Les plans de continuité informatique des cloud à l'épreuve de l'ouragan Sandy

Yannick Neff | Consultant

Les plans de continuité informatique des cloud à l'épreuve de l'ouragan Sandy

[Article rédigé en collaboration avec Pierre Debussche & Arsene Lizo]

Quand l'ouragan « Katrina » a frappé la Côte du Golf des États-Unis, en Août 2005, ravageant une bonne partie de l'infrastructure de télécommunications, seule une poignée de datacenters a pu tenir le choc. « Katrina » n'a pas seulement anéanti ces centres de données, mais a également mis en défaut un nombre important de plans de continuité informatique (PCI).

Des sinistres de cette ampleur ont permis d'alerter les DSI sur leur exposition face aux risques naturels. La régularité et la violence de ces évènements climatiques ont poussé les entreprises à prendre des mesures pour faire face à de futures tempêtes de la dimension de «Sandy». Les leçons du passé ont-elles pour autant été retenues ? Ont-elles toutes réussi ce test grandeur nature ? si oui, comment y sont- elles parvenues ?

Les conséquences de l'ouragan « Sandy »

Annoncé comme une catastrophe majeure dans l'histoire des États-Unis, l'ouragan « Sandy » a capté l'attention de la plupart des DSI des acteurs économiques de la côte Est qui ont mobilisé leurs efforts pour déclencher leurs plans de continuité informatique. Ces PCI, mis à niveau depuis les attentats du 11 Septembre 2001, sont fondés notamment sur des procédés de géo-réplication.

Les acteurs du web et plus largement du marché du cloud sont plus enclins à communiquer sur leur capacité de reprise et à faire des retours sur les incidents subis que les entreprises traditionnelles. Les informations disponibles proviennent donc essentiellement de ces acteurs.

De nombreuses pannes d'électricité causées par la tempête, ont entraîné une indisponibilité partielle ou totale de services (Huffington Post, Gawker, Cafemon, Gizmodo, Buzzfeed, etc.) dans bon nombre de datacenters. Les hébergeurs et fournisseurs de services cloud **Datagram** et **75 Broad** ont été indisponibles à causes d'inondations ou réserves insuffisantes de carburant pour le fonctionnement des groupes électrogènes.

« Sandy » a ainsi rendu apparente la vulnérabilité des nombreux datacenters présents dans cette zone (New York, New Jersey, et Virginie) des États-Unis. En effet, plusieurs centres de données géo-répliqués n'étaient distants que d'une centaine de kilomètres (150 datacenters) et donc dans le rayon d'impact de Sandy.

Ces dysfonctionnements mettent en exergue la nécessité, même pour des PCI bien pensés comme ceux de Wall Street, d'être mis à l'épreuve dans des conditions proches de la réalité, avant d'être jugés comme fiables.

Les plans de continuité informatique des cloud à l'épreuve de l'ouragan Sandy

Des PCI à l'épreuve des ouragans

Certains opérateurs de datacenter, comme **Telx**, ont résisté à Sandy car ils avaient appliqué précédemment des tests simulant jusqu'au bout un sinistre. Par cette initiative, Telx a pu identifier certaines insuffisances dans son PCI comme la surchauffe de ses générateurs en mode dégradé et a donc pu limiter l'impact de Sandy.

Un cas d'école est celui de Buzzfeed qui, malgré le crash de Datagram qui hébergeait ses serveurs primaires, a réussi à réduire considérablement le temps d'indisponibilité de ses services. Cette réussite s'explique par :

- la mise en cache de la plupart de ses pages chez Akamai, le gestionnaire et diffuseur de contenu
- l'hébergement dans un second datacenter des données répliquées en temps réel.

La réplication de ces données a permis le rétablissement des services de Buzzfeed chez Amazon Web services (AWS). Quelques heures ont suffi pour assurer la migration complète des données vers AWS et ainsi basculer leur service sur les infrastructures d'Amazon. Cet exploit est à relativiser car il a nécessité la configuration manuelle d'une bonne partie du socle technique de Buzzfeed et reste donc peu applicable en l'état à un SI complexe.

Les leçons de « Sandy »

Chaque incident majeur est une façon pour les Grands Comptes d'apprendre par le réel et d'anticiper les futures catastrophes. Au-delà d'une stratégie multi-datacenters, Sandy a mis en exergue la nécessité d'anticiper, de tester et d'adapter le PCI.

Elle a aussi révélé le cloud comme une alternative envisageable pour réaliser un PCI. Alternative que les offreurs cloud commencent à mettre en avant par le biais de leurs offres packagées de Disaster Recovery As A Service.

Les entreprises européennes et notamment françaises, qui ont moins l'occasion de mettre à l'épreuve de la réalité leur PCI, devraient néanmoins s'inspirer des retours d'expériences plus nombreux acquis par les américains. D'autant plus que les hébergeurs de cloud ne rechignent pas à communiquer sur leur stratégie PCI gagnante afin d'en faire un argument marketing. En effet, même si moins fréquentes, l'Europe n'est pas à l'abri de catastrophes équivalentes en termes d'impact à « Sandy ».