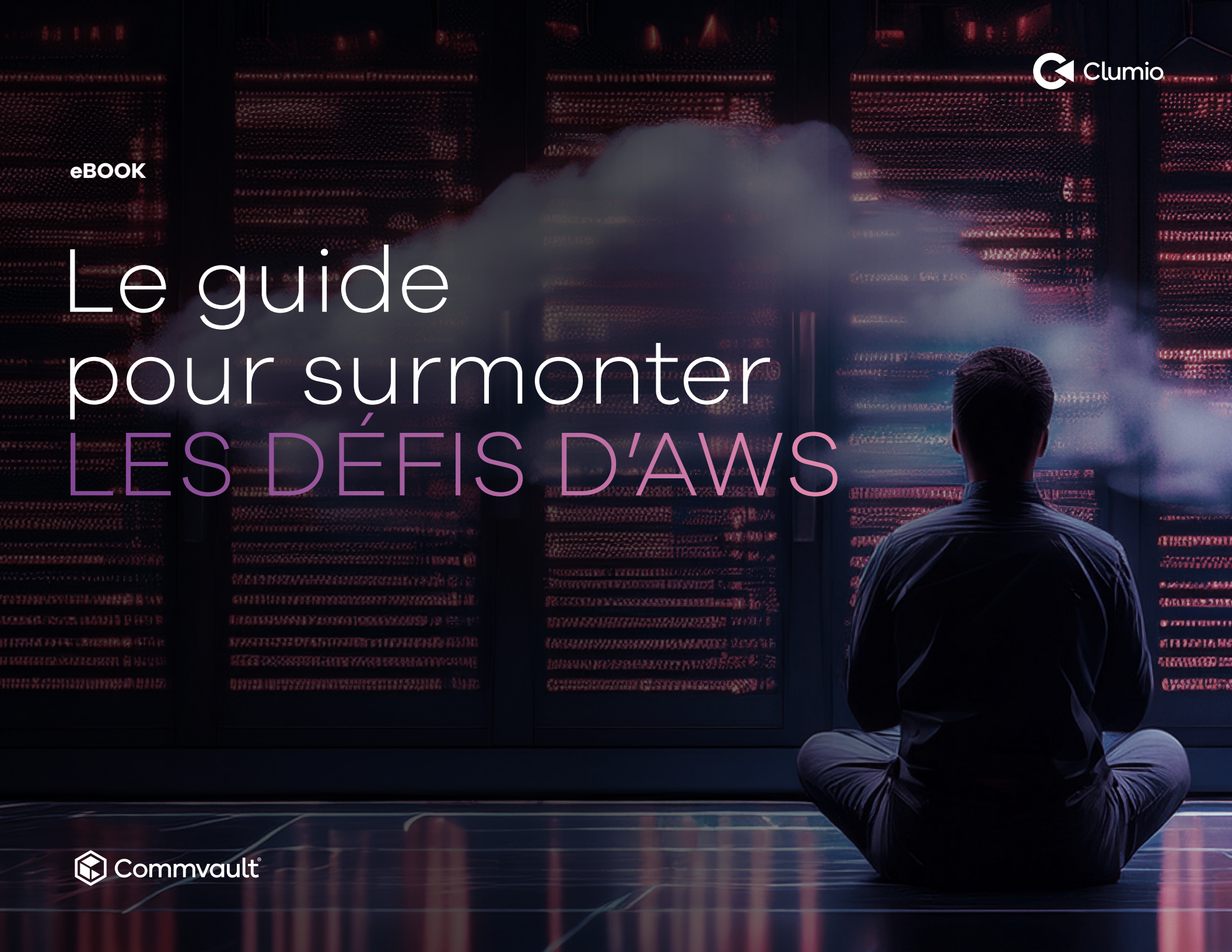


Clumio

eBOOK

Le guide pour surmonter LES DÉFIS D'AWS

Commvault®

Sommaire

01

Libérer toute la valeur du cloud

Depuis plusieurs années, les organisations se sont engagées dans un parcours de transformation numérique visant à moderniser leurs services et à améliorer l'expérience client. L'année 2020 a encore accentué ces exigences, obligeant les entreprises de toutes tailles à repenser leur mode de fonctionnement. La transformation numérique est passée du statut d'option permettant de rester compétitif à celui d'impératif pour assurer la réussite.

Être contraint à un site physique pour gérer les opérations quotidiennes n'est plus viable, car le monde actuel exige la capacité de fonctionner efficacement à 100 % depuis n'importe quel endroit. Les clouds publics, comme AWS, étaient déjà une option pour atteindre cet objectif, mais en 2020, leur adoption s'est accélérée de manière spectaculaire.

Les moteurs de la migration vers le cloud incluent l'accès aux technologies les plus avancées, la possibilité d'innover plus rapidement et la suppression de la gestion de l'infrastructure informatique. Ces avantages permettent aux organisations de se concentrer sur leur cœur de métier et de croître beaucoup plus rapidement. Le cloud est là pour rester, et presque toutes les organisations auront une présence dans le cloud.

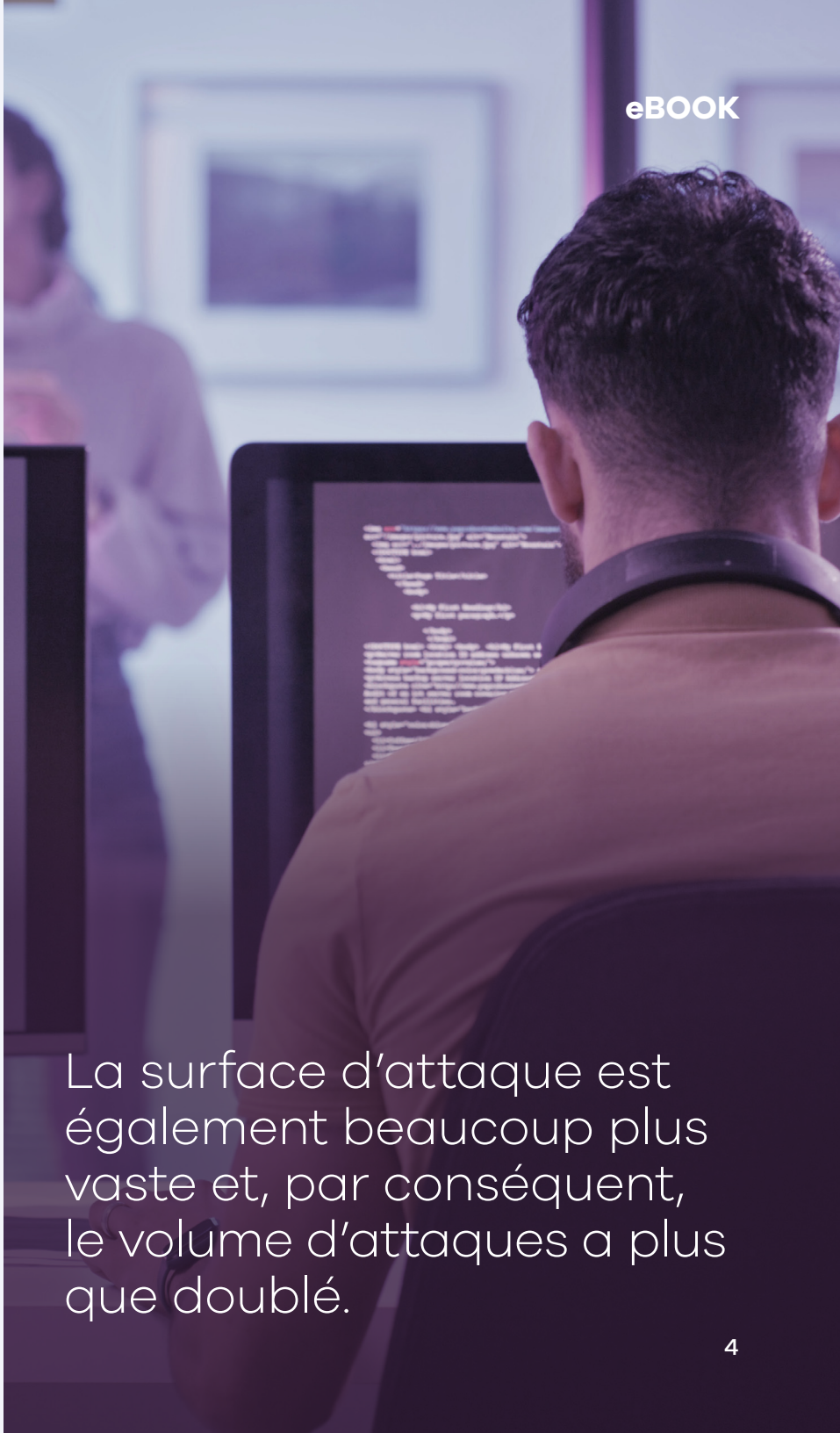
Avec le rythme rapide d'innovation de leurs services, AWS est devenu le choix de cloud privilégié pour de nombreuses entreprises. Cependant, malgré tous les avantages qu'offre AWS, il existe également des défis importants qui empêchent de libérer pleinement le potentiel du cloud.

