ebook

Revendeurs IT : Découvrez le potentiel des sauvegardes cloud pour booster vos ventes

Développez votre activité commerciale.

leviia

Sommaire

Partie 1
Introduction et rappel des bonnes pratiques p.3

Partie 2
Combiner stockage sur site et stockage cloud p.5

Partie 3
Optimiser les coûts du stockage cloud p.9

Partie 4
Souveraineté et certifications p.12

Et après ? p.16

Partie 1

Introduction et rappel des bonnes pratiques

a. Introduction

Vous le savez, **les entreprises et les collectivités produisent et stockent de plus en plus de données.** Par conséquent, les incidents et les **cyberattaques se multiplient** et les conséquences peuvent être désastreuses, pour leurs clients, leur stabilité financière et leur réputation.

Pour ces organisations, la sécurisation des sauvegardes est donc aujourd'hui plus critique que jamais.

La question n'est plus de savoir pourquoi sauvegarder ses données, mais plutôt **comment le faire de la manière la plus sécurisée possible, en maîtrisant les coûts.**

Ce livre blanc vous aidera à **comprendre les enjeux des sauvegardes cloud et à les transformer en levier de croissance pour votre activité.**

b. Les stratégies de sauvegarde recommandées

1. Pourquoi suivre les recommandations de l'ANSSI pour la sauvegarde de données ?

L'ANSSI est l'autorité française en matière de cybersécurité.

Créée en 2009, elle a une mission de défense des systèmes d'information de l'État mais elle est aussi chargée d'une mission de conseil et de soutien aux administrations et aux entreprises françaises.

Cette agence fournit régulièrement des recommandations et des bonnes pratiques suivies par de nombreux professionnels du secteur.

2. Stratégie 3-2-1 : la préconisation de l'ANSSI pour les sauvegardes de vos clients

Voici ce que la stratégie 3-2-1 implique :

- **3 copies des données :** ils doivent avoir trois copies distinctes de leurs données (une principale et deux sauvegardes).
- **2 types de supports différents :** les deux sauvegardes doivent être stockées sur au moins deux types de supports (disques durs locaux, bandes magnétiques, cloud, etc.).
- **1 copie hors site :** au moins une des copies doit être stockée à un emplacement hors site, pour protéger les données contre des incidents localisés (incendie, vol, inondation, etc.).

3. Nouvelle variante 3-2-1-1-0 encore plus avancée : avec l'ajout d'une copie immuable.

- **1 copie immuable :** impossible à modifier ou supprimer pendant une période définie. Cette copie offre une meilleure protection contre les erreurs humaines et contre les ransomwares qui cherchent à effacer ou à bloquer les données.
- **0 erreur :** pour des sauvegardes sans erreurs.
  Les sauvegardes n'ont de valeur que si elles sont vérifiées.
  Effectuez des tests de restauration pour vérifier que tout fonctionne correctement.

Partie 2

Combiner stockage sur site et stockage cloud

Vous l'avez compris, les bonnes pratiques en matière de stratégie de sauvegarde recommandent de **combiner stockage sur site et stockage hors site** (y compris stockage en ligne). **Voyons ensemble pourquoi cette approche est devenue incontournable aujourd'hui.**

a. Les limites et risques des infrastructures locales

Avec l'augmentation du volume de données, les systèmes et outils internes comme les NAS et les serveurs privés deviennent **de plus en plus complexes à gérer pour les entreprises.**

Maintenance et ressources

Les entreprises doivent **mobiliser des équipes spécialisées et allouer des budgets conséquents** pour maintenir et développer leur système informatique.
La sauvegarde, par exemple, exige des **mises à jour fréquentes de matériel, des débogages et une surveillance régulière pour assurer la disponibilité et la sécurité des données.** Sans ces efforts, les risques d'obsolescence et de perte de données augmentent considérablement.

Vulnérabilité

Les infrastructures sur site sont exposées aux **pannes matérielles** et aux **cyberattaques**, notamment aux ransomwares, qui ciblent spécialement les données critiques stockées localement. Par ailleurs, **les catastrophes physiques**, comme les incendies ou les inondations, constituent une menace directe pour les infrastructures sans redondance, où tout est stocké sur site.

Manque de scalabilité et coûts croissants

L'augmentation constante des volumes de données entraîne également des dépenses de plus en plus importantes. **Les clouds privés**, par exemple, doivent **constamment être redimensionnés pour répondre aux nouveaux besoins**, ce qui engendre des dépenses continues en matériel et en logiciels.

