

Internet : Les plans de secours informatique Ã l'heure du Cloud

Internet

PostÃ© par : JPilo

PubliÃ©e le : 11/6/2013 11:00:00

Le rÃ´le de lâ€™informatique est devenu fondamental dans les processus mÃ©tiers de lâ€™entreprise. Lâ€™interruption du fonctionnement du systÃ¨me dâ€™information a aujourdâ€™hui des consÃ©quences importantes, qui se concrÃ©tisent gÃ©nÃ©ralement par une perte nette de chiffre dâ€™affaires.

MalgrÃ© cela, prÃ¨s dâ€™un tiers des entreprises de plus de 200 salariÃ©s nâ€™ont mis aucun plan en place pour gÃ©rer la continuitÃ© de leur activitÃ©, et ceci malgrÃ© la poussÃ©e des obligations rÃ©glementaires (SOX, SSAE16, ISAE 3402, BÃ¢le II, LSF).

Pourtant, les risques sont bien rÃ©els : avec le dÃ©veloppement du BYOD, la progression du nomadisme, les attaques virales, sans oublier les catastrophes naturelles subies ces derniÃ¨res annÃ©es dans plusieurs pays, les systÃ¨mes dâ€™information (SI) sont de plus en plus exposÃ©s. Une simple panne informatique ou de rÃ©seau peut affecter sÃ©rieusement la disponibilitÃ© du SI.

En dehors des grands groupes et des activitÃ©s soumises Ã des contraintes rÃ©glementaires fortes, les entreprises sont souvent freinÃ©es par le coÃ»t non nÃ©gligeable de la mise en place dâ€™un Plan de Reprise dâ€™ActivitÃ© (PRA) ou dâ€™un Plan de ContinuitÃ© dâ€™ActivitÃ© (PCA). Mais des solutions existent pour adapter le dispositif au risque encouru, avec des coÃ»ts optimisÃ©s, en profitant notamment du Cloud.



Quantifier le risque

Le coÃ»t dâ€™un plan de secours, quâ€™il sâ€™agisse dâ€™un PRA ou dâ€™un PCA, doit Ãªtre mis en regard du coÃ»t des dommages subis lors dâ€™un sinistre, jusquâ€™au retour Ã lâ€™Ã©tat nominal. Il ne faut pas oublier de regarder aussi les consÃ©quences indirectes sur le revenu et sur la dÃ©gradation de lâ€™image de lâ€™entreprise suite au temps perdu et Ã lâ€™interruption de services critiques tels que logistiques, financiers. Pour quantifier ces dommages potentiels et choisir le plan le mieux adaptÃ©, la premiÃ¨re Ã©tape est de recenser les applications ou domaines les plus critiques, dont lâ€™impact est le plus important sur lâ€™activitÃ© de lâ€™entreprise.

Prenons le cas, par exemple, de la plateforme e-commerce d'une entreprise, grande ou petite. Le risque est facilement quantifiable : il s'agit de la perte de chiffre d'affaires générée par l'interruption de services, à laquelle s'ajoute le dommage subi par la marque (une interruption trop longue décourage les internautes de revenir sur le site).

Plusieurs solutions s'offrent à elle pour répondre aux effets d'une interruption de services :

Externaliser sur une plateforme redondante

Généralement, l'entreprise externalise sa plateforme chez un hébergeur, dans un DataCenter pour bénéficier d'un environnement technique à l'état de l'art ainsi que de connexion performante à Internet. Ceci permet également de comparer une plateforme « ouverte » avec d'autres systèmes internes de l'entreprise.

Au-delà du risque de perte de données, il est important de définir le temps de rétablissement du service, RTO (Recovery Time Objective) qui peut être différent selon la criticité (2h, 4h ou 24h). Le premier élément est donc de disposer d'une architecture redondante au sein du DataCenter primaire et, en cas d'interruption, de pouvoir restaurer rapidement l'environnement et les données.

Envisager la virtualisation et les architectures hybrides

La virtualisation est une solution à envisager : plus grande est la part virtualisée de votre plateforme, plus vous pouvez bénéficier de la haute disponibilité du Cloud. Avec l'économie réalisée, vous pouvez augmenter la résilience de la part non virtualisable de votre plateforme. Vous obtenez une architecture hybride composée de Cloud, d'éléments dédiés et d'une interconnexion réseau performante : c'est le Cloud Hybride ou « Hybrid Cloud ».

Le Cloud permet de bénéficier d'une mise à disposition de la puissance non utilisée pour d'autres machines virtuelles et donc d'augmenter le ROI de la plateforme.

Plan de Secours en mode actif/passif

Si le coût d'une interruption de services est élevé, il faut alors envisager un plan de secours mobilisant deux DataCenters, en mode actif/passif ou voire même atteindre un mode actif/actif, où la résilience est plus élevée et si l'application supporte un tel dispositif.

En mode actif/passif, le mode de répliquage des données est, en général, asynchrone. Une attention particulière devra être portée sur le système de répliquage afin de prendre éventuellement en compte une éventuelle dégradation des solutions de stockages.

