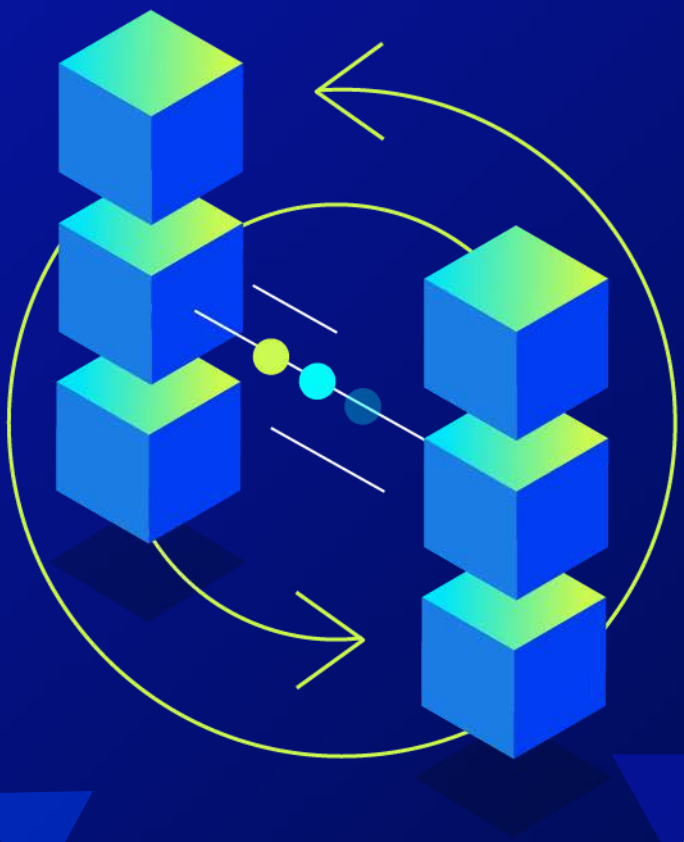
OVHcloud

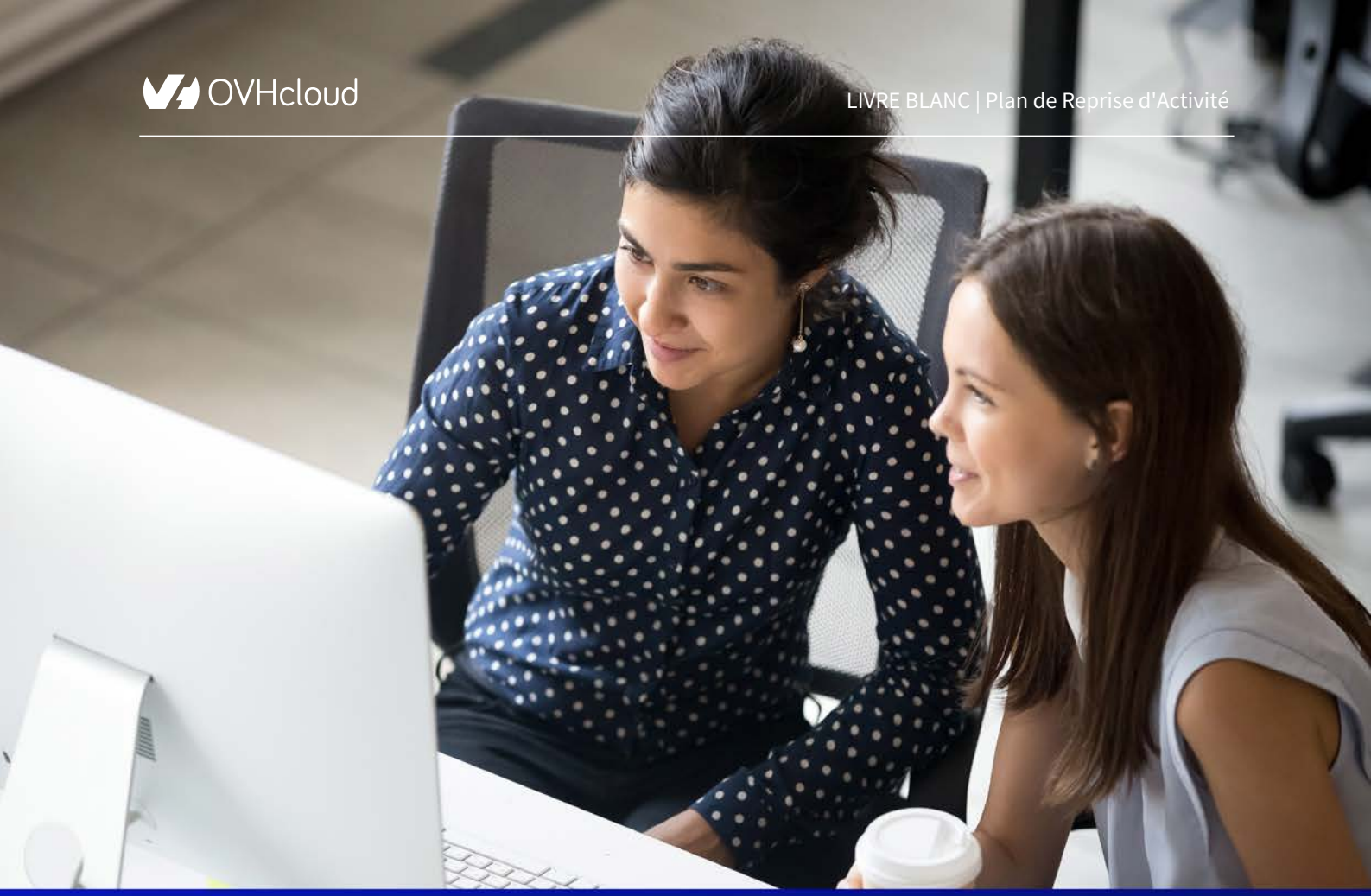
LIVRE BLANC

Résistez aux cybermenaces et préparez-vous à l'inattendu

Le moment est venu d'examiner de près votre plan de reprise d'activité.



Sommaire



Un plan de reprise d'activité est un élément essentiel de votre plan de continuité d'activité

Il fut un temps où la reprise d'activité consistait principalement à se protéger contre les catastrophes naturelles, les erreurs humaines, les pannes d'équipement et les attaques physiques. Aujourd'hui, le risque est beaucoup plus élevé et il est plus probable que les dommages soient causés par des cyberattaques. Le rapport 2022 sur les tendances en matière de protection des données a révélé que **76 % des entreprises participant à l'étude ont subi une attaque par ransomware**. De plus, au cours des deux dernières années, **les événements liés à la cybersécurité** ont été **les pannes les plus importantes** qu'elles aient connues.[1] C'est ainsi que le cyberterrorisme est devenu la source la plus probable de perte de données.

Les dommages liés à la cybercriminalité devraient atteindre 10,5 milliards de dollars par an d'ici 2025. [2]

1 2022 Data Protection Trends Report, Veeam
2 2022 Official Cybercrime Report, Cybersecurity Ventures

Plans de continuité et de reprise d'activité : quelle est la différence ?

Le plan de continuité d'activité (PCA) se concentre sur **les politiques, les procédures et la vision globale de la manière dont l'entreprise continuera à fonctionner quel que soit l'incident** : défaillance de la chaîne d'approvisionnement, embargo gouvernemental sur des pays étrangers, troubles civils, incident informatique, pénurie de carburant, etc. **Le plan de reprise