DOSSIER

FALLAIT SAUVEGARDER

LE B.A.-BA DU BACKUP

PAR **DANDU** @**DANDUMONTP**
ET **ONI** @**NICO_ONI**

LA SAUVEGARDE. Un mot important pour une tâche que peu de personnes effectuent. Nous l'avons évoqué en fin de magazine dans le numéro précédent, en nous énervant (virtuellement) sur ceux qui n'en font pas. Et nous avons donc profité de cette occasion pour dédier un dossier entier à cette tâche. Il ne s'agit pas d'un tutoriel, d'un pas-à-pas, mais d'un guide pour vous proposer de bonnes pratiques, vous aider dans vos choix, et vous expliquer les erreurs que vous ne devez pas faire. Nous espérons ainsi vous convaincre de faire une sauvegarde, si possible avant que vous ayez perdu des données.

Avant même de commencer, il faut préciser quelques points. Premièrement, pourquoi sauvegarder ? Si vous n'avez jamais perdu de données, vous n'avez pas nécessairement le réflexe ni l'envie de sauvegarder, et c'est un comportement classique. Vous allez vouloir le faire pour éviter les problèmes mais souvent en dilettante, et généralement le déclic ne se fera que dans la douleur : quand vous aurez justement perdu des données (photos, etc.) auxquelles vous teniez.

Perdre des données ? Mais comment ? Vous vous demandez peut-être comment on peut perdre des données. Les raisons sont pourtant multiples. La plus évidente vient d'un périphérique de stockage qui tombe en panne ou – plus insidieux – qui corrompt le contenu de vos HDD ou SSD. Si vous ne le saviez pas, le taux de panne des disques durs se situe en moyenne aux environs de 1 à 2 %, avec des pics parfois nettement plus hauts sur des séries précises (parfois 6, 7, 10 ou 20 %). Et si vous avez la malchance de posséder une de celles-ci, nous sommes désolés pour vous. Sur les SSD, la fiabilité reste généralement meilleure, mais avec là aussi des exceptions, même si elles sont de plus en plus rares. Vous n'êtes tout de même pas à l'abri d'un bug de firmware inopportun qui se déclenche après plusieurs mois ou années. Deuxième point, l'accident. Un PC portable ou le disque dur externe contenant l'unique exemplaire des photos qui tombe par terre, la foudre, un problème électrique, etc. Troisièmement, le vol ou la perte dans le sens littéral du terme. Vous pouvez oublier un laptop contenant votre thèse dans un train, sur un banc, on peut vous voler votre sac, cambrioler votre maison. Tout ça peut arriver. Ensuite, vous pouvez aussi faire la bêtise de stocker des données sur une clé USB ou une carte mémoire sans avoir de copie. Nous pourrions presque vous dire que vous ne pouvez vous en prendre qu'à vous-même, mais nous allons quand même rappeler un point : **les clés USB et les cartes mémoire ne sont pas fiables.** Vous avez beaucoup plus de chances de perdre des informations avec ces périphériques qu'avec un disque dur ou un SSD (même si – comme absolument personne – vous éjectez vos périphériques en toute sécurité). Dans une autre veine, un logiciel peut avoir un bug. Vous pouvez être contaminé par un virus qui va effacer ou chiffrer vos données. Une mise à jour de l'OS peut poser des soucis. Enfin, il y a l'erreur accidentelle, mais de votre part. Vous pouvez supprimer un dossier contenant des informations importantes, sans passer par la corbeille. Mal lire un message de votre OS ou de votre logiciel préféré. Faire une mauvaise manipulation[1]. Eh oui, ça arrive à tout le monde.

C'est plus important avec un SSD. Même si la fiabilité des SSD est meilleure que celle des disques durs, nous vous conseillons de sauvegarder plus fréquemment avec ces derniers. Ça peut sembler paradoxal, mais récupérer des données sur un HDD endommagé reste du domaine du possible dans certains cas, contrairement aux SSD. La gestion de l'usure couplée au chiffrement du contenu, sans même prendre en compte qu'il est parfois impossible d'accéder à la mémoire flash en dehors de l'appareil d'origine, implique que des données perdues sur un SSD sont… perdues.

Définissons la sauvegarde. Vous allez peut-être trouver ça bizarre, mais il faut vraiment définir ce qu'est une sauvegarde et son but. Nous avons vu trop souvent des personnes penser en toute bonne foi qu'elles en avaient une… alors que non. Premièrement, une sauvegarde est une copie de vos données. C'est-à-dire qu'il existe plusieurs exemplaires des mêmes informations. Déplacer les photos du SSD trop petit du PC portable vers un disque dur externe, ce n'est pas sauvegarder. Garder une copie des photos avant d'effectuer les retouches, ce n'est pas une sauvegarde. Nous devons aussi préciser que la modification d'une version n'affecte pas l'autre directement. Placer les données sur un NAS avec des disques en RAID1 n'est pas une sauvegarde. De même, un service de *cloud* qui effectue une synchronisation n'est pas une sauvegarde. S'il existe différentes possibilités pour faire un *backup*, et c'est

Une sauvegarde est une copie de vos données. C'est-à-dire qu'il existe plusieurs exemplaires des mêmes informations.

SUR LE CRUCIAL M4, LE PREMIER FIRMWARE PLANTAIT LE SSD APRÈS 5 200 HEURES.

CE MODÈLE 12 TO DE SEAGATE ATTEINT UN PEU PLUS DE 3 % DE TAUX DE PANNE CHEZ BACKBLAZE.

PAS BESOIN D'ALLER VERS DES CLÉS USB ACHETÉES SUR WISH POUR AVOIR DES SOUCIS DE FIABILITÉ.

LE FAIT QU'UN NAS UTILISE DEUX DISQUES EN RAID1 N'IMPLIQUE PAS UNE « *SAUVEGARDE* ».

SI VOUS AVEZ BESOIN D'UN GROS DISQUE DUR EXTERNE, LACIE PROPOSE DES MODÈLES 12 BAIES.

le sujet de ce gros dossier, nous pouvons tout de même faire une distinction entre les sauvegardes « *d'usage* » et les sauvegardes *froides*. La première va être essentiellement présente pour éviter de perdre des données à court terme, pour continuer à travailler, etc. C'est la plus courante, et son but n'est pas de préserver les données dans le temps, mais d'avoir une solution pour récupérer rapidement des informations en cas de soucis, avec les points évoqués dans la page précédente. Il peut s'agir d'une copie sur un disque dur externe, sur un NAS, dans le *cloud*. Elle doit être régulière, idéalement automatisée, et sur un support fiable. Nous allons expliquer dans la suite comment faire. La sauvegarde *froide*, elle, va servir pour des archives, pour garder des documents à long terme. Elle ne doit pas nécessairement contenir vos fichiers de travail, n'a pas besoin d'être accessible dans la minute, etc. Elle a moins d'intérêt dans un usage grand public classique, et nous en parlerons page 70.

Le piège de la sauvegarde manuelle. Dans la suite, nous allons vous expliquer quel matériel utiliser, et quel(s) logiciel(s) choisir, avec en ligne de mire une sauvegarde automatisée. La manuelle, quoi que vous puissiez penser, ne fonctionne pas. Certains préfèrent effectuer une copie complète de leurs données tous les dimanches à 14 h (par exemple), ou déplacer manuellement les photos, sauvegarder le contenu du smartphone en le branchant à un PC, etc. Mais l'expérience montre que vous oublierez de le faire, que vous ferez des erreurs, que vous omettrez des données. Soit parce que vous n'avez pas pensé à les sauver, soit parce que votre application décide de stocker ses informations à un endroit improbable. Se dire que vous allez sauver vos données sans vous reposer sur des automatisations demeure le meilleur moyen de se rendre compte qu'il n'y a plus de sauvegarde depuis des mois, évidemment au moment où vous en avez besoin.

Que faut-il sauver ? Le dernier point, avant de passer à des conseils pratiques, va consister à définir le périmètre de la sauvegarde. Dans l'idéal, vous pouvez tout sauver. Pas mal de logiciels partent de ce postulat et gardent donc une copie de votre OS, de vos fichiers de travail, de l'ensemble de vos données. Ce choix implique que vous disposez soit de peu de documents, soit d'un bon espace de stockage externe avec d'excellentes performances. Si vous travaillez sur de la vidéo ou dans des domaines qui génèrent beaucoup d'informations, nous vous conseillons d'essayer de ne pas sauvegarder les fichiers de travail, pour accélérer les transferts et ne pas remplir trop vite vos disques durs. Vous risquez évidemment de perdre quelques heures de boulot, mais en contrepartie vous simplifierez les autres tâches. Le problème reste un point évoqué plus haut : sélectionner les données à sauvegarder explicitement (ou celles à ne pas sauver) peut amener des erreurs. Malgré tout, il faut arriver à trouver un bon compromis entre transparence et efficacité. Si votre ordinateur passe une partie de son temps à faire des sauvegardes, avec parfois un impact visible sur les performances, vous aurez envie de les désactiver complètement. Et c'est justement pour éviter ce genre de choses que nous avons choisi d'écrire ce dossier.

1. L'auteur de ces lignes, pendant le test du dock Thunderbolt de Seagate (page 35), a par exemple formaté son disque dur de sauvegarde par erreur.

Sous Windows

Sous Windows, la sauvegarde n'a jamais vraiment été mise en avant. L'OS propose des solutions intégrées, mais les logiciels externes offrent souvent plus de fonctions.

La solution de base consiste à utiliser les fonctions de Windows 10. Dans les **Paramètres**, allez dans **Mise à jour et sécurité**, puis dans **Sauvegarde**. Vous pouvez choisir le disque dur de sauvegarde, la fréquence, restaurer des fichiers, etc. Si l'idée semble bonne, l'intégration de Microsoft manque tout de même de finition : comme dans pas mal de fonctions de Windows 10, vous passerez d'une interface moderne (« Metro ») à une ancienne, proche de ce qui se faisait sous Windows 7. Le principal problème, c'est que la fonction de sauvegarde se limite à quelques dossiers par défaut, ceux contenant les données des utilisateurs. Le bureau, les différents dossiers liés aux documents, mais pas l'OS lui-même ou les programmes. Vous pouvez bien évidemment ajouter les dossiers où vous stockez vos données, ou en exclure certains, mais l'ensemble reste assez limité. C'est suffisant pour sauver vos photos, mais pas pour pouvoir récupérer un système complet par exemple. Typiquement, si vous êtes la cible d'un ransomware, la sauvegarde de Windows 10 risque de ne pas être très utile : les *backups* seront sûrement chiffrés. Enfin, l'interface n'est pas très *user friendly*, l'ensemble étant bien camouflé dans les menus, etc. En clair, ça existe, ça peut être intéressant… mais personne ne sait que c'est là.

L'OUTIL DE MICROSOFT PROPOSE PEU D'OPTIONS.

WINDOWS 10 INTÈGRE UN OUTIL DE SAUVEGARDE. SI.

