eBOOK

PROTECTION DES

Joyaux de la Couronne

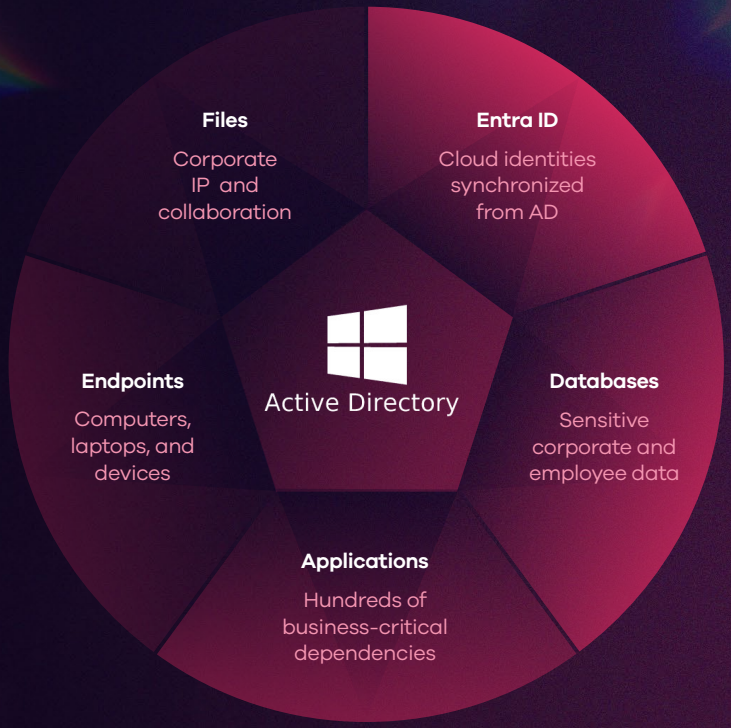
Sécuriser **Active Directory** Contre les Menaces Cyber

Commvault®

L'Importance d'Active Directory

Microsoft Active Directory (AD) et Entra ID sont les bijoux de la couronne de la gestion des identités et des accès dans les entreprises, authentifiant des millions d'utilisateurs à l'échelle mondiale et contrôlant l'accès aux systèmes d'affaires critiques. Que ce soit pour les connexions aux postes de travail ou l'accès physique aux bâtiments, AD permet le fonctionnement fluide de votre organisation.

Si les données AD sont corrompues ou si l'annuaire lui-même est indisponible, cela peut gravement perturber les applications et processus métier, bloquant l'accès des utilisateurs aux systèmes et ressources essentiels.



Sans AD, les opérations commerciales s'arrêtent.

Le personnel bancaire ne peut plus accéder aux comptes clients.

Les médecins et les infirmières ne peuvent plus accéder aux dossiers médicaux.

Les développeurs ne peuvent plus publier du code.

Les gestionnaires ne peuvent plus envoyer des e-mails.

Les équipes ne peuvent plus collaborer ou discuter.

L'Importance et la Complexité d'Active Directory en Font une Cible de Premier Choix pour les Attaquants

Étant donné que AD et la gestion des identités sont des composantes cruciales des opérations commerciales, ils représentent une cible très attractive pour les attaquants cherchant des systèmes de valeur à rançonner. Pour ceux qui souhaitent simplement semer le chaos, AD est l'un des systèmes qui peut paralyser tous les autres et dévaster l'entreprise.

AD est le centre de l'authentification sécurisée et des services, et il est crucial de maintenir sa sécurité et sa récupérabilité, en se préparant aux diverses catastrophes qui pourraient l'affecter.

AD soit impliqué dans environ

9/10

attaques[1]

Étant donné son importance, il n'est pas surprenant

Le rapport Microsoft Digital Defense indique que

88%

des clients

touchés par des incidents de sécurité avaient une configuration AD non sécurisée, ce qui en fait un actif de haute valeur que les acteurs malveillants sont impatients d'exploiter.[2]

Pour les attaquants, AD est un point d'entrée unique pour élever leurs privilèges et voler, corrompre ou refuser l'accès aux applications et données critiques.

