Assurer la haute disponibilité en environnement IBM Power i

7 Questions à un expert

Interview de Benoît MASSIET DU BIEST
Directeur des logiciels et services, ACMI

Si le choix d'une bonne solution de haute disponibilité est critique pour l'entreprise, il doit surtout permettre d'améliorer le niveau de service auprès des clients et aborder les évolutions futures sans contraintes ou avec des facilités nouvelles.

Dans cette Interview, Benoît Massiet du Biest, directeur des logiciels et services chez ACMI, revient sur les enjeux de la haute disponiblité en environnement IBM Power combiné à l'OS IBM i.

- Quels sont les risques à contrôler ?
- Comment identifier les objectifs de protection (RPO, RTO) ?
- Quels sont les besoins dictés par l'activité de l'entreprise ?
- La haute disponibilité est-elle encore d'actualité à l'heure du cloud ?
- Comment faire le choix d'une solution de PRA ?
- Quel partenaire pour mettre en œuvre une solution de haute disponibilité ?

La sécurité et la disponibilité des données sont des préoccupations majeures des DSI. Cette tendance est-elle en phase avec vos observations de terrain ?

Benoît MASSIET DU BIEST : Présents sur le marché depuis plus de 30 ans, nous constatons à quel point la sécurité et la disponibilité permanente des données et des applications sont des exigences de plus en plus fortes au sein des DSI. Différentes enquêtes au niveau mondial ont d'ailleurs démontré que la sécurité et la haute disponibilité sont les deux premières préoccupations des DSI.
L'engouement pour le Cloud n'a donc pas fait disparaître les enjeux autour de la haute disponibilité. Par ailleurs, le phénomène de consolidation des plateformes logicielles et matérielles engendré par la virtualisation rend les serveurs très sensibles à toute indisponibilité, qu'elle soit liée à un sinistre ou à des opérations de maintenance planifiées ou non planifiées. Durant les 20 dernières années, les applications sur Power i sont passées du « back-office » au « front-office », leur arrêt pour quelque raison que ce soit, a un impact important sur l'activité de l'entreprise et ses clients. En parallèle, les exigences des utilisateurs sont de plus en plus élevées. Au même titre qu'il est impensable pour un utilisateur de ne pouvoir accéder à ses comptes en raison d'une opération de maintenance, les entreprises ne peuvent plus se permettre d'interrompre leurs collaborateurs ou leurs clients pour des raisons de maintenance ou de sauvegardes.

> "La sécurité et la disponibilité permanente des données et des applications sont des exigences de plus en plus fortes au sein des DSI"

Une anecdote pour illustrer cette tendance : nos clients nous posent souvent la question du temps maximum acceptable de redémarrage en cas d'arrêt (RTO). Or, cette question en cache une autre, qui est celle du RPO (le Recovery Point Objective), autrement dit la quantité de données que l'organisation accepte de perdre en cas d'arrêt des services. Généralement, ce sujet du RPO n'est tout simplement

pas abordé… car la réponse implicite est zéro. Repartir sur les données de la veille et expliquer aux clients que les données et transactions sont perdues est clairement inacceptable en 2019. Pour résumer, le RPO est implicitement 0 et le RTO se situe entre quelques minutes ou quelques heures selon le type d'activité.

Quels sont les risques les plus couramment cités par vos interlocuteurs ?

Malgré les qualités de sécurité reconnues de l'architecture IBM Power et de son OS IBM i, qui en font un système résistant à la plupart des virus et attaques d'aujourd'hui sur Internet, un serveur principal est également soumis aux risques technologiques, humains et environnementaux : comme les pannes de réseaux, les inondations ou les incendies… Ce sont des risques incontrôlables qui monopolisent l'attention mais ne doivent pas faire oublier les erreurs humaines, bien plus fréquentes. Ne perdons pas de vue que 99% des arrêts ne sont pas des sinistres mais principalement des arrêts de maintenance ou des erreurs humaines.

Parmi ces erreurs humaines, il faut mentionner les actes de malveillance qui représentent 60% des cas. Il faut donc repositionner cette notion de risque dans un contexte plus global de sécurité. Il est tout simplement impossible de s'assurer que toute personne ayant accès au système avec des droits d'utilisation privilégiés ne soit pas amenée à faire un acte de malveillance.
D'où l'importance de garantir et de contrôler quoi qu'il arrive l'accès permanent aux données et aux applications. Ceci est possible aujourd'hui à l'aide de logiciels dédiés à la sécurité.

La haute disponibilité est-elle encore d'actualité à l'heure du Cloud, des solutions SaaS et de l'informatique hybride ?

