Smals

Concept vaporeux ou réelle innovation ?

Cloud computing

Gestions des Clients

Section Recherches

Date : mars 2011
Deliverable : 2011/TRIM1/03
Statut : final
Auteurs : Johan Loeckx
Grégory Ogonowski

Fonsnylaan 20
1060 Brussel

Avenue Fonsny 20
1060 Bruxelles

Tel : 02/787.57.11
Fax : 02/511.12.42

Management Summary

Le cloud computing a été le hype informatique de l'année 2010. Derrière ce terme un peu flou se cachent des concepts déjà connus tels que la virtualisation et l'externalisation des données.

Durant les derniers mois, les offres se sont multipliées et quasiment tous les acteurs majeurs de l'informatique proposent des solutions dans le cloud. Les petits acteurs proposent également des solutions dans le cloud en utilisant parfois les ressources matérielles mises à disposition par les géants de l'informatique que sont Amazon, Google ou Microsoft.

Le cloud existe sous plusieurs formes : on parle de cloud privé lorsque l'on mutualise les ressources de l'entreprise (au moyen de la virtualisation) et l'on parle de cloud public lorsque les données vont être placées directement chez le fournisseur. Cette dernière option suscite de nombreuses craintes légitimes, mais parfois également mal ciblées. Il ne faut pas perdre de vue que la sécurité est un enjeu majeur pour le fournisseur de services : il y va de sa crédibilité et un gros manquement pourrait s'avérer fatal. Garantir la confidentialité des données dans le cloud constitue un réel défi dans un monde où tous les grands noms de l'informatique sont américains. En effet, une loi américaine du nom de Patriot Act donne les pleins pouvoirs aux services secrets américains qui peuvent saisir du matériel dans les entreprises basées aux Etats-Unis sans en donner la raison. La seule parade pour les fournisseurs consiste à construire des centres de données en dehors des Etats-Unis pour ne plus être sous la juridiction de cette loi très contraignante.

Il existe une classification des services que l'on retrouve dans le cloud. Le type de service le plus populaire actuellement est le SaaS, qui consiste à mettre à disposition une application web prête à l'emploi et directement utilisable dès que le mode de paiement a pu être validé. La popularité de ces solutions vient de leur très faible coût d'entrée et de la rapidité de mise à disposition des utilisateurs. De plus, ces solutions s'avèrent généralement moins coûteuses que les applications traditionnelles, ne nécessitent pas de personnel technique pour la maintenance (aucun serveur à gérer) et il n'y a jamais de mise à jour à réaliser (les nouvelles fonctionnalités apparaissent progressivement).

S'il est facile de rentrer dans le cloud, en sortir est une opération plus délicate. Le cloud peut être utilisé sans trop de danger pour répondre à un besoin ponctuel, il sera probablement plus efficace et moins coûteux qu'une solution traditionnelle. Pour un usage à long terme, diverses précautions sont à prendre sous peine de ne plus maîtriser l'évolution des coûts. Quoi qu'il en soit, le cloud présente de nombreux avantages et mérite que l'on s'y intéresse : que ce soit pour les PME, les grandes entreprises ou le secteur public, il y a des opportunités à saisir dans le cloud (que ce soit en tant qu'acteur ou consommateur).

Table des matières

Management Summary 2

But et structure du document 5

1. Introduction 6

1.1. Le hype de l'année 2010 6
1.2. Caractéristiques du cloud 7
1.3. Qui et que retrouve-t-on derrière le cloud ? 8
1.4. Types de cloud 9
1.4.1. Aspects organisationnels 9
1.4.2. Niveaux d'abstraction 10

2. Analyse critique du cloud 12

2.1. Avantages 12
2.1.1. Scalabilité 12
2.1.2. Efficacité 12
2.1.3. Orientation service 13
2.1.4. Flexibilité & maniabilité 13
2.1.5. Pas de CapEx 13
2.2. Obstacles 13
2.2.1. Sécurité & vie privée 14
2.2.2. Fiabilité 14
2.2.3. Compliance 16
2.2.4. Processus, organisation & intégration 16
2.2.5. Portabilité 18
2.2.6. Modèle de prix 19
2.2.7. Facteur humain 20

3. Sécurité 21

3.1. Attaques externes 21
3.2. Attaques internes 22
3.3. Patriot Act 23
3.4. Recommandations et solutions des fournisseurs 24

4. Gestion des coûts 26

4.1. Pourquoi certains services dans le cloud sont-ils si bon marché ? 26
4.2. Réduire les coûts grâce au cloud computing 26
4.2.1. Augmenter l'efficacité 27
4.2.2. Mettre l'accent sur les activités clés 27
4.3. Coûts cachés 28
4.3.1. Administration 29
4.3.2. Intégration 29
4.3.3. Migration 29
4.3.4. Licences 29
4.4. Conclusion 30

5. Marché 31

5.1. Infrastructure as a Service (IaaS) 31
5.1.1. Public 31
5.1.2. Privé 33
5.2. Platform as a Service (PaaS) 35
5.2.1. Public 35
5.2.2. Privé 36
5.3. Software as a Service (SaaS) 37
5.3.1. Public 37
5.3.2. Privé 38
5.4. Tableau récapitulatif 39
5.5. Exemples d'utilisation 40
5.5.1. Secteur privé 40
5.5.2. Secteur public 41

6. Use cases, recommandations & checklist 43

6.1. Use cases 43
6.1.1. Introduction 43
6.1.2. Cloud public 44
6.1.3. Cloud privé 45
6.2. Recommandations 46
6.3. Checklist 47
6.3.1. Business case 47
6.3.2. Compliance 47
6.3.3. Économique 48
6.3.4. Intégration 48
6.3.5. Technique 48
6.3.6. Sécurité 48
6.3.7. Organisationnel 49

7. Conclusion 50

8. Bibliographie 53

9. Glossaire 56

But et structure du document

Le cloud computing a été un sujet très débattu en 2010 dans la presse informatique. Le sujet est très vaste et il n'est pas forcément trivial d'en saisir les principaux concepts. Ce rapport a donc pour objectif de présenter au lecteur les principaux concepts du cloud computing et de donner un avis le plus impartial possible sur cette thématique parfois abordée de manière trop commerciale dans la presse.

Dans le premier chapitre, les concepts de base du cloud computing ainsi que les différents types de cloud seront décrits. Le second chapitre apportera une analyse critique du cloud : quels en sont les avantages et inconvénients réels.

Le cloud computing implique la mutualisation des ressources. Le cloud peut être privé ou public. Lorsqu'il est public, cela signifie que les données des utilisateurs seront stockées et manipulées en dehors de l'entreprise. Il est donc tout à fait légitime de s'interroger sur la sécurité des données. Actuellement, la sécurité est d'ailleurs le principal frein à l'adoption du cloud. Le troisième chapitre se focalisera donc sur ce point afin de déterminer quels sont les risques réels et quelles sont les précautions à prendre.

L'avantage le plus recherché par ceux qui souhaitent migrer leurs applications dans le cloud est la réduction des coûts. Le quatrième chapitre abordera donc la gestion des coûts et expliquera pourquoi et dans quelles conditions des services dans le cloud peuvent se révéler moins onéreux que des applications locales traditionnelles.

Le cinquième chapitre propose un aperçu du marché. Pour chaque forme de cloud, de nombreuses solutions existent. Dans ce chapitre, celles qui semblent les plus prometteuses seront présentées.

Choisir une application dans le cloud n'est pas une tâche anodine, il faut pouvoir trouver le bon outil pour la bonne tâche. Par ailleurs, certains pièges sont à éviter. Le sixième chapitre donnera donc quelques pistes pour faire ses premiers pas avec le cloud : quelques exemples d'utilisation, quelques recommandations et également une liste de contrôle qui permettra d'éviter de choisir une solution qui pourrait, à moyen ou long terme, se révéler problématique.

Ce rapport se termine par une conclusion qui fait le point sur tous les sujets qui auront été abordés.

1. Introduction

Le cloud a été un sujet assez abordé, mais paradoxalement, il n'en demeure pas moins difficile à définir. Même les spécialistes ont du mal à s'accorder sur une définition commune du cloud. L'exercice n'est pas aisé, ce chapitre va donc fournir des éléments permettant non pas de définir le cloud, mais de le caractériser. Un point sur lequel tout le monde est d'accord est le caractère très vaste du cloud et la nécessité d'établir une classification des différentes formes de cloud existantes. Celle-ci sera présentée dans ce chapitre.

1.1. Le hype de l'année 2010

Le cloud computing a fait couler beaucoup d'encre cette année : chez Gartner, plus de 1000 articles traitent du cloud et plus de 700 d'entre eux ont été publiés au cours des 12 derniers mois. Selon une enquête effectuée par leurs soins en janvier 2010, la virtualisation et le cloud computing constituent la priorité absolue des CIO de par le monde [1].

Il est actuellement très difficile de trouver un magazine informatique ne contenant pas un seul article sur le cloud. Le phénomène a pris de l'ampleur et les fournisseurs ne pouvaient naturellement pas ignorer cette tendance au point qu'il leur est parfois nécessaire de définir le cloud à leur manière afin de mieux le faire correspondre à leurs produits.

Bref, les définitions sont nombreuses et le chevauchement entre celles-ci n'est pas toujours trivial [2]. Ce flou qui entoure le cloud n'est pas sans rappeler celui du Web 2.0 pour lequel il est également difficile de trouver une définition. Comme cela sera montré dans la suite du rapport, le cloud utilise les concepts du Web 2.0 ; définir le cloud risque donc d'être ardu.

Pour le moment, retenons simplement la remarque de James Urquhart (Cisco) : « the market seems to have come to the conclusion that cloud computing has a lot in common with obscenity--you may not be able to define it, but you'll know it when you see it ».

Compte tenu du hype, peut-être trop prononcé, que l'on trouve autour du cloud, il est naturel de trouver des avis divergents sur son utilité. Pour certains, il ne s'agit là que d'un thème « overhypé » qui a monopolisé la presse et la tendance s'estompera dans un ou deux ans. À l'inverse, on trouve également des personnes très enthousiastes qui considèrent que le cloud est une véritable révolution qui changera le paysage de l'informatique pour les 10 prochaines années [3].

Le cloud existe sous plusieurs formes ; celle qui fait le plus parler d'elle pour le moment est le cloud public qui implique de sortir les données de l'entreprise. Pour certains, c'est une aberration qui représente un grand danger en matière de sécurité. Cette problématique est d'ailleurs très souvent associée au cloud, à tort ou à raison, et constitue actuellement le frein à l'adoption le plus fréquemment cité.

Pour terminer, on retrouve également des personnes qui considèrent que le cloud comprend des aspects intéressants et souhaitent mettre en pratique, en interne, certains concepts qui y sont associés.

Naturellement, chacun de ces points de vue possède des arguments en sa faveur et peut également être critiqué.

1.2. Caractéristiques du cloud

Comme mentionné au point précédent, il existe déjà de très nombreuses définitions du cloud qui sont parfois contradictoires. Pour cette raison, au lieu d'en proposer une définition supplémentaire, il est préférable de le caractériser et de laisser au lecteur la possibilité de se faire sa propre opinion du cloud.

En étudiant divers services disponibles sur le cloud, un ensemble de caractéristiques communes ont pu être mises en évidence. Il s'est alors avéré que le cloud pouvait être vu comme une sorte de supermaché de l'IT. Voici donc les caractéristiques principales des services que l'on trouve sur le cloud (ou, du moins, les caractéristiques que l'on attribue aux services disponibles dans le cloud) :

- **Accès instantané**. Pour faire ses courses, le client ne doit pas prévenir un vendeur de son arrivée ou réserver une heure de passage. Il se rend au magasin au moment où il décide d'effectuer ses achats. La situation est la même dans le cloud : pour utiliser un service, il suffit généralement de se créer un compte qui sera directement utilisable une fois le mode de paiement validé.
- **Self service**. Dans un supermarché, les clients choisissent eux-mêmes les produits qu'ils souhaitent acheter sans qu'un commercial ne soit présent à leur côté. Ce principe se retrouve également dans le cloud où les utilisateurs ont accès à un catalogue de services et choisissent eux-mêmes ceux qu'ils souhaitent consommer.
- **Élasticité.** Lorsqu'une personne effectue ses achats en grande surface, elle choisit non seulement les produits qu'elle souhaite acheter mais également la quantité. Cette dernière peut varier d'une semaine à l'autre en fonction des besoins. Ici aussi il est possible de faire l'analogie avec le cloud : non seulement l'utilisateur choisit les ressources à consommer, mais il en détermine également la quantité. Celle-ci peut varier à tout moment en fonction des besoins.
- **Paiement à la carte.** Dans un supermarché, le prix de chaque article est connu et le client sait ce qu'il devra payer à la caisse. Par ailleurs, sur sa facture, le client ne retrouve que les prix des articles choisis. Ces prix englobent également le coût des infrastructures et du personnel. Les choses sont similaires dans le cloud : les utilisateurs ont une facture qui ne regroupe que le listing des services consommés : tout ce qui touche à la maintenance, au personnel ou aux infrastructures matérielles n'apparaît pas. Signalons au passage que cette facturation se fait généralement à court terme, par exemple, mensuellement. Un peu de

manière analogue au principe des cartes de crédit que l'on retrouve dans certaines grandes surfaces.

- **Abstraction physique de la localisation des ressources consommées.** Lorsqu'il réalise ses achats en grande surface, le client n'est pas obligé de se soucier de la provenance des articles qu'il achète. Celle-ci est cependant indiquée sur l'étiquette de chaque produit ; le client a donc la possibilité de choisir des produits en fonction de leur origine, mais il peut néanmoins ignorer cet aspect. Une fois de plus, l'analogie est possible avec le cloud : les utilisateurs ont bien souvent la possibilité de savoir où se trouvent physiquement les machines exécutant les ressources qu'ils ont choisies et, parfois, ils peuvent même choisir l'endroit où les ressources sont exécutées.

Voilà donc les caractéristiques fréquemment retrouvées dans les services présents sur le cloud. Tous les services existants n'ont pas forcément toutes ces caractéristiques et ces dernières ne sont pas obligatoirement des avantages, mais c'est généralement de cette manière que l'on vend le cloud. Au passage, on peut remarquer que parmi les caractéristiques citées, aucune d'elles n'est véritablement technique.

Une autre notion plus technique qui revient fréquemment lorsque l'on parle du cloud est la « **multitenancy** » [5]. Avec cette dernière, une même instance d'un logiciel va être partagée entre plusieurs utilisateurs. Ceci a l'avantage d'offrir un coût d'entrée plus faible qu'un modèle « single tenant » (où chaque utilisateur a sa propre instance du logiciel qu'il utilise). Le modèle multitenancy peut néanmoins offrir moins de possibilités de personnalisation et peut avoir un coût plus élevé à long terme qu'un modèle single tenant.

1.3. Qui et que retrouve-t-on derrière le cloud ?

Derrière les services accessibles au travers du cloud, on retrouve en premier lieu des géants de l'informatique tels que Amazon, Google, IBM ou Microsoft. Ceux-ci mettent à disposition du monde leur énorme puissance de calcul. Au-dessus de cette dernière, ils ont construit des services génériques qui peuvent être utilisés par leurs clients.

Derrière le cloud, on retrouve également de petits acteurs qui vont, dans certains cas, utiliser les ressources mises à disposition par ces géants de l'informatique afin de proposer leurs propres services. Par exemple, certaines sociétés qui proposent du stockage en ligne ne possèdent pas leurs propres infrastructures mais louent de l'espace disque chez Amazon.

Quant aux services proprement dits, ils sont très variés. Cela peut aller de la boîte e-mail classique au montage vidéo. Il est également possible de louer un serveur sur lequel l'utilisateur est libre de faire ce qu'il veut ou encore trouver des « plateformes d'exécution ». Concrètement, grâce à celles-ci, l'utilisateur peut apporter son propre programme qui s'exécutera sur les machines du fournisseur de cloud.

Comme on peut le constater, l'offre est très variée : difficile de comparer un service de location de serveurs avec une boîte e-mail. Par conséquent, pour mieux s'y retrouver, il est nécessaire d'introduire une certaine classification au sein du cloud.

1.4. Types de cloud

Il est possible de caractériser les solutions cloud au moyen d'une classification en deux dimensions :

1. Les aspects organisationnels
2. Les niveaux d'abstraction

1.4.1. Aspects organisationnels

La forme la plus connue du cloud est le **cloud public** (Figure 1 point 1). Au moyen de ce dernier, les utilisateurs exploitent les ressources du fournisseur de services pour faire tourner ses applications. Par conséquent, les données sortent de l'entreprise pour être placées chez le fournisseur. Les clients se retrouvent donc réunis dans une énorme infrastructure partagée.

Sortir des données de l'entreprise pour les mettre sur une grande infrastructure partagée n'est pas du goût de tout le monde. Néanmoins, les concepts du cloud intéressent les entreprises qui peuvent alors en appliquer les principes chez elles : en mutualisant leurs ressources informatiques et en exploitant la virtualisation [4], elles vont créer leur propre cloud à usage interne. On parle alors de **cloud privé** (Figure 1 point 2).