d'activité** (PRA), quant à lui, est un sous-ensemble qui se concentre **sur l'infrastructure, les données et les applications IT**. Il permet de savoir si tout est protégé de manière optimale, comment les dirigeants et les employés accèdent au système et par quels moyens restaurer les systèmes critiques le plus rapidement possible afin de limiter l'impact sur les activités de l'entreprise.

Un PRA sans solution pour rendre les données disponibles et utilisables par votre personnel, et ce, de manière hautement sécurisée, peut s'avérer extrêmement coûteux en termes de continuité de l'activité. Si ce sujet vous préoccupe, pas de panique ! Vous n'êtes pas seul.

Les désastres liés à un plan mal étudié

Le problème est aggravé par le fait que le périmètre et la surface d'exposition sont beaucoup plus importants qu'auparavant. En effet, les employés travaillent en mode hybride, de même que les systèmes et applications interconnectés produisent et consomment des données à une vitesse exponentielle. On estime que plus de sept milliards de personnes et d'entreprises sont connectées à Internet par le biais d'au moins 30 milliards d'appareils. De plus, les données augmentent et devraient atteindre 175 zettaoctets d'ici 2025.[1]

Les charges de travail sont plus diversifiées, mobiles et disparates, au sein de différentes plateformes et régions géographiques, qu'elles proviennent du cloud, de l'edge computing ou d'une version hybride. Tous ces éléments doivent donc être connectés pour offrir une expérience numérique cohérente. Pour les applications qui ont un impact sur l'expérience des clients et des employés, il y a une demande importante pour qu'elles soient protégées - et disponibles 24/7/365 pour répondre aux attentes des utilisateurs.

