Prologue.

AVIS D'EXPERT

Comment bien choisir son nuage…
Et éviter des averses incontrôlées !

Par Najah Naffah, Directeur Général de Prologue France

Le Cloud : une technologie dont tout le monde parle, mais qui reste encore un concept un peu brumeux, pour le grand public comme pour les entreprises. Mais avec des appellations comme s'il en pleuvait, Cloud Privé, Cloud Public, Cloud Hybride, Cloud Communautaire, SaaS, PaaS, IaaS… comment faire le bon choix pour éviter la douche froide ?

Récemment, le vol de photos très privées de plusieurs célébrités américaines a mis le cloud à la Une de l'actualité. Les données confiées à des espaces de stockage en ligne pourraient-elles donc être récupérées par des tiers non autorisés ? Cette mésaventure hollywoodienne n'a pas contribué à rassurer les particuliers et les entreprises déjà frileux. En France, seulement 1 entreprise sur 9 aurait mis en place une stratégie cloud, selon le cabinet PAC.

Pourtant, l'informatique en nuage intègre un certain nombre de principes et de technologies à travers lesquels les entreprises peuvent bénéficier d'une nouvelle approche pour gérer leur système d'information et leur parc applicatif. Mais la multitude d'appellation, dont certaines restent absconses (Cloud Privé, Cloud Public, Cloud Hybride, Cloud Communautaire, SaaS, PaaS, IaaS…) et qui peuvent différer d'un acteur informatique à l'autre dû à l'absence de normes, n'aide pas à comprendre les spécificités, les enjeux et les implications de chacune des formules disponibles. Or, à chaque type d'utilisateur correspond un type de solutions, avec des points bien spécifiques à vérifier en matière de sécurité des données.

Pour l'utilisateur particulier, le Cloud n'est pas une finalité en soi

Dans un premier temps, l'utilisateur particulier est confronté à l'utilisation du Cloud généralement au travers de ceux de ses réseaux sociaux préférés. Dans ce cadre, pour chaque réseau social qu'il fréquente, il sera tributaire de la technologie de Cloud propre audit réseau social. Il doit pourtant avoir conscience des risques liés à son utilisation. La lecture des clauses de confidentialité lui permettront, en premier réflexe, de se munir d'un parapluie – ou plus concrètement de choisir ce qu'il accepte de partager et avec qui. Pour éviter les giboulées, il doit également penser à changer régulièrement le mot de passe lui ouvrant l'accès à l'espace en ligne où il stocke ses documents.

Dans un second temps et pour des utilisateurs plus technophiles, l'utilisation des nuages relève du « multi-cloud » au travers de solutions dites de box (Dropbox, Google Drive, OneDrive…) pour y stocker sa base d'informations personnelles. Selon PC Expert, on estime la moyenne de consommation de nuage à 3 solutions différentes utilisées par personne. Une des box ne suffit plus, l'utilisateur va en ouvrir une autre chez un autre prestataire.
Dans ce cadre d'utilisation, afin d'éviter les risques d'averse, il devra enfiler un imperméable et prendre un parapluie ; c'est-à-dire bien choisir son fournisseur de box en fonction de ses besoins (capacité de stockage, sécurité…) et y associer des solutions de sécurité complexe (identifiant et mot de passe, solution de content filtering, certificats numériques …).

Dans certains pays, l'Etat peut avoir accès aux données des utilisateurs de Cloud. Rappelez-vous, aux Etats-Unis d'Amérique, les révélations de Snowden ont permis de démontrer que PRISM (le code du programme de la NSA pour collecter les données numériques auprès des grands acteurs de

l'internet) avait pénétré **Microsoft** (septembre 2007), **Yahoo** (mars 2008), **Google** et **Facebook** (janvier 2009), **Youtube** (septembre 2010), **Skype** (février 2011) et **Apple** (octobre 2012). Ce programme donnait à la NSA la capacité d'accéder aux données personnelles de millions d'utilisateurs, dont les emails, les chats vocaux et vidéos, les vidéos, les photos, les échanges en voix sur IP, les transferts de fichiers, les log-in, les requêtes spéciales, ou les échanges en visioconférence - : Cette réalité et probabilité, il faut hélas l'accepter ou bien renoncer à utiliser ces services.

Une problématique plus complexe : l'utilisateur entreprise

Pour les **entreprises – petites ou moyennes -**, le Cloud revêt un véritable intérêt de compétitivité et doit donc être considéré comme tel. En effet, l'utilisation de ces nuages a totalement transformé la façon dont les entreprises s'équipent et consomment les nouvelles technologies. Avec le Cloud, les cycles longs n'existent plus ; les entreprises s'équipent plus vite et mieux. Fini les investissements à amortir (CAPEX) qui se révèlent, en outre, vite obsolètes !

Aujourd'hui l'équipement informatique via le Cloud relève de l'opérationnel (OPEX) : on loue des **infrastructures** (IaaS), des **plateformes** (PaaS) ou des **applications** (SaaS) et on en change dès que l'on souhaite. Cette nouvelle distribution apportée par les nuages permet ainsi de réduire les coûts informatiques et donc le prix de vente de ses produits, de réduire les délais de fabrication et de mise sur le marché, et d'augmenter la productivité des collaborateurs en mettant à leur disposition des solutions informatiques toujours à la pointe.

