

Haute disponibilité : sept défis dans la mise en œuvre de solutions d'accès aux données

Dans ce contexte, la disponibilité des données en permanence (« Always On ») est devenue une exigence clé pour les services informatiques. Auparavant, les entreprises utilisaient des plans de reprise d'activité après sinistre (« Disaster Recovery ») semi-automatisés, qui n'étaient bien souvent opérationnels qu'après plusieurs heures.

Des délais qui créent aujourd'hui un vrai manque à gagner et qui peuvent avoir des répercussions conséquentes.

Pour qu'une solution soit vraiment hautement disponible, elle doit avoir une perte de données maximale admissible nulle (PDMA (RPO)= 0) et une durée maximale d'interruption admissible nulle (DMIA (RTO)= 0). Deux conditions nécessaires, mais qui ne sont pas suffisantes.

Actuellement, de nombreuses entreprises rencontrent des difficultés avec des systèmes traditionnels s'appuyant sur des solutions Always On dédiées (des passerelles haute disponibilité) qui compliquent le processus d'administration et augmentent le coût total de possession (total cost of ownership, TCO).

L'expérience utilisateur pour les clients est également primordiale dans le contexte commercial actuel. Ainsi, lors de la mise en œuvre d'une solution Always On, il convient de réfléchir à la manière de simplifier et de configurer correctement la gestion des données pour réduire la latence.

Confrontés à de nombreux points de défaillance potentiels, les services informatiques peinent depuis des années à concevoir des infrastructures de données répondant aux exigences de disponibilité non-stop, par leur complexité et leur coût élevé.

La mise en œuvre d'une solution de ce type s'accompagne de nombreux défis informatiques dont les entreprises doivent impérativement tenir compte au moment de choisir une solution de [stockage](#), afin de déterminer d'emblée les bonnes pratiques à adopter.

Défi n° 1 : surcharge administrative et complexité accrue

Aujourd'hui, la plupart des produits sur le marché requièrent l'ajout d'une solution dédiée supplémentaire (passerelle haute disponibilité), dotée de fonctionnalités, d'outils de gestion et d'exigences de surveillance différents. L'ajout d'une solution de ce type augmente la complexité des opérations et des processus administratifs.

Le déplacement d'un LUN (numéro d'unité logique) vers une solution de réplication active-active nécessite souvent une migration totale des données et un changement de configuration complet. De plus, les tâches de gestion de données, telles que la sauvegarde et la récupération, sont effectuées dans la passerelle haute disponibilité, tandis que les tâches de gestion de la capacité sont effectuées dans le stockage sous-jacent. Les besoins d'administration s'en trouvent alors

multipliés.

Solution : en mettant en œuvre un système entièrement intégré avec des capacités de stockage en répllication active-active, les impératifs d'administration et la complexité peuvent être considérablement réduits.

Défi n° 2 : domaine d'erreur physique

Les systèmes de stockage sont toujours limités par leur emplacement physique : si un élément essentiel de l'infrastructure datacenter (électricité, réseau, WAN) tombe en panne, les données de ces baies de stockage peuvent être inaccessibles pour les hôtes, même si elles restent protégées.

Solution : toute solution destinée à résoudre ce problème doit être étendue géographiquement pour éviter la possibilité d'une panne au niveau du datacenter et ainsi limiter les conséquences de la panne.

Défi n°3 : surcoûts

Au-delà des coûts liés au stockage de deux copies des données, l'utilisation d'une solution Always On entraîne des coûts directs, puisqu'elle impose l'utilisation d'un produit dédié (passerelle haute disponibilité) ou d'une structure Fibre Channel (FC) entre les sites pour diminuer la latence.

L'acquisition d'une passerelle haute disponibilité (souvent synonyme d'achat de licence selon la capacité) et le coût continu de l'infrastructure FC créent des frictions quant à l'adoption des solutions Always On.

Solution : la meilleure manière de résoudre ce problème consiste à encourager les entreprises à étendre la protection en cessant de leur faire payer cette dernière pour un plus grand nombre d'applications. Il s'agit aussi d'utiliser des infrastructures IP rentables partagées pour plusieurs cas d'utilisation.

Si l'objectif est de réduire les coûts et de favoriser l'adoption de l'utilisation d'une solution de garantie d'accès aux données à plus grande échelle, la solution doit s'appuyer sur une infrastructure IP rentable et être entièrement intégrée dans la couche de stockage (sans utiliser un système de licence selon la capacité).

