarios una visión general de los cambios recientes, como:

   i. Archivos nuevos o eliminados en carpetas compartidas

   ii. Modificaciones de archivos

   iii. Descarga de archivos compartidos.

   iv. Nuevos comentarios o etiquetas

   v. Invitaciones calendario

vi. Llamadas entrantes o solicitudes de chat

La aplicación Nextcloud Activity permite a los usuarios habilitar o deshabilitar la visualización de cualquiera de los eventos en su sesión y recibir notificaciones de correo solo para el tipo de eventos que requieren.

Los usuarios pueden los sucesos en el navegador, elegir recibir notificaciones por correo electrónico o seguir los cambios a través de un canal RSS.

b) **Monitor del sistema:** Nextcloud se escala a millones de usuarios y, a esa escala, es importante vigilar la salud de un sistema. La aplicación de información del servidor proporciona una forma para que los administradores supervisen el estado y el rendimiento de una instalación del servidor Nextcloud. Además de la interfaz gráfica de usuario, un punto final de la API permite a los administradores del sistema importar estos datos en su aplicación de monitorización para que puedan vigilar las operaciones de Nextcloud desde el mismo lugar en el que monitorizan el resto de su infraestructura.

c) **Herramientas de monitorización externas:** Las herramientas de monitorización e inteligencia de sistemas openNMS y Splunk tienen soporte para monitorizar los sistemas Nextcloud y el módulo de configuración de openNMS se puede modificar fácilmente para otras herramientas como Nagios.

Los administradores también pueden optar por iniciar sesión en el registro de systemd, permitiéndoles administrar todos los registros del sistema en un solo lugar. Cuando está habilitado, el registro de auditoría está en un archivo separado.

7.3.3.3 CONTROL DE INTEGRIDAD DE HARDWARE

AIDE es una alternativa libre a Tripwire, que se emplea principalmente para detectar cambios en los ficheros de configuración y binarios importantes, generalmente generando un resumen cifrado único de los ficheros a ser verificados, y almacenándolos en un lugar seguro. Con un procedimiento regular (mediante el planificador cron), los resúmenes originales se comparan con los generados a partir de la copia actual de cada fichero, para determinar si el fichero ha cambiado. Se le proporcionará a AIDE parámetros, para controlar al menos los siguientes puntos:

d) La información referente a permisos (parámetro p).

e) La información de los inodos (parámetro i).

f) La cantidad de enlaces (duros y blandos) a cada fichero y al directorio (parámetro n).

g) El propietario de cada fichero (parámetro u).

h) El grupo propietario de cada fichero (parámetro g).

i) El tamaño de cada fichero (parámetro s).

j) La cantidad de bloques utilizados por cada fichero (parámetro b).

k) Las fechas de modificación (parámetro m) y creación (parámetro c) de cada fichero.

l) El tipo de fichero (parámetro ftype).

m) Las listas de control de acceso (parámetro acl).

n) Las modificaciones en SELinux (parámetro selinux).

o) Los atributos extendidos de ficheros (parámetro xattrs).

p) Además, se generará un resumen en sha512 por medio del parámetro sha512.

7.3.3.4 COPIAS DE SEGURIDAD

La realización de copias de seguridad debe responder a una política definida y preestablecida que determine claramente:

a) Qué información es importante incluir en la copia de seguridad: documentos de usuarios, ficheros de configuración, registros de log, etc.

b) Cuál será la política de nombrado de los ficheros de copias de seguridad, para su rápida localización en caso de necesidad. Dicha política debe permitir la rápida localización por parte de los administradores del sistema, pero sin dar excesiva información a alguien externo acerca del contenido de las copias de seguridad.

c) La periodicidad de realización de estas copias de seguridad y el modo de copia (total, incremental, etc.).

d) El soporte, sistema, localización física, etc. en la que se almacenará la copia de seguridad. Siempre que sea posible, deberán almacenarse dos copias de seguridad, una de fácil acceso para ser utilizada en caso de pérdida de datos, y otra en una localización diferente para prevenir posibles desastres en la localización original de los datos.

e) Las medidas de protección a aplicar a cada copia de seguridad: control de integridad, confidencialidad, etc. No hay que olvidar que los datos en las copias de seguridad tienen los mismos requisitos de seguridad que los archivos originales.

8. 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.

El esquema de particionamiento más común en ordenadores con CentOS 7 Linux como sistema operativo base es el siguiente:

f) Una partición swap

g) Una partición /boot

h) Una partición /

i) Una partición home

Una partición swap (de al menos 256 MB): Las particiones swap sirven para soportar la memoria virtual. En otras palabras, los datos se escriben en una partición swap cuando no hay suficiente memoria RAM para almacenar la información que el sistema está procesando.

En años anteriores, la cantidad recomendada de espacio swap aumentaba en forma lineal con la cantidad de RAM en el sistema. No obstante, debido a que la cantidad de memoria en sistemas modernos ha aumentado a cientos de GB, ahora se reconoce que la cantidad de espacio swap que el sistema necesita es una función de la carga de trabajo de la memoria que se ejecuta en ese sistema.