Considérant les contraintes que nous venons de détailler, de nombreuses entreprises choisissent aujourd'hui de se tourner vers une stratégie qui combine stockage local et stockage cloud. **Nous allons voir comment cette approche hybride leur offre plus de flexibilité et plus de sécurité.**

b. Pourquoi le stockage cloud gagne en popularité pour les sauvegardes des entreprises ?

Pour deux raisons principalement :

- Il s'intègre parfaitement dans la stratégie de **sauvegarde 3-2-1** voire **3-2-1-1-0** en permettant **la copie hors-site, la copie sur deux supports différents et la copie immuable.**
- Il présente **quatre grands avantages :**

Accessibilité et temps de récupération

Si les infrastructures locales tombent en panne ou deviennent inaccessibles, **le stockage cloud assure un accès ininterrompu aux données depuis n'importe quel ordinateur.** Une solution pratique, mais surtout vitale, notamment dans le cadre d'un **Plan de Reprise d'Activité** (PRA). En effet, en cas de sinistre, cette continuité d'accès permet de relancer rapidement les opérations, **minimisant les interruptions et les pertes financières.**

Scalabilité et réduction des coûts

Contrairement, on l'a vu, aux infrastructures sur site qui nécessitent des investissements initiaux importants et des frais d'entretien réguliers, le stockage cloud offre une facturation à l'usage qui permet de **mieux maîtriser les dépenses.**

Aussi, il permet d'ajuster **facilement la capacité de stockage** en fonction de l'évolution des besoins de l'entreprise.

Sécurité et conformité

Certains fournisseurs de stockage cloud sont **certifiés ISO 27001 et HDS**. Ces certifications garantissent des audits réguliers et des processus conformes aux **meilleures pratiques de protection des données**. En plus, ces fournisseurs utilisent des outils de sécurité avancés, comme **le chiffrement des données, des systèmes anti-DDoS et des protections contre les ransomwares.**

Optimisation des ressources internes

Les services cloud sont opérés par des entreprises spécialisées, dont c'est le cœur de métier. **En externalisant ces tâches, vos clients sont allégés des lourdeurs de gestion quotidienne**. Les fournisseurs cloud mettent à jour leurs systèmes en permanence pour intégrer les dernières avancées en matière de **sécurité** et de **performance**.

c. Pourquoi privilégier le stockage S3 pour le stockage cloud des sauvegardes ?

Le stockage S3 ou stockage objet se différencie des autres types de stockage cloud car il **dissocie les données de leur emplacement physique.** Ces données ne sont pas organisées en arborescence de dossiers, mais sont regroupées dans un **espace sans hiérarchie**. Cette approche permet une **grande souplesse pour la copie, le déploiement et l'accès aux données.**

Coût / Efficacité

Grâce à son architecture distribuée, le stockage objet permet de **stocker et de gérer de vastes volumes de données en s'appuyant sur des disques durs moins coûteux que d'autres technologies de stockage.** Ses coûts opérationnels sont donc réduits et la facturation est généralement basée sur la consommation réelle.

Scalabilité

L'un des principaux avantages du stockage objet est sa **scalabilité pratiquement illimitée.** Les objets peuvent être stockés **sans les limitations de taille** inhérentes aux systèmes de fichiers traditionnels.

Haute durabilité

Le stockage objet se distingue par sa capacité à assurer **une très haute durabilité des données**. Ce qui en fait une option privilégiée par les professionnels de l'IT pour les **sauvegardes longue durée**. Dans le cadre du stockage objet, la durabilité est souvent exprimée en pourcentage annuel, avec des normes industrielles atteignant 99.999999999% (11 neuf), ce qui équivaut à une probabilité de perte de données quasiment nulle.

Sécurité renforcée

Le stockage objet peut être utilisé avec des mécanismes de sécurité avancés tels que :

- **le chiffrement** côté serveurs et côté client ;
- **le versioning** pour conserver toutes les versions antérieures de vos données ;
- **le locking / immuabilité** pour éviter toute modification ou suppression accidentelle ou malveillante ;
- **le contrôle d'accès** pour limiter l'accès aux données à des personnes spécifiques

Interopérabilité

Les **API** standards du stockage objet permettent aux applications sur différentes plateformes de communiquer facilement, facilitant ainsi **l'intégration et le transfert de données entre divers services et fournisseurs**, notamment avec des solutions comme les NAS ou des outils de sauvegarde tels que Veeam, Commvault, Bacula, Iperius, ArcServ, Rubrik ou Atempo.