Pour une **grosse entreprise**, les besoins en matière de cloud différeront, car elle agit au niveau régional, national ou international ; c'est la distribution géographique qui orientera le choix du bon cloud. Selon une étude réalisée par le cabinet NTT sur plus de 1000 entreprises utilisatrices, 95% estiment que la localisation géographique de leur cloud a une grande incidence sur sa viabilité.
Le choix de ce type d'entreprises va donc s'orienter autour de 3 types de nuages : cloud public, cloud privé ou cloud hybride (combinant public et privé). Elle pourra également alterner régulièrement entre l'utilisation de l'un ou l'autre de ces types de nuages.
En phase de démarrage de nouveaux projets, elle pourra utiliser soit ses propres ressources cloud en local, soit un cloud public qui lui apportera les ressources complémentaires nécessaires à la phase de développement (capacités de calculs plus grandes, infrastructures plus solides ou avec une capacité de stockage plus grande, applicatifs plus à jour…). Une fois le projet développé et prêt à entrer en phase de production, l'entreprise aura alors intérêt à rapatrier ses informations sur son cloud privé et s'équipera en fonction des besoins nécessaires. Ou bien, en cas d'intervention sur des marchés saisonniers, avec des pics ponctuels d'activité, l'entreprise pourra passer sur un cloud public le temps de faire face à ces périodes de haute charge puis rebasculer sur son cloud privé quand l'activité revient à la normale.

Sécurité : Peut-on vraiment se mettre à l'abri ?

A partir du moment où une entreprise est connectée à Internet, les risques existent : le challenge est de posséder la meilleur protection. Cette prise en compte de la sécurité va s'exercer à 3 niveaux :

- sécurité physique,
- sécurité sur la continuité de service,
- sécurité des réseaux informatiques et télécoms ainsi que leurs points d'accès.
  Là encore, les solutions à adopter varient selon les cas.

La première des solutions tient dans l'IAM (identity and access management) qui va permettre à l'entreprise de gérer les comptes utilisateurs, de définir une politique d'accréditation, et de décider du process d'authentification (mot de passe, double-mot de passe, identification physique, certificat numérique…). Ensuite, se posera alors la question de l'hébergement de ses données en fonction de ses décisions de sécurité. Ainsi, pour les applications informatiques standards (Word, Excel, etc.) l'hébergement peut se faire sur le cloud privé de l'entreprise, ce qui n'engendre pas assez de bénéfices supplémentaires par rapport à un nuage public pour justifier le coût supplémentaire.
La location en mode SaaS (Software as a Service) est en revanche parfaitement adaptée. L'entreprise devra néanmoins effectuer quelques paramétrages afin de les sécuriser (contrôles d'accès, différents niveaux d'accréditation, antivirus…). Pour les applications à données stratégiques, en revanche,

l'entreprise aura tout intérêt à les héberger sur son propre cloud, afin de limiter au mieux les possibilités d'intrusion et de vols de données. Toutefois, il est également possible de demander à son fournisseur de cloud public de proposer un cloud privé au sein même de ce nuage public. Quelle que soit la décision de l'entreprise, cette dernière a tout intérêt à examiner de près le contrat de SLA et de back-up proposé par son fournisseur.

Pour les outils de productivité interne (RH, Compta, Supply Chain …) et de gestion de la relation clients, parfaitement opérables en mode SaaS, l'entreprise va devoir analyser les risques et les solutions de sécurité au cas par cas. Elle devra ainsi veiller aux différents niveaux d'accréditation et d'accès aux données proposés par les solutions mises à disposition.
Dans certains cas, il sera même judicieux d'utiliser plusieurs clouds différents pour héberger ces applications. Et dans ces cas-là, une solution de brokering en Cloud prend toute sa signification, d'autant plus qu'elle permet un monitoring en permanence de tout le réseau basculant facilement d'un cloud à l'autre.

EN CONCLUSION

Face aux diverses problématiques de l'entreprise, **un seul type de Cloud ne peut prétendre constituer la panacée universelle**.
Pour éviter les risques d'averse, il s'agira donc d'évaluer au plus près les besoins en matière de disponibilité, de sécurité et les contraintes budgétaires afin de retenir le meilleur compromis pour chaque situation. Celui-ci pourra passer par l'utilisation d'une solution associant différents types de clouds : public / public, public / privé…
On se protège de façon différente face à une petite averse et en cas de mousson ! Avec le Cloud, c'est pareil : chaque situation demande une solution adaptée très spécifique.

Pour éviter l'averse, il est donc recommandé aux utilisateurs de cloud de procéder de façon méthodique en parcourant les points suivants (check-list) :

Pour l'utilisateur particulier :

1. Quelle box je souhaite utiliser pour archiver et partager mes documents (en particulier, les photos et photocopies) ?
2. Quel type de réseau social je souhaite fréquenter et utiliser ?
3. Quel type de messagerie j'utilise pour échanger des mails avec d'autres utilisateurs ?