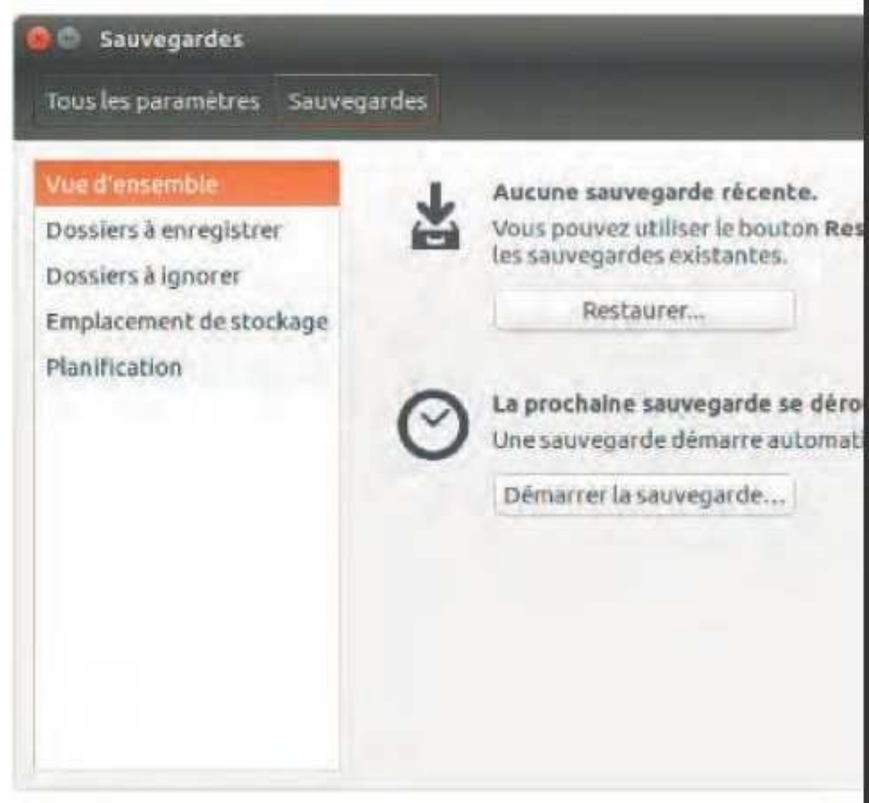
Les autres logiciels. Il existe des dizaines (littéralement) de logiciels pour effectuer des sauvegardes, que ce soit d'une partie des fichiers ou de l'ensemble du système. Nous pouvons vous conseiller quelques programmes, que nous avons testés. Le premier, que nous préférons, est Veeam Agent (*cpc.cx/VeeamAgent*) dans sa version gratuite. Il a le défaut de nécessiter une inscription pour être téléchargé, mais une fois installé, il reste très discret. Le logiciel permet – par défaut – de garder un historique des modifications sur 14 jours, de sauvegarder en externe ou sur un NAS, etc. Veeam est une application professionnelle et ça se voit : il propose de créer une clé USB pour restaurer si l'OS ne démarre pas, ne demande pas en permanence d'acheter une licence, etc. La version gratuite n'a pas de grosses limites, en dehors du fait qu'elle ne peut gérer qu'une seule tâche. Par défaut, une sauvegarde quotidienne est programmée – le logiciel peut même allumer votre PC –, et vous ne pouvez donc pas décider de sauvegarder le C:\ à une heure précise et le D:\ à un autre moment. Un inconvénient mineur en pratique, tant le logiciel est efficace. Le second est EaseUS Todo Backup (*cpc.cx/EaseUs*) dans sa version gratuite. Il permet de sauvegarder facilement tout le système sur le *cloud*, sur un disque dur externe ou un NAS, et fonctionne bien. La version payante (27 €) ajoute quelques options qui peuvent servir si vous avez beaucoup de PC à sauver, mais elle n'a rien d'obligatoire. Nous n'avons pas la place dans le magazine pour vous détailler les nombreux autres programmes, mais il en existe beaucoup, comme BackupChain, Comodo BackUp, etc. le choix dépendra tout de même de vos connaissances (certains visent des utilisateurs aguerris) et de votre patience face à la publicité : beaucoup de logiciels gratuits forcent la main pour passer à la version payante (ce qui n'est pas le cas de Veeam). Reste que dans tous les cas, le fonctionnement demeure assez similaire : un programme lancé au démarrage surveille votre disque dur et sauve les fichiers modifiés sur un support externe. Et nous allons détailler les possibilités dans les pages suivantes.

PAS BESOIN DE LICENCE.

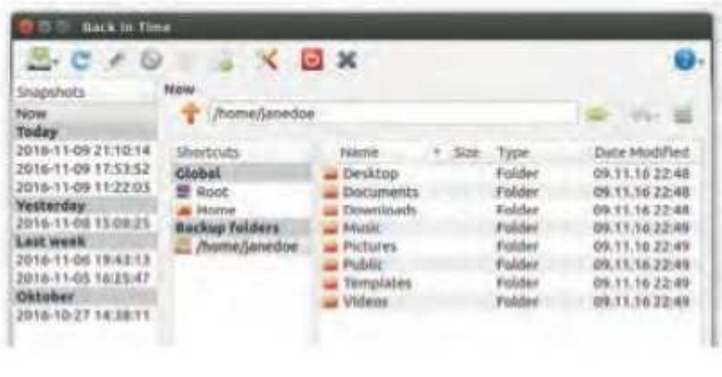
LES RÉGLAGES DE VEEAM, ASSEZ COMPLETS.

Sauvegarder ses données sous Linux

Linux dispose de nombreux outils pour gérer ses données, aussi bien pour de la sauvegarde locale que distante. Notez que nous vous proposerons, pour chaque application, un lien vers les sources afin de le compiler et l'installer vous-même, mais la plupart des distributions actuelles disposent d'un gestionnaire automatique de paquets où vous pourrez également les trouver.



BackInTime CPC.CX/BACKINTIME



BackInTime est un logiciel de sauvegarde qui mise beaucoup sur sa simplicité, et passe donc par une interface graphique assez claire. Son fonctionnement rappelle quelque peu celui de Time Machine pour macOS, à savoir qu'il propose entre autres la possibilité d'effectuer une sauvegarde incrémentale distante (via SSH) et chiffrée de son disque dur. Il se base pour cela sur rsync, un outil de synchronisation automatique de fichiers qui constitue d'ailleurs le cœur de nombreux programmes de sauvegarde sous Linux. Concernant les autres options, BackInTime gère également la sauvegarde locale (chiffrée ou non), la planification d'une ou plusieurs sauvegardes ou la gestion automatique de l'espace sur le disque recevant les données (par exemple la suppression des sauvegardes plus anciennes). Notez que le fichier de configuration est indispensable au fonctionnement de BackInTime, pensez donc à copier ce dernier dans un endroit sûr si vous comptez restaurer vos données sur une nouvelle machine plus tard. Bien entendu, ne l'incluez pas dans votre sauvegarde, cela reviendrait à enfermer vos clés dans votre voiture.

Bacula CPC.CX/BACULA

Bacula est un système de sauvegarde basé sur MySQL, ce qui signifie que son utilisation et ses réglages pourront se faire directement depuis un navigateur (en passant par Webmin) et de n'importe quelle machine sur votre réseau local. Cela veut dire également que ses paramètres pourront être un peu plus complexes qu'avec un logiciel disposant de sa propre interface, et nécessiteront souvent d'aller modifier directement les fichiers de configuration (de nombreux tutoriels sont disponibles en français sur Internet). En outre, son interface a la réputation de ne pas être des plus intuitive. En contrepartie, vous pourrez alors planifier la sauvegarde de plusieurs machines sur votre réseau, retrouver différentes versions d'un même fichier à une date précise, et accéder à de nombreux autres paramètres que certains outils ne proposent pas. Il est possible de choisir entre une sauvegarde différentielle ou incrémentale, ainsi que les données à inclure ou exclure d'une sauvegarde.

Déjà Dup CPC.CX/DEJADUP

Si vous avez installé Ubuntu, vous disposez déjà d'un outil de sauvegarde livré avec le système et plutôt performant. Évidemment, il est également disponible pour d'autres distributions, et vous avez toujours la possibilité de compiler les sources pour le lancer sur votre propre machine. Déjà Dup est assez simple d'utilisation et propose sa propre interface graphique (une norme sous Ubuntu). Il vous permettra notamment de paramétrer les dossiers à sauvegarder et ceux à ignorer, l'emplacement de destination et la planification de vos sauvegardes. Pour le reste, vous n'aurez qu'à faire confiance à deux gros boutons sur l'écran principal : sauvegarder et restaurer. Il gère également la sauvegarde et la restauration sur un disque dur en réseau *via* SSH et est compatible avec certains services de stockage en ligne comme Amazon S3. Enfin, cet outil est capable de chiffrer vos sauvegardes pour les rendre illisibles en cas de vol de votre matériel.

Sauvegarder chez Apple

Chez Apple, le problème de la sauvegarde est réglé depuis pas mal d'années, que ce soit sous macOS ou sous iOS. Mais même si les outils existent, certains ne prennent pas la peine de le faire : nous vous proposons donc un petit aperçu.

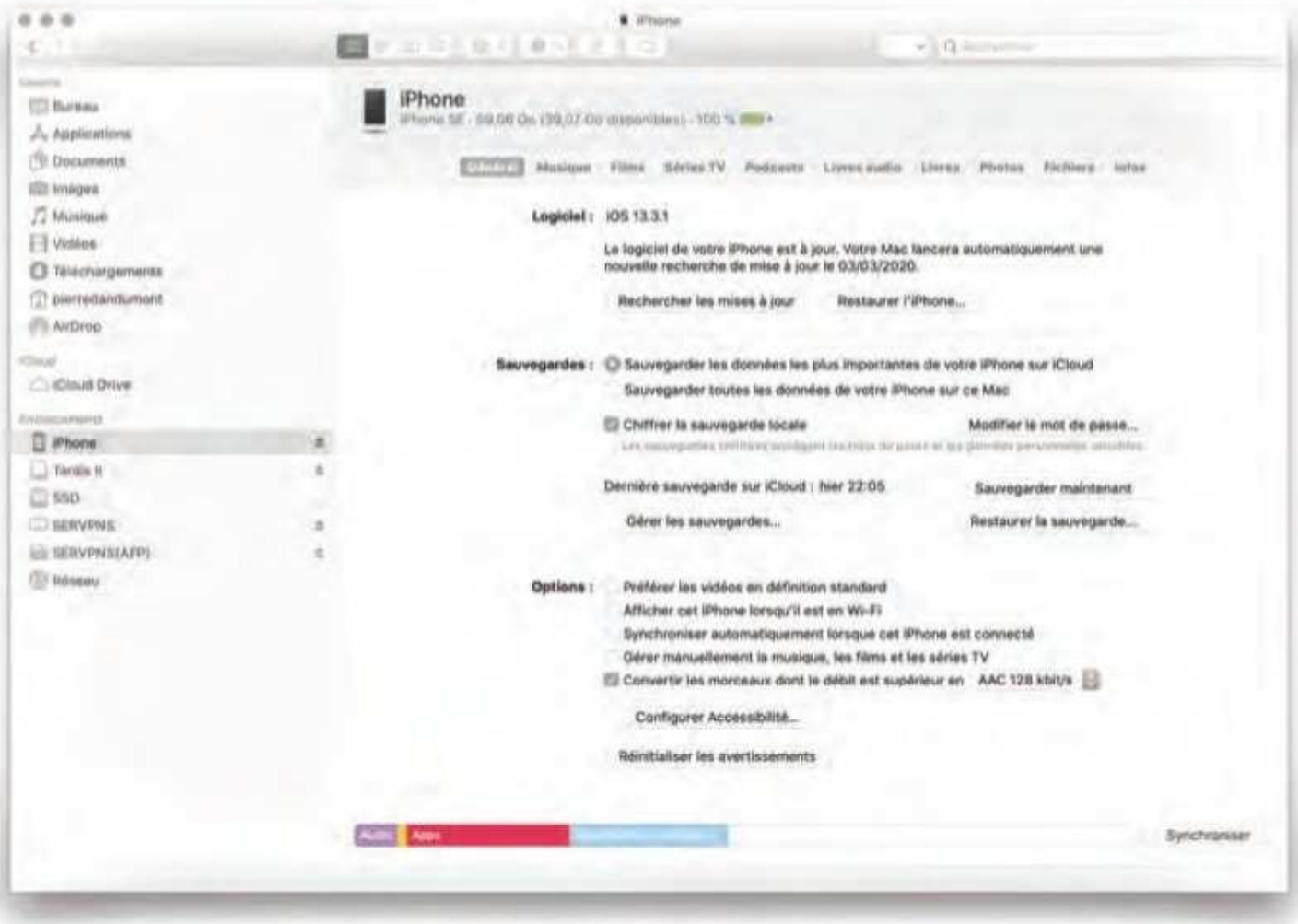
Commençons par macOS (le nom actuel de Mac OS X). Apple a intégré un logiciel de sauvegarde directement dans les fondations de l'OS dès 2007 avec Mac OS X Leopard. Depuis, Time Machine permet de sauvegarder facilement et de façon transparente le contenu d'un Mac. La solution travaille véritablement en tandem avec les systèmes de fichiers d'Apple (HFS+ et APFS plus récemment) pour déterminer les fichiers modifiés et ensuite sauver ces derniers toutes les heures, dans un cas idéal. Les possibilités de retour en arrière qui donnent son nom à la technologie dépendent évidemment de l'espace disque, et le Time Machine garde plusieurs versions de chaque fichier. Si tout se passe bien, il enregistre toutes les modifications horaires de la dernière journée, toutes les modifications quotidiennes du dernier mois, et toutes les modifications hebdomadaires depuis la création de la sauvegarde (ouf). L'interface permet de revenir en arrière assez facilement et de récupérer un document effacé ou modifié. La seconde fonction va être la réinstallation rapide : en démarrant le Mac sur la partition de restauration, il devient possible de retourner à un instant *t*.