Le fait de recourir à des solutions SaaS ou dans un Cloud ne règle pas pour autant la question de la continuité d'accès aux données et aux applications. Or, c'est une exigence souvent mentionnée par nos clients dans leurs cahiers des charges. Un serveur Power dans un Cloud ou sur le site d'un client a toujours les mêmes raisons de s'arrêter, d'effectuer des maintenances. Il est essentiel de pouvoir offrir une solution d'accès aux données quelles que soient les causes d'arrêt, par exemple pendant les sauvegardes des systèmes.

A titre d'exemple, dans le cadre d'un projet de PRA avec une grande banque située en Nouvelle Calédonie – qui opère la majorité des serveurs GAB et DAB de l'île – nous avons mis en œuvre des solutions permettant la consultation des données sans interruption, y compris pendant les sauvegardes complètes du système, qui ont lieu une fois par semaine. Grâce à une méthode de réplication spéciale, les utilisateurs des distributeurs et guichets automatiques peuvent continuer à consulter et agir sur leurs transactions, y compris pendant les phases de sauvegarde.

"99% des arrêts ne sont pas des sinistres mais principalement des arrêts de maintenance ou des erreurs humaines !"

Par ailleurs, ACMI est depuis 2005, un opérateur du Cloud sur IBM Power et X86 et met en place des systèmes de haute disponibilité pour ses clients hébergés. Une offre de services managés « on premise » vient compléter nos offres, avec une équipe d'une dizaine d'experts, pour la majorité, dédiés aux sujets liés à IBM Power. Cette activité est certifiée ISO 27001, à savoir le plus haut niveau de certification pour la gestion de la sécurité. Ensuite, tous les scénarios sont envisageables : partition de production on-premise et partition de secours chez ACMI, la totalité hébergée chez ACMI, ou chez le client…

"Toute restauration induit un risque important sur l'intégrité ou la cohérence des données"

Comment vos solutions sur Power i répondent-elles à cette demande accrue de sécurité et de disponibilité des données et des applications ?

La plateforme IBM i possède une caractéristique bien connue qui est sa sécurité et sa résistance aux attaques informatiques externes de tout genre. Malgré ces qualités, elle n'en reste pas moins, comme tous les serveurs, sensible aux pannes extérieures ou aux indisponibilités planifiées – ce qui justifie de faire appel à l'expertise d'ACMI.

Pour être plus précis, nos solutions de haute disponibilité consistent à dédoubler l'activité d'un serveur principal en y adjoignant un serveur de secours chargé de copier en permanence les données et les transactions effectuées sur le serveur de production. Ce deuxième serveur va disposer d'un miroir logique permanent de toutes les transactions et de toutes les données. Il servira donc à déporter les sauvegardes pour pouvoir les exécuter pendant l'activité, et permettra également d'assurer la reprise en cas d'arrêt planifié ou de sinistres en autorisant un basculement rapide sans aucune perte de données.

Les solutions de haute disponibilité se résument en un mirroring actif de systèmes qui permet un basculement à chaud vers un serveur de secours. Il s'agit d'une réplication en mode actif / passif dans la mesure où l'activité principale se situe sur un serveur qui est autorisé à lire et écrire, le serveur de secours ne faisant que recevoir les transactions et n'autorisant que la lecture des données. En cas d'arrêt, le basculement se fait en trente minutes maximum, sans perte de transaction.

Quels sont les points à prendre en compte pour faire le choix d'une solution de PRA pertinente ?

Bon nombre d'opérateurs promettent des reprises rapides avec des phases de restauration. Or, on constate que toute restauration induit un risque important sur l'intégrité ou la cohérence des données. Pour contourner ce problème, ACMI met en œuvre des solutions de haute disponibilité ne nécessitant pas un redémarrage à froid du serveur de secours. Ce dernier peut donc prendre le relai très rapidement en ayant reçu la copie des dernières transactions, ce qui permet d'assurer

la haute disponibilité en un temps record.

Pour illustrer cette solution, je citerais l'exemple d'une importante société spécialisée dans l'informatique financière et travaillant avec des banques qui opèrent sur la bourse EURONEXT. Cette société gère les transactions sur les valeurs mobilières, une activité dont le niveau de criticité atteint des sommets. Dans la première demi-heure d'ouverture de la bourse, il doit pouvoir assurer la protection des données à la transaction près, lesquelles sont estampillées au milliardième de seconde, et reprendre la main dans un délai maximal de dix minutes en cas d'arrêt.

Pour répondre à ces exigences peu communes, ACMI a mis en œuvre un PRA à chaud combiné à des mécanismes de basculement automatique. Techniquement, la solution a nécessité la mise en place d'un cluster de 6 couples de machines représentant 12 nœuds afin d'assurer une reprise à chaud sur les dernières transactions en moins de 3 minutes, sans perte de données.

"Seuls les mécanismes de réplication logicielle permettent d'assurer une reprise à chaud rapide et sans perte de données."