Un cloud privé vise à organiser le data center de la manière la plus efficace et la plus orientée service que possible. En dépit d'un coût d'entrée important, un cloud privé se révèle à long terme presque toujours meilleur marché qu'un cloud public. On peut considérer cette forme de cloud comme un data center efficace en matière de coûts en se basant sur les piliers suivants :

- Virtualisation
- Standardisation
- Automatisation
- Orientation service

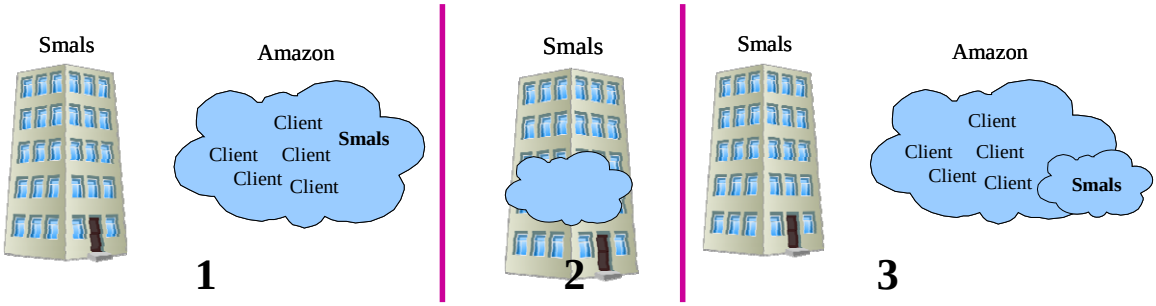


Figure 1: Différentes formes de cloud. 1: Cloud Public, 2 : Cloud privé, 3 : Cloud privé virtuel

Mettre en place un cloud privé n'est pas trivial. Un compromis peut alors être trouvé grâce au **cloud privé virtuel**. Dans ce dernier, les données vont également résider chez un fournisseur externe, mais à la différence du cloud public, les machines utilisées sont dédiées à un seul client (Figure 1 point 3). Pour résumer, cette forme de cloud revient à louer des machines chez un fournisseur.

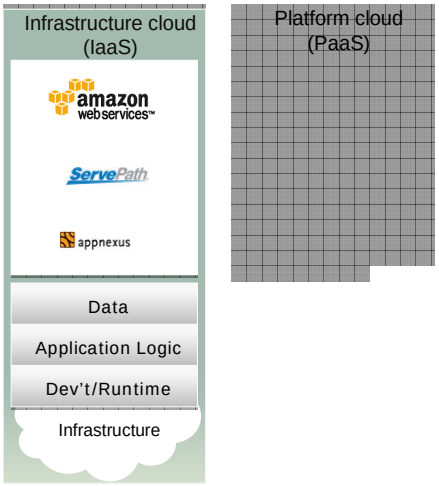
Il est également possible de combiner ces modes (Figure 1 points 1 et 2, points 2 et 3) pour obtenir ce que l'on appelle des **clouds hybrides**. On peut imaginer créer son propre cloud privé et l'associer à un cloud privé virtuel qui fera office de back-up et ne prendra la main qu'en cas de défaillance du cloud privé.

Lorsqu'une entreprise offre un cloud public à un *groupe de clients restreint* ayant généralement des intérêts communs, on parle alors de **communauté cloud**. D'un point de vue technique, il s'agit d'une forme de cloud où les problématiques de sécurité et privacy sont plus simples à gérer étant donné que les ressources ne sont pas ouvertes au monde entier et que le fournisseur et les clients ont généralement une relation privilégiée.

Bien que les termes ne diffèrent que d'un seul mot, il existe donc une distinction essentielle entre un cloud privé et public. Du point de vue d'une entreprise, il s'agit en réalité de deux formes intrinsèquement différentes, bien qu'ayant des caractéristiques communes. Les conclusions valables pour un type de cloud (par exemple la problématique de la sécurité et de la vie privée dans le cloud public) ne sont par conséquent généralement pas d'application à l'autre type !

1.4.2. Niveaux d'abstraction

Le cloud permet de faire abstraction de différentes couches matérielles et logicielles. À partir de ces couches, il est possible d'effectuer une classification. Dans le modèle communément utilisé, on retrouve quatre couches : Infrastructure, Runtime, Application Logic, Data.



Windows Azure de Microsoft (voir point 5.2.1) : il s'agit d'une plate-forme .NET sur laquelle l'utilisateur peut déployer l'application qu'il a lui-même développé. L'utilisateur ne doit pas se soucier des aspects scalabilité et disponibilité qui sont garantis par la plate-forme. En PaaS, l'utilisateur a donc le contrôle des applications qu'il déploie, mais également des données qu'elles produisent. Bien que les plate-formes PaaS sont, à priori, génériques, la portabilité est moins facile à garantir qu'en IaaS. En effet, afin de pouvoir garantir une bonne scalabilité (et parfois aussi pour des raisons de sécurité), la plate-forme peut interdire l'usage de certaines fonctions (ex : interdiction de certains types de requêtes SQL jugées peu performantes). En pratique, cela se traduit par une portabilité diminuée : une application J2EE correcte pourrait ne pas se déployer sur l'une ou l'autre plate-forme PaaS en raison de l'utilisation de certaines fonctions prohibées par le prestataire de service PaaS. Cette situation est analogue à ce qui se passe actuellement chez les hébergeurs de sites Web : une application écrite en PHP ne peut parfois s'exécuter chez un hébergeur en raison de la désactivation de certaines fonctionnalités.

Dernier niveau d'abstraction : les applications, c'est-à-dire le SaaS [5] (Software as a Service). Concrètement, le SaaS se présente sous la forme d'applications prêtes à l'emploi auxquelles on accède directement depuis un navigateur. Ici, le seul contrôle dont on dispose se situe au niveau des données générées. Il s'agit actuellement de la forme de cloud la plus populaire (surtout au niveau du particulier) et la plus diversifiée. Tout utilisateur d'une boîte mail Hotmail, Yahoo, Gmail ou autre est en fait un utilisateur de SaaS. En mode SaaS, l'utilisateur ne contrôle pas véritablement l'application : il peut seulement se contenter de la personnaliser en fonction des paramètres qui sont à sa disposition. Ici, l'utilisateur ne contrôle que les données produites. La facilité de passer d'un prestataire de service à un autre dépend du type de service choisi : si pour de l'hébergement de fichier, changer de fournisseur n'est généralement pas complexe d'un point de vue technique, pour une suite bureautique en ligne, la situation est tout autre : les suites bureautiques en ligne permettent généralement d'exporter des fichiers dans des formats standards, mais cela peut se traduire par un changement de mise en page ce qui est naturellement gênant.

2. Analyse critique du cloud

À la lecture des nombreux articles parus dans la presse au sujet du cloud, il apparaît que celui-ci ne laisse personne indifférent. Certains articles ont un côté pûrement marketing et présentent le cloud comme étant la solution miracle pour toutes les entreprises. À l'opposé, on peut trouver des articles où le cloud est décrit comme étant une véritable menace pour les entreprises. Pour le lecteur, il est difficile de se faire une idée des avantages et inconvénients réels du cloud sur la base d'articles parfois trop engagés. Ce chapitre présentera les avantages et inconvénients du cloud en tentant de rester le plus objectif possible.

2.1. Avantages

Lorsque l'on parle de cloud computing, il est le plus souvent question des possibles économies à réaliser et des dangers liés à la sécurité. Les deux sont en fait équivoques et dépendent fortement du type d'utilisation et de l'implémentation réelle. Dans cette section, nous discuterons des avantages du cloud computing de manière plus générale. Le cloud computing se targue en effet de résoudre deux problèmes fondamentaux de l'IT : réduire les coûts et doper l'innovation.

2.1.1. Scalabilité

Le cloud computing introduit sans aucun doute une ère de possibilités encore inconcevable il y a quelque temps : ainsi, plus de deux milliards de vidéos sont visionnées quotidiennement sur Youtube (chaque minute s'ajoutent pas moins de 24 heures de nouveau matériel vidéo), des milliards de pages web sont consultées et indexées, on peut traiter graphiquement des images en ligne, etc. Afin que ceci soit possible, on s'appuie sur une technologie permettant de mettre à disposition un nombre quasi infini de ressources (puissance de calcul, stockage de données,…), le tout de manière flexible.

Une différence avec le grid-computing est que ces moyens ne sont pas mis à la disposition uniquement d'une « élite » (par exemple les universités) ni seulement utilisés par une sorte bien définie d'applications. Au contraire, le cloud offre toute une série de services, disponibles à toute personne ayant les connaissances business et les moyens financiers nécessaires.

2.1.2. Efficacité

En raison de l'ampleur gigantesque du cloud, ses fournisseurs sont obligés de gérer leur infrastructure de manière extrêmement efficace. Là où dans les divisions IT traditionnelles le nombre moyen de serveurs par administrateur est

typiquement de l'ordre de 10-50, il est chez les fournisseurs de cloud facilement de l'ordre de 1000 ! Si ceci n'avait pas été le cas, Microsoft, par exemple, aurait eu besoin de 20 000 administrateurs système. Cette efficacité a comme conséquence que le client obtient un très bon rapport qualité prix.

2.1.3. Orientation service

Le cloud computing est *orienté service*, ce qui constitue une différence essentielle avec le grid computing et l'IT traditionnels. Au lieu de développer le data center « verticalement », on quitte ce système de silos et on opte pour un modèle horizontal.

Le grand avantage de ceci est que le business s'aligne à l'IT de façon naturelle. Là où auparavant une application business donnée avait des retombées dans une architecture donnée, il est fait abstraction de l'implémentation concrète et la division IT fournit un *service* donné directement traduit en un avantage business. Il est clair que ceci implique une méthode de travail entièrement différente où la division IT devient une unité de business à part entière.

2.1.4. Flexibilité & maniabilité

Il est de plus en plus important d'être en mesure de réagir rapidement à un contexte économique en perpétuel changement. Un Time-To-Market plus bref signifie souvent un rendement plus élevé. La forte flexibilité et maniabilité du cloud computing constituent donc l'un des majeurs avantages. Ceci s'exprime par exemple dans le rapide approvisionnement de serveurs ou la scalabilité automatique et quasiment en temps réel d'applications et de bases de données. Toutefois, on verra plus loin que dans le cadre du secteur public, c'est aspect n'est pas toujours évident.

2.1.5. Pas de CapEx

En principe, les services cloud sont facturés sur la base d'un schéma « pay-for-use ». Lorsque l'on loue un serveur (virtuel) chez Amazon EC2 par exemple, on ne paie que la durée et la bande passante utilisée. De cette manière, l'investissement de capital (CapEx) disparaît et est remplacé par les « frais d'exploitation » (OpEx).

Une conséquence est que le coût de base pour le cloud computing est beaucoup plus bas car il n'est pas nécessaire de réaliser de lourds investissements. Cela permet aux petites entreprises qui n'ont pas le capital nécessaire d'exploiter un data center et d'entrer en concurrence avec des entreprises plus grandes.

En ce qui concerne la formation, le coût d'entrée est assez bas ; des connaissances préalables sont peu voire pas nécessaires (CapEx humain) car les services sont utilisables out-of-the-box. Ainsi, il n'est pas besoin d'avoir un administrateur avec des années d'expérience pour utiliser une mailbox dans le cloud.

2.2. Obstacles

Outre les avantages attrayants du cloud computing, on rencontre parfois aussi des inconvénients.

2.2.1. Sécurité & vie privée

La sécurité et la vie privée forment sans aucun doute le frein le plus important à l'adoption du cloud. Il est toutefois essentiel de bien se rendre compte que la plupart des histoires que l'on lit dans la presse ne concernent que le *cloud public*. De plus, de nombreux dangers ne sont pas uniquement liés au cloud computing.

Le cloud computing public constitue un cas à part au niveau de la sécurité en raison des trois faits suivants :

- Les fournisseurs de cloud public forment une cible intéressante pour les hackers vu le nombre d'utilisateurs (l'échelle) ;
- L'accès se fait sur internet (public) ;
- Les données ne se trouvent pas en interne mais auprès d'un fournisseur externe.

La dépendance au cloud computing peut être comparée à la dépendance au transport public, en l'occurrence le transport aérien. Pour la majeure partie des personnes, il est économiquement impossible de disposer d'un jet privé et elles sont donc tenues de faire confiance au transport public (charters). Bien que ceci implique certains risques, l'avantage est trop important pour qu'on n'en fasse pas usage. La confiance/méfiance dans le cloud peut aussi être comparée à la confiance que l'on a dans un opérateur télécom ou dans la Poste. L'aspect de la sécurité sera traité plus en avant dans le chapitre 3.

2.2.2. Fiabilité

En comparaison avec des solutions internes, les possibilités de contrôles sont moindres, donc logiquement, des questions surgissent régulièrement quant à la fiabilité du cloud. En effet, il n'est pas toujours aussi évident de savoir à quel point un service dans le cloud est fiable (surtout en ce qui concerne le disaster recovery). Pour l'utilisateur, les solutions se comportent en effet comme une « boîte noire » : on ne connaît rien du logiciel ni de la manière dont l'infrastructure, les back-ups etc. sont gérés. En outre, les données restent entièrement entre les mains du fournisseur.

Il existe des histoires de petites start-ups sans le savoir-faire nécessaire en disaster recovery qui, suite à une erreur architecturale, ont perdu toutes les données de leurs clients [6]. Pour ces raisons, nous aborderons trois aspects liés à la fiabilité : qualité de service, garanties en cas d'échec éventuel et la volatilité économique de certaines applications.

Qualité de service

Les vendeurs de cloud public fournissent en général une bonne disponibilité (souvent > 99,9%). Leurs architectures sont robustes de manière que la défaillance d'un composant individuel n'entraîne pas une indisponibilité du service/système. En raison de l'échelle énorme sur laquelle ils travaillent, les pannes individuelles (de l'un ou l'autre composant) se produisent régulièrement… L'indisponibilité doit être évitée car son impact est beaucoup plus grand que dans le cas d'un vendeur traditionnel, vu le nombre important d'utilisateurs. De plus, de nombreuses solutions cloud dépendent les unes des autres, pensons par exemple à une application SaaS tournant sur l'infrastructure IaaS d'un autre fournisseur : en cas de défaillance de l'IaaS, tous les SaaS qui en dépendent seront impactés.

Réparation des pannes

Les SLA définissent en général une indemnisation partielle en fonction de l'indisponibilité. Pour le client, les dommages liés à cette dernière peuvent engendrer des coûts bien supérieurs aux indemnités prévues par le fournisseur de cloud en cas de non-respect du SLA ! C'est pourquoi il peut être plus intéressant de convenir avec le fournisseur de définir ensemble comment les dommages peuvent être limités en cas d'une indisponibilité éventuelle.

Une différence essentielle entre le hosting in-house et l'outsourcing vers un cloud public est qu'il n'est plus possible d'effectuer un contrôle d'infrastructure en cas d'une défaillance éventuelle. À ce moment-là, on dépend entièrement du fournisseur. Des accords clairs sont donc essentiels ! De nombreux SLA garantissent souvent uniquement l'accès au service et non pas sa performance. Il faut donc vérifier si les ressources nécessaires comme la puissance du processeur, la bande passante et la latence peuvent être livrées tant part l'ISP que par le fournisseur de cloud (surtout dans le cas de plateformes virtuelles).

Volatilité de l'offre

Les initiatives dans le cloud se multiplient à très grande vitesse. Pour le fournisseur d'un service cloud, le coût de base est également bas. Toutes les solutions ne sont pas fiables et certaines ont une durée de vie assez courte. On peut par exemple citer le cas de Xdrive qui permet de faire du stockage en ligne. En 2005, le service avait été racheté par AOL qui y a mis fin en 2008 obligeant ainsi les utilisateurs à se tourner vers une alternative.

Figure 3: Illustration de la volatilité de l'offre : le service Xdrive n'est plus. Ses utilisateurs sont invités à se tourner vers des alternatives.

2.2.3. Compliance

Localisation

Le secteur public est soumis à certaines règles qui, dans le cadre du cloud, peuvent s'avérer pénalisantes. La loi peut, par exemple, interdire de sortir certaines données du territoire. En matière de cloud, il s'agit là d'une contrainte très forte : Google dispose d'un data center en Belgique, mais pas deux. En négociant, il est certainement possible d'obtenir un contrat garantissant que les données hébergées chez ce dernier ne sortent pas du territoire, mais dans ces conditions, il ne faut pas espérer de miracle : si pour une raison ou l'autre leur data center placé en Belgique tombait en panne, les données qui y seraient placées ne seraient plus accessibles.

e-discovery

Electronic Discovery ou e-discovery est le processus où de l'information électronique (souvent historique) est recherchée et demandée en vue d'être utilisée au cours d'un procès. Comme le cloud public fait abstraction du lieu où les données se trouvent en réalité, des problèmes peuvent surgir en matière de e-discovery. Seul le temps démontrera la sécurité de la conservation à long terme pour les solutions existantes. Cette conclusion n'est pas valable pour le cloud privé, où les contrôles nécessaires peuvent être effectués.

Marchés publics

Parmi les caractéristiques du cloud, il en est qui se prêtent mal à la fonction publique. Pour rappel, ce dernier est soumis à la loi des marchés publics. Un achat ne peut être « spontané », mais nécessite de passer par des appels d'offre. Lorsque le coût du produit souhaité dépasse un montant d'environ 200 000€ sur une période de 3 ans, il faut alors passer par un cahier des charges européen ce qui peut entraîner un délai d'un an entre le moment où l'on commence à spécifier ce que l'on veut et le moment où une solution est retenue et mise en production. Difficile donc de faire du « on demand » dans ces conditions. L'aspect self-service des solutions de type cloud est également difficile à exploiter. Dans le secteur public, tout le monde ne peut signer de bons de commande…

En réfléchissant un peu, le secteur public n'est pas pour autant pénalisé : même dans le monde privé, il est rare de sauter sur une application et de l'utiliser immédiatement : le choix d'un logiciel ne s'improvise pas.