Le matériel nécessaire. Time Machine peut fonctionner soit avec un disque dur local (interne ou externe), soit en réseau. Dans le premier cas, il doit être formaté en HFS+ (l'ancien système de fichiers d'Apple) et connecté régulièrement (ou même être branché à demeure pour éviter les sauvegardes à rallonge). À chaque lancement de Time Machine (toutes les heures par défaut), le programme va lister les modifications et copier les données en question sur le disque, après avoir nettoyé les anciennes sauvegardes. Si vous manquez d'espace de stockage, il effacera les fichiers les plus anciens – Time Machine garde toujours une copie complète du système – ou vous expliquera qu'il est impossible d'effectuer une sauvegarde. Dans l'absolu, nous vous recommandons évidemment un périphérique externe rapide, USB 3.0 ou Thunderbolt. Pour la sauvegarde en réseau, il existe plusieurs choix. Les deux premières sont datées : sur un Mac équipé de la variante *serveur* de macOS (un cas rare) ou sur un boîtier Time Capsule. Cette gamme de produits, abandonnée, combinait un disque dur (sans redondance) avec un point d'accès Wi-Fi. La troisième ne vous étonnera pas : un NAS. Attention, beaucoup de vieux modèles utilisent une implémentation *open source* pour la sauvegarde en AFP (un protocole réseau Apple), avec une fiabilité assez aléatoire. Il vaut donc mieux passer sur un NAS qui intègre Time Machine avec la prise en charge du protocole SMB, dont Apple a publié la documentation. En pratique, les NAS des grands constructeurs (Synology, QNAP, etc.) sont généralement compatibles. La seule contrainte sera de posséder un Mac récent : la sauvegarde en SMB nécessite macOS Sierra (10.12, 2016) au minimum. Sur les OS précédents, vous ne pourrez utiliser que l'AFP et sa fiabilité aléatoire avec les NAS.

UN BOÎTIER TIME CAPSULE : POINT D'ACCÈS WI-FI ET DISQUE DUR DE SAUVEGARDE.

L'INTERFACE DE TIME MACHINE : ON CHOISIT UN DISQUE, ON VÉRIFIE DE QUAND DATE LA SAUVEGARDE LA PLUS ANCIENNE.

TIME MACHINE PERMET DE REMONTER DANS LE TEMPS.



MACOS CATALINA DÉPLACE LA SAUVEGARDE LOCALE DANS LE FINDER.

LA SAUVEGARDE ICLOUD S'EFFECTUE NORMALEMENT LA NUIT.

L'IPAD PRO ET SA CAPACITÉ DE 1 TO : GROS FORFAIT ICLOUD RECOMMANDÉ.

Les défauts de Time Machine. La technologie d'Apple n'est pas sans défaut. En dehors de la fiabilité aléatoire en AFP sur un NAS, elle peut être très lente, spécialement sur les Mac modernes avec macOS Catalina. Si vous modifiez beaucoup de fichiers, la sauvegarde peut prendre plusieurs heures, surtout si vous travaillez en même temps : les processus se lancent avec une priorité assez faible. Ensuite, les gros *backups* peuvent parfois se corrompre, surtout s'ils remontent à plusieurs années. Enfin, mais c'est inhérent à tous les systèmes présentés, il faut tout de même penser à brancher un disque. Si macOS propose d'utiliser Time Machine au premier branchement d'un HDD compatible (formaté en HFS+), il ne demande pas de le faire à l'installation. Malgré tout, l'OS notifie l'utilisateur quand le disque de sauvegarde n'a pas été connecté depuis 10 jours.

iOS et la sauvegarde en local. Pour iOS, qui est apparu à peu près en même temps que Time Machine, Apple a intégré un dispositif de sauvegarde dès le départ. Contrairement à son pendant macOS qui permet un retour en arrière, la sauvegarde sert à garder un *backup* en cas de soucis. Elle va essentiellement être utilisée lors d'un changement d'appareil (iPhone, iPad, Apple Watch, etc.), que ce soit pour un problème matériel (chute, coque pliée, etc.) ou tout simplement le passage à un modèle plus récent. La première méthode, historique, passe par iTunes (et le Finder sous macOS Catalina). Elle permet d'effectuer une sauvegarde sur un ordinateur (Mac ou PC) avec une liaison filaire (et un câble propriétaire) ou en Wi-Fi. Depuis quelques versions d'iTunes, cette sauvegarde comprend tous les paramètres ainsi que les données personnelles, mais pas les applications, qui sont récupérées depuis les serveurs d'Apple. Il est donc impossible de sauvegarder une app' qui n'est plus proposée sur l'App Store. Pour ceux qui utilisent un ordinateur partagé (par exemple), la sauvegarde peut être chiffrée, une option obligatoire pour qu'elle garde les informations sur la santé et les mots de passe.

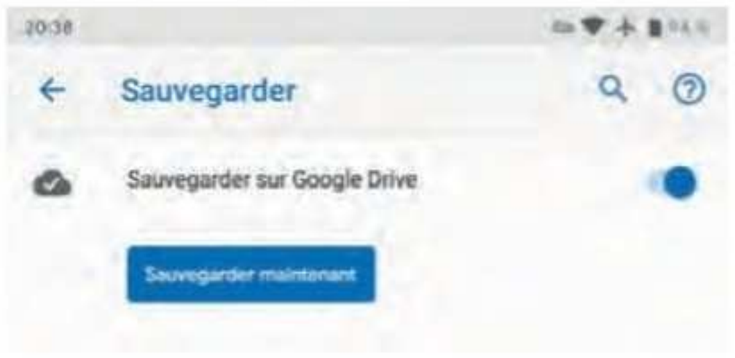
Le cas iCloud. La seconde méthode passe par iCloud, et elle possède des avantages mais aussi des inconvénients. Le plus gros atout reste la transparence, dans une certaine mesure : iOS effectue une sauvegarde quand l'appareil est en charge, verrouillé, et connecté à un réseau Wi-Fi. Pour résumer, s'il est en train de charger chez vous la nuit. Le premier problème dépend de ce fonctionnement : sans connexion à Internet fixe, pas de sauvegardes. Le second va être lié au coût : Apple n'offre que 5 Go d'espace de stockage avec iCloud, et si vous commencez à enregistrer beaucoup de données (photos, vidéos, etc.), vous arriverez vite aux limites. Comme pour la sauvegarde locale, iCloud sauve les informations de l'utilisateur mais pas les applications : en cas de restauration, elles sont téléchargées directement depuis les serveurs. Si vous avez plusieurs périphériques ou si vous filmez beaucoup, vous devrez tout de même débourser quelques euros pour passer sur une offre iCloud payante (dès 1 €/mois pour 50 Go). Enfin, en dehors des contraintes pécuniaires, les performances d'iCloud dépendent – comme toujours avec le *cloud* – de votre connexion. Avec une ligne ADSL et un *upload* anémique, les sauvegardes peuvent prendre beaucoup de temps, en particulier si vous filmez beaucoup par exemple.

Sauvegarder sous Android

Un vol de téléphone étant vite arrivé, il est essentiel de sauvegarder régulièrement les données de son smartphone, histoire de ne pas perdre définitivement vos photos, contacts et autres fichiers personnels en même temps que votre précieux appareil. Voici donc quelques options qui s'offrent à vous, utilisateurs d'Android.

Google Drive

La solution la plus simple et la plus répandue sous Android est certainement l'outil de sauvegarde fourni par Google, ne serait-ce que parce qu'il est intégré au système. Depuis Android 5.0 (Lollipop), cette option est d'ailleurs présente et activée par défaut, utilisant alors votre espace de stockage gratuit pour sauvegarder sur le *cloud* via votre compte Google. Cet outil propose des réglages assez intéressants, comme les données à inclure dans le transfert (applications, SMS, contacts, etc.) et permettra, lors de l'utilisation d'un nouvel appareil Android, de restaurer automatiquement la sauvegarde à partir de votre compte Google. Notez que si



cette fonction est compatible avec les photos stockées sur votre téléphone, elle nécessitera néanmoins d'activer un espace Google Photo pour que leur transfert soit effectif, puisque c'est là qu'elles seront conservées. Enfin, même si les sauvegardes sont effectuées automatiquement lors de la mise en charge, à condition que votre téléphone ait accès à un réseau Wi-Fi, il est aussi possible de lancer une sauvegarde manuelle à tout moment.

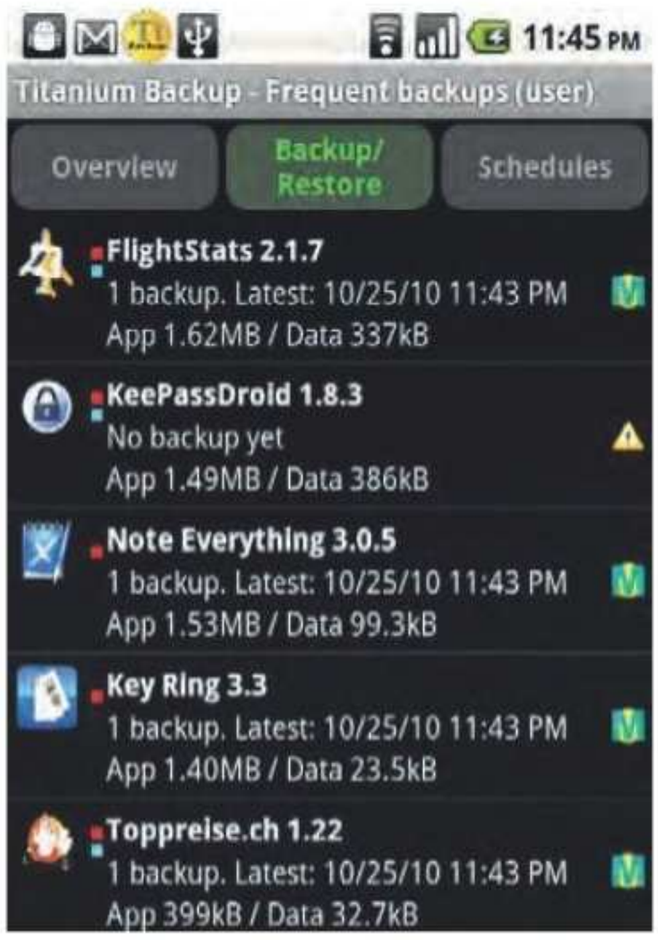
Helium CPC.CX/HELIUM

Helium est une application disponible gratuitement sur le Google Play Store (anciennement nommée Carbon), et qui nécessite de fonctionner de pair avec une extension fournie pour Google Chrome. Cela a l'avantage de rendre la solution compatible avec n'importe quel système d'exploitation (Windows, macOS ou Linux) et ne demande pas d'apporter de modifications particulières au téléphone. Une fois l'application installée, elle permet d'effectuer des sauvegardes ou la restauration de vos données depuis le disque dur de votre ordinateur. Vous pourrez également planifier vos sauvegardes et leur périodicité, ainsi que la nécessité ou non de passer par un réseau Wi-Fi ou d'avoir un appareil en charge. Enfin, Helium est compatible avec la sauvegarde sur des services en ligne, notamment Dropbox, Google Drive et Box.

