

LIVRE BLANC

La règle du « 3-2-1 » de la sauvegarde

Une protection des données sûre et efficace

Résumé

Au-delà de son personnel, les données comptent parmi les biens les plus précieux d'une entreprise. La protection des données et la continuité de l'activité sont essentielles pour permettre aux organisations de poursuivre leurs opérations à la suite d'une perte de données catastrophique. Une telle perte peut aller jusqu'à l'impossibilité de restaurer ou reconstituer les données par un quelconque moyen.

D'innombrables causes peuvent être à l'origine d'une perte totale ou partielle d'informations :

- vos sauvegardes locales peuvent subir des dommages en cas de sinistre local ;
- vos données peuvent être inaccessibles en raison d'une attaque de rançongiciel ;
- un utilisateur peut, de façon accidentelle ou intentionnelle, supprimer des données indispensables à la conduite de votre activité ;
- certaines solutions et mises à jour matérielles et/ou logicielles peuvent causer une perte de données ou un retard dans la continuité de l'activité

Ce livre blanc décrit des méthodes de protection des données efficaces, qui permettent de réduire au minimum les coûts liés aux temps d'arrêt et aux pannes en cas d'incident entraînant une perte de données. Des règles de bonne pratique sont exposées pour mettre en œuvre une stratégie de reprise après sinistre dans les environnements de petite, moyenne ou grande entreprise.

Contexte

Les incidents entraînant des pertes de données peuvent se produire à tout moment. Qu'il s'agisse d'erreurs matérielles, de fautes humaines, de virus, d'attaques par des programmes malveillants ou de sinistres locaux, les entreprises doivent être parées à garantir la continuité de leur activité et la disponibilité de leurs données. Différentes causes et conséquences possibles d'une perte de données sont décrites ci-après.

Défis liés aux produits et aux technologies :

- Au total, 21 % des pertes de données sont provoquées par des défaillances matérielles.
- 1 ordinateur portable sur 3 tombe en panne avant trois ans.
- Une unité de disque connaît une défaillance toutes les 15 secondes.
- Plus de 390 000 programmes malveillants sont découverts chaque jour.
- Les attaques par des rançongiciels causent 16,2 jours d'interruption d'activité en moyenne.
- 43 % des cyberattaques visent les petites entreprises, alors que seules 14 % d'entre elles sont prêtes à se défendre.

Un arrêt d'activité lié à une perte de données a de multiples conséquences. Le bilan financier peut être déséquilibré par les risques de pertes sur les ventes. Le respect des obligations financières est compromis, d'où des taux d'intérêt plus élevés et des réclamations en dommages et intérêts de tiers. Les employés ne peuvent plus exécuter leurs tâches et sont donc mis en défaut.

Votre réputation peut également en subir le contrecoup. Les retards dans l'assistance peuvent inciter votre clientèle à se tourner vers la concurrence. La pénurie temporaire de liquidités inquiète les fournisseurs et les banques et restreint votre solvabilité.

Des défis financiers et économiques existent :

- Les petites entreprises sont particulièrement affectées par de telles situations ; 98 % d'entre elles ferment leurs portes après avoir été piratées.
- 93 % des entreprises dépourvues de plan de reprise après sinistre ferment dans l'année qui suit un piratage de données.
- 60 % des entreprises ferment dans un délai de 6 mois après une perte de données.
- Le coût d'une heure d'interruption d'activité se chiffre à :
 - 8 000 \$ (7 000 €) pour une petite entreprise
 - 74 000 \$ (63 000 €) pour une entreprise de taille moyenne
 - 700 000 \$ (600 000 €) pour une grande entreprise

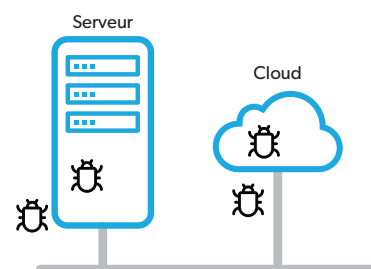
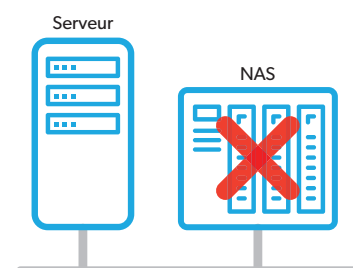
Le problème

Bon nombre d'entreprises ne sont pas prêtes à assurer la continuité de leur activité. Les sauvegardes sont généralement effectuées sur des périphériques de stockage tels que des disques locaux, via un système de stockage NAS (Network Attached Storage), ou dans le cloud. Cette solution est viable, mais ne tient pas compte des catastrophes locales, ni des attaques par les virus et rançongiciels.