1 The Digitization of the World, IDC, November 2018

Le bon moment prime sur l'éventualité

Si ce n'est pas déjà fait, il est temps d'examiner de très près vos plans de continuité et de reprise d'activité. En effet, la protection de votre infrastructure et de vos données contre les logiciels malveillants et les attaques par ransomware implique de prévoir le moment où de tels événements se produiront, et non l'éventualité qu'ils surviennent un jour. Un PCA complet permet d'atténuer les risques pour vos opérations, tandis qu'un PRA bien conçu peut réduire considérablement, voire empêcher, les temps d'arrêt.

Pendant le confinement lié au COVID-19, nous nous sommes tournés vers Internet pour retrouver un semblant de normalité : travailler, faire du shopping, apprendre de nouvelles choses… Malheureusement, ces nouvelles habitudes sont ouvert un champ des possibles aux cybercriminels qui ont profité de la société lorsqu'elle était la plus vulnérable. L'ingénierie sociale et le hameçonnage sont utilisés pour permettre d'autres types de cyberattaques et les hackers mettent en œuvre des technologies innovantes pour augmenter le volume et l'efficacité de ces attaques. Si l'on se penche sur les systèmes d'information (SI) des entreprises, la surface exposée à Internet est plus importante aujourd'hui qu'il y a 5 ans. Et qui dit plus de surface dit plus de risques, ce qui nécessite davantage de surveillance.

Le rapport 2023 de Thales concernant les menaces pesant sur les données mondiales révèle que la part des cyberattaques visant les pays de l'Union européenne a augmenté de manière spectaculaire au cours des six derniers mois, passant de 9,8 % à 46,5 %.[1] Les personnes interrogées ont constaté une augmentation du volume des attaques de logiciels malveillants (59 %) et 22 % d'entre elles ont subi une attaque par ransomware. Par conséquent, la lutte contre la cybercriminalité est devenue un élément central de la politique de l'UE.[2]

Les principaux problèmes IT qui nécessitent un basculement complet du site sont les défaillances matérielles et logicielles. Mais la cause la plus fréquente des pannes reste la cybersécurité, notamment les ransomwares, les logiciels malveillants et le piratage, suivis de la suppression ou de la corruption accidentelle de données et des pannes de réseau.[3]

Les cyberattaques peuvent être à l'origine de véritables catastrophes, c'est pourquoi votre PRA doit les traiter comme la menace qu'elles représentent pour votre reprise et votre continuité d'activité. Envisagez le pire scénario possible: quelles donnéesdevront alors être récupérées et à quelle vitesse ? Gardez à l'esprit qu'il n'existe pas de solution universelle. Chaque PRA est aussi unique que l'entreprise qui le conçoit, tout comme les données qui devront être détectées et récupérées.

> **La part des cyberattaques visant les pays de l'Union européenne a augmenté à 46,5 %.**

[1 2023 Thales Global Data Threat Report, https://cpl.thalesgroup.com/data-threat-report
2 https://www.europol.europa.eu/crime-areas-and-trends/eu-policy-cycle-empact
3 2022 Data Protection Trends Report, Veeam

Les trois piliers de la résilience informatique

La résilience informatique repose sur trois piliers essentiels qui vous permettent de résister à n'importe quelle perturbation, d'exploiter les nouvelles technologies en toute simplicité et d'aller de l'avant avec confiance.

- **Reprise d'activité continue** – Pour vous protéger contre les perturbations et offrir la meilleure expérience client en permanence, votre sauvegarde doit être continue, et non pas périodique ou basée sur des snapshots. La réplication est recommandée pour assurer une disponibilité continue, sans temps d'arrêt ni perte de données.
- **Mobilité des charges de travail** – Des migrations, aux consolidations en passant par la transition vers de nouvelles infrastructures, assurez-vous de pouvoir déplacer vos applicatifs métier et vos charges de travail liées aux données sans accroc, sans risque et en bénéficiant d'une protection complète tout au long du processus.
- **Multicloud et cloud hybride** – Il est essentiel de tirer parti du cloud pour booster votre activité. Profitez des avantages qu'il a à offrir et assurez-vous que vous avez la liberté de choisir votre type de cloud et que vous êtes en mesure de passer d'un cloud à l'autre sans encombre.

