MYTHES ET LEGENDES DES SERVICES DE CLOUD COMPUTING

Jean-Marc Gremy

INTRODUCTION

Ce document est un extrait du livre collectif "Mythes et légendes des TIC" développé dans le cadre de l'association Forum ATENA.

Si vous désirez obtenir la version complète PDF la plus récente du livre "Mythes et légendes des TIC", il est téléchargeable en :
http://www.forumatena.org/LB47/MythesEtLegendesDesTIC1605.pdf

Si vous désirez commander la version papier c'est sur :
http://www.lulu.com/product/couverture-souple/mythes-l%C3%A9gendes-des-tic/15739496

Si vous êtes intéressés d'être tenus au courant de ses développements, voire si vous désirez en devenir un des auteurs, demandez le moi par e-mail.

Gérard Peliks
gerard.peliks@cassidian.com
Président de l'atelier sécurité de Forum ATENA

MYTHES ET LEGENDES DES SERVICES DE CLOUD

Jean-Marc Grémy, Cabestan Consultants

MYTHE N° 1 :
CELA FAIT DEJA 30 ANS QUE NOUS FAISONS DU CLOUD COMPUTING !

Non ! La définition des services de Cloud Computing est complètement en opposition avec cette idée. Depuis 30 ans nous externalisons la fonction Informatique chez des tiers (les tant redoutés contrat de *Facility Management* des années 90) ou nous optons pour l'hébergement de systèmes dans des Datacenter. Dans le premier cas on mutualise les ressources humaines, dans le second cas les infrastructures physiques (bâtiment, énergie, accès télécoms…). Mais en aucun cas nous avons mutualisé sur la même machine des applications, des systèmes d'exploitation divers appartenant soit au prestataire de Cloud dans le cas du IaaS soit au client final dans le cadre du PaaS.

Peut-être le seul cas rencontré jusqu'ici est celui de l'hébergement des sites Web institutionnels des entreprises. Ils étaient hébergés, souvent pour des questions de couts, sur une machine physique avec des instances du service Web. Ainsi une même machine pouvait supporter plusieurs sites web de différentes entités juridiques. Dans ce contexte l'hébergeur garantissait l'exploitation du système, la disponibilité des infrastructures d'accès (souvent le seul réseau Internet) ainsi que la sauvegarde des données applicatives.

La définition[1] du Cloud impose l'idée du partage de ressources et de la colocation de systèmes. A elle seule cette définition exclue les modèles que nous avions construit jusque là. Une machine, un service, un propriétaire.

Le Cloud Computing a ceci de particulier qu'il propose à travers ces différentes architectures[2] une évolutivité des implémentations : de la machine dédiée (hardware) à l'application en passant par des OS dédiés, des bases de données dédiées… sur des machines partagées. Le service suivant la même logique : exploitation du hardware uniquement jusqu'à l'exploitation de l'application et ses données en passant par l'exploitation unique d'une instance de l'OS.

Pour comprendre les évolutions et les possibilités de la technologie, projetons-nous en avant pour en voir l'évolution. Si nous repartons de l'idée de payer en fonction des besoins (i.e. *pay as you grow*) ne pourrions nous pas imaginer que cette seule assertion prédit la fin des serveurs informatiques dans nos Datacenter privés ? L'idée serait que finalement nous pourrions ne plus avoir de systèmes mais uniquement des unités d'œuvre de calcul chez un opérateur de service. En fonction des besoins, du moment de notre activité, de sa saisonnalité, nous aurions plus ou moins de capacité de calcul. L'institut d'étude IDC prédit un marché mondial du Cloud Computing en 2013 à une valeur de $45mds ; le prix d'une machine virtuelle étant inférieur à $1 chez certain opérateur, le nombre possible de machines avec $45mds est vertigineux.

[1] *NIST : National Institute of Standards and Technology. Agence du Department of Commerce Américain.*

[2] *Voir* Mythes et Légendes des systèmes de Cloud

Pour mettre en perspective les définitions des architectures de Cloud, et pour donner quelques repères au lecteur, nous pouvons illustrer la définition que nous avons donnée avec les offres[3] suivantes :

- Software aaS (SalesForce, GoogleApps...)
- Platform aaS (Force.com, Google App Eng, Microsoft Azur...)
- Infrastructure aaS (Amazon EC2, Microsoft Azur...)

Alors si les constructeurs de serveurs vont se positionner, qu'en est-il des opérateurs télécoms et Internet ? Leur légitimité est tout aussi importante que les constructeurs, si ces derniers ont la puissance de calcul, les opérateurs disposent du transport. Mariage de raison ou prise de pouvoir ? L'histoire le dira…

Si on ne sait pas qui sera demain le grand gagnant de cette « nouvelle vague », une chose est sûre, cela fait 30 ans que l'on se prépare à l'arrivée du Cloud.