Lorsqu'un sinistre local se produit, les sauvegardes locales peuvent elles aussi être endommagées. Les attaques de virus et rançongiciels peuvent infecter les jeux de sauvegardes quel que soit leur emplacement, que ce soit sur ordinateur, en réseau ou dans le cloud.

Dans les deux cas, il peut être impossible de restaurer les données et de les récupérer à la suite de tels incidents. Certaines données sont susceptibles d'être reconstituées à partir de lettres, factures ou autres documents papier. Les clients peuvent contribuer à fournir des informations perdues, mais celles-ci sont irrécupérables dans la majorité des cas.

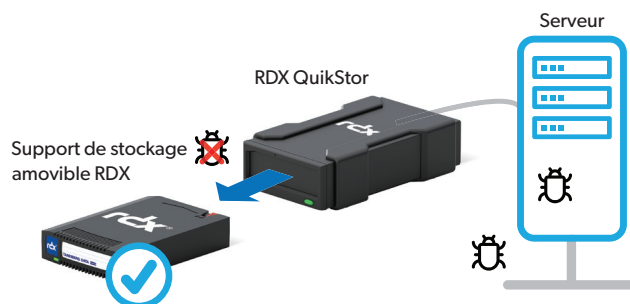
En cas d'attaque par rançongiciel, il n'existe parfois pas d'autre choix que celui de verser une rançon pour obtenir le déchiffrement des données. Les entreprises subissent alors un préjudice dans tous les domaines : chiffre d'affaires, investissements, réputation, confiance et clientèle.



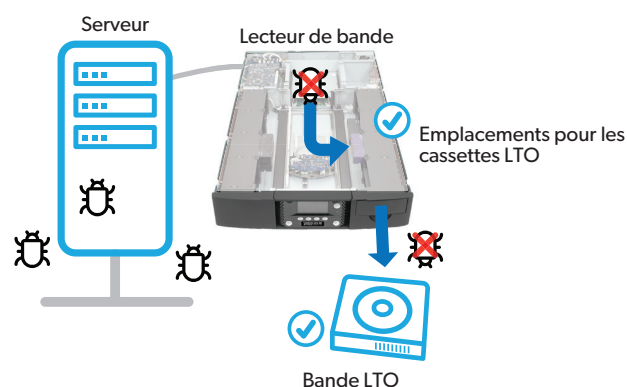
La solution : mettre en place une sécurité Air Gap

Une fois les périphériques de stockage déconnectés du réseau, les données de sauvegarde sont sécurisées et à l'abri des attaques par des programmes malveillants. Les entreprises ont donc tout intérêt à utiliser des supports de stockage amovibles. Les systèmes à disques amovibles permettent de déconnecter le support de stockage du réseau, de manière à garantir l'accessibilité des données après un sinistre local ou une attaque par un rançongiciel.

Pour ce faire, le périphérique de stockage peut être mis hors ligne afin d'être transporté en lieu sûr à l'extérieur du site (hors site). Les opérations d'éjection peuvent être configurées ou exécutées sous forme de scripts par la plupart des logiciels de sauvegarde.



Le même principe s'applique aux données stockées sur bande. Celles-ci sont protégées contre les virus et rançongiciels. Le format sur bande n'étant pas géré par un système de fichiers, les programmes de crypto-verrouillage et autres virus n'ont aucune chance d'infecter les données, même en présence d'un support de bande dans le lecteur. Néanmoins, le risque de sinistre local, qui peut lui aussi entraîner une destruction totale des bandes, doit être pris en considération. Les bandes doivent donc être stockées hors site en dehors du centre de données. Lorsque des bibliothèques de bandes contenant plusieurs centaines ou milliers de supports sont utilisées, elles doivent être localisées dans un centre de données distinct.