Par ailleurs, les contraintes s'appliquent principalement au niveau du cloud public. Dans un cloud privé dédié au secteur public, rien n'empêche d'utiliser à la demande les ressources mises à disposition des fonctionnaires.

Recommandation : *pour le secteur public, les aspects juridiques peuvent s'avérer bloquants ; ils doivent donc être pris en considération dès le départ.*

2.2.4. Processus, organisation & intégration

Gouvernance

Le cloud computing oblige les entreprises à bien maîtriser leur gouvernance en matière d'IT. Lorsque des entreprises hésitent à appliquer en interne les principes

du cloud computing ou de sous-traiter certains services vers le cloud public, cela a *souvent moins à voir avec les défis qu'implique le cloud lui-même* qu'avec le fait de savoir *si les systèmes internes sont prêts.*

De nombreuses entreprises doivent tout d'abord résoudre en interne des problèmes comme la sécurité, l'interopérabilité et la gouvernance avant de pouvoir passer au cloud computing [7]. Le cloud computing, c'est en effet :

- une orientation horizontale au lieu de verticale (silos)
- une orientation entièrement service
- une priorité donnée à la flexibilité et à l'efficacité plutôt qu'au contrôle et à la fiabilité.

Processus

Dans le cloud, tout tourne autour de la fourniture de services. Une façon de faciliter l'intégration est l'introduction d'initiatives SOA (Service Oriented Architecture) [66], ce qui permet de se passer des silos d'infrastructure et d'application. Il est aussi important de savoir que les processus de management comme la comptabilité et les achats peuvent être mis dans une SOA et être automatisés.

User Access Management

Lors de la sous-traitance de certains services dans le cloud public, il ne faut pas oublier de tenir compte de la gestion et de l'authentification des utilisateurs.

Licences

Dans un cloud privé, l'aspect « licences » joue aussi son rôle. Lors du provisionnement automatique de machines virtuelles, il faut s'assurer de disposer de suffisamment de licences pour les logiciels présent sur ces machines virtuelles.

Passage d'un data center traditionnel à un cloud privé

La politique d'un data center organisé en cloud privé diffère fondamentalement d'une IT traditionnelle. Là où les data center actuels visent à optimiser le contrôle, la confiance et la fiabilité, les caractéristiques d'un data center organisé en cloud privé sont totalement différents :

- le dynamisme (déploiement rapide, agilité)
- l'efficacité
- la délivrance de services « à la demande »
- la flexibilité (scalabilité)

Le passage d'un data center traditionnel à un data center organisé en cloud privé n'est donc pas trivial et se fait de préférence en différentes étapes :

- centraliser la gestion IT (assets, configurations,…)
- standardiser les configurations
- consolider & virtualiser
- automatiser les processus
- prévoir le self-service & les API

2.2.5. Portabilité

Dépendance vis-à-vis d'un fournisseur

De nombreux clients sont séduits par le cloud public en raison de son coût d'entrée exceptionnel. En revanche, on ne parle pas de son *coût de sortie*, à savoir les frais à payer pour récupérer les données lorsque l'on résilie le contrat. Ce coût peut souvent être significatif et l'export de données peut même se révéler impossible, ce qui entraîne une situation de *vendor lock-in* (impossibilité de changer de fournisseur).

Dans ce contexte, l'initiative de Google, « the Data Liberation Front » [8] est intéressante. Ce mouvement a pour but de faciliter l'échange de données entre clouds : *« Les utilisateurs devraient être en mesure de contrôler les données qu'ils entreposent dans tout produit Google. L'objectif de notre équipe est de faciliter l'entrée et la sortie de données. »*

Mises à jour

Un point qui peut s'avérer gênant vis-à-vis du cloud est la perte de contrôle des **mises à jour** surtout au niveau du SaaS. Avec un client lourd traditionnel, l'utilisateur choisit le moment où il veut migrer ainsi que la version vers laquelle il veut migrer. Avec le SaaS, les choses ne se passent pas de cette manière. Tout d'abord, il n'y a pas vraiment de mises à jour : les applications s'enrichissent progressivement et en douceur. En pratique, cela se traduit par l'apparition d'une nouvelle fonctionnalité ou d'une nouvelle entrée dans un menu. Du moment que la compatibilité ascendante est maintenue, cela ne pose pas de problèmes. Du moins à première vue. Dans certains cas, l'apparition de nouvelles fonctionnalités peut amener l'utilisateur à partager des données à son insu. Un exemple de mise à jour critiquée des utilisateurs fut l'apparition de Google Buzz, un réseau social qui est apparu un jour pour tous les utilisateurs de Gmail (version gratuite) qui se sont donc automatiquement retrouvés « inscrits » sur un réseau social sans rien avoir demandé à qui que ce soit. Google a cependant bien réagi et très vite : 2 jours après le lancement de Google Buzz, la politique de confidentialité de ce dernier a été adaptée ainsi que la possibilité de le désactiver facilement.

Il y a un autre type de mise à jour qui peut par contre s'avérer problématique : celle du navigateur web. Cette application est le point d'entrée de toute application SaaS. À priori, c'est l'utilisateur qui décide du moment où il met à jour son navigateur. Néanmoins, le fournisseur de cloud peut l'inciter à précipiter cette mise à jour. En février 2010, Google avait annoncé ne plus supporter IE6 et invitait ses clients à mettre à jour leur navigateur. Cette annonce n'est pas sans conséquences : cela signifie qu'à partir de ce moment, les nouvelles fonctionnalités pourraient très bien ne plus fonctionner sous IE6. Plus contrariant encore, les fonctionnalités déjà présentes mais mises à jour, étaient également susceptibles de ne plus fonctionner sous IE6 pouvant ainsi empêcher un utilisateur d'effectuer une tâche qu'il avait l'habitude de réaliser.

Il est vrai qu'IE6 est un navigateur ancien (2001), très lent avec Javascript et respectant peu les standards du web. À titre d'information, IE6 obtient un score de 4/100 au test ACID3 [9] alors que d'autres navigateurs obtiennent 100/100. Difficile dans ces conditions d'exploiter les standards du web pour créer des applications qui fonctionnent sous IE6. Cependant, jusqu'en avril 2010, IE6 était encore le navigateur web le plus répandu. La suppression de son support peut être vu comme une pression exercée sur les clients pour mettre leur logiciel à jour. Pour le particulier ou les petites sociétés, cela ne représente pas un problème, mais pour les grands organismes publics, ce n'est pas le cas. Ces derniers doivent s'assurer que les applications utilisées fonctionnent encore toutes. Si l'on prend le

cas d'une application importante telle qu'un Intranet, il faut penser à vérifier tous les modules développés pour ce dernier et s'assurer que tout fonctionne encore de la même manière à travers le nouveau navigateur.

Recommandation : *le cloud implique d'accéder à un service au travers d'un navigateur web. Ce dernier doit donc être à jour. Évitez IE6 et si possible IE7 (pour ce dernier, ce sont surtout les performances qui posent des problèmes).*

Standards

De nombreuses initiatives sont lancées autour de la standardisation du cloud : Cloud Security Alliance, Open Grid Forum, Distributed Management Task Force,… pour n'en citer que quelques unes. Et pourtant, aucune ne parvient vraiment à décoller. Il semble souvent trop difficile de réunir tous les acteurs principaux autour de la même table.

Deux standards sont dignes d'être mentionnés : **OVF ou Open Virtualisation Format** est un standard ouvert pour l'empaquetage et la distribution d'appliances virtuelles (logiciel plus général). Le standard n'est pas lié à un hyperviseur spécifique ni à une architecture de processeur bien précise. Il est donc possible de récupérer une machine virtuelle dans le cloud (sur Amazon, par exemple) et de l'exécuter sur un serveur en interne ou même sur sa propre machine.

Plus récemment, la **Cloud Data Management Interface (CDMI)**, définie par la SNIA (Storage Networking Industry Association), a vu le jour. Elle définit les spécifications pour un nouveau standard qui facilite les échanges sécurisés de données entre des clouds publics et privés et qui prévoit des standards pour la définition de métadonnées, afin qu'elles ne doivent pas être créées de nouveau à chaque fois.

2.2.6. Modèle de prix

Le modèle de prix du cloud computing rompt radicalement avec les schémas traditionnels car on ne paie en principe que pour l'*utilisation* des services/ressources. On passe donc d'un modèle CapEx à un modèle OpEx. Aucun des deux modèles n'est meilleur que l'autre et la préférence pour l'un ou l'autre dépend de différents facteurs :

- L'entreprise a-t-elle beaucoup de liquidités ou est-il au contraire difficile de faire des investissements importants ?
- Pour le secteur public, il est plus facile de trouver un financement pour CapEx que pour OpEx ;
- Les OpEx ne peuvent être amorties.

Notre expérience avec le SaaS (où *seules 10% des solutions fonctionnent réellement selon un schéma pay-for-use complet !)* nous a appris que le modèle OpEx :

- ne peut pas toujours être assumé par le fournisseur (par exemple si celui-ci ne parvient plus à supporter les coûts) ;
- peut s'avérer trompeur (le prix semble plus bas mais ne l'est pas en réalité) ;

- n'est pas toujours intéressant pour le client (par exemple lorsque les revenus ne varient pas en fonction des ressources utilisées) ;
- rend difficile la prévision des coûts (par exemple le coût du stockage dépend du nombre d'accès aux fichiers et de la bande passante).

Actuellement, au niveau des modes de facturation, le SaaS s'oriente vers le modèle pay-for-use alors que les autres formes de cloud computing (surtout l'IaaS) choisissent une direction opposée et optent des définitions de prix plus traditionnelles. De son côté Microsoft Azure offre en ce moment quatre formules de facturation, adaptées à chaque sorte de business partner :

- *consumption :* l'utilisateur ne paie que lorsqu'il utilise une ressource
- *subscription :* une formule d'abonnement traditionnelle
- *volume-license :* une licence pour grandes entreprises
- *developer credits :* une promotion afin d'attirer les développeurs

2.2.7. Facteur humain

L'obstacle le plus difficile à gérer est le facteur humain surtout lorsqu'il est question de cloud public. Il est aisément compréhensible que les responsables informatiques soient peu enclins à sous-traiter les ressources qu'ils contrôlaient. Ceci peut être perçu comme un risque de perte de contrôle, voire un risque de perte d'emploi.

Par conséquent, en arrivant avec une proposition visant à remplacer des infrastructures existantes par des solutions tournant dans un cloud public, il est fort probable de rencontrer de la résistance. À ce niveau-là, il est difficile de formuler des recommandations, il faut voir au cas par cas et déterminer l'origine réelle des craintes : peur de la détérioration de la qualité de service ou peur de perdre son emploi (ou une partie de ses tâches).

3. Sécurité

Le cloud implique de mutualiser des ressources pour les partager : plusieurs utilisateurs vont se retrouver sur une même infrastructure. Si l'on parle de cloud public, cela implique en plus de sortir des données de l'entreprise et de les placer sur une infrastructure où se trouveront également des utilisateurs d'autres sociétés pouvant provenir de n'importe où dans le monde. Il est donc légitime de se poser des questions et de s'assurer que les données confiées au cloud seront bien en sécurité.

Une étude a montré que 68% [67] des Directeurs des Systèmes d'Information ont des craintes en matière de sécurité qui les dissuadent d'utiliser le cloud public. Il est donc évident que les grands acteurs du cloud, dont l'objectif est de vendre leurs produits, vont devoir réagir et apporter des réponses concrètes à ces craintes.

Un autre point important est la vie privée : en plus de savoir qui aura accès à ses données, l'utilisateur doit être certain de connaître l'usage qui en sera fait.

En matière de sécurité du cloud, nous distinguerons trois types de dangers : les attaques externes (point 3.1), les attaques internes (point 3.2) et le Patriot Act (point 3.3). Ce dernier est une loi américaine qui représente un réel frein à l'utilisation du cloud pour les sociétés non basées aux Etats-Unis.

3.1. Attaques externes

Pour un pirate, les services hébergés dans le cloud s'avèrent très intéressants : derrière un service tel que Gmail, ce sont les mails de plus de 170 millions d'utilisateurs que l'on retrouve. Une autre manière de le présenter consisterait à dire que 170 millions d'utilisateurs emploient un même logiciel avec une configuration quasi identique pour chaque personne. De là, on peut se demander quel serait l'impact d'une attaque réussie : serait-il possible pour le pirate d'entrer dans le système et d'accéder aux données de tout le monde ?

Une attaque classique consiste à retrouver les mots de passe faibles pour ensuite s'introduire dans le compte de la victime et récupérer ses données. La portée de l'attaque est généralement limitée aux données de la victime. La parade est tout aussi classique que l'attaque : choisir un mot de passe fort. Naturellement, si l'on utilise une dizaine voire plus de services dans le cloud, il n'est pas trivial de choisir et surtout de retenir toute une série de mots de passe forts. Il est alors plus prudent de passer par des *solutions de gestion de services clouds* tels que myOneLogin [11], Opacus [12] ou CloudSherpas [13]. Les solutions citées permettent d'effectuer du SSO [14] et de générer les mots de passe des services utilisés et hébergés dans le cloud. Certains fournissent également des mécanismes d'authentification forte pour se connecter. L'authentification étant un point crucial pour l'accès des données, l'usage de ces solutions est recommandé.

Au lieu de s'attaquer à un compte utilisateur, le pirate peut également choisir de s'attaquer au service lui-même et essayer d'en trouver les failles. En cas d'attaque réussie sur un service mutualisé, l'impact peut être dévastateur. Un exemple concret est celui d'une attaque qui avait frappé la société vaserv.com (société qui fournit de l'hébergement web mutualisé qui s'appelle à présent cheapvps [15]). Un pirate a réussi à exploiter une faille dans le logiciel HyperVM qui gérait l'hyperviseur utilisé par vaserv.com ce qui lui a permis d'effacer 100 000 sites webs [16]. HyperVM est donc une surcouche pour hyperviseur créé par la société LXLabs [17] (qui a également changé de nom pour devenir LXCenter). Il est impossible, pour l'utilisateur, de prévenir ce genre d'attaque, néanmoins, pour y faire face, la seule solution consiste à faire un back-up régulier de ses données auprès d'un autre fournisseur de service. Ne pas placer ses données en production et ses back-ups chez un même fournisseur**.**

Cet exemple tragique est plutôt rare, mais possible. L'hyperviseur se situe à un niveau très bas dans le système, une attaque réussie peut donc impacter tout ce qui se trouve au-dessus. Bien que possible, attaquer un hyperviseur est une tâche très ardue. Pour s'en convaincre, on peut regarder les publications de la société InvisibleThings Lab [18] qui expliquent comment réaliser concrètement ce type d'attaques. Après la lecture de ces documents, on est convaincu qu'il sera plus facile pour la grande majorité des pirates d'opter pour d'autres pistes (XSS, SQL Injection, …).

Les géants de l'informatique tels que Google ont les moyens de s'armer contre les pirates : s'ils doivent recruter une dizaine de spécialistes en sécurité reconnus dans le monde ou dépenser des millions pour sécuriser les données qu'ils hébergent, ils le feront car ils en ont les moyens et qu'il s'agit là d'un enjeu majeur pour leur crédibilité (un problème de sécurité peut coûter très cher au fournisseur). Pour les petits acteurs du cloud, la situation est plus délicate et il convient de se renseigner au cas par cas sur les mécanismes mis en œuvre pour assurer la sécurité de leurs clients.

Recommandation : *se renseigner sur les mécanismes de protection mis en place par le fournisseur. Pour la sauvegarde des données, choisir* ***un autre fournisseur*** *que celui utilisé pour la manipulation de celles-ci.*

3.2. Attaques internes

Dans une autre étude de la section Recherches [19], il avait été dit que 70% des attaques provenaient de l'intérieur. Dans le cadre du cloud, cela veut donc dire que les utilisateurs doivent avoir les moyens de protéger leurs données contre les administrateurs système du service hébergé dans le cloud.

Une précaution de base consiste à chiffrer ses données si le système permet de le faire. Cependant, cela n'est pas toujours suffisant. Lors de nos tests, il a été montré qu'il est possible, pour celui qui manipule l'hyperviseur, de récupérer les clés de chiffrement utilisées par les utilisateurs. Le scénario suivant a été pris : un utilisateur chiffre son disque virtuel au moyen du logiciel Truecrypt [20]. L'administrateur va ensuite utiliser le principe de l'Evil Maid [21] appliqué aux machines virtuelles afin de récupérer le mot de passe nécessaire au déchiffrement du disque dur de la machine virtuelle (dans notre exemple : « Hello Smals » en qwerty ➔ « Hello S;qls »). La réalisation de cette attaque s'est avérée très simple et, en pratique, il suffit de simuler une panne en stoppant violemment la machine virtuelle.

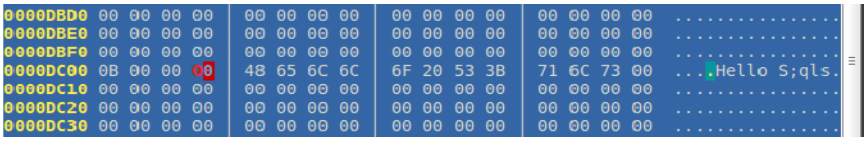


Figure 4: Récupération du mot de passe d'une partition chiffrée avec TrueCrypt.