MYTHE N° 2 :
LE CLOUD COMPUTING C'EST UTILISER DES INFRASTRUCTURES VIRTUALISEES.

Oui, c'est le principe fondateur ! Quand Harry rencontre Sally, ou quand la technologie rend possible des choses qui ne l'étaient pas ou très peu autrefois. Mais qui dit "virtualisation" ne dit pas nécessairement "éditeur unique". Il existe aujourd'hui plusieurs offres sur lesquelles l'entreprise peut s'appuyer pour bâtir son propre Cloud Privé. Les critères de choix sont multiples : évolutivité (élasticité pour certain), sécurité, exploitabilité, interopérabilité…

La différence essentielle avec la virtualisation proposée par les grands systèmes, depuis maintenant plusieurs années, réside dans le fait que l'on peut toujours cloisonner des instances de systèmes d'exploitation, mais ces derniers peuvent être de nature différente : Windows™, Linux™, Mac OS™…

Cette définition de la virtualisation et son association aux offres de Cloud Computing sont essentielles. C'est en partie pour ce point que le Mythe n°1 est en opposition avec l'idée d'une existence ancienne du Cloud. La virtualisation est le moteur économique et technique du Cloud. Elle représente à elle seule l'idée du Cloud. Les instances applicatives sont mutualisées sur des équipements physiques communs. Sans ce partage de ressources techniques, il n'y a pas de Cloud.

La dimension économique de la virtualisation est avant tout liée à la capacité de la technologie à proposer une agilité de l'entreprise à pouvoir déployer à la demande son informatique : des serveurs à la demande aux postes de travail à la demande l'ensemble de la chaîne technique peut-être virtualisé. L'avantage de la virtualisation est la capacité qu'elle offre de permettre une instanciation rapide et facile d'une machine (au sens système d'exploitation). Dans certains cas de figure cette idée, poussée à son extrême, permet de mettre en place des plans de contingence informatique jusque là réservés aux grandes entreprises. Comment ? Redémarrer sur un autre site physique le serveur logique qui aura été préalablement sauvegardé. Dans des temps record de restitution.

Mais attention à ne pas faire trop de raccourci ou définir les services de la virtualisation, sa souplesse, son évolutivité et sa sécurité à la seule offre d'un éditeur, fut'il le « *best-of-breed* ». Ne pas recréer un « frigidaire » de la virtualisation.

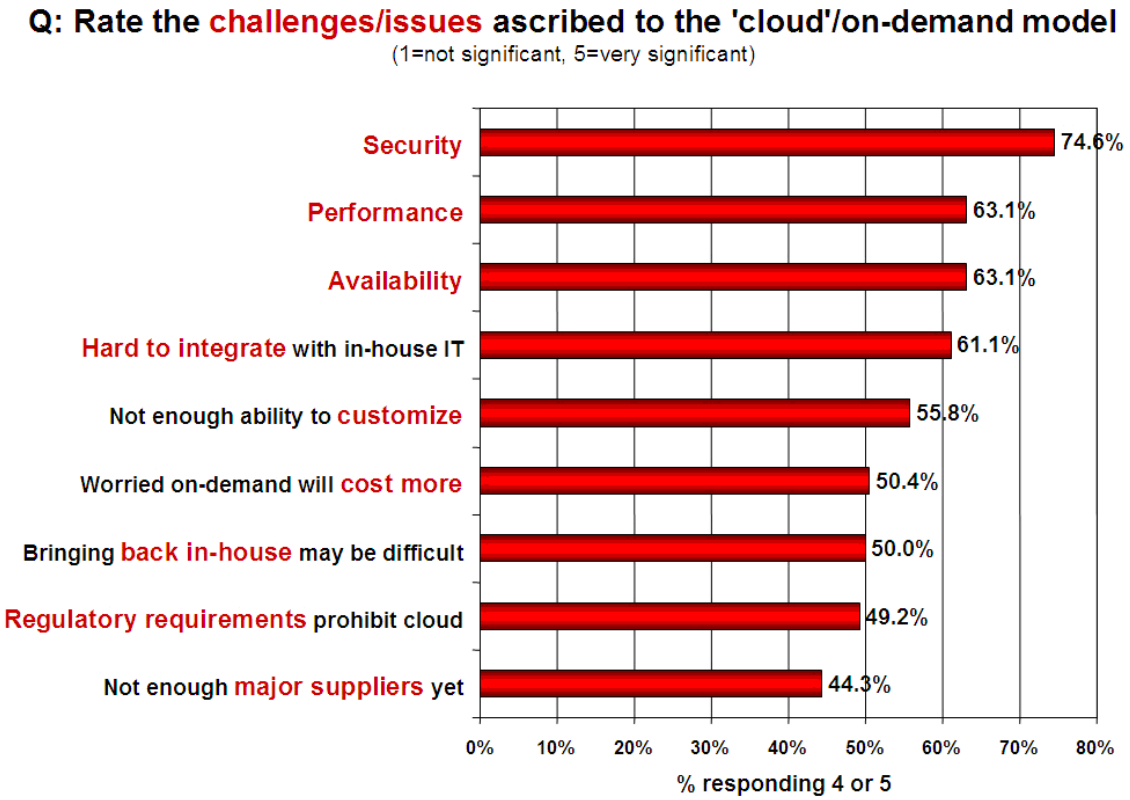
[3] *Les produits commerciaux énoncés restent la propriété de leurs ayants droit, cette liste ne saurait être exhaustive en termes de définition d'offre et d'appellation.*

