Consejos Básicos de Seguridad en NAS: RAID no es Backup

Carpe Diem • June 12, 2020

Uno de los principales motivos de comprar un NAS es que tienen varias bahías para discos, lo que permite crear los conocidos "arrays" de discos, o RAIDs, que pueden venir en múltiples formas y colores, o mejor dicho, tipos (RAID1, 5, 10, etc) y se caracterizan por distribuir nuestros datos entre múltiples discos, y de esta forma ofrecer redundancia de datos. A menudo, esto general la falsa sensación de seguridad de que "mis datos están protegidos", cuando en realidad, no es así. Un RAID nunca ha sido, es, ni será una alternativa o sustituto a un backup (copia de seguridad), y me gustaría explicaros los motivos.

¿Qué es RAID?

RAID es el acrónimo de "redundant array of independent disks", y en esencia es una forma de distribución de datos a través de múltiples discos, lo que proporciona mayor rendimiento de lectura/escritura (dependiendo del tipo de RAID) y redundancia ante el fallo de uno o más discos.

Es importante especificar que el objetivo de RAID no es la protección de los datos (como explicaré a continuación), si no evitar los conocidos "downtimes". En caso de fallo de disco, RAID permite que todo el sistema siga funcionando hasta que el usuario pueda sustituir el disco dañado, momento en el cual el array se reconstruirá automáticamente hasta volver a ser estable.

Por lo tanto: RAID nos proporciona REDUNDANCIA.

¿Qué NO es RAID?

RAID NO ES BACKUP

RAID no es una forma de protección de datos porque solamente protege contra una única forma de fallo: Fallo de uno (o más, dependiendo del tipo de RAID) de los discos que lo conforman. Ya está.

RAID no protege contra el resto de incidencias que pueden destruir tus datos, entre las que se encuentran (pero no se limitan a):

- Error humano (borrado accidental de archivos)
- Error / configuración errónea de software (por ejemplo un bug en Plex que borre toda la carpeta de películas)
- Ransomware / Malware
- Apagón que desconecte el NAS de forma brusca y produzca que se corrompa la tabla de particiones del array

- Fallo de hardware / subida de tensión que fría componentes/discos
- Ladrones que entren en tu casa y roben los discos // El NAS
- Un ataque nuclear estratégico, que en caso de ocurrir, destruirá tu array, tu NAS, tu casa, y probablemente varios kilómetros a la redonda.

Debes pensar en RAID como pensarías en archivos duplicados en tu ordenador. Ni más, ni menos.

Imagina que tienes una carpeta "fotos" con todas las fotos de tu vida dentro (por poner un ejemplo), y que esa carpeta está en C:\fotos. Ahora imagina que simplemente copias esa carpeta a C:\fotos2. ¿Considerarías eso una copia de seguridad? No, ¿verdad?, porque los archivos están dentro del mismo disco. Es peligroso, porque si te falla el disco, lo pierdes todo.

Ahora imagina que copias la carpeta C:\fotos en otro disco dentro del mismo ordenador, a D:\fotos. ¿Considerarías eso como algo seguro? ¿Qué pasa si te entra un ransomware y te encripta todos los discos? ¿Realmente confiarías todas las fotos de tu vida a una copia de una carpeta dentro del mismo ordenador? No, ¿verdad? Lo mínimo que exigirías sería copiar las fotos a un disco duro externo por USB. ¿A que sí?