Simplicité

Le **stockage objet** est une technologie relativement **simple à utiliser**.
Les interfaces de gestion, comme les consoles, sont généralement conviviales et faciles à comprendre, ce qui permet aux entreprises de **gérer leurs sauvegardes de manière autonome** sans devoir recourir à un personnel informatique spécialisé.

d. Où en sont aujourd'hui vos clients/prospects avec leurs sauvegardes ?

Ils ont probablement adopté l'une de ces deux approches :

Approche 1

Ils stockent leurs sauvegardes uniquement sur site, via des infrastructures locales comme des NAS ou des serveurs privés. Dans ce cas, l'adoption du **stockage cloud S3 améliorera significativement la sécurité de leurs sauvegardes**, la question qui se pose désormais est : **à quel coût ?**

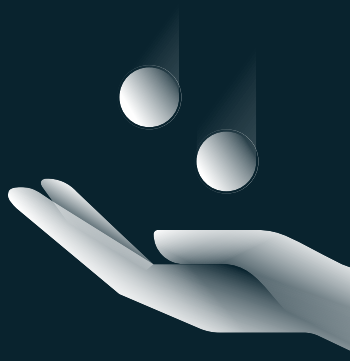
Approche 2

Ils combinent déjà stockage sur site et stockage cloud. Dans ce cas, il est pertinent de leur proposer des **alternatives plus transparentes et avantageuses**, notamment sur le plan financier.

Pour répondre à ces deux scénarios, nous aborderons en troisième partie l'épineuse question **des coûts du stockage cloud.**

Partie 3

Optimiser les coûts du stockage cloud pour vos clients



Un des principaux atouts du stockage objet ou S3 réside dans son modèle de tarification. Sa facturation est basée sur la quantité de données déposée. **L'utilisateur paye donc uniquement ce qu'il consomme.**

Mais tous les fournisseurs de stockage S3 n'offrent pas les mêmes tarifs et la même transparence… Des services comme Amazon S3, Google Cloud ou Microsoft Azure peuvent sembler attractifs, en termes de flexibilité et de fonctionnalités, mais les coûts augmentent vite, surtout si l'utilisateur gère un volume important de données ou effectue régulièrement des opérations de suppression…

Derrière ces services se cachent trop souvent **des frais imprévisibles** qui peuvent augmenter drastiquement vos factures.

Ces frais cachés ou difficilement calculables sont des freins importants à l'adoption du stockage cloud dans les stratégies de sauvegarde des organisations.

Trois types de frais cachés se distinguent particulièrement

Frais de suppression (delete fees)

S'activent lorsque vous **supprimez des fichiers avant une période minimale de rétention.** Ces frais peuvent paraître contre-intuitifs, mais ils visent à décourager les suppressions fréquentes et à stabiliser les prévisions de stockage des fournisseurs.

Frais de requêtes API

Ici, des frais sont appliqués chaque fois que votre client interroge son stockage cloud via une API. Au départ, ces frais peuvent sembler insignifiants mais ils s'accumulent rapidement si les applications accèdent fréquemment aux données ou exécutent de nombreuses requêtes. Pour les entreprises ayant des systèmes de sauvegarde ou de synchronisation automatisés, ces frais peuvent faire grimper le montant des factures de manière importante…

Frais de sortie (egress fees)

Les frais de sortie sont l'un des coûts les plus importants et les plus trompeurs du cloud. Il s'agit de **frais facturés lorsque l'entreprise récupère ou transfère ses données hors du cloud vers un autre service ou un stockage local.** Cela peut rapidement devenir un gouffre financier si une entreprise doit fréquemment récupérer ses sauvegardes, migrer des données importantes ou tester son Plan de Reprise d'Activité (PRA).

Face aux abus et à l'incapacité des principaux acteurs du marché à proposer une tarification transparente, de nouvelles alternatives ont émergé dans le domaine du stockage de sauvegarde pour proposer aux entreprises **des modèles tarifaires plus clairs et plus compétitifs.**

b. Nouvelles solutions alternatives aux GAFAM

- **Des entreprises américaines** proposent des alternatives, à première vue intéressante, avec un **modèle de facturation plus simple, sans frais de sortie.** Cependant, attention, **des frais de suppression s'appliquent encore** si les fichiers sont supprimés avant 90 jours.

- **Leviia Storag3** se démarque comme une **solution souveraine et transparente, avec un tarif fixe de 9,99 € par mois sans frais cachés,** que ce soit pour les suppressions, les requêtes API ou les sorties de données. Ce **modèle de tarification simple et prévisible** permet aux entreprises de sécuriser leurs données tout en maîtrisant totalement leurs coûts.