La transition vers la résilience informatique

La première étape vers la résilience informatique consiste à réduire le risque systémique. Vous devez faire converger et automatiser vos processus de reprise d'activité, en veillant à ce que votre entreprise soit protégée contre les perturbations. Ainsi, vos services continuent d'être accessibles en permanence et vous garantissez le respect des SLA de votre entreprise. En automatisant vos PRA, vous réduisez la charge de travail de votre personnel, les coûts et les risques, tout en vous assurant une meilleure protection contre les perturbations imprévues.

Une fois cette étape franchie, vous pouvez réorienter vos ressources pour vous concentrer sur la mise en place d'une stratégie multi-cloud et cloud hybride afin d'apporter à votre entreprise l'agilité dont elle a besoin. L'affectation réfléchie des charges de travail liées aux données, que ce soit sur site ou dans le cloud, permet de moderniser votre infrastructure en vous affranchissant des applications héritées : vous permettez ainsi à vos opérations et à votre entreprise d'évoluer. En alignant vos ressources pour mieux accompagner votre croissance et votre transformation continue, vous pouvez viser une meilleure efficacité opérationnelle et votre système informatique peut s'adapter à la vitesse de votre entreprise.

Sauvegarde ou réplication : quelle est la meilleure approche ?

La **sauvegarde** consiste à effectuer une ou plusieurs copies des données. C'est un moyen relativement abordable de réduire les pertes de données. Elle peut s'appuyer sur des snapshots pris à des moments prédéterminés. La sauvegarde permet généralement de dupliquer tout ce qui se trouve au sein de l'entreprise, notamment pour l'archivage à long terme des documents commerciaux. L'approche qui associe **sauvegarde et restauration se base sur une sauvegarde externe** qui permet de **rétablir une application** dans le même datacenter que celui où se trouvait la charge de travail originale, si celui-ci est disponible, ou dans un autre datacenter en cas d'incident majeur.

La réplication, quant à elle, peut offrir un niveau de résilience plus élevé. Elle consiste à effectuer des copies ou à prendre des **snapshots des données d'application à chaque fois qu'un changement se produit**, puis à les déplacer entre les différents sites d'une entreprise. Elle peut être **synchrone ou asynchrone**.

La **réplication asynchrone** repose sur des snapshots qui **capturent un point dans le temps avant d'envoyer les données vers un emplacement secondaire par la suite**. Cela signifie que les copies situées sur différents sites peuvent ne pas être complètement à jour, il existe donc un risque de perdre des données avant que chaque réplique soit actualisée et cohérente.

La **réplication synchrone** porte la protection et la disponibilité des données à un tout autre niveau. Les donnéessont écrites dans des emplacements de stockage primaires et secondaires où elles sont reconnues par le système. Ainsi, l'**ensemble des répliques contient les mêmes données à tout moment et il n'y a aucun risque de perte en cas de panne**. Cette méthode nécessite toutefois une faible latence, c'est pourquoi elle doit être appliquée uniquement sur une couche de stockage. Pour les entreprises avec de gros volumes de données ou des charges d'écriture élevées, la réplication peut s'avérer peu pratique et les fraisgénéraux liés à l'écriture des données sur plusieurs sites peuvent devenir trop élevés.

La technologie de réplication nécessitant un investissement dans un second site (actif ou inactif), elle est donc plus coûteuse. Cependant, il s'agit véritablement d'une reprise d'activité, car elle permet de reprendre les opérations rapidement et facilement : une machine virtuelle est répliquée en permanence et attend d'être basculée si nécessaire.

RPO et RTO : vos guides pour la reprise d'activité

La reprise d'activité est généralement mesurée en termes d'**objectif de point de reprise** (RPO) et d'**objectif de temps de reprise** (RTO). Ces paramètres clés vous guideront vers les meilleures options de sauvegarde et de réplication des données pour votre plan de reprise d'activité.

Le RPO décrit l'intervalle de temps écoulé depuis la dernière sauvegarde des données. Le RTO comprend la durée et le niveau de service du rétablissement d'un processus. En d'autres termes, il s'agit de savoir quelle quantité de données vous pouvez vous permettre de perdre et quel délai de restauration maximal vous pouvez tolérer pour votre application. Il est donc essentiel de définir le bon équilibre entre le RPO et le RTO pour votre entreprise.

La quantité de données à récupérer (RPO)

Le RPO se réfère à la quantité de données exposées à un risque par le biais d'une méthode particulière. Voici un exemple.

