OVHcloud VEEAM

WHITE PAPER

Backup-as-a-Service : un incontournable pour la continuité de vos activités

SOMMAIRE

INTRODUCTION

L'activité et la performance des entreprises dépendent directement de la disponibilité de leurs systèmes d'information. Or, ces systèmes sont soumis à **une multitude de risques pouvant affecter leur fonctionnement :** pannes, dysfonctionnements, manipulations malencontreuses, sinistres, cyberattaques.... Ces incidents peuvent entraîner de très fortes perturbations, voire l'arrêt complet des activités pour une durée indéterminée.

Pour protéger vos activités de ce type de risque, **une stratégie de sauvegarde de vos données est indispensable**. Ces backups vous permettront de récupérer des données saines. Cette capacité à restaurer des données est essentielle pour pouvoir reprendre votre activité au plus vite.

La sauvegarde (ou backup) consiste à copier les données d'un système d'information sur autre support, de manière à pouvoir les restaurer en cas de défaillance ou d'indisponibilité.

Le recours à des architectures hybrides, avec une part croissante d'hébergement cloud, implique une bonne compréhension des responsabilités entre entreprise cliente et hébergeurs quant à la sécurisation des données. Les responsabilités de chacun peuvent varier selon la nature de la prestation d'hébergement souscrite. Elles sont précisées dans le contrat passé avec votre hébergeur.

Dans la grande majorité des cas, vous êtes responsable de vos données résidentes dans le cloud, au même titre que celles que vous conservez sur vos infrastructures (on-premise). Il vous revient donc de mettre en place des mesures adaptées pour assurer leur sauvegarde et leur récupération.

Dans cet eBook, nous revenons sur l'importance des sauvegardes et vous présentons **des solutions concrètes, adaptées à un éventail de situations**, pour contribuer à protéger vos données et vos activités.

Dans quels cas les sauvegardes sont-elles utiles ?

- Suppression accidentelle, mauvaise manipulation sur les données
- Échec d'une montée de version (OS ou applicatif)
- Sécurisation des déploiements hybrides et des migrations
- Menaces internes : utilisateur malveillant, salariés quittant l'entreprise…
- Menaces externes : Ransomware / Applications malveillantes
- Indisponibilité fortuite de systèmes et de réseaux
- Obligations légales de conservation et exigences de conformité (archivage).

Les menaces qui pèsent sur les données d'entreprise sont multiples et toujours imprévisibles, mais ces dernières années, ce sont souvent des cyberattaques (ransomwares, malwares…) qui ont été recensées auprès des entreprises.
Le ransomware est d'ailleurs toujours le risque majeur.

Des entreprises ont connu au moins une attaque ransomware durant l'année passée*

Des entreprises ont été capable de restaurer sans payer de rançon**

Des entreprises ont payé une rançon mais n'ont jamais récupéré leurs données*

*2023 Veeam Data Protection Report
**2022 Veeam Ransomware Trends Report

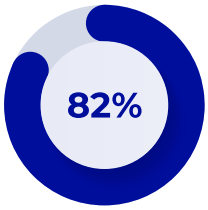
1 SAUVEGARDE DE DONNÉES : ADOPTEZ LES BONS RÉFLEXES !

La sauvegarde de vos données répond à un enjeu de restauration à partir d'une source fiable et intègre. Elle vous aide à redémarrer en cas de perte, de compromission ou d'incident affectant une des versions de vos données. Les modalités de ce redémarrage sont à inscrire dans le cadre plus général de votre Plan de reprise d'activité (PRA). Quelle que soit votre situation, il est recommandé de suivre un certain nombre de bonnes pratiques pour garantir la pertinence et la sécurité de vos sauvegardes.

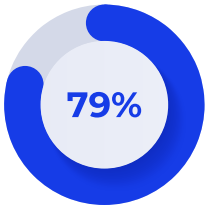
Révisez vos fondamentaux

La plupart des entreprises s'estiment parées à toute perte de données grâce à leurs sauvegardes mises en place, mais la réalité est parfois surprenante.

Le Veeam Data Protection Report 2023 révèle quelques chiffres qui interrogent :



82 % des entreprises souffrent d'un "écart de disponibilité" entre la vitesse à laquelle elles peuvent restaurer leurs applications et celle à laquelle elles devraient le faire.