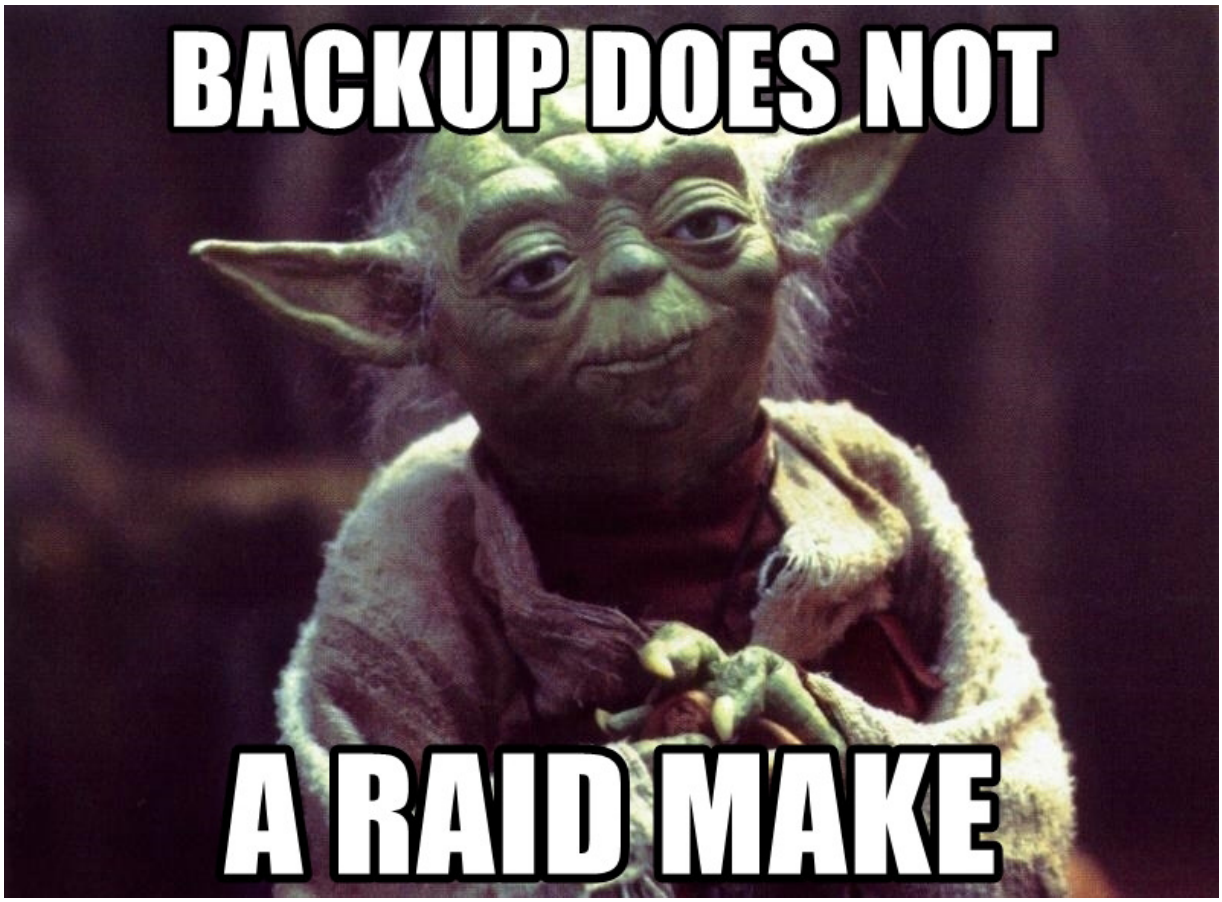
Pues con RAID es lo mismo. Para proteger tus datos necesitas que estos estén FUERA DEL DISPOSITIVO. Si no es así, tienes que asumir que no hay copia de seguridad, y tienes que estar mentalmente preparado para perder tus datos en cualquier momento. Es lo que hay, y va a ocurrir, antes o después.

No se trata de si serás afectado por un Ransomware o no, sino de CUANDO

Algunas preguntes frecuentes:

> *"Yo uso RAID6/7 que tiene dos/tres discos de paridad, así que mi array puede tolerar el fallo de muchos discos. Sigo necesitando un Backup?*

Sí. RAID NO ES BACKUP.



Escuchad al maestro. Sabe de lo que habla.

> *"Uso una función de mi NAS llamada "instantáneas". Sigo necesitando Backup"*

Sí. Las instantáneas se guardan dentro del mismo NAS. No son backup. Además las instantáneas habitualmente utilizan software y sistemas específicos del fabricante, no universales.

> *"Y si uso un disco dedicado en la bahía 4 para hacer copias de los datos que están en las otras bahías, ¿eso es un backup?"*

No. Backup tiene que ser forzosamente fuera de la unidad. No es distinto a lo que comentábamos antes de duplicar la carpeta "fotos" en el disco D:

> *"Entonces, ¿para qué quiero RAID, de qué me sirve?*

RAID te permite no tener que recuperar de tus backups en caso de fallo de disco, lo cual es muy cómodo. Te pongo un ejemplo: Tienes tus NAS con Plex/Emby/Jellyfin, Nextcloud, carpetas compartidas en SAMBA, etc. De repente te falla el disco 1, donde tienes instalado el sistema.

Sin RAID: El NAS dejará de arrancarte porque te ha fallado el disco, y el OS está instalado en él. Tienes que comprar un disco nuevo, esperar a que llegue, sacar el que ha fallado, instalar el nuevo, reiniciar el NAS y volver a configurar todo,

reinstalar aplicaciones (básicamente como si acabaras de comprar el NAS). Cuando acabes, tienes que acceder a tus backups, y recuperar todos los archivos. Volver a configurar Plex, nextcloud, etc etc. Y durante todo este periodo, a todos los efectos no tienes NAS. Nada de plex, de pelis, carpetas compartidas, nada.