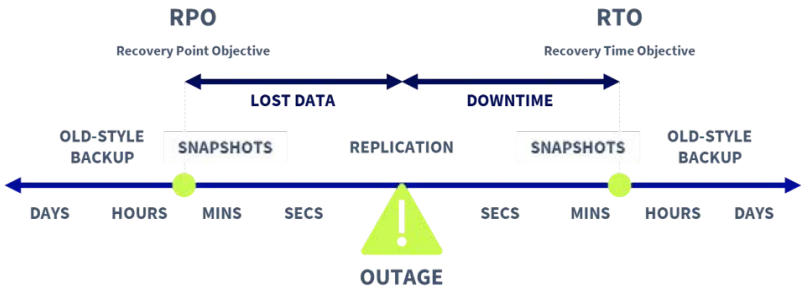
Supposons qu'une entreprise effectue une sauvegarde complète de ses données tous les jours et que celles-ci soient régulièrement modifiées au cours des dernières 24 heures. Si elle effectue une sauvegarde à midi et que ses systèmes tombent en panne à 13 heures, elle n'aura perdu qu'une heure de données. Mais si tout se passe bien jusqu'à ce qu'un dysfonctionnement survienne le lendemain à 11h59, l'entreprise aura perdu près de 24 heures des données modifiées depuis la dernière sauvegarde.

Une organisation dont les données évoluent lentement peut se contenter d'un RPO de 24 heures si les changements perdus au cours de cette période n'ont pas d'impact majeur ou si les données peuvent être facilement recréées. Vous pouvez, par exemple, déplacer des factures d'un système à l'autre. Mais pouvez-vous demander à vos clients de retourner sur une boutique en ligne qui était indisponible pendant quelque temps ? Pour les entreprises qui gèrent des transactions financières ou des données médicales par exemple, une perte de données ne serait-ce que de 10 minutes a un impact important. Le RPO devrait donc être beaucoup plus court.

Le temps nécessaire à la récupération des données (RTO)

Le RTO est le temps nécessaire pour redonner aux données perdues un format consommable afin que vous puissiez reprendre vos activités. Il vous aide à déterminer la méthode et les technologies à utiliser.

Un service de sauvegarde conserve généralement l'ensemble des données de la première copie (**sauvegarde complète**) et y ajoute ensuite uniquement les données qui ont été modifiées (**sauvegarde incrémentielle**). Ces données peuvent également être dédupliquées et compressées au sein d'un fichier, qui est ensuite transféré vers un autre dispositif de stockage. Pour récupérer la sauvegarde, vous devez accéder aux données, les lire, les réhydrater et les récupérer sur le serveur de remplacement (physique ou virtuel) afin de les rendre à nouveau utilisables.



Par rapport à la sauvegarde et en termes de RTO, la réplication est rapide comme l'éclair. En effet, les modifications apportées à un serveur virtuel sont copiées sur un emplacement secondaire en temps réel. En cas de panne, le site secondaire peut être mis en service (failover), ce qui permet au serveur de reprendre ses fonctions beaucoup plus rapidement.

Lorsque vous examinez vos plans de continuité et de reprise d'activité, **il est essentiel de prendre en compte le RTO : quelles données, quels systèmes et quelles applications doivent être disponibles en quelques minutes, quelques heures ou quelques jours** ? Si vous avez besoin de toutes vos données instantanément parce qu'elles sont indispensables au bon fonctionnement de votre entreprise, optez pour une réplication en quasi temps-réel. Il vous suffit d'appuyer sur un interrupteur, d'activer la machine virtuelle et de reprendre vos activités. À l'inverse, si vos donnéeset applications ne présentent pas les mêmes besoins, vous pouvez opter pour un plan qui comprend à la fois la réplication et la sauvegarde, tout en tenant compte des dépendances et des priorités de chaque application.

Trois niveaux pour la reprise d'activité de votre entreprise

Maintenant que vous comprenez les processus et les paramètres, vous pouvez envisager les choses sous trois angles différents : ce qui est indispensable et doit être rétabli immédiatement, ce qui est **essentiel** mais peut attendre quelques heures, et ce qui est m**oins impactant** et peut attendre quelques jours. Vous pouvez utiliser différentes méthodes de protection des données en fonction de ces niveaux. Par exemple, plusieurs téraoctets de données datant de la dernière décennie peuvent être importants pour des raisons d'historique ou de conformité, mais le fait qu'il faille quelques jours pour les récupérer ne pose pas de problème majeur. De même, il n'y a aucun inconvénient à ce que les données critiques qui sont importantes pour le fonctionnement quotidien de votre organisation soient rétablies en quelques heures. En revanche, s'il s'agit de données qui ne peuvent absolument pas être perdues, c'est une situation différente.