El espacio swap suele designarse durante la instalación, aunque puede ser difícil determinar la carga de memoria de un sistema en ese momento. Durante una instalación de kickstart, puede solicitar que la cantidad de espacio swap se establezca de forma automática.

Sin embargo, esta configuración no está calibrada para su sistema, por lo tanto, use la siguiente tabla si requiere una cantidad de espacio de swap más precisa.

Cantidad de RAM en el sistema	Cantidad recomendada de espacio swap
4GB de RAM o menos	Un mínimo de 2GB de espacio swap
De 4GB a 16GB de RAM	Un mínimo de 4GB de espacio swap
De 16GB a 64GB de RAM	Un mínimo de 8GB de espacio swap
De 64GB a 256GB de RAM	Un mínimo de 16GB de espacio swap
De 256GB a 512GB de RAM	Un mínimo de 32 GB de espacio swap

Una partición /boot (250 MB): La partición montada en /boot/ contiene el kernel del sistema operativo (el cual permite a su sistema arrancar CentOS Linux) junto con archivos utilizados durante el proceso de arranque. Para la mayoría de los usuarios, una partición de arranque de 250 MB es suficiente.

Una partición root (3.0 GB - 5.0 GB): Aquí es donde se localiza "/" (el directorio raíz). En esta configuración, todos los archivos (excepto aquellos almacenados en /boot) están en la partición raíz. Un tamaño de 3.0 GB le permite instalar una instalación mínima, mientras que una partición raíz de 5.0 GB le permite realizar una instalación completa, seleccionando todos los grupos de paquetes.

Una partición home (al menos de 100 MB): Para almacenar datos de forma independiente de los datos del sistema, cree una partición dedicada dentro de un grupo de volumen para el directorio /home. Así podrá actualizar o reinstalar CentOS Linux sin borrar archivos de datos de los usuarios.

8.1 ALMACENAMIENTO EXTERNO

Una posibilidad para un servidor de alojamiento de archivos como es Nextcloud es utilizar los sistemas de almacenamiento del propio sistema operativo. Pero existen otras alternativas que permitirán un control y una gestión mucho mayores sobre los datos procesados, como las tecnologías NAS y SAN. El uso de cualquiera de estas tecnologías es independiente de la existencia de un clúster, aunque resulta idóneo como método de almacenamiento cuando se dispone de uno, especialmente si se complementan con utilidades para la realización de copias de seguridad.

8.1.1 ALMACENAMIENTO CONECTADO A LA RED

Los dispositivos NAS (Almacenamiento conectado a la red) son dispositivos de almacenamiento específicos, a los cuales se accede utilizando protocolos de red, como NFS (Sistema de archivos de red), FTP (Protocolo de Transferencia de Archivos), CIFS (Common Internet File System nombre que adoptó Microsoft en 1998 para el protocolo SMB). O SMB (Server Message Block).

La idea consiste en que el usuario solicita al servidor un fichero completo y, cuando lo recibe, lo maneja localmente, lo cual hace que este tipo de tecnología sea ideal para el uso con ficheros de pequeño tamaño, ofreciendo la posibilidad de manejar una gran cantidad de ellos desde los equipos clientes.

El uso de NAS permite, con bajo coste, realizar balanceo de carga y tolerancia a fallos, por lo que es cada vez más utilizado en servidores Web para proveer servicios de almacenamiento, especialmente contenidos multimedia. Hay otro factor a tener en cuenta, y es que los sistemas NAS suelen estar compuestos por uno o más dispositivos que se disponen en RAID, lo que permite aumentar su capacidad, eficiencia y tolerancia ante fallos.

8.1.2 RED DE ÁREA DE ALMACENAMIENTO

Una red SAN (Storage Area Network) o red con área de almacenamiento, está pensada para conectar servidores, discos de almacenamiento, etc., utilizando tecnologías de fibra (que alcanzan hasta 8Gb/s) usando protocolos como Isasi (Abreviatura de Internet SCSI, es un estándar que permite el uso del protocolo SCSI sobre redes TCP/IP).

El uso de conexiones de alta velocidad permite que sea posible conectar de manera rápida y segura los distintos elementos de esta red, independientemente de su ubicación física. De modo general, un dispositivo de almacenamiento no es propiedad exclusiva de un servidor, lo que permite que varios servidores puedan acceder a los mismos recursos. El funcionamiento se basa en las peticiones de datos que realizan las aplicaciones al servidor, que se ocupa de obtener los datos del disco concreto donde estén almacenados.

Dependiendo de lo cantidad de información manejada, se puede optar por el uso de una u otra tecnología. Paro grandes volúmenes, sería conveniente utilizar una red SAN, mientras que paro pequeñas compañías lo idóneo sería un dispositivo NAS. Esto no quiere decir que ambas tecnologías sean excluyentes; existe, de hecho, la posibilidad de combinarlas en sistemas cuyas características así lo requieran.