Défi n°4 : surcharge sur les performances (latence)

Dans la mesure où les données doivent traverser le WAN (qui cause la majorité de la latence de la solution), toute solution déployée dans plusieurs emplacements avec une perte de données maximale admissible nulle entraînera une surcharge supplémentaire sur les performances.

Les opérations synchrones via deux systèmes de stockage sur deux sites augmentent la latence, la multipliant généralement par deux ou plus. Quand la latence d'une application, a fortiori de plusieurs, est primordiale, alors le choix de la sécurisation des données est encore plus compliqué. Ce phénomène s'en trouve amplifié si la solution considère un ensemble de données comme local pour un site, et pas pour l'autre : lorsqu'un utilisateur travaillera sur des données à partir du site distant, les données devront traverser deux fois le WAN, ce qui augmente fortement la latence.

Solution : pour permettre à plus d'applications de bénéficier du basculement automatique, toute solution avec une PDMA nulle doit être vraiment de type « cluster de baies » et peser le moins possible sur les performances.

À cet égard, il est important de réduire la latence d'au moins un tiers du côté distant afin de favoriser l'adoption et d'améliorer l'expérience utilisateur.

Défi n° 5 : utilisation limitée à certaines applications

Les passerelles haute disponibilité sont chères et leur prix est souvent fondé sur la volumétrie à maintenir à 100% disponible. L'emploi de ces solutions est donc souvent limité aux applications considérées comme vitales pour l'entreprise. En conséquence, les applications importantes pour l'expérience client mais non vitales, doivent alors se satisfaire de solutions de reprises manuelles ou semi-automatisées.

Solution : l'impact de la solution sur les performances doit être minime afin qu'elle puisse également bénéficier aux applications de deuxième et même de troisième niveau, pour mieux protéger l'entreprise en minimisant l'incidence des pannes.

Une solution de garantie de 100% d'accès aux données doit encourager les entreprises à plus se protéger en cessant de leur faire payer la protection d'un plus grand nombre d'applications.

Défi n° 6 : fonctionnalités variables entre les copies

Les solutions qui se revendiquent 100% disponible présentent souvent des fonctionnalités très disparates. Certaines proposent une copie en lecture seule sur l'un des sites avec une fonctionnalité de basculement automatique, tandis que d'autres incluent des pénalités de performance lors de l'envoi d'accès en écriture à la copie « secondaire ». Cela complique la comparaison et le déploiement de ces solutions.

Solution : en considérant les deux copies de la même manière, avec une pénalité de performance nulle ou minimale entre les deux, les hôtes peuvent écrire des deux côtés (sur les copies véritablement actives) sans processus de basculement.

Défi n° 7 : manque de fiabilité dû à la répartition géographique

Comme toute autre solution géographiquement distribuée, les clusters Haute Disponibilité (HA : High Availability) risquent de connaître un split-brain (d'être déconnectés) et doivent pouvoir « trancher » en cas de problème de communication entre les deux systèmes.

Solution : idéalement, les entreprises doivent déployer un témoin dans un troisième site, indépendant des sites qui hébergent les deux systèmes, avec des réseaux redondants pour chaque site, pour obtenir un quorum dans le cas où les deux systèmes seraient incapables de communiquer directement. La responsabilité du fournisseur est de rendre ce témoin adapté à la méthode de déploiement privilégiée par le client – cloud ou on-premise.

Les chefs d'entreprise doivent aujourd'hui s'adapter de plus en plus vite, que ce soit pour répondre aux changements technologiques, aux nouvelles exigences des clients ou à la concurrence technologique accrue des nouveaux acteurs du marché. Diriger une entreprise dans ce contexte agité peut s'avérer difficile et coûteux. La fidélisation des clients et le développement de la clientèle sont deux aspects clés pour construire une place pérenne sur le marché.

Le coût total de possession doit être intégré à toute stratégie de disponibilité 100% dès le début, afin d'éviter que l'entreprise ne se retrouve piégée dans un plan coûteux et non viable. L'accès aux données en continu permet d'améliorer la réputation d'une entreprise, mais la capacité de cette dernière à évoluer rapidement et à adopter de nouveaux produits et services adaptés aux besoins d'une clientèle changeante lui permet de connaître une véritable croissance.

Pour cela, les entreprises doivent repenser leur approche en matière de disponibilité des données. Les jours de Disaster Recoveries sont comptés. Les entreprises modernes et agiles doivent adopter une approche plus intelligente pour continuer à satisfaire leur clientèle.