★★★★★

Stockage de sauvegarde hiérarchisé ExaGrid

Les sauvegardes les plus rapides.

Les récupérations les plus rapides.

Une évolutivité inégalée et rentable.

ExaGrid

Retention Time-Lock, la protection contre les ransomwares

Les attaques de ransomwares sont en augmentation, engendrant des perturbations et potentiellement des coûts élevés pour les entreprises. Même si une entreprise suit méticuleusement les bonnes pratiques pour protéger ses précieuses données, les pirates semblent garder une longueur d'avance. Ils chiffrent de manière malveillante les données primaires, prennent le contrôle de l'application de sauvegarde et suppriment les données de sauvegarde.

La protection contre les ransomwares est aujourd'hui une préoccupation majeure des entreprises. ExaGrid propose une approche unique pour garantir que les pirates ne puissent pas compromettre les données de sauvegarde.

Le problème est de savoir comment protéger ses données de sauvegarde contre la suppression tout en permettant la purge de la rétention de sauvegarde lorsque les points de rétention sont atteints. Si vous verrouillez toutes vos données de rétention, vous ne pourrez plus supprimer les points de rétention et vos coûts de stockage deviennent vite incontrolables. Si vous autorisez la suppression de vos points de rétention pour économiser sur le stockage, vous laissez le système ouvert aux pirates et ils peuvent ainsi supprimer toutes vos données.

L'approche unique d'ExaGrid s'appelle Retention Time-Lock. Cette solution empêche les pirates de supprimer les sauvegardes tout en permettant de purger les points de rétention. Le résultat ? Une solution fiable de protection et de récupération des données à un coût de stockage très bas.

ExaGrid est un stockage de sauvegarde hiérarchisé avec une zone de destination de cache disque frontale et une zone de rétention distincte contenant toutes les données de rétention. Les données sont enregistrées directement dans la zone de destination du cache disque ExaGrid « accessible depuis le réseau ». Elles sont ensuite hiérarchisées dans une zone de rétention à long terme « isolée du réseau » où elles sont stockées sous forme d'objets de données dédupliqués pour réduire le coût de stockage des données de rétention à long terme. Comme les données sont hiérarchisées au niveau de rétention, elles sont dédupliquées et stockées dans une série d'objets et de métadonnées. Comme avec d'autres systèmes de stockage d'objets, les objets et les métadonnées ExaGrid ne changent jamais, permettant uniquement la création de nouveaux objets ou la suppression d'anciens lorsque la rétention est atteinte.

L'approche d'ExaGrid vis-à-vis des ransomwares permet aux entreprises de définir une période de verrouillage qui régit le traitement de toutes les demandes de suppression dans la zone de rétention, cette zone est isolée du réseau donc inaccessible aux pirates. La combinaison d'une zone inaccessible depuis le réseau, d'une suppression différée sur une période donnée et d'objets qui ne changent jamais garantissent la solution ExaGrid Retention Time-Lock. Par exemple, si la période de verrouillage pour le niveau de rétention est définie sur 10 jours, si des demandes de suppression sont envoyées à ExaGrid à partir d'une application de sauvegarde qui a été compromise ou d'un CIFS piraté ou d'autres protocoles de communication, les données dans le niveau sont verrouillées contre toute suppression jusqu'à 10 jours. Les données de la zone de destination seront supprimées ou cryptées, cependant, les données du niveau de rétention ne sont pas supprimées sur demande externe pour la période configurée. Lorsqu'une attaque de ransomware est identifiée, il suffit de mettre le système ExaGrid dans un nouveau mode de récupération, puis de restaurer toutes les données de sauvegarde sur le stockage principal. La période de verrouillage est distincte et s'ajoute aux jours, à la semaine, aux mois et à l'année ou à la rétention définis par l'application de sauvegarde et stockés par ExaGrid dans le référentiel de rétention.

