collection DataPro

Cloud privé, hybride et public

Quel modèle pour quelle utilisation ?

Un état de l'art et des bonnes pratiques

Marc ISRAEL

eni

Avant-propos

Chapitre 1
Le cloud, cette belle nébuleuse

Chapitre 2
Limites et contraintes du cloud

Chapitre 3
Légendes urbaines

Chapitre 4
Législation

Chapitre 5
Bonnes pratiques

Chapitre 6
Chances et opportunités

Chapitre 7
Et maintenant, on fait quoi ?

Conclusion

Annexes

Chapitre 2
Limites et contraintes du cloud

« Je ne crois point au sens philosophique du terme, à la liberté de l'homme. Chacun agit non seulement sous une contrainte extérieure, mais aussi d'après une nécessité intérieure. »

Comment je vois le monde, Albert Einstein

Alors le cloud, est-ce la panacée, le remède à tous les maux de l'informatique locale et du développement économique ? Si on ne peut pas nier son colossal apport au développement de certaines entreprises, voire de certains états, il est primordial d'en comprendre les limites et les contraintes.

Ce n'est pas nier ses qualités que d'en regarder ses limites. C'est s'assurer honnêtement avec lucidité que ce n'est pas toujours la réponse à tout et, surtout, que ce n'est pas ni aussi facile, ni aussi économique, ni aussi rapide que certains prestataires veulent le laisser entendre. En revanche, c'est une réelle innovation qui, une fois correctement appréhendée, permet de repousser toutes les limites d'une informatique locale et une accélération de toutes les ambitions de développement.

Les Anglo-Saxons disent que le ciel est la limite (*sky is the limit*) pour signifier qu'il n'y a en fait aucune limite à tel ou tel sujet. Cela tombe bien, car les nuages (le cloud) s'y trouvent déjà. Le cloud est porteur de nombreuses promesses, mais toutes ne peuvent pas être tenues si l'on ne comprend pas les limites dans lesquelles on opère afin de pouvoir les repousser.

Il existe trois limites immédiates aux technologies cloud et toutes sont du côté du client. En effet, du côté du prestataire, en tout cas en ce qui concerne les prestataires globaux comme Microsoft, Amazon ou Google, les limites n'existent pas. Leurs infrastructures sont gigantesques, englobant des centres de données contenant plusieurs millions de serveurs, massivement redondants, géographiquement répartis et de plus en plus utilisant des énergies renouvelables. Il n'y a donc quasiment aucune limite aux traitements que l'on peut y exécuter.

Les trois limites et contraintes côté clients sont donc les suivantes :

1. *La sécurité des applications, des matériels, des infrastructures et des individus*. Liés à la sécurité, on trouve la confidentialité et la souveraineté des données, primordiales pour garantir une relative indépendance des états et des entreprises.

Remarque

La souveraineté des données est traitée en détail au chapitre Législation.

2. *La bande passante*. La connexion Internet devient un goulot d'étranglement et potentiellement le maillon faible (*single point of failure*).
3. *Les coûts*. En particulier les coûts financiers cachés et les coûts humains si l'on ne prend pas en compte l'évolution du système d'information.

On y voit une quatrième pointer dans de nombreux pays développés et qui devraient prendre de l'importance dans les mois et les années à venir en Afrique : l'impact environnemental. Même s'il n'existe aucune législation en ce sens dans nombre de pays africains pour privilégier l'utilisation des énergies renouvelables ou favoriser les comportements durables, il y a fort à parier que cela arrivera, plutôt rapidement.

Regardons ces quatre aspects en détail, afin de pouvoir en déduire les démarches et processus à la fois les plus économiques, et les plus cohérents à court et long terme.

1. Sécurité

Que n'a-t-on dit sur la sécurité d'Internet et de ses données? Alors que les scandales vont bon train, du vol des données de Dailymotion ou de Yahoo! aux Panama Papers et autre Wikileaks, la sécurité du cloud est constamment remise en question. La cybercriminalité et l'espionnage sont sur toutes les lèvres. Mais qu'en est-il vraiment ? Le cloud est-il aussi risqué qu'on le dit ? Nous revenons sur les nombreuses histoires, rumeurs et idées fausses dans le chapitre Légendes urbaines, intéressons-nous ici à ce qu'est la sécurité des données stockées dans le cloud et comment faire pour tout protéger au mieux de nos possibilités et de celles proposées par le prestataire de service.

1.1 Menaces

Avant de débattre de la sécurité, posons la question des menaces. De quoi nous protégeons-nous ? Généralement, la première réponse qui vient à l'esprit est le vol de données. Pour une organisation, cela peut signifier vol de propriété intellectuelle, vol de clientèle ou perte de réputation. Pour un individu, c'est un accès à ses comptes bancaires, l'usurpation de son identité ou la publication d'information confidentielle dans le but de nuire.

Comme le disait Éric Schmidt, ancien PDG de Google, « Si vous faites quelque chose et que vous voulez que personne ne le sache, peut-être devriez-vous déjà commencer par ne pas le faire. » Facile à dire, surtout quand il s'agit d'informations purement confidentielles qui n'ont pas à être diffusées. Au-delà de la question du stockage de ces informations, la question est : sont-elles plus en sécurité dans le cloud que sur un serveur de l'entreprise ou sur mon ordinateur personnel ? Nous allons y revenir.