Titanium Backup

CPC.CX/TITANIUM

Titanium Backup a la réputation d'être l'un des meilleurs outils de sauvegarde pour Android, avec un défaut majeur toutefois : il nécessite de *rooter* son téléphone afin d'en modifier les droits d'administration. Cette opération est expliquée dans de nombreux tutoriels en ligne, et vous permettra de profiter de cette application, elle aussi disponible gratuitement sur le Google Play Store. Titanium Backup est capable de sauvegarder n'importe quelle donnée de votre téléphone vers une archive compressée, que vous pourrez ensuite transférer vers votre ordinateur ou un disque dur quelconque. Vous aurez également le choix de planifier vos sauvegardes et de restaurer celles-ci en un clic le cas échéant. Notons que Titanium Backup existe dans une version payante, ce qui ajoute la possibilité de mettre une application en hibernation ou encore une gestion plus complète de la restauration des données.



Les disques durs externes

La solution de base, pour une sauvegarde simple, va passer par un disque dur externe. Mais le choix du modèle a de l'importance et dépendra de vos besoins et de votre usage.

Commençons par les disques durs, nous évoquerons les SSD ensuite. Il existe deux grandes familles de disques durs externes : les modèles portables – équipés d'un HDD 2,5 pouces – et ceux de bureau. Les premiers restent évidemment les plus populaires : le format est compact, la capacité peut atteindre 5 To et ils s'alimentent directement à travers le bus USB. Les seconds demandent une prise de courant (sauf dans des cas très particuliers en USB-C), mais la capacité peut monter nettement plus haut (10 To et plus), tout comme les prix.

Avantages et inconvénients des modèles portables. Un disque dur portable classique proposera une capacité suffisante pour de la sauvegarde et pour transporter des données. Comptez environ 60 € pour 1 To, ~90 € pour 2 To, 100 à 120 € pour 3 To, 120 à 170 € pour 4 To et jusqu'à 200 € pour 5 To. L'interface la plus courante reste l'USB 3.0, mais quelques modèles – rares et onéreux – passent par du Thunderbolt (1, 2 ou 3), une technologie sans intérêt dans ce cas. Préférez un HDD doté d'un câble amovible, pour plusieurs raisons. D'abord, ce choix vous permettra de passer sur un câble plus court ou plus long, en fonction de vos besoins. Ensuite, vous pourrez évoluer vers l'USB-C (si votre PC n'en a pas) ou brancher le disque sur n'importe quel PC, même s'il est USB-C au départ. Enfin, la connexion au disque dur peut être fragile, et perdre une sauvegarde ou des données à cause d'un câble endommagé pourrait vous énerver. Pour les performances, les disques durs actuels dépassent 100 Mo/s en lecture et en écriture et ce point ne devrait pas vous gêner. Mais si c'est le cas, tournez-vous vers un SSD. La différenciation entre les modèles viendra essentiellement du design, et ce n'est pas uniquement esthétique. Si vous êtes un baroudeur, un périphérique renforcé avec une coque en mousse peut être intéressant. Si nous vous déconseillons de fabriquer votre propre disque dur externe pour une question bassement financière (voir l'encadré), le choix de la marque peut avoir de l'importance. Il existe actuellement trois grands constructeurs : Seagate, Toshiba et Western Digital, et le dernier a la désagréable habitude d'intégrer le contrôleur USB directement sur le disque dur. En cas de casse sur la prise USB avec un Seagate ou un Toshiba, il reste parfois possible de récupérer le disque dur en le branchant en SATA dans un PC, ce qui n'est pas permis avec les WD. Enfin, méfiez-vous des modèles de plus de 3 To (notamment chez Seagate) pour des usages lourds (lancement d'applications, sauvegardes très fréquentes ou incrémentales, etc.) : ils utilisent généralement la technologie SMR, et cette dernière réduit les performances en écriture si le HDD est rempli dans certains cas (voir *CPC Hardware* n° 42). Pour du stockage froid, en revanche, le problème ne se posera pas.

Préférez un HDD doté d'un câble amovible, pour plusieurs raisons pratiques.

CERTAINS MODÈLES WD INTÈGRENT DIRECTEMENT DE L'USB SUR LE PCB, SANS SATA.

LES DISQUES DURS EXTERNES SEAGATE PEUVENT ATTEINDRE 5 TO EN 2,5 POUCES, MAIS EN SMR.

Une histoire de taxe

Certains conseillent d'acheter un disque dur interne et un boîtier pour réduire les coûts, en espérant éviter la fameuse rémunération pour copie privée française. Mais en pratique, vous procurer un modèle externe va être plus simple et souvent plus intéressant financièrement : malgré la redevance en question, les variantes externes valent moins cher qu'un disque dur interne seul, sans même prendre en compte le prix du boîtier. Les raisons sont multiples, la principale demeure que les volumes de ventes sont bien plus élevés sur l'externe, ce qui permet de réduire les marges.

LES SSD EXTERNES CONTIENNENT SOUVENT UN SSD CLASSIQUE EN FORMAT « BARRETTE », MSATA OU M.2 SATA.

Acheter un externe pour de l'interne ?

Petit parallèle avec la page précédente. Si un disque dur externe est moins onéreux qu'un interne, pourquoi ne pas acheter une version externe pour le disque qu'il contient ? L'idée peut paraître séduisante et fonctionner, mais attention : les disques durs vendus en externe ne sont pas garantis s'ils sont utilisés en dehors du boîtier. De plus, nous l'évoquons, certains modèles 2,5 pouces (notamment WD) offrent de l'USB en natif, sans SATA. Enfin, les 2,5 pouces externes sont souvent épais (12,5 ou 15 mm) et les PC portables n'acceptent que les modèles de 7 et 9,5 mm.

Les modèles desktop pour les grandes capacités. Les modèles de bureau sont en perte de vitesse, c'est une évidence : ils se retrouvent entre des versions portables de 5 To et des NAS, plus polyvalents. Les recommandations demeurent identiques : préférez un câble amovible et restez en USB 3.0 car la bande passante suffit amplement. Un bon HDD *desktop* restera plus rapide qu'un portable, et certains atteignent plus de 200 Mo/s, mais ce critère reste biaisé : un simple SSD externe montera bien plus haut. Dirigez-vous vers un HDD qui tourne à 5 400 tpm, les variantes 7 200 tpm sont plus bruyantes et le gain éventuel demeure limité dans un usage classique. Pour l'alimentation, préférez un modèle avec un transformateur externe et une prise standard : en cas de panne, le changement sera aisé. Actuellement, la capacité peut atteindre 16 To en 3,5 pouces, mais les disques durs externes qui dépassent 10 To utilisent aussi parfois deux disques en RAID. Nous vous déconseillons fortement ce choix : la fiabilité en prend un coup, et un NAS semble plus adapté dans ce cas de figure. Reste qu'un des avantages des modèles *desktop* va être l'éventuelle récupération en cas de panne : vous aurez dans tous les cas la possibilité de transplanter le disque dur dans un PC, en le branchant en SATA.

La mémoire flash pour les sauvegardes ? Les SSD externes se retrouvent dans les poches des adeptes des nouvelles technologies, spécialement depuis la mi-2019, avec des prix assez bas sur la mémoire flash. Ils offrent pas mal d'avantages sur le papier : des performances élevées (jusqu'à 1 Go/s en USB, encore plus en Thunderbolt 3), un format parfois plus compact, un coût jugé abordable. Fin février 2020, on a pu trouver des SSD de 500 Go pour moins de 100 € et les variantes de 1 To restent sous les 150 €. Pour autant, nous pensons qu'ils remplacent les clés USB et ne devraient servir que pour transporter des données facilement, pas pour des sauvegardes. Premièrement, pour des questions de capacité et de prix : les modèles de 2 To et plus valent encore assez cher. Deuxièmement, parce que la mémoire flash pose quelques soucis pour des *backups* pérennes. La NAND possède une durée de vie limitée et la rétention n'est pas éternelle. Si les constructeurs indiquent souvent au moins 10 ans – ce qui reste finalement peu pour des sauvegardes à long terme –, elle diminue avec l'usure de la mémoire, donc avec l'usage. Enfin, la récupération des données sur un SSD endommagé demeure compliquée. Dans la majorité des cas, entre le chiffrement et le fait que les pannes sont plus brutales que sur les HDD (voir page 73), un problème implique la perte totale des données. Nous l'avons déjà indiqué dans ce dossier, mais il semble important de le marteler : évitez soigneusement les cartes SD et clés USB pour les sauvegardes ; la fiabilité est trop faible dans le temps, notamment à cause de l'absence de gestions de l'usure (ou d'algorithmes trop basiques). Et les versions haut de gamme qui corrigent ce problème valent souvent plus qu'un SSD externe tout en offrant les mêmes soucis pour ce type d'usage.

DANS LES DISQUES DURS EXTERNES, LA CAPACITÉ PEUT ATTEINDRE 14 TO.

LES MICROSD « ENDURANCE » (LE NOM VARIE SELON LE FABRICANT) RÉSISTENT BIEN DANS LE TEMPS, MAIS SONT PLUS ONÉREUSES QU'UN SSD EXTERNE.

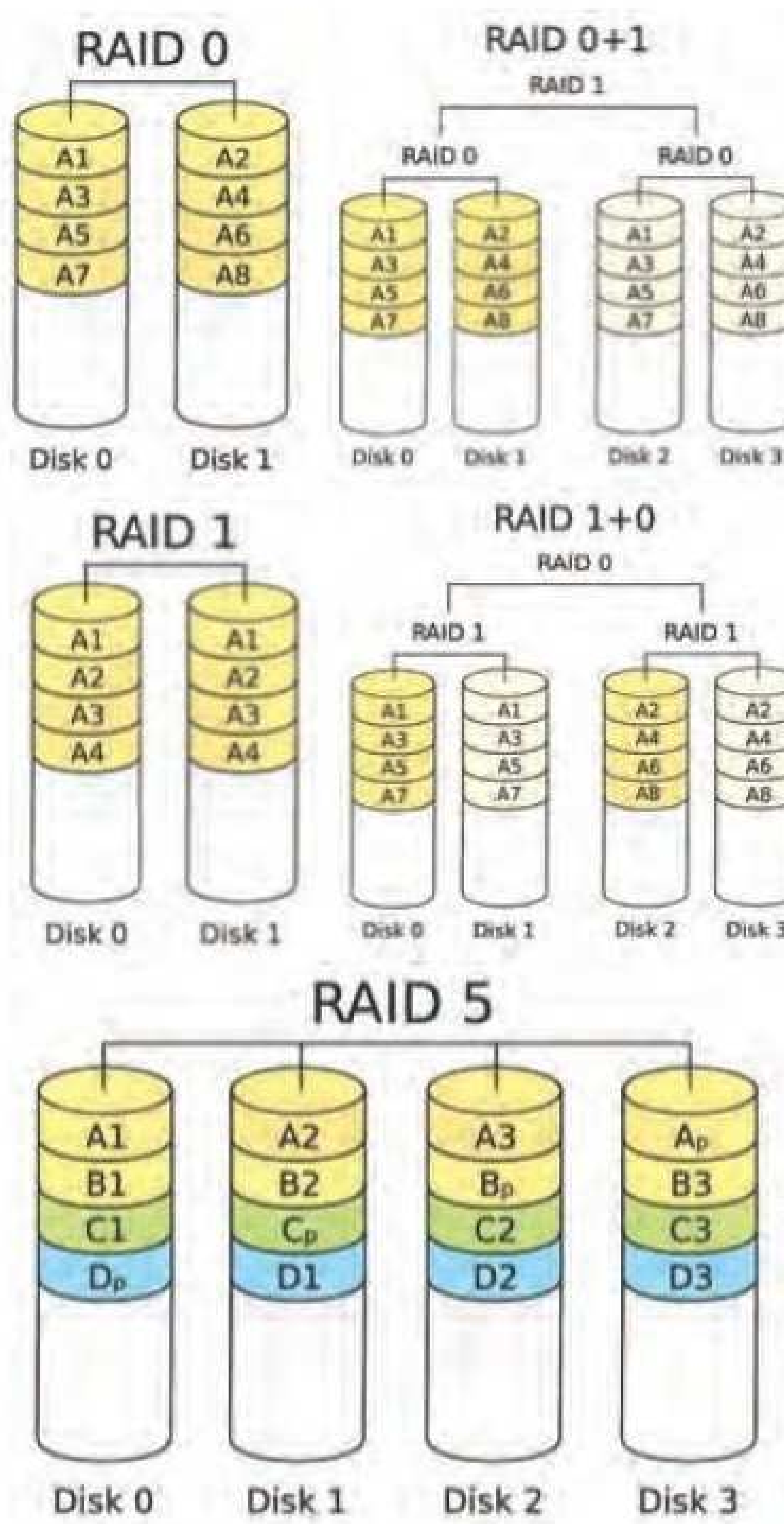
Un NAS pour les sauvegardes

Le NAS semble être le choix le plus intéressant pour des sauvegardes en 2020, mais il y a tout de même quelques points importants à prendre en compte.