79 % constatent un "écart de protection" entre la fréquence de sauvegarde de leurs données et ce qu'elles peuvent se permettre de perdre après une panne.

En outre, **58 % des restaurations échouent**, ce qui laisse les données des entreprises sans protection et ne permet pas une récupération en cas de cyberattaque.

Dans un contexte de cybermenaces omniprésentes et de dépendance accrue entre le business et les moyens de production informatiques, il est important de **respecter les fondamentaux en matière de sauvegardes des données**.

La règle historique “3-2-1” (3 copies distinctes des données / 2 supports différents pour chaque jeu de copies / 1 site distant entre chaque jeu de copies) continue de s’appliquer ! L’évolution de la menace a conduit à la compléter en ajoutant :

- 1 jeu de copies hors-ligne ou immuable
- 0 erreur lors des tests de restauration et reprise des données

Protection des données : la règle des sauvegardes 3-2-1 étendue

Trois copies distinctes des données

Deux supports différents

Une copie hors site

Une copie hors ligne (air gap) ou immuable

Zéro erreur lors des tests de backups automatisés et de restauration

Nous vous conseillons donc de prendre le temps de **faire un état des lieux de votre stratégie de récupération des données** pour identifier les potentiels axes d’amélioration ou manquements.

Définissez un plan de sauvegarde selon votre activité

Selon une **recommandation de l'ANSSI** (Agence nationale de la sécurité des systèmes d'information), les entreprises doivent évaluer leurs besoins (type de sauvegardes, fréquence, espace de stockage, etc.), **en tenant compte de leurs impératifs Business**.

Voici quelques points essentiels à aborder dans l'optique d'un plan de sauvegarde pertinent.

- Quelles sont les données et bases de données critiques/sensibles ?
- Quelles applications sont indispensables pour assurer la continuité de l'activité ?
- Quelles sont les interdépendances entre les applications ?
- Quelle est l'interruption d'activité maximale "tolérable" (Recovery Time Objective) ?
- Quelle quantité de données vous autorisez-vous à perdre (Recovery Point Objective) ?
- Quelles sont les fréquences de sauvegarde et durées de rétention nécessaires pour atteindre ces objectifs ?
- Quels sites distants "de secours" sont disponibles ?

Cette évaluation vous aidera à mettre en place une stratégie de sauvegarde et restauration de données efficace pour sécuriser vos activités.

Respectez les contraintes réglementaires et la souveraineté des données

Il est primordial de vous assurer que vos sauvegardes sont stockées **dans le respect des contraintes réglementaires liées à votre activité et de la souveraineté** des données.

Côté réglementation, le RGPD (Règlement Général sur la Protection des Données) définit à l'échelle européenne les règles de conservation des données personnelles ! Au-delà, votre métier vous impose peut-être des conditions spécifiques de traçabilité, d'archivage réglementaire ou de roll-back (devoir rejouer des transactions ou des opérations passées). Cela conditionne vos besoins de sauvegarde.