Con RAID: Tu NAS te notifica que el disco 1 ha fallado, y el RAID entra en estado degradado. Todo sigue funcionando igual. Compras el disco nuevo, cambias el disco que ha fallado por el nuevo, y el NAS automáticamente restaura el array a la normalidad. Durante todo el proceso, tu NAS ha seguido funcionando.

Para eso sirve RAID. Es cómodo de tener, y ofrece cierta protección, así que si tienes la opción de usarlo, adelante.

> *"Entonces, ¿Si no me importa todo el tema del downtime, puedo prescindir de usar RAID, y usar solo Backup?"*

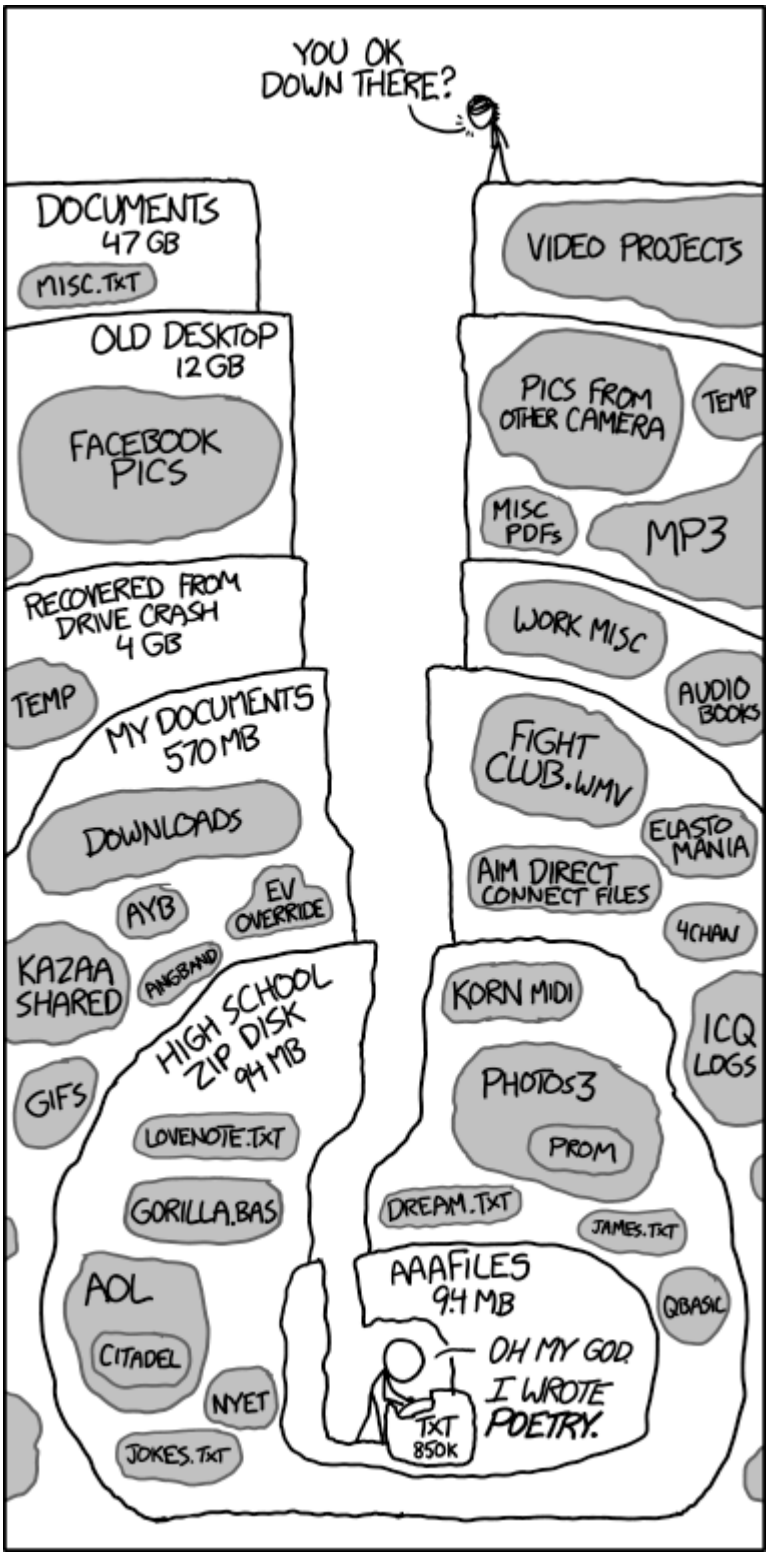
ABSOLUTÁSTICAMENTE SÍ.