Veuillez, s'il vous plait, trouver ci-dessous un tableau comparatif :

		Leviia	Wasabi	Amazon
1	Souveraineté des données	🇫🇷	🇺🇸	🇺🇸
2	Prix au To déposé	9,99€	6,99€	23€
3	Frais de suppression	Gratuit	Payant augmente le coût initial de 25% à 100%.	Payant augmente le coût initial de 25% à 100%.
4	Frais de trafic sortant	Gratuit	Gratuit	Payant
5	Frais de réplication	Gratuit	Payant	Payant
6	Frais de requête API	Gratuit	Gratuit	Payant
7	Certifications ISO 27001&HDS	✓	—	✓
8	Version cloud privé	✓	—	—

Comment fonctionne l'immuabilité ?

Elle repose sur **plusieurs mécanismes techniques qui garantissent que les données ne peuvent être ni modifiées, ni supprimées pendant une période déterminée.** Voici comment cela fonctionne en détail :

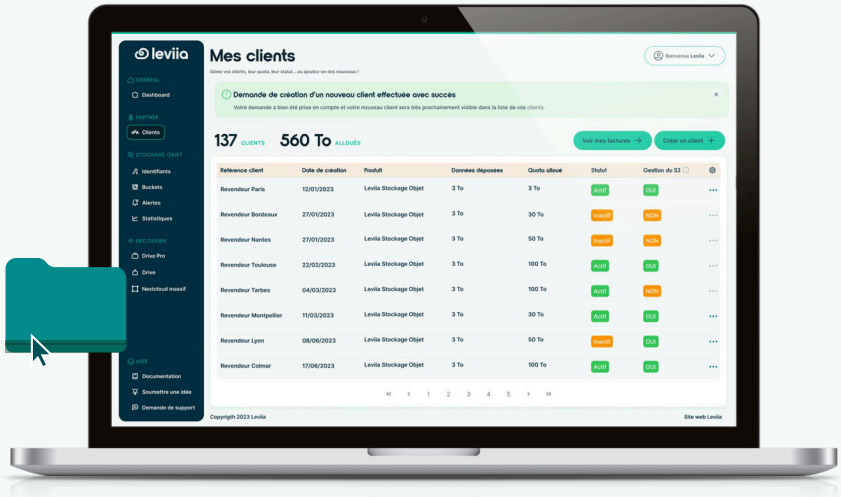
Écriture unique, lecture multiple (WORM) : la technologie WORM (Write Once, Read Many) permet de créer des fichiers ou des blocs de données qui peuvent être écrits une seule fois et lus autant de fois que nécessaire, sans possibilité de modification ou de suppression. Cela est souvent implémenté au niveau matériel ou logiciel pour s'assurer que les données une fois écrites sont figées.

Politiques de rétention : l'utilisateur définit des politiques de rétention qui spécifient la durée pendant laquelle les données doivent rester immuables. Ces politiques sont souvent configurées via le logiciel de sauvegarde ou directement sur la plateforme de votre fournisseur de stockage.

Verrouillage des objets : l'utilisateur définit une période pendant laquelle les données sont verrouillées. Pendant cette période, l'objet est inaltérable et ne peut être supprimé ni modifié. Il existe généralement deux types de verrouillage :

- **Mode compliance :** aucun utilisateur, y compris les administrateurs, ne peut modifier ou supprimer l'objet pendant la période de verrouillage. C'est le mode le plus strict et le plus sûr.

- **Mode gouvernance :** seuls les utilisateurs ayant des privilèges spéciaux peuvent supprimer ou modifier l'objet pendant la période de verrouillage.



Partie 4

Souveraineté et certifications

a. L'importance de la souveraineté des données

Les sauvegardes de vos prospects ou de vos clients contiennent souvent des informations sensibles, comme des documents stratégiques, des secrets commerciaux, des données financières, des données de santé, etc.

Or certains services, notamment américains et chinois, ne garantissent pas la confidentialité des données qu'ils stockent. Par exemple, le Cloud Act et la FISA sont deux lois étasuniennes qui autorisent les autorités judiciaires et les agences fédérales gouvernementales (FBI, NSA, CIA...) à consulter sur demande ou non les données de toute organisation cliente d'un fournisseur cloud américain.

Les risques d'espionnage économique, de fuite de données ou de violations de la confidentialité sont donc très importants. De plus en plus d'entreprises et de collectivités françaises privilégient désormais des solutions de stockage souveraines.

Sauvegarder chez un acteur souverain protège donc les données des abus des législations extraterritoriales. Vous assurez donc à vos clients que leurs données restent sous la protection des lois françaises et européennes, connues pour offrir un cadre réglementaire strict et exigeant.