Un rapport récent d'IBM met en lumière une augmentation de **100%** des attaques par "kerberoasting",

Toù les attaquants tentent d'obtenir des privilèges élevés en abusant de Microsoft AD.[3]

1 Researchers Explore Active Directory Attack Vectors
2 Microsoft Digital Defense Report 2022
3 IBM Report: Identity Comes Under Attack Straining Enterprises' Recovery Time from Breaches

Récupération d'AD : La Base de la Continuité du Business"

L'importance de prioriser la récupération d'AD est évidente lorsque l'on considère son effet en cascade sur les autres charges de travail. Les applications, les systèmes de fichiers, les services de messagerie et les bases de données dépendent toutes d'AD pour une authentification correcte et l'accès des utilisateurs.

Lorsque AD est endommagé ou complètement hors ligne, les applications et services critiques deviennent inaccessibles.

Comme presque tout dans les entreprises modernes repose sur l'identité, la restauration d'AD avant les autres charges de travail est une priorité critique.

En restaurant AD en premier, les organisations peuvent rétablir le contrôle sur leurs réseaux et systèmes, vérifier que les politiques de sécurité des données et d'accès sont appliquées, et fournir une base stable pour la récupération des autres systèmes et services.

La Nécessité d'une Récupération Granulaire

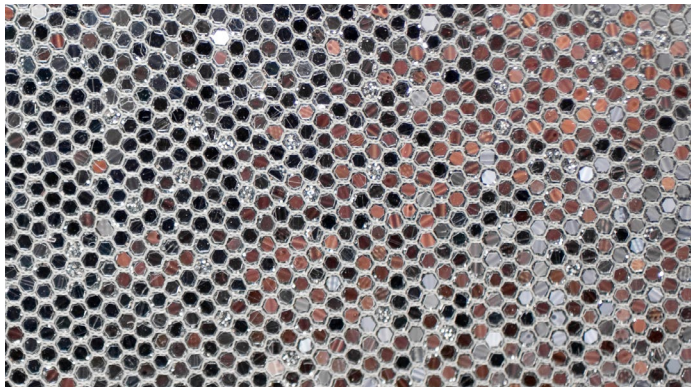
L'un des aspects les plus critiques de la protection d'AD est la capacité de restaurer rapidement les données perdues ou corrompues. Lorsque des données importantes dans AD sont supprimées, modifiées ou corrompues par accident ou de manière malveillante, il est essentiel de pouvoir rapidement identifier ces modifications et restaurer et récupérer des objets et attributs individuels.

Bien que le Corbeille d'AD puisse temporairement récupérer des objets supprimés, s'y fier est risqué. Le Corbeille ne conserve les objets supprimés qu'un temps limité avant de les supprimer définitivement. Elle ne permet pas de revenir en arrière sur des modifications au niveau des attributs ou de rétablir des modifications apportées aux Objets de Stratégie de Groupe (GPO) ou aux configurations AD.

Parfois, les catastrophes ne entraînent pas la suppression d'objets, mais plutôt l'écrasement des données d'attributs sur plusieurs objets. Par exemple, un script PowerShell mal conçu pourrait provoquer des modifications inattendues dans l'annuaire. Lorsque cela se produit, il est nécessaire de pouvoir localiser et annuler des attributs spécifiques sur plusieurs objets au sein d'AD. Cependant, le Corbeille ne peut pas annuler des modifications au niveau des attributs ou rétablir des modifications apportées aux GPO ou aux configurations AD.

Pour une protection complète, il est préférable d'avoir une sauvegarde complète et fréquente de l'ensemble d'AD.

Une solution dédiée de protection des données permet une récupération granulaire, en restaurant uniquement l'attribut d'objet manquant, endommagé ou mal configuré. Cette granularité peut rapidement remettre en ligne les systèmes d'affaires ou les utilisateurs sans nécessiter une restauration complète de l'environnement AD.



Avez-vous un Plan de Récupération ?

Lorsqu'un ransomware verrouille et met hors ligne les serveurs hébergeant votre AD, vous devez avoir la capacité de récupérer l'environnement AD. Cela implique de reconstruire le service d'annuaire, y compris les domaines, les contrôleurs de domaine et les données associées, à un état pré-attaque.

L'impact d'une attaque AD qui désactive les contrôleurs de domaine est réel et peut être dévastateur. Les systèmes critiques cessent de fonctionner. Les employés ne peuvent plus se connecter. Les politiques de sécurité basées sur l'identité ne peuvent pas être appliquées.