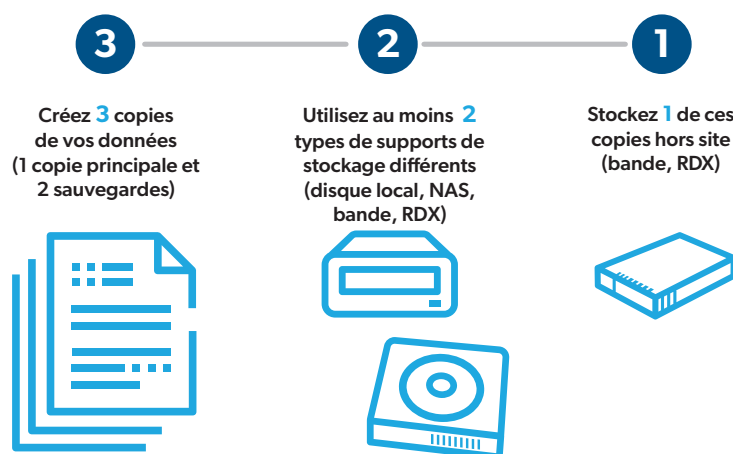


La stratégie de sauvegarde « 3-2-1 »

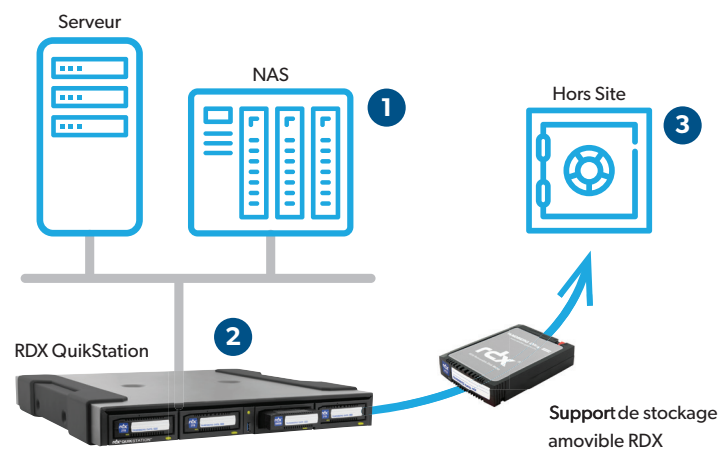
Que votre environnement professionnel soit celui d'une TPE, d'une PME ou d'une grande entreprise, vous devez mettre en œuvre une stratégie de sauvegarde « 3-2-1 », qui consiste à conserver trois copies de vos données sur deux supports différents et à stocker une copie hors site.

La quasi-totalité des applications de sauvegarde permettent d'exécuter une tâche de copie de la sauvegarde une fois la tâche de sauvegarde principale terminée. Pour les plus grandes entreprises, une unité de disque, NAS, DAS ou SAN est recommandée en tant que cible de sauvegarde principale. Cette solution accélère la restauration en cas de perte de données. Elle permet de réduire les temps d'arrêt et de reprendre rapidement l'activité.

Pour la cible de sauvegarde secondaire, il convient de mettre en œuvre un système de stockage avec support amovible. Si le support principal, en l'occurrence un disque, tombe en panne, l'autre support reste disponible pour les besoins de la restauration. En fonction de la quantité de données, un système à bande ou RDX s'impose. Si l'entreprise a besoin de sauvegarder une quantité de données importante, un chargeur automatique de disque ou une bibliothèque de bandes est l'option indiquée. Ces systèmes permettent l'automatisation et la gestion complète des supports. En outre, ils offrent un coût de stockage plus faible et une durée d'archivage de 30 ans. Ils sont par conséquent indiqués pour l'archivage à long terme des données rarement utilisées.



L'unité RDX QuikStation est une solution iSCSI à disques amovibles conçue pour offrir une plateforme flexible de protection des données et de récupération après sinistre hors site dans un contexte de cloud hybride, adaptée à l'environnement tant matériel que virtuel. Plusieurs configurations sont possibles : cibles à disque unique, chargeur automatique de disque ou émulation de chargeur ou bibliothèque de bande et volumes logiques à travers toutes les cibles RDX avec tolérance aux pannes RAID 5 ou RAID 6. L'unité RDX QuikStation utilisant des supports encapsulant un disque dur, elle offre les mêmes avantages en termes de performances que la cible de sauvegarde principale.