Charges de travail non critiques

Pour les applications non critiques, les sauvegardes restent une solution très rentable qui permet de conserver des copies des données et des machines virtuelles. Ces sauvegardes peuvent être stockées **sur site, hors site dans un autre emplacement géographique** ou vous pouvez adopter une combinaison de ces deux options pour une protection accrue de vos données et si vous avez des besoins de conservation à long terme. Le choix dépend du **volume de données, de la durée de conservation et du processus de restauration** que vous souhaitez mettre en place. Pour les archives volumineuses qu'il vous faut conserver pendant plusieurs années, le cold storage (ou archivage) présente le meilleur rapport prix/To. Cependant, son délai de restauration plus long en fait une solution insuffisante pour les copies de sauvegarde hebdomadaires.

Charges de travail essentielles

Pour les applications critiques, il existe des solutions de sauvegarde et de reprise d'activité qui vous permettent de restaurer rapidement et automatiquement vos charges de travail sur votre site principal ou secondaire.

La **règle d'or de la sauvegard**e veut que vous disposiez d'au moins **3 copies de vos données, stockées sur 2 supports différents**, et qu'au moins **une de ces copies se trouve hors site**. Pour une protection renforcée, l'une de vos copies peut être entièrement hors ligne : de cette façon, votre organisation peut se prémunir des risques de ransomware. Mais attention, toute sauvegarde n'est valable que dans la mesure où elle est vérifiée, il vous faudra donc surveiller quotidiennement vos tâches de sauvegarde et tester régulièrement le processus de restauration.

Fonctions essentielles

Pour les applications essentielles, la solution la plus fiable est la **technologie de réplication**, qui consiste à **créer en permanence une copie des données** sur un site distant. Dans le cas d'une réplication quasi synchrone, le délai entre l'écriture des données sur l'hôte de production et leur envoi hors site est infime. Le RPO peut littéralement être mesuré en secondes, de sorte que vous ne perdrez jamais ne serait-ce que cinq minutes de données.

Cette méthode de réplication quasi instantanée est une solution de reprise d'activité aux architectures virtuelles. En effet, l'orchestration de la réplication en temps réel permet aux utilisateurs d'effectuer des tests granulaires de basculement et de reprise d'activité. Elle peut répliquer une seule machine virtuelle aussi bien que toute une application, de sorte que si vous rencontrez des problèmes avec une BDD, une application ou un site web spécifique, vous pouvez orchestrer le basculement uniquement pour cette charge de travail.Vous profitez ainsi d'une certaine flexibilité pour maintenir la disponibilité de vos applications et pouvez prendre des mesures correctives avec peu de temps d'arrêt.

Les solutions de reprise d'activité qui répondent à vos besoins et à votre budget

Les experts Professional Services et les architectes de solutions OVHcloud peuvent vous aider à déterminer la meilleure solution de reprise d'activité en fonction de votre entreprise IT, de vos opérations commerciales et de votre budget. Découvrez nos scénarios de sauvegarde et de restauration.

Protéger vos données contre les pertes, où qu'elles soient hébergées

Que vous hébergiez vos applications sur site ou dans le cloud, vous avez besoin d'une solution de sauvegarde durable qui vous protégera contre les pertes de données. Pour les applications non critiques qui tolèrent un RPO > 24 heures et un RTO > 48 heures, il est important de disposer d'une solution simple à utiliser et compatible avec votre environnement. **Object Storage** d'OVHcloud, **certifié Veeam Ready**, est une solution de stockage performante, économique et compatible S3 que vous pouvez facilement ajouter à votre paysage IT existant, qu'il s'agisse d'un **Public Cloud**, d'un **Hosted Private Cloud** ou même d'un environnement 100 % **Bare Metal**.

Solutions de sauvegarde managées pour les applications cloud-natives

Chez OVHcloud, vous trouverez toutes les briques essentielles pour vos applications cloud-natives, une variété d'instances de calcul, **Object Storage** et **Block Storage**, ainsi qu'une vaste gamme de services de BDD managées. Pour accélérer et simplifier vos déploiements, OVHcloud propose également des solutions de sauvegarde prêtes à l'emploi pour chaque composant de votre application. Vous pouvez opter pour **Volume Backup** pour vos données de stockage en bloc. Concernant la protection des données hébergées sur le disque d'une instance, **Instance Backup** sera votre meilleure arme. Enfin pour les BDD Managées, OVHcloud a développé **les sauvegardes automatisées**. Toutes ces options sont intégrées à votre projet Public Cloud et gérées via API et CLI.