IL N'Y A PAS QUE SYNOLOGY OU QNAP SUR LE MARCHÉ.

Un NAS, *Network Attached Storage*, est parfois comparé à un disque dur externe comme ceux présentés dans les pages précédentes. C'est à la fois vrai et faux. Vrai dans le sens ou pour certains, l'usage sera le même : stocker des données. Faux, parce qu'un NAS récent est un ordinateur complet, qui propose souvent bien plus que le simple stockage de données. Il peut lire ou partager des vidéos, télécharger, diffuser de la musique, etc. Les OS modernes offrent la possibilité d'installer des applications, se gèrent depuis un navigateur avec une interface (plus ou moins) accessible, et l'ensemble va bien plus loin que le stockage. Dans le cadre de ce dossier, nous allons nous circonscrire à ces fonctions.

Les baies, le RAID. L'avantage d'un NAS par rapport à un disque dur externe, outre l'accès en réseau, va souvent être la possibilité de gérer plusieurs HDD. L'entrée de gamme propose deux baies, mais des modèles avec quatre baies se trouvent facilement, et ceux qui ont besoin de beaucoup de stockage peuvent même se diriger vers six ou huit. Dans la grosse majorité des cas, vous devrez installer des disques durs 3,5 pouces, qui offrent une capacité maximale de 16 To actuellement. Si des versions 2,5 pouces existent, elles restent rares : ils ne sont pas compétitifs avec 5 To au mieux dans ce format, et utiliser des SSD pour de la sauvegarde semble irréaliste. Dans un NAS, vous entendrez souvent parler de RAID (*Redundant Array of Independent Disks*). Arrêtons-nous directement sur une chose : le RAID n'est pas une sauvegarde. Il existe différents niveaux (0, 1, 5, etc.), avec comme but principal (sauf dans un cas particulier comme le RAID0) d'éviter une perte d'activité, mais absolument pas de sauver les données. Le premier mode courant, le 0, consiste à mettre deux (ou plus) disques en parallèle pour obtenir un espace de stockage unifié équivalent à l'ensemble de la capacité, avec des performances élevées. En RAID0, les lectures et les écritures sont réparties sur tous les disques, pour potentiellement multiplier les débits par le nombre de HDD. Il ne doit jamais être utilisé dans un NAS destiné à la sauvegarde : la perte d'un disque implique la perte de toutes les données. Le RAID1 travaille en miroir : les informations sont écrites sur deux (ou plusieurs) disques simultanément. La lecture peut être accélérée (ce n'est pas systématique) et la perte d'un disque n'a pas d'impact direct sur les données. Si le RAID1 est parfois présenté comme une sauvegarde, ce n'est absolument pas le cas : l'effacement accidentel d'un fichier le supprime sur tous les disques. Le RAID5, assez courant dans les NAS, demande trois disques au moins. L'idée, en simplifiant, consiste à répartir les données sur trois supports de façon à pouvoir récupérer l'ensemble avec la perte d'un disque sur les trois en utilisant les données et les informations de parité stockées. La capacité totale est celle de tous les disques moins un (avec 3 disques, vous avez la capacité de 2, etc.). Enfin, les RAID01 et RAID10 combinent les niveaux 0 et 1 avec quatre disques au minimum. Les deux offrent de bonnes performances et peuvent potentiellement supporter la perte de deux disques sur quatre. Potentiellement,



LES IMAGES MONTRENT BIEN LES DIFFÉRENTS NIVEAUX DE RAID CLASSIQUES : 0, 1, 01, 10 ET 5. L'ORGANISATION DES DISQUES (ET LE NOMBRE DE HDD) VARIE BEAUCOUP.

LE RAID5, QUE NOUS VOUS DÉCONSEILLONS, DEMANDE AU MOINS TROIS DISQUES.

CERTAINS NAS ANNONCENT 2 GB/S EN AGRÉGEANT DEUX CONNEXIONS. OUBLIEZ CETTE POSSIBILITÉ : ELLE N'A AUCUN INTÉRÊT.

car avec quatre disques, deux contiennent les données, deux les copies. Si vous perdez les deux *originaux* **ou** les *deux copies*, tout va bien. Mais si vous perdez un *original* **et** la *copie* correspondante, vous perdez toutes les données. Avec plus de quatre disques, le RAID10 (1+0) offre une meilleure tolérance de panne.

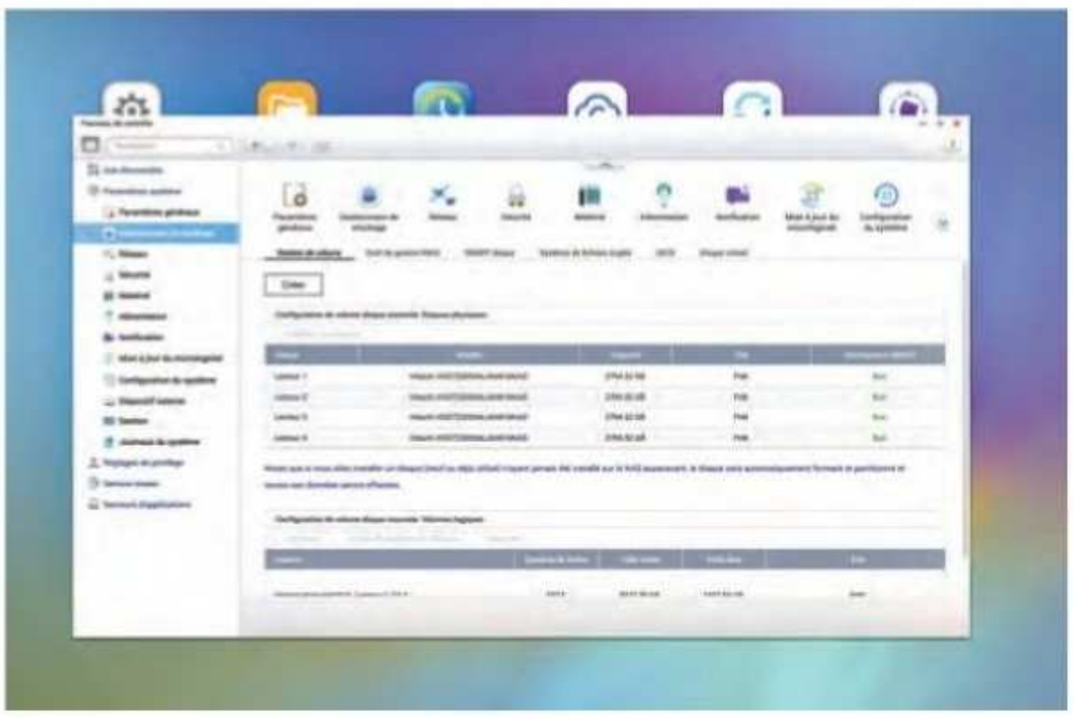
Évitez le RAID5. Certains tiqueront peut-être, mais le RAID5 devient de moins en moins praticable avec l'augmentation de la capacité des disques durs. La première raison est liée aux performances : la distribution des données passe par des calculs de parités nécessaires à la récupération, et ces calculs demandent énormément de puissance. Sur un NAS basique, surtout si vous activez le chiffrement, les débits en écriture seront faibles à cause du processeur. La seconde vient de l'éventuelle reconstruction. Le RAID5 permet la perte d'un disque dur sur l'ensemble, qui doit – en théorie – être évidemment remplacé rapidement. Une fois le disque changé, le contrôleur effectue une reconstruction, qui consiste à générer les données perdues à partir des informations stockées sur les autres HDD. Et cette dernière affecte les performances globales de la grappe et prend énormément de temps avec des disques durs de grande capacité. D'un point de vue pratique, les chances de voir un second disque dur tomber en panne pendant la reconstruction sont élevées, avec une perte de données à la clé. Sur un NAS milieu de gamme avec quatre baies, une solution à base de RAID10/01 offre une fiabilité plus élevée et de meilleures performances, avec de plus l'avantage de pouvoir survivre (dans certains cas) à la perte de deux disques. La seule contrainte vient de l'espace : le RAID10 offre 50 % de la capacité totale, le RAID5 monte à 75 % dans ce cas.

Une solution à base de RAID10/01 offre une fiabilité plus élevée et de meilleures performances.

Les performances des NAS. Ça peut sembler un peu bizarre, mais un NAS standard sera souvent moins rapide qu'un disque dur externe. La majorité se limite en effet à une connexion Ethernet à 1 Gb/s, ce qui permet en pratique des débits de l'ordre de 100 à 110 Mo/s. C'est l'équivalent d'un disque dur portable basique, et un simple modèle desktop (3,5 pouces) peut atteindre le double. De plus, surtout en entrée de gamme, le passage en RAID5 va réduire les débits en écriture, et la sauvegarde de données implique assez logiquement plus d'écriture que de lecture. Pour ce dernier point, il existe deux solutions : abandonner le RAID5 ou le chiffrement, ou acheter un NAS avec un CPU performant. L'entrée de gamme utilise des SoC ARM, le milieu de gamme des CPU Intel basse consommation (Celeron ou Pentium en architecture Atom), le haut de gamme intègre tout simplement les CPU (ou presque) de vos PC (Core ix, Ryzen, etc.). Forcément, le prix varie énormément en fonction de ce point, tout comme les nuisances sonores et la consommation. Pour les taux de transfert, certains proposent de l'Ethernet à 2.5, 5 ou même 10 Gb/s (~300, ~600 et ~1 200 Mo/s en pratique dans de bonnes conditions) mais ils nécessitent une infrastructure adaptée. Vous pouvez vous référer au *Canard PC Hardware* n° 39, mais voici un petit résumé. Une carte Ethernet

QNAP PROPOSE UNE CARTE AVEC DE L'ETHERNET 10 Gb/s ET DEUX EMPLACEMENTS NVME POUR SES NAS.

CLOUD SYNC CHEZ SYNOLOGY, POUR SYNCHRONISER LE CLOUD (SI).



L'INTERFACE DE QNAP, COMPLÈTE MAIS PARFOIS TROP.