> *"Si no puedo permitirme (por los motivos que sean) tener tanto RAID como Backup, y tengo que elegir lo uno o lo otro, ¿Que elijo?*

Backup. Si quieres proteger tus datos, Backup. Siempre Backup. Es mejor tener protección de datos sin redundancia, que redundancia sin protección de datos.

Como planificar backups. Estrategia 3-2-1.

Todos tenemos datos que queremos proteger, y otros que... bueno.



Todos y cada uno de nuestros datos son valiosos... mas o menos

La solución actualmente aceptada como "ideal" para los backups es la estrategia 3-2-1: AL MENOS 3 copias de los datos, en AL MENOS dos unidades distintas, con AL MENOS una copia off-site (en otra localización geográfica).

Esto es así para evitar por ejemplo, desastres naturales, como el incendio de tu domicilio, o un robo, situaciones en las cuales perderás todos los backups que estén en el mismo lugar.

No obstante, a menudo no es posible/conveniente tener una política 3-2-1, sobre todo cuando es mucha la cantidad de datos a proteger. En tal caso, el mínimo absoluto imprescindible podría ser 2-2-0, aunque no es lo recomendable.

También es esencial probar a restaurar tus backups una vez hechos. No sería la primera vez que alguien hace backups de sus datos durante años, solo para descubrir, al intentar restaurarlos tras una pérdida masiva, que hizo algo mal desde el principio, y sus datos no son recuperables. Un backup solo es tan bueno como su capacidad de ser restaurado.

Very Very Importanter!

Primer paso: Determinar tus necesidades de espacio

Es más fácil hacer backup de 3TB que de 40TB. Deberías separar tus datos en tres tipos:

- Datos vitales que quieres proteger (datos personales y fiscales, documentos, fotos, etc). Sobre este grupo deberías aplicar la política 3-2-1. Puedes conseguir cuentas gratuitas de hasta 15GB online (Google Drive, Mega, etc). ¡Asegúrate de encriptar tus backups si vas a subirlos online!
- Datos no tan vitales que te gustaría proteger, pero por los que no estás dispuesto a pagar para almacenar online, y que si se perdieran, podrías continuar con tu vida (más o menos) bien. Puedes aplicar una política 2-2-0 sobre estos datos (ej, cópialos a un disco duro externo).
- Datos que te importan un pimiento. No hagas backup de esto.

Pero ojo, debes tener claro qué te importa y qué no. Yo pensaba que mis 6TB -hoy en día ya casi 8- de multimedia no me importaban en absoluto porque podía descargarlas de nuevo si lo necesitaba, hasta que tuve un apagón y casi pierdo mis datos... y me imaginé el palo enorme que me daba volver a buscar y bajarlo todo. Desde entonces incluí mi biblioteca multimedia dentro de mis backups. Tienes el poder de elegir quien vive y quien muere. Úsalo sabiamente.

Segundo paso: Elegir donde realizarás tus copias de seguridad

- Si el total de datos a respaldar es menor de 12TB, la forma más sencilla es comprar un disco duro externo de alta capacidad (12-14TB) y hacer los backups allí. Los discos Western Digital Elements o My Book son una solución popular, que cuando están de rebajas, pueden conseguirse por hasta 18€/TB. Simplemente conéctalo a tu NAS, y usa el software más te guste para hacer el backup. ¡¡Recuerda SIEMPRE desconectarlo tras acabar la copia, o de lo contrario, puede verse afectado en caso de Ransomware!!