Si cette attaque est simple à réaliser, elle est également très simple à détecter, à condition d'avoir pris les mesures nécessaires. Ici, il suffit simplement d'installer sur le système virtuel un logiciel qui va vérifier que l'amorce du système n'a pas été altérée depuis le dernier redémarrage.

Par cet exemple, nous avons montré qu'il peut être facile pour un administrateur d'attaquer les machines virtuelles, mais qu'au moyen de précautions simples, les attaques peuvent être facilement détectées. L'utilisation de machines virtuelles dans le cloud présente donc effectivement certains dangers, mais rien de difficilement surmontable.

Recommandation : *chiffrer ce qui peut l'être. En cas d'activité anormale (ex pour IaaS : arrêt d'un serveur non planifié), interroger le fournisseur et vérifier que rien n'a été modifié à notre insu.*

3.3. Patriot Act

Lorsque l'on regarde les acteurs majeurs du cloud, force est de constater qu'ils sont tous américains. Héberger ses données sur le sol américain implique un risque qui peut être considéré comme intolérable.

Suite aux attentats du 11 septembre 2001, une loi du nom de Patriot Act a été mise en application. Celle-ci permet notamment aux services secrets américains d'aller dans des sociétés pour prendre des équipements sans en fournir la raison ou de placer des dispositifs sans en expliquer l'utilité. Toute société basée sur le territoire des Etats-Unis est soumise à cette loi et ne peut s'y soustraire. Dans ces conditions, il est impossible à un fournisseur de services de garantir que personne n'ira accéder aux données de leurs clients. D'un point de vue commercial, ce n'est pas sans conséquence : lorsque l'on voit que 93% des utilisateurs d'Amazon ou de Rackspace viennent des Etats-Unis, ce n'est probablement pas une coïncidence : en hébergeant leurs données sur le sol américain, les entreprises européennes et asiatiques se trouvent alors soumises à la loi américaine et donc au Patriot Act. Celui-ci est, par ailleurs, en contradiction avec certaines directives internationales visant la protection des données telles que le Data Protection Act [22] et le Safe Harbor [23].

Une autre conséquence de ce Patriot Act avait de quoi inquiéter : pour établir une connexion chiffrée vers un site web et s'assurer que le site sur lequel on se trouve est bien celui auquel on souhaite se connecter, il faut utiliser des certificats. Ceux-ci sont signés par des hôtes de confiance. Le plus connu est Verisign qui est basé… aux Etats-Unis. En théorie, le Patriot Act permet donc aux services de renseignements de générer de faux certificats qui seraient tout à fait valides aux yeux des navigateurs web.

Face à ce Patriot Act, les fournisseurs n'ont pas d'autres solutions que de proposer de l'hébergement en dehors du territoire américain. Si l'on reprend le cas d'Amazon, ils disposent d'un datacenter en Europe et d'un autre en Asie. Quand à Google, ils ont réparti une quarantaine de datacenters un peu partout dans le monde. Cela permet aux clients de choisir les zones à exclure pour l'hébergement de leurs données.

Recommandation : *se renseigner sur la localisation physique des machines (surtout pour les services SaaS s'appuyant sur d'autres services tels qu'Amazon). Éviter de placer ses données aux Etats-Unis. Vérifier la validité des certificats SSL et ne pas accepter les certificats de classe 1 (classe 2 minimum).*

3.4. Recommandations et solutions des fournisseurs

Étant donné la gamme très variée de services que l'on retrouve dans le cloud, fournir des recommandations génériques n'est pas aisé. De manière générale, il faut privilégier les connexions chiffrées et également vérifier la validité des certificats utilisés et ne pas placer tous ses œufs dans le même panier (séparation des données et back-ups).

Pour le reste, il faut voir au cas par cas :

- IaaS :
  - Ne pas faire confiance aux templates virtuels fournis qui peuvent contenir des backdoors ou failles critiques
  - Chiffrer ses disques virtuels
  - En cas de redémarrage du serveur virtuel, vérifier que le système n'a pas été modifié
- PaaS :
  - Appliquer les mêmes règles que pour le développement d'applications hébergées en local (ex : surveiller systématiquement toutes les données introduites par les clients)
  - Ne surtout pas croire que le fait de placer une application dans le cloud en renforce la sécurité
- SaaS :
  - Paramétrer au mieux les fonctions mises à disposition
  - Désactiver les fonctionnalités non utilisées

Si la sécurité est très importante pour les utilisateurs, pour les fournisseurs de services, il s'agit-là d'un enjeu capital : la sécurité est actuellement la principale crainte vis-à-vis du cloud. Par conséquent, une affaire de piratage pourrait ternir la réputation d'un fournisseur de manière irréversible. C'est donc, en premier lieu, dans l'intérêt du fournisseur d'optimiser la sécurité. Pour cela, les grands acteurs déploient des moyens conséquents et ce y compris au niveau de la recherche.

Parmi les pistes intéressantes, on peut citer le *chiffrement homomorphique* sur lequel IBM travaille assez bien. Pour résumer, le chiffrement homomorphique permet d'effectuer des opérations sur des données chiffrées sans avoir à les déchiffrer. Concrètement, l'utilisateur chiffre les données avant de les envoyer chez le fournisseur. Une fois arrivées chez ce dernier, les données vont pouvoir être manipulées sans devoir être déchiffrées. Au terme des opérations, le résultat (chiffré) est retourné à l'utilisateur qui va pouvoir le déchiffrer.

Au moyen du chiffrement homomorphique, même un administrateur qui copierait le contenu entier de la mémoire d'une machine ne serait pas en mesure de récupérer des données en clair. Quoiqu'il en soit, le chiffrement homomorphique est encore jeune et il ne faut pas espérer qu'il se démocratise avant plusieurs

années. Le chiffrement homomorphique a cependant déjà été utilisé avec succès dans le cadre de votes électroniques.

4. Gestion des coûts

Lorsque l'on parle des avantages du cloud computing, on cite souvent l'économie de coûts. Cependant, l'image que l'on donne est le plus souvent mal étayée et pas toujours très correcte. Il convient donc de nuancer quelque peu ce propos. Dans les paragraphes suivants, nous examinerons pourquoi certains services dans le cloud proposent des prix très bas, comment des économies peuvent être réalisées et quels coûts cachés doivent être pris en compte.

4.1. Pourquoi certains services dans le cloud sont-ils si bon marché ?

Un « fournisseur de cloud » est en principe un prestataire de services. La différence avec un prestataire traditionnel réside dans le fait qu'il offre des services standard très spécialisés, et ce à très grande échelle. C'est la raison pour laquelle il peut souvent pratiquer un prix unitaire moins élevé :

- ils bénéficient de réductions sur le hardware, l'électricité, la bande passante, les logiciels, etc. grâce à des commandes volumineuses ;
- ils gèrent leurs ressources de manière centralisée (par exemple des upgrades horizontaux de logiciels) ;
- ils font usage de commodités (ordinateurs bon marchés au lieu de serveurs onéreux) ;
- le coût par activité (surtout dans le modèle SaaS) est plus bas en raison de la « multi-tenancy » ;
- il gèrent leur portefeuille de manière extrêmement efficace : c'est le fournisseur cloud qui définit l'offre et non pas le client.

4.2. Réduire les coûts grâce au cloud computing

On entend à tort et à travers que l'introduction d'une technologie X ou Y autorise une baisse des coûts. Or, sur ce plan, il convient de faire preuve de réalisme. Pour le cloud computing par exemple, il n'y a que trois manières de réduire les coûts, à savoir augmenter l'effectivité, se concentrer sur les activités-clés de l'entreprise et standardiser.

4.2.1. Augmenter l'efficacité

Le cloud computing peut augmenter l'efficacité des opérations pour de nombreuses raisons. Tout d'abord, le cloud computing est orienté service, ce qui permet d'organiser la prestation de services plus efficacement. Ensuite, des caractéristiques de la prestation de services même permettent au business de mieux organiser ces services :

- La flexibilité permet d'utiliser efficacement les ressources, par exemple en évitant le surprovisionnement. Examinons l'exemple dans l'illustration ci-dessous. Dans un environnement traditionnel, l'infrastructure statique est réservée sur la base de la demande de pointe ; dans une architecture cloud, les ressources sont allouées proportionnellement à la demande.

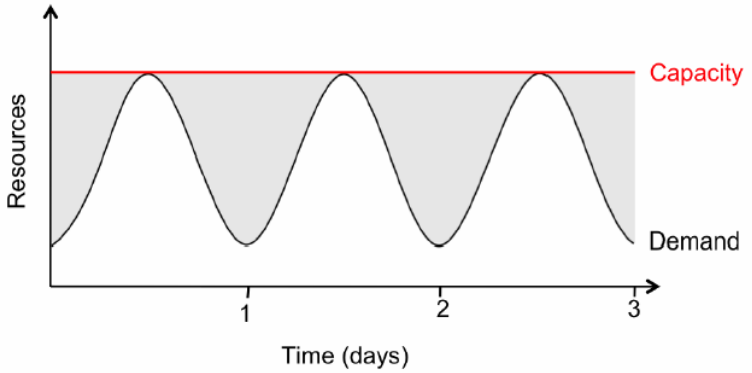


Figure 5: Provisionnement traditionnel: la quantité de ressources est choisie en fonction des pics de demandes auxquelles il faut pouvoir répondre. En dehors de ces pics, les ressources sont sous-exploitées.

- Les délais sont réduits grâce au provisionnement rapide ;
- Les coûts administratifs et de support peuvent être diminués car ces coûts reposent désormais auprès du fournisseur (par exemple la sous-traitance de l'e-mail) ;
- Le SaaS utilise généralement les technologies Web 2.0 les plus actuelles. La collaboration dans l'entreprise peut être augmentée grâce à des outils de collaboration intégrés (par exemple : Google Apps) ;

4.2.2. Mettre l'accent sur les activités clés

Les entreprises peuvent perdre beaucoup d'argent par l'absence d'un portfolio management approfondi. Elles exercent un trop grand nombre d'activités, de sorte qu'elles doivent dépenser des sommes colossales pour maintenir les compétences nécessaires en interne. De ce fait, l'organisation devient aussi bien plus complexe. En se concentrant sur les compétences-clés, les entreprises peuvent donc réduire les dépenses et améliorer leur stratégie de sourcing. Dans ce contexte, le cloud computing permet de réduire les dépenses comme suit :

- Les activités secondaires sont déplacées vers le cloud (par exemple développer les enquêtes avec SurveyMonkey).
- Il y a là une opportunité de simplifier l'organisation et donc, d'en améliorer l'efficacité.

- Se focaliser sur les besoins et les aspects business et non sur les aspects techniques.

4.2.3. Standardisation

Le cloud computing part du principe que le département IT est une unité d'exploitation à part entière. Plutôt que d'exécuter tous les souhaits du business, cette unité va prendre son indépendance et définir une stratégie. L'une des méthodes est la standardisation de l'offre, permettant de réduire les dépenses liées à l'organisation, grâce à une moindre complexité et à une économie d'échelle.

4.3. Coûts cachés

Lorsque l'on évalue les économies faites grâce au cloud computing, il faut bien examiner *où se situent les coûts réels*. Si l'on compare les coûts de ses propres serveurs à ceux d'Amazon, ces derniers semblent très bon marché et offrent en plus un provisionnement très rapide. Cette comparaison n'est cependant pas valable car on compare deux choses qui ne peuvent l'être. Amazon offre des *serveurs virtuels* avec une *performance limitée* (en pratique, une machine virtuelle ne peut pas, dans la plupart des cas, fournir les mêmes performances qu'une machine physique) et en plus, des éléments tels que la bande passante, le monitoring, le support et la maintenance ne sont pas inclus dans le prix.

À titre d'illustration, le tableau ci-dessous propose un comparatif de coût de serveurs virtuels (y compris le support, le monitoring et la maintenance) d'une puissance de calcul donnée où on autorise un volume défini pour le trafic réseau (4000 Gb).

	CLOUD	**Hébergement traditionnel**	
	Amazon	Hostway	Combell
Lieu	**USA/Europe**	**USA**	**Belgique**
Disponibilité	**99.9%**	**99.9%**	**99.9%**
Trafic réseau autorisé	**4 Tb**	**4 Tb**	**4 Tb**
Délai de réception	**Minutes**	**Heures**	**24 heures**
Prix	**€660 / mois**	**€280 / mois**	**€369 / mois**

On remarque d'emblée que les solutions d'hébergement traditionnelles comme Hostway sont plus de 50% meilleur marché. Le grand avantage d'Amazon n'est donc pas le prix brut mais le provisionnement flexible, le démarrage et l'arrêt d'un serveur au moyen d'un appel distant (Service Web).

Dans les paragraphes qui suivent, nous discuterons de quelques « coûts cachés » qui doivent être pris en compte dans l'étude d'une solution cloud.

4.3.1. Administration

Chaque processus business a un coût, qu'il soit exécuté en interne, sous-traité ou exécuté par le cloud. En règle générale, plus le degré d'abstraction du cloud est « élevé » (SaaS > PaaS > IaaS), plus les possibilités d'économies sont grandes, car il faut de moins en moins de processus internes.

Des processus « administratifs » typiques sont :

- l'achat
- le monitoring
- la maintenance
- le support

4.3.2. Intégration

Un coût important trouve son origine dans l'intégration dans les processus actuels. Les fournisseurs de cloud public offrent en effet des solutions standard qui peuvent être personnalisées mais il n'existe pas ou peu de marge dans les négociations de contrat pour simplifier l'intégration. Typiquement, le fournisseur offrira une interface API / SOA (fixe) par laquelle toute la communication devra se dérouler.

Outre l'intégration des logiciels entre-eux, il existe bien sûr aussi des processus d'un « ordre plus élevé » devant être intégrés, nous pensons par exemple au user access management (UAM), Data Integration, Single-Sign on,… Pour cette raison, il faut établir des politiques qui englobent la chaîne entière.

Dans le domaine des processus, il faut également prendre les mesures nécessaires : l'organisation actuelle doit être réglée de telle manière que certaines étapes du processus se fassent de manière entièrement électronique et automatique. Cette intégration peut exiger un coût significatif ainsi qu'une modification de la mentalité.

4.3.3. Migration

Comme avec tout changement technologique, la migration peut se révéler très risquée et chère. Ceci est surtout le cas avec le cloud public, car les données ne sont plus gérées, traitées ni conservées en interne. En outre, la marge de négociation est beaucoup plus étroite avec le fournisseur dont les offres sont standardisées. Il faut aussi se demander (au préalable !) si les données peuvent facilement être *retirées du cloud* et à quel prix.

4.3.4. Licences

Le coût de la gestion et de l'achat de licences ne doit pas non plus être oublié. Dans le cas d'applications effectuant des allocations de ressources automatiques, cette problématique doit être reprise dès le début dans la stratégie générale de Software Asset Management.

4.4. Conclusion

Le cloud computing est une intéressante évolution du paysage des technologies de l'information. Au lieu de considérer les services IT comme « secondaires », purement dédiés au « business », on positionne le département IT comme une véritable unité d'exploitation, au même titre que toutes les autres. Le cloud computing repose sur un modèle de coûts dans lequel une multitude de services IT sont facturés exclusivement en fonction de leur utilisation.

Les possibilités de réduction des coûts résident dans la hausse de l'efficacité et de la flexibilité, la baisse du prix par utilisation résultant d'un effet d'échelle et d'une standardisation, l'accélération de l'approvisionnement, etc. Le fait que le cloud computing permette de se concentrer sur les compétences-clés contribue également à réduire les coûts.

La prudence est toutefois de mise. De nombreuses entreprises ne sont pas encore préparées à ce nouveau mode (orienté service) de travail et de facturation, n'ont pas encore de stratégie business en matière de sourcing et de portfolio management ou présentent encore une trop grande diversité pour pouvoir utiliser de manière optimale les services standard d'un cloud.

En outre, il y a encore de nombreux frais cachés (monitoring, licences, intégration et migration...) qu'il n'est pas toujours possible d'éliminer avec le cloud computing. Il est donc recommandé de procéder à une analyse suffisamment approfondie des réels coûts actuels et futurs avant de se prononcer sur la réduction des coûts.

5. Marché

Le cloud connaît un engouement très prononcé et les offres sont très diversifiées, aussi bien en termes de type de services proposés qu'en termes de qualité. Spécifions également que beaucoup d'offres ne sont pas encore très matures.

Ce chapitre effectuera un tour d'horizon de l'offre existante. La classification proposée au point 1.4 sera utilisée. Pour chaque type de solution, celles qui semblent actuellement les plus prometteuses seront citées.

5.1. Infrastructure as a Service (IaaS)

L'IaaS a commencé à faire parler de lui grâce à l'offre d'Amazon. Cette dernière sert d'ailleurs de base à d'autres offres qui utilisent son infrastructure pour fournir leurs propres services.

5.1.1. Public

Durant l'étude, l'offre d'Amazon, Amazon EC2 (Elastic Cloud Computing) [24], a pu être testée. Au travers d'une interface web, il est possible de créer et de gérer des machines virtuelles sur lesquelles on peut installer les applications de son choix.