MYTHE N° 3 :
LES OFFRES DE SERVICES DU CLOUD COMPUTING NE PROPOSENT PAS DE SECURITE LOGIQUE

Nous n'aborderons pas dans ces pages la question de la sécurité physique. On présume, peut-être à tord, qu'elle fait partie des fondations des offres de services ; notamment pour la couverture des risques.

Pour faire écho à ce point et pour conserver une vision impartiale de tout constructeur/offreur de service, nous appuierons notre développement de la sécurité des offres de Cloud sur les travaux communs : de la *Cloud Security Alliance*[4], de l'*European Networks and Information Security Agency*[5] ainsi que sur les premiers travaux de *l'Open Datacenter alliance*[6].

Cela étant posé, revenons à la sécurité logique. Pour développer ce point, quelques chiffres issus d'une étude publiée en 2008 par le cabinet d'étude IDC :



Source: IDC Enterprise Panel, August 2008 n=244

Sur le podium des préoccupations du panel ressort la sécurité à la première et troisième place. On pourrait, dans une certaine mesure, associer la performance à la sécurité mais nous ne développerons pas ce point ici.

Quelle différence peut faire l'interviewé entre sécurité et disponibilité ? Dans les critères fondamentaux de la sécurité, on a l'habitude de discerner la **disponibilité**, de la **confidentialité** et de l'**intégrité**. Donc dans cette étude, l'aversion au risque de perte des

[4] *CSA : www.csa.org.*

[5] *ENISA : www.enisa.europa.eu*

[6] *Open Datacenter Alliance : www.opendatacenteralliance.org.*

services est telle que cette préoccupation ressort telle quelle. Dont acte. Nous reviendrons sur ce point dans le mythe suivant.

La sécurité, l'intégrité des données et leur confidentialité sont donc la préoccupation majeure. Par habitude, nous pouvons même penser que par sécurité, le panel devait penser au seul critère de confidentialité.

MYTHE N° 4 :
SI JE CHANGE DE PRESTATAIRE DE CLOUD, JE NE POURRAI PAS RECUPERER LES INFORMATIONS QUE JE LUI AI CONFIEES

Il est évident que les données confiées sont récupérables. Mais attention, là encore la plus grande prudence est à observer quant aux capacités réelles de les récupérer. L'entreprise doit tout d'abord considérer deux points :

- le volume de ses données stockées. A lui seul ce paramètre constitue l'élément de la faisabilité, nous reviendrons dessus dans le prochain Mythe,
- la possibilité technique de l'offre de Cloud.

Cette question importante, qui fait appel à un concept sous-jacent, quelle est ma possibilité réelle de changer de prestataire ? L'idée ici est de mettre en perspective les situations dans lesquelles les entreprises auront cloudisées des penta octets de données. Comment les transférer vers un autre opérateur de cloud ? Nous considérons l'opérateur de Cloud dans le cas des offres de service de type IaaS ou PaaS. Dans le cas du SaaS, la question est plus simple et peut-être plus complexe qu'il n'y paraît. Nous reviendrons sur ce cas, ultérieurement.

Pour faire écho à cette possibilité technique, qui de toute façon doit prendre une forme quelconque, l'évolution des offres de Cloud verra peut-être arriver des opérateurs de stockage qui fourniront leur service aux opérateurs commerciaux (Paas ou SaaS). De telle sorte que les données n'aient plus à être « techniquement récupérées ».

MYTHE N° 4 BIS :
QUAND JE DEMANDE UNE SUPPRESSION DE FICHIER, OU DE L'ENSEMBLE DE MON INFORMATION NOTAMMENT QUAND JE CHANGE DE PRESTATAIRE, LES FICHIERS ET ENREGISTREMENTS SERONT SUPPRIMES

Si la possibilité technique de récupérer ses données nous est donnée par les éléments à vérifier sur l'offre de service telle que nous l'avons abordée précédemment, le point est maintenant tout autre, quelle est la rémanence des données chez le prestataire ?