« Si nous ne pouvons pas récupérer nos contrôleurs de domaine, nous ne pouvons rien récupérer »

ADMINISTRATEUR IT, MAERSK

Face à de telles menaces, disposer d'un plan de récupération bien documenté et fréquemment testé pour reconstruire et restaurer votre environnement AD à un état précédent et sain pré-attaque est crucial et la clé pour reprendre rapidement vos activités.

Attaque par Ransomware

En 2017, le géant mondial du transport maritime Maersk a été victime de l'attaque cyber NotPetya, qui a chiffré les systèmes de fichiers de

45K PCs

4K servers

149/150 contrôleurs de domaine AD

Avec AD complètement hors ligne, les opérations se sont arrêtées instantanément, fermant

17 ports de transport maritime à l'échelle mondiale et laissant des

100s de navires conteneurs à l'arrêt pendant 10 jours.

Au total, l'attaque a coûté à l'entreprise au moins

$300M[4]

4 The Untold Story of NotPetya, the Most Devastating Cyberattack in History

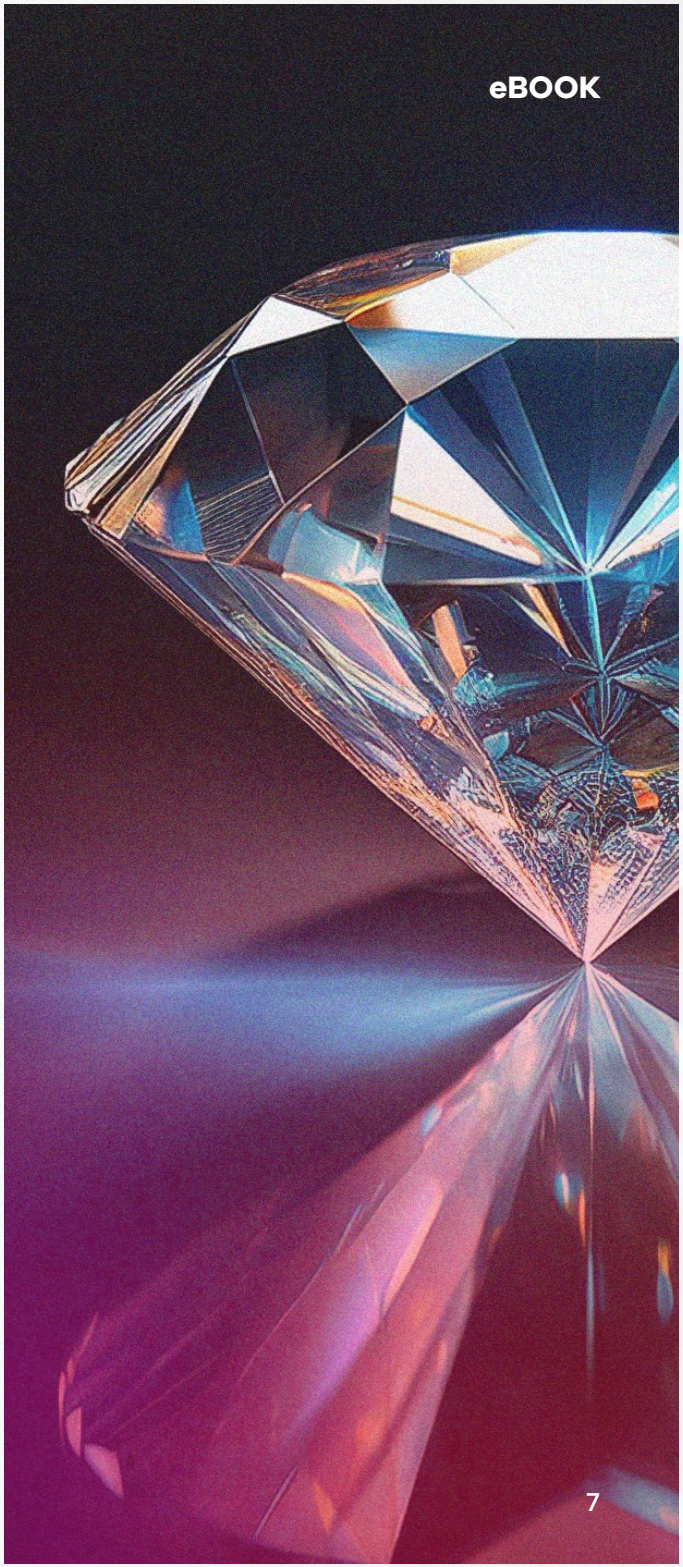
Récupération d'Active Directory : Une Entreprise Complex