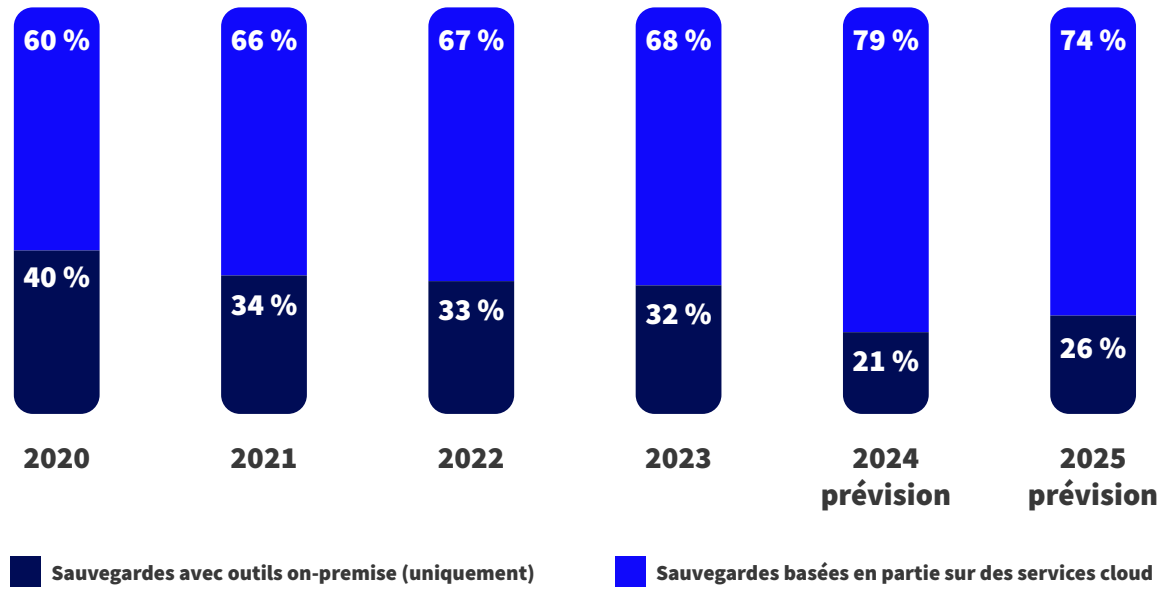
La notion de souveraineté de données garantit que vos données ne sont soumises qu'aux lois du pays dans lequel elles sont stockées. Elle s'applique aussi à vos sauvegardes. Comme pour vos données primaires, il est préférable que vos sauvegardes soient hébergées dans **des centres de données localisés en France**. Vos données restent ainsi soumises au droit français et non exposées à des lois extra-territoriales ou de pays étrangers. Confier vos sauvegardes à un **hébergeur souverain** est donc recommandé.

Pensez “Backup-as-a-Service”

Dans un contexte de sophistication des systèmes d’information et de menace, les entreprises manquent de ressources pour adapter la protection de leurs données. Les offres de **“Backup-as-a-Service”** (BaaS) se développent. Ainsi en 2023, la tendance à **l’externalisation des sauvegardes** chez un hébergeur cloud se confirme.

Selon le Veeam Data Protection Report 2023, 74 % des entreprises envisagent d’utiliser une solution de backup basée sur le cloud en 2025. Elles étaient 67 % à le faire en 2022.

Déléguer la réalisation des sauvegardes à un fournisseur de services cloud est une solution intéressante pour simplifier/automatiser la gestion des backups. Vous bénéficiez ainsi de services spécialisés et d’engagements concrets (SLA, pénalités…).



2 VOTRE STRATÉGIE DE SAUVEGARDE DEMANDE-T-ELLE À ÊTRE PERFECTIONNÉE ?

Quel que soit votre mode d'hébergement actuel (on-premise ou cloud), **la responsabilité de la protection de vos données vous incombe**. Face à une menace protéiforme, certains dispositifs de sécurisation communément utilisés se révèlent insuffisants. En voici une illustration avec deux cas concrets.

Vous hébergez vos données dans le cloud … un snapshot n'est pas une sauvegarde !

Vous disposez d'une offre cloud de type IaaS hébergée chez un fournisseur (par exemple avec l'offre Hosted Private Cloud powered by VMWare on OVHCloud…). Votre contrat prévoit possiblement des dispositifs de protection de vos machines virtuelles (VM) **ou de vos instances**. Vous pouvez aussi opérer ces snapshots par vous-même.

Ce que cela apporte

- Les snapshots sont une image de vos VM réalisée à un instant donné. Ils permettent donc de restituer un état antérieur récent de vos VM.
- Cela couvre certaines situations : erreur de manipulation, problème de montée de version, défaillance des systèmes hébergeant les VM...

Ce que cela ne couvre pas

- Les snapshots ne permettent pas de récupérer des fichiers individuels ou une partition de données/système (ils sont limités à une récupération de machine entière).
- Les snapshots résident sur le même média que les données de production. Ils restent donc soumis aux incidents pouvant toucher ce média.
- Les snapshots, d'après les bonnes pratiques, visent des durées de rétention courtes (quotidienne ou hebdomadaire), selon la fréquence choisie. Ils ne permettent pas de remonter à un état ancien de la VM et des données.
- Si les données de production sont cryptolockées par un ransomware, le snapshot les copiera telles quelles. Il ne permettra donc pas de restituer des données saines.