Listo, ya tienes un backup 2-2-0 de tus datos. Si quieres una solución barata

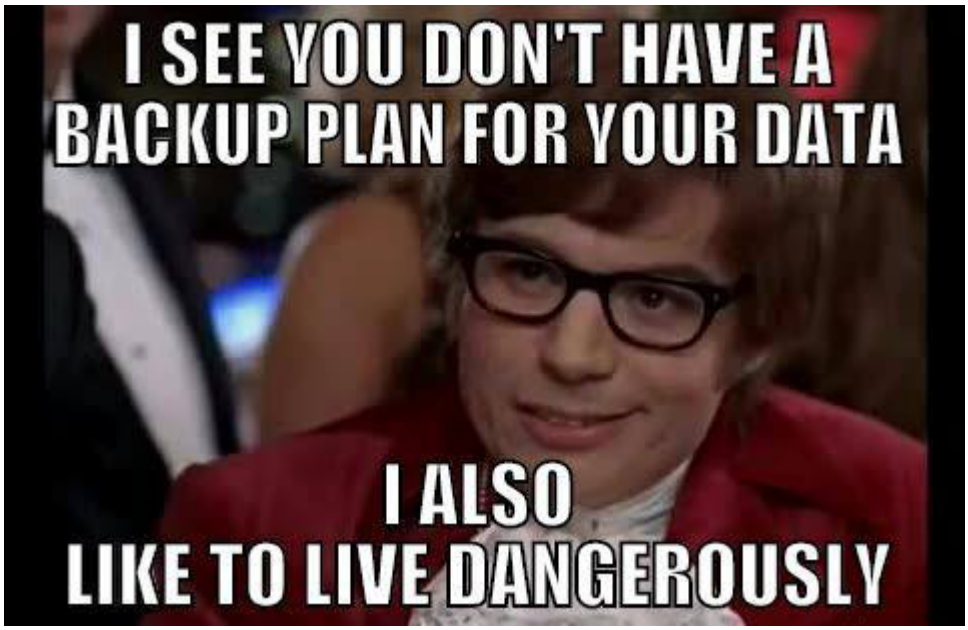
para tener 3-2-1, puedes comprar otro disco (llamemos disco B) y repetir el backup. Entonces te llevas ese disco B y lo guardas en casa de un familiar/amigo (recuerda encriptar solo por si acaso, no sea que alguien curiosee dentro de tu carpeta de "Otros"). Cuando quieras actualizar el backup, lo haces en el disco que tienes en casa (Disco A), te lo llevas a la casa de tu familiar/amigo y dejas allí el Disco A y te traes a casa el disco B y actualizas de nuevo el backup. De este modo tienes copias off-site de forma barata.

- Si el total de datos a respaldar es mayor de 12TB, la cosa se complica. La única forma factible es adquirir otro NAS y crear un RAID o JBOD para usarlo como backup del NAS primario. Sí, ya lo sé.

Si quieres copias off-site, puedes dejar este NAS en casa de un familiar/amigo y hacer las copias de seguridad directamente a través de internet. Si un amigo tuyo también tiene un NAS, podéis acordar que cada uno de vosotros deje X cantidad de TB disponible para el otro en su unidad, de modo que tú haces backup en su NAS, y él hace backup del suyo en el tuyo (recuerda encriptar, lo de la carpeta "Otros").

Siempre puedes simplemente pagar por almacenamiento en la nube (Backblaze, Amazon, etc) y hacer los backups off-site allí. Esto ya depende de cada uno, de sus necesidades, y su poder adquisitivo.

Y por supuesto, siempre puedes decidir no hacer backups. Y es una opción totalmente legítima, siempre que tengas claro que automáticamente pierdes el derecho a cabrearte y patalear cuando (no si, cuando) pierdas tus datos, ya que será 100% culpa tuya.



¿Qué software debería usar?

Esto es una cosa muy personal. Yo personalmente soy muy fan de todo lo que sea FOSS (Free Open Source Software), como por ejemplo Borg Backup, Duplicati o Restic. De todos modos, todas las marcas de NAS ofrecen su propia solución para hacer copias de seguridad (Por ejemplo en QNAP el software se llama Hybrid Station 3), así que alternativas tienes. Elije el que más te guste, y que te sea más fácil de utilizar (que normalmente suele ser el software incluido de serie en el NAS) . Si vas a encriptar, normalmente todos los programas de backup tienen esa opción incluida, así que es suele ser tan fácil como seleccionar esa opción.

Mi setup personal es:

NAS Primario: TS-673 con 5 discos de 10TB en RAID6 (unos 27TB de espacio total usable).

NAS de backup: Synology DS218J con dos discos de 10TB en JBOD.

Agrupo mis datos en dos tipos: Los datos esenciales, que suman menos de

15GB, y los datos menos esenciales, que suman actualmente 13TB. Los datos esenciales se guardan en el DS218J usando un contenedor con Borg Backup, y además se suben online usando un contenedor con rclone a una cuenta en Mega (ambas copias encriptadas).

Los datos menos esenciales se guardan en el DS218J usando Borg Backup, pero no tienen respaldo online (principalmente descargas, copias de seguridad de los múltiples dispositivos/ordenadores, y la biblioteca multimedia).

Espero que este telegraph haya sido de utilidad. Un saludo a todos. :)

Referencia de memes: principalmente Google, xkcd y data-protection-memes