2.5 Gb/s vaut environ 50 €, un modèle 5 Gb/s s'approche de 100 €, et les variantes 10 Gb/s se trouvent entre 100 et 200 €. De plus, il faudra penser à installer un switch compatible, ce qui alourdira la facture d'au moins 200 €. Enfin, les NAS possèdent rarement du MultiGig en standard et demandent souvent d'ajouter une carte (les mêmes que celles que nous venons de citer). En clair, pour transférer (et sauvegarder) plus vite, il va falloir ouvrir le portefeuille.

Le choix de la marque du NAS et des HDD. Le marché des NAS est assez large, mais quelques marques sortent du lot, en offrant des modèles avec des interfaces (plus ou moins) accessibles, des mises à jour régulières et de nombreuses fonctions. Il s'agit de Synology (avec le DSM), QNAP (QTS) et Asustor avec ADM. Il existe évidemment d'autres fabricants de NAS (Buffalo, Seagate, Netgear, Western Digital, etc.) mais ils proposent généralement moins de références ou des interfaces moins pratiques. Les plus bricoleurs peuvent aussi tenter de monter un NAS maison en sélectionnant une carte mère, un processeur, des disques durs et un boîtier, mais il faut avouer que l'ensemble sort du cadre de ce dossier. De plus, les personnes qui prennent la peine de le faire ne se posent *a priori* pas de question sur la meilleure manière de sauvegarder. Le choix de la marque dépendra d'abord de ce que le fabricant propose au niveau matériel, et ensuite de vos affinités avec l'interface. Ces dernières peuvent généralement être essayées sur un site web (*demo.synology.com* par exemple). D'un point de vue très personnel, nous préférons le DSM de Synology au QTS de QNAP, notamment pour sa facilité d'accès. L'OS de QNAP peut être plus complet, mais il l'est parfois trop et rend certaines tâches plus compliquées. L'autre point qui déchaîne les passions vient des disques durs : il existe trois constructeurs (Seagate, Western Digital, Toshiba) et chaque personne que vous interrogerez vous donnera une marque qu'elle n'aime pas parce qu'elle a perdu un de ses HDD. De façon plus pragmatique, Backblaze – qui utilise plus de 120 000 HDD dans son infrastructure – indique régulièrement les taux de panne des différentes marques, et le dernier rapport montre que les modèles HGST (une marque qui appartient à Western Digital) se situent sous les 1 %, que Toshiba offre aussi une excellente fiabilité et que Seagate se place entre ~1 et 3,3 %, avec quelques références visiblement un peu moins fiables. En pratique, tournez-vous vers des variantes spécifiques pour les NAS, surtout pour un NAS à quatre baies. Ils sont plus onéreux, mais la garantie est souvent plus longue (3 ans contre 2 chez Seagate par exemple) et certains réglages internes améliorent la fiabilité et la résistance aux vibrations. Il s'agit des IronWolf chez Seagate, des séries N Toshiba (pour NAS) et des modèles Red de Western Digital. Deuxièmement, dans la mesure du possible, vous pouvez essayer de vous procurer des disques issus de lots différents pour éviter que la reconstruction après la panne d'un disque amène celle d'un second à cause d'un défaut structurel commun. En théorie, un nombre d'heures d'utilisation trop proche peut aussi provoquer des pannes concomitantes, mais il faut bien avouer qu'il semble assez logique que des disques en RAID possèdent le même nombre d'heures de vol.

La synchronisation vers le cloud. En plus de servir de support pour les sauvegardes, les NAS peuvent gérer la synchronisation de vos données placées sur des services de *cloud* pour vous. Le passage par un NAS a l'avantage d'éviter d'utiliser le processeur de votre machine pour cet usage, mais aussi de permettre une synchronisation durant la nuit ou quand vous êtes absent, deux tâches compliquées avec les PC portables. Les services pris en charge dépendent évidemment du fabricant de votre NAS. Synology propose par exemple l'inévitable Dropbox, mais aussi Backblaze, Amazon Drive, Microsoft Azure, etc. Chez QNAP, la liste est très longue, avec Dropbox (encore), Google One, etc. Si la synchronisation d'un NAS avec le *cloud* ne règle pas les contraintes habituelles – sans un débit en upload conséquent, vous aurez des problèmes –, elle permet au moins d'envisager une sauvegarde en local sur un NAS, avec une duplication dans le *cloud* de façon transparente.

LES DISQUES DURS POUR NAS SONT « OPTIMISÉS » POUR CET USAGE.

CETTE SECTION NE VA PAS PARLER DE CE GENRE DE NUAGES.

Sauver dans le cloud

Certains sauvent en local, sur un disque dur externe ou un NAS. Mais il reste une possibilité bien plus moderne, et surtout à la mode : le fameux *cloud*.

Vous vivez dans une grotte depuis des années ? Vous ne connaissez ou ne comprenez pas le concept de *cloud* ? C'est pourtant assez simple : le *cloud* est juste un disque dur qui n'est pas chez vous, mais dans un centre de données. L'idée semble séduisante : vous n'avez pas besoin de vous promener avec votre sauvegarde, elle est accessible partout (si vous avez Internet), et vous palliez deux inconvénients des *backups* locaux, les vols et les incendies. Bon, en réalité, et il faut bien l'avouer, des malandrins – parfois appelés hackers – peuvent s'attaquer à vos données (à défaut de partir avec le disque dur ou le PC portable) et tous les fournisseurs ne dupliquent pas les informations, donc un incendie dans un data center peut entraîner la perte de vos données.

Deux contraintes majeures. La première contrainte va être le prix. Une capacité de 2 To semble être un bon point de départ pour un utilisateur standard, et un simple disque dur de cette capacité vaudra moins de 100 €. Les offres de *cloud* et de synchronisation, elles, tournent autour d'une dizaine d'euros par mois, soit en gros le coût d'un disque dur par an. D'un autre côté, si vous voulez uniquement de la sauvegarde, les services proposent souvent de l'illimité pour un prix parfois plus faible (Backblaze facture 60 $ par an). Le *cloud* reste donc assez cher et nécessite un abonnement, ce qui exclut en partie l'idée de sauvegarde à long terme : rien ne dit que la société sera encore là dans 10 ou 15 ans. Vous pourrez rétorquer qu'il existe des solutions gratuites ou en tout cas moins onéreuses, mais dans un usage centré sur la sauvegarde, quelques gigaoctets (même

VOUS AVEZ UN ABONNEMENT À UN SERVICE AVEC 2 TO DE STOCKAGE ? C'EST L'ÉQUIVALENT DU PRIX D'UN DISQUE DUR DE 2 TO PAR AN.

gratuits) semblent un peu légers. La seconde contrainte va être votre connexion, et dans les deux sens (*upload* et *download*). Si vous avez une ligne de type xDSL, vous ne pourrez pas vraiment en profiter : avec un upload (l'envoi des données vers le cloud) sous les 10 Mb/s (l'ADSL classique se limite à 1 Mb/s, le VDSL peut atteindre environ 10), la gestion incrémentale est compliquée et l'envoi de sauvegardes froides (par exemple vos fichiers finaux) devient difficile. Dans une moindre mesure, la récupération peut aussi être assez tendue : en cas de gros problèmes, télécharger plusieurs dizaines de gigaoctets peut prendre plusieurs heures ou jours. La sauvegarde en *cloud* ne doit être envisagée qu'avec une connexion en fibre optique, idéalement rapide : les fournisseurs d'accès proposent des offres capables d'atteindre 600 Mb/s (75 Mo/s) en *upload*, de quoi effectuer des sauvegardes sans monopoliser la connexion. Si vous utilisez une offre cellulaire (4G), la sauvegarde reste envisageable mais dépendra énormément de votre localisation et de la capacité de votre forfait.

Les services de synchronisation. Nous allons considérer que le prix n'est pas un problème et que vous disposez d'une connexion très haut débit pour la

UN CENTRE DE DONNÉES BACKBLAZE, AVEC BEAUCOUP (BEAUCOUP) DE DISQUES DURS.

VOUS AVIEZ PENSÉ QUE HUBIC D'OVHCLOUD ÉTAIT UNE BONNE IDÉE ? DOMMAGE.

LES OFFRES DE DROPBOX : OFFRE GRATUITE LIMITÉE, OFFRES PAYANTES UN PEU ONÉREUSES.

démonstration, avec une question : que choisir ? Nous allons arbitrairement diviser les offres de *cloud* en deux. Premièrement, les services de synchronisation fournis avec les OS. Nous parlons ici de Google One (pour les appareils Android), iCloud (chez Apple) ou OneDrive (chez Microsoft). Les trois s'intègrent de façon poussée dans les OS associés, et peuvent s'ajouter à d'autres systèmes d'exploitation de manière plus ou moins heureuse. Les offres de ce type ne visent pas réellement la sauvegarde : le but est de synchroniser les données, centraliser

Le cloud n'est pas réellement une sauvegarde : il ne s'agit pas d'une copie du contenu de votre disque.

les informations et permettre de partager facilement du contenu. Elles amènent à peu près la même chose, avec une offre gratuite limitée (5 ou 15 Go), une intermédiaire (50 à 200 Go, entre 1 et 3 €/mois) et une solution avec 2 To de stockage pour 10 €/mois. Microsoft couple 1 To avec l'abonnement Office 365 pour 70 € à l'année, un prix plutôt intéressant. Hors de l'OS, il existe des services plus ouverts, comme Dropbox (le vétéran et sûrement le plus connu), Amazon Drive, etc. Les coûts demeurent assez proches, avec des variantes professionnelles qui proposent plus d'espace. Chez Dropbox, l'offre gratuite reste trop légère (2 Go) et la payante un peu onéreuse (12 €/mois) pour 2 To, sans intermédiaire. Ces offres agnostiques ont l'avantage de s'intégrer dans tous les OS, avec des applications adaptées pour la majorité des cas de figure. Ce n'est pas parfait, étant donné que certains OS limitent les interactions possibles (coucou Apple), mais ça peut suffire. À chaque fois, vous pourrez déplacer vos données dans le *cloud* (manuellement ou automatiquement), revenir en arrière en cas d'effacement, mais pas réellement faire une sauvegarde : il ne s'agit pas d'une copie du contenu de votre disque. Les services peuvent synchroniser des dossiers, mais pas un OS complet. De plus, typiquement, un fichier effacé sur un appareil sera supprimé du *cloud* et des autres périphériques, ce qui n'est pas très sécurisant. Il reste bien évidemment une corbeille, mais l'accès n'est pas toujours aisé et nécessite souvent un passage sur le site web.

Les services de sauvegarde. Pour des sauvegardes, dirigez-vous vers des services dédiés à cet usage. Ils n'amèneront pas la synchronisation entre vos appareils ni le partage, sont évidemment payants, mais restent plus adaptés tout de même. Ils proposent un grand espace de stockage (parfois illimité) pour un prix plus faible mais ne font qu'une chose : une copie de vos données. Vous n'éviterez pas les problèmes liés à l'envoi (un *upload* correct demeure obligatoire) mais ils offrent souvent par exemple la possibilité – payante – de vous envoyer vos données physiquement. Si vous n'avez pas le nécessaire pour récupérer rapidement des dizaines ou des centaines de Go, ils peuvent missionner un transporteur avec un disque dur, une solution qui semble archaïque mais reste diablement efficace. Nous vous conseillons Backblaze (60 $/an) pour un usage grand public, ou CrashPlan pour une (petite) entreprise, dès 10 $/mois.

Les sauvegardes froides. Si vous trouvez les services de sauvegarde trop onéreux et que vous n'avez pas besoin de mise à jour fréquente, il existe des solutions de stockage adaptées, comme Glacier chez Amazon (le plus connu). Vous pourrez y stocker des données à long terme, par exemple vos fichiers finaux. La tarification s'effectue au Go avec un prix assez faible (0,005 $ par Go environ) mais la récupération est facturée (0,01 $ en France). L'offre ne vise pas nécessairement le grand public, mais est intéressante pour garder une copie de sécurité d'informations sauvegardées à un autre endroit, en considérant qu'on n'y aura accès qu'en cas d'énorme problème.

Et les petits services ?