Les snapshots ne sont pas donc des systèmes de sauvegarde complets. Ils s'avèrent insuffisants dans le cadre d'une stratégie de protection de données. Le snapshot n'est en outre pas adapté à des archivages réglementaires. De plus, il ne fait l'objet d'aucun SLA de la part de l'hébergeur.

Les snapshots capturent l'état, les données et la configuration d'une machine virtuelle en cours d'exécution, afin que vous puissiez récupérer rapidement et facilement la machine virtuelle dans son état précédent.

Vous réalisez vos sauvegardes en interne…
… une copie sur un deuxième site est nécessaire !

Vous hébergez vos données de production on-premise et/ou chez un hébergeur. **Vous effectuez vos sauvegardes vous-mêmes, sans externalisation et sans réaliser de seconde copie sur un site distinct de celui où se situent les données de production**. Vous faites des tests de restauration réguliers. A priori, cela fonctionne sans difficulté.

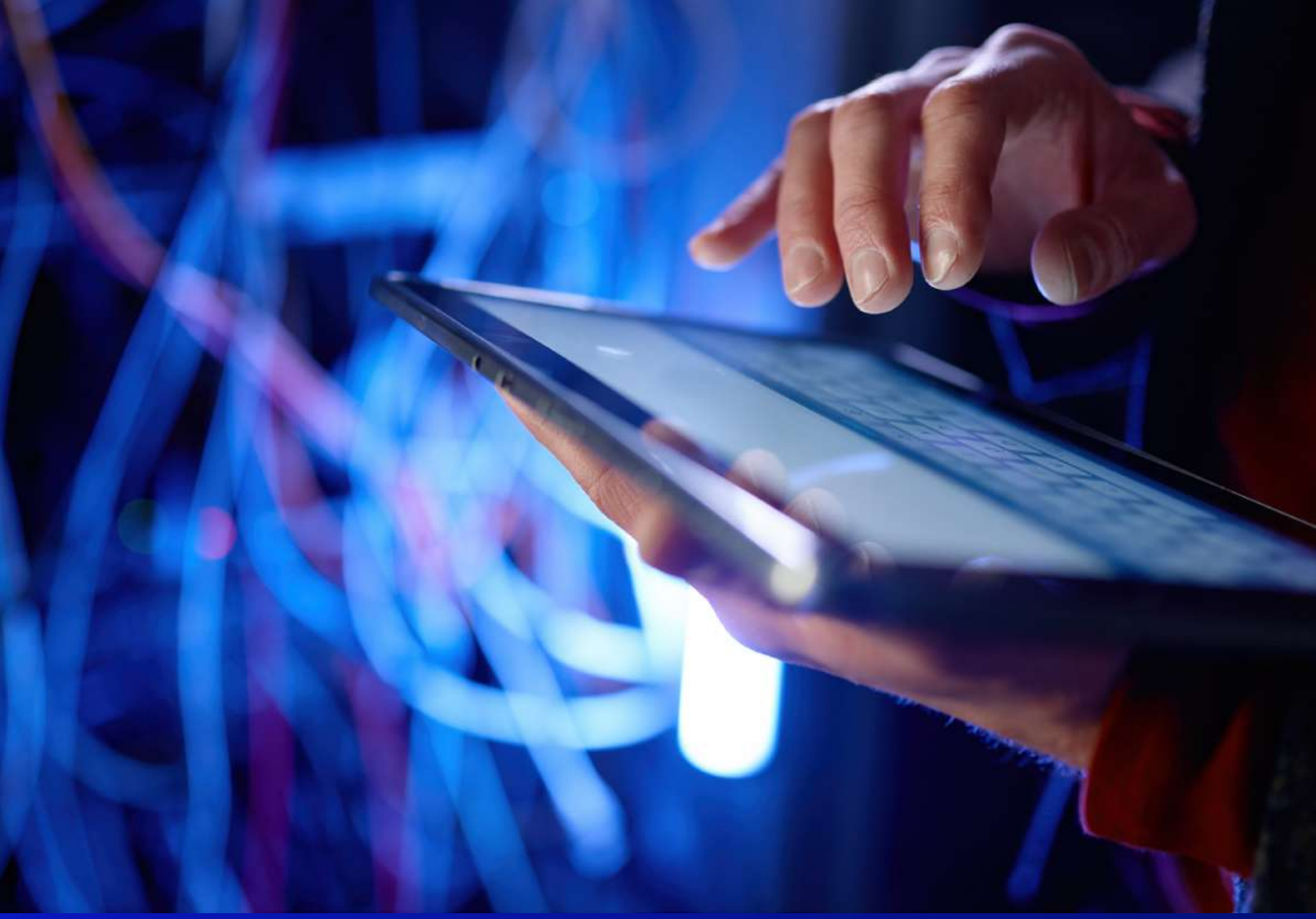
Ce que cela apporte

- Vous disposez d'un premier niveau de sécurisation cohérent de vos données en environnement hybride.
- Vous êtes protégé contre les erreurs de manipulation ou des défauts de montée de version.
- Vous pouvez restaurer vos données avec différents niveaux de granularité : fichier, système complet, logique, physique… avec une possibilité de choisir les durées de rétention (pour archivage et audits).
- Vous pouvez faire face à certaines pannes matérielles sur vos systèmes ou sur ceux de votre hébergeur.

Ce que cela ne couvre pas

- Votre dispositif n'adresse pas certains risques.
- Vous n'êtes pas protégé **contre un sinistre majeur** touchant vos infrastructures ou celles de votre hébergeur (catastrophes naturelles ou accidentelles, incendies, inondations, rupture d'alimentation…). Vous ne réunissez donc pas les conditions pour établir un PRA.
- Votre dispositif ne vous protège pas **des attaques de type ransomware**. Celles-ci vont en effet contaminer vos sauvegardes avant de chiffrer les données primaires.

Pour se prémunir d'un sinistre, il est hautement recommandé de faire une sauvegarde sur un site distant. Celui-ci ne sera pas soumis aux mêmes règles d'attaque et ne possédera donc pas les mêmes vulnérabilités. En outre, pour être certain de disposer de données de sauvegardes saines en cas d'attaque ransomware, ces sauvegardes devront être "hors ligne" (air-gapped) ou être rendues immuables.