Protéger les données dans AWS

Protéger les données de l'entreprise et celles des clients dans le cloud constitue l'un des défis majeurs. Disposer d'une stratégie solide de sauvegarde et de restauration dans AWS est tout aussi important que dans un environnement sur site — voire davantage. Sous plusieurs aspects, cette tâche est également plus complexe.

Avec l'accélération de l'innovation permise par le cloud, les organisations déploient et étendent leurs applications à un rythme beaucoup plus rapide, générant ainsi d'énormes volumes de données de production qui doivent être protégées. Les données dans le cloud sont également plus dispersées — entre les applications, les comptes, les régions et même différents clouds publics.

La surface d'attaque est également beaucoup plus vaste, et en conséquence, le volume d'attaques ne cesse d'augmenter. Enfin, en matière de protection des données, les organisations évoluent dans un environnement bien plus décentralisé que dans le monde traditionnel sur site.



La sauvegarde AWS est-elle la solution?

De nombreuses organisations commencent à utiliser le cloud au travers de projets de « shadow IT » ou dans le cadre d'une initiative de transformation numérique incluant une migration vers le cloud. AWS permet aux ingénieurs de lancer facilement quelques instances EC2 et de commencer à déployer des workloads de bases de données dans RDS.

Une fois bien avancées, ces organisations réalisent qu'il n'existe aucune stratégie solide de protection des données pour toutes ces nouvelles charges clou: aucun véritable plan de sauvegarde et de restauration. Après tout, la sauvegarde ne fait généralement pas partie du vocabulaire des ingénieurs, et beaucoup supposent que tout est déjà pris en charge. En matière de protection des données, il peut être difficile de savoir par où commencer dans le cloud.

Une voie simple, à ce stade, consiste à utiliser les services de sauvegarde natifs d'AWS. Une des méthodes les plus courante's qu'adoptent les organisations pour commencer à protéger leurs données dans AWS est l'utilisation du service de gestion des snapshots.

Au premier abord, les snapshots semblent proposés à un prix raisonnable, environ 0,05 $/Go par mois. Les entreprises pensent disposer d'un moyen simple de prendre des snapshots via la console de gestion AWS. En réalité, pour éviter toute mauvaise surprise, certaines d'entre elles prennent même l'initiative de créer des snapshots sur tous les volumes EBS et RDS en quelques clics.

La protection des données semble sous contrôle, mais les choses ne sont pas toujours ce qu'elles semblent être.

La protection des données semble sous contrôle, mais les choses ne sont pas toujours ce qu'elles semblent être.

02

Les défis de la sauvegarde AWS

Malheureusement, il ne faut pas longtemps avant que les organisations commencent à constater les limites de l'utilisation des snapshots pour protéger leurs données critiques — qu'il s'agisse de données d'entreprise ou de données clients — dans AWS.

Bien que les snapshots offrent des capacités de protection des données élémentaires — comme la récupération après des erreurs opérationnelles — ils ne constituent pas une solution complète, simple et économique de protection des données. En réalité, les snapshots sont au mieux rudimentaires et exigent des processus complexes et chronophages pour exécuter des tâches quotidiennes pourtant basiques — ce qui va à l'encontre même des raisons pour lesquelles les entreprises adoptent le cloud public.

En fin de compte, les fournisseurs de cloud, y compris AWS, garantissent la sécurité de l'infrastructure, mais pas celle des données. Les clients restent responsables de la gestion de leurs propres données. Ainsi, pour tirer pleinement parti d'AWS, il est essentiel que les entreprises adoptent une stratégie de protection cloud adéquate.

Examinons de plus près ce qui rend l'utilisation des snapshots pour la sauvegarde et la restauration dans AWS si problématique.

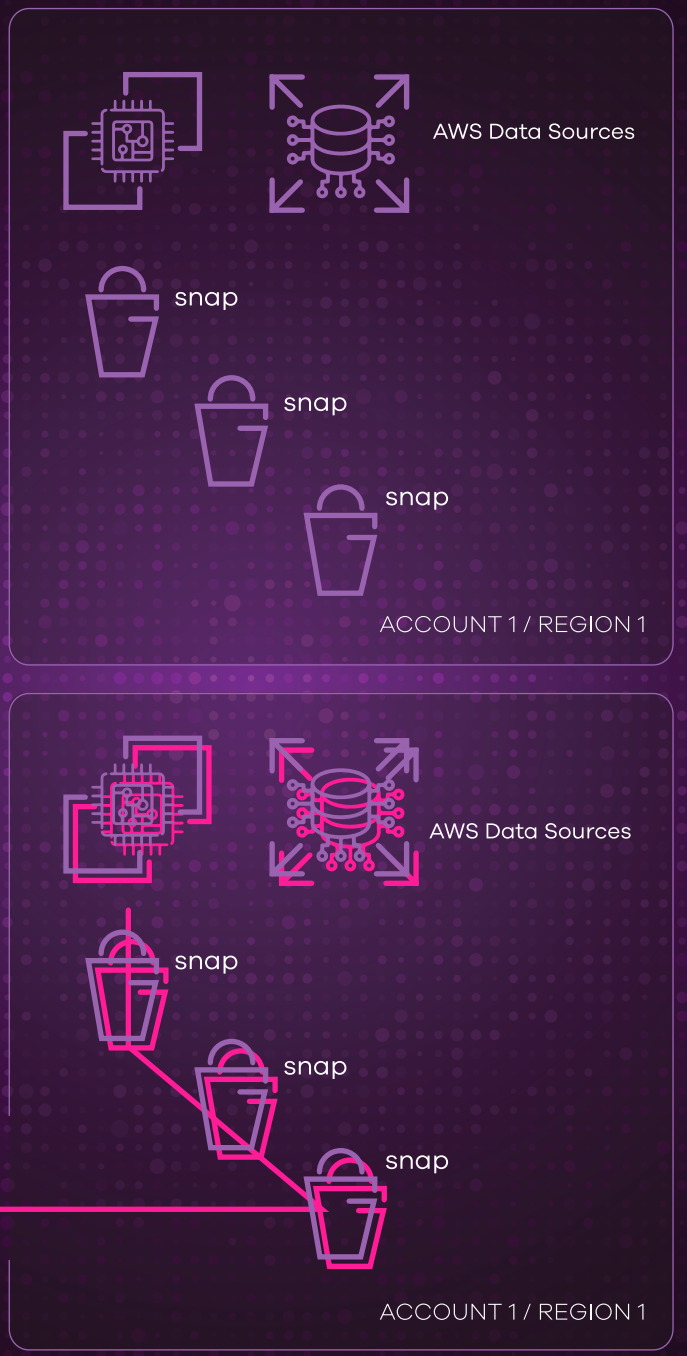
Absence d'air gap

Les attaques par ransomware explosent, et la crainte que des criminels prennent en otage les données d'entreprise est devenue le pire cauchemar de nombreux DSI et décideurs IT. Selon Cybersecurity Ventures, les ransomwares devraient coûter aux victimes environ **275 milliards de dollars par an d'ici 2031**, avec **une nouvelle attaque toutes les 2 secondes.** Il est donc essentiel de disposer d'une solution de cyber-résilience capable de contrer efficacement ces menaces.

