MASTER EN SCIENCES INFORMATIQUES

Cloud Broker
Essai d'une typologie

Kips, David

Award date:
2013

Awarding institution:
Universite de Namur

Facultés Universitaires Notre-Dame de la Paix, Namur
Faculté d'Informatique
Année académique 2012-2013

Cloud Broker: Essai d'une typologie

David KIPS

Promoteur : _____ (Signature pour approbation du dépôt - REE art. 40)

Philippe THIRAN

Mémoire présenté en vue de l'obtention du grade de
Master en Sciences Informatiques.

« *Quel que soit le secteur d'activités et quel que soit le pays, les sociétés se tournent uniformément vers le cloud*» (Carrel-Billiard, 2011)

Remerciements

Ce travail est la concrétisation de mes études commencées en vue de l'obtention du diplôme de Master en informatique. Avant toute chose, je souhaite adresser mes remerciements aux différentes personnes m'ayant apporté leur aide lors de la réalisation de ce mémoire.

Tout d'abord, je voudrais remercier Monsieur Philippe Thiran, professeur aux Facultés Universitaires Notre-Dame de la Paix de Namur, pour avoir accepté d'être le promoteur de ce mémoire. Je le remercie tout particulièrement pour les conseils qu'il a su me prodiguer et pour le temps qu'il a consacré à la relecture de cet écrit.

Je tiens aussi à remercier tout spécialement ma compagne Marie Labaisse pour sa précieuse aide lors de la réalisation de ce mémoire, pour sa patience et ses mots d'encouragement qui m'ont particulièrement aidé dans les périodes de doute.

Je voudrais aussi remercier Benjamine Lurquin pour son travail accompli au sein de l'université ainsi que l'aide et les petites attentions qu'elle sait constamment apporter auprès des étudiants.

Je voudrais remercier aussi mon ami Vincent Cordonnier pour son soutient.

Enfin j'adresse mes plus sincères remerciements à ma famille, ma belle-famille, mes collègues ainsi que mes amis, qui ont su m'aider en m'apportant le soutien ainsi que le courage nécessaire pour la réalisation de ce mémoire. Ils m'ont été d'une aide incontestable pour la relecture et l'amélioration de celui-ci.

Table des matières

Table des illustrations

Introduction

Imaginons une entreprise modeste de vente en ligne hébergeant son application sur son propre serveur interne et lançant une promotion spéciale sur son site personnel. La promotion fait directement son effet et quelques clients supplémentaires se connectent sur ce site. Au fur et à mesure, la sollicitation est de plus en plus importante jusqu'au moment où les clients saturent le serveur, qui ne peut dès lors plus répondre à la demande.

Prenons cette même entreprise où le serveur est hébergé au sein même de celle-ci et dont les données en backup sont logées sur ce serveur. Imaginons maintenant qu'un incendie se déclare, emportant avec lui les serveurs hébergeant les données ainsi que toutes les données de backup.

Voilà deux exemples que nous pourrions rencontrer dans la vie courante. Chaque entreprise préférerait que cela ne lui arrive pas et pourtant, tous les paramètres ne sont pas maitrisables. Quoique … Prenons maintenant l'exemple très concret de la société « Amazone ». Durant les fêtes de fin d'années, les serveurs de cette entreprise dédiés au commerce en ligne étaient surchargés. Elle a donc décidé de faire preuve de créativité afin de solutionner ce problème : elle a investi dans un parc informatique permettant de pallier aux surcharges de ces serveurs durant les fêtes. Une fois cette période passée, les ressources informatiques d'Amazone restaient peu utilisées. Elle a alors eu l'idée de louer ces capacités à d'autres entreprises afin qu'elles y stockent leurs données et qu'elles utilisent ces serveurs. Tout ce petit « commerce » était accessible via internet, facturé à la consommation et avait une capacité d'adaptation en temps réel de la capacité de traitement : le cloud computing est né.

Cette technologie ne date pas d'hier mais ne connait ses jours glorieux que maintenant. En effet, c'est un sujet prisé par bon nombre de professionnels mais aussi par « Monsieur et Madame tout le monde ». A l'heure où l'accès à internet s'est démocratisé et où les tablettes et Smartphone en tout genre sont « monnaie courante », le cloud computing intéresse. Et lorsque les gens parlent, ils racontent des éléments vrais qui font sens et d'autres qui collent beaucoup moins à la réalité. Le premier chapitre de ce mémoire traitera de ce sujet révolutionnaire qu'est le cloud computing, ayant alors pour but de l'éclaircir: définitions, sortes de services, types d'hébergement et caractéristiques nous permettront de mieux appréhender ce que revête le cloud computing. Une fois le contexte planté, nous pourrons aborder le « gros morceau » de ce chapitre, à savoir les divers bénéfices dont peuvent tirer parti les clients mais également présenter le revers de la médaille : les différents risques encourus par ces mêmes clients faisant appel au cloud. Le cloud est en effet une nuance de gris incroyable…

Face à cette nuance de gris naissent des incertitudes. Malgré une vue d'ensemble du cloud computing, certaines zones d'ombre persistent et un nouvel élément nous permettra d'éclairer un peu la situation : le cloud broker, acteur particulier au milieu « du nuage ». Après avoir défini ce qu'est un cloud broker, nous parcourrons son architecture. Nous commencerons avec une vue très générale du broker : le business broker et le technical broker. Ensuite, nous pourrons effectuer un zoom sur les différents services qu'il peut proposer aux consumer et sur les composants dont il a besoin pour respecter ses

engagements. Finalement, nous pourrons faire un petit « arrêt sur image » sur les avantages et les inconvénients liés au broker, procurant ainsi une vision collant au plus près de la réalité.

Le troisième chapitre aura pour but de souffler le voile sur ce nuage constitué de clouds consumers, clouds providers et de clouds brokers. Les brokers, à force de vouloir fournir des services épaulant les utilisateurs, se complexifient également. Et pour éviter que les clients soient à nouveau aveuglés par l'ampleur de la complexité, je tenterai un essai de typologie des brokers. Pour cela, j'élaborerai un listing des attentes éventuelles des clients, ce qui permettra de constituer le socle de ma typologie. Enfin la typologie à proprement parlé viendra clôturer ce chapitre.

Chapitre 1 : Cloud computing

1. Introduction

A l'époque actuelle, un utilisateur peut se connecter à son webmail en toute facilité et accéder au contenu de ce dernier depuis n'importe quelle station du moment que celle-ci possède une connexion internet. C'est le cas des messageries en ligne telles que Gmail, Hotmail, Yahoo, … Ce genre de manœuvre semble maintenant être à la portée d'énormément d'utilisateurs et paraît être d'une simplicité infantile. Mais derrière ce mécanisme se cache une technologie qui prend de plus en plus d'ampleur : le cloud computing.

C'est grâce à l'amélioration sans cesse croissante des réseaux informatiques ces dernières années que cette technologie est devenue possible et put se développer. En effet, dans la pratique, de plus en plus de clients utilisent des services informatiques en ligne, ce qui peut aller de la simple application de consultation de mails au stockage de données en passant par des outils de conception d'applications.

Dans ce premier chapitre, il sera avant tout question d'aller à la découverte du cloud computing, de s'approprier ce concept quelque peu révolutionnaire mais qui ne date pas d'aujourd'hui. Il esquisse les lignes directrices du cloud computing mais n'en procure pas une explication exhaustive.

Pour s'approprier un concept, il faut commencer par le comprendre. C'est pour cette raison que cette partie du mémoire sera amorcée par quelques définitions de ce qu'est le cloud computing. S'ensuivra alors une explication quant aux services offerts par le cloud et aux types d'hébergement existants, qui permettra de mieux appréhender son fonctionnement. Ensuite, nous passerons rapidement en revue 5 caractéristiques du cloud. A l'heure où le cloud devient de plus en plus populaire, il est important de soulever la zone d'ombre autour de ce qui le constitue, ce qui fait sa particularité. Une fois ces éléments traités, nous pourrons entrer dans le vif du sujet, à savoir les bénéfices et les risques liés au cloud : quels avantages peuvent être tirés du cloud computing ? Qu'est-ce qui fait sa popularité ? Pourquoi s'attarder sur cette technologie ? Mais quel est le revers de la médaille ? Quels sont les réels risques encourus par les utilisateurs amateurs de cloud et de quelle manière peuvent-ils contourner ces risques ? Désirant m'approcher au plus près de la réalité du cloud computing, la note de fin de ce chapitre sera donc axée sur les multiples atouts que le cloud peut offrir mais également sur les « fausses notes » qui le constituent. En effet, comme toute technologie, celle-ci n'est pas parfaite, sans accros et le chemin vers le cloud peut s'avérer parsemé d'obstacles pour le client.

2. Définitions

Le cloud computing est devenu attrayant ces dernières années pour toutes sortes de raisons qui seront présentées tout au long de cette partie qui lui est dédiée. Dans ce contexte, d'innombrables définitions jaillissent, chacun y mettant sa petite touche personnelle et y jetant un regard particulier. Voici donc quelques définitions émanant de spécialistes.

La première définition du cloud computing est appuyée sur les dires du CACM (Communications of the Association for Computing Machinery) nous livrant un premier aperçu de cette technologie :

> "Cloud computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services. (…)
> The data center hardware and software is what we will call a cloud. (…) This, cloud computing is the sum of SaaS and utility computing, but does not include small or medium-sized data centers, even if these rely on virtualization for management." (Armbrust, 2010)

Les trois prochaines définitions, provenant du NIST (National Institute of Standards and Technology), des entreprises Gartner et Forrester Research, viennent appuyer et apporter quelques spécificités à la précédente:

NIST: "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." (Peter Mell, 2011)

Gartner: "Gartner defines **cloud computing** as a style of computing in which scalable and elastic IT-enabled capabilities are delivered as a service using Internet technologies." (Gartner, 2013)

Forrester Research: "A standardized IT capability (services, software, or infrastructure) delivered in a pay-per-use, self-service way." (Forrester, 2013)

Afin d'ajouter « ma pierre à l'édifice » et soucieux de m'approprier ce concept au mieux, je tenterai ici la rédaction d'une ébauche de définition. Cette définition ne reste donc qu'une construction strictement personnelle sans caractère officiel et est loin de refléter toute la richesse dont recèle le cloud computing :

> Le cloud computing (ou informatique en nuage) consiste, par le biais d'un réseau, à mettre des traitements informatiques évolutifs et élastiques à la disposition de clients (un particulier, une entreprise, une administration,…). Le terme « cloud » renvoie au fait que l'utilisateur ne connait pas l'emplacement physique de ce service sur le réseau, les applications ne se trouvant plus nécessairement sur un serveur résidant chez le fournisseur (entreprise informatique) mais hébergées au niveau de data centers reliés entre eux. Ces traitements informatiques peuvent se décliner de différentes manières, offrant ainsi de nombreuses possibilités. En effet, cet éventail de propositions peut s'étendre de l'utilisation d'une application à la gestion des données et de la maintenance de celle-ci, en passant par le développement de logiciels. Le client obtient alors un service à la demande, standardisé, qu'il peut régler selon un modèle « pay-per-use ».

Un constat peut dès lors être posé : aucune définition officielle commune concernant le cloud computing n'était arrêtée jusqu'à récemment. Cette absence de définition claire n'a fait qu'alimenter le flou flottant autour de cette technologie. En 2013, le groupe de travail du CIGREF (Club Informatique des Grandes Entreprises Françaises) s'est alors intéressé à l'élaboration d'une base commune à chaque protagoniste et a décidé de revisiter ce concept en se basant sur la mise en œuvre du cloud computing au sein des entreprises. Voici ce qui fut retenu :

> « Le groupe de travail a identifié quatre points qui permettent de définir le Cloud :
> 1. Un *Cloud* est toujours un espace virtuel,
> 2. Contenant des informations qui sont fragmentées,
> 3. Dont les fragments sont toujours dupliqués ou répartis (ou distribués) dans cet espace virtuel, lequel peut être sur un ou plusieurs supports physiques,
> 4. Qui possède une « console (ou programme) de restitution » permettant de reconstituer l'information. » (CIGREF, 2013)

Les professionnels ayant participé à cette élaboration tiennent à préciser que si l'un de ces éléments n'est pas présent, nous ne sommes pas en présence d'un Cloud.

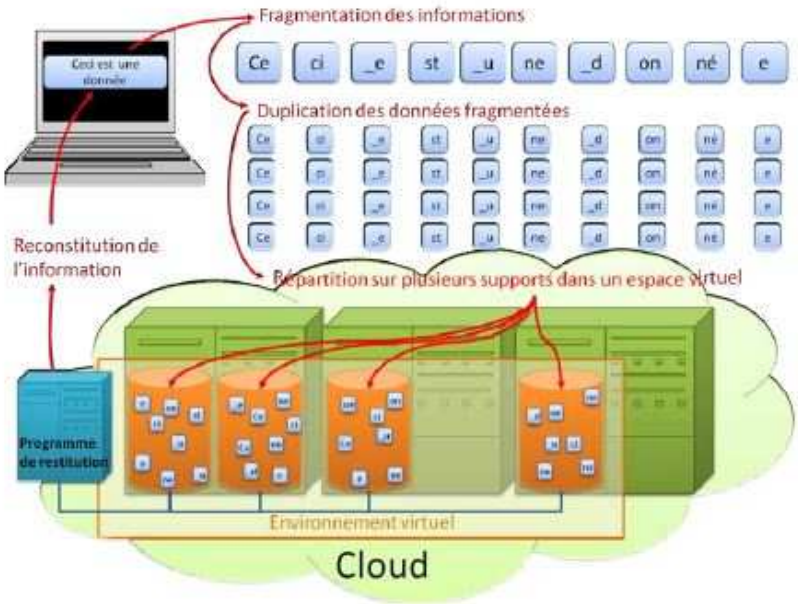

Figure 1: Les 4 points permettant d'identifier un Cloud (CIGREF, 2013)

3. Modèles de services

Un cloud computing est avant tout un vaste espace virtuel mis à la disposition des clients. Dans cet espace, il est possible de placer d'innombrables sortes d'outils que ce soit des infrastructures serveur, des plate-formes de développement ou encore de simples applications. Tous ces services peuvent être classifiés en trois couches différentes qui constituent le modèle appelé « as a service » : la couche application utilisateur (couche PaaS), framework de développement (couche PaaS) et infrastructure (couche IaaS). (Cigref, 2013)

Tout le monde n'effectue pas cette segmentation de couche. En effet, le CACM, pour sa part, prend le parti de présenter ces trois différentes couches du modèle sous une seule et unique forme de prestation de service dénommée SaaS.

> "The services themselves have long been referred to as Software as a Service (SaaS). Some vendors use terms such as IaaS (Infrastructure as a Service) and PaaS (Platform as a Service) to describe their products, but we eschew these because accepted definitions for them still vary widely. The line between "low-level" infrastructure and a higher-level "platform" is not crisp. We believe the two are more alike than different, and we consider them together." (Armbrust, 2010)

Par souci de clarté, le parti pris ici a été de faire tout de même cette division. Néanmoins, il ne faut pas la considérer comme une coupure nette entre les 3 couches car elles peuvent s'imbriquer étroitement et communiquer entre elles.

Ici, une cartographie rapide sera établie. Certaines spécificités à chaque couche seront expliquées tout au long de ce premier chapitre. Généralement ces différentes couches se présentent de la façon suivante :

3.1. Couche SaaS

Dans une couche SaaS (Software as a Service), le fournisseur propose comme service une application qui est disponible sur le cloud. Le client peut alors consommer ce service à la demande, sans être dans l'obligation d'en acheter la licence afin de l'installer sur ses machines de travail. Il pourra en bénéficier à distance, sans devoir connaitre son emplacement précis. (Schulle, 2008)

> « Le matériel, l'hébergement, le framework d'application et le logiciel sont dématérialisés et hébergés dans un des data centers du fournisseur. » (Direccte, 2012, p. 6)

Ces outils étant dématérialisés et mis à disposition du client, celui-ci n'a plus qu'à aller se servir quand il le souhaite. En bref, le client ne doit se préoccuper ici que de l'utilisation de son application. La conception et la maintenance de celle-ci sont du ressort du fournisseur de service. Cette facilité d'accès explique le fait que le SaaS est la forme de cloud la plus prisée. (Direccte, 2012, p. 6)

> « L'application est déjà construite et opérationnelle, il n'y a **pas véritablement de développement mais plutôt du paramétrage** ; d'où le succès de ce modèle de service : il concerne et met à la portée de n'importe qui tout un ensemble de services modelables et personnalisables très simplement » (Cigref, 2013)

Le Docteur Mark I Williams, dans son ouvrage intitulé « A quick start guide to cloud computing », nous livre une liste des services possibles au niveau de la couche Saas.

> « SaaS capabilities provided online include tools for:
> - Accessing virtual Microsoft Windows desktops on a per-user-per-month rental basis;
> - Accounting, financial management, inventory and e-commerce;
> - Collaborations between employees and clients on projects;
> - Creating flowcharts, diagrams, floor plans and other technical drawings;
> - Customer Relationships Management (CRM);
> - Editing, storing and sharing documents, presentations, spreadsheets, blogs, web pages and videos;
> - Project management;
> - Web-mail, calendaring, instant messaging, video conferencing and social networking." (Williams, 2010, p. 11)

En guise d'exemple le système de messagerie « Gmail » peut être cité, qui est le genre d'application assez basique que le client peut trouver dans le cloud. Mais d'autres applications plus complexes peuvent également être offertes telles qu'un ERP (Entreprise Resource Planning). (Czernicki, 2011)

3.2. Couche PaaS

La couche PaaS (Platform as a Service) offre aux clients un environnement de type middleware. C'est une plate-forme de développement permettant la création et l'exploitation de logiciels. Cet environnement contient les bases de données, les logiciels serveur,... mais aussi l'infrastructure: serveur, stockage,... (Schulle, 2008)

> « Le matériel (serveurs), l'hébergement et le framework d'application (kit de composants logiciels structurels) sont dématérialisées. L'utilisateur loue une plateforme sur laquelle il peut développer, tester et exécuter ses applications. » (Direccte, 2012, p. 5)

Le client n'est plus seulement l'utilisateur d'une application mais également le créateur de celle-ci grâce aux outils et aux librairies offertes par le fournisseur de cloud. Il gère alors lui-même le déploiement de l'application, la maintenance et la configuration de celle-ci sans devoir acheter de nouveaux logiciels ou réaliser des installations ultérieures supplémentaires. Le fournisseur de cloud, lui, s'occupe de la gestion du réseau, du serveur et du stockage.

> « (…) le *Cloud* de niveau *PaaS* **concerne les développeurs et les producteurs d'applications**, soit deux niveaux de service ; les plateformes de développement, et les applications qui fournissent le service du niveau supérieur (*SaaS*). (…) Il permet aussi de donner aux applications un **cadre d'exécution** qui produira des services *SaaS* (par exemple Salesforce). » (Cigref, 2013)

Comme ce fut fait pour la couche SaaS, voici quelques éléments de précision quant aux fonctions que peut fournir la couche PaaS, selon le Dr Mark I Williams:

> "PaaS systems typically include some or all of the following features:
> - browser-based development environment for creating databases and editing application code
> - either directly or through visual, point-and-click tools:
> - built-in scalability, security, access control and web service interfaces;
> - easy integration with other applications on the same platform;
> - tools for connecting to applications outside the platform's cloud;
> - tools for designing web forms, defining business rules and creating workflows"
> (Williams, 2010, pp. 12-14)

> « Windows Azur » ou « Google App Engine » en sont deux exemples qu'il est possible de rencontrer dans la vie courante. (Czernicki, 2011)

3.3. Couche IaaS

La couche IaaS (Infrastructure as a Service) permet d'offrir un service encore plus spécifique. Ici, le fournisseur met à la disposition du client des services concernant l'infrastructure matérielle. Cela peut aller du stockage des données, aux serveurs en passant par le réseau. Le client utilise une infrastructure informatique se trouvant physiquement chez le fournisseur. Il peut donc aisément bénéficier d'une augmentation de la puissance de calcul ou de stockage initial. Les ressources sont ainsi allouées et libérées à la demande. (Schulle, 2008) Ici, seul le serveur est dématérialisé. (Direccte, 2012, p. 5)

> « Ces derniers fournissent à la demande un ensemble de services de niveau « bas », c'est-à-dire des serveurs, réseaux etc. Cela permet ainsi à une entreprise cliente de pouvoir **bénéficier de la puissance d'une infrastructure, ponctuellement, sans devoir investir beaucoup**. » (Cigref, 2013)

Concrètement, et toujours selon le Dr Mark I Williams, la couche IaaS offre la possibilité d'utiliser ces différents services :

> "- A choice of ready-made virtual machines with pre-installed operating systems including numerous versions of Windows, Linux and Solaris;
> - A choice of virtual appliances – virtual machines with specific sets of software pre-installed;
> - Ability to store copies of particular data in different locations around the world to make downloads of the data as fast as possible;
> - Software tools to help process large amounts of data (in Data Grids) and perform complex calculations (in Compute Girds) using large arrays of virtual servers working in parallel on the same problem;
> - ability to manually increase or decrease the computing resources assigned to you using a web browser as your requirements change;
> - ability to automatically scale computing resources up and down in response to increases and decreases in application usage." (Williams, 2010, p. 15)

A la différence d'un data center où le client dispose d'un service permettant le stockage de données, l'IaaS propose comme service la gestion de cet emplacement de stockage.

3.4. Synthèse

Afin d'avoir une vue d'ensemble de ces trois couches de service cloud, voici deux illustrations : la première représente les trois couches selon leurs spécificités et la deuxième reprend les différents types d'utilisateurs par rapport aux différentes couches dans le cloud.