La solution fournit un verrou de rétention, mais uniquement pour une période de temps réglable dans la mesure où elle retarde les suppressions. ExaGrid a choisi de ne pas implémenter Retention Time-Lock de manière illimitée car le coût du stockage en deviendrait ingérable. ExaGrid permet déjà la rétention de sauvegarde à long terme, il serait donc redondant d'avoir une solution de stockage séparée avec un verrou de rétention. Avec l'approche de suppression différée d'ExaGrid, il ne faut que jusqu'à 6 % de stockage supplémentaire dans le référentiel pour contenir le délai de suppression. ExaGrid permet le retard des suppressions de 1 à 30 jours.

Processus de récupération - 5 étapes faciles

- Appeler le mode de récupération.
    - L'horloge Time-Lock de rétention est arrêtée et toutes les suppressions sont mises en attente indéfiniment jusqu'à ce que l'opération de récupération des données soit terminée.
- Contacter l'ingénieur dédié du support client ExaGrid de niveau 2.
    - L'administrateur de sauvegarde peut effectuer la restauration à l'aide de l'interface graphique d'ExaGrid, mais comme il ne s'agit pas d'une opération courante, nous vous suggérons de contacter le support client d'ExaGrid.
- Déterminer l'heure de l'événement afin de pouvoir planifier la restauration.
- Déterminer quelle sauvegarde sur ExaGrid a réalisé la déduplication avant l'événement.
- Effectuer la restauration à partir de cette sauvegarde à l'aide de l'application de sauvegarde.

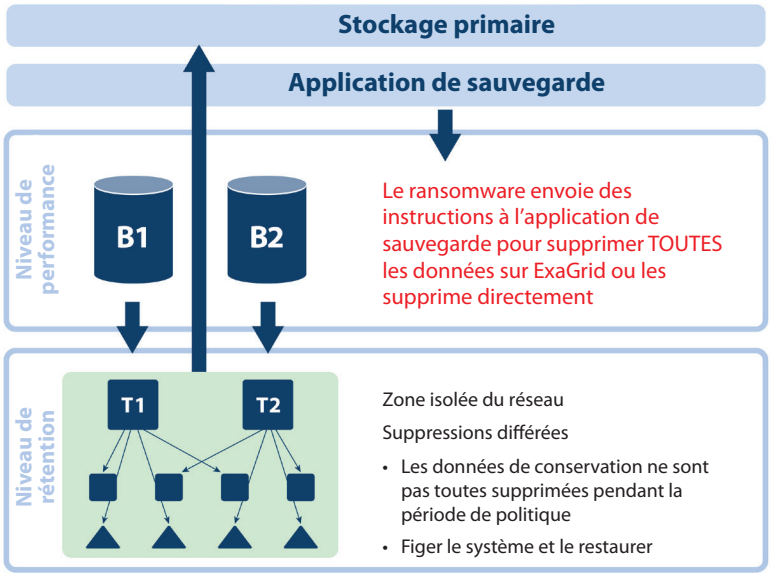
Les avantages d'ExaGrid sont :

- Gestion d'un seul système pour le stockage de sauvegarde et la récupération des ransomwares
- Deuxième zone de rétention unique visible uniquement par le logiciel ExaGrid et non par le réseau
- Les données ne sont pas supprimées, les demandes de suppression étant retardées et donc prêtes à être récupérées après une attaque de ransomware
- Des purges hebdomadaires, mensuelles, annuelles et autres peuvent se poursuivre pour contenir les coûts de stockage grâce aux périodes de conservation
- Ne nécessite pas plus de 6 % de stockage de référentiel supplémentaires
- Le stockage ne se développe pas indéfiniment et reste contenu dans la période de rétention des sauvegardes définie pour réduire les coûts de stockage
- Les données de rétention sont toutes conservées et ne sont pas supprimées