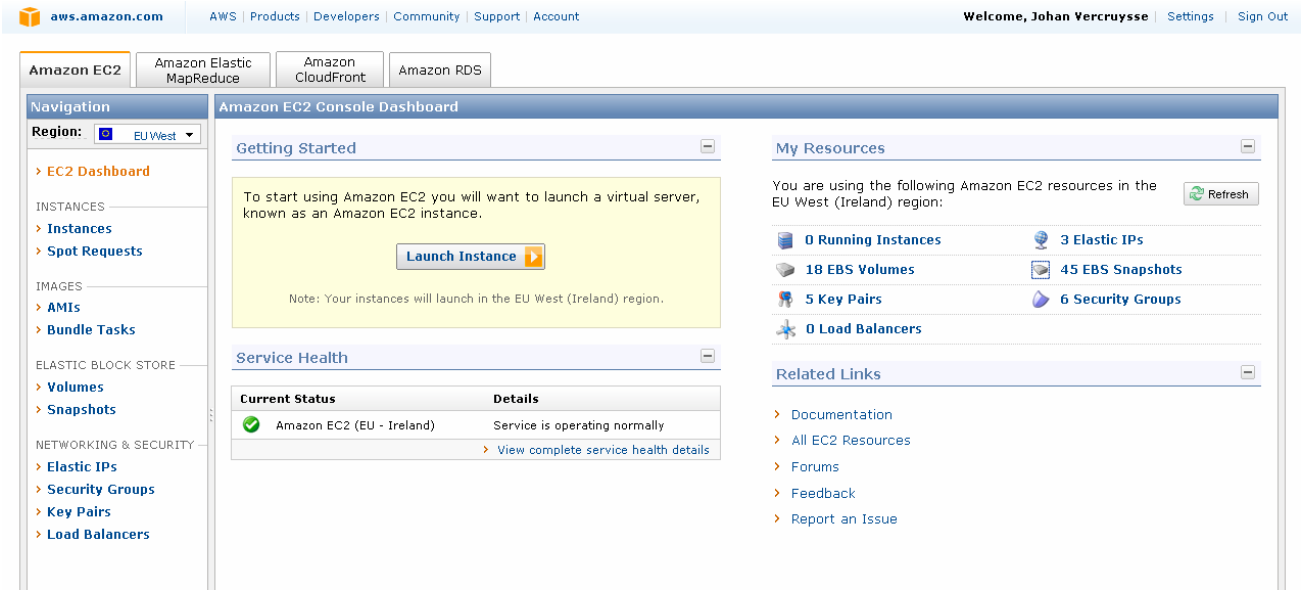


Figure 6: Interface utilisateur d'Amazon

La création de machines virtuelles est aisée : il suffit de choisir des images virtuelles pré-configurées et spécifier le data center où l'on souhaite les exécuter. Il est aussi possible de déterminer les caractéristiques de la machine virtuelle (nombre de CPU, RAM). Le prix varie entre $0.085 et $1.16 par heure suivant le type de machine choisie et le lieu où elle se trouve [25]. Il est également possible de réserver une machine pour une ou trois années, les prix varient alors de $227,5 à $1820 (pour une année) et de $350 à $2800 (pour trois ans).

Il ne faut pas perdre de vue que le trafic réseau entrant et sortant d'Amazon est également facturé à l'aide de forfaits. Suivant le forfait choisi, le Go transmis coûtera entre $0.08 et $0.15. Par conséquent, pour un site à trafic élevé, la facture peut vite grimper. De plus, pour qu'une machine du cloud d'Amazon soit visible de l'extérieur, il faudra également payer pour la réservation d'une adresse IP.

Les machines créées sur Amazon n'offrent pas de persistance : une fois éteintes, leur contenu disparaît. La persistance est possible, mais nécessite la location de blocs persistants (S3). Le modèle de facturation, bien que simple, peut donc réserver quelques surprises : pour déployer des services fonctionnels, l'utilisateur risque de devoir consommer plus de services que prévus.

Un autre point d'attention est le catalogue de machines virtuelles. Celui-ci contient des templates de machines virtuelles créés par Amazon, mais également par la communauté. La sécurité de ces templates doit être évaluée. Ceux-ci peuvent contenir des failles ou des backdoors. L'analyse des templates, qui revient en réalité à analyser un système d'exploitation, n'est pas une opération élémentaire. En milieu professionnel, il est donc préférable de créer ses propres templates et de les déployer dans Amazon.

Parmi les concurrents les plus sérieux d'Amazon, on retrouve GoGrid [26] et Rackspace [27] qui offrent des services similaires.

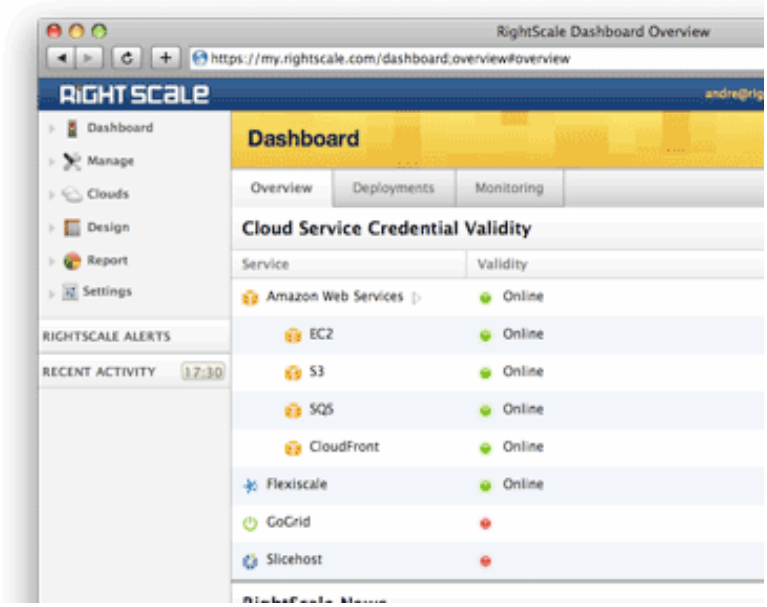


Figure 7: Interface utilisateur de RightScale. On peut y gérer des ressources provenant de plusieurs fournisseurs IaaS.

Parallèlement à cela, on trouve également des offres qui permettent de gérer des machines réparties à travers plusieurs infrastructures cloud. C'est notamment le cas de RightScale [28] qui permet de gérer le cycle de vie, de monitorer et déployer des machines virtuelles chez Amazon, Flexiscale [29], GoGrid, Rackspace et Slicehost [30]. Il existe également certaines solutions plus spécifiques, tel que Joyent [31] qui offre, par exemple, des systèmes avec des instances de MySQL optimisées.

Recommandation : *en cas d'utilisation, bien évaluer tous les composants nécessaires et en quelle quantité (surtout pour la bande passante réseau) pour ne pas se laisser surprendre par la facture.*

5.1.2. Privé

En matière de cloud privé, il existe des solutions tant propriétaires qu'Open Source. Au niveau des solutions propriétaires, une qui nous a semblé prometteuse pour utilisation en milieu professionnel est celle de Fujitsu.

Bien que lors de l'étude la solution s'avérait être encore au stade de développement, les fonctionnalités présentes permettent d'implémenter les concepts du cloud au sein d'une entreprise : séparation des rôles, gestion du cycle de vie des machines virtuelles, module de facturation, ...

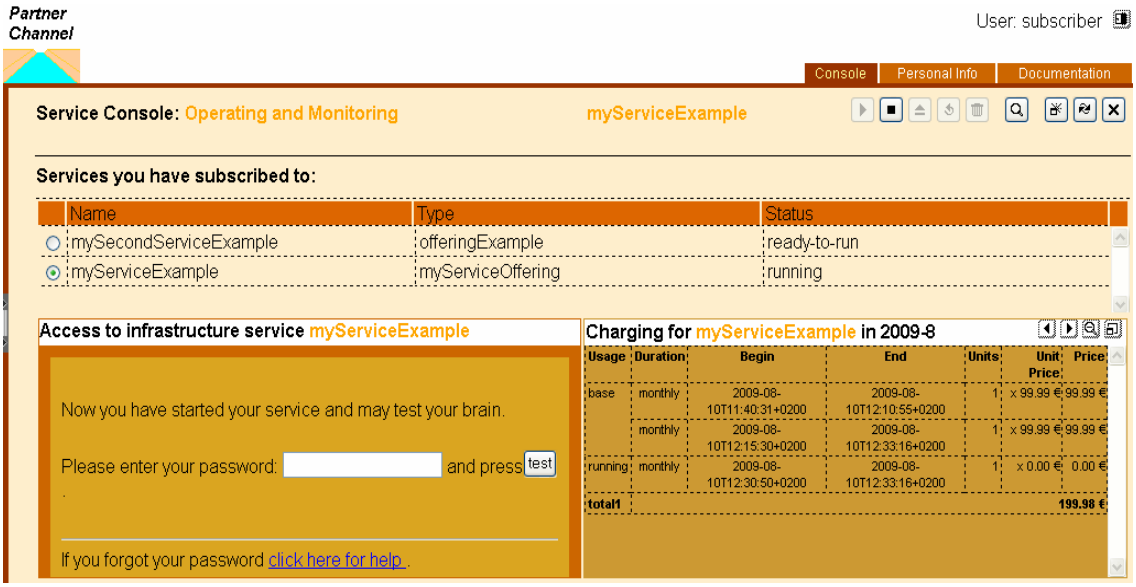


Figure 8: Interface utilisateur de la solution de Fujitsu. Ici, on peut voir le module de facturation.

Dans le monde Open Source, plusieurs solutions existent et ont été testées. Parmi celles-ci, on peut citer Eucalyptus [32], OpenNebula [33] et Abicloud [34]. Tout comme leurs homologues propriétaires, ces solutions peuvent bénéficier d'un support professionnel.

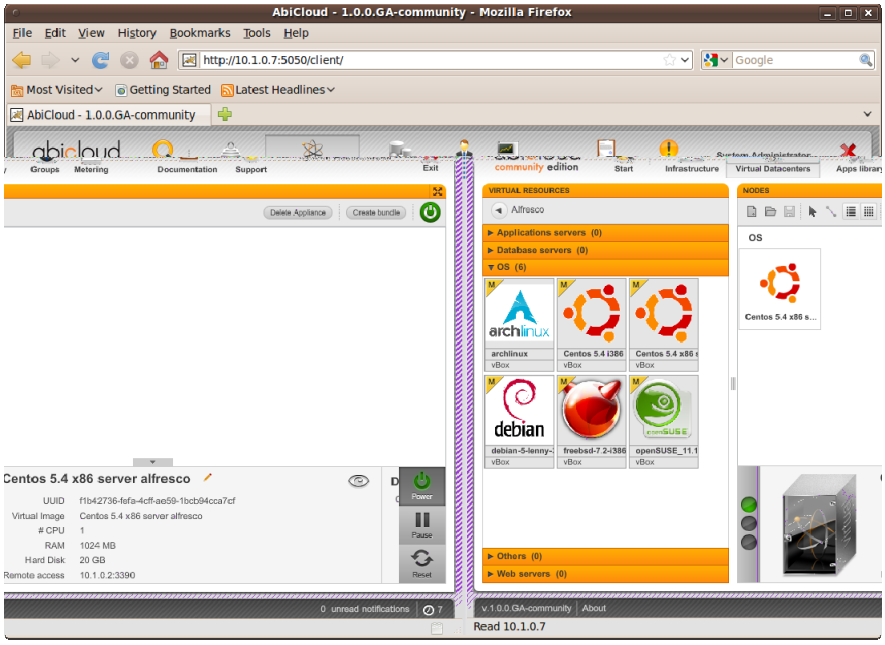


Figure 9: Interface utilisateur d'Abicloud.

De manière générale, ces solutions semblent toutes assez prometteuses mais, lors des tests[1], elles ont surtout donné une impression de manque de maturité. Si du point de vue technique, ces solutions permettent de mettre en œuvre un cloud privé qui fonctionne effectivement, au niveau des fonctionnalités, il semble que les développeurs se focalisent sur les aspects techniques et non les aspects business (pas de module de facturation de service, pas de gestion élaborée du cycle de vie des machines virtuelles, …).

En outre, la documentation fait parfois défaut ou est incorrecte. Dans le cas d'Abicloud, après avoir scrupuleusement suivi la documentation (qui variait au fil des jours), le système ne fonctionnait pas. Pire, celle-ci comportait parfois des références à des documents (pages web) inexistants. Les solutions aux problèmes ont cependant pu être trouvées dans les forums.

Une fois le système correctement installé, l'application s'avère simple d'emploi. L'utilisateur doit créer ses appliances virtuelles et les démarrer. Dans le cadre d'Abicloud, une appliance virtuelle n'est pas obligatoirement constituée d'une seule machine, mais peut comprendre un groupe de machines. On peut ainsi imaginer une appliance virtuelle constituée d'un load balancer, de plusieurs serveurs web et d'un serveur de base de données.

Comme mentionné plus haut, un des problèmes des solutions Open Source est leur caractère purement technique. Si leur utilisation est simple, en pratique, on se retrouve vite avec toute une série d'appliances non documentées et sans aucune uniformité au niveau de la configuration.

Recommandation : *ne pas sous-estimer le coût de mise en place d'une infrastructure de type IaaS. Les aspects organisationnels ne sont pas négligeables (définition d'une politique d'attribution des machines, mise en place du système de facturation, intégration, …)*

[1] Configuration de l'environnement de test : 5 serveurs Intel Core i7 - 12Go Ram – 1 To HDD

5.2. Platform as a Service (PaaS)

Bien que la presse n'accorde pas autant d'attention au PaaS qu'à l'IaaS et au SaaS, beaucoup s'accordent à dire que cette forme de cloud aura à terme beaucoup d'influence sur les petites et moyennes entreprises. Ceci n'a rien d'étonnant : alors que l'IaaS est très éloigné du côté business et que SaaS ne peut être intégré ou personnalisé suffisamment, le PaaS permet de créer des applications sur mesure répondant exactement aux besoins de leurs concepteurs tout en préservant les avantages du cloud.

On peut d'ailleurs remarquer que les vendeurs IT traditionnels (Microsoft, Oracle, IBM,…) ont opté pour cette voie.

5.2.1. Public

L'histoire de PaaS a commencé il y a quelques années avec *force.com*, une plateforme issue de la solution SaaS salesforce.com. Force.com est actuellement la plateforme la plus importante et la plus connue. Elle offre un environnement intégré de développement, de test et de déploiement intégrant des aspects comme les bases de données, la sécurité, le workflow, l'interface utilisateur et autres outils. La plateforme garantit en outre la scalabilité et la disponibilité. Il est ainsi plus facile de construire des applications plus rapidement et à moindre frais. En ce moment, plus de 77 000 entreprises utilisent cette plateforme, ce qui revient à quelque 135 000 applications avec plus de 2 millions d'utilisateurs.

Google a aussi rejoint les rangs avec la plateforme appelée *AppEngine*. Il est possible d'y procéder à des développements dans les langages de programmation traditionnels : Python et Java. Afin de garantir la disponibilité et la scalabilité, certaines restrictions ont été mises en place au niveau des langages de programmation :

- Toutes les instructions ne peuvent être utilisées, seul un subset du langage est disponible
- Le moteur de base de données mis à disposition n'est pas aussi riche qu'une base de données relationnelle (les jointures externes ne sont ainsi pas autorisées car il n'est pas possible de les implémenter tout en garantissant des performances suffisantes pour offrir une bonne scalabilité)
- Seul l'accès en lecture des fichiers est possible (toujours dans une optique de garantir une bonne scalabilité)

Microsoft n'est pas en reste avec « *Azure* ». Cette solution est constituée de plusieurs services dont un système d'exploitation orienté cloud, une base de données SQL allégée scalable, une plateforme .NET, etc. Actuellement, les applications développées ne tournent que sur le data center de Microsoft mais la Windows Azure Platform Appliance (WAPA), récemment présentée, sera disponible dans un an et permettra aux clients de faire tourner un cloud PaaS privé dans leur propre data center (les serveurs ainsi que le réseau et le stockage sont fournis par Microsoft).

Une utilisation intéressante de cette plateforme a été découverte lors de la compétition des « 20 km de Bruxelles » [65] : l'organisation souhaitait offrir un film de l'arrivée de chaque participant. Comme il était difficile d'évaluer à l'avance la densité du trafic et que l'offre n'était que temporaire, il a été choisi d'offrir cette fonctionnalité par le biais de la plateforme Azure.

5.2.2. Privé

Oracle, un acteur important dans le marché des entreprises, était à l'origine très sceptique par rapport au Cloud Computing. Ce sentiment a d'ailleurs été clairement exprimé par Larry Ellison (CEO d'Oracle) en 2008 : « Maybe I'm an idiot, but I have no idea what anyone is talking about. What is it? It's complete gibberish. It's insane. When is this idiocy going to stop? ».