La figure suivante présente le cloud computing sous ses trois différentes facettes : SaaS, PaaS et IaaS. La couche SaaS est la plus répandue, constituant un cloud de service pouvant être directement exploité par les utilisateurs. La seconde couche, dénommée PaaS, offre deux grands types de services : cloud d'exécution et cloud de développement. La dernière couche, l'IaaS, est un cloud d'infrastructure physique, mettant à disposition de clients des serveurs, réseaux, …

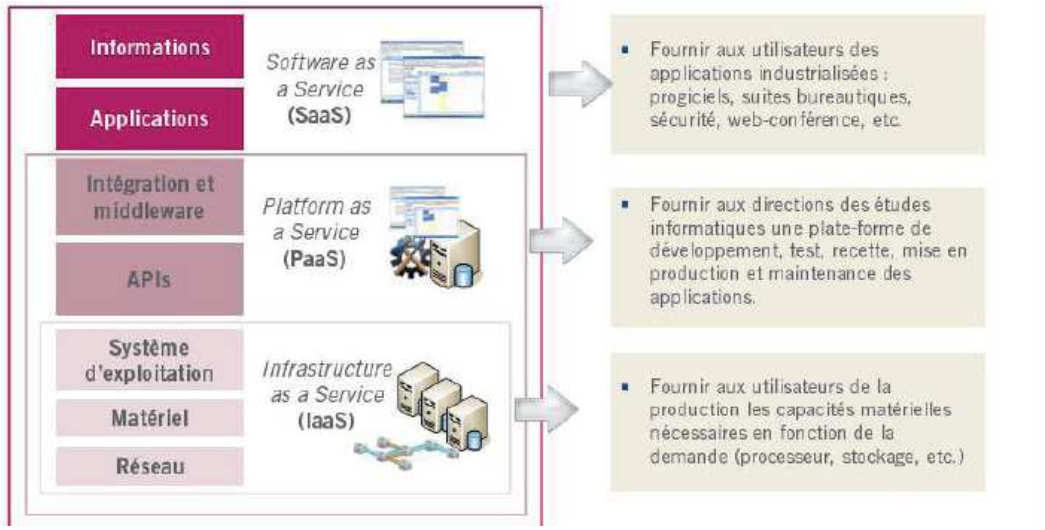

Figure 2: les 3 dimensions du cloud computing (Solucom, Cloud computing: comment en tirer parti?, 2010)

Au niveau du second schéma, une certaine imbrication des couches peut être d'emblée mise en évidence, comme ce fut expliqué en préalable. En effet, la couche SaaS englobe les utilisateurs des deux autres couches et la seconde couche inclus les utilisateurs IaaS. Ces derniers, constitués d'architectes réseau qui vont notamment pouvoir paramétrer le service de stockage, sont représentés en minorité. Ensuite vient la couche PaaS, offrant aux développeurs d'applications un environnement permettant de créer ces dernières. Finalement, la couche SaaS est la plus représentée, constituée d'utilisateurs de logiciels. Nous pouvons dès lors constater que plus l'offre est spécifique, moins les utilisateurs sont nombreux.

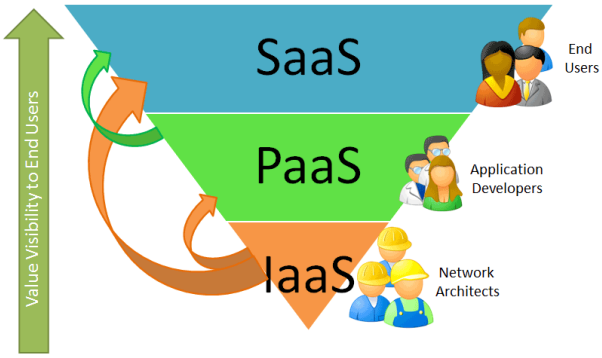

Figure 3: Type d'utilisateurs par rapport aux différentes couches (Schulle, 2008)

4. Types d'hébergement

Afin d'appréhender un peu plus ce qu'est le cloud computing, il est intéressant de s'attarder sur les différentes façons qu'ont la gestion et l'usage du cloud de s'articuler. Deux pôles sont dès lors à prendre en compte : celui du fournisseur et celui du client.

En respectant la classification érigée par Cigref dans son ouvrage « Fondamentaux du Cloud Computing : Le point de vue des grandes entreprises », 4 grands types de clouds peuvent être dégagés : (Cigref, 2013, p. 11)

- Le cloud privé interne
- Le cloud privé externe
- Le cloud ouvert interne
- Le cloud ouvert externe

De plus, le cloud hybride peut être rajouté à la liste et le cloud communautaire peut également être cité, qui est une sorte de cloud privé externe.

4.1. Cloud privé (interne ou externe)

Un cloud dit « privé» est une solution personnalisée dédiée aux besoins propres d'un seul client qui dispose de l'ensemble des ressources informatiques. Deux cas de figures sont alors possibles : soit le cloud est déployé et géré au sein de l'entreprise même (**cloud privé interne**), soit il est géré par un prestataire externe (**cloud privé externe**). (Cigref, 2013)

> « Ce sont des solutions complètement gérées par la DSI. La DSI peut faire éventuellement appel à un prestataire (type infogérant) mais elle garde la maitrise complète de la solution. » (Cigref, 2013, p. 12)

Cependant, garder « la maitrise complète de la solution » ne signifie pas que l'infrastructure appartiendra exclusivement à ce client. Une même infrastructure pourrait accueillir plusieurs clouds privés différents, dédiés à des clients différents. Le cloud computing fonctionnant sur base d'un réseau, chaque utilisateur pourra accéder à son cloud privé en passant par son réseau personnel. (Direccte, 2012, p. 6)

Ce style de cloud est souvent préféré par les entreprises qui désirent avoir plus de garanties au niveau de la sécurité. Ce système leur permet tout de même de bénéficier de certains avantages du cloud sans pour autant bénéficier de la totalité de ceux-ci.

> « Many large organizations prefer, or are legally obligated, to keep their servers, software and data within their own data centers ; and private clouds enable them to achieve some of the efficiencies of cloud computing while taking responsibility for the security of their own data. (…) Unlike the pay-as-you-go model of public clouds, however, private clouds require significant up-front development costs, data centre costs, ongoing maintenance, hardware, software and internal expertise." (Williams, 2010, pp. 16-17)

Comme exemple de cloud privé, nous pouvons prendre la mise en place d'un ERP ou d'un CRM qui sont deux services qui peuvent être propres à une entreprise et qui fonctionnent selon leurs propres règles. (Accenture, 2011)

Un cas particulier de cloud privé externe peut être cité : **le cloud communautaire**. C'est un cloud qui est exclusivement dédié à des entreprises ou organisations qui veulent partager leurs ressources, ce qui leur permettent de bénéficier d'un cloud tout en ayant un peu plus de maitrise et de garantie quant à leur sécurité (par rapport aux autres membres qui partagent cette plateforme). (Williams, 2010, p. 16)

4.2. Cloud public/ouvert (interne ou externe)

On parle de cloud ouvert ou public quand le service offert par le fournisseur est ouvert au public via Internet. Comme l'explique le site « CloudWatt », « le **Cloud public est** une **structure souple** et **ouverte**, **gérée** par un **fournisseur tiers** » (CloudWatt, 2013). Plusieurs clients peuvent y accéder et partager les mêmes ressources informatiques. Les différentes ressources informatiques et bases de données du client peuvent être hébergées dans n'importe quel data center du fournisseur. Ces données peuvent même passer d'un data center à un autre pour permettre l'optimisation des capacités. (CloudWatt, 2013) C'est d'ailleurs grâce à ces possibilités de mobilité d'un serveur à un autre qu'un cloud public peut supporter de fortes montées en charge en absorbant les pics de charges.

Deux sortes de clouds ouverts peuvent être alors mises en évidence en fonction de l'acteur qui gère ce cloud. Soit le cloud est géré par une entreprise particulière tout en ayant un usage ouvert au grand public (**cloud ouvert interne**), soit le cloud destiné au grand public est géré par une organisation tierce (**cloud ouvert externe**).

La particularité du cloud ouvert géré en interne est que l'entreprise devient elle-même fournisseur de cloud, offrant les services de cloud à ses clients. Le cloud ouvert à usage externe est, pour sa part, le plus controversé du fait, notamment, du manque de visibilité des données par les clients. Les données sont même souvent hébergées dans un data center étranger. (Cigref, 2013, p. 9)

Comme exemple de structure externe Google, DropBox ou encore Amazone peuvent notamment être cités. (Cigref, 2013)

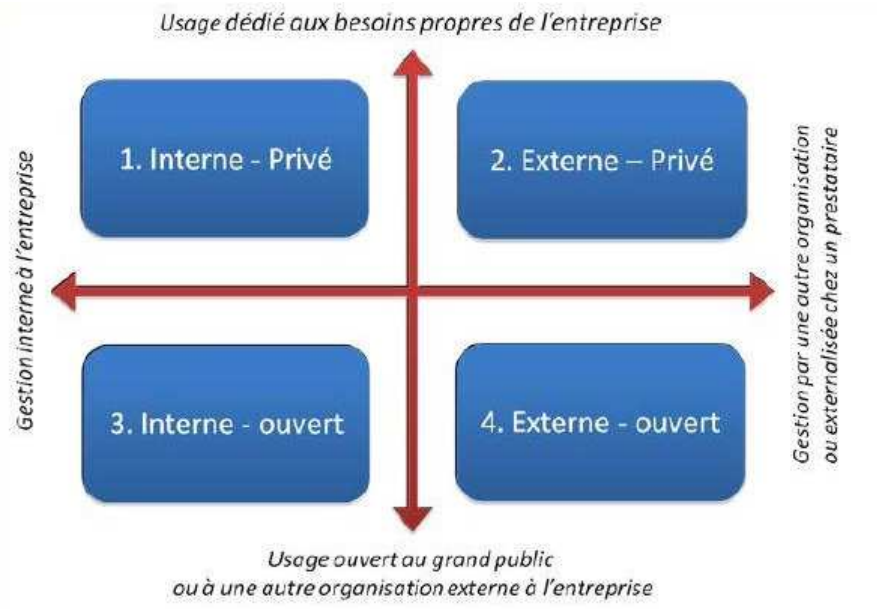

Figure 4: Les typologies du cloud computing (CIGREF, 2013)

4.3. Cloud hybride

Le cloud hybride, quant à lui, est une solution basée sur un mélange des clouds précédemment exposés. Il s'agit surtout de les allier et d'utiliser les avantages de chacun, notamment le fait qu'un cloud public pourra mieux supporter une montée en charge et qu'un cloud privé pourra être géré personnellement par le client. (Cigref, 2013)

De nombreuses possibilités s'offrent alors au client qui décide d'opter pour cette solution, désirant manipuler certains avantages du cloud tout en évitant certains inconvénients. En effet, un cloud hybride laisse la possibilité au client de différencier le lieu de traitement de ses données en fonction de leur importance. Pour des informations à caractère plus confidentiel ou stratégique pour l'entreprise, il peut opter pour un cloud privé. Par contre, pour certaines données considérées comme moins critiques, elles peuvent être externalisées vers un cloud public qui est plus performant. Le client peut également balancer d'un cloud privé à un cloud public lorsque les capacités de son entreprise sont dépassées, lui permettant ainsi de bénéficier du fait qu'un cloud public supporte beaucoup mieux les montées en charge. (Direccte, 2012, p. 7)

> « This option is attractive to businesses that have invested in their own IT infrastructure or have data protection responsibilities, but would like to take advantage of the scalability and flexibility that cloud computing affords. » (Williams, 2010, p. 17)

Information	Privé	Hybride	Communautaire	Public
Client	• Une seule entreprise	• Une seule entreprise	• Quelques entreprises	• Multiplicité d'entreprises
Emplacement géographique des données	• Site du client	• Principalement sur le site du client. • Chez le prestataire en cas de basculement	• Chez le prestataire • Emplacement connu	• Chez le prestataire • Emplacement non connu
Type de facturation	• Palier	• Palier + à l'utilisation lors d'un dépassement	• Partie forfaitaire + à l'utilisation	• À l'utilisation
Catalogue / Niveau de service	• Spécifique	• Spécifique	• Assez standard	• Complètement standa
Moyens d'accès	• Intranet	• Intranet et internet	• Internet	• Internet
Innovation	• Portée par le client	• Portée par le client	• Portée par les clients	• Portée par le prestatai
Flexibilité	• Inexistante	• Limitée	• Partagée	• Totale
TCO	• Investissement important	• Investissement plus limité	• Investissement partagé	• Aucun investissement

Figure 5: Comparaison des 4 modèles de fourniture cloud (Solucom, les nouveaux modes d'externalisation: une remise en question des modèles?, 2011)

5. Principales caractéristiques du cloud

Présenter toutes les caractéristiques d'un domaine aussi vaste et complexe que le cloud computing n'est pas chose aisée. C'est pourquoi seules 5 caractéristiques sont rapidement reprises ici, mises en avant par la société NIST : (Fang Liu, NIST Cloud Computing Reference Architecture, 2011)

5.1. Self-service

Lorsqu'un client souhaite utiliser un service ou une application, il peut le faire lorsqu'il le souhaite, sans demander à un quelconque responsable technique.

> « Les services doivent être conçus pour être prêts à l'usage, packagés comme des produits « finis », à peine configurables et standardisés pour s'adapter au plus grand nombre d'entreprises. » (Solucom, les nouveaux modes d'externalisation: une remise en question des modèles?, 2011, p. 1)

5.2. Large accès réseau

Le client peut avoir accès au cloud via n'importe quel endroit, à partir du moment où il a accès à un réseau. Nous pouvons donc imaginer l'accès à partir d'un ordinateur mais également d'une tablette, d'un Smartphone, … qui sont très en vogue

5.3. Mutualisation des ressources

Le cloud computing est un immense champ virtuel au sein duquel les ressources peuvent être partagées entre les différents clients et hébergées à de nombreux endroits. Lorsqu'une ressource n'est pas suffisante, un balancement peut s'effectuer pour pallier directement à ce manque de capacité.

5.4. Elasticité importante

En fonction de leurs besoins, les clients peuvent faire évoluer les ressources demandées à la hausse ou à la baisse et ce, de manière très rapide. On s'appuie ici sur le principe de la scalability, point qui sera développé plus amplement plus loin.

5.5. Paiement à l'usage

Dans le cas du cloud computing, les clients paient à l'usage, à la consommation. Cette caractéristique est probablement la plus prisée vu ce qu'elle peut faire gagner aux clients qui décident d'opter pour cette technologie. Le calcul de la facture change quelque peu selon le service offert, comme nous l'exposerons par la suite.

6. Cloud computing et virtualisation

De nombreux utilisateurs pensent que virtualisation et cloud computing sont deux choses identiques. Or, même s'il y a de fortes similitudes, ce sont deux principes indépendants mais qui, une fois mis ensemble, permettent une certaine optimisation des ressources informatiques.

6.1.1. Définition

La virtualisation est un procédé qui consiste à faire cohabiter plusieurs systèmes d'exploitation ou applications sur un ou plusieurs ordinateurs ou serveurs au lieu de ne pouvoir en installer qu'un seul par machine. (informatique R.) « La virtualisation c'est : le fait de rendre logique une ressource technique/physique dans le but d'optimiser l'utilisation des ressources et/ou de réduire l'adhérence entre ces éléments. Il s'agit donc d'un moyen, non d'une fin. » (Sonia Boittin, 2010, p. 5)

> « La "virtualisation" représente globalement le fait de dématérialiser le comportement et les données d'un serveur ou d'une machine. En d'autres termes, cela revient à pouvoir regrouper plusieurs serveurs et/ou machines (Messagerie Windows, Comptabilité SAGE, Web sous Linux, Backup, BlackBerry...) sur un seul et même serveur physique.» (informatique A. , 2011)
>
> Virtualization: "The ability to run multiple operating systems on a single physical system and share the underlying hardware resources" (VMware, 2011)

Cette plus grande flexibilité des serveurs peut être obtenue en les standardisant :

> "On peut comparer la situation à des bureaux. Dans un environnement non virtualisé, chaque collaborateur dispose de son propre bureau aménagé en fonction de ses besoins. Dans un environnement virtualisé, on dispose d'un pool de bureaux identiques et chaque collaborateur qui passe la journée en interne s'approprie n'importe lequel de ces bureaux. » (Perrenoud, 2013)

6.1.2. Principe

La virtualisation apporte quelques avantages aux utilisateurs qui décident d'opter pour cette technique permettant une optimisation intéressante des ressources. Voici quelques bénéfices relevés par l'entreprise Solucom dans « Virtualisation et Cloud computing : jusqu'où aller » : (Sonia Boittin, 2010, p. 8)

La réactivité :

Il n'y a que des composants logiques qui sont livrés et donc, il n'y a plus besoin de s'encombrer de stocks, de manœuvre de câblage, … la mise à disposition du service est dès lors beaucoup plus rapide. Un délai moindre fait bien entendu réfléchir mais avoir tout à disposition très rapidement pousse aussi à la consommation.

La disponibilité :

Les ressources étant virtualisées, certains incidents liés aux équipements physiques sont évités. Lorsqu'il y a un souci avec un serveur, il y a moyen de balancer le tout sur un autre serveur physique. Ici, l'utilisateur ne doit plus attendre de réparer le matériel physique mais peut agir directement. Cependant, n'oublions pas que plusieurs serveurs logiques peuvent se retrouver sur un serveur physique. Un incident sur ce serveur physique pourrait alors avoir des répercussions sur un ensemble important de serveurs logiques : les dégâts peuvent être dupliqués.

La souplesse :

La virtualisation des serveurs permet une grande modularité des répartitions des ressources lors d'une importante montée en charge du système. En effet, il arrive que des entreprises détiennent de nombreux serveurs mais n'exploitant qu'une petite capacité de ces derniers en temps normal. Sachant qu'un serveur fonctionnant à quasi plein rendement ne consomme pas beaucoup plus d'énergie qu'un serveur dont on exploite qu'une minime capacité, il peut donc être intéressant de rassembler plusieurs serveurs sur un seul lorsque les pics de montée en charge n'arrivent pas en même temps. Si ce cas de figure devait arriver, la virtualisation permettrait de déplacer les instances de serveurs sur d'autres machines. De plus, lors de l'augmentation de temps de réponse, dématérialiser les serveurs permet de passer du serveur utilisé à un serveur physique plus puissant. (Lévy-Abégnoli, 2008)

Les coûts :

La virtualisation pourrait permettre de regrouper plusieurs machines virtuelles en une seule machine physique, ce qui engendrerait une économie au niveau de l'achat du matériel et au niveau consommation de l'énergie. (VMware, 2011)

6.1.3. Virtualisation dans le cloud computing

Virtualisation et cloud sont deux principes qui offrent la possibilité d'exécuter une application en dehors d'une machine spécifique et donc qui améliorent la productivité des entreprises et qui, parallèlement, permettent aux utilisateurs de réduire leur budget en limitant l'investissement matériel. Néanmoins, ce sont deux choses différentes qu'il ne faut pas mélanger : le cloud peut tirer avantage de la virtualisation mais peut également exister sans son utilisation.

> « Virtualisation et cloud computing sont deux termes à la mode, souvent associés, qui renvoient à deux solutions distinctes : le premier dissocie les ressources logiques des ressources physiques afin d'optimiser l'utilisation de ces dernières ; le second vise à mettre à disposition des solutions allant de l'infrastructure à l'application et aux services utilisateurs, grâce à des ressources physiques réparties à travers le monde, accédées à la demande via internet, et dont l'entreprise n'est plus propriétaire » (Sonia Boittin, 2010, p. 4)

Comme annoncé au début de ce point et comme l'explique « Ebizq » dans son article, le cloud computing est une manière de mettre la virtualisation en application mais le cloud peut très bien être mis en place sans celle-ci. C'est juste que l'association des deux permet l'optimisation des ressources, l'utilisation à la demande et la flexibilité. (ebizQ, 2010)

> "In cloud computing, server virtualization is extended further, going beyond the more efficient use of a single physical machine or cluster to the aggregation and partitioning of computing resources across multiple data centres. This enables cloud providers to efficiently manage and offer on-demand storage, servers and software resources for many different customers simultaneously. More importantly the web interfaces they provide empower their customers to administer computing resources as if they owned them." (Williams, 2010, pp. 14-15)

Que ce soit l'utilisation du cloud ou de la virtualisation, voire des deux, les modifications architecturales sont de taille et ne sont pas à négliger. Les fournisseurs ont tendance à les présenter comme des éléments aisés à mettre en place mais ces dires relèvent plus du marketing que de la réalité. L'entreprise Solucom donne d'ailleurs un exemple de cette complexité à les mettre en place :

> « Sur l'axe plus technique, les changements doivent dans les deux cas être traités dans la globalité du SI. Par exemple, traiter le problème de la consolidation des infrastructures uniquement via la réduction du nombre de « boîtes » en virtualisant est une vision très et trop partielle. Plusieurs niveaux sont à étudier :
> • physique, avec les solutions de densification (formats *blades*, ...) ;
> • ressources, avec les solutions de virtualisation ;
> • *middleware*, avec la création de plusieurs instances sur un même socle serveur;
> • applicatif, avec l'urbanisation et la rationalisation fonctionnelle.
> À l'opposé, consolider toutes les couches conduit à un empilement potentiellement instable.(…) Elle ne peut s'atteindre que par une rigueur toute particulière dans chacune des phases projets : chaque couche doit être robuste, sans quoi les autres ne pourront s'appuyer sereinement dessus. » (Sonia Boittin, 2010, p. 10)

7. Bénéfices du cloud computing

7.1. Bénéfices financiers

Le côté financier est indéniablement le bénéfice qui attire le plus l'attention des utilisateurs. A l'heure où la crise est bien présente et où la concurrence ne faiblit pas, les entreprises cherchent par tous les moyens à maximiser leur production tout en minimisant leurs frais. Elles sont dès lors capables de faire preuve de beaucoup de créativité pour atteindre leur objectif et, surtout, sont également capables de prendre des risques, comme ce sera expliqué plus longuement par la suite.