Si le client souhaite limiter la perte des données il est possible de mettre en place une répliquage synchrone même en architecture active et passive.

A titre d'exemple, NTT Communications choisit le DataCenter de secours approprié (en France, en Europe ou dans le monde) en fonction du RPO (Recovery Point Objective) défini avec le client et de la technologie de stockage choisie.

Le plan de secours sera d'autant plus facile et économique, que la part du Cloud privé virtuel sera importante. En effet, le Cloud permet d'ajuster les coûts aux ressources réellement nécessaires. Ainsi, lorsque ce plan se déclenche, il est possible d'activer très rapidement davantage de ressources, pour prendre en compte l'augmentation de charge. L'intérêt est de pouvoir ajuster la puissance du système en quelques clics.

En mode actif/passif, nous faisons face au problÃme de lâinformatique Â« dormante Â» : le cÃtÃ passif â i.e. la plateforme de secours en attente - doit Ãtre diminuÃe au maximum, ou alors on doit veiller Ã lâutiliser Ã un autre usage, en rÃgime normal, comme la prÃ-production.

Profiter des plateformes de prÃ-production

En effet, pour les plateformes en production vitales (e-commerce, ERP, etc.), les nouvelles versions des sites ne peuvent plus Ãtre publiÃes directement. Des environnements sont utilisÃs, pour tester et valider les nouvelles versions avant leur mise en production. Ce systÃme, appelÃ plateforme de prÃ-production, peut Ãtre hÃbergÃ sur un autre DataCenter. Or, ces plateformes de prÃ-production ne sont pas critiques â puisqu'elles ne jouent pas de rÃle opÃrationnel.

Une astuce est donc d'attribuer Ã ces plateformes un double rÃle : celui de plateforme de prÃ-production et celui de plateforme de secours. GrÃce aux techniques au Cloud, et Ã des procÃdures bien rÃdÃes, il est possible, en cas de sinistre, de transformer rapidement la plateforme de prÃ-production en plateforme de secours, le temps de remettre en service le systÃme principal.

Pour pousser plus loin lâexercice, il est possible de mettre sur deux DataCenters diffÃrents, deux plateformes de production correspondant Ã deux applications diffÃrentes de telle maniÃre Ã ce qu'une plateforme puisse accueillir lâautre.

Plan de secours en mode Actif/Actif

En effet, si lâimpact Ãconomique d'un arrÃt de la disponibilitÃ de la plateforme est encore plus important, il faut envisager de mettre en place une double-plateforme, rÃpartie sur deux DataCenters en mode actif/actif. Les deux plateformes restent continuellement actives et le trafic est alors rÃparti sur les deux centres en permanence. Bien entendu, des contraintes supplÃmentaires apparaissent :

le dimensionnement est calculÃ de faÃon Ã ce que les deux plateformes puissent, en cas de sinistre, accueillir le trafic du DataCenter indisponible,

Un systÃme d'Ãquilibrage de charge global doit Ãtre mis en place entre les deux sites,

la rÃplication des bases de donnÃes entre les deux DataCenters doit se faire en quasi-temps rÃel. La mise en place d'un lien haut-dÃbit Ã latence faible entre les deux centres est nÃcessaire. La distance peut atteindre aujourd'hui 100 km.

La gestion des sinistres au cÃur de lâADN du groupe NTT

En tant qu'entreprise japonaise, NTT est particuliÃrement sensible aux risques majeurs qui peuvent affecter les rÃseaux et les systÃmes d'information. Les dispositifs existants ont fait leurs preuves notamment lors du tremblement de terre de 2011. Le PCA mis en place mondialement depuis de nombreuses annÃes a permis de limiter fortement les consÃquences de cette catastrophe sur les services proposÃs par lâopÃrateur, en mobilisant notamment prÃs de 5 000 personnes pour activer les solutions de secours et garantir la continuitÃ de services.

Une nouvelle Ãre

La virtualisation et les technologies de Cloud ont changÃ la donne car la virtualisation simplifie considÃrablement la tÃche de crÃation d'images miroir des serveurs critiques, et de

duplication des donnÃ©es sur un autre lieu. Certains Cloud PrivÃ© Virtuel, comme Enterprise Cloud chez NTT, offre des services automatiques de rÃ©plication de donnÃ©es entre un DataCenter du Cloud et un autre. Cette option Ã« Global Data Back-Up Ã» est gÃ©rÃ©e par le client et ne mobilise qu'un nombre minimal de ressources : du stockage et de la bande passante, facturÃ©e Ã la minute prÃ©s, pour l'interconnexion entre les deux DataCenter.

Ainsi, grÃ¢ce au Cloud, les plans de continuitÃ© de services qui n'Ã©taient accessibles qu'aux seules grandes entreprises, peuvent Ãªtre proposÃ©s d'Ã©ormais aux entreprises de toute taille, conclue **Samuel Charles**, responsable Architecture et Support chez [NTT Communications](#), France, travaille depuis plus de 10 ans au sein de NTT pour amÃ©liorer pro-activement les plateformes des clients.