Nous ne pouvons pas traiter toutes les offres existantes, mais nous devons être pragmatiques et vous mettre en garde ; par exemple, ce petit fournisseur avec des prix très intéressants n'est pas forcément le meilleur choix. Vous pourrez trouver votre bonheur, mais pour des sauvegardes pérennes, nous préférons de grosses sociétés bien implantées, pour avoir un peu de recul. Vous n'éviterez pas nécessairement les problèmes, mais serez moins à la merci d'une coupure franche, d'une application buguée ou de pertes de données.

Vérification et prophylaxie : sauver vos sauvegardes

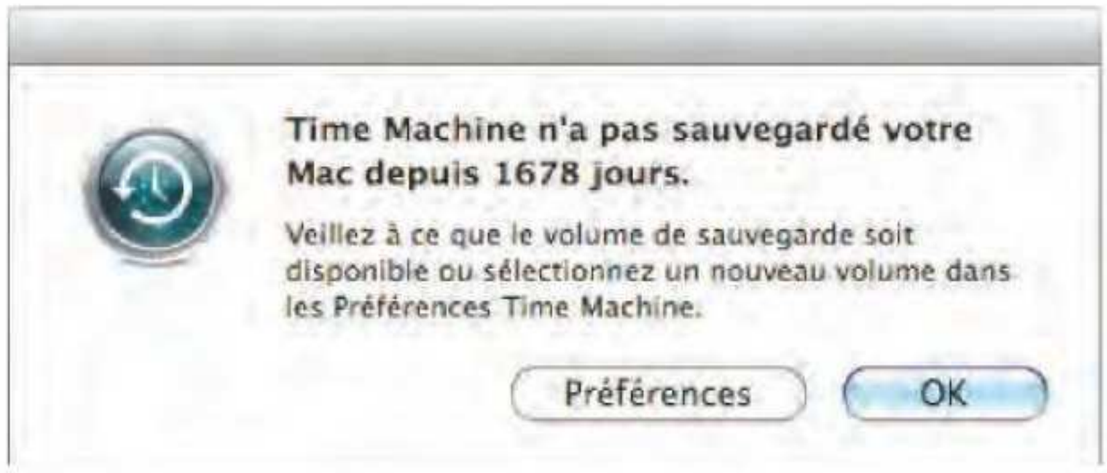
Vous avez effectué vos sauvegardes, et c'est une bonne nouvelle, mais avez-vous vérifié qu'elles fonctionnent ?

Commençons par la vérification. Dans un monde idéal, vous devriez pouvoir contrôler votre sauvegarde. Ne prenez pas ce point à la légère : ce n'est pas au moment de devoir restaurer vos données que vous aurez le temps ou l'envie de chercher *comment* le faire. La première étape, donc, consiste à examiner **comment la restauration fonctionne** et si elle s'effectue facilement. La méthode va dépendre du programme utilisé : macOS installe un OS basique permettant de démarrer sur les disques durs externes, mais nécessite un appareil qui s'allume correctement pour une sauvegarde en réseau. Pensez à garder une trace des identifiants pour accéder au NAS dans un endroit sécurisé (un Post-it sous le clavier n'en est pas un, un gestionnaire de mots de passe l'est) et vérifiez si des logiciels ne doivent pas être installés avant la restauration. Le cas échéant, stockez une copie au chaud. Sur un smartphone, vérifiez comment fonctionne la double authentification si ce dernier ne fonctionne pas. Dans tous les cas, nous le répétons, n'attendez pas de devoir restaurer pour découvrir les limites. La seconde étape consiste à tester régulièrement si **la sauvegarde s'effectue**. Vraiment. Le programme peut avoir eu un problème, s'être désactivé, vous avez peut-être raté une notification importante, etc. Se rendre compte au moment de restaurer que le dernier *backup* a deux ans n'est jamais agréable. Vous pouvez rigoler, mais il s'agit d'un problème assez fréquent. Ensuite, si votre logiciel offre l'option, une vérification de l'intégrité de la sauvegarde doit être effectuée régulièrement. Dans la même veine, surtout sur un NAS en RAID, pensez à bien configurer les alertes pour être prévenu en cas de défaillance d'un disque dur. Le RAID permet généralement une continuité de service avec un disque perdu, mais il faut tout de même commander rapidement un nouveau HDD (ou en avoir un en réserve) pour le changer. Sans alertes, avec un RAID dégradé, vous risquez surtout de perdre un autre disque et toutes vos données.

IL EXISTE DES LOGICIELS SOUS WINDOWS QUI PERMETTENT DE LIRE LES DONNÉES SMART. ATTENTION, LES DISQUES USB NE RENVOIENT PAS NÉCESSAIREMENT LES INFORMATIONS.

Prophylaxie numérique. Vous surveillez vos sauvegardes, elles s'effectuent régulièrement et le contenu semble valable. Mais pendant combien de temps ? Malheureusement, l'espace utilisé par la sauvegarde peut augmenter rapidement, et éventuellement de façon exponentielle. Vous pouvez limiter l'espace avec un NAS, mais la solution de base dans pas mal de logiciels consiste à effacer les anciennes sauvegardes, souvent de façon automatique. Si cette étape ne fonctionne pas – par exemple parce que vous avez trop de données –, la seconde solution sera de mettre à jour les disques durs, en gardant les anciens comme sauvegarde froide. Le coût financier n'est pas négligeable, mais vous pourrez augmenter l'espace disque facilement et améliorer la fiabilité. Avec un NAS, il est même possible de remplacer les disques durs sans perdre les données, en changeant les HDD en plusieurs fois avant d'étendre le volume RAID.

OUPS, IL N'Y A PLUS DE SAUVEGARDES DEPUIS 4 ANS.



TIME MACHINE PERMET DE VÉRIFIER L'INTÉGRITÉ DES SAUVEGARDES.

Le SMART

Tous les disques durs proposent une « détection de panne » intégrée, le SMART. Cette technologie se base sur des données renvoyées par le contrôleur, et elles peuvent indiquer qu'un problème arrive. Attention : une erreur SMART indique généralement une panne dans le futur (à plus ou moins court terme) mais l'absence d'erreur SMART ne permet pas d'être certain que tout va bien.

La sauvegarde froide et le problème des vieux formats

Nous évoquions dans les pages précédentes la possibilité d'effectuer des sauvegardes froides, pour des archivages à long terme. Si l'idée semble bonne, elle amène tout de même souvent des problèmes.

Une sauvegarde froide s'impose en principe pour des données dont vous n'avez pas besoin rapidement, qui seront ainsi disponibles à un autre endroit. Nous en avons parlé dans la partie sur le *cloud*, il existe des services dédiés à cet usage : le stockage est proposé à un prix assez faible, mais la récupération est facturée. Dans les entreprises, les sauvegardes de ce type s'effectuent sur des bandes magnétiques, qui offrent une grande capacité mais un accès assez lent, étant donné le fonctionnement séquentiel. Pour un usage grand public, les disques optiques ont été pendant longtemps des médias de choix : ils possédaient une bonne capacité, un débit correct, et avaient l'avantage de « protéger » les données contre un effacement accidentel dans la majorité des cas (oublions les DVD-RAM). En 2020, ils sont évidemment tombés en désuétude : la capacité maximale des Blu-ray (100 Go) demeure risible à l'heure des SSD de plusieurs téraoctets, sans même prendre en compte les contraintes liées à la gravure. Si certains tentent de remplacer ces derniers par des clés USB ou des cartes mémoire, nous devons rappeler une fois de plus que l'absence de gestion de l'usure et la fiabilité toute relative des périphériques de ce type les rendent inaptes à la sauvegarde. De plus, la rétention des données n'est garantie que pour une dizaine d'années dans le meilleur des cas, c'est-à-dire que les informations peuvent disparaître sans raison au-delà de ce laps de temps.

Pour une sauvegarde à long terme, le meilleur choix reste un DD externe en USB.

Pensez aux disques durs externes. Pour une sauvegarde à long terme, avec des données que vous voudrez peut-être relire dans 5, 10 ou 15 ans, le meilleur choix reste un disque dur externe en USB. Le coût est modique, il ne devrait pas perdre d'informations avec le temps si vous ne l'utilisez pas (hors sauvegardes), et l'omniprésence de l'USB ainsi que sa rétrocompatibilité garantissent son utilisation à moyen terme. Contrairement aux conseils précédents, et spécifiquement pour ce cas de figure, une simple copie des données offre plus d'espoir de réussite. Évitez les logiciels qui compressent, découpent ou tentent d'accélérer les débits en modifiant les données : vous n'avez aucune idée de leur pérennité.

Oubliez les technologies rares. Une sauvegarde à long terme doit utiliser des technologies éprouvées et durables, c'est pourquoi nous conseillons un disque dur externe en USB. Ne vous tournez pas vers les « *médias révolutionnaires qui durent 100 ans* », les interfaces de connexion « *qui vont s'imposer* » ou celles qui ne se retrouvent que sur 10 % des ordinateurs. Oubliez ce système de fichiers prometteurs, ce logiciel qui est une référence. Faites simple, quitte à y consacrer un peu plus de temps. Pensez aux personnes qui sauvegardaient sur des SyQuest, Zip, Jaz, disquettes, etc. dans les années 1980 et 90. Et qui dans les années 2020 doivent chercher un moyen d'arriver à lire les données.

100 GO, ~15 € PAR DISQUE SANS LE GRAVEUR. VOUS COMPRENEZ POURQUOI PERSONNE NE SAUVE SUR BLU-RAY ?

LE ZIP D'IOMEGA. 100 MO DANS UN DISQUE DE LA TAILLE D'UNE DISQUETTE, UNE RÉVOLUTION DANS LES ANNÉES 1990. ET DIFFICILEMENT LISIBLE EN 2020.

Renouvelez-vous. Nous allons terminer ce dossier en vous prodiguant un dernier conseil : ne restez pas sur vos acquis, évoluez. Si vous vous rendez compte que le système que vous avez mis en place pour sauvegarder devient une contrainte, cherchez une nouvelle méthode. Si vous remarquez que votre PC flambant neuf ou votre smartphone (etc.) ne peut pas accéder à vos anciennes données, posez-vous rapidement la question du renouvellement. Si vous manquez d'espace, remplacez les disques durs. Il s'agit finalement du point le plus important dans une sauvegarde, le but ultime : ne pas se retrouver bloqué en cas de problème. Et nous espérons que ce long dossier vous aidera à y arriver.

Crédit : iFixit

LA PUCE T2 DES MAC, CAUCHEMAR DES RÉPARATEURS.

La récupération des données

La question de la récupération des données se posera à un moment ou à un autre. Parce que vous n'avez pas de sauvegarde (sautez en page 54 et recommencez à lire ce dossier !) ou qu'elle n'a pas fonctionné correctement, etc.

C'est l'accident bête (oui, ils sont tous bêtes) : vous avez laissé tomber votre PC portable il n'a pas l'air de s'allumer. Avant de faire le deuil de vos données, la première étape va consister à vérifier si le périphérique de stockage est abîmé. Dans un portable, vous trouverez plusieurs cas de figure. Premièrement, vous avez un Mac récent : vous l'avez dans le baba. Apple soude la mémoire sur la carte mère et utilise une puce dédiée (la T2) comme contrôleur. Si rien ne démarre, point de salut. Au suivant. Dans un PC, le stockage peut se présenter sous la forme d'un disque dur 2,5 pouces (ou d'un SSD au même format) ou d'une barrette M.2 en SATA ou PCI-Express, généralement avec une interface logique NVMe. Dans les trois cas, vous pourrez brancher le périphérique en USB en utilisant des adaptateurs qui se trouvent facilement chez les revendeurs en ligne. Attention, les modèles USB vers M.2 n'acceptent qu'un type de SSD : SATA ou PCI-Express, choisissez bien. Dans un PC de bureau, c'est la même chose, mais avec en plus un éventuel HDD 3,5 pouces en SATA. Avec un peu de chance, si l'ordinateur ne démarre pas, votre périphérique de stockage n'a pas été endommagé et vous pourrez récupérer les données. En cas d'accident avec un disque dur externe, il se peut que le disque dur lui-même n'ait rien, mais que la partie liée à l'alimentation ou à l'USB pose un souci. Donc avant de pleurer (encore), vérifiez s'il est possible de le brancher en SATA, soit directement dans un PC, soit avec un autre adaptateur USB vers SATA. Si vous avez acheté un modèle 2,5 pouces Western Digital, désolé : ils utilisent souvent une interface USB native.