Comme ce fut expliqué précédemment, opter pour le cloud computing, c'est opter pour une solution de paiement selon le modèle « pay-per-use » qui est un paiement à la consommation. En effet, externaliser les données peut être intéressant lorsque l'entreprise connait de grands pics et des creux de demande de puissance de calcul, bénéficiant alors d'un supplément de ressources pour les moments de pics. Ce type de paiement permet donc de débourser la somme selon les besoins réels de l'entreprise. (Jefferson, 2009)

Cependant, il ne faut pas oublier que le cloud computing peut offrir trois sortes de prestations aux clients. Il en découle alors le fait que ce calcul de paiement dépend du service choisi : SaaS, PaaS ou Iaas. Le coût pour la couche SaaS dépendra du nombre d'utilisateurs, pour la couche PaaS cela se calcule en fonction de l'utilisation et de la taille des applications développées et, finalement, le coût pour la couche IaaS dépend de l'utilisation des serveurs et du stockage fait par l'utilisateur. (Williams, 2010)

« Les entreprises achètent ainsi des capacités, et sont facturées un peu comme le sont l'eau, le gaz ou l'électricité: on paye à la consommation. Comme le courant électrique, on peut consommer autant qu'on veut. Virtuellement, la puissance est infinie.» (Karayan, 2011)

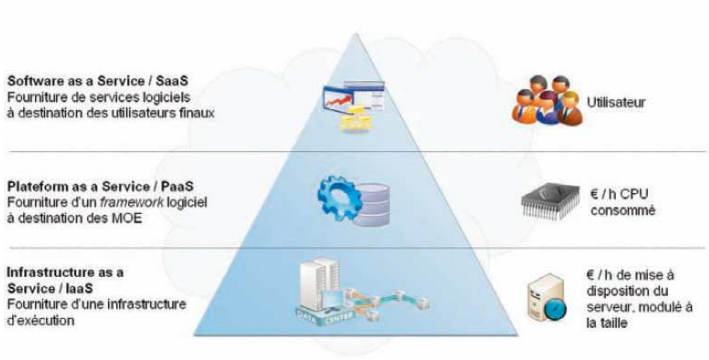

Figure 6: Principe de tarification du marché (Solucom, Virtualisation et cloud computing: jusqu'où aller?, 2010)

Comme nous pouvons rapidement le comprendre, ce style de facture permet de mieux maitriser les coûts, le prix dépendant de l'usage qui est fait du service. Mais il va de soi également que pour mieux maitriser ces coûts, il faut donc savoir maitriser l'usage fait de ces services.

> « - Côté SaaS (issu de l'ASP) : véritable atout car directement liés à des volumétries métiers (nombre de comptes utilisateurs par exemple). Mais il faut bien piloter la suppression et la migration de données de chaque utilisateur en cas de départ, sans quoi la facture peut augmenter proportionnellement à la croissance des effectifs et au *turnover* conjugués.
> - Côté PaaS/IaaS : la qualité du code développé impacte directement la facture puisque l'unité d'œuvre est souvent liée à la consommation de ressources (processeur/serveurs) : une livraison de code peu optimisé peut la doubler. » (Sonia Boittin, 2010, p. 12)

Cet aspect « alléchant » du cloud computing alimente l'intérêt de certaines entreprises. C'est le cas pour les petites entreprises, qui seront dès lors plus amatrices du service SaaS, et qui pourront accéder à des solutions auxquelles elles n'auraient pas pu prétendre sans cette technologie, faute de moyens financiers. A côté de cela, c'est également intéressant pour les entreprises de plus grande envergure, qui peuvent alors mettre sur place de nouveaux projets et les tester sans pour autant devoir « casser leur tirelire ». La couche Iaas, demandant plus d'investissement, peut également être très attractive pour les entreprises à dimension internationale. (Solucom, Cloud computing: comment en tirer parti?, 2010, p. 3) Le cloud computing peut donc être une solution intéressante pour lancer de nouveaux projets sans pour autant prendre trop de risques. En effet, ce peut être un contexte propice à l'innovation grâce à la flexibilité que le cloud apporte et à l'investissement moindre à court-terme.

> « Le Cloud computing est une solution de facilité pour une start-up, car il permet de tester son business plan rapidement et à coûts réduits. Chaque start-up, ou même division au sein d'une entreprise, devrait réfléchir à la manière d'utiliser le Cloud Computing » (Jefferson, 2009)

Et comme ces services sont facturés suivant l'utilisation ou suivant un abonnement, il est dès lors très facile d'arrêter un service chez un fournisseur et de migrer vers un autre. (PartageDeFichier, 2012)

Afin d'illustrer plus amplement les bénéfices financiers qu'apporte le cloud, vous trouverez en annexe [Annexe 1] un tableau comparatif des coûts entre le modèle SaaS et le modèle Software. (Direccte, 2012, p. 23)

Ce n'est pas pour autant que le cloud offre que des avantages financiers. En effet, il faut également prendre en compte les frais de transfert des données sur le réseau ainsi que les frais des services proposés par le fournisseur. D'ailleurs, la société « Sony Pictures Image Works », a renoncé à passer à un service de cloud externe suite à des problèmes de stockage, peut être prise en exemple. Chaque jour, les utilisateurs de Sony génèrent un trafic qui varie entre 4 et 12 To de données. Ça coûtait alors trop cher de mettre en place une solution cloud pour gérer cela.

> « *La bande passante qui serait nécessaire pour mettre cela dans le Cloud et le récupérer est gigantesque, et les coûts seraient tellement importants qu'il est plus avantageux d'acheter le stockage nous-mêmes plutôt que de payer quelqu'un d'autre pour s'en charger.* » (Derest, 2009)

7.2. Bénéfices technologiques

7.2.1. Scalability

Premièrement, la **scalability** dans le cloud est un point central. La scalability est la capacité d'un système à s'adapter en fonction de la demande. En effet, la capacité du matériel étant fixe mais la demande pouvant être croissante, il est important pour un système de pouvoir supporter la montée en charge du système afin d'éviter le phénomène de goulot d'étranglement provoqué par l'augmentation simultanée de demandes à traiter.

> "A system is scalable that can be "scaled" up or down, or enlarged or shrunk, and still maintain its basic composition and proportions. A scalable cloud can add further users, storage, or processing power simply by connecting extra hardware to the existing infrastructure. By definition this type of expansion does not require any extended integration or reworking of the existing system and will not disrupt the service of ongoing users." (Jason, 2012)

Deux méthodes permettent de gérer cette sollicitation du système:
- La scalability verticale
- La scalability horizontale

a) Scalability verticale

Pour reprendre l'exemple utilisé sur le blog de « Neoxia », une ligne de défense composée de 10 canons peut être imaginée. Pour multiplier la puissance de feu par 5, il est possible de remplacer les canons actuels par des canons 5 fois plus puissants. (Dasriaux, 2010)

La scalability verticale est le fait d'ajouter ou d'améliorer les composants d'un système afin de le faire évoluer. Dans le cas d'un serveur informatique, par exemple, nous allons améliorer l'efficacité de celui-ci grâce à l'ajout de RAM, disques, processeurs,... (Dasriaux, 2010)

La scalability verticale montre vite ses limites. En effet, il peut parfois être difficile d'investir dans du matériel de meilleure qualité en respectant les contraintes technologiques et financières. Pour preuve, même les processeurs n'évoluent plus en puissance comme autrefois (Microprocesseur) et la stratégie actuellement utilisée afin d'augmenter la puissance des machines, est de faire appel à une scalability horizontale en augmentant le nombre de cœurs des processeurs. (Rezzonico, 2009)

b) Scalability horizontale

Pour reprendre l'exemple de la ligne de défense, il faut imaginer cette fois non pas l'amélioration des canons existants mais l'augmentation de leur nombre avec des canons identiques. Le principe ici est d'augmenter le nombre d'ordinateurs pouvant exécuter le service fonctionnant à la base uniquement sur un ordinateur. (Dasriaux, 2010)

La scalability horizontale est un atout d'importance majeure pour le cloud computing. Il est dès lors possible d'imaginer la possibilité de pouvoir disposer d'une réserve de puissance quasiment illimitée, ce qui permettrait de largement satisfaire la demande.

Comme nous pouvons maintenant le comprendre, la scalability offre de nombreuses possibilités aux utilisateurs, comme l'explique concrètement le Dr mark I Williams :

> « You can quickly provide new employees with user accounts for your software as a service applications, and they can use any old personal computer to access it. You can develop new web-based business software applications using platform as a service without worrying about servers, firewalls, security or operating systems. And you can use infrastructure as a service to gain temporary access to seemingly unlimited computing power and data storage when you need it for as long as you need it." (Williams, 2010, p. 28)

7.2.2. Accès via un réseau

Un deuxième élément central dans le cloud computing est l'accès aux données via un **réseau** (intranet ou internet). Ceci change considérablement le contexte informatique, les utilisateurs pouvant maintenant se connecter de l'endroit de leur choix, à condition qu'il y ait une connexion disponible. Ce mode de fonctionnement peut faciliter la vie à bon nombre de travailleurs dits « nomades », ne restant pas sur une machine fixe. De plus, ce principe va de pair avec l'évolution de notre société qui est de plus en plus friande des tablettes, Smartphone, … et qui en usent et en abusent.

7.2.3. Automatisation de la maintenance

Ensuite, **l'automatisation de la maintenance** des applications peut être citée, permettant à bon nombre d'utilisateurs de moins se tracasser. Ils n'ont plus besoin d'acheter de nouvelles versions de leurs logiciels pour les installer sur chaque machine physique. De plus, ils ont également accès de cette manière aux nouveautés de manière instantanée. L'entreprise ne doit alors plus se soucier de l'évolutivité de ses logiciels. Une mise à jour créée et déployée par le fournisseur sera directement accessible depuis toutes les stations du client. Le client dispose du coup de plus de ressources disponibles en interne, ressources qu'il peut alors mettre à disposition pour l'innovation. (Dell, 2011)

> « Ainsi, on élimine les problèmes de compatibilité de fichiers, de versions obsolètes de logiciels. Cela permet d'être toujours en possession de la dernière version de l'application. » (Direccte, 2012, p. 22)

7.2.4. Sécurité

Enfin, même si la **sécurité** dans le cloud est très largement critiquée, elle peut également constituer un point fort. Les données ne sont plus stockées en local mais sauvegardées dans une infrastructure tierce. Elles peuvent être plus protégées que si elles avaient été stockées au sein de l'entreprise. Ici, il n'est donc plus question de backup de données, cette tâche étant exécutée par des spécialistes chez le fournisseur.

Ci-dessous, voici un graphique de Poujol reprenant en pourcentage les avantages centraux du cloud computing cités par les entreprises françaises interviewées.

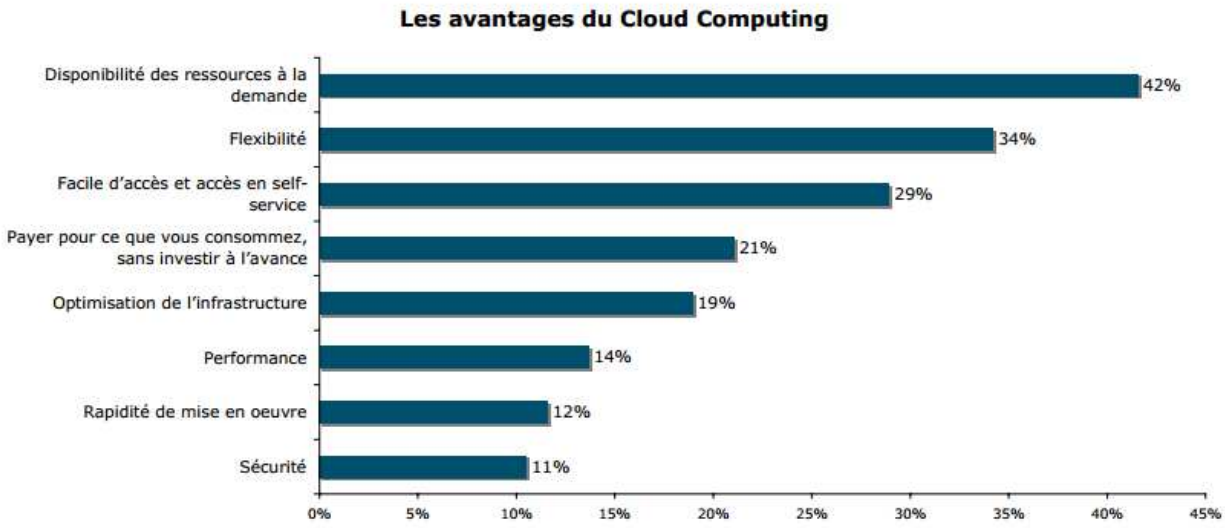

Figure 7: Les avantages du cloud computing. (Poujol, 2010, p. 10)

8. Risques liés au cloud computing

Le cloud computing élargit le champ des possibles à de nombreuses entreprises. Effectivement, nous ne pouvons nier que certains aspects revêtis par cette technologie sont attractifs. Néanmoins, le cloud computing est également controversé. Certains risques sont dès lors bien présents et les décrypter constitue déjà une avancée en soi. Pour lutter contre les risques, il faut commencer par les reconnaitre et les nommer.

8.1. Sécurité/confidentialité

Lorsque nous abordons le sujet du cloud computing, une des premières craintes revenant systématiquement est la question de la sécurité. En effet, les données des utilisateurs sont externalisées vers un « nuage », vers quelque chose de nébuleux dont on ne connait même pas l'emplacement physique. Ici, la relation de confiance entre client et fournisseur prend tout son sens et devient vitale. Or, nous sommes dans une société de plus en plus individualiste et où la concurrence prime. Dans ce contexte, il est aisé de comprendre la retenue dont peuvent faire preuve certaines entreprises face à cette technologie quelque peu déroutante qu'est le cloud computing, plongeant les entreprises dans un univers abstrait constitué de flous certains.

> « Les enjeux de sécurité de cloud sont le premier point d'achoppement de ces solutions : que ce soit en termes de sécurité des échanges utilisateurs et inter-applications, d'exposition potentielle des données de l'entreprise sur internet ou d'incidents. Ces derniers déclenchent souvent le buzz, rappelant que même dans le cloud il y a également des logiciels, des serveurs, du stockage, du réseau, des data centers et une production qui ne sont pas infaillibles. » (Sonia Boittin, 2010, p. 13)

Pour certaines entreprises, ces données peuvent valoir beaucoup, parfois même plus que la production de l'entreprise. Il n'est donc pas rare que d'autres les convoitent avidement. Les risques peuvent alors être multiples : une entreprise concurrente pourrait essayer de négocier ces informations à prix d'or, des hackers pourraient prendre ces données capitales pour cible afin de les revendre, ces informations pourraient être la source de chantage au sein même de l'entreprise, le fournisseur pourrait ne pas être digne de confiance et revendre ces informations ou s'en servir à mauvais escient, … Ainsi, les risques au niveau de la sécurité interne à l'entreprise sont bel et bien existants, mais même dans un cas où l'entreprise n'a pas opté pour le cloud computing : personnel mal intentionné qui ne travaille plus au sein de l'entreprise mais qui continue à avoir accès à des données en craquant des mots de passe, par exemple. Ces risques sont tout de même dupliqués lorsque nous sommes en présence d'un cloud computing, ayant plus facilement accès aux données par internet, ce qui constitue alors en soi une facilité et un risque. De plus, de nombreux risques de sécurité externe existent lorsqu'une entreprise adopte le cloud computing. Il est avant tout central de se remettre en mémoire que ce sont les entreprises qui sont responsables de la sécurité de leurs données et non pas les fournisseurs de cloud. (Williams, 2010, p. 43)

Par ailleurs, tous les protagonistes connaissent bien ces risques et les craintes qui en découlent, ce qui pourrait engendrer certains abus de la part des fournisseurs de cloud. En effet, à côté d'une application basique pourrait se trouver en option des outils de sécurité plus poussés. Larry Ellison va encore plus loin en expliquant que les fournisseurs vont jusqu'à aller « forcer les gens à acheter des systèmes de sécurisation, des applications propriétaires qui leur couteront, finalement, de plus en plus cher ». (Dailly, 2008)

Néanmoins, CIGREF met en évidence que ce n'est pas réellement le cloud qui pose problème au niveau de la sécurité mais plutôt l'application de restitution des données. C'est donc cette partie qu'il faut protéger méticuleusement.

> « De la même façon, le vol (ou la délivrance) des données d'un serveur ou d'un ensemble de serveurs ne permet pas de lire les informations s'y trouvant stockées puisque chacune d'elles ne contient que des fragments de données. Seul le programme de reconstitution des informations (« la console de restitution ») est capable de faire le lien entre les fragments. Si en plus les données ont été cryptées (avec une clé RSA par exemple) avant d'être fragmentées, la lecture des fragments en direct devient quasi impossible. Ce point particulier dépend néanmoins du niveau de fragmentation des données, des gros fragments seront plus signifiants et permettront de lire plus d'information. » (Cigref, 2013, p. 6)

En 2010, le cabinet de consultance PAC (Pierre Audoin Consultants) a décidé de mener une enquête auprès de 200 sociétés d'informatique françaises afin d'identifier les freins et inhibiteurs par rapport au cloud. (Poujol, 2010) Les clients reconnaissent les avantages du cloud mais restent quand même bloqués par ces divers problèmes de sécurité. A côté de cela, la dépendance et la perte de contrôle sur les données sont également deux préoccupations majeures des entreprises.

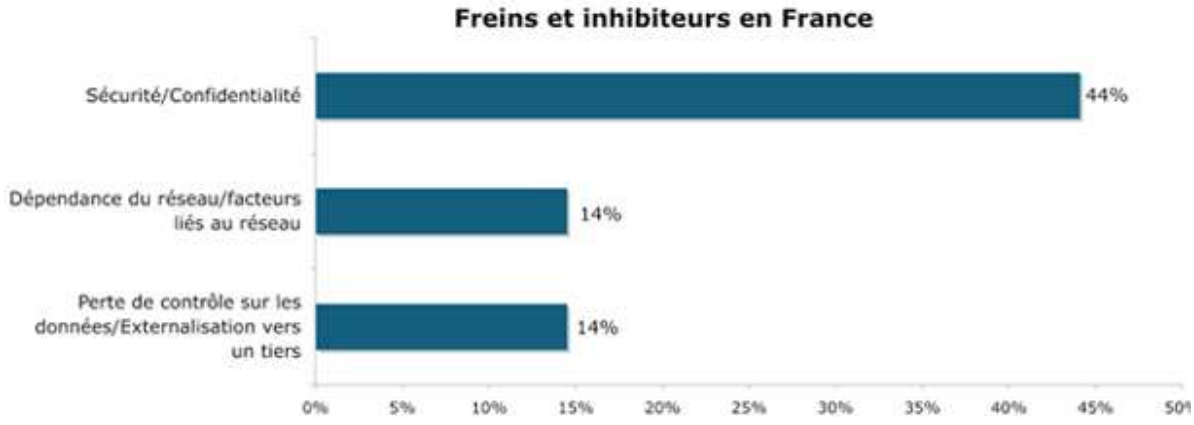

Figure 8: Les freins et inhibiteurs des entreprises Française au Cloud Computing. (Poujol, 2010, p. 8)

8.2. Dépendance/Perte de contrôle des données

Les entreprises qui décident d'utiliser le cloud computing deviennent dépendantes du fournisseur de service. Cette dépendance peut générer des difficultés concernant la disponibilité du fournisseur (et donc du service) : service hors d'usage, application lente, attente au niveau des réparations, …

En juillet 2012, plusieurs clients du fournisseur Amazone se sont vus dans l'incapacité à utiliser leurs services suite aux violentes tempêtes qui ont eu lieu dans l'Est américain. (Cheminat, 2012) Or un service bloqué pendant plusieurs heures suite à une coupure de courant peut provoquer d'énormes pertes financières.

De plus, une certaine perte de contrôle des données peut être ressentie par les entreprises du fait qu'elles ne savent pas exactement où se trouvent ces données et n'ont pas toujours la certitude de ce à quoi les fournisseurs les destinent. Il peut également y avoir des soucis techniques comme un crash disque et si le fournisseur n'a pas fait de backup, s'en suit la perte des données du client. Ce genre de mésaventure reste rare mais il est intéressant de savoir que ça peut toujours se produire. La traçabilité des données est donc un élément qui pose problème et qui inquiète, même si des efforts de la part des fournisseurs se font également dans ce sens :

> " A noter que sous la pression de l'Union Européenne et de la CNIL, les prestataires de Clouds publics assurent désormais plus de traçabilité sur l'emplacement des ressources mises à disposition en différenciant des grandes zones : Europe, Amérique et Asie. » (Direccte, 2012, p. 7)

Il est également bon de savoir que l'utilisation du cloud nécessite une connexion internet performante au risque de voir des ralentissements au sein des applications. En effet, la connexion internet sera utilisée de manière très intensive pour le transfert de données. Il faut donc s'assurer que le débit de la connexion sera suffisant et que celle-ci ne sera pas sujette aux coupures. De plus, l'utilisation d'applications web peut s'avérer lente même avec une connexion internet performante. Il faudra donc peut-être repenser les applications, voire même les limiter par rapport aux applications fonctionnant sur un ordinateur en local. Il est nécessaire aussi de vérifier que la productivité des employés utilisant les applications du cloud n'en soit pas diminuée suite à l'augmentation des temps des traitements de l'information.

Par ailleurs, la solidité du fournisseur est aussi à prendre en compte. En effet, il n'est pas question de prendre un fournisseur qui risque de mettre la clé sous la porte d'ici quelques mois. Or, ce cas de figure pourrait arriver et un changement de fournisseur pourra prendre beaucoup de temps. Il vaut mieux donc privilégier la stabilité. La difficulté réside dans le fait qu'il n'est pas toujours facile de déceler une entreprise qui se porte mal.