[En savoir plus sur les options de sauvegarde et de stockage]

Pour les charges de travail VMware on OVHcloud, vous pouvez facilement mettre en place une stratégie de sauvegarde avec notre service **Veeam Managed Backup**. Vos sauvegardes sont créées à partir de machines virtuelles sélectionnées avant d'être transférées vers votre espace de stockage dédié et complémentaire. Ces tâches sont gérées par les équipes d'OVHcloud qui vous enverront quotidiennement un rapport d'état de toutes vos tâches de sauvegarde.

[Découvrir Veeam Managed Backup]

Planification de la reprise d'activité pour les charges de travail essentielles

Une fois que vous avez établi votre approche de sauvegarde pour les applications non critiques, il est temps de mettre en place une solution de reprise d'activité pour vos charges de travail essentielles. Pour les applications critiques qui doivent être opérationnelles en quelques heures, vous pouvez créer un site secondaire en mode veille et y répliquer vos données. Ce datacenter secondaire fonctionnera avec des ressources minimales et s'adaptera à la capacité requise après l'incident.

Si, comme beaucoup d'autres[1], vous avez décidé d'héberger votre cloud d'entreprise sur des solutions VMware, vous pouvez bénéficier de la solution Zerto PRA. Peu importe si vous hébergez votre infrastructure sur site et avez besoin d'un site secondaire, si vos sites primaire et secondaire relèvent de deux localisations OVHcloud ou si vous souhaitez mettre en place un PRA depuis OVHcloud vers un fournisseur de cloud tiers. La plateforme Zerto permet d'améliorer la résilience de vos données dans le centre de données de votre choix.

Découvrir Zerto pour plan reprise d'activité VMware

TIPCO

TIPCO, une société FinTech autrichienne, associe des compétences informatiques à de nombreuses années d'expertise en matière de trésorerie pour proposer une plateforme d'information destinée aux départements de trésorerie. Pour répondre aux besoins de ses clients indexés DAX, de la gestion des comptes à l'automatisation des flux de travail et des rapports, TIPCO avait besoin d'une infrastructure IT sécurisée, dédiée et disponible immédiatement.

Le traitement des données financières de ces sociétés cotées en bourse nécessite d'adopter des politiques de sécurité strictes et de se conformer aux réglementations européennes. La souveraineté des données a également été un facteur supplémentaire en faveur du transfert des charges de travail critiques de TIPCO vers OVHcloud.

TIPCO a mis en œuvre un **Hosted Private Cloud** managé sur deux sites distants, à Roubaix et à Limburg, et a déployé un plan de sauvegarde et de reprise d'activité à plusieurs niveaux. Pour protéger les charges de travail en cas de défaillance d'un hôte, il y a toujours un hôte « vide » dans le datacenter virtuel. vSphere par VMware, doté de la résilience aux pannes intégrée, peut alors s'en servir pour redémarrer immédiatement les machines virtuelles prioritaires lorsque l'un des hôtes est déconnecté. Comme principale solution de sauvegarde, TIPCO utilise **Veeam Managed Backup** pour effectuer des copies automatisées de ses machines virtuelles. Les copies des sauvegardes sont stockées dans une infrastructure dédiée et complémentaire. Le troisième niveau de protection des données est assuré par **Zerto PRA**. TIPCO a configuré son PRA via Zerto Virtual Manager (ZVM) pour les machines virtuelles concernées. Les données sont répliquées en toute sécurité vers le site secondaire en France via notre réseau privé de fibre optique. De cette manière, les deux sites peuvent être soit des sites de récupération, soit des sites primaires.

1 VMware Continues to Lead the HCI Market in Q2 of 2022 for Market Share, according to IDC

Solutions sur mesure pour les fonctions essentielles

Pour adapter correctement votre approche PRA à vos applications essentielles, il ne suffit pas d'utiliser une solution prête à l'emploi. La plupart des paysages informatiques sont complexes et basés sur le multi-cloud, ce qui nécessite une approche personnalisée et des **solutions PRA sur mesure** qui prennent en compte les dépendances à plusieurs niveaux et les méandres de l'acheminement des données. Il est donc crucial de comprendre pleinement l'impact que chaque application peut avoir sur l'activité de votre entreprise. À moins de disposer d'une équipe d'experts en interne, la conception et le déploiement d'un plan de reprise d'activité solide peuvent vite devenir fastidieux.