La solution recommandée par les experts, tels que la CISA (Cybersecurity and Infrastructure Security Agency), consiste à disposer de **sauvegardes air-gappées,** c'est-à-dire isolées et sécurisées indépendamment du périmètre de sécurité de l'organisation. Cela empêche les pirates de localiser la copie de sauvegarde, même s'ils parviennent à accéder à votre compte cloud.

Comme illustré, lorsque les organisations utilisent AWS Backup pour protéger des sources de données telles que EC2, EBS, RDS, etc., les snapshots sont créés **dans le même compte** que les données primaires. Le problème de cette approche est qu'elle n'assure aucune séparation — aucun air gap — entre les données primaires et les snapshots. Bien qu'AWS ait introduit des coffres logiquement isolés pour certains services, ceux-ci restent dans le périmètre de sécurité de l'entreprise et peuvent encore être vulnérables à une compromission.

Si un pirate ou un acteur malveillant accède au compte principal, il compromettra d'abord les snapshots avant de s'attaquer aux données primaires. Il n'existera alors **plus aucune copie de sauvegarde valide et exploitable,** ce qui rend impossible toute restauration. C'est précisément la situation que les organisations cherchent à éviter, et cela constitue une limitation majeure des mécanismes de protection des données dans le cloud.

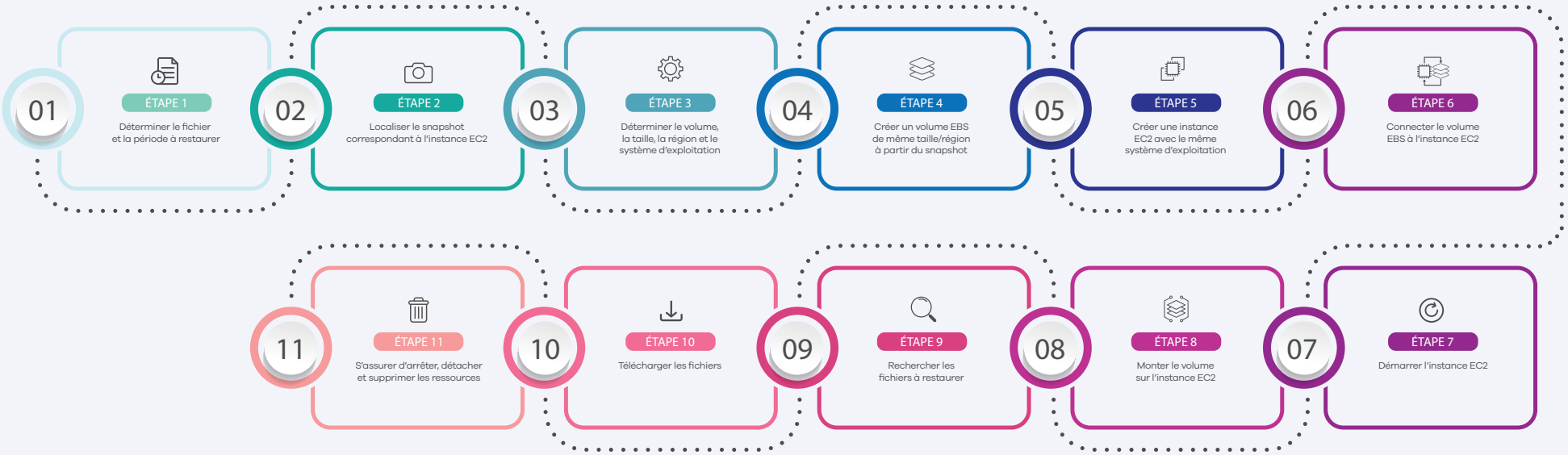


Temps de récupération longs

La protection des données repose sur deux fonctions fondamentales : la sauvegarde et la restauration. S'il est crucial de s'assurer que toutes les données critiques sont correctement sauvegardées, il est tout aussi important de disposer d'une solution permettant une restauration rapide en cas de défaillance ou de compromission des données. Ne pas pouvoir récupérer les données métier à temps lors de tels événements entraîne des interruptions de l'activité, une mauvaise expérience client et, dans les cas extrêmes, peut même mettre en péril la survie de l'organisation.

La restauration ne consiste pas seulement à accéder aux données: elle dépend du temps nécessaire pour accéder aux données de manière granulaire. Restaurer des données à partir de snapshots AWS peut prendre plusieurs heures, voire plusieurs jours.

Le processus de restauration s'apparente à une situation où l'on disposerait de nombreuses boîtes remplies de fichiers dans un entrepôt. Avec les snapshots, il n'y a pratiquement aucune visibilité sur le contenu de chaque boîte, ce qui oblige l'organisation à les ouvrir une par une et à fouiller dans chaque fichier. L'entreprise doit passer en revue toutes les boîtes pour tenter de trouver le fichier dont elle a besoin. Lorsqu'elle pense avoir trouvé le bon fichier, elle commence le processus de restauration, puis doit attendre que l'opération se termine — ce qui peut, à lui seul, prendre beaucoup de temps.



Ensuite, ils doivent monter le volume sur un serveur. Puis, ils doivent le charger et vérifier qu'il s'agit bien des données recherchées. Souvent, ils constatent que le fichier nécessaire n'est pas présent, ou qu'il ne s'agit pas de la bonne version. Ils doivent alors retourner aux « boîtes » et recommencer toute la procédure depuis le début. Ce processus peut facilement prendre plusieurs heures.

Examinons un scénario typique pour illustrer ce point. Une organisation utilise AWS Backup pour protéger ses volumes EBS et doit maintenant récupérer un fichier spécifique depuis l'un des volumes compromis. Elle devra effectuer les étapes complexes suivantes dans AWS pour récupérer le fichier.

Selon le temps nécessaire pour trouver le bon snapshot (Étape 2), identifier le bon système d'exploitation, la taille du volume, la région, etc. (Étapes 3 à 5), puis créer une instance EC2 correspondant à l'instance d'origine, ce processus complet peut facilement prendre plusieurs heures.

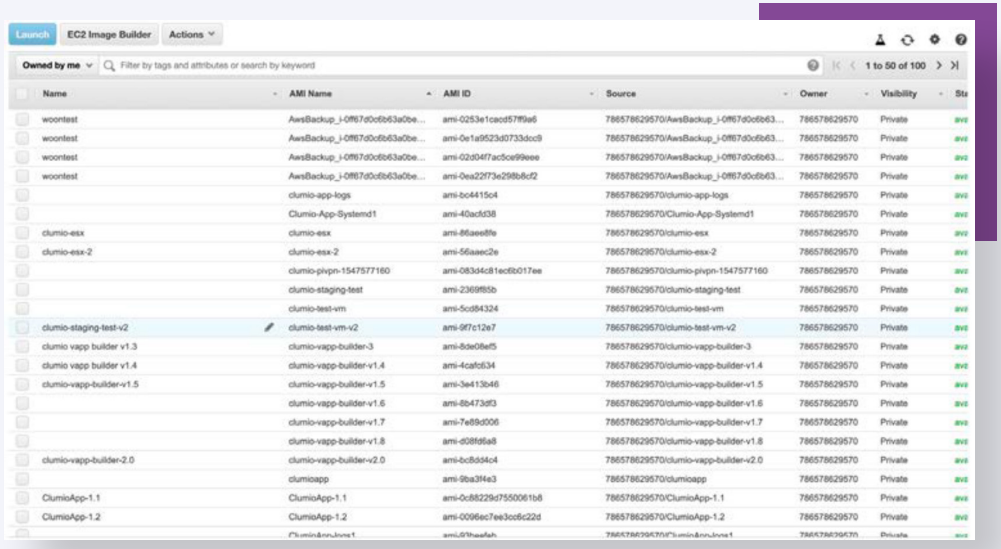
Et ces étapes complexes doivent être répétées pour chaque fichier à restaurer. La situation est encore pire avec RDS, car il faut restaurer une instance RDS entière pour accéder aux données — même si l'on ne recherche qu'un seul enregistrement. Enfin, il faut s'assurer que toutes les ressources créées dans le cloud pour effectuer la récupération sont ensuite arrêtées et supprimées afin d'éviter des coûts supplémentaires indésirables.