Ici, les clients ne sont plus réellement libres mais assujettis à un certain fonctionnement dont les règles du jeu sont décidées par le fournisseur de cloud computing. C'est en partie ce que reproche Richard Stallman, qui maintient que le cloud computing n'est qu'une façon d'emprisonner les utilisateurs en les rendant dépendants de services qui se trouvent dans des systèmes propriétaires. (Dailly, 2008)

Toujours en prenant Poujol comme référence, voici un graphique reprenant les principaux inconvénients associés au cloud computing selon le pourcentage d'utilisateurs rencontrant ces difficultés.

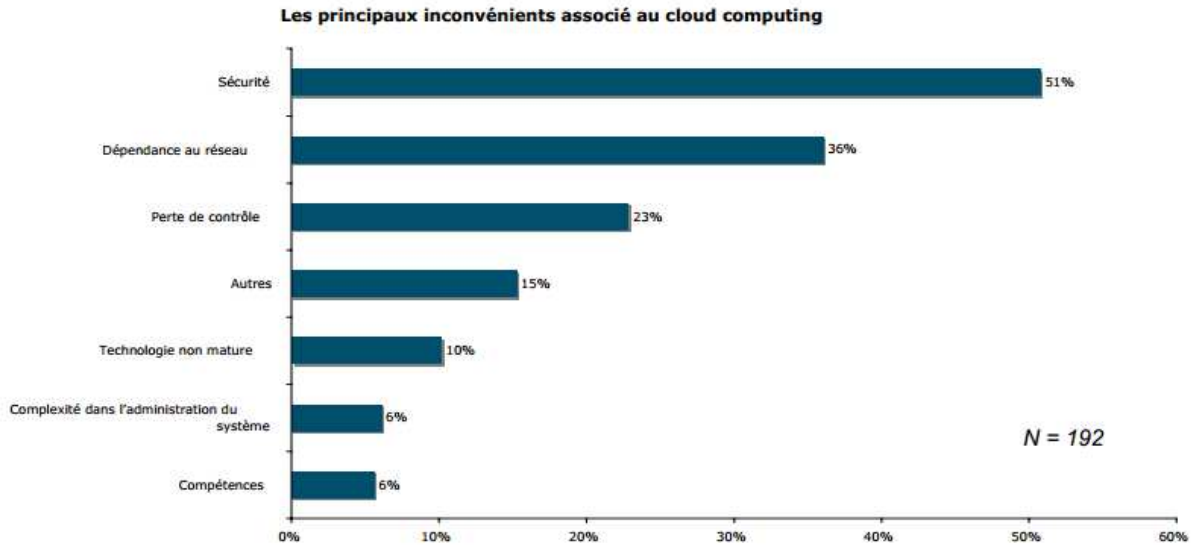

Figure 9: Les principaux inconvénients associés au cloud computing. (Poujol, 2010, p. 10)

8.3. Juridique

Comme ce fut déjà expliqué, les données des entreprises peuvent se retrouver hébergées au sein de data centers se trouvant à l'étranger sans en connaitre l'emplacement exact. Or, dans certains cas, la loi peut imposer de pouvoir localiser et accéder physiquement à ces données. (Dartyge, 2011)

Sachant que les règlementations sur la vie privée et le respect des données personnelles varient d'un pays à l'autre, les entreprises ont souvent quelques craintes à faire appel au cloud public. Dans certains pays, comme c'est le cas de la Chine, les autorités peuvent très rapidement avoir accès aux données stockées dans les serveurs. Une autre dérive possible peut être imputée aux entreprises qui se jouent de ce système pour éviter la loi et diriger leurs données à caractère illégal dans des pays plus tolérants.

Néanmoins, il faut savoir qu'une directive existe afin d'encadrer les transferts de données à caractère personnel : la Directive Européenne 95/46/CE. Celle-ci impose que les pays où sont hébergées ces données assurent une protection suffisante de ces dernières. Du coup, l'entreprise doit savoir dans quel pays elles sont stockées. Les Etats-Unis ne font pas partie de la liste des pays suivant ce principe, un cadre juridique spécifique a été créé, dénommé « Safe harbor ». (Direccte, 2012, p. 27)

Un autre aspect juridique concerne le contrat que nouent fournisseur et utilisateur.

> « Le contrat constitue la principale arme du client face aux nouveaux risques, en particulier celui de sa dépendance au fournisseur : capacité de retour en arrière, confidentialité, capacité à auditer. Le contrat est souvent la seule mesure engageante sur le volet sécurité. Or, la complexité juridique est souvent plus importante du fait de la dimension internationale qu'induit le *cloud computing*. » (Solucom, Cloud computing: comment en tirer parti?, 2010, p. 4)

8.4. ENISA

Pour répertorier plus d'informations concernant les risques liés au cloud, l'ENISA (European Network and Information Security Agency) a répertorié dans un rapport une série de 35 risques liés au cloud computing. Ce rapport est avant tout basé sur les avis d'experts issus de grandes entreprises informatiques. (Microsoft, Google, etc.) (Richard, 2009)

> « Cette publication est exactement le document de référence qui va aider les entreprises à avoir une bien meilleure vision des risques qu'elles prennent en sous-traitant un peu trop facilement, un peu trop aveuglément **»** (Schauer, 2009)

Dans ce document, les risques sont notamment divisés en 4 familles : (ENISA, 2009)

- Les risques politiques et organisationnels ;
- Les risques techniques ;
- Les risques légaux ;
- Les risques non liés au cloud.

A ces risques sont associés une probabilité d'apparition ainsi qu'un score d'impact au sein de l'entreprise si ce risque venait à se réaliser.

Des paramètres classent donc le risque sur une échelle d'importance des risques du cloud computing au sein de l'entreprise et indiquent au lecteur les points sur lesquels il doit se concentrer lors de la recherche d'un partenaire.

8.5. Solutions possibles

Face à ces risques et à la peur compréhensible des clients, certaines réponses peuvent être émises afin que les utilisateurs ne délaissent pas cette technologie.

8.5.1. Rassurer les clients

- Construire un cadre

Afin d'aider et de rassurer les clients, le cabinet d'analystes Gartner Group a établi une liste reprenant 7 points importants à clarifier lorsqu'un client souhaite établir un contrat avec un fournisseur de cloud. (Lambel, 2008)

Gartner recommande notamment que le client ait un droit de regard et de contrôle sur le personnel du fournisseur, que le fournisseur dispose de toutes les certifications de sécurité nécessaires, qu'il puisse isoler et crypter les données mais aussi récupérer ces données en cas de problème majeur. Gartner termine la liste en précisant que le fournisseur doit pouvoir localiser physiquement les données du client, collaborer avec la justice et enfin doit pouvoir vivre assez longtemps pour fournir les données au client. [Annexe 2]

- Respecter les normes

Les fournisseurs peuvent offrir un produit conforme à la norme Iso 27001. (Iso, 2008) Cette norme internationale décrit les exigences concernant la mise en place d'un système de gestion de la sécurité de l'information. Le respect de cette norme par les fournisseurs permet de garantir au client la protection de ses informations en cas de perte, de vol, d'intrusion ou de dommage. Le client a donc plus d'atouts pour faire confiance au fournisseur.

> « Pour rassurer les entreprises, la plupart des offreurs tendent également à se conformer aux standards du marché en matière de protection des données, de plans de continuité d'activité ou encore de respect des normes Iso » (Brunetière, 2011)

- Partager l'expérience

Ensuite, une autre façon de rassurer le client est de tout simplement organiser des visites au sein des data centers des fournisseurs. Cette technique a d'ailleurs été utilisée par la société « Accenture ». Cette même société propose aussi la diffusion de témoignages de clients. (News, 2011)

- Fournir des chiffres

Enfin, pour les clients à qui les études sembleraient plus parlantes et rassurantes, certains acteurs du cloud computing mettent tout en œuvre afin de rassurer ces clients plus sceptiques. (Brunetière, 2011) On peut prendre comme exemple le cas de la société « Accenture » qui a réalisé une étude sur le cloud computing. Cette étude rassure car elle témoigne de certains aspects positifs du cloud. (News, 2011)

Les chiffres se veulent parfois aussi rassurants. La société « Markness International » suit depuis quelques années l'évolution du cloud computing en France. Les données issues de sa dernière enquête menée auprès de 330 entreprises ont permis d'établir le graphique ci-dessous, montrant l'intérêt grandissant des entreprises françaises pour le cloud. (International, 2010)

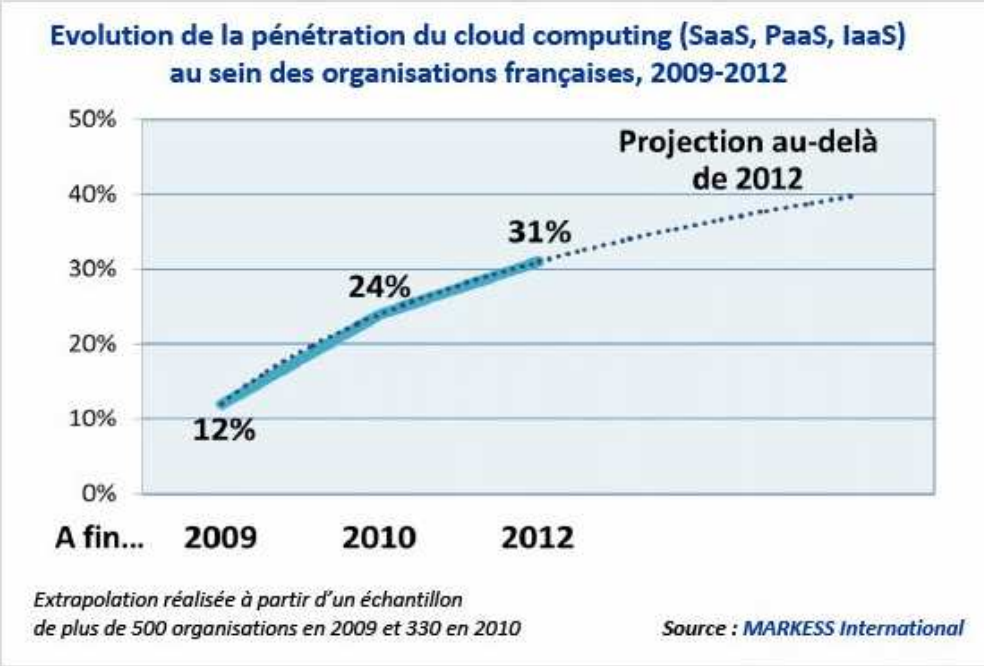

Figure 10: Intérêt grandissant pour le cloud computing. (International, 2010)

8.5.2. Utilisation du cloud privé ou de cloud hybride

Afin de garder un maximum de contrôle sur leurs ressources, les entreprises sont plus souvent tentées d'investir dans les clouds privés internes car l'infrastructure est totalement dédiée au client et gérée par celui-ci. (Pettey, Gartner Says Security Must Evolve as Organizations Move Beyond Virtualization to Private Cloud Infrastructures, 2010)

Néanmoins, cette solution aurait tendance à rester provisoire le temps que les clouds publics et hybrides fassent leurs preuves. (Zedi, 2010)

La figure 11 permet de montrer que le cloud privé est encore fortement privilégié dans les entreprises. Cette solution est en effet la plus adaptée pour rester maître de son infrastructure et assurer ainsi une meilleure administration de la sécurité.

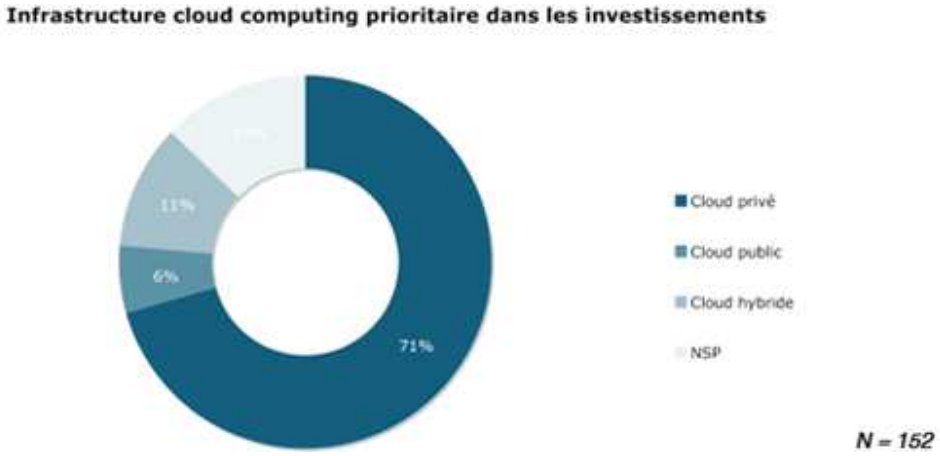

Figure 11: Le cloud privé est encore le choix préféré des clients. (Poujol, 2010, p. 14)

Il est également possible d'opter pour un compromis : adopter le cloud computing mais n'y confier que certaines données ciblées. Avec un cloud hybride, le client peut héberger certaines données dans ce cloud mais décider de garder les données les plus sensibles, plus critiques au sein de son entreprise. Mais comme rappelé précédemment, si l'utilisateur prend l'initiative de mettre toutes ses données au sein d'un cloud public, ça relève de sa responsabilité.

Mais quelles sont les données qui peuvent être considérées comme plus sensibles ? CIGREF, l'IFACI et l'AFAI, dans leur écrit « Guide pratique : Cloud computing et protection des données », mettent en avant l'importance de classifier les données selon trois catégories :

« - les données sensibles à caractère personnel (cfr CNIL),
- Les données stratégiques pour l'entreprise,
- Les autres données utilisées dans les applications métiers » (Cigref, 2013, p. 11)

Ils définissent alors ce que peut être une donnée stratégique : « (…) un ensemble d'informations qui, si elles étaient détenues ou mises en corrélation par des tiers, pourraient permettre de prendre de vitesse ou neutraliser une prise de position envisagée par l'entreprise et dont l'impact serait d'une telle ampleur, que la stratégie de l'entreprise serait fortement ou durablement impactée. » (Cigref, 2013, p. 11)

8.5.3. SLA (Service Level Agreements)

Un Service Level Agreements (SLA) est, de manière générale, un contrat qui spécifie la qualité de service proposé par un fournisseur à un client.

Dans le cadre du cloud computing, le SLA peut par exemple définir les niveaux de disponibilité, de performance, d'opération, …

On peut décrire un SLA grâce à deux spécifications techniques :

- Le Service Level Specification (SLS) qui est un guide spécifiant certains critères que le service doit fournir ;
- Le Service Level Object (SLO) qui, lui, fournit le nécessaire permettant les mesures de qualité des services telles que décrites dans le SLS. (Emmanuel Marilly, 2002)

Il n'est pas toujours aisé pour le fournisseur comme pour le client de bien baliser et conclure un business. Un SLA peut aider dans ce domaine. En effet, il peut être utile pour :

- Identifier et décrire les différents besoins et attentes du client ;
- Offrir un cadre général de compréhension au fournisseur et au client;
- Simplifier les problèmes complexes ;
- Encourager la conversation en cas d'oppositions ;
- Eliminer les perspectives irréalistes ;
- …

Alors le SLA est-il obligatoire? Non, celui-ci n'est pas obligatoire mais il est préférable car il constitue une garantie pour chaque protagoniste. De plus, un SLA va permettre au client de pouvoir comparer les offres des différents fournisseurs pour une même demande et donc de choisir le fournisseur qui sera capable de s'engager pour la globalité du SLA et pour le budget le plus intéressant. (Tonic, 2010)

9. Conclusion

En guise de conclusion, voici un extrait de Joset dans son ouvrage « Cloud computing, tentative de définition », reprenant les grandes lignes de ce que représente le cloud computing.

> « *L'informatique dans les nuages ou informatique en nuage, en anglais Cloud Computing, est un concept majeur dans l'évolution informatique de ces dernières années. Ce concept fait référence à l'utilisation des capacités de calcul et de stockage d'ordinateurs et de serveurs répartis dans le monde entier fournies en tant que service à travers les technologies internet vers une multitude d'utilisateurs externes.*
> *Le cloud computing est donc un concept de déportation sur des serveurs distants des traitements informatiques traditionnellement effectués sur des ordinateurs locaux. Les utilisateurs ou les entreprises ne sont plus gérants de leurs propres capacités informatiques mais peuvent ainsi accéder de manière évolutive à de nombreux services en ligne sans avoir à gérer l'infrastructure sous-jacente, souvent complexe. Les applications et les données ne se trouvent plus sur l'ordinateur local, mais - métaphoriquement parlant - dans un "nuage" (cloud) de serveurs distants interconnectés au moyen d'une excellente bande passante indispensable à la fluidité du système. L'accès aux services se fait par une application standard facilement disponible, la plupart du temps un navigateur web* » (Joset, 2011)

Le cloud computing est entouré d'un certain flou et chacun a tendance à en faire sa propre interprétation. Heureusement, avec cet essor du cloud, certains professionnels prennent l'initiative de mettre la main à la pâte et essaient d'esquisser les grandes balises de cette technologie.

Après avoir parcouru le cloud computing, nous pouvons dire que cette technologie est très complexe dans ce qu'elle représente : elle peut tout aussi bien apporter de nombreux bénéfices aux utilisateurs mais apporte également son lots de risques. Nous pouvons dire à ce stade que le cloud computing est la cible de nombreux enjeux : la sécurité, la dépendance au réseau, la perte de contrôle des données et l'aspect juridique en sont de beaux exemples. Mais face à ces risques, le client ne reste pas sans réponse : les entreprises tentent de rassurer les clients, l'utilisation du cloud privé est privilégiée ainsi que celle du cloud hybride, l'utilisation du SLA est possible.

Après avoir mis en évidence nombre d'atouts et de limites du cloud, il incombe à chacun de faire un choix personnel. En effet, prendre position par rapport au cloud, c'est avant tout un travail d'arbitrage. Comme pour toute décision à prendre, il est sage de peser les « pour » et les « contre » afin de se décider en tout état de cause. Le client se doit ainsi de calculer les risques sans pour autant tomber dans un extrême ou l'autre.

Mais à la suite de cette réflexion, certaines questions peuvent être soulevées : le cloud computing n'est-il pas un effet de mode comme a pu l'exprimer Dailly ? (Dailly, 2008) N'est-ce pas un concept marketing comme tant d'autres ? En effet, nous n'avons pas inventé la roue : les applications en ligne existent depuis déjà un bon nombre d'années. Il ne s'agit pas vraiment d'une nouvelle invention mais d'une popularisation d'une technologie déjà existante depuis longtemps. Et même si c'est un effet de mode, est-ce réellement une raison pour lui tourner le dos ?

Toutes ces interrogations ne sont pas nouvelles et ont sûrement déjà été posées par bien d'autres avant moi. Sur un plan idéologique, ces questionnements renvoient chacun à sa propre réflexion personnelle. Au niveau technique, nous avons pu constater que quelques tentatives de solutions étaient mises en avant, elles se montreront convaincantes pour certaines, pas suffisantes pour d'autres. Mais face aux réticences persistantes, une autre perspective s'ouvre aux clients, non plus technique mais humaine : le cloud broker.

Chapitre 2 : Cloud Broker

1. Introduction

Tout au long du chapitre précédent, j'ai tenté de mettre en évidence toute la richesse et la complexité du cloud computing. De toute évidence, cette technologie en intrigue plus d'un et à l'art d'alimenter les débats : pour ou contre ? Cloud, révolutionnaire ou aberrance ? Solutions concrètes et réelles ou poudre aux yeux ? Comme je le rappelle, ici, c'est une question d'arbitrage. Mais face au désarroi pouvant habiter certains utilisateurs, un acteur clé a fait son apparition : le cloud broker.

Mais qu'est-ce qu'un cloud broker ? Certaines personnes se diront probablement qu'on rajoute à nouveau de la complexité dans un contexte déjà nébuleux. Mais que du contraire… le cloud broker est tout autre chose selon moi : un facilitateur de cloud. Afin d'argumenter mes dires, cette partie sera amorcée par quelques définitions de ce qu'est un broker, suivi du contexte plus général dans lequel il opère, à savoir le two sided market. Ensuite, comme il est toujours primordial de savoir de quoi l'on parle précisément, l'architecture du broker sera abordée à la manière d'un zoom : d'abord les deux grands types de broker ; ensuite les trois services qu'un broker est censé pouvoir fournir et finalement les différents composants qui l'amènent à pouvoir concrétiser ces services. Afin de clôturer ce chapitre, nous ferons un petit « arrêt sur image » sur les différents avantages et inconvénients qui accompagnent la mobilisation d'un cloud broker.

2. Définitions

2.1. NIST

L'institut NIST, dans son rapport « NIST Cloud Computing Reference Architecture », revient sur l'architecture du cloud et présente une vue d'ensemble de celle-ci. Pour lui, lorsque nous nous trouvons dans un contexte de cloud, cinq principaux acteurs interagissent entre eux selon leurs spécificités : le cloud consumer, le cloud provider, le cloud auditor, le cloud broker et le cloud carrier. Via le tableau ci-dessous, il explique les spécificités imputées à chacun de ces protagonistes. (Fang Liu, NIST Cloud Computing Reference Architecture, 2011)

Actor	Definition
Cloud Consumer	A person or organization that maintains a business relationship with, and uses service from, *Cloud Providers*.
Cloud Provider	A person, organization, or entity responsible for making a service available to interested parties.
Cloud Auditor	A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation.
Cloud Broker	An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between *Cloud Providers* and *Cloud Consumers*.
Cloud Carrier	An intermediary that provides connectivity and transport of cloud services from *Cloud Providers* to *Cloud Consumers*.