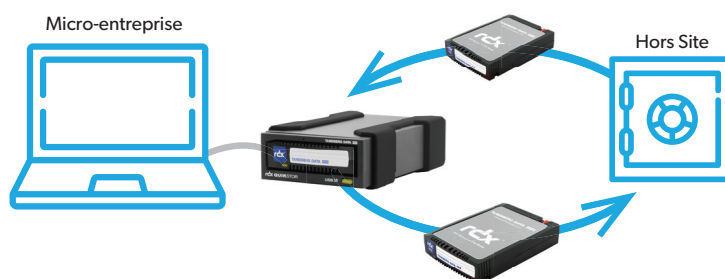
Les deux périphériques de sauvegarde secondaires permettent de réaliser la dernière étape de la stratégie de sauvegarde « 3-2-1 ». Les systèmes RDX QuikStation et à bandes offrent la possibilité d'exporter les données hors ligne afin de créer une sécurité Air Gap pour la protection contre les programmes malveillants, et/ou hors site pour la protection contre les catastrophes locales. Avec les produits d'automatisation sur bande, la mise hors ligne des données s'effectue en éjectant la cassette du lecteur et en la plaçant dans un emplacement libre au moyen du bras de la robotique. En outre, des ports d'Import/Export sont disponibles pour sortir le support de bande afin de le placer hors site, en lieu sûr.

Les unités RDX QuikStation permettent également de mettre des supports RDX hors ligne et/ou hors site. En mode chargeur automatique de disque ou d'émulation d'automatisation de bande, le support est déconnecté logiquement du réseau, de sorte que les données de sauvegarde soient hors de portée en cas d'attaques par des virus ou programmes malveillants. En mode de disque fixe, de support RDX et de volume logique, le support est physiquement éjecté et peut être mis hors site pour une protection contre les sinistres locaux.

Une autre copie doit également être stockée sur un support amovible afin d'être placée hors site. Cette configuration garantit la possibilité d'une restauration complète des données en cas de sinistre sur le site de l'entreprise.

Pour les environnements de petite taille dotés d'une infrastructure de serveur unique, les utilisateurs d'ordinateurs portables ou les mises en œuvre NAS uniques incompatibles avec des systèmes de stockage multiples, la meilleure solution est un schéma de rotation des supports avec RDX QuikStor et trois cassettes RDX. La stratégie de sauvegarde « 3-2-1 » se décline comme suit :

- un support se trouve dans le système, prêt pour la prochaine tâche de sauvegarde ;
- un deuxième support est placé hors site en lieu sûr ;
- le troisième est transféré depuis ou vers l'emplacement hors site.



L'utilisation d'une rotation des supports vous permet d'alterner ces derniers une fois la sauvegarde terminée. Il est très pratique, pour la rotation des supports, que chacun d'eux soit éjecté une fois la procédure de sauvegarde terminée. Pour cela, la plupart des logiciels de sauvegarde intègrent un système d'éjection des supports, ou des commandes de pré-scriptage et de post-scriptage lors de la configuration des tâches de sauvegarde, qui permettent de programmer l'éjection.

Conclusion

Assurer la continuité des activités est la tâche la plus importante pour n'importe quelle entreprise, quelle que soit sa taille. Les pertes de données et les interruptions d'activité entraînent des pertes financières qui peuvent aller jusqu'à des faillites d'entreprises

Le concept de sauvegarde « 3-2-1 » s'impose comme l'une des méthodes les plus sûres et les plus éprouvées pour se prémunir contre les pannes matérielles et les intrusions par des programmes malveillants. Si vous gérez une micro ou petite entreprise, la rotation des supports est une nécessité.



Les services de vente et d'assistance pour les produits et solutions d'Overland-Tandberg sont disponibles dans plus de 90 pays. Contactez-nous dès aujourd'hui à l'adresse salesemea@overlandtandberg.com.

Consultez le site [OverlandTandberg.com](https://www.OverlandTandberg.com).

©2021 Overland-Tandberg. Toutes les marques et marques déposées appartiennent à leurs propriétaires respectifs. Les informations contenues dans le présent document sont susceptibles d'être modifiées sans préavis et sont fournies « telles quelles » sans garantie d'aucune sorte. Overland-Tandberg décline toute responsabilité en cas d'erreurs ou d'omissions de nature technique ou éditoriale contenues dans le présent document.