Forts de plus de 10 ans d'expertise, les spécialistes **Professional Services d'OVHcloud** peuvent vous apporter des conseils techniques à chaque étape de votre PRA, de la définition de votre infrastructure cible à la formation de vos équipes. Nos experts peuvent réaliser des audits de charge de travail et d'infrastructure pour comprendre le degré de criticité de chacun de vos actifs informatiques et vous aider à estimer le RPO et le RTO. Ils vous aideront à concevoir et à déployer un scénario de reprise d'activité avant de le tester avec vos équipes pour s'assurer que tous les processus nécessaires sont en place. Pour les projets les plus exigeants, nous faisons appel à nos partenaires qui vous offriront la meilleure expérience pour vos environnements cloud et sur site.

Découvrir Professional Services

Consulter notre référentiel de partenaires

Pourquoi choisir OVHcloud ?

Infrastructure résiliente et interopérable

- Technologies standard et éprouvées (notamment VMware, Nutanix et OpenStack)
- Services hautement évolutifs
- Solutions mixtes pour répondre à vos besoins uniques

Contrôle des coûts et tarification prévisible

- Tarifs transparents
- Trafic illimité, sans frais de sortie ou d'entrée
- Appels API inclus

Sécurité et conformité

- Souveraineté des données
- Variété de certifications
- Sécurité par conception
- Réseau d'entreprise avec protection anti-DDoS

Contactez-vous

OVHcloud, acteur mondial et premier fournisseur de cloud européen, exploite plus de 450 000 serveurs dans 37 datacenters répartis sur 4 continents. Depuis plus de 20 ans, le groupe s'appuie sur un modèle intégré qui lui assure une maîtrise complète de sa chaîne de valeur, de la conception de ses serveurs, à la construction et à la gestion de ses datacenters, en passant par l'orchestration de son réseau de fibre optique. Cette approche unique lui permet de couvrir de manière indépendante tous les usages de ses 1,6 million de clients dans plus de 140 pays. OVHcloud propose désormais à ses clients des solutions de dernière génération alliant performance, prévisibilité des prix et souveraineté totale de leurs données pour accompagner leur croissance en toute liberté.

Mentions légales

Un plan de reprise après sinistre vise à renforcer votre protection contre la perte de données. Les solutions présentées dans cette documentation ne garantissent pas à elles seules une protection contre la perte de vos données. Il est de votre responsabilité de concevoir et de mettre en œuvre un plan de reprise après sinistre complet pour vous aider à reprendre rapidement vos activités en cas d'interruption de service, de perte de données ou de compromission.

CETTE DOCUMENTATION EST FOURNIE « EN L'ETAT » ET OVHCLOUD DECLINE TOUTE CONDITION, REPRESENTATION ET GARANTIE EXPRESSE OU IMPLICITE, Y COMPRIS TOUTE GARANTIE IMPLICITE DE QUALITE MARCHANDE, D'ADEQUATION A UN USAGE PARTICULIER OU D'ABSENCE DE CONTREFAÇON. EN AUCUN CAS OVHCLOUD NE POURRA ETRE TENU RESPONSABLE DE QUELQUE DOMMAGE QUE CE SOIT (TEL QUE, SANS LIMITATION, LES DOMMAGES POUR PERTE DE BENEFICES COMMERCIAUX, L'INTERRUPTION D'ACTIVITE, LA PERTE D'INFORMATIONS COMMERCIALES OU AUTRE PERTE PECUNIAIRE) RESULTANT DE LA FOURNITURE, DE L'EXECUTION OU DE L'UTILISATION DE CETTE DOCUMENTATION ET DES SERVICES OVHCLOUD, MEME SI OVHCLOUD A ETE AVISE DE LA POSSIBILITE DE TELS DOMMAGES. L'ENSEMBLE DES RISQUES DECOULANT DE L'UTILISATION OU DE LA PERFORMANCE DES SERVICES OVHCLOUD ET DE CETTE DOCUMENTATION VOUS INCOMBE.

OVHcloud se réserve le droit d'apporter des modifications et/ou d'interrompre tout service à tout moment.OVHcloud, le logo d'OVHcloud et toutes les autres marques OVH contenues dans le présent document sont des marques déposées d'OVH SAS. Toutes les autres marques contenues dans le présent document sont la propriété de leurs détenteurs respectifs.