Figure 12: Les différents acteurs et leur rôles suivant NIST (Fang Liu, NIST Cloud Computing Reference Architecture, 2011)

NIST place donc le cloud broker dans un certain contexte fait d'interactions avec les autres acteurs du cloud. Il ne constitue pas un élément isolé mais a justement été créé pour être en lien avec les autres. En effet, nous pouvons d'emblée le percevoir comme un « intermédiaire » au service des utilisateurs et des fournisseurs… au service du cloud, donc.

Plusieurs cas de figures peuvent bien entendu être imaginés ici, ces 5 acteurs pouvant entrer en relation selon de multiples façons. Mais nous allons plutôt nous attarder sur les relations que peuvent tisser le cloud consumer, le cloud provider et le cloud broker. Dans l'illustration suivante, toujours tirée du rapport de NIST, nous nous arrêterons donc sur cet aspect des choses.

Lorsqu'un cloud consumer désire faire appel à un (ou des) cloud(s) provider, il peut soit entrer en contact directement avec eux, soit interpeller un cloud broker qui fera office d'intermédiaire. Pour toutes sortes de raisons que nous expliquerons par la suite, il peut être avantageux de mobiliser un cloud broker et, ici, nous allons imaginer que c'est ce pour quoi l'utilisateur va opter. Une fois en relation avec le cloud consumer, le cloud broker va se mettre en contact avec différents clouds provider afin de négocier le(s) service(s) dont le client a besoin. Il est envisageable, comme nous le verrons par la suite, que le cloud broker crée un nouveau service pour le cloud consumer ou qu'il combine de multiples services provenant de fournisseurs différents. Dans ce contexte, le cloud broker constitue le pilier central de la relation alors que le cloud consumer et les clouds provider n'entrent pas directement en interaction. Nous pouvons ainsi dire que les clouds provider sont finalement totalement invisibles aux yeux du cloud consumer qui fait la demande de service. (Fang Liu, NIST Cloud Computing Reference Architecture, 2011)

Figure 13: Scénario d'échange cloud consumer – cloud broker – cloud provider (Fang Liu, NIST Cloud Computing Reference Architecture, 2011).

> "As cloud computing evolves, the integration of cloud services can be too complex for cloud consumers to manage. A cloud consumer may request cloud services from a cloud broker, instead of contacting a cloud provider directly. A cloud broker is an entity that manages the use, performance and delivery of cloud services and negotiates relationships between cloud providers and cloud consumers." (Fang Liu, NIST Cloud Computing Reference Architecture, 2011)

2.2. Forrester

Nous pouvons maintenant mettre en avant l'intérêt grandissant des utilisateurs pour le cloud computing. Et souvent, ce qui prend de l'ampleur se complexifie. Le cloud broker prend alors tout son sens dans ce contexte de complexification des demandes et des offres : il permet de « débroussailler » le terrain et d'opter pour l'offre la plus adaptée à la demande.

> "For this report, Forrester interviewed vendor strategists at more than 30 leading and emerging cloud vendors to discuss and identify possible business models and value propositions around cloud computing. (…) In particular, the cloud broker business model is emerging as one of the most promising and ambitious models because it offers a unified approach to virtually all cloud segments (…)." (Ried, 2011, p. 2)

L'entreprise Forrester met en évidence la transformation qui s'opère lorsque les trois business models traditionnels (pure software model, pure consulting model et pure infrastructure model) sont mis en présence au sein d'un cloud. En effet, nous voyons apparaitre 7 nouveaux clouds business model dont le cloud broker est au confluent. (Figure 14) Il fait alors du cloud broker l'élément le plus complexe de son cloud business model, précisant même qu'il peut offrir une plus-value au cloud. (Ried, 2011, pp. 4-5) [Annexe 3]

> "(…) the cloud broker represents the most complex business model, offering a wide value contribution in the emerging cloud space. Essentially, this model leverages skills and capabilities from all three of the traditional business models of software, consulting, and infrastructure." (Ried, 2011, p. 6)

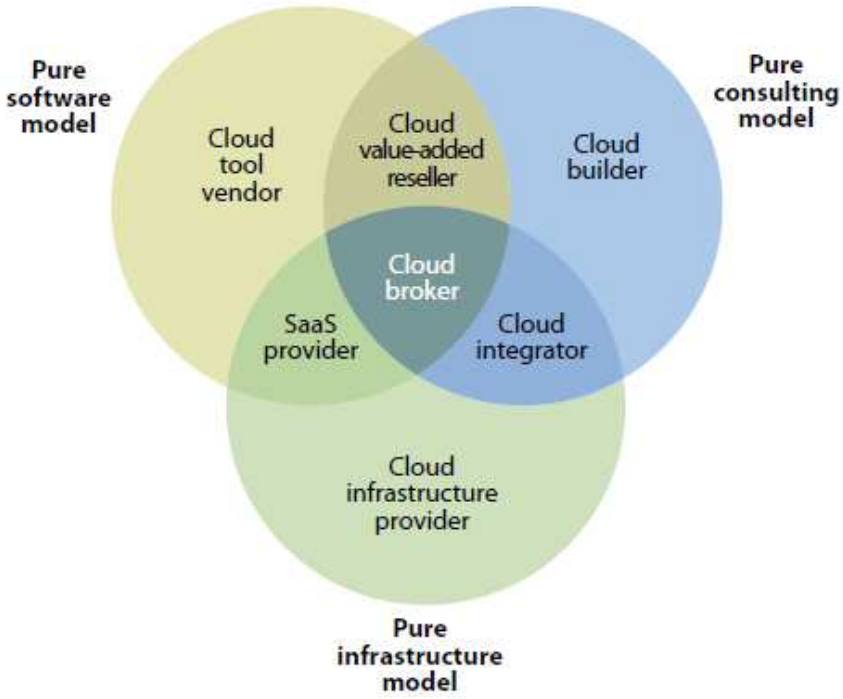

Figure 14: Cloud broker business model proposé par Forrester (Ried, 2011)

2.3. Source scientifique

Dans le rapport « Towards Secure Cloud Bursting, Brokerage and Aggregation », le cloud broker est présenté comme une plate-forme de gestion sécurisée permettant la simplification des prestations de services entre un cloud consumer et un cloud provider :

> "Cloud service broker creates a governed and secure cloud management platform to simplify the delivery of complex cloud services to cloud service customers. They enable customers to realize the full potential that cloud provider has to offer. They enforce the correct IT policies and effectively handle service level agreements between cloud providerand cloud service consumer. Cloud Service Broker creates a trusted, governed and secured cloud management platform between cloud service provider and cloud service consumer." (Srijith K. Nair, 2010, p. 3)

2.4. Définition personnelle

Parmi les différents acteurs du cloud, le cloud broker tient une place particulière « d'intermédiaire ». Un cloud broker est une entité (personne physique ou morale) qui représente le lien entre les utilisateurs (cloud consumer) et les fournisseurs de cloud (cloud provider) et doit donc être synonyme de confiance. Ainsi, nous pouvons dire qu'un cloud broker est un « facilitateur ». En effet, à l'heure où de nombreuses zones d'ombre planes encore autour du cloud, le cloud broker permettra de rendre les choses plus limpides et plus faciles. Ce dernier peut être perçu comme un atout pour les utilisateurs mais également pour les entreprises : d'une part il aide les consommateurs à trouver l'offre la plus adaptée à leur demande (le prix, les conditions, la livraison, le déploiement de service), d'autre part il épaule les entreprises afin qu'ils rentabilisent au mieux leur production. Il est possible que certains cloud broker offrent des services supplémentaires en proposant par exemple le monitoring du réseau, l'agrégation de services venant de multiples fournisseurs ou encore une couche de sécurité supplémentaire.

3. Principe général

Le cloud broker fonctionne suivant le principe général du two sided market. Le two sided market (ou marché biface) est un type de marché où deux clientèles différentes interagissent par l'intermédiaire d'une même et unique plate-forme. Le développement quasi-simultané de chaque côté du marché est important car il permet de garantir l'attrait des deux clientèles pour le marché. Une notion de dépendance s'établit entre les trois acteurs, chacun ayant besoin de la présence des deux autres pour fonctionner. (Thomas Eisenmann, 2006)

Nous pouvons reprendre l'exemple du site « Lexicon » qui illustre un cloud broker à l'aide d'un centre commercial. Celui-ci joue le rôle de la plate-forme intermédiaire, le broker, entre les acheteurs de différents bien d'un côté et les vendeurs de ces différents biens de l'autre. Le centre commercial prend de l'importance en soumettant aux acheteurs un vaste choix de vendeurs et en proposant aux vendeurs un large panel d'acheteurs. (lexicon)

Un cloud broker se positionne comme intermédiaire sur un marché biface. Pour qu'un cloud broker devienne populaire auprès des fournisseurs d'applications cloud, il faut que celui-ci puisse offrir un large public de clients potentiels. Et pour attirer un grand nombre de clients, il faut qu'il puisse offrir un vaste catalogue de fournisseurs de services cloud.

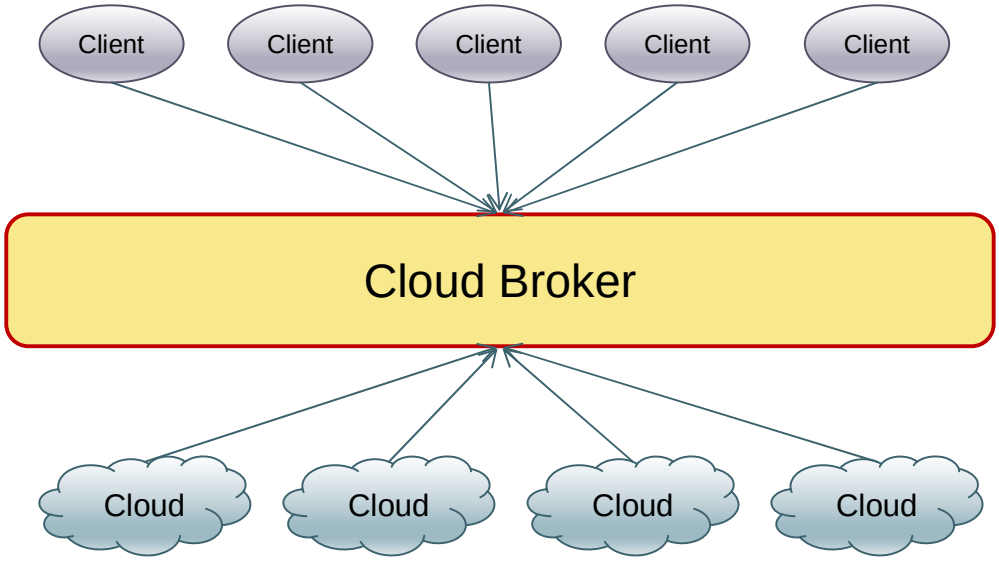

Figure 15: Cloud broker dans le two sided market.

4. Architecture

4.1. Types de cloud broker

Cette partie s'appuie sur les dires de l'institut NIST qui présente les brokers selon deux grands types possibles. D'un côté, nous avons des brokers plus axés sur le business et de l'autre, ceux qui sont plus axés sur la facette technique. Néanmoins, ces deux types de broker ne sont pas exclusifs : un broker qui est du type business broker dans un contexte peut être un technical broker dans un autre contexte, voire même les deux dans un troisième contexte.

4.1.1. Business Broker

Ici, le service proposé par le broker est plus orienté business. Il propose dès lors des services tels que la facturation, l'intermédiation contractuelle, l'arbitrage et l'agrégation. Un business broker n'aura aucun contact avec les données du cloud consumer, ses opérations et d'autres éléments du cloud tels que images, volumes, firewalls,… (NIST, 2013, p. 35)

Cette technique peut être intéressant dans le sens où un cloud consumer ne souhaiterait pas que ses données sensibles passent (et soient peut être stockées) par le cloud broker.

4.1.2. Technical Broker

Un technical broker permet la gestion des services d'agrégation, d'arbitrage et d'intermédiation à un niveau plus technique avec un focus plus particulier sur les problèmes d'interopérabilité entre plusieurs cloud provider. Le but ici est de pouvoir faire de l'agrégation de services en provenance de multiples provider et d'ajouter une couche de fonctionnalités techniques (par exemple single point of entry et interopérabilité).

Un technical broker peut offrir des services croisés provenant de divers fournisseurs tels que l'orchestration, la gestion de la charge, la gestion des autorisations, la gestion de la sécurité et les mesures de couts et d'utilisation… (NIST, 2013, p. 35)

4.2. Services proposés par le cloud broker

L'entreprise américaine Gartner spécialisée dans la recherche et la consultation dans le domaine des TIC, a publié un rapport sur les cloud service brokerage. Dans ce document, Gartner présente en trois principales catégories les différents types de services qu'un cloud broker peut proposer aux cloud customer: (Pettey & Meulen, Newsroom, 2009)

- Service Intermediation ;
- Service Aggregation ;
- Service Arbitrage.

Ce découpage en trois catégories de services est également approuvé et repris par l'institut NIST dans sa publication ayant pour but de référencer l'architecture du cloud computing (Fang Liu, NIST Cloud Computing Reference Architecture, 2011)

4.2.1. Service Intermediation

Le premier type de service qui sera détaillé dans cette partie est le service intermediation. Le rôle d'un service intermediation est de proposer au cloud consumer, en plus du service de base, une plus-value de service qui peut être créée par un autre fournisseur de cloud que le fournisseur de base ou créée par le broker lui-même. Ce sont donc des services supplémentaires qui sont fournis au consumer afin de satisfaire au maximum sa demande.

Ces services supplémentaires sont une véritable valeur ajouté pour le consommateur et permettent, par exemple, de pouvoir offrir la gestion globale des identités ou des accès, le reporting de la performance ou de renforcer la sécurité. Le cloud broker pourrait aussi ajouter des services concernant le contrôle de la tarification et de la facturation. (Pettey & Meulen, Newsroom, 2009)

Il est possible d'obtenir ce service intermediation à trois niveaux différents: - cloud provider – cloud consumer – cloud. Si l'intermédiation se trouve au niveau du provider, ça permet à ce dernier de pouvoir délivrer aux clients un niveau de gouvernance au-delà du niveau du service d'origine. Si c'est au niveau du consumer, ça lui permet la gestion locale de cette valeur ajoutée. L'intermédiation peut également se trouver au niveau du cloud et là, le broker peut mettre à disposition ce service lui-même. (Pettey & Meulen, Newsroom, 2009)

Dans un tel contexte, nous pourrions dire que le broker est soit un élément neutre soit il peut concurrencer directement les autres fournisseurs. Cette interprétation rejoint celle proposée par la GSA (General Services Administration) :

> « A broker could be a neutral intermediary prohibited from providing their own services in direct competition with [cloud service providers]. Alternatively, a broker could be permitted to introduce their own services into the brokerage environment and offer their services in competition with the [other providers]." (Lauchlan, US government explores Cloud Broker concept for public sector, 2012)

4.2.2. Service Aggregation

Dans un service aggregation, le cloud broker travaille simultanément avec plusieurs fournisseurs et s'occupe de rassembler divers services proposés par ces fournisseurs afin de les présenter au cloud consumer sous la forme d'un seul et unique service unifié. Le cloud broker se doit d'assurer la circulation et la sécurité du transfert des données entre le cloud consumer et les différents fournisseurs. (Pettey & Meulen, Newsroom, 2009)

Généralement, ce service se trouve au niveau du cloud et forme une couche se rapprochant de la couche applicative. (Pettey & Meulen, Newsroom, 2009)

Le service aggregation est un exemple du modèle de scalability horizontale vu précédemment. Le cloud broker augmente le nombre de fournisseurs de service lorsque la demande en ressource augmente.

4.2.3. Service Arbitrage

Le service arbitrage est comparable au service aggregation, dans le sens où il permet toujours de combiner les services provenant de plusieurs fournisseurs mais il offre en plus la possibilité au client de faire des choix plus opportuns parmi plusieurs services similaires. (Pettey & Meulen, Newsroom, 2009)

Ce service offre donc une flexibilité supplémentaire, permettant aux utilisateurs de faire des choix plus adaptés et qui collent plus à leur réalité, leur demande.

La figure suivante offre une vue d'ensemble de l'architecture du cloud et des trois catégories de service pouvant être offertes par le cloud broker. Nous pouvons visualiser clairement ici toutes les interactions que nouent le trio « cloud consumer-cloud broker-cloud provider ».

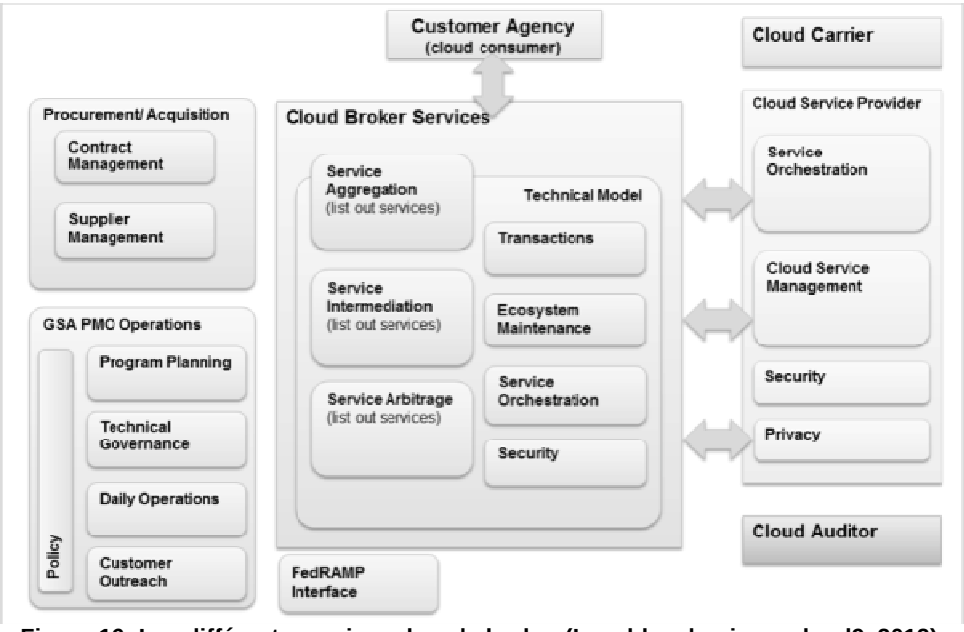

Figure 16: Les différents services dans le broker (Lauchlan, businesscloud9, 2012)

4.3. Composants du cloud broker

Comme il a été vu précédemment, lorsqu'un cloud customer décide de passer par un cloud broker, il est en droit d'attendre de celui-ci qu'un certain nombre de demandes soit pris en compte et respecté par le cloud broker. Voici quelques services de base qu'un broker est censé pouvoir réaliser : (Srijith K. Nair, 2010)

« - Ensure data confidentiality and integrity to service customers.
- Effectively match the requirements of cloud consumer with the service provided by the provider.
- Negotiate with service consumers over SLAs.
- Maintain performance check on these SLA's and take actions against SLA violation.
- Effectively deploy services provided by the cloud provider to the customer.
- Manage the API so that provider doesn't learn anything about the identity of the service consumer.
- Securely transfer customer's data to the cloud.
- Enforce access control decisions uniformly across multiple clouds.
- Scale resources during load and provide effective staging and pooling services.
- Securely map identity and access management systems of the cloud provider and consumer.
- Analyze and take appropriate actions against risks.
- Handle cloud burst/spill-over situations effectively."

Pour parvenir à réaliser sa tâche, le cloud broker va mettre en place certains composants au sein de son architecture. Ceux-ci sont représentés sur la figure suivante en fonction du domaine dans lequel ils interviennent.

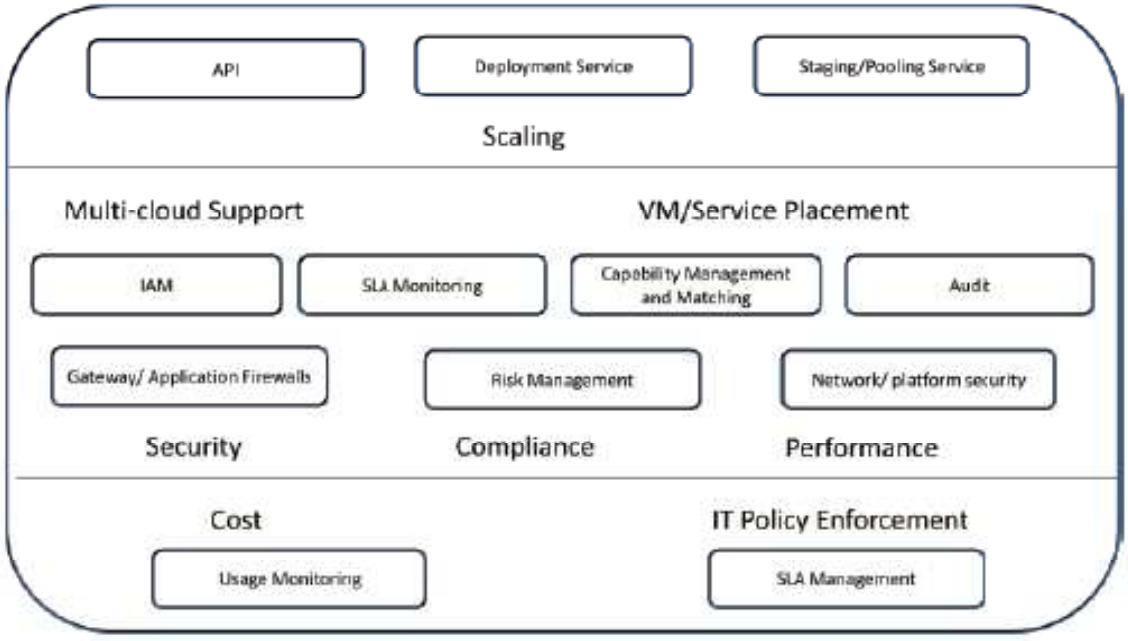

Figure 17: Composants d'un cloud broker (Srijith K. Nair, 2010)

4.3.1. Application Programming Interface (API)

L'API est le composant permettant aux utilisateurs d'interagir avec le broker afin d'effectuer les différents appels des services du cloud mais aussi la création et la gestion des ressources du cloud comme les composants de calcul et de stockage. (Srijith K. Nair, 2010)

De plus, c'est grâce à ce composant que le broker peut proposer au cloud consumer un panel de différents services provenant de multiples cloud provider. Ceci pourra donc répondre à une demande de service aggregation. (Jin, 2011)

4.3.2. Deployment Service

Cet élément permet la gestion du déploiement des services fournis par le cloud provider pour le cloud consumer. Par exemple, c'est à travers cette unité que le broker informe au cloud provider de démarrer une machine virtuelle en vue de fournir puissance de calcul et espace de stockage au cloud consumer. (Srijith K. Nair, 2010)

4.3.3. Staging/Pooling Service

Ce composant permet d'assurer la capacité du cloud broker à fournir une performance satisfaisante pour les différents services demandés par le cloud consumer.