Un cloud est souverain si :

- le fournisseur cloud est une **entreprise française, de droit français.**
- cette entreprise est soumise au droit français. Ainsi, elle dépend de la **même juridiction que celle de ses clients français.**
- le fournisseur cloud héberge ses données dans des **data centers localisés sur le sol français**.
- **chaque** maillon de la chaîne du traitement des données est soumis à la **juridiction française.**

Autrement dit, les solutions des GAFAM comme Microsoft One Drive ou Google Drive **ne peuvent pas être considérées comme souveraines.** Et ce, même si elles hébergent leurs données sur le sol français, car elles sont soumises à la législation étasunienne.

Les données de vos clients sont-elles stockées sur un cloud souverain ?

Les données sont-elles hébergées dans des **data centers en France** ?

Oui

L'entreprise qui héberge les données est-elle **française** et donc soumise au **droit français**?

Oui

Les données sont **stockées sur un cloud souverain**

Non

Les données **ne sont pas sur un cloud souverain** et sont soumises à une **juridiction étrangère**

b. L'importance des certifications HDS et ISO 27001 pour garantir la sécurité

Les certifications ISO 27001 et HDS garantissent aux clients que l'entreprise applique des politiques et des procédures strictes qui assurent l'intégrité et la confidentialité de leurs données, y compris les plus sensibles. L'entreprise est soumise à des audits réguliers par des organismes indépendants pour renouveler ces certifications et optimiser ses processus en permanence. **Ces mesures protègent efficacement contre les accès non autorisés, les fuites ou les pertes de données.**

Nous souhaitons aborder ce sujet avec une perspective plus subjective.

Chez **Leviia**, nous avons fait le choix de certifier notre **solution de stockage S3 ISO 27001** et **HDS** pour l'ensemble de nos clients, et ce, quelles que soient leurs données, même s'il ne s'agit pas de données de santé. Cette décision repose sur un constat simple : aujourd'hui, toutes les données sont sensibles. La donnée est devenue un actif stratégique et les cybermenaces ne cessent de croître. Par exemple, **les cyberattaques par ransomwares augmentent en moyenne de 84 % chaque année.**

En examinant de près les exigences des **certifications ISO 27001 et HDS**, il nous paraît évident qu'elles devraient constituer la norme pour toute entreprise proposant des solutions de stockage.

Pourquoi ? Car ces certifications concernent des aspects **indispensables de la sécurité** : la gestion des risques, la protection contre les violations de données ou la mise en place de contrôles rigoureux...

Adopter ces standards pour nos produits de sauvegarde de données nous paraît être une chose évidente à faire. Prenons l'exemple du port de la ceinture de sécurité : avant, ce n'était pas obligatoire, maintenant c'est indispensable. Personne ne remettrait cela en cause aujourd'hui. Chez Leviia, nous pensons que le secteur suit le même chemin pour la sécurité des données en ligne.

Attention, vous arrivez à la partie la plus importante !

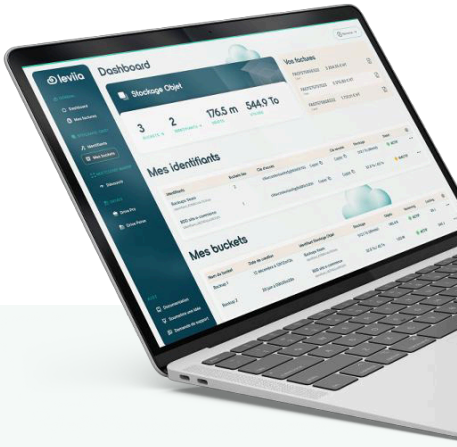
Quelle est l'étape d'après pour vous ?

Si vous êtes arrivé jusqu'ici, c'est que les sauvegardes cloud représentent sans doute une opportunité pour votre activité ou celle de vos clients.

Sachez que **Leviia Storag3** vous est accessible via un **programme partenaires avec des conditions tarifaires avantageuses**, spécialement pour les revendeurs.

Des dizaines de revendeurs font déjà confiance à Leviia Storag3 car notre solution :

- propose un **tarif prévisible et transparent,** sans frais cachés ni mauvaises surprises pour leur clients
- est **3 fois moins chère qu'AWS**
- est **certifiée ISO27001 & HDS**
- est **100% française 100% souveraine**



Ils nous font déjà confiance :

econocom · JCD groupe · CFi · SCC · WORLDLINE

Vous êtes intéressé ?

Contactez-nous en cliquant ici

Ou envoyez-nous un mail directement à info@leviia.com

On espère vous parler bientôt !
L'équipe Leviia.

Merci !

leviia