L'essence même du Cloud n'est elle pas de garantir en tout lieu (de la planète Internet), à tout moment l'accès à ces données ? Encore un point pour lequel la réponse n'est ni triviale ni définitive.

Elle n'est pas triviale, car elle dépend de l'offre de service.

MYTHE N° 5 :
LE PRESTATAIRE A UN ACCES COMPLET A MES APPLICATIONS ET MES DONNEES QU'IL HEBERGE

On attend une certification de Qualité de la sécurité dédiée aux offres de Cloud. Aurons-nous des approches de certification de la gestion de la sécurité de l'information, à l'instar des processus de certification ISO/IEC 27001 ? Le cadre normatif a développé des normes de bonnes pratiques à destination des professionnels de santé (ISO 27799), des professionnels

des télécoms (ISO 27011)… Auront-ils demain une démarche identique dans le Cloud ou pouvons nous appliquer les modèles de certification existant ?

Pour fermer ce point sur la certification des services, nous rappellerons la philosophie de la démarche de certification : apporter la confiance aux tiers. Cette confiance permet aussi au prestataire de s'assurer qu'il suit bien, au-delà de l'état de l'art, les attentes et les prérequis. Cette confiance lui est donc aussi destinée.

MYTHE N° 6 :

AVEC UN SERVICE DE CLOUD COMPUTING JE N'AI PLUS BESOIN DE ME PREOCCUPER DE MA SECURITE, NOTAMMENT DE LA DISPONIBILITE DES SERVICES

La question de la disponibilité est un point essentiel du Cloud. Observons-la sur deux axes :

Le premier celui de l'ubiquité des données. En effet, l'idée sous-tendue par les différentes offres de Cloud (rappel sur la définition du NIST) est que les machines virtuelles dans le cas du IaaS, les systèmes d'exploitation et applications de base dans le cas des PaaS ou des applications et leurs données dans le cas des SaaS sont en permanence disponibles, et ce, où que vous vous trouviez sur le globe.

Mais dans la réalité est-ce vrai ? Comment être sûr du respect de ce postulat ?

Si nous tenons compte des contraintes légales (lois et réglementations) dans certain cas de figures, les données doivent être stockées dans des localisations bien précises : en France, en Europe, les sites doivent être auditables. Dans ce contexte, la logique de Cloud et la disponibilité qu'il offre sont à revoir, si l'on imaginait que la disponibilité était implicitement garantie.

Le second point trop souvent ignoré est la résilience du réseau, donc cela nous ramène à la part que joueront demain les opérateurs. Mais deux écoles existent :

- L'opérateur disposant de son propre réseau est en mesure d'en assurer la continuité. Au détail prés que la quasi totalité des opérateurs utilise les services d'autres opérateurs pour améliorer la capillarité de leur réseau, les performances, la disponibilité. Dans ce cas une défaillance de l'opérateur du contrat serait potentiellement un problème
- La connexion aux services du Cloud se fait par Internet. Et dans ce cas on considère le réseau techniquement suffisamment résilient pour prendre en compte la majeure partie des problèmes à assurer tout le temps et en tout point

D'ailleurs, cette question de la disponibilité de l'information n'est pas très éloignée de celle de l'Intégrité de l'information. Un défaut d'intégrité d'une information peut avoir comme conséquence directe la perte de la disponibilité. Attention à ce point, lorsque par exemple, l'entreprise déploie des outils de cryptographie sans maîtrise de l'outil, de recouvrement voire de séquestre des clés de chiffrement… L'information est semble t'il disponible mais inaccessible par la transformation opérée par le chiffrement.

A PROPOS DE L'AUTEUR

Après une formation initiale militaire dans la Marine Nationale, **Jean-Marc GREMY** débute sa carrière civile au sein de la R&D d'Alcatel Business Systems puis se tourne rapidement vers les Systèmes d'Information et de télécommunication au sein d'Alcatel puis du Groupe Synthélabo.

Entrepreneur, il participe en 1997 à l'éclosion de Cyber Networks et fonde en 2002 Ipelium. Fort de cette expérience réussie de 18 années dans la technologie, le management et l'entreprenariat, il créé en 2007 un cabinet de conseil indépendant CABESTAN CONSULTANTS. Résolument tourné vers le conseil et la formation, pour laquelle il est instructeur européen pour le cursus CISSP® et Conférencier pour le Centre de Formation de l'ANSSI (le CFSSI).

philippe (at) vocalexpo.com