Comme il a déjà été expliqué précédemment, les services du cloud sont présentés sous une formule de pay-per-use et de service scalable. Les cloud consumer peuvent donc exiger des ressources supplémentaires de la part des fournisseurs. C'est au broker d'interagir avec le cloud provider approprié, via ce composant, afin qu'il soit disponible pour traiter la requête et libérer les ressources supplémentaires demandées. Mais si le cloud provider n'arrive pas à satisfaire la demande de ressource supplémentaire, le Staging/Pooling Service a aussi pour but de retrouver depuis le Pool un autre cloud provider pouvant répondre à cette demande de ressource. (Srijith K. Nair, 2010)

4.3.4. Identity and Access (IAM)

L'IAM est un composant important car il garde en mémoire les renseignements des cloud consumer, des cloud provider et du type de service qu'ils proposent (service de stockage ou de calcul par exemple) ainsi que les critères de classification que le broker et le cloud consumer ont déterminés ensemble. C'est suivant ces critères de classification que l'IAM pourra contrôler de façon sécurisée l'accès aux services pour les cloud consumer grâce à la génération d'un token unique d'accès. (Srijith K. Nair, 2010)

4.3.5. SLA Monitoring

Le SLA Monitoring effectue la surveillance (monitoring) en permanence de toute la SLA. Cela a pour but de vérifier s'il y a des violations de SLA et si oui, ce composant permettra alors de prendre les mesures préventives nécessaires. (Srijith K. Nair, 2010)

4.3.6. Capability Management and Matching

Ce composant permet de garder en mémoire toutes les fonctionnalités fournies par les différents cloud provider comme la livraison, le modèle de déploiement, le mécanisme de sécurité, la structure de frais, les fonctionnalités IT et tous les autres détails nécessaires à l'utilisation. Chaque fois qu'un cloud consumer passe par le broker pour utiliser un service du cloud, ce composant fait correspondre les exigences SLA avec les services offerts par le cloud provider et trouve celui qui est le plus approprié. C'est donc ce composant qui permet de répondre au rôle de sélection qu'on attend du cloud broker afin de trouver pour le cloud consumer la solution la plus appropriée à ses besoins. (Rouse, 2011)

Ce composant est aussi mobilisé par le composant Staging and Pooling lors d'une hausse soudaine de montée en charge afin de pouvoir solliciter plus d'espace de stockage ou de puissance de calcul. (Srijith K. Nair, 2010)

4.3.7. Audit

Ce module permet de réaliser périodiquement un audit de la plate-forme du cloud broker grâce aux capacités fournies par le cloud provider. L'audit est surtout effectué afin de s'assurer de la validité et de la fiabilité de l'information des cloud consumer mais aussi pour fournir une évaluation des contrôles internes du broker. (Srijith K. Nair, 2010)

4.3.8. Gateway/Application Firewalls

Ce composant permet de bloquer le trafic malveillant en provenance des différents composants exposés par les interfaces du cloud broker. (Srijith K. Nair, 2010)

4.3.9. Risk Management

Le composant Risk Management identifie, évalue et hiérarchise les risques sur base des effets engendrés par un événement. Il vise à réduire, monitorer et contrôler la probabilité qu'un événement malheureux se produise. Les stratégies mises en place pour gérer les risques sont notamment d'éviter que ceux-ci se produisent, réduire l'impact négatif et accepter certaines ou toutes les conséquences d'un risque particulier. (Srijith K. Nair, 2010)

4.3.10. Network/Platform security

Le module Network/Platform security vient en complémentarité du module Firewall car il permet de gérer la sécurité globale de la plate-forme du broker. Différentes dispositions sont alors adoptées afin de prévenir les accès non autorisés au réseau, les utilisations abusives, les modifications ou refus du réseau et les ressource indisponibles sur celui-ci. Il fournit aussi une protection aux frontières de la plate-forme du broker en gardant en dehors de celle-ci les intrus et pirates souhaitant s'infiltrer dans le système. Le système de détection d'intrusion qui est une partie de ce composant est centré sur la protection des données venant de malware, virus, worms ou chevaux de Troie. (Srijith K. Nair, 2010)

Un exemple d'un tel composant est l'API « Apigee » de la société « Gartner » qui offre des possibilités de surveillance du cloud, cela pouvant aller de la collecte des messages échangés entre le client et le fournisseur à la taille des requêtes passant par le service. (Sampson, 2012)

4.3.11. Usage Monitoring

Ce composant permet la surveillance de l'utilisation des différents services par le cloud consumer. Le but étant par la suite de leur générer mensuellement les factures du cloud consumer. (Srijith K. Nair, 2010) Des outils tels que « Cordys » permettent la mise en place d'un système de consultation de la consommation des services par le client, de surveillance et de mesure des services. (cordys, 2013)

4.3.12. SLA Management

Le SLA Management est un module pouvant permettre la gestion des différents SLA mis en place entre le cloud broker et le cloud consumer. (Srijith K. Nair, 2010)

C'est grâce à cela que les exigences du cloud consumer seront transmises au cloud broker qui devra alors mettre tout en œuvre afin de les satisfaire.

5. Avantages et inconvénients du cloud broker

5.1. Avantages du cloud broker

Comme je l'ai déjà expliqué, le cloud, en prenant de l'ampleur, se complexifie et les utilisateurs pourraient vite se perdre dans la montagne d'offres qui leur sont faites. Le cloud broker est présent pour faciliter la vie des consommateurs mais pas seulement, car il apporte aussi certains bénéfices aux fournisseurs de cloud. Il est dès lors indéniable qu'un cloud broker apporte certains avantages, dont les principaux seront rapidement exposés ici.

Premièrement, l'utilisation d'un cloud broker permet à un cloud consumer de travailler avec plusieurs cloud provider tout en bénéficiant d'un seul point de contact : le cloud broker. Celui-ci s'occupera alors de gérer les échanges avec les différents providers, sans que le cloud consumer doive s'en inquiéter. C'est ainsi que nous pouvons aboutir à des services du genre « service aggregation », qui permettent au cloud broker de rassembler plusieurs services émanant de plusieurs fournisseurs afin d'en proposer un seul unifié au client.

Le deuxième atout d'un cloud broker est qu'il ne se limite pas à proposer certains services offerts par les providers mais peut aller plus loin dans sa démarche en proposant le service intermediation. Non seulement il proposera des services provenant de divers fournisseurs répondant à la demande du client mais mieux encore il lui offrira des services supplémentaires. Ces services peuvent être une amélioration de la gestion de la sécurité, du monitoring des services ou le contrôle de la facturation et de la tarification.

Enfin, un cloud broker peut aussi proposer du service arbitrage. Comparable au service aggregation, le service arbitrage propose toujours la combinaison de différents services venant de multiples clouds providers mais offre en plus la dimension de choix pour des services comparables. Le but pouvant être par exemple la recherche du service le moins cher afin de réaliser des économies.

Quoi qu'il en soit, le cloud broker a pour objectif de proposer au client une solution optimale en offrant la possibilité de personnaliser l'offre de service et ce, en essayant de réduire les coûts. En faisant office d'intermédiaire entre les utilisateurs et les fournisseurs, il devient facilitateur de relation et essaie de pallier aux manquements et dérives incombés au cloud (manque de sécurité, manque de visibilité, manque de garanties,…).

5.2. Inconvénients du cloud broker

Il va de soi que notre réalité n'est pas parfaite. Avoir le cloud broker pour palier à la totalité des risques liés au cloud, ça semblerait trop facile ! Malgré les multiples avantages qu'un cloud broker peut apporter, celui-ci peut donc aussi apporter son lot d'inconvénients.

Tout d'abord, nous pouvons noter qu'avant de pouvoir bénéficier de l'avantage de la diminution du coût des services, il ne faut pas oublier qu'il faudra avant tout s'acquitter des frais engendré par le passage par un prestataire. Il sera dès lors primordial de réaliser une étude auparavant afin de s'assurer de la possibilité d'amortir les coûts.

Ensuite, le passage par un cloud broker rend le client dépendant. En effet, il n'est plus totalement maitre de ce qu'il fait, déléguant une partie de ses tâches et prises de décision au cloud broker. Le client peut avoir le sentiment d'être dépossédé. Une nouvelle fois, l'importance de la confiance dans ce style de relation peut être mise en évidence.

De plus, un client peut être très content de sa collaboration avec le cloud broker choisi mais ne pas être totalement satisfait pour autant. En effet, la qualité des services du broker peut être mise en corrélation avec la qualité des services des fournisseurs. L'impact d'un mauvais fournisseur peut avoir d'énormes conséquences. Par exemple, un fournisseur ne respectant pas le SLA pourrait compromettre, perdre voir même diffuser les données du client.

Enfin, la mobilisation d'un cloud broker peut aussi poser des problèmes quant aux données dites sensibles. En effet, dans certains cas, le broker se trouvant au centre des transactions entre clients/fournisseurs, il est nécessaire que les échanges de données passent par lui. Celui-ci peut même aller jusqu'à en garder une copie. Une nouvelle fois, c'est une question de confiance et de sécurité qui est mis en jeu ici.

Bref, comme nous pouvons le constater, l'univers du cloud broker n'est pas non plus tout rose. Comme toute collaboration, celle-ci comporte des aspects positifs et des aspects moins agréables. Tout est une question de choix et d'arbitrage : c'est au client de peser le pour et le contre !

6. Conclusion

A l'image du cloud computing, le cloud broker s'avère plein de richesses et de ressources. A travers les différentes parties de ce deuxième chapitre, à savoir les définitions, le principe général au sein duquel le cloud broker s'inscrit et son architecture, nous avons pu faire connaissance avec cet intermédiaire assez hors du commun. En effet, face à la complexité du cloud computing et à l'essor qu'il connait, c'est un réel « nouveau métier » qui a fait son apparition dans le but de faciliter la tâche à chaque protagoniste désirant œuvrer au quotidien avec un cloud. Mieux connaitre l'architecture précise du broker nous a permis de déceler toutes les facettes qu'il peut revêtir. Il est assez aisé à ce stade d'imaginer alors toutes les possibilités que ce phénomène nous offre.

Résumons alors rapidement la situation : le cloud computing a su montrer toute sa complexité tout au long du premier chapitre. Face au scepticisme de certains, le cloud broker fit son apparition, que l'on peut considérer comme un nouvel acteur de valeur facilitant les interactions « client-fournisseur ». Néanmoins, il faut savoir regarder un peu plus loin que le bout de son nez et anticiper les choses pour pouvoir mieux les maitriser. Le cloud computing, en prenant de l'ampleur, se complexifie. Ceci engendre le fait qu'il y ait de plus en plus de demandes et d'offres, les clients et les fournisseurs étant noyés dans une tonne d'informations à appréhender, à ingérer et tout autant de choix à faire. La solution du broker apparait presque comme une évidence ici… mais il y a également de fortes chances qu'à force, les consumer ne se retrouvent plus non plus face à tous ces brokers. Non seulement ils ne sauront plus quel fournisseur appeler, mais ils ne sauront plus vers quel broker se tourner. Comme pour beaucoup de choses, lorsque nous pensons solutionner un problème, cette « solution » dévoile à son tour bien des complications… C'est donc dans cette optique qu'est née l'idée de tenter de créer une typologie des brokers.

Chapitre 3 : Cloud Broker : Essai d'une typologie

1. Introduction

Comme ce fut exprimé dans le chapitre précédent, il n'est pas aisé pour un client de faire son choix parmi la variété de cloud broker présents sur le marché, même si choisir un broker est probablement plus simple que de trouver un fournisseur soi-même. De multiples questions peuvent alors jaillir dans l'esprit du client : comment choisir le cloud broker qui me conviendra ? Sont-ils tous équivalents sur le marché ? Ou revêtent-ils chacun leurs propres « spécialités » ?

En réponse à ces questionnements, et dans une optique de soutien aux clients souhaitant opter pour le cloud computing via un cloud broker, ce chapitre consiste en la création d'une typologie classifiant différentes sortes de brokers. Pour ce faire, un listing rapide des attentes des clients sera effectué, reprenant les demandes centrales qui pourraient être formulées par ceux-ci. Nous explorerons alors les différents composants permettant au broker de répondre à ces attentes. S'ensuivra l'essai de typologie à proprement parlé. Finalement, désirant refléter au mieux la réalité, certaines limites liées à cette typologie seront abordées.

2. Pourquoi créer une typologie?

Comme ce fut expliqué tout au long de ce mémoire, le contexte autour du cloud computing est assez nébuleux. De ce fait, le monde des cloud broker peut également vite devenir flou pour le client.

Afin de détailler l'architecture du cloud broker, nous avions mis en évidence trois sortes de grands services (intermediation, aggregation et arbitrage). Ainsi, un cloud broker peut proposer au client un service unique construit sur base de plusieurs services offerts par les fournisseurs, il peut également offrir une plus-value à ce service en lui rajoutant un élément personnalisé ou encore prendre le parti de laisser la possibilité au client de choisir entre des services similaires. Vu sous cet angle, nous pouvons imaginer toutes les possibilités s'ouvrant aux clients. Or, le but d'un broker est de faciliter les interactions entre les consommateurs et les fournisseurs et non pas d'y rajouter de la complexité. Pour cette raison, l'idée de créer une typologie est née. En effet, classifier les différents brokers selon des critères bien précis permettrait au client de cibler ses demandes directement, de pouvoir être guidé lorsque le moment arrive de choisir un broker.

3. Construction de la typologie

3.1. Démarche

Tout le chemin parcouru jusqu'à présent peut nous amener à un certain nombre de constats :

- Le cloud offre de nombreux avantages aux clients mais supporte également son lot d'inconvénients ;
- Des solutions techniques peuvent être trouvées afin de tenter de pallier à ces inconvénients ;
- Une solution humaine existe également : le cloud broker ;
- Le cloud broker, lorsque les clients l'ont choisi, est l'interlocuteur particulier des clients et des fournisseurs ;
- Les clients délèguent alors un certain pouvoir au broker mais sont également en droit de nourrir certaines attentes par rapport au cloud et donc envers ce broker.

Afin de pouvoir créer cette typologie, il a donc d'abord été nécessaire de retracer les différentes attentes que les clients peuvent nourrir pour le cloud computing. Une fois ces différentes attentes mises en évidence, il a fallu retrouver les composants du broker pouvant répondre à ses besoins. Une fois ces besoins et ces composants récoltés, il a été possible de recouper les informations et de les répertorier. Pour cela, la mise en commun de certains composants était nécessaire afin de pouvoir garantir une réponse adéquate au besoin du client.

Le résultat est le suivant : les composants du broker sont regroupés et classifiés afin de former des packages pouvant répondre spécifiquement aux besoins éventuels des clients.

3.2. Attentes éventuelles des clients

En se glissant dans la peau d'un client désirant opter pour une solution de cloud via un broker et en passant en revue tous les éléments exposés jusqu'ici dans ce mémoire, nous pouvons lister une série de besoins éventuels qui pourraient être rencontrés par un client. Le but ici est de relever quelques critères pouvant apparaitre comme primordiaux aux clients optant pour le cloud. Néanmoins, cette liste n'est pas exhaustive et pourrait évoluer au cours du temps.

Pour commencer, le client pourrait probablement souhaiter que son service ne soit pas victime des attaques malveillantes extérieures.

Deuxièmement, le client est en droit de souhaiter un système qui s'adapte suivant la demande de calcul ou de stockage. Il faut qu'il puisse répondre à la demande même si l'application subit une sollicitation forte de manière soudaine.

Ensuite, il serait tout à fait envisageable que le client ressente le besoin de bénéficier d'un backup de ses données au cas où un problème surviendrait (perte de données, corruption, …)

Une attente importante pourrait être d'avoir une sélection des fournisseurs plus rigoureuse qu'à la normale.

A l'heure où la crise fait rage, un point non négligeable pouvant être désiré par le client est la réduction de ses frais.

Enfin, un client pourrait souhaiter voir son service fonctionner constamment, ne connaissant jamais de panne ni de temps d'arrêt.

3.2.1. Sécurité

Comme ce fut expliqué à plusieurs reprises, la sécurité constitue la pierre d'achoppement du cloud computing. Il n'est donc pas étonnant que ce soit une des attentes majeures par rapport au cloud broker. Les clients ont besoin de garanties, d'être rassurés et de savoir que leurs données sont en lieux sûrs.

L'Institut de recherche Ponemon a réalisé un sondage parmi différentes grandes entreprises mondiales. Selon cette étude, les problèmes de sécurité viennent avant tout d'un fossé existant entre les fournisseurs qui placent la responsabilité de la sécurité chez les clients et les clients qui pensent qu'ils n'ont pas besoin de s'inquiéter pour celle-ci. (Institute, 2011, p. 3) C'est réellement un danger qui découle de la dépendance du client au fournisseur, lui conférant certains pouvoirs tout en oubliant ses responsabilités.

Une autre problématique concernant la sécurité est pointée du doigt par Robert Lemos de Dark Reading dans son rapport «Cloud Brokers Seek To Simplify, Secure Services». (Lemos, 2012) Voici ce qu'il met en évidence : chaque fournisseur de service propose sa propre gestion des identités, des contrôles et des mots de passe. Cela peut donc vite devenir chaotique pour le client qui doit tenter de s'y retrouver parmi ces différentes méthodes. Le cloud broker peut alors gérer ces différentes manières de procéder afin que ça paraisse plus limpide au client.

Comme expliqué précédemment, un broker peut également apporter une plus-value au service initial, en l'occurrence ici une couche supplémentaire de sécurité. Cette initiative prise par le broker afin d'améliorer la sécurité peut être un élément permettant de combler ce manque de confiance ressenti actuellement par les entreprises envers le monde du cloud computing. (Lemos, 2012)

3.2.2. Scalability

Comme expliqué au premier chapitre, la scalability est un bénéfice prisé par les clients optant pour le cloud computing. En effet, la scalability horizontale permet d'améliorer l'efficacité du système : il supportera mieux une montée en charge, par exemple, grâce à l'apport de puissance supplémentaire fournie ici par d'autres fournisseurs de cloud. (Institute, 2011, p. 3)

3.2.3. Sélection

J'ai déjà mis en avant le fait que d'innombrables possibilités s'offrent aux clients grâce au cloud computing. Sélectionner un fournisseur peut alors devenir extrêmement compliqué : pourquoi choisir celui-là plutôt qu'un autre ? Sur quels critères ? Le cloud broker peut alors entrer en scène et aider le client à faire ce choix. En effet, c'est souvent la raison principale pour laquelle un client accepte d'adopter un broker. Cette sélection et la flexibilité dans le choix d'un fournisseur de service est d'ailleurs mis en avant comme étant un critère primordial pour le client dans l'étude de Ponemon. (Institute, 2011, p. 3) La sélection dans ce cas est donc un rôle qui incombe au cloud broker. Cette tâche ne doit pas être sous-estimée par le broker car de cette sélection dépendra le pourcentage de résistance à la charge d'un service, la disponibilité de celui-ci ou encore la performance du cloud.

3.2.4. Backup

Dès le premier chapitre de ce mémoire, il fut mis en évidence la crainte des clients face à la perte de leurs données survenant à la suite d'un crash disque ou d'une attaque malveillante. Le backup, pour toute personne s'y connaissait un tant soit peu en informatique, est une démarche primordiale que ce soit pour les petites ou grandes entreprises. Ces pertes de données peuvent être limitées, voire évitées, grâce à un backup réalisé efficacement. Lorsque le client opte pour l'aide d'un cloud broker, ses données peuvent transiter par lui avant de rejoindre le service chez le fournisseur.

3.2.5. Economie

Annoncé comme l'élément prédominant par Ponemon, le gain engendré par la réduction des coûts est certainement un des facteurs les plus importants dans le choix d'un broker. (Institute, 2011, p. 3)

Il a déjà été vu précédemment que le cloud computing permettait le paiement des services suivant la demande. Le broker peut jouer un rôle afin de veiller à cette diminution du coût des services. Celui-ci peut sélectionner le service le moins cher parmi les différents fournisseurs en jouant sur le principe de concurrence mais aussi offrir aux utilisateurs des outils permettant la consultation de la consommation et de l'utilisation des différents services.

3.2.6. Disponibilité

Un autre élément qu'un client pourrait demander à son broker est de lui fournir des services qui ne soient jamais (ou très peu) indisponibles. Le risque d'indisponibilité pouvant se présenter du coté du fournisseur ou du coté du broker, le broker doit mettre tout en place afin d'éviter que cet événement se produise. Certains clients ne pouvant pas se permettre de grandes périodes de chômage technique.

3.3. Composants du cloud broker

Les différents composants du broker exposés au deuxième chapitre permettent au broker de tenter de satisfaire les attentes des clients. Détaillons maintenant quels sont les composants qui pourraient jouer un rôle prépondérant dans la sécurité, la scalability, la sélection, le backup, l'économie et la disponibilité.