Pourquoi utiliser un logiciel alors qu'il existe de nombreuses solutions de réplication entre disques ou au niveau des couches de virtualisation ?

Par sa nature même, IBM i est une plateforme qui ne stocke pas toutes les données comme les autres plateformes (IBM Z, x86 en général, Windows, Linux...). Elle utilise la mémoire principale comme un cache de ses disques. Sur une plateforme IBM i, toutes les données et les dernières transactions se trouvent en mémoire. Lors d'un arrêt imprévu, si on ne récupère que les données répliquées sur disque (de baie à baie) on ne récupère qu'une partie de l'activité au moment de la panne. Les solutions basées sur de la réplication de baie exposent donc à un risque de perte de données, ou à des temps de récupération longs. En revanche les mécanismes de réplication logicielle permettent d'assurer une reprise à chaud sans perte de données, avec des temps de reprise courts.

D'où la pertinence de la solution logicielle MIMIX Availability de notre partenaire l'éditeur Precisely (anciennement Syncsort). Basée sur la journalisation, cette solution garantit à elle seule la réplication en temps réel des transactions dès leur écriture sur le serveur de production.

Quel que soit le lieu où se trouve la donnée – en mémoire ou sur disque – elle sera correctement répliquée sur le serveur de secours. Nous avons pu l'expérimenter chez un grand opérateur téléphonique utilisateur de IBM i sur Power, dans le cadre du remplacement d'une solution de réplication de baie à baie. Après un POC, cet opérateur a constaté que nous étions capables de redémarrer rapidement les systèmes sur une partition de secours, pour un ensemble d'environ 150 Tera-octets de données actives.

Quel rôle assure ACMI dans la mise en œuvre de ces solutions ?

ACMI intervient dans un premier temps pour définir l'architecture qui permettra d'atteindre les objectifs de RPO et de RTO fixés par le client. Il n'y a pas de solution idéale mais uniquement du sur-mesure.

Nous commençons généralement par protéger le serveur principal, qui représente souvent le noyau central du système. Il faut comprendre qu'un projet de haute disponibilité est un processus global et relativement long, qui commence le plus souvent par la sécurisation d'une brique principale et se poursuit par l'identification des activités et serveurs liés, point par point.

C'est pourquoi la méthodologie d'ACMI débute par un PRI (plan de reprise informatique) puis se poursuit par la définition d'un PCA (plan de continuité informatique) qui englobe l'ensemble des serveurs et implique non seulement l'informatique, mais également tout le réseau, tous les administrateurs et utilisateurs de l'entreprise afin d'instaurer à terme un cercle vertueux.

"Un projet de haute disponibilité est un processus global et relativement long, qui commence le plus souvent par la sécurisation d'une brique principale"

À propos de

Benoît MASSIET DU BIEST

Directeur des logiciels et services, ACMI

Son parcours

Benoit MASSIET du BIEST, ingénieur en Sciences et Technologies (PolyTech Paris) est spécialiste d'IBM Power i depuis 25 ans. Il dirige l'activité logiciels et service chez ACMI. Après avoir passé 15 ans chez IBM dans différentes fonctions commerciales, il développe depuis 20 ans chez ACMI l'offre logicielle sur IBM Power avec les éditeurs Precisely (anciennement Syncsort & Vision Solutions) et Carbonite (anciennement Double Take), permettant ainsi à ACMI de développer une valeur ajoutée unique autour du PRA.
Ces solutions équipent environ 500 clients qu'ils soient « on premise » ou dans un « cloud ACMI ou autre », autonomes ou accompagnés des services managés ACMI.

À propos d'ACMI

Partenaire Platinum d'IBM, ACMI est reconnu comme un acteur majeur du marché des serveurs IBM Power Systems, IBM Z, IBM Linux One et du stockage associé. ACMI est également leader sur le marché des Services managés et de la Cybersécurité.

ACMI couvre tous les composants d'une infrastructure informatique en collaborant avec les plus grands éditeurs et constructeurs mondiaux (IBM, Lenovo, Precisely, Varonis...) dont les technologies garantissent fiabilité et efficacité. ACMI assure ainsi une pérennité des solutions mises en œuvre pour ses clients.

Pour répondre aux demande croissantes de ses clients, ACMI a développé une offre d'infrastructure à la demande, le Cloud ACMI, qui fournit des ressources informatiques en mode IaaS (Infrastructure as a Service), complétée par une offre exclusive de PRAaaS (Plan de reprise d'activité as a Service) et par de nombreux services globaux d'infogérance en 24/7 à forte valeur ajoutée.

L'intégralité de l'activité Cloud & Infogérance d'ACMI, soit toute l'offre IAAS et Services Managés associés, est certifiée ISO 27001.

ACMi