Visibilité nulle

La configuration des stratégies de protection des données pour l'ensemble des applications n'est pas une tâche quotidienne. En réalité, ces stratégies devraient être définies une fois, avec les bons paramètres, puis rarement modifiées afin de respecter les exigences de conformité. Dans ce mode de fonctionnement, il est difficile pour les administrateurs IT de se souvenir de chaque politique, de l'historique des sauvegardes et des exigences de conformité associées à chaque source de données protégée dans leur environnement.

Cependant, il est essentiel d'avoir facilement accès à ces informations lorsque cela est nécessaire. Par exemple, ils doivent être en mesure de:

- Prouver rapidement la conformité lors des audits
- Trouver facilement le bon snapshot au moment de la restauration
- Sélectionner la politique adéquate pour protéger une nouvelle application ou une nouvelle source de données
- Faire tout cela à travers des centaines de comptes



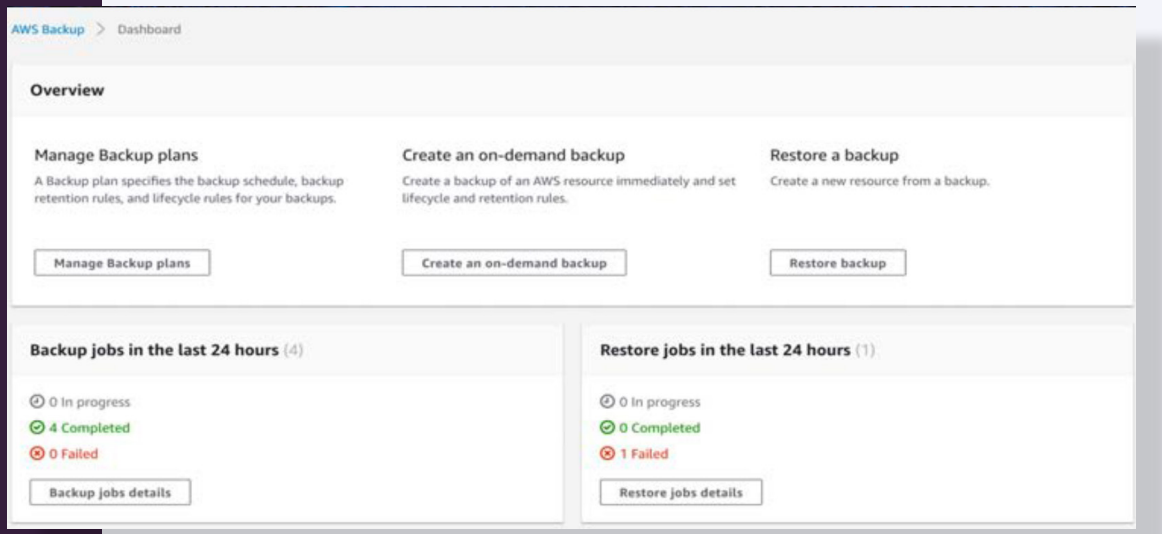
Beaucoup de snapshots à faire défiler

Trouver un snapshot à restaurer est un processus compliqué et chronophage.

AWS Backup ne fournit pas les fonctionnalités ci-dessus, ce qui entraîne une visibilité limitée de votre stratégie de protection des données. Examinons un exemple concret illustrant les dangers que cela peut représenter pour une entreprise.

Les services informatiques sont souvent audités afin de démontrer qu'ils respectent différentes normes de conformité. Un assureur, par exemple, peut exiger qu'une entreprise prouve qu'elle conserve **30 jours de sauvegardes.**

Pour répondre à cette exigence avec AWS Backup, une organisation devrait soit écrire du code pour en apporter la preuve, soit la démontrer manuellement à la demande d'un auditeur. Or, un processus manuel introduit un risque d'erreurs, tant pour la protection des données que pour le respect de la conformité. Le service IT devra probablement passer par cette procédure fastidieuse plusieurs fois par an, selon le calendrier des audits, et pourrait y consacrer **près d'une semaine** à générer des rapports — en plus de toutes ses autres responsabilités.

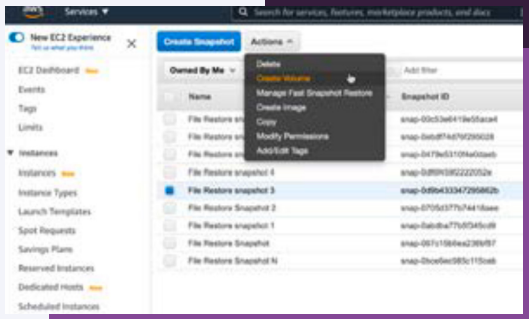


Aucune visibilité sur la conformité

Complexité supplémentaire

Compte tenu des lacunes d'AWS Backup présentées jusqu'ici, il est clair que les snapshots offrent des capacités très basiques. Les organisations qui commencent à utiliser les snapshots pour sauvegarder leurs données AWS rencontrent rapidement ces limites et se retrouvent contraintes d'y remédier.

Elles finissent par écrire des scripts complexes pour ajouter les fonctionnalités manquantes à leur solution de protection des données. Elles doivent alors consacrer de précieuses ressources IT à développer et à maintenir ces scripts en continu, plutôt que de les mobiliser sur leur cœur d'activité. Cela va à l'encontre du rôle attendu du cloud, censé apporter agilité et favoriser une innovation plus rapide au sein de l'entreprise.