L’immuabilité des sauvegardes : un enjeu de taille

Une sauvegarde est dite immuable lorsque **les données sauvegardées ne peuvent absolument plus être modifiées**. Le but d’une sauvegarde immuable est de **pouvoir être restaurée sur des serveurs de production en toute confiance**, avec la certitude de disposer de données saines, non altérées.

Les sauvegardes classiques peuvent ne pas suffire pour restaurer les données cryptolockées lors d’une attaque : la sauvegarde pouvant elle-même avoir été contaminée. **Vos données de sauvegarde doivent donc être isolées et immuables** : c’est le seul moyen de garantir la restauration si les systèmes en production sont infectés.

Les bonnes pratiques de mise en place d’immuabilité préconisent une rétention minimum de 14 jours.

3 QUELLES SOLUTIONS POUR RENFORCER LA SÉCURITÉ DE VOS SAUVEGARDES ?

Voici deux types de solutions, développées face aux menaces actuelles, pour mettre en place ou renforcer la sécurité de vos backups.

Le service de backup managé

Une solution de Backup-as-a-Service (BaaS) assurée par votre fournisseur de services cloud vous offre un plan de sauvegarde complet et sur-mesure pour vos systèmes hébergés chez ce prestataire. Les sauvegardes sont stockées dans des centres de données sécurisés. Les sauvegardes reposent sur des technologies et des architectures pouvant garantir leur immuabilité. Cela renforce l'intégrité des données sauvegardées, et leur protection contre toute modification ou attaque ultérieure.

Les services de backup managés sont des solutions clés en main qui renforcent le niveau de protection de vos systèmes et données résidants dans le cloud. En termes d'usage, ils vous apportent :

- **Des capacités de restauration logiques avancées** au niveau de chaque fichier,
- **Une réversibilité totale**, avec la possibilité de récupérer l'ensemble de vos données sauvegardées si vous le souhaitez,
- Une flexibilité dans **le choix des durées de rétention**,
- Un **gain de temps** et l'accès à des compétences à l'état de l'art,
- L'utilisation d'**outils de sauvegarde à jour**.