En novembre 2009 cependant, Oracle change d'avis et s'investit résolument dans le cloud privé avec des slogans comme « Private Cloud : A Natural Evolution for Enterprises »… Cette évolution ressort aussi clairement de la feuille de route et des produits qu'ils offrent : l'entreprise vise une plateforme Weblogic performante intégrée et scalable sur laquelle des applications peuvent être développées et déployées comme il ressort de l'illustration ci-dessous :

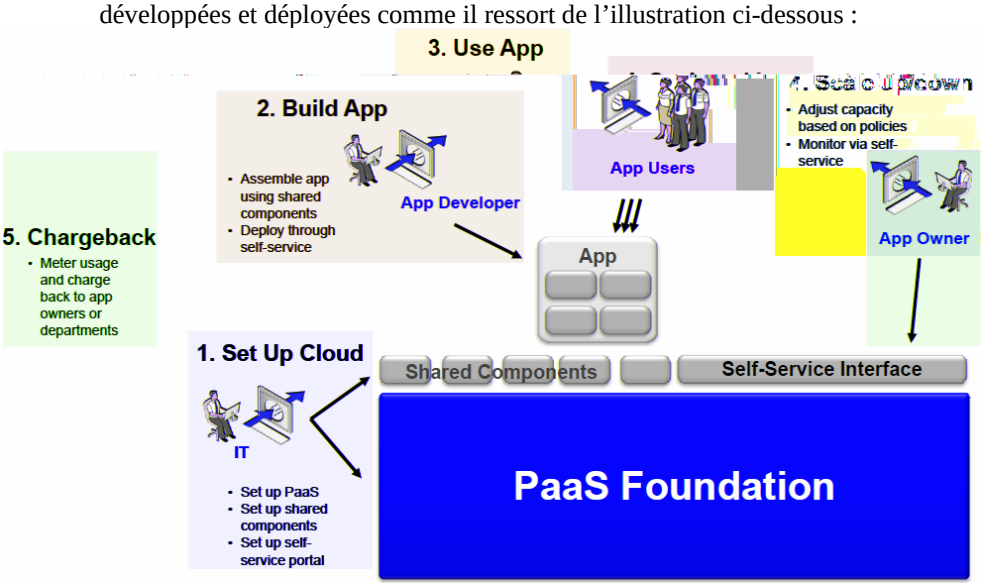


Figure 10: Concepts du PaaS selon Oracle

Leurs « Fusion Middleware technologies » fournissent différents services dont une plateforme Weblogic scalable, une plateforme de traitement de transactions, une suite BPM, un portail self-service et une User Access Management Suite intégrée.

IBM est également présent sur le marché du PaaS son « WebSphere CloudBurst Appliance », permettant de déployer et de gérer facilement et de manière contrôlée des applications WebSphere où la sécurité, la disponibilité, etc. sont prises en charge par la plateforme.

L'utilisation et la pénétration du marché du PaaS sont actuellement encore restreintes, on peut cependant remarquer que l'intérêt des utilisateurs se focalise surtout sur le PaaS privé.

La communauté open source se dirige aussi lentement sur le terrain du PaaS, bien que timidement étant donné que le PaaS soit surtout pertinent dans un contexte d'entreprise. De nombreuses initiatives sont lancées, mais, actuellement, seul AppScale mérite vraiment une mention.

AppScale, avec à son origine la même équipe universitaire que pour le projet Eucalyptus, vise à construire une variante open source de AppEngine de Google. La plateforme permet de déployer des applications AppEngine sur Amazon EC2 ou Eucalyptus. Alors qu'Eucalyptus s'est développé en une entreprise

commerciale, il n'est aujourd'hui pas clair si AppScale peut lui aussi avoir un avenir commercial.

5.3. Software as a Service (SaaS)

Le SaaS [35] est actuellement la forme de cloud la plus connue et la plus populaire. Il s'agit aussi de la forme de cloud la plus ancienne et que chaque internaute utilise déjà peut-être sans s'en rendre compte ne serait-ce qu'au travers d'un Webmail tel que Yahoo, Gmail ou Hotmail. Le Web 2.0 [36] a apporté des technologies et concepts qui ont sensiblement enrichi le web et permettent la création d'applications aux interfaces très riches, les RIA [37] pouvant concurrencer les clients lourds traditionnels.

5.3.1. Public

Le SaaS public est la forme de cloud où le marché est le plus riche. Il existe des solutions couvrant quasiment tous les besoins : mail, bureautique, intranet, gestion d'utilisateurs, applications multimédia, ... Pour avoir un rapide aperçu de la richesse de l'offre, on peut consulter le site Go2Web2 [38] qui répertorie un grand nombre d'applications classées par catégories. C'est également la forme de cloud où les solutions sont les plus volatiles. En cherchant sur le site Go2Web2, il arrive parfois de trouver un service suspendu.

Parmi les solutions plus pérennes, difficile de ne pas parler de Google Apps. La suite bureautique de Google composée de différents outils : Google Docs, Gmail, Google Calendar, Google Talk,… En dehors du Webmail qui gagne en popularité, Google Docs, qui se positionne comme un concurrent de Microsoft Office avec lequel il est compatible, séduit de plus en plus. Web 2.0 oblige, l'accent est mis sur la collaboration.

La solution s'avère simple d'emploi et peu de problèmes ont été rencontrés lors des tests. Au niveau de la compatibilité avec Microsoft Office, des documents utilisant les templates de Smals ont été chargés dans le système. Dans l'ensemble, le résultat était bon hormis quelques modifications dans la mise en page principalement des schémas qui n'apparaissaient pas toujours au bon endroit. Concernant ces derniers, il est à noter que lors de l'exportation d'un document Google Docs vers le format Microsoft Office, les schémas sont convertis en images et ne sont donc plus éditables.

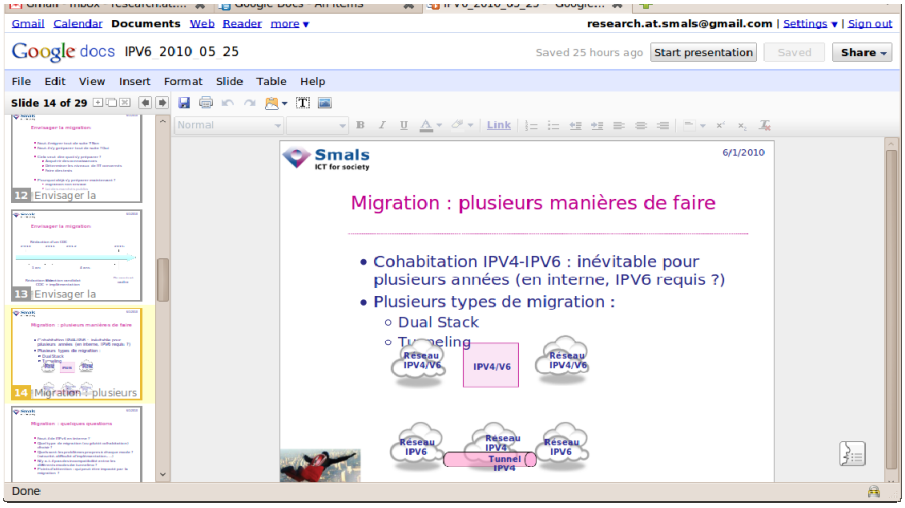


Figure 11: Interface utilisateur de Google Docs. Ici, il s'agit de l'édition d'une présentation.

Recommandation : *privilégier les services fournis par les gros fournisseurs. Vérifier aussi les moyens d'exporter les données pour préparer une éventuelle sortie.*

5.3.2. Privé

Le SaaS privé consiste à créer ses propres applications que l'on déploie sur une infrastructure privée. Jusque là, rien de bien différent par rapport aux applications traditionnelles sauf qu'ici, les applications doivent être pensées pour exploiter la puissance des machines du cloud (privé).

En passant du mainframe au cloud, on passe d'un modèle de Scale UP à un modèle de Scale OUT. Le premier a l'avantage d'être plus simple : le gain de puissance s'obtient en remplaçant le matériel ou du moins certains de ses composants par d'autres plus puissants. On a alors un potentiel de croissance limité par la puissance des machines disponibles sur le marché.

En optant pour le Scale Out, le gain de performance s'obtient en ajoutant des machines. L'augmentation de la puissance est, en théorie, quasi illimitée, mais est dans les faits alors limitée par le budget disponible pour l'ajout de machines et également par la capacité à produire du code adapté aux infrastructures parallèles.

Par ailleurs, avant de vouloir paralléliser un code, il faut s'assurer que cela permettra effectivement d'avoir un gain substantiel : le simple fait de doubler le nombre de processus ne suffit pas pour doubler les performances.

La loi d'Amdahl permet de calculer le gain théorique maximum que l'on peut obtenir en parallélisant un code. Pour cela, il faut appliquer une formule qui tient compte de la proportion de code parallélisable, appelée *s*, dans un programme et le gain est parfois décevant. Par exemple, pour un programme dont le *s* vaut 0.5, en passant d'un processus à 2, le gain de temps sera au maximum de 25%. En pratique, le gain sera même inférieur à 25% car la formule ne tient pas compte de certaines contraintes matérielles telles que l'affinité processeur (qui fait qu'une tâche peut passer d'un processeur à l'autre nécessitant le transfert des registres et du cache du processeur source vers le processeur de destination).

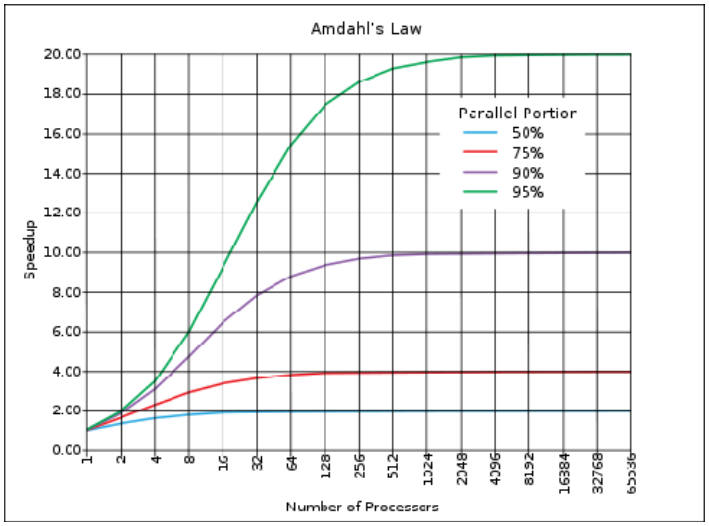


Figure 12: Loi d'Amdahl. Gain de performances par rapport à la proportion de code parallélisable.

Pour obtenir de bonnes performances, il peut être nécessaire de repenser l'algorithme pour en augmenter le paramètre *s*.

Il est également conseillé d'utiliser une librairie/framework de parallélisation plutôt que de gérer ces aspects soi-même. Dans le domaine du cloud, *MapReduce* [68] est assez populaire : ce framework introduit par Google facilite la création d'applications parallèles sur des données volumineuses. Pour simplifier, la parallélisation s'effectuera en 2 étapes :

Map : Un noeud va découper le problème en sous problèmes et les transmettre à d'autres nœuds (nœuds fils). L'opération pourra être répétée de manière récursive par ceux-ci.

Reduce : Après avoir effectué leur travail, les nœuds retournent leur résultat au nœud qui leur avait soumis la tâche (nœud parent). Celui-ci combinera les résultats reçus et les enverra à son tour à son nœud parent (s'il en a un).

Ici aussi il peut être nécessaire de repenser l'application pour que les données puissent être fragmentées de la sorte.

5.4. Tableau récapitulatif

Le tableau suivant donne un aperçu des fournisseurs qui offrent actuellement des solutions sérieuses. Dans chaque cas, la maturité de leur solution est suffisante pour être utilisée en production ou du moins, le produit semble prometteur et mérite que l'on s'y intéresse.

Au niveau du SaaS public, étant donné l'énorme quantité de solutions disponibles sur le marché, le tableau se limite aux solutions les plus génériques répondant à des besoins classique (mail, suite bureautique, CRM, BPM).

Pour le SaaS privé, aucun fournisseur n'est retenu étant donné que le SaaS privé revient à développer ses propres applications de manière telle qu'elles disposent des caractéristiques mentionnées au point 1.2.

	Public	Private
IaaS	Amazon EC2 Rackspace GoGrid	Fujistu EMC V-Plex
PaaS	Force.com Microsoft Azure Google App Engin	Oracle Fusion IBM CloudBurst
SaaS	Google Apps Saleforce NetSuite	

5.5. Exemples d'utilisation

C'est peut-être un effet du hype qui entoure le cloud, mais actuellement, dans la presse, on trouve plus d'articles sur les nouveaux produits que sur des exemples d'implémentation. Pourtant le cloud est utilisé, son usage reste encore marginal mais progresse et ce, de manière paradoxale.

Pour le moment, le principal obstacle à l'adoption du cloud est la sécurité : en d'autres termes, les entreprises ne font pas confiance aux fournisseurs sur ce point. Cependant, dans les faits, la progression du cloud est essentiellement due au SaaS, c'est-à-dire la forme de cloud où la confiance vis-à-vis du fournisseur doit être la plus grande en matière de sécurité.

Fin 2009, 12% des sociétés françaises utilisaient au moins un service à la demande et, si la tendance se poursuit, cela pourrait passer à 24% fin 2010 [39]. Estimer le nombre d'entreprises qui utilisent le cloud n'est cependant pas aisé compte tenu du fait que certaines exploitent des services SaaS sans pour autant l'associer au cloud.

5.5.1. Secteur privé

Au sein des utilisateurs du cloud dans le secteur privé, on retrouve aussi bien des petites que des grandes sociétés. Parmi les petites sociétés, il y en a qui s'appuient sur la puissance de calcul mise à disposition par les géants de l'informatique pour fournir leur propre service cloud. C'est notamment le cas d'Animoto [40]. Cette dernière offre la possibilité d'effectuer du montage vidéo en ligne. Leurs services sont également disponibles sur le célèbre site Facebook. À un moment donné, probablement suite à un effet de buzz, Animoto a dû gérer 750 000 inscriptions en 3 jours et plus de 25 000 utilisateurs simultanés par heure. Ce pic a pu être géré sans problèmes par Animoto grâce à l'infrastructure d'Amazon.

Pour les petites sociétés, Amazon peut constituer une solution efficace pour pouvoir fournir un service qui s'adapte à une demande susceptible de varier fortement. C'est également le cas de Dropbox [41], un service de stockage de fichiers en ligne qui utilise l'espace disque d'Amazon.

Le cloud peut aussi servir pour des besoins ponctuels. C'est ce qu'a fait le NY Times. Leur objectif était de créer une immense base de données numérique regroupant des articles datant de plus de 100 ans. Ceux-ci ont été numérisés en 405 000 fichiers TIFF volumineux qu'il fallait convertir en 810 000 fichiers PNG (la moitié de ces images sont des miniatures des images originales). À cela s'ajoutent 3,3 millions de fichiers SGML (les articles en format texte) et 405 000 fichiers javascripts (qui contiennent les coordonnées des articles au sein des images scannées). Le traitement de toutes ces données a été réalisé en moins de 36 heures au moyen d'une centaine d'instances d'Amazon. Le résultat est à présent disponible sur le web [42].

Pour les petites sociétés, l'intérêt du cloud public est assez évident : il leur permet de bénéficier de services sans avoir à acquérir de ressources (matérielles ou humaines). Pour les grandes entreprises, le cloud public peut également fournir des solutions intéressantes en particulier pour des commodités telles que l'e-mail ou la bureautique.

C'est le choix fait la société Valeo (spécialisée dans l'électronique embarquée pour automobile). Celle-ci est constituée de 193 sites répartis dans 27 pays et a choisi d'opter pour Google Apps pour ses 30 000 employés connectés au Web. L'objectif annoncé était une amélioration de la collaboration entre les employés répartis sur les différents sites. Chose regrettable dans cet exemple : il aurait été intéressant de connaître les coûts de migration pour lesquels Valeo reste assez discret. La seule information officielle est que le coût le plus important résidait dans les formations des utilisateurs afin de leur apprendre à travailler différemment [43]. Quand au ROI, il faudrait entre 1 et 3 ans pour pouvoir en bénéficier : la durée dépendra de la rapidité avec laquelle les utilisateurs vont exploiter les fonctionnalités collaboratives de Google Apps.

Un exemple assez impressionnant d'utilisation du cloud est celui de MySpace. Afin de tester une nouvelle fonctionnalité, il leur fallait simuler 1 000 000 d'utilisateurs simultanés. Ce test (ponctuel et intensif) a été réalisé au moyen d'Amazon. Pour y parvenir, ils ont utilisé 800 instances d'Amazon pendant 20 minutes [44]. À titre d'information, voilà ce qui a été simulé :

- 1 million d'utilisateurs simultanés
- Débit réseau de 16 gigabits par seconde
- 6 terabytes de données transférées par heure
- 77000 hits par seconde

5.5.2. Secteur public

Le secteur public s'intéresse également au cloud, mais plus particulièrement au cloud privé. Parmi les pays qui s'intéressent au cloud, il y a naturellement les Etats-Unis [45], mais aussi le Japon [46], la Chine [47], Singapour [48], la Corée du Sud [49] et le Royaume-Uni [50].

L'initiative de ce dernier est assez séduisante. Leur objectif est de créer un cloud privé qui servirait l'ensemble de la fonction publique du pays. Ce projet impliquerait plusieurs choses :

- La mutualisation des centres de données du pays qui ferait passer leur nombre de 120 à 12 ou 13.
- Un inventaire de toutes les applications utilisées par la fonction publique (estimées à 10 000).

- Une rationalisation de ces applications (que l'on utilise Exchange, Notes ou autre, le besoin est le même : de la messagerie électronique).
- Création d'un catalogue d'applications auquel auraient accès les fonctionnaires. Ceux-ci pourraient ou non utiliser certaines applications suivant l'organisme pour lequel ils travaillent.

6. Use cases, recommandations & checklist

Ce chapitre propose quelques exemples d'utilisations potentielles du cloud ainsi que des recommandations. Choisir une solution dans le cloud pour un usage à long terme n'est naturellement pas une opération anodine, il convient donc de prendre certaines précautions. Pour cela, une checklist est proposée : celle-ci regroupe quelques questions à se poser avant d'opter pour une solution dans le cloud (principalement pour un usage à long terme).