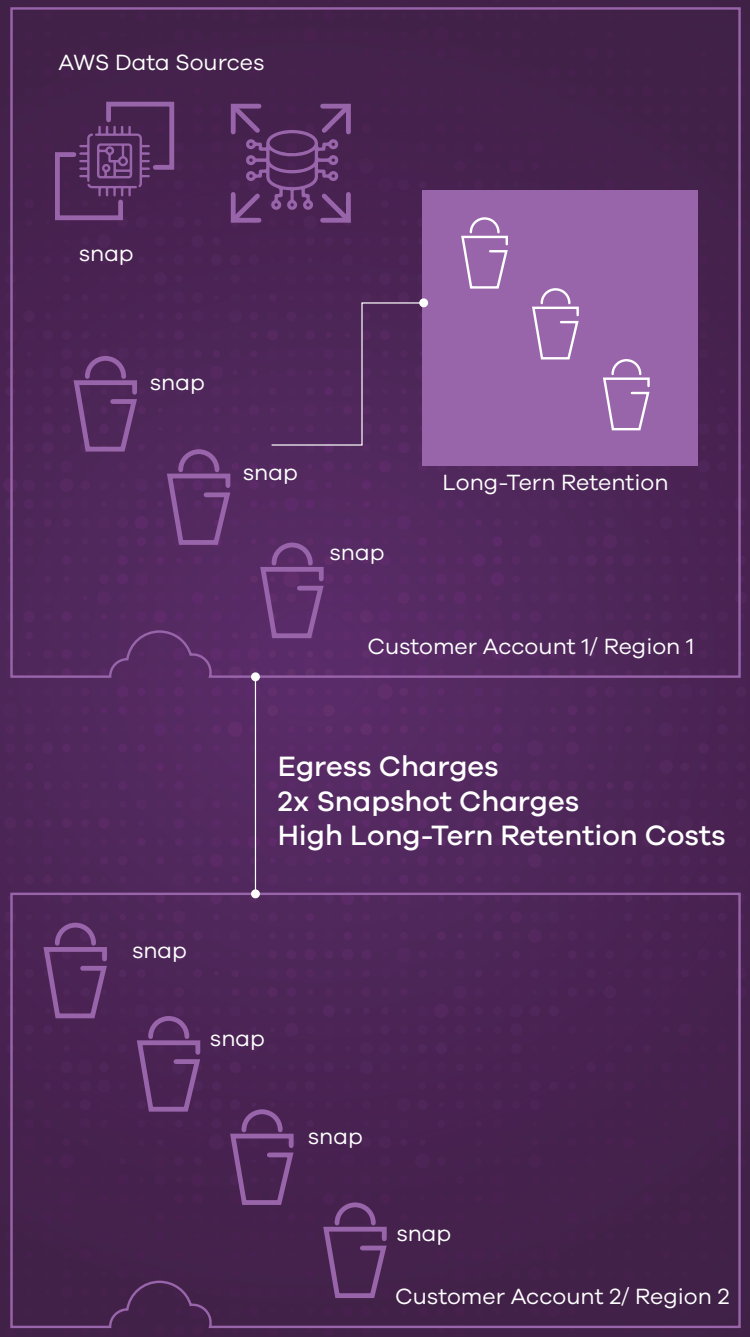
Restauration d'instance uniquement Restauration d'instance limitée au même compte uniquement	
Indisponible	**Parcourir et restaurer**
Indisponible	**Recherche globale**
Indisponible	**Restauration granulaire d'enregistrements**

Protection des données dans AWS

Dans le cadre d'une stratégie de protection des données, il est courant pour les organisations de mettre en place une rétention à long terme pour les données de production, ainsi qu'une protection contre les compromissions de compte résultant d'attaques telles que les ransomwares. Pour atteindre ces deux objectifs avec AWS Backup, les organisations procèdent généralement de la manière suivante :

- Créer une rétention à long terme basée sur des snapshots, ce qui entraîne la création d'un grand nombre de snapshots par compte, stockés dans un niveau de stockage coûteux.
- Répliquer les snapshots d'un compte vers un autre compte afin de se protéger contre les compromissions de compte, ce qui a pour effet de doubler le nombre de snapshots et donc les coûts de sauvegarde. Des frais d'egress supplémentaires s'ajoutent également pour les transferts entre comptes.

Dans un scénario typique, après quelques mois, une organisation commence à constater une tendance inquiétante : sa facture AWS augmente régulièrement et ne semble pas se stabiliser. De plus, elle n'a aucune visibilité sur ce qui génère réellement ces coûts de sauvegarde AWS. Pendant ce temps, la protection des données via AWS peut lui coûter jusqu'à 50 % de plus.



Le défi des gestionnaires de snapshots tiers

À mesure que les organisations cherchent à maîtriser le coût de leurs sauvegardes AWS, elles commencent à se tourner vers des gestionnaires de snapshots tiers. Ces outils promettent de réduire considérablement les coûts en permettant, par exemple, de transférer les données vers S3.

Le coût peut sembler raisonnable au premier abord, souvent présenté sous la forme d'une licence par instance. Toutefois, le coût total est en réalité plus élevé, car il inclut les dépenses supplémentaires que l'organisation doit assumer pour stocker les données dans AWS et, souvent, pour les ressources de calcul nécessaires à la gestion des sauvegardes. Par exemple, pour un volume EBS classique avec des modifications quotidiennes, vous continuez à payer AWS 0,05 $/Go/mois pour le stockage sous-jacent des snapshots, et la licence s'ajoute à ce montant. Cela crée une majoration immédiate.

En outre, ces solutions exécutent fréquemment leurs propres instances EC2 de gestion des sauvegardes ainsi que des instances EC2 temporaires pour le traitement, ce qui ajoute des coûts d'utilisation supplémentaires, intégrés à votre facture AWS.

Le coût par instance EC2 protégée et par mois peut sembler raisonnable, mais le coût total est en réalité plus élevé.

Encore plus de coûts cachés

Mais les organisations réalisent-elles réellement des économies grâce à la fonctionnalité de transfert vers S3? Pour offrir cette capacité, les gestionnaires de snapshots tiers lancent des instances EC2 temporaires qui fonctionnent pendant de longues périodes, ajoutant ainsi un coût caché à votre facture. Ces coûts ne sont pas évidents, car ils se retrouvent intégrés à votre propre facture EC2. Les instances temporaires doivent parcourir les snapshots EBS de l'entreprise et copier des blocs de données vers S3.

Le seuil de rentabilité pour simplement déplacer les données vers S3 se situe généralement autour de trois mois, en raison de tous ces coûts cachés. Cela signifie que si une entreprise a une période de rétention inférieure à trois mois pour ses sauvegardes quotidiennes, elle pourrait en réalité dépenser davantage que si elle avait simplement conservé les snapshots EBS. Si l'on ajoute les coûts de licence évoqués plus tôt, la facture devient encore plus élevée.

De plus, comme les snapshots EBS sont incrémentiels, il est difficile pour le tiering vers S3 de ne transférer que ce qui est réellement nécessaire. En effet, les snapshots quotidiens (que l'on ne souhaite pas déplacer vers S3) peuvent référencer des blocs plus anciens appartenant à une sauvegarde annuelle déjà transférée vers S3. En raison de cette complexité, il est probable que l'outil de sauvegarde conserve une grande partie de vos données à la fois dans les snapshots EBS et sur S3.

Scripts AWS Backup personnalisés

La direction constate combien les sauvegardes AWS coûtent, en particulier avec un gestionnaire tiers, ce qui la convainc de mobiliser une ressource d'ingénierie partagée afin de développer des scripts de sauvegarde personnalisés capables de répondre aux besoins de l'organisation.

L'entreprise finit par obtenir une solution fonctionnelle, sans frais de licence, et a enfin le sentiment de maîtriser ses politiques de sauvegarde. Cependant, à mesure qu'AWS modifie ses API et que les besoins métier évoluent (comme la nécessité d'effectuer des sauvegardes entre régions ou de protéger les sauvegardes contre les ransomwares), les scripts doivent également évoluer. La ressource d'ingénierie initialement partagée devient alors un poste à plein temps. L'entreprise se retrouve avec un coût, loin d'être caché, pour gérer, affiner et créer ces scripts de sauvegarde personnalisés.

03

L’approche de Commvault pour la protection des données AWS

Face à tous les défis évoqués dans la section précédente — temps de récupération longs, absence de véritable air gap, manque de visibilité, coûts croissants — il est facile de conclure qu’une protection efficace des données dans AWS est presque impossible. Pourtant, les avantages qu’offre AWS pour une entreprise engagée dans sa transformation cloud sont trop importants pour être ignorés.

Il devient de plus en plus essentiel que les organisations trouvent et mettent en place la bonne solution de protection des données afin de tirer pleinement parti des bénéfices d’AWS. Pour y parvenir, elles doivent adopter une solution qui réponde à chacun des défis majeurs posés par AWS Backup aujourd’hui.