Les engagements et les garanties apportées par un service de BaaS sont formalisés par des engagements de niveaux de service (SLAs), en cohérence avec les règles de transfert de responsabilités entre client et hébergeur. Les procédures de reprise d'activité ou de restauration restent à la charge du client, selon les modalités de son PRA. Elles doivent en outre être régulièrement testées.

La sauvegarde dans un cloud distant

Si vos données sont hébergées dans votre propre centre de données (on-premise), ou si vous disposez d'une infrastructure hybride, vous pouvez opter pour une sauvegarde distante chez un 2ème fournisseur de services cloud. Avec cette approche, l'environnement de sauvegarde est distinct de vos environnements de production. **Cela renforce la protection de vos systèmes sur plusieurs points** :

- Vos sauvegardes s'effectuent et résident dans un centre de données distant. Elles sont donc **à l'abri de tout incident ou sinistre sur votre/vos site(s) de production**.

- Vous bénéficiez de **technologies distinctes entre site de production et site de sauvegarde**, dans la mesure où les formats de stockage des sauvegardes diffèrent de ceux du site de production. Cela constitue une partie de la réponse aux attaques de type ransomware, en agissant comme une barrière empêchant leur propagation.

- Vous pouvez avoir accès, sur le site de backup, à des **technologies de sauvegardes immuables**, comme le stockage objet certifié. Moyennant une rigueur de mise en place, cela vous confère une protection contre les modifications ultérieures des données sauvegardées et répond au besoin d'immuabilité pour assurer des données saines.

Le stockage objet : la clé pour l'immuabilité

Dans le domaine du stockage de données numériques, la technologie WORM (Write Once Read Many) permet d'écrire des données sur un support une seule fois et d'en empêcher l'effacement ou la modification ultérieure. Les données sont considérées comme immuables : les utilisateurs autorisés peuvent les lire aussi souvent que nécessaire, mais ils ne peuvent pas les modifier ou les supprimer. Cet aspect immuable joue un rôle essentiel dans le respect des exigences de sécurité et de conformité des données et dans la protection contre les ransomwares et autres menaces.

Basés sur un ensemble d'outils et de matériels certifiés, l'Object Storage d'OVHCloud (stockage objet) assure l'immuabilité des objets en utilisant le model WORM via la fonctionnalité d'Object Lock. L'Object Lock empêche la suppression ou l'écrasement des objets pendant une durée déterminée et/ou indéfiniment.

4 LES OFFRES OVHCLOUD / VEEAM

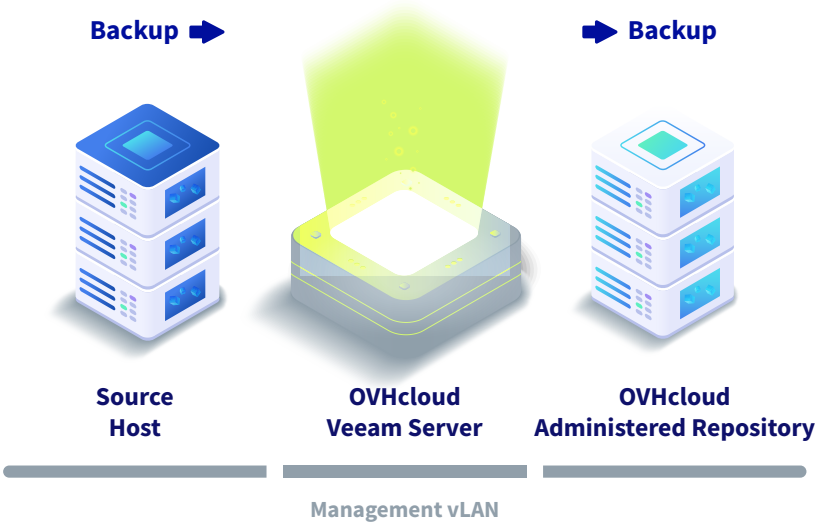
Les offres OVHCloud basées sur les technologies de sauvegarde Veeam vous permettent de déployer des plans de protection de vos données adaptés aux risques actuels.