Récupérer les données. Si votre périphérique semble être reconnu par un ordinateur mais que les données ne sont pas présentes, bonne nouvelle : il y a d'éventuelles solutions. Dans le cas contraire, si vous n'avez pas de sauvegarde (quelle drôle d'idée), vous pouvez tenter le recours à des sociétés spécialisées. La plus connue est Ontrack (anciennement Kroll Ontrack) mais il en existe d'autres. Elles peuvent généralement récupérer vos données sur un disque dur (sur un SSD, commencez à pleurer ; voir encadré) mais les prix restent élevés. Ils sont rarement indiqués au départ, car elles veulent éviter d'effrayer les clients, mais il faut compter en général entre 400 et 1 000 €, en fonction des problèmes. Revenons aux appareils accessibles. Ce n'est pas le sujet de ce dossier, mais il existe des logiciels capables de chercher d'éventuelles données effacées, comme Recuva, Pixel8 (*cpc.cx/pixel8*) ou Easy Recovery (OnTrack, ~90 €). De plus, certaines cartes mémoire arrivent avec un logiciel dédié exclusivement aux photos. Ils ne font pas des miracles, mais sur un média formaté par erreur et sans réécritures, ils peuvent parfois obtenir un résultat. Attention, ils limitent souvent la récupération à quelques fichiers… sauf si vous payez. Dernier point à retenir : dans le cas où vous effaceriez des données ou formateriez un disque dur par inadvertance, ne continuez pas à travailler, essayez de tenter une récupération le plus rapidement possible.

UN ADAPTATEUR USB POUR SSD M.2. ATTENTION À LA COMPATIBILITÉ.

UNE SALLE BLANCHE, DANS UNE SOCIÉTÉ DÉDIÉE.

Attention aux SSD

Si le contenu d'un disque dur endommagé peut parfois être récupéré par des sociétés spécialisées, ce n'est pas le cas sur les SSD, ou très rarement. Les pannes impliquent souvent la perte complète des données. De plus, dans beaucoup de SSD modernes, le contrôleur chiffre les données à la volée. S'il ne fonctionne plus, elles ne seront donc plus lisibles.

Sécurité et chiffrement

La question peut se poser : comment chiffrer les sauvegardes, qu'elles soient locales ou dans le *cloud* ? Parce qu'évidemment, vous ne voulez probablement pas qu'une autre personne se promène dans vos fichiers.

Commençons par les sauvegardes locales. Sur un disque dur externe, vous pouvez d'abord chiffrer – pas crypter, merci – le volume lui-même. La méthode dépend de votre OS : il peut le faire dans certains cas, sinon un logiciel dédié (parfois fourni par le vendeur du disque dur) suffit. Il s'agit d'un choix assez transparent à l'usage : vous entrez le mot de passe au branchement et votre logiciel de sauvegarde va travailler de façon classique, mais les données seront chiffrées. La seconde méthode passe par une image disque chiffrée, placée sur le disque dur externe. Une fois le disque dur ouvert, elle doit être montée (c'est-à-dire ouverte) en utilisant un mot de passe, et votre programme de sauvegarde devra sauver, dans cette image disque, l'équivalent d'un disque dur virtuel. Vous pouvez choisir VeraCrypt dans les deux cas, la principale différence vient de la compatibilité. Dans le premier, vous aurez besoin du logiciel pour accéder au disque dur, alors que dans le second, il peut être branché de façon standard sur n'importe quel PC. La dernière, que nous vous déconseillons même si elle existe, consiste à compresser vos données dans une archive avec un mot de passe (par exemple avec 7-Zip). Cette solution manuelle et lente possède le défaut de ne pas être très amie avec les sauvegardes incrémentales… De plus, elle dépend de la présence du logiciel qui a servi à compresser, surtout si vous oubliez de créer une archive auto-extractible. Pour les performances, tant que votre CPU supporte les instructions AES-NI (dès 2010 chez Intel), le chiffrement ne devrait pas avoir d'impact réellement visible.

Les fournisseurs de cloud chiffrent les données mais ont les clés pour les lire.

Dans les NAS. Dans un NAS, vous pouvez utiliser la méthode de l'image disque, mais aussi chiffrer directement le contenu du NAS, en passant par les fonctions de ce dernier. Cette seconde option est évidemment plus transparente pour l'utilisateur, qui n'a rien de spécial à faire, mais les performances peuvent parfois diminuer énormément. Sur les puces ARM d'ancienne génération ou sur certains CPU Intel sans accélération, vous risquez de diviser les débits en écriture par deux et descendre sous les 50 Mo/s.

Et le *cloud* ? Le cas du *cloud* est compliqué. D'un point de vue technique, les fournisseurs classiques (Google, Microsoft, Apple, Amazon, Dropbox, etc.) chiffrent les données mais disposent des clés donc peuvent les lire, par exemple en cas de demandes émanant de la justice. Si c'est inacceptable pour vous, la création d'une image disque chiffrée ou d'une archive permet de garantir la confidentialité de vos données. Pour le reste, n'oubliez pas d'utiliser un mot de passe fort avec une authentification à deux facteurs, idéalement avec autre chose qu'un SMS.

VeraCrypt

VERACRYPT, POUR CEUX QUI VEULENT CHIFFRER LEURS DONNÉES.

LES CLÉS POUR LA DOUBLE AUTHENTIFICATION DE GOOGLE, PRATIQUE POUR SÉCURISER LES ÉCHANGES.

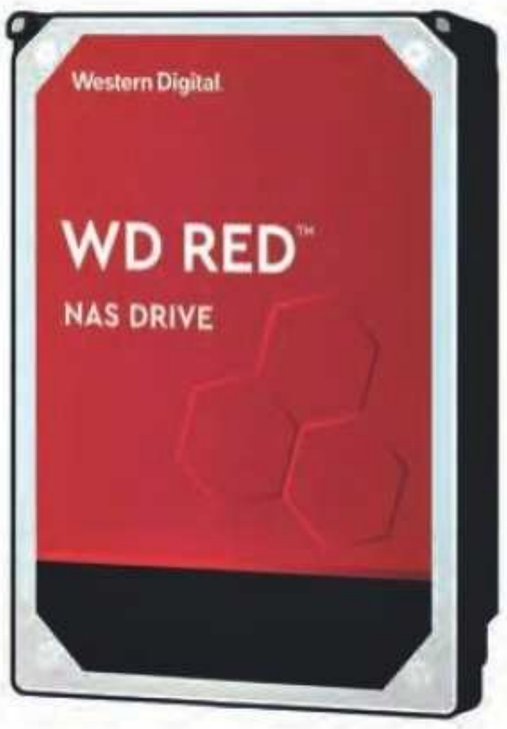
Smartphone et sauvegarde. Pour les smartphones, la question du chiffrement va dépendre de la façon de faire la sauvegarde. Généralement, les *backups* en local (sur un ordinateur, une carte microSD, etc.) sont chiffrés et le fabricant de l'OS n'a pas la clé. Pour les sauvegardes dans le *cloud*, encore une fois, Google ou Apple possèdent la clé. La première raison vient des éventuelles demandes de la justice ; la seconde – dixit Apple – est que la présence de la clé permet de restaurer une sauvegarde quand le client a perdu son mot de passe. Une excuse pas très convaincante : la société pourrait parfaitement laisser le choix aux utilisateurs en expliquant les conséquences.

Et en pratique ?

Notre dossier, comme expliqué au début, reste un ensemble de conseils, de choses à éviter et de bonnes pratiques. Pour terminer, nous vous proposons cependant une sélection un peu plus concrète.

Prenons le cas d'une personne paranoïaque, comme le rédacteur en chef de ce magazine. Je passe à la première personne pour expliquer mon *setup*. Ma machine principale est un MacBook Pro avec un SSD de 512 Go. À la maison – vive le télétravail –, il est relié à plusieurs SSD externes (environ 2 To de données au total). Les informations importantes sont synchronisées sur iCloud, pour un accès rapide depuis un autre appareil. Je dispose de quatre sauvegardes – oui, je suis paranoïaque. Les deux premières dans des boîtiers Time Capsule équipés d'un disque dur de 6 To. Time Machine sauve de façon incrémentale, en alternant les boîtiers. Chaque semaine, une troisième sauvegarde est effectuée sur un HDD externe (3 To) qui est ensuite rangé dans un endroit protégé. Enfin, à la rédaction, une quatrième sauvegarde automatique est faite sur un disque dur de 6 To. Le dispositif semble exagéré (il l'est sûrement) mais il permet d'éviter les pertes de données, avec une récupération rapide. Il est évidemment parfaitement possible de faire la même chose sous Windows ou GNU/Linux.

IL EXISTE DES NAS 4 BAIES SOUS LES 400 €.



JUSQU'À 14 TO POUR LES NAS.

Un petit guide d'achat. Par rapport aux explications des pages précédentes, et en considérant que vous ne comptez pas sauvegarder vos films de vacances, nous pouvons vous conseiller quelques références. Pour le *cloud*, une offre avec 2 To de stockage suffit normalement pour synchroniser vos données importantes et elles valent ~10 € par mois. Sur ce point, le choix dépend de vos préférences et de votre OS. Pour les disques durs externes, la gamme Expansion de Seagate offre un bon rapport qualité/prix en desktop : ~100 € en 4 To, ~140 € en 6 To, ~180 € en 8 To (au-delà, le coût explose). Les My Book de Western Digital valent quasiment le même prix. Si vous voulez un modèle portable, Seagate propose une gamme intéressante en SATA natif. Restez sous les 2 To (~85 €) pour éviter les HDD SMR, parfois très lents en écriture. Pour un smartphone Android – Apple ne permet pas l'utilisation des cartes microSD –, une Samsung ou Sandisk de 128 Go se trouve aux alentours de 30 €. Notre seul conseil ? Passez par un vendeur fiable et reconnu, pas par un *marketplace* ou un site obscur avec d'excellents prix qui vous enverra une contrefaçon.

Et le NAS ? Pour un NAS, nous apprécions la série 218 de chez Synology, avec par exemple le DS218j (2 baies, en ARM, ~190 €) et le DS218+, plus performant mais plus cher (~370 €). QNAP, Asustor ou Buffalo proposent des modèles équivalents : comptez ~200 € pour un NAS correct avec deux baies, 100 à 150 € de plus si vous voulez un CPU x86 et plus de fonctions. Pour quatre baies, il faudra compter entre 300 et 400 € sans disque pour un modèle de base (comme le QNAP TS-431P), nettement plus si vous voulez transmettre à 5 ou 10 Gb/s. En plus du prix du NAS, l'investissement passe par les HDD. Vous pouvez utiliser des variantes grand public dans une version deux baies, mais pour la version quatre baies, choisissez des disques « NAS ». Ils sont un peu plus chers, mais plus fiables pour cet usage. Le choix dépend de vos préférences, entre Western Digital, Seagate ou Toshiba. Les HDD de 3 To valent aux environs de 100 € et vous pouvez atteindre 14 To pour moins de 500 €/pièce. Les 16 To existent, mais restent trop onéreux.

CERTAINES MICROSD SONT PLUS ENDURANTES QUE D'AUTRES.

Ce dossier est maintenant terminé, nous espérons que vous aurez appris des choses et, si vous ne sauvegardiez pas régulièrement, que nous vous avons convaincu de le faire.