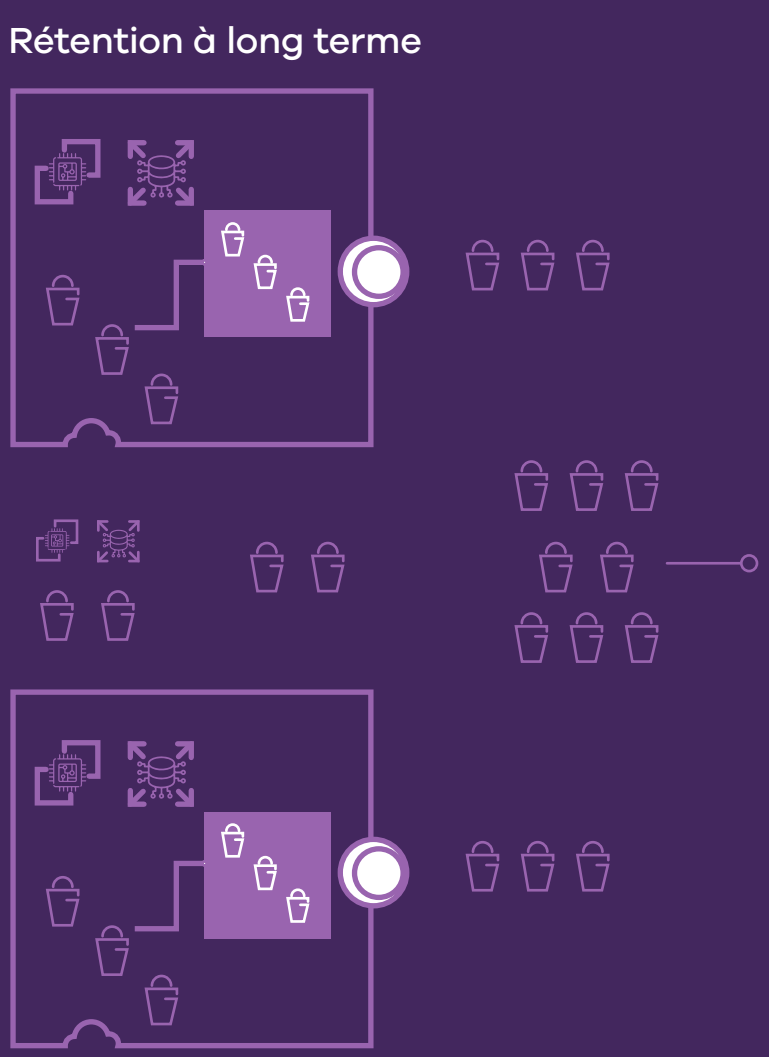
Les organisations doivent se tourner vers Clumio. Nous avons étudié en profondeur les limites d’AWS Backup et conçu une solution qui s’appuie sur les snapshots natifs tout en répondant à ces défis. Voyons comment cela fonctionne.

Sécurité de premier ordre

Pour garantir que les sauvegardes soient valides et utilisables lors d'un processus de restauration lorsque les données primaires sont compromises, il est nécessaire que ces sauvegardes soient stockées en dehors du périmètre de sécurité des données primaires. C'est ce que l'on appelle des sauvegardes avec air gap. Grâce à cet isolement, les pirates ou acteurs malveillants ne peuvent pas accéder aux sauvegardes, ce qui permet une restauration réussie en cas de compromission de compte. Compte tenu de l'augmentation des attaques par ransomware, combinée à la surface d'attaque vaste et décentralisée du cloud, les organisations doivent accorder une attention particulière à la posture de sécurité de leur solution de protection des données cloud.

La solution doit offrir :

- Sauvegardes avec air gap
- Sauvegardes immuables, afin que les copies de sauvegarde ne puissent pas être modifiées même si des acteurs malveillants y accèdent d'une manière ou d'une autre
- Absence d'option de suppression pour les données de sauvegarde, ce qui, combiné à l'immutabilité, garantit une sécurité renforcée
- Chiffrement de bout en bout des données utilisateur, en transit et au repos



Air gap + rétention à long terme
Protection contre les ransomwares et les acteurs malveillants

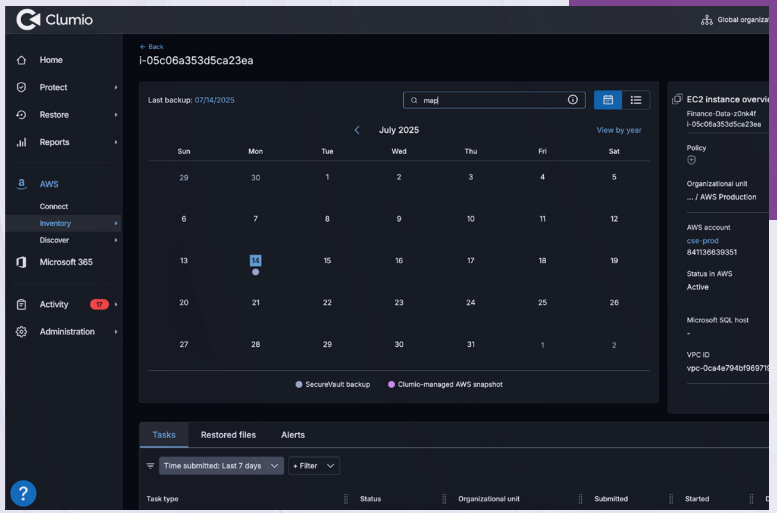
Sauvegardes immuables

Aucun bouton de suppression

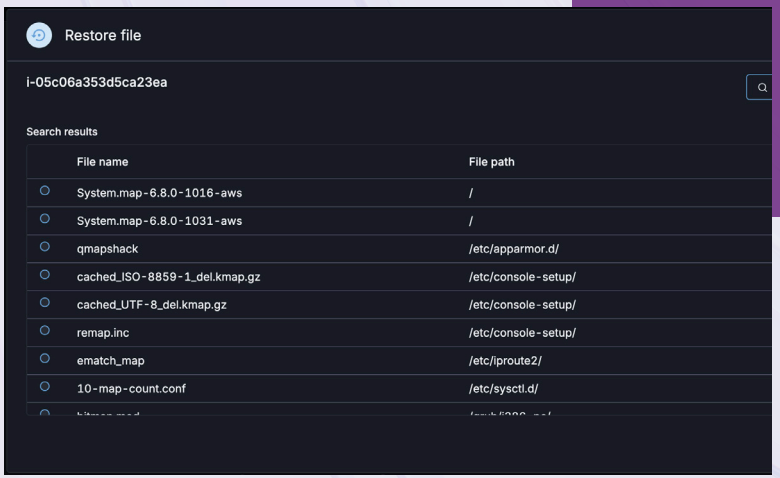
Gestion du cycle de vie permettant des économies

Restauration rapide

Lorsqu'il est nécessaire de récupérer des données après une défaillance, cela doit pouvoir se faire rapidement afin de maintenir la continuité des activités. La bonne solution de protection des données doit permettre de trouver rapidement les éléments à restaurer (snapshots, instances, fichiers, enregistrements, etc.) puis de les restaurer. Voici comment Clumio permet une restauration rapide des fichiers dans Amazon EC2.



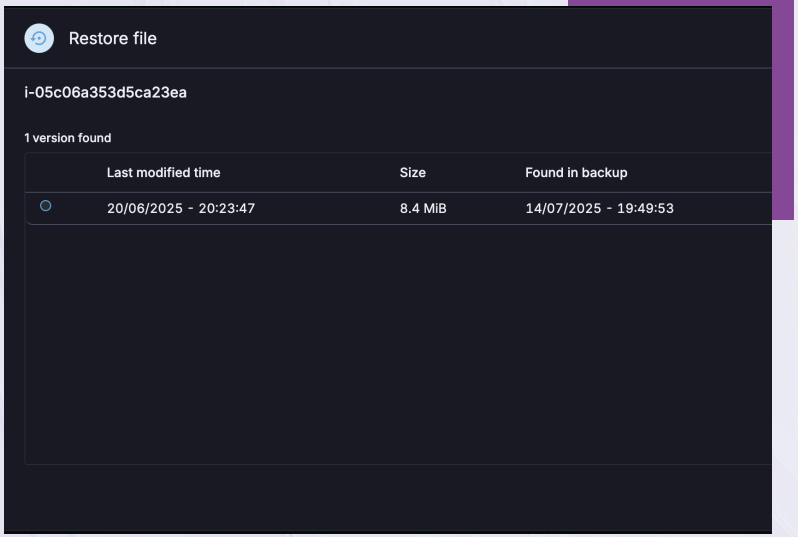
Étape 1: Saisir un terme de recherche pour le fichier à récupérer