L'autre menace est la destruction pure et dure de l'information. C'est le cas de certains virus qui se contentent « juste » de tout détruire dans l'intention de nuire. Ce sont dans ces moments que l'on s'aperçoit que les sauvegardes qui ont été faites ne sont pas complètes ou accessibles. La fameuse loi de Murphy !

Enfin, depuis quelques années, une menace croissante est le rançongiciel ou ransomware. Cette pratique consiste soit à voler des données, soit à les chiffrer, puis à demander à leurs propriétaires une rançon pour les récupérer ou obtenir la clé de déchiffrement. Ce type d'attaque est en progression d'année en année. Il est à noter que d'après Kaspersky Lab, vingt pour cent des victimes qui payent ne récupèrent pas leurs fichiers. La question est donc : doit-on payer ?

Que faire pour se protéger de ces menaces ? Les experts de la sécurité informatique et les éditeurs de solution de sécurité recommandent plusieurs actions :

– Se protéger. Cela semble du bon sens, mais plus simple à dire qu'à faire. En effet, la surface d'attaque augmente (nous y reviendrons), les menaces évoluent sans cesse et l'information des utilisateurs ne suit généralement pas, mettant tout le système en danger.
– Évaluer les risques et les coûts. La sécurité a un coût et des conséquences. Il n'est pas possible de se protéger de tout à moins de vivre en vase totalement clos. Il convient alors d'évaluer les risques de perte ou de vol de données et de prendre les mesures adéquates.
– Classifier les informations. Cet aspect est abordé dans le chapitre Législation. Classifier ses données permet de savoir ce qui est public, ce qui ne l'est pas, ce qui est hautement confidentiel et ce qui l'est moins. Cela permet alors de mettre en place des règles de sécurité en fonction des données traitées.
– Mettre en place des bonnes pratiques. L'humain est souvent le maillon faible. C'est de plus en plus le vol d'identité qui sert de point d'entrée pour le vol d'information. Il convient alors de structurer une politique de protection de l'identité au travers de mots de passe forts ou d'authentification multifacteur pour limiter au maximum ces risques.

1.2 Concepts de base de la sécurité

La sécurité de l'information est un vaste sujet. Vous trouverez de nombreux livres et articles qui en traitent, ainsi que de nombreuses sociétés dont c'est le métier quasi unique. Afin de pouvoir apprécier la sécurité des services cloud, il me paraît primordial de savoir ce dont on parle. La sécurité de l'information se définit autour de trois concepts principaux : confidentialité, intégrité et disponibilité, auquel s'ajoute parfois la non-répudiation.

1.2.1 Confidentialité

Dans la norme ISO/CEI 27001, la confidentialité est définie comme « le fait de s'assurer que l'information n'est accessible qu'à ceux dont l'accès est autorisé ». L'identification des utilisateurs, les droits qu'on leur attribue et le chiffrage de l'information jouent un rôle majeur dans la protection de l'accès aux informations.

1.2.2 Intégrité

L'intégrité signifie que l'information est complète et exacte. Cela indique aussi qu'elle ne peut pas être modifiée de façon fortuite, imprévue ou malintentionnée. Généralement, la traçabilité des modifications, la sauvegarde continue des versions précédentes et les sommes de contrôles permettent de garantir l'intégrité des informations.

1.2.3 Disponibilité

La disponibilité définit que l'accès à l'information est possible dans les limites définies par son propriétaire. Dans le cas du cloud, nous avons vu que la disponibilité faisait l'objet d'une classification précise. À celle-ci peut s'ajouter le temps d'accès, qu'on peut définir en fonction du type d'information (une donnée archivée pouvant nécessiter un temps plus long qu'une donnée « vivante »).

1.2.4 Non-répudiation

Cette caractéristique est juridique et fait généralement partie de l'intégrité. Elle signifie que l'expéditeur et le destinataire d'une information sont bien ceux qu'ils prétendent être et que l'information envoyée est conforme à celle reçue et qu'elle n'a pas été altérée. Le mécanisme de certificats numériques est généralement utilisé et accepté par la justice pour prouver la non-répudiation. Encore faut-il pouvoir garantir la sécurité (intégrité, confidentialité et disponibilité) de sa clé privée, d'où la solidité logique des mécanismes comme les cartes à puce.

1.3 Et mon centre de données dans tout ça ?

Maintenant que nous avons défini les concepts de base et avons une idée des menaces qui ciblent nos informations, regardons ce qu'il en est de la sécurité du centre de données. Si nous souhaitons protéger nos informations et en garantir une sécurité maximale, il faut tout d'abord nous intéresser à la surface d'attaque de notre système.

1.3.1 Surface d'attaque

La surface d'attaque d'un système informatique peut être définie par l'ensemble des points d'entrée et des points de communication avec l'extérieur. Sur tout système accessible, elle est généralement importante et doit être précisément connue. On distingue généralement quatre types de surface d'attaque :

1. La surface d'attaque réseau : ports ouverts sur les routeurs et les pare-feu, adresses IP publiques, protocoles réseau utilisés et disponibles...
2. La surface d'attaque logicielle : formulaire de saisie, système d'exploitation, services démarrés du serveur, interfaces d'administration...
3. La surface d'attaque humaine : la réaction de l'utilisateur à toutes les sollicitations auxquelles il peut répondre, comme cliquer sur un lien, ouvrir une pièce jointe ou cliquer sur un bouton. Le phishing ou l'engineering social nécessite ces actions par exemple.