3.3.1. Sécurité

Pour qu'un broker puisse proposer une gestion de la sécurité, il est nécessaire pour celui-ci de mettre en place certains composants tels que la gestion des identités permettant l'identification des utilisateurs ainsi que les services auxquels ce dernier a le droit d'accéder. Il y a également des composants tels que le « SLA Monitoring » qui permet de vérifier que les conditions de sécurité sont respectées, le firewall qui protège le système des intrusions, une gestion des risques pour évaluer la possibilité qu'un risque surgisse ainsi que la façon dont gérer ce risque et enfin, un composant pouvant s'occuper de la gestion du réseau.

3.3.2. Scalability

Le broker souhaitant offrir le principe de scalability devra se munir de composants tels que le « Staging/Pooling Service » qui permettra de proposer un catalogue de services pouvant venir en aide au système actuel quand cela sera nécessaire. Mais aussi un composant permettant la gestion du choix du fournisseur se trouvant dans le pooling. Il est également intéressant de pouvoir ajouter une gestion des risques, ceci permettra d'évaluer les possibilités qu'une montée de la charge se produise. Enfin, une gestion du réseau permettant la surveillance du trafic au sein du système permettra d'avertir directement lors d'un pic de demande de ressource.

3.3.3. Sélection

Selon l'article présenté par « Internal Journal of Multidisciplinary Sciences and Engineering», un broker pourrait gérer la sélection en gardant dans une base de données propre au broker les différentes informations relatives aux services proposés par les fournisseurs (service demandé, la distance pour atteindre les fournisseurs, tarification…) Ces informations permettront alors au broker d'effectuer son choix de sélection lorsqu'une requête de demande de service se présentera. (Rabia Khan, 2012)

Le composant « Capability Management and Matching » prendra le rôle de l'agent effectuant le choix. Le composant « Staging/Pooling service » fournira le pool de provider pouvant répondre à la requête. Enfin, le composant « SLA Management » permettra la gestion des différents accords avec les fournisseurs.

3.3.4. Backup

Le broker qui souhaite mettre en place une solution de backup doit s'équiper de composants tels que « l'Audit » afin de s'assurer de la conformité des informations transitant sur le réseau, d'une gestion des risques permettant d'évaluer la possibilité qu'une perte des données se produise et d'un système permettant de gérer les solutions à prendre au cas où celles-ci se produiraient. Et enfin d'une surveillance de l'état du réseau et de la plate-forme afin de permettre la découverte d'anomalies.

3.3.5. Economie

Les composants que le broker devra mettre en place pour permettre la diminution des coûts sont le composant « Staging and Pooling Service », permettant de disposer d'un panel de fournisseurs différents et le composant « Capability Management and Matching » qui permettra de choisir parmi les services les plus intéressants pour le client. Le composant «Usage Monitoring » permettra, quant à lui, la surveillance de la consommation et de l'utilisation des services.

3.3.6. Disponibilité

Pour garantir cette mission, le broker doit donc pouvoir proposer des services équivalents chez d'autre fournisseurs en cas de problème, prendre les décisions afin de changer de fournisseur si cela s'avérerait nécessaire, gérer les risques qu'un service soit indisponible et agir en conséquence si cela se produisait, vérifier l'état du réseau et enfin permettre la gestion des SLA.

Le tableau suivant reprend les différents types de services qu'un broker peut offrir ainsi que les composants qui seraient présents au sein de l'architecture du broker.

	Sécurité	Scalability	Sélection	Backup	Economie	Disponibilité
API	✓	✓	✓	✓	✓	✓
Deployment service	✓	✓	✓	✓	✓	✓
Staging/pooling Service		✓	✓		✓	✓
IAM	✓					
SLA Monitoring	✓			✓		✓
Capability Management and Matching		✓	✓		✓	✓
Audit				✓		
Gateway/Application firewalls	✓					
Risk Management	✓	✓		✓		✓
Network/Platform security	✓	✓		✓		✓
Usage Monitoring					✓	
SLA Management		✓	✓			✓

4. Typologie

Ici, je propose une classification des brokers suivant le type de prestation qu'ils pourraient fournir, en fonction de la demande précise des clients.

4.1. Safe Broker

Safe Broker

Architecture :

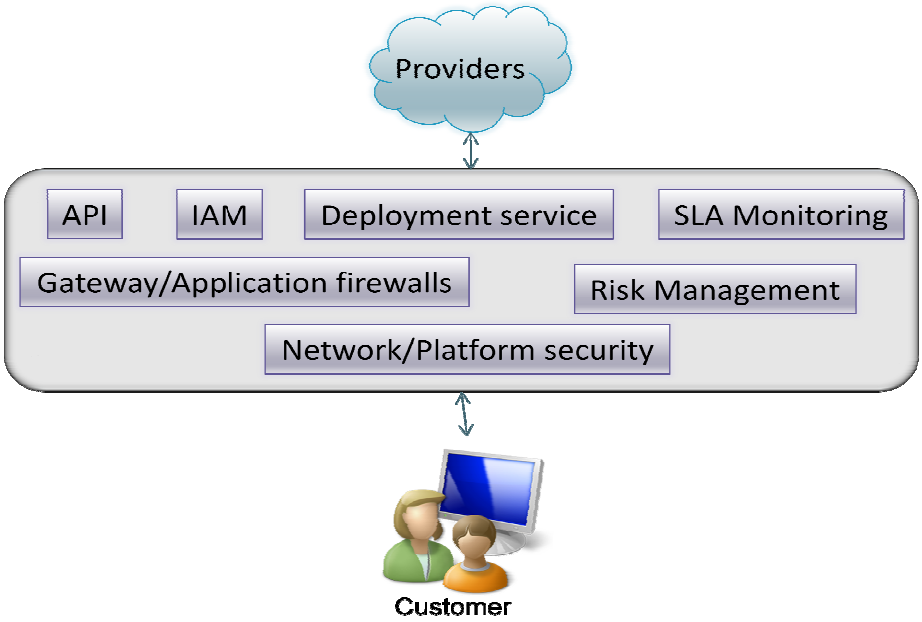

Figure 18: Architecture d'un Safe Broker

Composants :

API
Deployment service
IAM
SLA Monitoring
Gateway/Application firewalls
Risk Management
Network/Platform security

Fonctionnalités :

Grâce à la mise en place de ces différents composants, le broker peut proposer des services axés sur la sécurité. Cela peut aller de la gestion des identités ainsi que des permissions d'accès aux services à la gestion de l'infrastructure du réseau en passant par la mise en place de firewalls pour protéger des intrusions, de technique de gestion des risques mais aussi de monitoring des SLA.

4.2. Scalability Broker

Scalability Broker

Architecture :

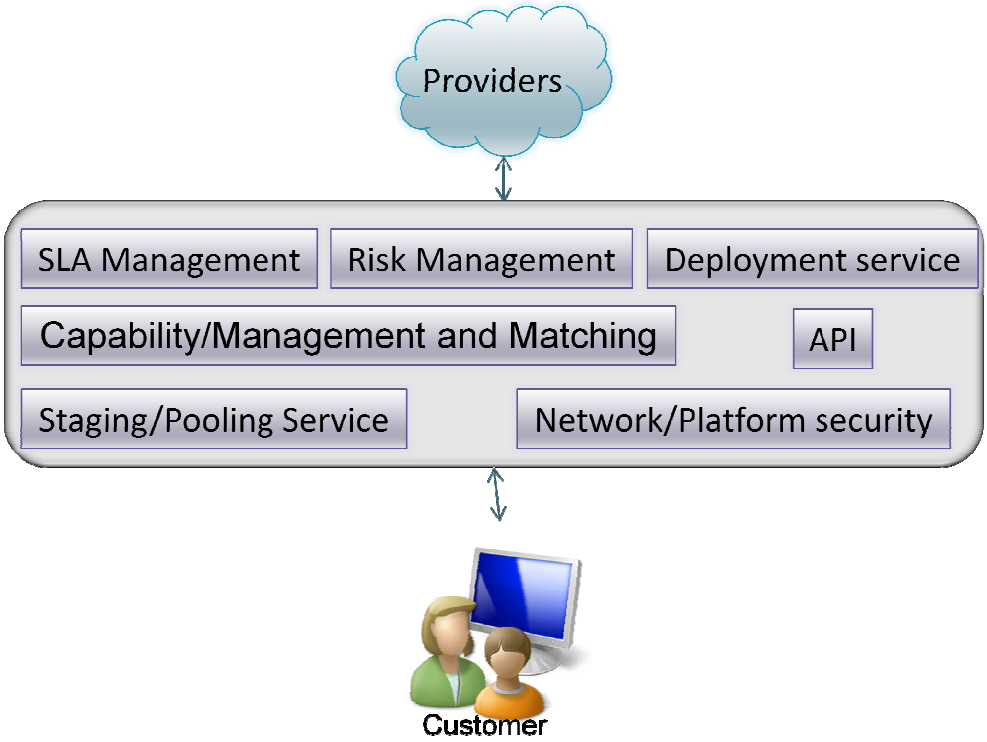

Figure 19: Architecture d'un Scalability Broker

Composants :

API
Deployment service
Staging/pooling Service
Capability Management and Matching
Risk Management
Network/Platform security
SLA Management

Fonctionnalités :

Cette architecture a pour but de proposer un service permettant la scalability des services, c'est-à-dire que les composants qui seront utilisés au sein de cette infrastructure permettront de surveiller l'état du réseau et des demandes sur les applications et de répondre en fonction de cette demande. Il sera donc nécessaire de pouvoir surveiller l'état du réseau, de prendre la décision de choisir un fournisseur permettant de supporter la montée en charge, d'opter pour un composant permettant le référencement des différents fournisseurs et enfin d'effectuer une étude des risques.

4.3. Selection Broker

Selection Broker

Architecture :

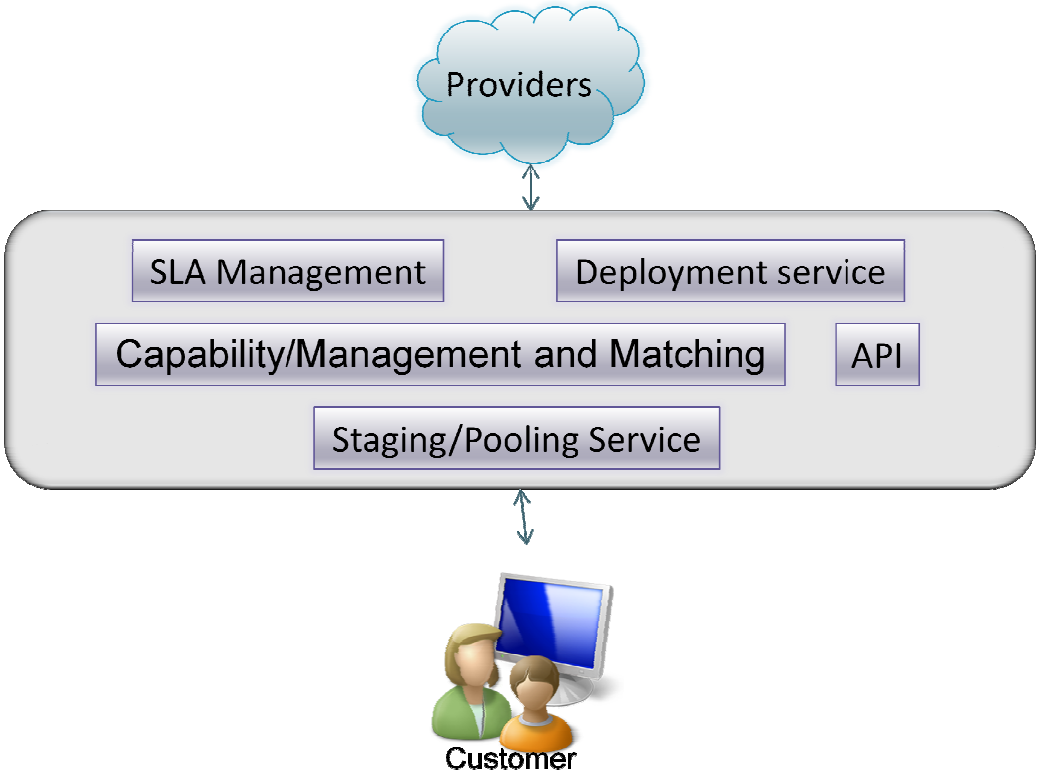

Figure 20: Architecture d'un Selection Broker

Composants :

API
Deployment service
Staging/pooling Service
Capability Management and Matching
SLA Management

Fonctionnalités :

Le package permettant de faire la sélection du broker doit pouvoir fournir les composants permettant de faire la gestion et le choix des fournisseurs, les API permettant de communiquer avec les services et l'annuaire permettant de retenir les différents fournisseurs présents.

4.4. Backup Broker

Backup Broker

Architecture :

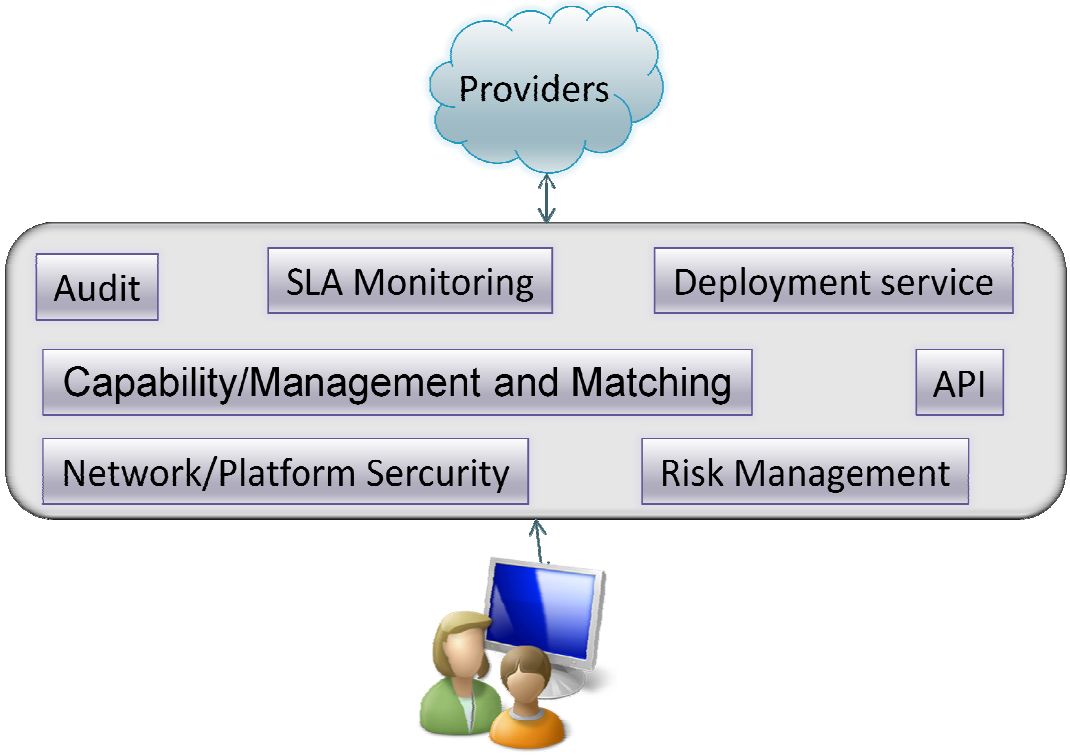

Figure 21: Architecture d'un Backup Broker

Composants :

API
Deployment service
SLA Monitoring
Capability Management and Matching
Audit
Risk Management
Network/Platform security

Fonctionnalités :

La mise en place des composants tels que l'audit, la management and matching, la sécurié du réseau ou encore l'étude des risques permet de fournir des solutions de backup dans les services. Les composants permettront de récupérer les données des clients en cas de problème.

4.5. Cheap Broker

Architecture :

Composants :

API
Deployment service
Staging/pooling Service
Capability Management and M
Usage Monitoring

Fonctionnalités :

Pour que le client puisse faire
moins chers pour le client. En u
différents fournisseurs, l'annuair
broker pourrap

4.6. Avaibility Broker

Avaibility Broker

Architecture :

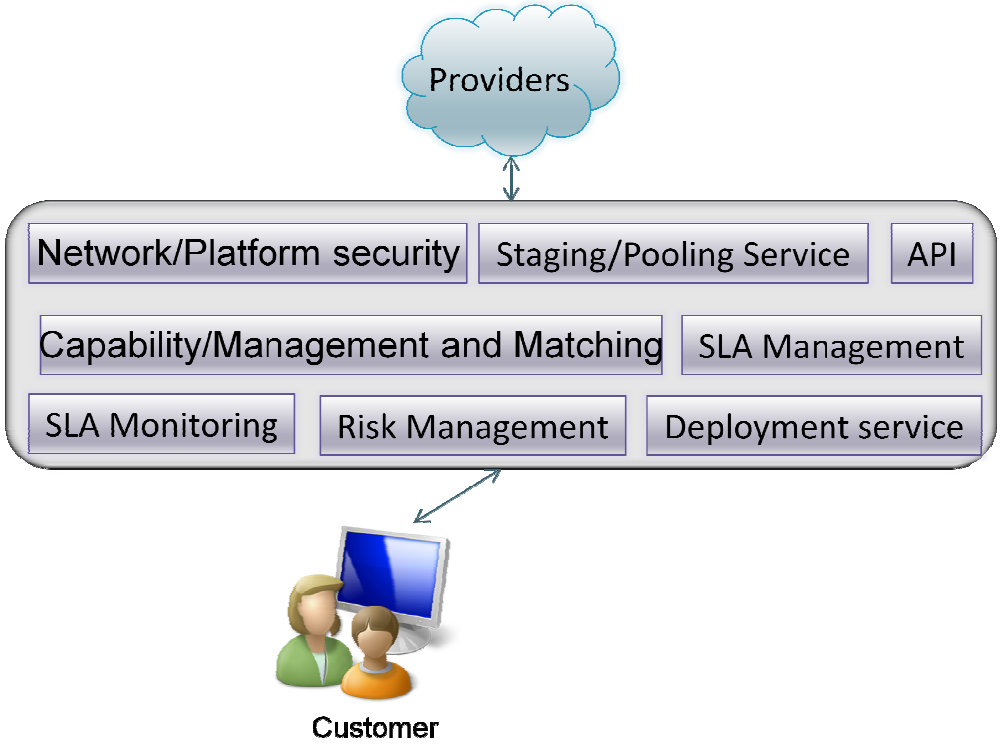

Figure 23: Architecture d'un Avaibility Broker

Composants :

API
Deployment service
Staging/pooling Service
SLA Monitoring
Capability Management and Matching
Risk Management
Network/Platform security
SLA Management

Fonctionnalités :

Ici, le broker doit pouvoir garantir la disponibilité d'un service suivant ce qui est décrit dans le SLA. Pour ce faire, il est nécessaire de disposer d'un composant permettant la surveillance des règles SLA mais aussi d'éléments permettant les choix de services, la gestion de sécurité du réseau et l'étude des risques.

5. Limites de la typologie

Pour le client comme pour le broker, une typologie n'est pas infaillible et peut aussi montrer des limites. En effet, plus nous allons « zoomer » et vouloir compartimenter, plus nous allons y perdre en généralité.

Du côté du client, cette typologie pourrait finalement le mettre à mal. S'il n'a pas une demande précise (ou plusieurs demandes différentes), ça peut s'avérer compliqué pour lui de faire son choix parmi les catégories. De plus, si de nouveaux composants et de nouvelles fonctionnalités font leur apparition sur le marché, celles-ci ne seront pas mises en place instantanément dans la typologie et un décalage peut apparaitre entre demande et offre.

Du côté du cloud broker, cette typologie peut ne pas virer à son avantage. En effet, chaque broker ne bénéficiera plus du monopole de l'ensemble du marché mais sera bien classifié dans une catégorie spécifique. Il peut en découler le fait que moins de clients feront appel à ses services, sa spécificité étant moins « populaire » que les autres. De plus, ce système risque d'amplifier la concurrence déjà présente : le broker sera confronté directement à ses concurrents les plus directs en permettant aux clients une comparaison plus aisée.

Conclusion

Le cloud computing apporte de multiples avantages qui ne seront pas rappelés ici mais apporte également son lot d'inconvénients. Lorsqu'un client opte pour l'utilisation d'un cloud, il a toujours certaines attentes par rapport à ce que ce dernier pourrait lui fournir. En effet, selon ses besoins, le client sera plus dans l'attente de certains services particuliers. J'en ai répertorié 6 principaux : la sécurité, la scalability, la sélection, le backup, l'économie et la disponibilité. Néanmoins, il est difficile d'en procurer une liste exhaustive, les attentes des clients mouvant sans cesse selon les « effets de mode », les besoins à un moment particulier, les nouveautés, …

Une explication plus approfondie quant au choix de la typologie et à son élaboration s'imposait, permettant de comprendre le cheminement qui a conduit à cet essai. Il convient alors d'en tirer les conclusions suivantes : cette typologie permet avant tout au client de s'y retrouver, de savoir où et qui chercher et donc, en gros, de ne plus chercher « à l'aveugle ». Le cloud broker, de son côté, gagne en spécificité.

Néanmoins, certaines limites ont été nommées. En effet, comme c'est souvent le cas, un avantage peut rapidement basculer dans le côté des inconvénients. Cette spécification accrue pourrait engendrer des difficultés pour le client de trouver un cloud broker pouvant lui fournir tous les services dont il a besoin. Du côté du cloud broker, il a plutôt intérêt à avoir misé sur la (les) bonne(s) « catégorie(s)» s'il veut continuer à être sollicité par les clients.

Cependant, cette typologie n'est pas arrêtée et demande une certaine souplesse en fonction des demandes des clients. Il ne faut donc pas l'envisager comme une classification fixe mais plutôt comme un classement en perpétuelle évolution.

