

Technologies concernées :

- Sauvegardes
- Infrastructure on-premise
- Applications SaaS (Ex : M365)
- Plateformes de stockage
- Librairies de bandes

Charge estimée : 1-3 Jours

Budget estimé : 2-5 KCHF



Audit sauvegardes Veeam

Introduction

La continuité d'activité des entreprises dépend directement de leur capacité à restaurer rapidement leurs applications ou leurs données en cas d'incident majeur. Les cyberattaques, les erreurs humaines, les pannes matérielles ou les catastrophes naturelles peuvent entraîner une interruption complète des opérations, ainsi que la perte de données vitales à la survie d'une organisation. Dans un scénario de désastre, les sauvegardes représentent généralement la dernière ligne de défense.

De nombreuses organisations pensent être protégées simplement parce qu'une solution de sauvegarde est en place. Pourtant, l'expérience montre qu'en situation de crise, les sauvegardes peuvent être incomplètes, mal configurées ou impossibles à restaurer dans les délais attendus.

Notre offre d'audit dédiée aux sauvegardes se concentre actuellement sur Veeam Data Platform pour la protection des infrastructures on-premise et/ou Veeam Backup for M365 pour les

applications SaaS de Microsoft (Ex : Teams, OneDrive, Sharepoint Online, Exchange Online).

Cette prestation vous permet d'obtenir rapidement une vision claire et objective de l'efficacité réelle de votre architecture et de vos stratégies de sauvegarde, et d'identifier les améliorations nécessaires pour garantir la protection de vos données.

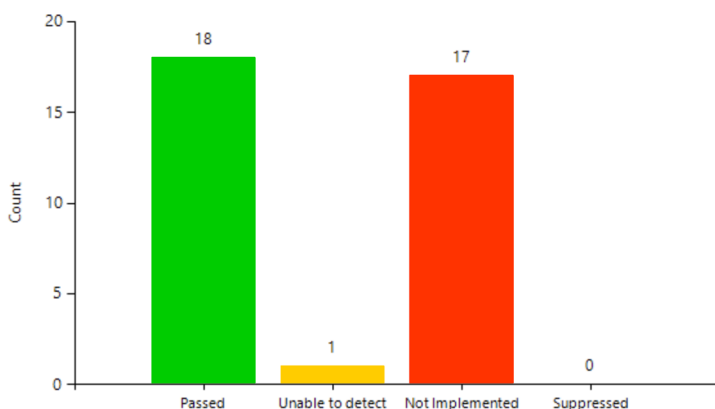
Périmètre de la prestation

Une solution de sauvegarde telle que Veeam offre de nombreuses fonctionnalités avancées, souvent méconnues des clients et même de nombreux prestataires. Cependant, son efficacité dépend fortement de la qualité de son architecture et de sa configuration.

Un audit permet notamment de vérifier que toutes les données critiques sont correctement protégées, garantir que les sauvegardes sont réellement restaurables, identifier les failles de sécurité exploitables par un ransomware, optimiser les performances et les ressources, aligner la stratégie de sauvegarde avec les objectifs de reprise d'activité de l'organisation (RPO / RTO).

En résumé, l'audit transforme vos sauvegardes en une véritable assurance opérationnelle pour votre entreprise.

Best Practices



Prérequis du mandat

Ce mandat nécessite la pleine collaboration des équipes du client durant tout le déroulement de la prestation.

Les équipes de CloudEdge doivent pouvoir disposer d'un accès à distance durant la phase d'audit, l'autorisation d'exécuter un ou plusieurs scripts d'audit depuis le(s) serveur(s) de backup, et de disposer de droits suffisants pour pouvoir exécuter les différents prélèvements d'informations techniques.

Déroulement de la prestation

La prestation d'audit des sauvegardes se concentre en premier lieu sur l'architecture de l'environnement de backup Veeam, et plus particulièrement la configuration du backup server, des proxies, des repositories, les intégrations avec des environnements de virtualisation ou des plateformes de stockage (NAS/SAN/HCI), ou avec certaines applications métier (Ex : SQL, Oracle, SAP, etc.). Cette analyse permet d'identifier les points de faiblesse et les écarts avec les bonnes pratiques de l'éditeur.

La seconde étape du mandat consiste à analyser les stratégies de sauvegarde (Ex : jobs, planification, politiques de rétention, configurations avancées pour les restaurations granulaires, etc.). L'objectif est de vérifier que la stratégie mise en place protège réellement les données essentielles de votre organisation.

Le troisième objectif du mandat se concentre sur les capacités de restauration de l'organisation (Ex : cohérence des points de restauration, historique des sauvegardes, procédures de reprise spécifiques, etc.). Suivant la criticité des applications et des systèmes, nous recommandons la mise en oeuvre de tests de restauration automatisés depuis une sandbox.

Le quatrième axe de l'analyse se concentre sur les fonctionnalités de cybersécurité mise en oeuvre au sein de l'environnement (Ex : gestion des identités, droits d'accès, comptes de service, immutabilité, analyse antivirus proactive ou réactive, principes de vaulting). En effet, les infrastructures de sauvegarde sont aujourd'hui les cibles prioritaires des cyberattaques. L'objectif est donc de garantir que votre système de sauvegarde reste opérationnel même en cas de compromission du système d'information.

Bénéfices attendus par le client

Cet audit de votre environnement de sauvegarde vous permet donc de renforcer la sécurité de vos sauvegardes, d'améliorer la rapidité de restauration des systèmes critiques, de réduire les risques liés aux cyberattaques et ransomwares, d'optimiser les performances ou votre stratégie de stockage, et enfin de garantir la continuité de vos activités. Votre infrastructure de sauvegarde devient ainsi un véritable pilier de votre stratégie de résilience numérique.