6.1. Use cases

6.1.1. Introduction

La question de savoir quand et quelle forme de cloud computing est intéressante dépend fortement du contexte. Pour les star

utilisés afin de transformer progressivement le data center en un cloud privé. Nous aborderons plus en détail quelques exemples concrets d'utilisation des clouds privé et public.

6.1.2. Cloud public

Le SaaS public fournit des solutions prêtes à l'emploi généralement simples à utiliser et à moindre coût. Si l'on prend l'exemple d'un système d'enquête, il existe des solutions bon marché telles que SurveyMonkey [51]. Celle-ci coûte 200 € par an (ou 16,67€ - 19,95€ par mois) : il est évident qu'il n'est pas possible de mettre en place en interne une solution similaire pour le même prix.

Si pour des besoins ponctuels, le choix d'une solution peut s'effectuer relativement facilement pour une utilisation à moyen ou à long terme, des précautions sont requises : pérennité du service, possibilité d'exporter les données dans un format ré-exploitable, ...

De manière générale, pour des besoins standardisés, le SaaS est une solution sérieuse. SalesForce, avec son CRM, en est la preuve [52] : cette société fondée en 1999 a plus de 72 000 clients.

Parmi la grande quantité d'applications que l'on retrouve dans le cloud, l'e-mail est la plus ancienne et la plus populaire. En 1996, c'est à dire il y 15 ans, Hotmail était lancé. Un an après, le système a été racheté par Microsoft et a sensiblement évolué pour devenir Windows Live Hotmail, un système utilisé par 360 millions de gens dans le monde. Hotmail n'est pas la seule solution à avoir atteint un tel niveau de popularité : Yahoo Mail regroupe plus de 275 millions d'utilisateurs.

En plus de 10 ans d'existence, le Webmail a su mûrir et a fait ses preuves. Utiliser une boîte e-mail dans le cloud pour usage professionnel est tout à fait possible : fin 2009, 2 millions d'entreprises avaient opté pour Google Apps et son système de messagerie [53].

Un argument en faveur des webmails est leur popularité auprès des utilisateurs en raison de leur simplicité d'emploi, de leur légèreté et rapidité à l'inverse d'une application telle que Lotus Notes, particulièrement impopulaire auprès des utilisateurs [54]. Par ailleurs, les utilisateurs en connaissent déjà les principes : cela fait déjà plusieurs années qu'ils les utilisent à usage privé.

Afin de faciliter la migration depuis Lotus Notes vers Google Apps, Google fournit des outils [55] qui permettent d'automatiser la migration des comptes. Pour ceux qui souhaiteraient aussi migrer les applications développées en Notes, force.com fournit également des outils pour passer les applications Notes dans le cloud [56].

Comme mentionné précédemment, le Webmail est une solution mûre qui a déjà séduit des centaines de millions utilisateurs. Il s'agit là d'un cas intéressant qui mérite d'être envisagé. En matière de coût, alors qu'il faut environ 110€ par an et par utilisateur pour Lotus Notes sans même compter le prix du matériel (+ électricité + maintenance de ce dernier), Google Apps ne coûte que 40€ par an et par utilisateur sans devoir gérer de serveurs [57].

De son côté, le **PaaS public** offre des opportunités en matière d'hébergement Web. Tout comme le Webmail, l'hébergement Web n'est pas nouveau et les offres professionnelles d'hébergement mutualisé sont nombreuses. On peut ainsi très facilement trouver des plateformes LAMP pour 2 à 10€ par mois (support compris). L'hébergement Java EE existe lui aussi, mais est plus cher : de 3 à 40€ par mois [58]. Dans ce domaine, il y a probablement des opportunités intéressantes : ces sociétés spécialisées dans l'hébergement offrent bien souvent un service de qualité à des tarifs très agressifs.

L'IaaS et PaaS publics peuvent s'avérer intéressants pour les développeurs. Lorsque ceux-ci sont amenés à faire des tests, il est parfois préférable de travailler sur un système dédié : lorsqu'il s'agit de réaliser un test pouvant mettre à mal la stabilité ou la sécurité d'un système, il est évident que le test ne doit pas être réalisé sur une machine ou sur un environnement où sont exécutées d'autres tâches. Il est alors intéressant de pouvoir accéder à un environnement (PaaS) ou à une machine virtuelle (IaaS) dédiée. Une solution telle qu'Amazon s'avère utile : le développeur peut créer une instance d'un système le temps d'effectuer ses tests. L'instance sera alors ensuite détruite. Il y a cependant un risque : le contrôle de la quantité de ressources allouées. La création des machines virtuelle est aisée : sans une certaine rigueur, on peut vite se retrouver avec un grand nombre de machines virtuelles en cours d'exécution. Un raisonnement similaire peut être appliqué avec des solutions de type PaaS : au moyen de ce dernier, l'utilisateur peut disposer d'une puissance de calcul conséquente pour tester ses programmes.

Le principal avantage de ce procédé est la flexibilité : les utilisateurs ont la possibilité d'accéder à des ressources au moment voulu alors qu'en interne, il peut s'écouler plusieurs semaines entre le moment où une ressource est demandée et le moment où cette dernière est acquise et utilisable.

6.1.3. Cloud privé

Le SaaS privé ne peut s'envisager que si l'on dispose d'un service standard que l'on souhaite délivrer à ses clients. Les applications nécessitant des adaptations pour chaque client ne sont pas de bonnes candidates pour le SaaS.

Quels services proposer sous forme de SaaS ? Des commodités tel qu'un service de messagerie électronique. On peut aussi imaginer un service de gestion de contenu accessible à la demande : à travers une interface web, l'utilisateur a la possibilité de créer une instance d'un CMS (préconfigurée) et de la personnaliser sans avoir besoin de qui que ce soit. Ceci permettrait la mise en œuvre rapide de sites web élémentaires (ex : site annonçant un évènement).

Les opportunités en matière de **IaaS et PaaS privés** sont similaires à celles de leurs homologues publics. Après avoir testé l'utilisation de l'IaaS et PaaS publiques pour la réalisation de tests, on peut envisager, si l'expérience est concluante, de créer une infrastructure similaire en interne. Tout comme pour le cloud public, les développeurs auraient la possibilité d'allouer eux-mêmes les ressources requises pour leurs tests. L'avantage par rapport au cloud public serait d'avoir un meilleur contrôle de la quantité de ressources utilisées par chacun, du moins pour l'IaaS. Au moyen du PaaS, il est possible de créer une grande plateforme de développement commune pour l'ensemble des développeurs présents.

Concernant le PaaS, en raison du faible choix disponible pour le moment, la marge de manoeuvre est assez réduite. Si l'on prend le cas de la solution d'Oracle décrite au point 5.2.2, déployer une infrastructure de ce type est naturellement coûteux. Il convient donc d'avoir suffisamment d'applications pouvant être portées sur cette plateforme.

***Recommandation** : commencer par du cloud public. Le coût d'entrée y est plus faible et il y a peu de choses à préparer pour prendre connaissance de la solution.*

6.2. Recommandations

Il est évident que le cloud a été un sujet overhypé et que l'aspect marketing a été fortement exploité par les fournisseurs qui se sont empressés d'adapter leurs solutions pour en faire quelque chose qui puisse être assimilé au cloud. Cela ne doit pas faire perdre de vue qu'il existe de réelles opportunités dans le cloud. Ne pas s'intéresser à ce dernier serait une erreur.

Pour un besoin ponctuel, les solutions de type SaaS s'avèreront bien souvent meilleur marché qu'une solution traditionnelle. Pour un usage sur une courte période (ne dépassant pas une année), les risques sont moindres que pour une utilisation prolongée.

Pour une solution devant être utilisée de manière récurrente et sur une durée prolongée, des précautions supplémentaires doivent être prises. Pour cela, la checklist proposée au point suivant énonce diverses questions auxquelles il faut idéalement pouvoir répondre avant d'utiliser un service.

Bien que présentant des avantages certains, le cloud n'est cependant pas une solution miracle qui garanti une réduction des coûts pour tous les projets. Au niveau financier, les avantages se situent dans la flexibilité surtout au niveau du provisionnement (on ne paie que pour un nombre de ressources équivalent aux besoins) et aussi dans le fait qu'il n'est pas nécessaire de se soucier de la maintenance des logiciels et des serveurs qui les accompagnent. Si la période d'utilisation s'étend sur plusieurs années, il ne faut pas négliger le fait que la notion d'amortissement n'existe pas dans le cloud : durant toute la période d'utilisation, les ressources sont louées.

Si, dans un projet, la partie des coûts liés à la gestion et maintenance des machines et logiciels ne représente qu'une faible part des coûts globaux, il ne faut pas espérer de réduction sensible des coûts simplement par le fait de placer ses infrastructures dans le cloud. Sur une période plus longue, cela pourrait même se traduire par un effet inverse : une augmentation des coûts.

Au niveau de la sécurité, l'existence de risques est une notion réelle et bien intégrée auprès des utilisateurs. On constate malheureusement que les risques sont parfois mal évalués, voire mal compris. De manière générale, les services dans le cloud sont mieux sécurisés que les services in-house. Il est cependant vrai que le cloud présente de nouvelles opportunités pour les pirates qui y trouvent une énorme masse d'utilisateurs. Le Patriot Act expliqué au point 3.3 est, pour le moment, le principal « élément perturbateur » lorsque la question de la sécurité est abordée.

Les principaux acteurs du cloud sont actuellement tous américains : les craintes liées aux conséquences du Patriot Act sont donc bien réelles. Le cloud n'est cependant pas exclusivement lié aux Etats-Unis : on trouve des solutions SaaS ou IaaS créées et hébergées ailleurs (ex : BlueKiwi, Combell, PlanetHoster, …). Au niveau du PaaS, il est plus difficile de trouver un fournisseur indépendant des Etats-Unis.

Même si le cloud privé est perçu comme étant plus rassurant et offre un meilleur contrôle des couches systèmes sous jacente, il est cependant recommandé de faire ses premiers pas dans le cloud public : ce dernier est déjà opérationnel et peut donc servir de source d'inspiration pour une création ultérieure d'un cloud privé. Le cloud public peut donc servir à la phase d'apprentissage.

Concrètement, sans pour autant présager d'une éventuelle utilisation du cloud, il est déjà possible d'entreprendre les actions suivantes :

- acquérir de l'expérience avec le cloud public pour des besoins simples;

- comprendre quels sont les avantages réels du cloud computing dans le contexte actuel de l'entreprise ;
- analyser les risques et les comparer aux risques actuels ;

	Public Faibles coûts (au départ)	Private Coût d'entrée élevé
IAAS	Besoin rapide et ponctuel de serveurs (ex : pour faire des tests)	Mutualisation de serveurs de test Mutualisation du stockage
PAAS	Besoins élémentaires (ex : web hosting 50-200€/an)	Plate forme de développement
SAAS	Besoins standardisés (ex : SurveyMonkey 200€/an)	"Services spécifiques"

Figure 13 : Quel modèle de cloud choisir et pour quel type d'usage.

- identifier les projets pouvant être transférés au cloud.

6.3. Checklist

Utiliser une solution dans le cloud ne s'improvise pas. Il faut préalablement se poser quelques questions. Les points qui suivent proposent un ensemble de questions essentielles à se poser avant d'opter pour une solution devant être utilisée sur une longue période (plus d'un an).

6.3.1. Business case

- Le delivery model est-il adapté ?
- Où exactement se situent les coûts ? Si l'essentiel du coût d'un projet ne réside pas dans l'achat, la gestion et la maintenance des infrastructures, les gains liés à l'utilisation du cloud ne seront pas conséquents.
- La feuille de route business du fournisseur correspond-elle à celle de l'entreprise ?

6.3.2. Compliance

- L'intégrité et la sécurité des données peuvent-elles être garanties ?
- Le fournisseur est-il accrédité ? (ex. SAS70-II)
- Où les données se trouvent-elles ? (physiquement)
- En tant qu'utilisateur, que peut-on contrôler ? (monitoring, informations en cas de pannes, …)
- Les données peuvent-elles être récupérées sous une forme utilisable ? (e-discovery)

- Quelle est la stratégie de back-up/disaster recovery du fournisseur ?

6.3.3. Économique

- Quel coût est-il lié à la récupération des données ? (par exemple, pour pouvoir changer de fournisseur)
- Existe-t-il des vendeurs alternatifs sur le marché afin d'éviter le « vendor-lock-in » ?
- Le fournisseur retenu est-il stable ? Le marché est-il mature ?
- Quel est l'impact d'une faillite du fournisseur ?
- Le savoir-faire nécessaire est-il disponible dans notre pays, par exemple en matière de consultance ?
- Quelle est la réputation du fournisseur en matière de continuité et de support ?
- Les conditions du contrat sont-elles intéressantes (peut-on négocier, peu ou pas, sur les conditions) ?
- Que se passe-t-il en cas de non respect de la SLA ? Les dédommagements du fournisseur suffissent-ils à couvrir les frais liés au non respect de la SLA ?
- Quel est l'impact du modèle de coût du service choisi ?

6.3.4. Intégration

- Comment le User Access Management et SSO seront-ils intégrés ?
- Les données actuelles peuvent-elles être migrées vers la solution choisie ?
- Les processus internes sont-ils prêts à fonctionner avec des services Web ?

6.3.5. Technique

- Les mises-à-jour sont-elles transparentes ?
- Quel est l'impact sur le réseau interne ? (utilisation de la bande passante)
- La scalabilité nécessaire peut-elle être livrée ?

6.3.6. Sécurité

- Qui a accès à vos données ?
- Y a-t-il une séparation physique entre les données et leurs back-ups ?
- Chiffrez les back-ups
- Vérifiez la présence ou non de rootkits

- Signaler tout changement anormal dans les données ou logiciels (ex avec l'IaaS : en cas de redémarrage forcé d'une machine virtuelle, vérifier que cette dernière n'a pas été modifiée)

6.3.7. Organisationnel

- Existe-t-il une politique en matière de IaaS visant à éviter la prolifération de serveurs virtuels ?
- Les possibilités de reporting sont-elles suffisamment étendues ?
- Existe-t-il, en interne, de l'expérience en négociation de contrats cloud ?
- Est-on préparé à la nouvelle prestation de services ? (par exemple en matière de politique des licences, d'intégration dans la CMDB et l'orientation service)
- Est-ce que le fournisseur est en mesure de délivrer le support requis ?

7. Conclusion

Le cloud computing a été le hype de l'année 2010 et fera encore beaucoup parler de lui en 2011. Les avis sont très partagés à son sujet. Alors que certains y voient un potentiel énorme, d'autres sont plutôt inquiets car ils y voient des risques en matière de sécurité et une dépendance plus accrue que jamais vis-à-vis d'un fournisseur. Quoiqu'il en soit, le cloud ne laisse personne indifférent.

Le sujet a été très souvent traité dans la presse à un point tel que toute personne travaillant dans le milieu informatique en a certainement déjà entendu parler. Assez paradoxalement, définir le cloud reste encore un exercice ardu, même lorsqu'il s'agit de citer les grands concepts du cloud ou du moins ce qui est supposé caractériser les services dits cloud, tout le monde n'est pas d'accord. Cela n'est pas sans rappeler le flou qui a entouré le Web 2.0 pour lequel, même à l'heure actuelle, il est difficile de trouver une définition mettant tout le monde d'accord. Ce qui est certain, c'est que le Web 2.0 est, avec la virtualisation, une « technologie » qui a rendu possible la naissance du cloud. Avec le Web 2.0 sont arrivés un ensemble de techniques d'applications riches telles qu'Ajax qui ont permi la création d'interfaces web riches se rapprochant de plus en plus de ce qui se fait au niveau des clients lourds. La virtualisation, quant à elle, a rendu possible le provisionnement en temps réel.

Le cloud ne se limite pas qu'à quelques aspects techniques : les aspects organisationnels sont également importants. Le changement le plus radical est peut-être le modèle économique dans lequel on n'achète plus un produit, mais où l'on loue un service. En quelque sorte, en utilisant un service dans le cloud, on va tout simplement louer de la puissance de calcul auprès d'un fournisseur afin d'exécuter des applications. En partant de ce point de vue, on peut alors considérer le cloud comme étant un immense supermarché de l'IT.

Derrière ce cloud, on retrouve en premier lieu des géants de l'informatique qui mettent à disposition leur énorme puissance de calcul répartie dans plusieurs data centers afin de fournir toutes sortes de services. On retrouve aussi un grand nombre de petits acteurs qui proposent également leurs services parfois même en utilisant les ressources mises à disposition par les grands acteurs.

Il existe une classification des types de services que l'on retrouve dans le cloud. Celle-ci s'effectue sur deux dimensions : une première va déterminer le niveau d'abstraction qui est réalisé (IaaS, PaaS, SaaS), le second permet de déterminer si le cloud est situé dans l'entreprise même ou chez un tiers (Public, Privé, Hybride, Privé virtuel).

Actuellement, le SaaS public est la forme de cloud la plus populaire qui consiste à mettre à disposition du monde des applications prêtes à l'emploi. À ce niveau, l'offre est très riche : il est actuellement possible de trouver des solutions SaaS pour quasimment tous les besoins traditionnels (boîtes e-mail, intranet, CRM, stockage, montage vidéo, …). Il y a là de réelles opportunités à ne pas manquer. Si l'on reprend le cas de SurveyMonkey cité au point 6.1.2, il est évidemment

impossible de bâtir soi-même une offre similaire à un coût si bas. L'offre est également assez volatile et ce parfois même auprès des grands fournisseurs (cf. point 2.2.2). Si pour un usage ponctuel, cela ne représente pas un grand risque, pour une utilisation à long terme, certaines précautions sont donc à prendre.