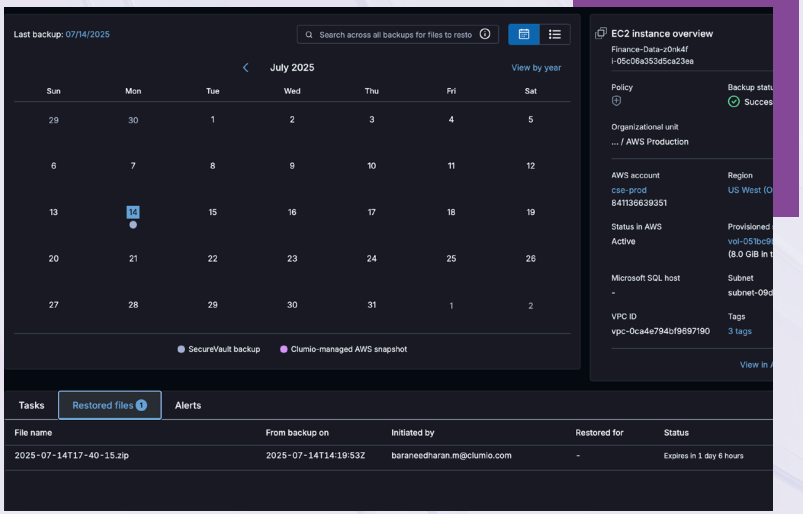
Étape 2: Sélectionner le fichier à restaurer

Contrairement au manque de visibilité du processus AWS Backup, la vue calendaire de Clumio permet à une organisation de parcourir efficacement l'ensemble du système de fichiers. Au lieu de devoir charger ou restaurer un fichier pour vérifier qu'il s'agit du bon, l'organisation peut identifier le fichier nécessaire simplement en saisissant quelques paramètres puis en lançant une recherche. L'utilisateur voit alors toutes les versions enregistrées, avec leurs horodatages, et peut facilement identifier et restaurer le ou les fichiers souhaités. Clumio réduit ainsi considérablement le temps de récupération en permettant à l'organisation de rechercher dans l'intégralité de son « entrepôt » de fichiers sans avoir à ouvrir chaque « boîte ».

Un processus de restauration rapide aussi simple d'utilisation a permis aux clients de Clumio de réduire leur temps moyen de récupération de plus de 4 heures à seulement 10 minutes.



Étape 3: Choisir la version à télécharger

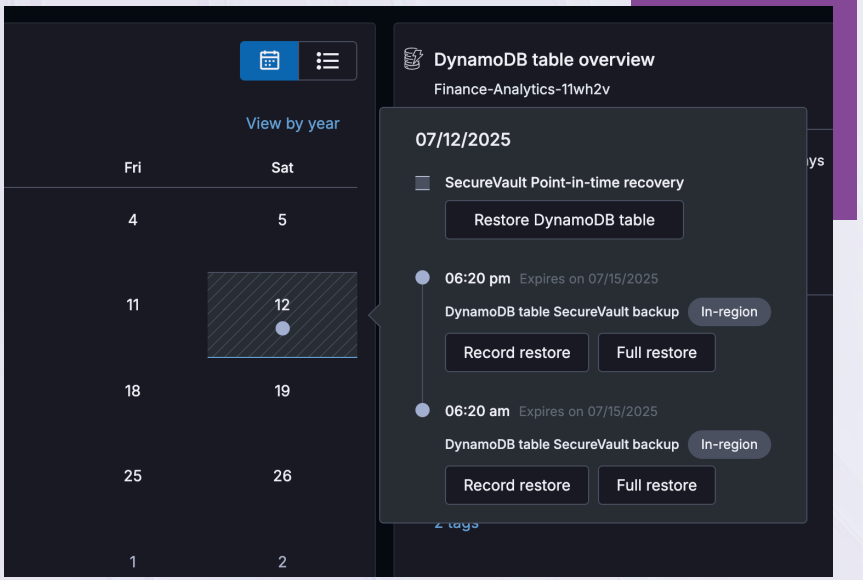


C'est fait ! Téléchargez le fichier.

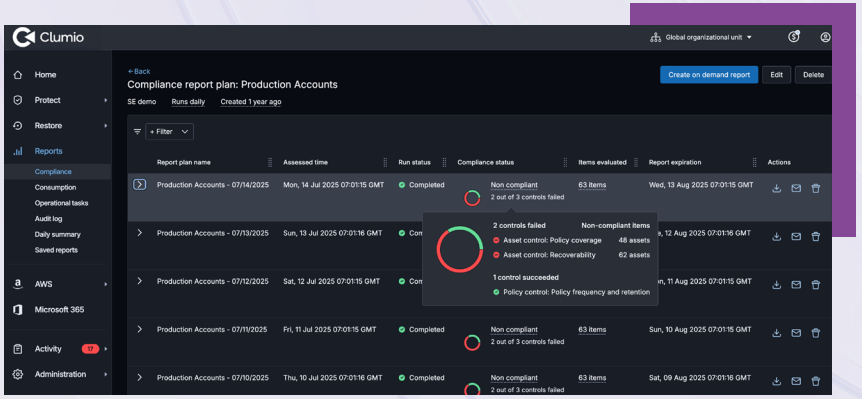
Meilleure visibilité

Une bonne solution de protection des données doit être capable de fournir les informations nécessaires sur les ressources protégées de manière simple et compréhensible. Si l'utilisateur doit créer des rapports et des tableaux de bord personnalisés pour obtenir une vue des ressources protégées, des politiques appliquées, de l'état global des comptes ou encore pour vérifier la conformité, cela augmente le risque d'erreurs et entraîne une consommation continue de ressources précieuses. Ces fonctionnalités devraient au contraire être intégrées directement dans la solution de protection des données.

La vue calendaire de Clumio offre une compréhension globale de tous les snapshots et sauvegardes créés pour une source de données AWS (EC2, EBS, RDS, etc.). Vous pouvez alors effectuer facilement une restauration à un point précis de l'ensemble de la source de données ou visualiser des fichiers ou enregistrements individuels pour effectuer des restaurations sélectives. Le tableau de bord de l'environnement Clumio et le rapport de conformité fournissent un état de conformité en temps réel pour des comptes sélectionnés ou pour l'ensemble de l'environnement. Cela permet à l'équipe de sécurité de rester informée des exigences de gouvernance des données et d'être prête pour les audits lorsque cela est nécessaire.



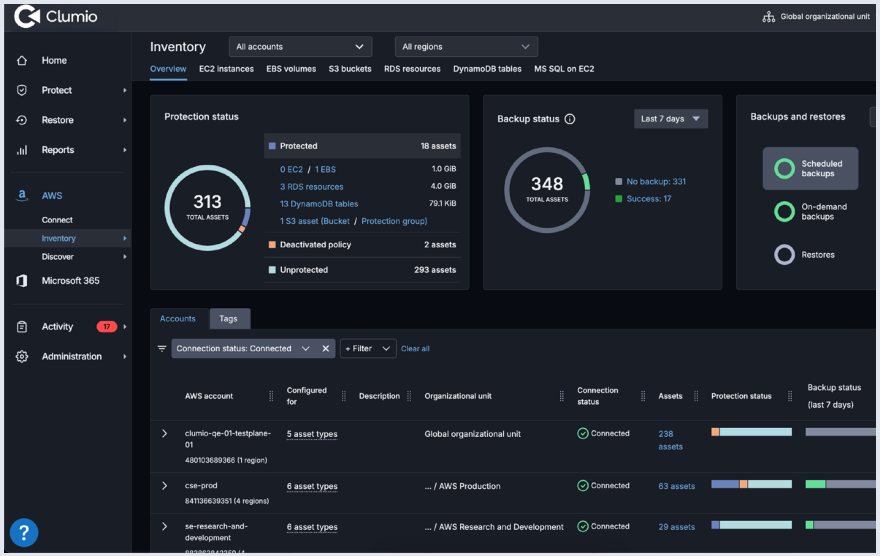
Vue calendaire de l'historique des sauvegardes : Trouver rapidement n'importe quelle sauvegarde pour effectuer une restauration rapide à tout moment.