VEEAM BACKUP MANAGED

Un Backup-as-a-Service pour la sauvegarde de vos systèmes hébergés sur VMWare on OVHcloud

La solution de backup managée d'OVHcloud, basée sur les technologies de Veeam Backup & Replication, vous permet de **déléguer la sauvegarde automatique de vos systèmes**. Le niveau d'engagement sur la qualité du service est garanti par un SLA clair et précis.

- **Backup-as-a-Service** : la sauvegarde de vos systèmes est totalement automatisée et supervisée par OVHcloud.
- **Stockage inclus** : la sauvegarde de vos données est stockée dans nos infrastructures souveraines et dédiées. Un lien d'administration vous permet d'y accéder facilement.
- **Suivi quotidien** : un rapport personnalisable vous est envoyé chaque jour. Celui-ci reprend la liste et les états de toutes vos sauvegardes.
- **Restauration / Réversibilité** : Vous pouvez restaurer vos machines à n'importe quel moment, au niveau de chaque fichier. Vous bénéficiez d'une réversibilité totale afin de récupérer l'ensemble de vos données sauvegardées si besoin.



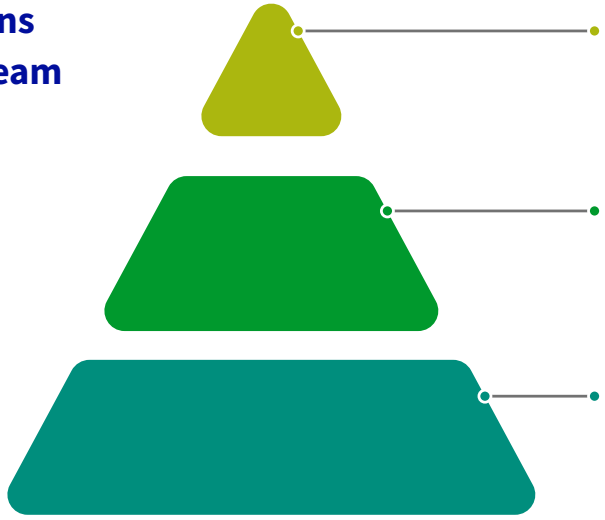
OVHCLOUD OBJECT STORAGE CERTIFIÉ VEEAM READY

Le stockage objet certifié pour vos sauvegardes

Utilisé dans le cadre de sauvegarde (mais pas que !), Veeam Ready permet d'utiliser du stockage objet certifié chez OVHcloud pour **faire une deuxième copie de vos données sur les infrastructures** OVHcloud. Vous disposez ainsi d'une sauvegarde supplémentaire et inaltérable pour vos systèmes hébergés on-premise ou chez un autre fournisseur de services cloud.

- **Sauvegardes distantes et localisation** : dans le cadre de vos sauvegardes distantes avec Veeam Cloud Connect, vous pouvez opter pour le stockage Veeam Ready et choisir la localisation de vos backups.
- **Immuabilité** : garantie de non altération, de non modification des sauvegardes réalisées en stockage objet.
- **Réversibilité** : vous accédez au contenu à l'intégralité de vos sauvegardes pour les restaurer au besoin chez OVHcloud ou ailleurs.
- **Facturation** : la facturation est basée sur le volume de stockage utilisé. Les appels récurrents d'API n'entraînent aucune facturation supplémentaire.
- **Certification Veeam Ready** : compatibilité au protocole S3 garantie par Veeam.