Les forêts AD sont des environnements complexes avec plusieurs domaines, plusieurs contrôleurs de domaine pour chacun de ces domaines, et une hiérarchie complète d'utilisateurs, d'ordinateurs et de paramètres d'accès et de sécurité. En cas d'attaque cyber, il ne suffit pas de restaurer simplement un seul contrôleur de domaine à partir d'une sauvegarde. Le processus de récupération et de reconstruction de l'environnement est extrêmement délicat et nécessite une coordination méticuleuse. Chaque contrôleur de domaine doit être synchronisé et restauré avec soin pour éviter les incohérences de données et les éventuelles corruptions.

Le Guide de Récupération de la Forêt AD de Microsoft fournit une méthode détaillée et étape par étape pour cela, qui peut impliquer entre 50 et 100 étapes ou plus, en fonction de la taille de votre organisation.

Le processus de récupération est manuel, chronophage et complexe – souvent nécessitant plusieurs jours, voire plusieurs semaines pour être achevé. Pendant ce temps, les opérations commerciales cessent de fonctionner et les utilisateurs ne peuvent pas accéder aux applications importantes.

Sans automatiser et orchestrer le processus, vous risquez de restaurer AD dans un état inutilisable, ce qui pourrait encore plus perturber l'activité et prolonger l'interruption de service.



Commvault Rend votre Active Directory Résilient

Commvault Cloud Backup & Recovery for Active Directory vous permet de protéger et d'accélérer la récupération des données AD en cas de corruption, de suppression accidentelle et d'attaques par ransomware.

Accélérez la récupération AD et reprenez vos activités plus rapidement grâce à :

Récupération forestière automatisée :

Rétablissez rapidement les forêts à un point dans le temps avant une attaque, vous permettant de reprendre vos activités en quelques heures plutôt qu'en quelques jours ou semaines.

Comparaisons interactives :

Identifiez les modifications apportées au domaine, vous permettant de récupérer rapidement les objets supprimés par erreur ou de manière malveillante, ou de revenir en arrière sur des attributs écrasés dans l'annuaire.

Récupération flexible et granulaire :

Rétablissez rapidement uniquement les attributs d'objets manquants, endommagés ou mal configurés, et remettez rapidement en ligne vos systèmes d'affaires ou vos utilisateurs.online quickly.

Support des annuaires hybrides :

Protégez les objets critiques de Microsoft AD et Entra ID, y compris les GPO, les utilisateurs, les groupes, les politiques d'accès conditionnel, les rôles et plus encore.

Tests de récupération AD :

Assurez-vous que les récupérations peuvent être réussies et permettez aux équipes de sécurité et d'IT de s'entraîner en temps normal pour être prêtes en cas de crise.

La Récupération Cyber Va Au-Delà de l'AD

Faire face à une attaque cyber ou à une situation de rançon est une expérience terrifiante.

La restauration d'AD est généralement la première étape, et trouver des moyens d'automatiser un processus autrement chronophage et intensif en ressources peut aider à relancer rapidement le processus de récupération et à rétablir rapidement les activités. C'est encore mieux lorsque votre récupération AD repose sur la même plateforme que le reste de votre récupération cyber.

Unifier le processus de récupération et de reconstruction cyber sur une plateforme commune permet une coordination, une automatisation et une orchestration faciles qui vont au-delà de la simple récupération d'identité – vous pouvez orchestrer la récupération d'applications, de données, de clouds et d'infrastructure. Cela aidera vos équipes à travailler ensemble pour reconstruire vos systèmes après des attaques cyber et des catastrophes, et à renforcer la résilience pour assurer une continuité des activités.

eBOOK

Request a demo and see how you can restore your entire AD forest in just a few clicks to help maintain continuous business.

commvault.com | 888.746.3849 | get-info@commvault.com

Commvault®