La première concerne la sécurité. Les entreprises l'ont déjà compris au point tel qu'il s'agit actuellement du principal obstacle à l'adoption du cloud (cf. point 3) ; le Patriot Act ne va pas contribuer à rassurer les utilisateurs potentiels. Il doit d'ailleurs être pris en considération lors du choix d'une solution ou du moins le lieu d'hébergement des données : si le fournisseur en offre la possibilité, il faut privilégier la zone européenne aux Etats-Unis. À cela, il faut ajouter le fait que le cloud implique l'usage d'Internet (le plus grand vecteur de malwares existant) et d'un navigateur web (le type d'applications pour lesquelles on trouve le plus grand nombre de failles de sécurité).

La crainte en matière de sécurité est réelle et tout à fait légitime. Sur le terrain, cela se traduit par une très nette préférence du cloud privé : d'après une étude réalisée par Brocade (qui vend des solutions de virtualisation), 60% des sociétés européennes l'envisageraient d'ici 2012 [59].

Fournir un service sécurisé est donc un enjeu capital pour tout fournisseur de cloud. Sur ce point, on peut raisonablement faire confiance aux géants de l'informatique : étant donné les enjeux du cloud et les sommes déjà investies dans les immenses data centers qu'ils ont construits, ne pas sécuriser leurs systèmes pourrait s'avérer très coûteux voire fatal pour leurs services. Malgré cela, nul n'est infallible, même les géants ont parfois des problèmes : les services d'Amazon [60] et Google [61] ont déjà connu des pannes de plusieurs heures et même des problèmes de sécurité [62]. Pour les petits acteurs, la situation est plus délicate encore : les moyens mis en œuvre ne sont pas les mêmes. À titre d'exemple, au début du mois d'août 2010, Evernote (un service de prise de notes en ligne) a confirmé que plus de 6000 utilisateurs pouvaient avoir perdu leurs données suite à un problème [63].

Pour le secteur public, le cloud présente des opportunités et ce, particulièrement en temps de crise. Pour les petites entités, le cloud public, surtout au travers du SaaS, peut fournir des solutions efficaces pour des besoins tels que la messagerie : Google Apps sera une alternative intéressante à Lotus Notes ou Exchange. Cette solution peut également être utilisée comme espace de stockage : le To y est facturé 256$ [64] par an. Google Apps peut aussi servir d'intranet et permet la création de pages Web avec insertion de documents divers. En dehors de l'aspect coût très intéressant, l'avantage est qu'il n'y a aucun serveur à gérer et peu de connaissances techniques sont requises pour l'administration. L'usage de ces solutions crée cependant une très forte dépendance vis-à-vis du fournisseur.

À moyen et long terme, le private cloud pourrait offrir une solution grâce au IaaS et PaaS. Grâce à ces derniers, il serait possible de créer une grande infrastructure sur laquelle pourraient être développées les nouvelles applications de la sécurité sociale.

Parmi les solutions disponibles dans le cloud public, toutes n'offrent naturellement pas la même qualité de service : la richesse, les performances et le support varient d'une solution à l'autre. Étant donné que l'on n'achète pas un service dans le cloud, mais qu'on le loue, la pérennité du service est un critère capital dans le choix d'une solution. Il faut également prévoir un scénario de sortie du cloud : en cas d'arrêt imminent de service, sera-t-il possible de récupérer facilement les données dans un format réutilisable ?

Dans le cadre du secteur public, on peut comprendre les craintes et réticences en matière de sécurité. L'argument juridique (cf. point 2.2.3) est, quant à lui, plus

problématique car impossible à négocier. Le cloud privé semble donc plus séduisant. À ce niveau-là, l'approche britannique est peut-être le modèle à suivre : la création d'un grand cloud privé dédié à l'ensemble de la fonction publique du pays. Pour des besoins standardisés, le SaaS public est certainement l'option à choisir (si aucun obstacle juridique ne l'empêche).

Malgré des débuts difficiles, le cloud trouve son chemin petit à petit : les entreprises sont passées progressivement du stade de la curiosité au stade de l'intérêt pour en arriver finalement doucement à l'adoption. Celle-ci est encore minoritaire et en cours de planification pour la plupart. Le constat est à peu près le même dans le secteur public où le cloud intéresse de plus en plus. À nouveau, l'initiative britannique, à savoir la création d'un cloud pour l'ensemble de la fonction publique, pourrait servir de modèle aux autres pays d'Europe.

Le cloud est encore jeune, trop jeune pour que l'on puisse le qualifier de mature. Quoi qu'il en soit, il fera encore parler de lui pendant longtemps. Lorsque l'on regarde les sommes investies par les géants de l'informatique dans la création d'infrastructures et solutions dédiées au cloud, il est évident qu'ils ne sont pas prêts de le laisser tomber. Sans pour autant être une révolution, le cloud public s'avèrera très pratique notamment pour les petites sociétés n'ayant pas les moyens humains et financiers d'investir dans des commodités de base tel qu'un serveur d'e-mails. Les grandes sociétés, quant à elles, vont privilégier le cloud privé. Il est vrai que le cloud a monopolisé la presse informatique cette année et que l'aspect marketing était lui aussi présent. Cela ne doit pas faire perdre de vue qu'il y a de véritables opportunités à saisir dans le cloud et y rester indifférent serait une erreur. On peut d'ailleurs constater que même les sociétés qui n'ont pas l'intention de se lancer dans le cloud s'intéressent à ce dernier, ce qui est une preuve qu'en dehors du tapage médiatique, le cloud n'est pas un concept vaporeux, mais bien une réelle innovation.

8. Bibliographie

[1]	"Leading in Times of Transition: The 2010 CIO Agenda" , Gartner, januari 2010
[2]	Definition of Cloud Computing – Again : http://jameskaskade.com/?p=594
[3]	La révolution industrielle ... Informatique : http://nauges.typepad.com/my_weblog/2010/04/la-r%C3%A9volution-industrielle-informatique.html (http://bit.ly/98zkBv)
[4]	Virtualisation de Serveurs – une technologie bien réelle. Grégory Ogonowski. Smals, Research. November 2008
[5]	Software as a Service en Public Cloud Computing. Adelbert Groebbens. Smals, Research. August 2009
[6]	Magnolia : http://blogs.techrepublic.com.com/tr-out-loud/?p=805
[7]	Laurent Lachal , "Cloud governance: an overview", OVUM, 1 juni 2010
[8]	The Data Liberation Front : http://www.dataliberation.org/
[9]	Test Acid 3 : http://acid3.acidtests.org/
[10]	Portio Research, decembre 2009
[11]	myOneLogin : http://www.myonelogin.com/?ref=tricipher_home
[12]	Secure the cloud : http://www.securethecloud.com/
[13]	Cloud Sherpas : http://www.cloudsherpas.com/
[14]	Desktop Single Sign-On / Enterprise Single Sign-On. Bob Lannoy. SMALS, Research. July 2007
[15]	Cheap VPS Hosting : http://www.cheapvps.co.uk/
[16]	Webhost hack wipes out data for 100,000 sites : http://www.theregister.co.uk/2009/06/08/webhost_attack/
[17]	LxCenter : http://lxcenter.org/
[18]	ITL Resources : http://www.invisiblethingslab.com/itl/Resources.html
[19]	Bescherming van de interne gegevens – Beveiliging van gevoelige data in de organisatie. Pieter Jorissen. SMALS. Feb 2009
[20]	Truecrypt : http://www.truecrypt.org/
[21]	Evil Maid goes after TrueCrypt! : http://theinvisiblethings.blogspot.com/2009/10/evil-maid-goes-after-truecrypt.html (http://bit.ly/2iiXBN)
[22]	Data Protection Act 1998 (c. 29) : http://www.statutelaw.gov.uk/content.aspx?activeTextDocId=3190610 (http://bit.ly/9iuEp6)

[23]	Safe Harbor : http://www.export.gov/safeharbor/
[24]	Amazon EC2 : http://aws.amazon.com/ec2
[25]	Amazon EC2 pricing : http://aws.amazon.com/ec2/pricing/
[26]	GOGRID : http://www.gogrid.com
[27]	Rackspace : http://www.rackspace.com/index.php
[28]	RightScale : http://www.rightscale.com
[29]	FlexiScale Public Cloud : http://www.flexiant.com/products/flexiscale/
[30]	Slicehost : http://www.slicehost.com/
[31]	Joyent : http://www.joyent.com/
[32]	Eucalyptus : http://open.eucalyptus.com/
[33]	OpenNebula.org : http://www.opennebula.org/
[34]	Abicloud : http://www.abicloud.org/
[35]	Software as a Service en Public Cloud Computing. Adelbert Groebbens. SMALS. August 2009
[36]	Web 2.0 : Enterprise 2.0 – Government 2.0. Karl Vom Berge, Adelbert Groebbens, Arnaud Hulstaert, Grégory Ogonowski, Bert Vanhalst. SMALS. January 2009
[37]	Rich Internet Applications : bruikbare en optimaal toegankelijke applicaties. Adelbert Groebbens. SMALS. June 2008.
[38]	Go2Web2 : http://www.go2web20.net/
[39]	Cloud computing : l'évolution soutenue des usages depuis 2008 ouvre à de nouvelles perspectives d'ici 2012 : http://markess-blog.typepad.fr/pressrelease/PR_SS10A_CLOUD_0510_FINAL.pdf (http://bit.ly/ciZqG2)
[40]	Animoto : http://animoto.com/
[41]	Dropbox : https://www.dropbox.com/
[42]	TimesMachine : http://timesmachine.nytimes.com/browser
[43]	Valeo roule pour les Google Apps... mais sans soulever le capot: http://www.lemagit.fr/article/google-bureautique-cloud-computing-projets-cloud/3405/1/valeo-roule-pour-les-google-apps-mais-sans-soulever-capot/ (http://bit.ly/9iAWll)
[44]	How MySpace Tested Their Live Site With 1 Million Concurrent Users : http://highscalability.com/blog/2010/3/4/how-myspace-tested-their-live-site-with-1-million-concurrent.html (http://bit.ly/cWYt9b)
[45]	Des Nuages pour réduire les dépenses informatiques du gouvernement : http://www.bulletins-electroniques.com/actualites/060/60527.htm
[46]	NTT commence les tests d'une nouvelle plate-forme en nuage : http://www.bulletins-electroniques.com/actualites/59720.htm
[47]	Le TS850, premier serveur chinois à 8 processeurs : http://www.bulletins-electroniques.com/actualites/63075.htm
[48]	Développement du Cloud Computing à Singapour : http://www.bulletins-electroniques.com/actualites/56044.htm
[49]	117 millions d'euros dédiés au développement du "cloud computing" en Corée : http://www.bulletins-electroniques.com/actualites/61610.htm
[50]	La stratégie TIC du gouvernement britannique : http://www.bulletins-electroniques.com/actualites/61976.htm
[51]	Surveymonkey : http://www.surveymonkey.com/
[52]	Salesforce : http://www.salesforce.com/
[53]	Google Apps séduit 2 millions d'entreprises, assure sa promo à l'international : http://www.clubic.com/actualite-306024-google-apps-2-millions-entreprises-campagne-promo.html (http://bit.ly/d8jd2I)
[54]	Survival of the unfittest : http://www.guardian.co.uk/technology/2006/feb/09/guardianweeklytechnologysection (http://bit.ly/14ksFU)

[55]	Make the swith from Lotus Notes : http://www.google.com/apps/intl/en/business/notes.html
[56]	Lost on Lotus Island ? : http://www.salesforce.com/campaigns/lotusmigration/
[57]	Le nouvel Economiste, n°1488 - Cahier 2 - du 10 au 16 septembre 2009, p.26.
[58]	Hébergement Java : http://www.hebergement-java.fr/ VISION Web Hosting : http://www.visionwebhosting.net/
[59]	Les entreprises Européennes migrent à grand pas vers le CLOUD computing : http://www.artesi.artesi-idf.com/public/article.tpl?id=21432 (http://bit.ly/9z4NkS)
[60]	Les déboires d'Amazon EC2 : http://www.presence-pc.com/actualite/Amazon-EC2-37511/ (http://bit.ly/8Vc0Oo)
[61]	Les limites du cloud computing : nouvelle panne sur Google App Engine : http://www.clubic.com/actualite-327080-panne-google-app-engine.html#alerte-neteco (http://bit.ly/d7yDtt)
[62]	Google, piraté, menace de quitter la Chine : http://www.lemonde.fr/asie-pacifique/article/2010/01/13/google-pirate-menace-de-quitter-la-chine_1290944_3216.html (http://bit.ly/8VZaCK)
[63]	Evernote's July 1st Server Problem : http://blog.evernote.com/2010/08/09/july1/
[64]	Stockage Google: Évolution des tarifs de stockage : http://docs.google.com/support/bin/answer.py?hl=fr&answer=165214 (http://bit.ly/basKKt)
[65]	20km de Bruxelles : http://chronorace-web.cloudapp.net/CMS20km.aspx
[66]	Service Oriented Architecture, .Bert Vanhalst. SMALS, Research. Maart 2006
[67]	La sécurité, le principal frein à l'adoption du cloud computing : http://www.colt.net/FR-fr/MediaCentre/COLT_086341
[68]	Introduction to Parallel Programming and MapReduce : http://code.google.com/intl/fr-FR/edu/parallel/mapreduce-tutorial.html

9. Glossaire

Ajax	Asynchronous JavaScript and XML. Ajax n'est pas une technologie à proprement parler, mais fait référence à l'utilisation conjointe de diverses technologies telles que HTML, CSS, Javascript, … Ajax est notamment utilisé pour effectuer des requêtes asynchrones pour rafraîchir certaines parties d'une page web. Ajax sert à la création de certaines applications de type RIA.
API	Application Programming Interface. Il s'agit de l'interface fournie par un programme/bibliothèque. L'API est utilisée pour faire interagir les programmes/librairies entre-eux.
Backdoor	Également appelée porte dérobée. Il s'agit d'une fonctionnalité présente dans un logiciel et inconnue de ses utilisateurs légitimes. La backdoor a pour objectif de fournir un point d'entrée dans le système pour une personne bien souvent malintentionnée. Une backdoor peut servir à transformer un logiciel en cheval de Troie.
Capex – Opex	Capital Expenditure – Operationnal Expenditure. Capex représente les dépenses d'investissement, Opex les dépenses d'exploitation. Par exemple, pour une imprimante, l'achat de cette dernière ainsi que la procédure d'achat sont le Capex, la configuration, l'électricité, l'encre et l'entretien représentent l'Opex.
CMDB	Configuration management database. Une base de données cadrant dans le framework ITIL qui conserve la configuration des systèmes informatiques dans un endroit central. Elle se compose de CI ou Configuration Items (serveurs, adresses IP, logiciels, applications, bases de données, etc.) liés les uns aux autres. Une CMDB est un élément essentiel dans la gestion contrôlée d'un data center.
CMS	Content Management System. CMS désigne une famille de logiciels servant à créer et à mettre à jour des sites web dynamiques (ex: Joomla!, Drupal).
CRM	Customer relationship management. Logiciels permettant de gérer la relation avec les clients.
DSI	Directeur des systèmes d'information.
Hyperviseur	Élement de base de la virtualisation. L'hyperviseur est un logiciel autonome (qui ne nécessite pas la présence d'un système d'exploitation) qui va permettre l'installation et l'exécution de plusieurs systèmes d'exploitation simultanés.
Java EE	Spécifications techniques de Java Sun destinées aux applications d'entreprise.
JVM	Java Virtual Machine. La JVM est une machine virtuelle permettant l'exécution d'applications JAVA.
LAMP	LAMP est un acronyme désignant plusieurs logiciels Open Source: Linux – Apache – MySQL – PHP/Perl/Python. LAMP est souvent utilisé comme plateforme pour l'exécution d'applications Web Open Source (principalement en PHP).
Multitenancy	Architecture logicielle dans laquelle une seule instance d'un logiciel tourne côté serveur afin de répondre aux requêtes des différents clients, même si ceux-ci sont issus de différentes

	organisations/sociétés.
RIA	Rich Internet Application. Par RIA, on fait référence a des applications Web dont l'interface utilisateur est riche et peut être comparée à celle d'une application locale traditionnelle. Les applications de type RIA sont généralement interactives et la réactivité de celles-ci est bien souvent optimisée.
ROI	Return on Investment. Il s'agit simplement du retour sur investissement.
SLA	Service Level Agreement. Document décrivant la qualité de service fournie par un prestataire de service à un client.
SOA	Service Oriented Architecture. Modèle d'architecture de mediation où les services sont employés pour l'interaction applicative.
SQL Injection	Type de faille de sécurité : le pirate va introduire une requête SQL au sein d'un autre en utilisant des caractères spéciaux non prévus. L'objectif est de pouvoir exécuter des requêtes non autorisées ou non prévues (récupération de données, mots de passe ou suppression de données).
SSL	Secure Socket Layer. Protocole servant à sécuriser les échanges de données sur le Web. Des algorithmes de chiffrement et des certificats sont employés pour y parvenir.
SSO	Single Sign On. Méthode permettant à l'utilisateur de ne s'authentifier qu'une seule fois pour accéder à différents services.
XSS	Cross-site scripting : type de faille de sécurité propre aux applications web. Le pirate va tenter d'injecter des données dans un site (par exemple, dans un message posté dans un forum) pour que celles-ci soient exécutées par les autres personnes qui consulteront le site ultérieurement.