Conclusion

Nous voilà à la fin du mémoire et une dernière vue d'ensemble s'impose…

Au commencement du chapitre 1, nous ne savions pas du tout vers quoi nous nous dirigions. En effet, ça commençait fort : le cloud computing n'étant pas strictement balisé, chacun pouvait y aller de sa propre interprétation. Or, au fur et à mesure de ce chapitre, nous avons pu nous rendre compte que le cloud computing revêt certaines particularités que nous ne pouvons retrouver dans d'autres services. Le but de ce chapitre était de faire connaissance avec le cloud computing, d'en comprendre les bases. Rapidement, nous avons pu constater des avis très divergents sur le sujet : certains prônent les côtés « magiques » de cette technologie alors que d'autres la considèrent comme ingérable et à éviter. Les extrêmes sont à prendre avec des pincettes, c'est pour cette raison que j'ai tenté d'introduire de nombreuses nuances afin de permettre à chacun de se faire sa propre opinion..

Ensuite, les risques liés au cloud et les difficultés de s'y retrouver pour les clients nous ont amené au concept de « cloud broker », fil conducteur du chapitre 2. Il semblait évident ici de suivre la même trame que pour le premier chapitre, partant du principe que pour comprendre un concept, il faut d'abord avoir une idée de sa signification et de son fonctionnement. C'est seulement à partir de ce moment que l'on peut aborder les bénéfices et limites liés également au cloud broker, qui ne constitue nullement une « solution miracle ». Cependant, certains avantages intéressants ont jailli, ce qui m'a donné l'envie d'aller encore plus loin, à savoir un essai de typologie des brokers.

Le chapitre 3 fut alors consacré à cet essai, basé sur des attentes des clients et donc en respectant cette logique de conduite qui consiste à trouver des solutions pour que les clients puissent bénéficier du cloud tout en s'y retrouvant un peu plus. Comme j'ai également pu l'expliquer, cette typologie n'est pas non plus une « solution miracle » mais ajoute une corde à l'arc du client, lui offre un support en plus avant qu'il aille faire ses propres armes s'il opte pour le cloud.

Le but de ce mémoire était réellement de se familiariser avec les principes de cloud computing et de cloud broker, me permettant de cette manière de créer une typologie basée sur les brokers. Je voulais créer une vue d'ensemble permettant à chacun de faire sa propre idée et offrant à chacun l'opportunité de se positionner par rapport à tous ces concepts: soit le désir de s'en arrêter là, soit l'envie d'aller découvrir ce qui se cache plus loin…

Bibliographie

Accenture. (2011, 11 9). *Accenture lance une solution de cloud privé dédiée au support des applications SAP.* Consulté le 11 27, 2012, sur Accenture: http://www.accenture.com/fr-fr/company/newsroom-france/Pages/private-cloud-solution-dedicated-sap-application-support.aspx

Armbrust, M. (2010). A View of Cloud Computing. *Communications of the ACM* , 50-58.

Brunetière, A. (2011). *Les enjeux du cloud computing*. Consulté le 05 12, 2013, sur Sage: http://www.sage.fr/fr/mediatheque/dossiers-d-experts/enjeux-du-cloud-computing

Carrel-Billiard, M. (2011). *Sentiment sur le cloud*. Consulté le 02 10, 2013, sur ItPro: http://www.itpro.fr/n/plus-de-600-cadres-donnent-leur-sentiment-sur-le-cloud-5105/

Cheminat, J. (2012, 07 02). *Les utilisateurs du Cloud d'Amazon victimes de pannes d'électricité.* Consulté le 05 12, 2013, sur reseaux-telecoms: http://www.reseaux-telecoms.net/actualites/lire-les-utilisateurs-du-cloud-d-amazon-victimes-de-pannes-d-electricite-24321.html

Cigref. (2013). *Fondamentaux du Cloud Computing.*

CIGREF. (2013). *Fondamentaux du Cloud Computing: le point de vue des grandes entreprises.* Paris.

CloudWatt. (2013). *Cloud public, privé et hybride : quelles différences?* Consulté le 07 22, 2013, sur CloudWatt: https://www.cloudwatt.com/questions/cloud-public-prive-hybride-difference

cordys. (2013, 03). *Cordys for Cloud Brokers*. Consulté le 06 10, 2013, sur cordys: http://www.cordys.com/cordys-for-cloud-brokers

Czernicki, B. (2011, 02 27). *Exemples de SaaS, Paas et Iaas*. Consulté le 06 10, 2013, sur Silverlighthack: http://www.silverlighthack.com/post/2011/02/27/IaaS-PaaS-and-SaaS-Terms-Explained-and-Defined.aspx

Dailly, M. (2008, 09 30). *Cloud computing: Richard Stallman, Larry Ellison insurgent*. Consulté le 05 2013, sur Clubic: http://www.clubic.com/actualite-166094-cloud-computing-richard-stallman-larry-ellison-insurgent.html

Dartyge, F. (2011, 01 01). *10 inconvénients du cloud computing pour les PME*. Consulté le 05 2013, sur Blog PME: http://www.blogpme.fr/10-inconvenients-du-cloud-computing-pour-les-pme/

Dasriaux, N. (2010, 11 03). *Scalabilité, le choix des armes* . Consulté le 06 2013, sur Neoxia: http://blog.neoxia.com/scalabilite-choix-des-armes/

Derest, V. (2009). Cloud Computing : les bonnes pratiques. *Reseax-telecoms* , 2.

Direccte. (2012, 09). le cloud computing une nouvelle filière fortement structurante. *Etudes sectorielles* .

ebizQ. (2010, 01 19). *How Different is Cloud Computing from Virtualization, and How Similar Are They?* Consulté le 05 2013, sur ebizQ: http://www.ebizq.net/blogs/ebizq_forum/2010/01/how-different-is-cloud-computing-from-virtualization-and-how-similar-are-they.php

Emmanuel Marilly, O. M. (2002). SERVICE LEVEL AGREEMENTS:A MAIN CHALLENGE for Next Generation Networks. *10.1109/ECUMN.2002.1002118* .

ENISA. (2009). *Cloud computing. Benefits, risks and recommendations for information security.* Daniele Catteddu and Giles Hogben.

Fang Liu, J. T. (2011, 09). NIST Cloud Computing Reference Architecture. *Recommendations of the National Institute of Standards and Technology* , p. 8.

Fang Liu, J. T. (2011, 09). NIST Cloud Computing Reference Architecture. *Recommendations of the National Institute of Standards and Technology* , p. 8.

Fang Liu, J. T. (2011, 09). NIST Cloud Computing Reference Architecture. *Recommendations of the National Institute of Standards and Technology* , p. 1.

Forrester. (2013). *CLOUD COMPUTING*. Consulté le 06 17, 2013, sur Forrester: http://www.forrester.com/Cloud-Computing

Gartner. (2013). *Cloud Computing*. Consulté le 06 17, 2O13, sur gartner: http://www.gartner.com/it-glossary/cloud-computing/

informatique, A. (2011). *Virtualisation et cloud computing*. Consulté le 06 17, 2013, sur Aims informatique: http://www.aims-informatique.com/pour-en-savoir-plus/virtualisation-et-cloud-computing.html

informatique, R. (s.d.). *La virtualisation, qu'est-ce que c'est ?* Consulté le 07 22, 2013, sur Reseau informatique: http://reseau-informatique.prestataires.com/conseils/virtualisation

Institute, P. (2011). *Security of Cloud Computing Providers Study.* Ponemon Institute.

International, M. (2010, 05 05). *Cloud computing : l'évolution soutenue des usages*. Consulté le 05 10, 2013, sur finyear: http://www.finyear.com/Cloud-computing-l-evolution-soutenue-des-usages-depuis-2008-ouvre-a-de-nouvelles-perspectives-d-ici-2012_a14492.html

Iso. (2008, 10 15). *ISO/IEC 27001:2005*. Consulté le 05 10, 2013, sur Iso: http://www.iso.org/iso/fr/catalogue_detail?csnumber=42103

Jason. (2012, 03 19). *From Cloudy to Clear*. Consulté le 07 22, 2013, sur onthenetoffice: http://www.onthenetoffice.com/blog/2012/03/cloud_terms_3/

Jefferson, B. (2009, 07 15). Cloud Computing : les bonnes pratiques. (V. Derest, Intervieweur)

Jin, S. (2011, 01 03). *Cloud Architecture Patterns: Cloud Broker*. Consulté le 06 17, 2013, sur VMware: http://blogs.vmware.com/vcloud/2011/01/cloud-architecture-patterns-cloud-broker.html

Joset, P. (2011). Cloud computing, tentative de définition. *Abissa Informatique* , p. 1.

Lambel, F. (2008, 07 17). *Les 7 risques du cloud computing*. Consulté le 05 12, 2013, sur Direction informatique: http://www.directioninformatique.com/les-7-risques-du-cloud-computing-2/9353

Lauchlan, S. (2012, 07 24). *businesscloud9*. Consulté le 06 17, 2013, sur US government explores Cloud Broker concept for public sector: http://www.businesscloud9.com/content/us-government-explores-cloud-broker-concept-public-sector/11226

Lauchlan, S. (2012, 07 24). *US government explores Cloud Broker concept for public sector*. Consulté le 08 07, 2013, sur businesscloud9: http://www.businesscloud9.com/content/us-government-explores-cloud-broker-concept-public-sector/11226

Lemos, R. (2012). Cloud Brokers Seek To Simplify, Secure Services . *Dark Reading* .

Lévy-Abégnoli, T. (2008, 03 03). *Cloud Computing : vers la dématérialisation des salles informatiques*. Consulté le 05 12, 2013, sur Zdnet: http://www.zdnet.fr/actualites/cloud-computing-vers-la-dematerialisation-des-salles-informatiques-39381489.htm

lexicon. (s.d.). *two-sided markets*. Consulté le 05 13, 2013, sur lexicon: http://lexicon.ft.com/Term?term=two_sided-markets

Microprocesseur. (s.d.). *Limite de miniaturisation*. Consulté le 06 17, 2013, sur Microprocesseur: http://microprocesseur.over-blog.com/pages/Limite_de_miniaturisation-1096898.html

News, I. (2011, 01 31). *Cloud Computing : l'étude qui rassure*. Consulté le 05 22, 2013, sur Itr News: http://www.itrnews.com/articles/114631/cloud-computing-etude-rassure.html

NIST. (2013, 05 15). NIST Cloud Computing Security Reference Architecture. *NIST Special Publication 500-299* .

Perrenoud, J.-L. (2013, 03 28). L'informatique dans un nuage: le Cloud computing pour les nuls. *jlpi informatique* , p. 3.

Peter Mell, T. G. (2011, 09). The NIST Definition of Cloud . *Recommendations of the National Institute* , p. 2.

Pettey, C. (2010, 11 08). *Gartner Says Security Must Evolve as Organizations Move Beyond Virtualization to Private Cloud Infrastructures*. Consulté le 05 06, 2013, sur Gartner: http://www.gartner.com/newsroom/id/1464514

Pettey, C., & Meulen, R. v. (2009, 07 09). *Newsroom*. Consulté le 06 10, 2013, sur Gartner: http://www.gartner.com/newsroom/id/1064712

Poujol, M. (2010). *Le Cloud Computing en France.* PAC – EMC, Intel, VMware.

Rabia Khan, E. N. (2012, 09). User's Involvement in Cloud Selection Exercising Cloud Broker. *INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY SCIENCES AND ENGINEERING* , p. 1.

Rezzonico, V. (2009, 10 27). Editorial. *FLASH INFORMATIQUE* , p. 2.

Richard, P. (2009, 11 04). *L'agence européenne de la sécurité relève 35 risques liés au cloud*. Consulté le 05 10, 2013, sur 01Business: http://pro.01net.com/editorial/508894/lagence-europeenne-de-la-securite-releve-35-risques-lies-au-cloud/

Ried, S. (2011, 08 10). Cloud Broker — A New Business Model Paradigm. *For Vendor Strategy Professionals* , p. 2.

Rouse, M. (2011, 09). *cloud broker*. Consulté le 06 05, 2013, sur techtarget: http://searchcloudprovider.techtarget.com/definition/cloud-broker

Sampson, L. (2012, 05). *A cloud broker can be a cloud provider's best friend*. Consulté le 06 10, 2013, sur searchcloudprovider: http://searchcloudprovider.techtarget.com/feature/A-cloud-broker-can-be-a-cloud-providers-best-friend

Schauer, H. (2009, 11 24). L'agence européenne de la sécurité relève 35 risques liés au cloud. (P. Richard, Intervieweur)

Schulle, S. (2008, 12 1). *Demystifying The Cloud.* Consulté le 12 15, 2012, sur Saasblogs: http://www.saasblogs.com/saas/demystifying-the-cloud-where-do-saas-paas-and-other-acronyms-fit-in/

Solucom. (2010, 08). Cloud computing: comment en tirer parti? *les focus solucom* , p. 3.

Solucom. (2011, 03). les nouveaux modes d'externalisation: une remise en question des modèles? *Les synthèses Solucom* , p. 6.

Solucom. (2010, 03). Virtualisation et cloud computing: jusqu'où aller? *Les synthèses Solucom* , p. 9.

Sonia Boittin, D. G. (2010, 03). Virtualisation et cloud computing :jusqu'où aller ? *LES SYNTHÈSES SOLUCOM* .

Srijith K. Nair, S. P. (2010, 12). Towards Secure Cloud Bursting, Brokerage and Aggregation. *Paper presented at the IEEE European conference on Web Services* .

Thomas Eisenmann, G. P. (2006). Strategies for Two-Sided Markets. *Harvard Business Review* .

Tonic, F. (2010). Cloud computing et SLA. *Cloud Magazine* .

VMware. (2011). Virtualization overview. *VMware whithe paper* , p. 3.

Williams, D. M. (2010). *A quick start guide to Cloud computing.* Kogan Page.

Zedi, J. (2010, 11 18). *Comprendre le Cloud Computing : acteurs et enjeux*. Consulté le 05 2013, sur Clubic: http://pro.clubic.com/it-business/cloud-computing/article-376690-5-cloud-computing.html

Annexes

Annexe 1: Tableau de comparaison des couts dans le modèle SaaS

Tableau 6 : Comparaison des coûts entre le modèle SaaS et le modèle « Software »[23]

	Modèle SaaS	Modèle Software
Le prix du logiciel	L'utilisateur paye mensuellement, comme un abonnement téléphonique. Il a le droit d'utiliser le logiciel mais également à un certains nombre de services. Les mises à jour sont automatiques. Il paye à la quantité d'utilisateurs. Cela permet de lisser et d'optimiser les coûts. Cela évite d'acheter des licences en masse sans les utiliser.	L'utilisateur paye une fois et est propriétaire du logiciel. Mais il faut renouveler les licences tous les 2 à 3 ans pour toujours avoir la version à jour.
Le prix de la maintenance logicielle du parc utilisateur	Aucun déploiement n'est nécessaire. Tout se fait automatiquement et est compris dans l'abonnement.	Des mises à jour à faire sur chaque poste utilisateur ont un coût important en termes de licence ou de main d'œuvre.
Le prix de la maintenance logicielle du parc serveur	Idem	Idem, de plus une mise à jour peut entrainer une corruption ou une perte de données.
Le prix du parc des postes de travail	On peut utiliser les SaaS via des interfaces RIA[24] qui peuvent fonctionner avec des clients légers ou des notebooks. Ces interfaces consomment peu de puissance sur le poste de travail.	Les logiciels traditionnels fonctionnent la plupart du temps sur des PC gourmands en énergie et rapidement obsolètes.
Le prix du parc de serveurs	Tous ces arguments plaident pour le déport vers des spécialistes de l'exploitation de data centers. De plus, souvent, les entreprises n'utilisent qu'une petite partie de la capacité de leurs serveurs. Ainsi, 80% des frais partent en pure perte.	Le prix d'un parc de serveurs dédié coûte cher. Il faut au moins 2 centres de données entièrement équipées (badges de sécurité, groupe électrogène, climatisation, système d'injection de gaz inerte en cas d'incendie, etc) chacun géré par une équipe. La consommation électrique est le plus gros poste de dépense.
Synthèse	L'utilisation du modèle SaaS permet généralement la réduction du coût total par utilisateur. Il doit néanmoins être calculé au cas par cas. Il permet aux entreprises de se recentrer sur leur cœur de métier au lieu d'avoir à se soucier de problèmes informatiques. Il existe des sociétés spécialisées qui s'y connaissent beaucoup plus et qui leur permettront de faire des économies, tout en préservant la sécurité de leurs données.	

Annexe 2: Liste des 7 points capitaux selon Gartner

1-La qualité des superviseurs
Sous-traiter ses données les plus sensibles ne peut s'envisager que si on a la certitude que les informaticiens du sous-traitant sont dignes de confiance et que leurs faits et gestes sont contrôlés. Gartner recommande un droit de regard et de contrôle sur les personnels du fournisseur.

2-Conformités légales
En fin de compte, c'est le propriétaire des données qui est tenu responsable en cas d'infraction à la législation. Les fournisseurs de doivent se plier à toutes les demandes d'audit externes et disposer de toutes les certifications de sécurité nécessaires pour que leurs clients aient la certitude d'être couverts.

3-Localisation des données
L'utilisation de sites de stockage multiples fait partie des points forts de cette approche, mais aussi de ses points faibles. En effet, la dématérialisation touche à ses limites lorsqu'on s'intéresse au lieu où se trouve implanté un site de stockage. Les données qu'il contient relèvent alors du régime juridique local. Autant savoir sous lequel peuvent se trouver ses données.

4-Isolement des données
Par définition, le cloud computing rime avec partage des ressources. Cela engendre une menace sur la confidentialité des données. Il faut s'assurer de leur cryptage correct et qu'il est possible de les isoler. Ce point est crucial. Un cryptage qui ne respecte pas les règles de l'art peut déboucher sur une perte irréversible.

5-Récupération
Ignorer où se trouvent ses données ne veut pas dire que l'on ne puisse pas avoir l'assurance des moyens mis en place pour leur sauvegarde en cas de problème majeur. La réplication sur plusieurs sites distants est un impératif. Une restauration complète dans des délais contractuels l'est aussi.

6-Collaboration avec la justice
Une architecture en cloud computing ne doit pas empêcher de répondre aux injonctions de la justice, que ce soit pour des raisons fiscales ou d'autres d'ordre juridique. La traçabilité de l'accès aux données, en particulier, peut être une gageure pour le fournisseur. Un accord contractuel voire, dans l'idéal, la démonstration qu'il a été répondu facilement aux demandes lors d'une précédente enquête, s'imposent.

7-Viabilité à long terme
Le fournisseur idéal ne défaille jamais et gagne suffisamment bien sa vie pour, d'une part, ne pas déposer le bilan et, d'autre part, ne pas devenir une cible et être absorbé. Quoi qu'il en soit, les données de ses clients doivent traverser ces éventuels aléas sans en être affectées et, surtout, pouvoir être restituées. La description précise de cette restitution (conditions, délais, formats) doit figurer dans le contrat originel. Après, il sera trop tard.

Annexe 3: Cloud Business Model selon Ried

• **Cloud builder.** Although this may not seem obvious, consulting models also exist in the cloud. The cloud builder helps enterprises establish the required technology and business strategy needed to build a private cloud. For example, IT service providers like Capgemini, CSC, HP, and IBM maintain blueprint road maps and playbooks for building private cloud infrastructures. Some cloud builders even address local cloud providers, which use these consulting services to build their virtual private cloud infrastructure.[6]

• **Cloud tool vendor.** These ISVs offer licensed software tools, which help enterprises and cloud providers build and provide their cloud services. Companies in this category include specialists like Cloud.com, Eucalyptus Systems, and RightScale as well as larger players like IBM, Microsoft, Oracle, and VMware. The private and virtual private cloud segments are again the best target markets for this new value proposition, as public cloud providers develop many tools on their own and leverage open source solutions extensively.

• **Cloud infrastructure provider.** Although fairly similar to the traditional IT outsourcing model, vendors in this category provide infrastructure and hosting services specifically for cloud needs. The key characteristics of the offerings include highly standardized and virtualized data center infrastructures as well as the supplying of the appropriate service provisioning and billing platforms. Vendors in this space include Amazon.com and GoGrid as well as traditional hosting providers like Rackspace and T-Systems International with virtual private cloud offerings.

• **Cloud integrator.** This model is pretty close to the traditional systems integrator value proposition with its mix of consulting, integration, and hosting offerings. However, the skills of a cloud integrator have evolved significantly beyond that. For example, the traditional expertise around traditional middleware is extended by the knowledge of configuring cloud-based integration (CBI).[7] Traditional IT service providers like HP, IBM, and T-Systems International have started to focus on this opportunity more explicitly as an extension of their traditional business. IBM, meanwhile, underpins its service offerings in this space with an integrated product suite that it evolved in particular through the acquisition of Cast Iron Systems in 2010.[8]

• **SaaS provider.** Probably the most mature and prominent of all the cloud business models, specialist software providers like NetSuite, salesforce.com, and Workday offer business application functionality as a service over the public cloud. Because this model requires the converged skill sets of traditional ISVs and hosting providers, the cloud-native pure plays drive most of the growth and innovation while many traditional software vendors struggle to catch up.

• **Cloud value-added reseller (VAR).** While the assumption in the early days of cloud computing was that self-service provisioning would eliminate the reseller model completely, an increasing number of SaaS providers are using a VAR channel to manage local subscriptions. Companies like Capgemini are, in many instances, acting as resellers of SaaS subscriptions and provide additional services around customization and integration with core systems.[9]

• **Cloud broker.** Last, but not least, the cloud broker represents the most complex business model, offering a wide value contribution in the emerging cloud space. Essentially, this model leverages skills and capabilities from all three of the traditional business models of software, consulting, and infrastructure. We dedicate the following sections of this report to this new business model.