Et pour chacun de ses services, faire le choix du fournisseur, en tenant compte de règles de sécurité appliquées par les fournisseurs. Cette analyse pourrait déjà éliminer certains fournisseurs (en particulier les fournisseurs américains car les données stockées sont accessibles par les autorités américaines), et en retenir d'autres (par exemple, les fournisseurs de Cloud souverains qui garantissent une confidentialité totale des données privées).

Pour l'entreprise :

1. **Dans le cas d'une start-up**, adopter une solution Cloud, pour les applications génériques et applications verticales et métier
2. ***Inventaire applicatif*** : La meilleure approche est de dresser un inventaire des applications utilisées par l'entreprise ou à développer, pour répondre aux besoins stratégiques de cette entreprise.
3. ***Applications horizontales*** : Identifier celles qui sont horizontales (ou génériques – bureautique, collaboration, Réseau Social d'Entreprise RSE, communication temps réel, CRM, achats, commandes, finances, notes de frais, …) et celles qui sont verticales (applications métier développées spécifiquement pour l'entreprise, et qui sont généralement considérées comme critiques pour la compétitivité de l'entreprise et de ses produits et services.
4. ***Abonnements SaaS*** - Pour les applications génériques, valider le choix de fournisseur de SaaS pour chacune des applications sans exception.
   L'économie de passer en SaaS, ainsi que l'amélioration des performances et optimisation des coûts récurrents peuvent être significatifs, et associés à un usage des applications les plus

modernes tout en bénéficiant en permanence des évolutions des logiciels sans avoir à payer des licences supplémentaires.

5. ***Applications Verticales*** : Pour celles-ci, il est important d'opérer une analyse fine de leur adéquation par rapport aux besoins :
   a. Faut il les garder telles quelles et les opérer dans l'infrastructure (Data Center) existante ?
   b. Quels sont les coûts récurrents de la maintenance de ces applications et des coûts du data center ?
   c. Est-ce que la nature des applications permet de l'héberger dans un Cloud public, beaucoup moins cher, sans risque (tel qu'un site web orienté clients ou visiteurs externes de l'entreprise ?)

   Ou bien, est-il préférable de garder cette application, de la réécrire ou de la maintenir en interne ? Le même raisonnement s'applique aux données qui peuvent être hébergées à moindre coût dans un Cloud public externe, versus les garder en interne, car elles sont critiques et aucun risque de piratage ne doit exister.
6. ***Cloud Simple et Multi-Cloud :*** C'est à partir de cette analyse des applications verticales et des données sensibles ou non de l'entreprise, que l'on va pouvoir définir une stratégie multi-Cloud. Qui dans sa forme la plus simple, sera d'adopter ce qu'on appelle un Cloud Hybride (composé d'un Cloud privé – le Data Center de l'entreprise transformé en Cloud privé) et dans sa forme la plus sophistiquée, sera une configuration multi-Cloud (plusieurs Clouds publics) ayant chacun sa spécificité technique ou économique ou juridique.
7. ***Le Broker*** : Pour pouvoir déployer l'ensemble des applications verticales dans les divers Clouds constituant la solution finale, l'entreprise aura à choisir une plateforme de management de Clouds (appelé parfois Cloud Broker). Cette plateforme permettra d'orchestrer les applications selon des schémas prédéfinis, de les faire communiquer, de les sécuriser dans un réseau virtuel privé, de les migrer d'un Cloud vers un autre, d'en assurer la supervision et l'analyse des coûts réels liés à la consommation des ressources dans chacun des Clouds.

   Ce Cloud Broker offre aussi une interface unique « Dashboard » à travers lequel, toutes les applications et données hébergées dans divers Clouds seront suivies et administrées.
8. ***La sécurité*** : Dans chacune des solutions listées ci-dessus, exiger du fournisseur les mécanismes de sécurité, qui assurent la protection technique et juridique que vous souhaitez pour vos applications et vos données

A propos de Najah NAFFAH :

Najah NAFFAH a commencé sa carrière à l'**INRIA**, en tant que chercheur sur les réseaux d'ordinateurs (projet *Cyclades*) et les systèmes de bureautique avancée (projet *Kayak*). Il rejoint ensuite le groupe Bull, en tant que responsable des applications bureautiques, où il développe et lance des produits innovants de GED, Workflow et multimédia. Il intègre le groupe Sabre pour diriger sa filiale européenne d'où il lance sur le marché des produits d'optimisation des revenus pour le secteur de voyage. Il rejoint ensuite EDS, première société mondiale d'*outsourcing*, et devient VP pour l'Europe des services BPO (*Business Process Outsourcing*). En 2010, il crée la société de conseil Naffah Consulting spécialisée dans le BPO, et rejoint ensuite la société Prologue en tant que directeur général.

Contact Presse :
Cayen Consulting
Bruno Sanvoisin / Laurent Doumergue
Tel : 06 82 52 62 39 / 06 11 43 41 76
bruno@sanvoisin.net / Laurent.doumergue@gmail.com