Rapport global de conformité : Source unique de vérité pour les audits et la conformité.

Gestion simplifiée

Les organisations devraient rechercher des solutions de protection des données cloud qui simplifient et automatisent l'orchestration des sauvegardes. Une telle solution doit permettre une intégration facile, des sauvegardes rapides, la définition de politiques globales et une restauration facilitée.



Avec un service de protection des données SaaS comme Clumio, il faut aussi peu que 10 minutes pour commencer à protéger les sources de données AWS, tout en bénéficiant d'un contrôle précis sur les opérations de sauvegarde et de restauration. Cela simplifie et automatise les tâches quotidiennes des équipes informatiques et opérationnelles, leur permettant de se concentrer sur leur activité principale.

Restauration d'instance

Restaurer une instance entière vers n'importe quel compte

Parcourir et restaurer

Parcourir le système de fichiers pour restaurer le fichier

Enregistrement granulaire

Navigateur de schéma avec récupération d'enregistrements via requête SQL

Recherche globale

Rechercher n'importe quel fichier à travers n'importe quelle instance ou volume

Politiques globales

Simplifier la définition des politiques sur plusieurs comptes

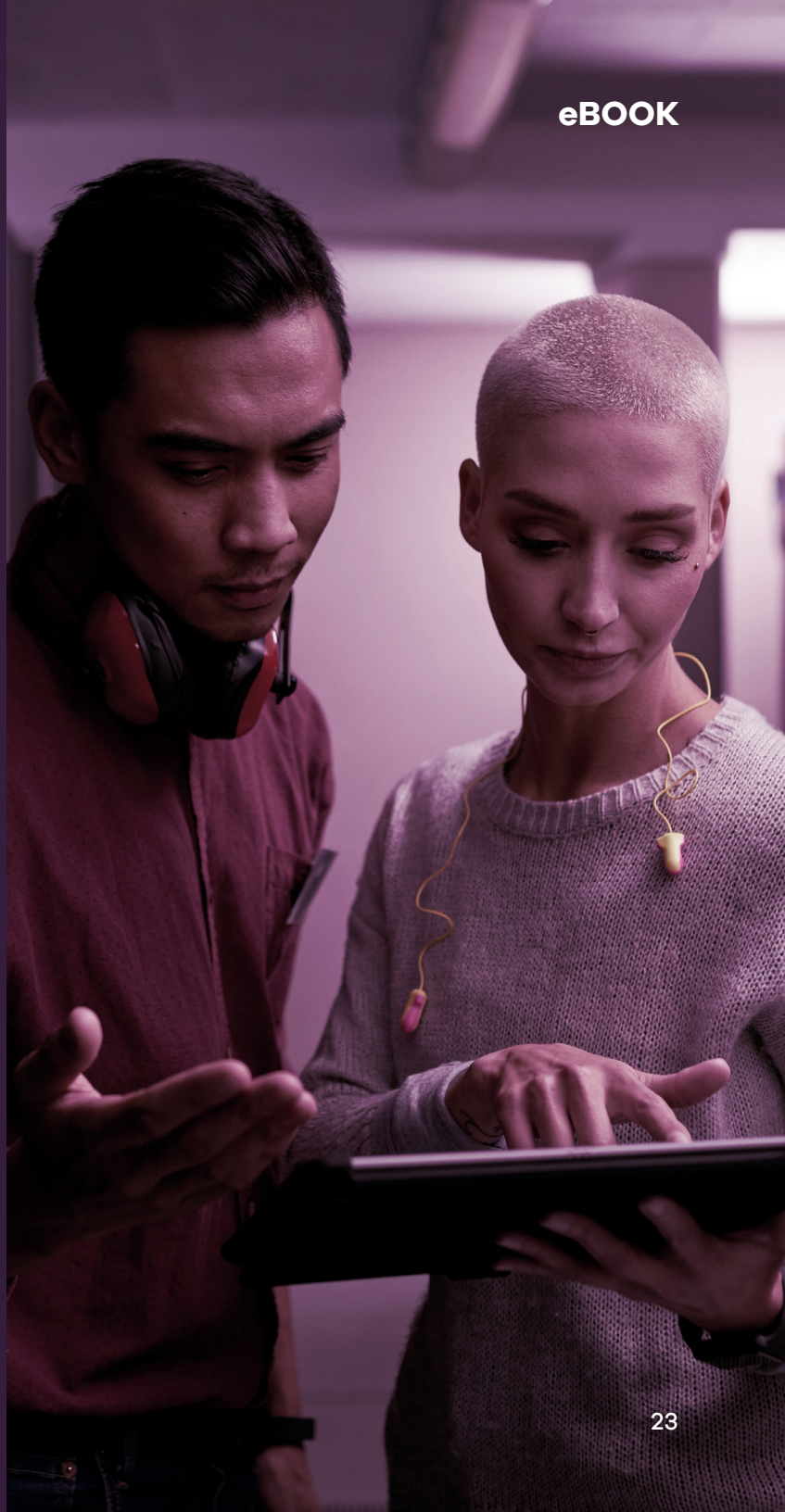
Réduction du TCO

L'un des avantages majeurs de Clumio en matière de coût total de possession réside dans la façon dont il met en œuvre l'air gap. Dans un scénario typique, si une organisation possède pour 100 000 dollars de snapshots dans son compte et souhaite copier ces fichiers vers un compte « air-gappé » (c'est-à-dire sauvegarder une copie dans un compte avec un mot de passe différent), l'investissement total doublerait pour atteindre 200 000 dollars.

Avec Clumio, le processus est automatique et entièrement géré. Il n'existe aucun mécanisme de tiering dont le client doit se préoccuper ; tout est pris en charge automatiquement, et le client paie simplement selon un modèle clair de coût par gigaoctet. En à peine dix minutes, une organisation peut cliquer sur un bouton et sauvegarder ses données dans un environnement air-gappé. L'entreprise n'a pas besoin de créer des scripts, de gérer le processus ou de maintenir des copies miroir de ses snapshots, ce qui permet d'économiser du temps et de réduire les coûts de sauvegarde.

Le graphique de la page suivante montre qu'en utilisant un service de protection des données comme Clumio, qui intègre la protection air gap ainsi qu'une gestion du cycle de vie pour la rétention à long terme, les organisations peuvent éviter des méthodes inefficaces de sauvegarde et réduire en moyenne de 30 % ou plus leurs coûts de sauvegarde AWS. En tenant compte de tous les autres avantages offerts par cette solution, c'est véritablement la cerise sur le gâteau.

De plus, nous aidons nos clients à comprendre ce qui génère leurs coûts de sauvegarde. Et pour ceux qui souhaitent protéger facilement leurs sauvegardes dans un coffre-fort air-gappé sécurisé, ils peuvent transférer leurs snapshots vers Clumio à un coût inférieur à celui des snapshots natifs AWS. Il n'est donc pas surprenant de voir autant de clients migrer rapidement leurs sauvegardes AWS vers Clumio.



LE GUIDE DÉFINITIF DE LA SAUVEGARDE AWS

En passant à Clumio, vous bénéficiez de tous les avantages d'une solution personnalisée sans les coûts permanents liés à son développement et à sa maintenance: aucune licence cachée, une administration plus simple, des coûts inférieurs à ceux des snapshots natifs AWS et de meilleurs rapports.

Clumio

Prêt à simplifier la sauvegarde pour AWS?

Demandez une démonstration personnalisée :

www.clumio.com/demo

commvault.com | 01 73 13 00 23 | talktous@commvault.com

Commvault®