Avis d'expert : évitez les risques lors de votre transition vers le cloud

Cet avis d'expert, proposé par **Vincent Berny**, directeur des offres infrastructure services chez Gfi Informatique, explique comment gérer le risque lors de la transition dans le *cloud*.

Le *cloud computing* a continué à prendre de l'ampleur tout au long de l'année 2011 et les enjeux ne vont pas se démentir en 2012. On peut cependant comprendre la réticence de certaines entreprises à déporter hors de leurs propres centres de traitements leurs données, sensibles ou non. Les risques perçus sont largement évoqués sur les forums du web : intrusions malveillantes, virus, failles logicielles, défaillances matérielles, pertes de données…

Cependant ces menaces, bien que réelles, sont largement prises en charge par les politiques de sécurité des opérateurs *cloud*. Lors des négociations contractuelles, le client potentiel peut obtenir une description de la politique de sécurité appliquée. Il peut parfois négocier une politique spécifique et renforcée, et même auditer régulièrement son exécution. Mais au-delà du choix du « meilleur » prestataire, inhérent à tout projet informatique, les risques liés à la transition dans le *cloud* sont à chercher ailleurs. On les retrouve en particulier en amont, pendant et après la bascule du SI vers la plateforme *cloud*.

Transformer l'architecture de son SI

Pour les contrats de type IaaS et PaaS, en préambule de tout projet de migration dans le nuage, il faut garder à l'esprit que l'architecture informatique du prestataire peut ne pas correspondre (et ne correspond généralement pas) à l'architecture initiale de son SI.

Une phase préparatoire nécessaire pour réussir sa migration va donc consister à transformer l'architecture de son SI pour qu'elle puisse fonctionner correctement dans le *cloud*. En effet peu de SI sont adaptés de façon initiale et dans cette perspective, la virtualisation et la standardisation des composants du SI sont des facteurs clés.

Les architectures proposées par les opérateurs sont basées sur la virtualisation et un catalogue limité de composants disponibles. Ces derniers permettent au client de constituer chacun des éléments de la plateforme cible (systèmes d'exploitation, *middleware*, base de données…). Ils sont souvent proposés pour un nombre restreint de versions courantes et supportées par les éditeurs partenaires.

Or, l'actualisation des composants des SI n'est fréquemment pas une tâche prioritaire au sein des entreprises. Bien souvent, une grande partie des applications en production intègrent des composants spécifiques qui ne sont pas maintenus dans les dernières versions des éditeurs. Il n'est pas rare même que des SI reposent sur des composants dont les versions ne sont plus supportées.

Passer au *cloud*, c'est se contraindre avant la bascule, à migrer ses applications vers la virtualisation, intégrer des composants standards et à jour, puis à gérer rigoureusement l'actualisation des composants intégrés dans le SI. Il faut apprendre à gérer ses configurations dans le temps :

l'architecture du SI va devoir évoluer au rythme des mises à jour du *provider*.

Lorsque l'on souscrit à une offre SaaS, il faut savoir que c'est souvent le prestataire opérateur qui va décider de la date de mise à jour d'une nouvelle version, comme cela doit être précisé dans le contrat. Cette mise à jour sera alors disponible simultanément pour tous ses clients. Cet aspect doit être anticipé par l'entreprise : la gestion des changements et de la synchronisation, de la formation des utilisateurs… sont des aspects très importants et gérés différemment de ce qui est fait dans une DSI interne.

Apprendre à externaliser

Le *cloud* peut révolutionner la productivité d'une entreprise, mais aussi bouleverser la façon de travailler de sa DSI. Son enjeu majeur se résume en trois mots : maîtriser son externalisation.

Contrôle des niveaux de service, gestion des changements, information des utilisateurs, accompagnement dans la durée, opérations en dehors de la plateforme vont devenir le quotidien de la DSI.

La DSI et l'entreprise doivent apprendre à travailler autrement et en particulier adopter une maîtrise d'ouvrage forte face à leur prestataire afin de contrôler le fonctionnement des SI externalisés, l'adéquation aux exigences de sécurité, les SLA (*Service Level Agreement*), piloter financièrement le contrat… Cette fonction de maîtrise d'ouvrage est essentielle et doit avoir été aménagée au sein de la DSI.

Le support aux opérations

Un autre point de vigilance concerne le support aux opérations, en particulier dans le cadre d'un SI complexe disposant d'interfaces et de besoins de contrôle spécifiques. Il faut définir dès le départ qui, du client ou de l'opérateur, va prendre en charge ces opérations.

Dans le premier cas, l'opérateur devra permettre au client de disposer des droits nécessaires sur la plateforme *cloud* afin de pouvoir administrer et exploiter ses applications. Dans le second cas, le client devra s'assurer que l'opérateur dispose des compétences *ad hoc* pour s'en occuper. Ces dispositions simples sont pourtant essentielles et très proches d'un projet d'infogérance. Si elles n'ont pas été envisagées, on peut se retrouver avec une application dans le *cloud*, mais sans la possibilité de l'exploiter.

Dans le cadre d'un ERP ou d'un portail avec de nombreuses connexions et passerelles vers des SI internes, les clients, les partenaires… l'important est de définir clairement en amont qui va exploiter, qui va assurer la gestion des incidents, en bref toutes les opérations habituellement menées dans un SI en exploitation. Les deux options (délégation ou conservation de l'exploitation) sont à envisager au cas par cas pour chaque application, en fonction des compétences et besoins des deux parties.

Réversibilité

Dans les faits, la réversibilité est toujours possible et ne pose pas de difficulté technique. L'éventualité d'une sortie du *cloud* doit cependant être envisagée avec sérieux. Si les logiciels utilisés sont standards, l'opération consiste à récupérer les données et à les réinjecter dans un SI en propre ou un autre *cloud*. Mais il faut que tout ceci ait été mentionné dans le contrat d'infogérance.

Dans le cas de logiciels non standards sur le marché, on se retrouve dans un cas de figure proche du contrat logiciel : il faut alors prévoir la notion d'achat ou de location de la solution logicielle. Il faut aussi qu'en cas de disparition du prestataire, ses clients puissent récupérer en plus des données, les objets et sources du logiciel.

Ce sont là des précautions spécifiques d'une prestation de type SaaS. Travailler en mode SaaS nécessite donc de cumuler les précautions que l'on doit prendre vis-à-vis d'un éditeur et d'un infogérant. Différents types de clauses doivent être associées ce qui résulte en des contrats souvent assez complets.

Vers un label pour le cloud ?

Les bonnes pratiques du *cloud computing* sont donc aujourd'hui proches de celles de l'externalisation IT et de l'acquisition de logiciels. Une labellisation spécifique au *cloud* pourrait à l'avenir être un nec plus ultra pour les prestataires, un tel outil permettant aux entreprises de clarifier l'offre *cloud* qui leur est proposée.

De la même façon que l'on sait aujourd'hui certifier les processus d'un centre de service, les services *cloud* seront amenés à être certifiés selon des normes permettant de comparer les opérateurs entre eux, au plus grand bénéfice des clients.

Crédit photo : © Gfi Informatique