Les certifications partenaires Veeam



Veeam Integrated
Partenaires avec intégrations complexes ou profondes

Veeam Ready
Partenaires avec compatibilité Veeam certifieé par des tests

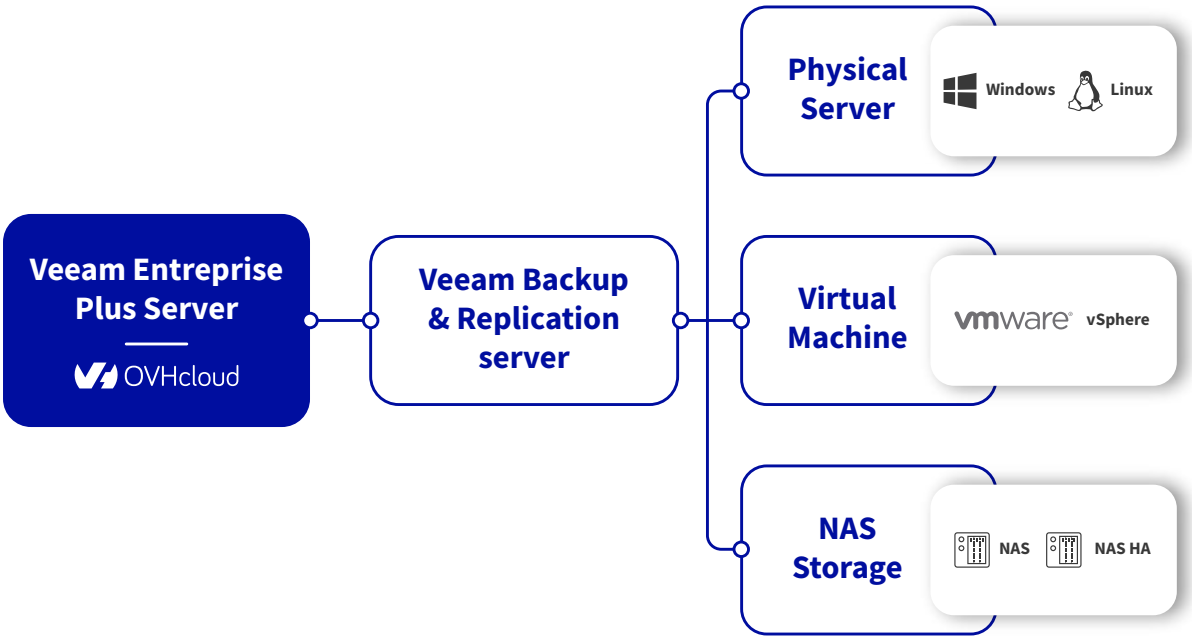
Veeam Infused
Partenaires utilisant les APIs disponibles

VEEAM ENTERPRISE PLUS

La protection des données adaptée aux infrastructures hybrides

Déployez votre socle Veeam Backup & Replication et utilisez les licences Enterprise Plus de OVHcloud afin d'**assurer vous-mêmes la sauvegarde de vos systèmes**.

- **Sécurisez votre activité** : mettez en place une sauvegarde et une réplication de vos applications, machines et données afin de pouvoir redémarrer rapidement en cas de dysfonctionnement.
- **Reprenez la main sur vos sauvegardes** : pilotez l'ensemble de vos sauvegardes, chez OVHcloud ou dans votre propre centre de données, quel que soit le nombre de machines en votre possession ou leur localisation.
- **Activez l'immuabilité** : vous pouvez choisir de réaliser vos sauvegardes sur du stockage objet S3 "Veeam Ready" chez OVHcloud.
- **Pay-as-you-go** : vos services sont facturés au plus près de votre consommation réelle de notre solution, dès le mois suivant.



Vous construisez entièrement votre solution, par exemple avec un Object Storage S3 hébergé chez OVHcloud, qui vous permettra un stockage compatible avec immuabilité.

Les engagements d'OVHCloud en tant que leader européen du cloud souverain

Chez OVHcloud, **la sécurité des données est une priorité absolue**. Nos solutions sont conformes aux réglementations applicables au niveau de l'union européenne en matière de protection des données. Nous maîtrisons également la sécurité de notre réseau, afin de garantir un haut niveau de sûreté.

- Protection des données personnelles / RGPD
- Souveraineté des données
- Qualification ANSSI SecNumCloud

Mentions légales OVHcloud

La performance des services varie selon leur usage, configuration et d'autres facteurs.

Les services d'OVHcloud sont soumis aux conditions générales et particulières en vigueur à la date de la commande. OVHCloud se réserve le droit de modifier et mettre fin à ses services en tout temps.

Un système de sauvegarde est un outil visant à renforcer votre protection contre la perte de vos données. Seul, il ne vous garantit pas contre la perte de vos données. Il est de votre responsabilité de concevoir et mettre en place un ensemble de dispositifs dans un plan global de reprise d'activité afin de favoriser un redémarrage rapide de vos services en cas d'interruption de service, de perte ou de compromission de vos données.

Vous souhaitez renforcer votre stratégie de sauvegarde ?
Faire le point sur le niveau de protection dont vous disposez ?

Contactez-nous