Exemples de scénarios

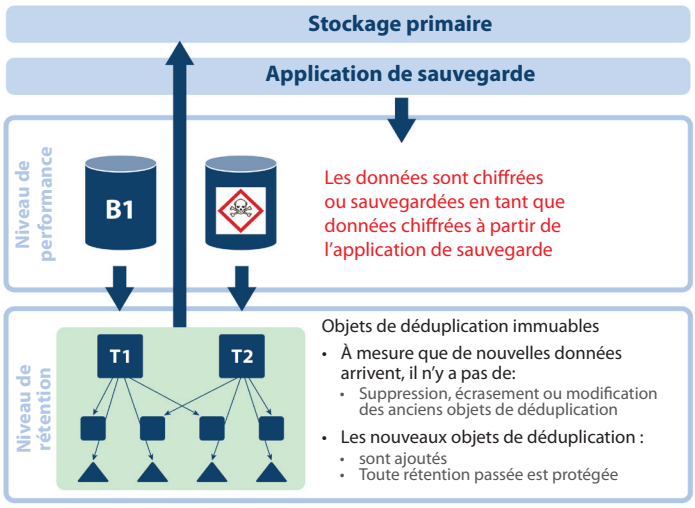
- Les données sont supprimées dans la zone de destination du cache disque ExaGrid via l'application de sauvegarde ou par un piratage du protocole de communication. Étant donné que les données de la zone de rétention ont une période de verrouillage de suppression différée, les objets restent intacts et disponibles pour la restauration. Lorsque l'événement de ransomware est détecté, il suffit de mettre l'ExaGrid dans un nouveau mode de récupération et de restauration. Le temps pour détecter l'attaque du ransomware correspond alors à la période de verrouillage telle que définie sur l'ExaGrid. Si le verrouillage est réglé sur 10 jours, vous avez 10 jours pour détecter l'attaque du ransomware et mettre le système ExaGrid dans le nouveau mode de récupération pour restaurer vos données.

Protection contre la suppression des données de sauvegarde sur ExaGrid



- Les données sont cryptées dans la zone de destination du cache disque ExaGrid ou sont cryptées sur le stockage principal et sauvegardées sur ExaGrid afin qu'ExaGrid puisse chiffrer les données dans la zone de destination et les déduplique dans la zone de rétention. Les données de la zone de destination sont chiffrées. Cependant, tous les objets de données précédemment dédupliqués ne changent pas (ils sont immuables), ils ne sont donc jamais affectés par les données chiffrées nouvellement arrivées. ExaGrid conserve toutes les sauvegardes précédentes avant l'attaque du ransomware et peut les restaurer immédiatement. En plus de pouvoir récupérer à partir de la sauvegarde dédupliquée la plus récente, le système conserve toutes les données de sauvegarde conformément aux exigences de rétention.

Protection contre la suppression des données de sauvegarde sur ExaGrid



Caractéristiques :

- Toutes les demandes de suppression sont retardées du nombre de jours de la politique de protection.
- Les données chiffrées écrites sur ExaGrid ne suppriment ni ne modifient aucune des sauvegardes précédentes dans le référentiel.
- Les données chiffrées de la zone de destination ne suppriment ni ne modifient les sauvegardes précédentes dans le référentiel.
- La suppression différée peut être définie par incréments de 1 à 30 jours.
- Protection contre la perte de toutes les sauvegardes conservées, y compris mensuelles et annuelles.
- L'authentification à deux facteurs (2FA) protège les modifications apportées au paramètre Time-Lock.
  - Seul le responsable de la sécurité est autorisé à approuver les modifications du paramètre Time-Lock.
  - Un système 2FA avec login et mot de passe et code QR généré par le système protège tous les comptes.
- Mot de passe distinct pour le site principal et le deuxième site ExaGrid.

États-Unis 350, Campus Drive/ Marlborough, MA 01752 / (800) 868-6985
Royaume-Uni 200 Brook Drive / Green Park, Reading, Berkshire RG2 6UB / +44 (0) 1189497051
Singapour 1 Raffles Place, # 20-61 / One Raffles Place Tower 2/048616 / +65 6808 5574

exagrid.com