

LE CLOUD COMPUTING : DÉFINITION, ENJEUX ET BÉNÉFICES

Plus qu'une énième technologie, le Cloud Computing inaugure une nouvelle façon de concevoir et de consommer l'informatique. Aujourd'hui incontournable, il constitue une véritable révolution dans la fourniture de solutions de gestion.

Quelles en sont les caractéristiques ? En quoi est-il bénéfique pour les entreprises ? Dans ce premier volet sur le sujet, nous aborderons la définition du Cloud et analyserons les enjeux et les bénéfices du modèle.

DÉFINITION & APPROCHE

Le terme de « Cloud Computing » a déjà fait couler beaucoup d'encre et chacun y va de sa définition. Pour les uns, le Cloud est un ensemble de services d'hébergement, pour d'autres, c'est de la fourniture d'infrastructures à distance, et pour d'autres encore, le Cloud est une fédération de services applicatifs à la demande.

Ce qu'il faut d'abord bien comprendre, c'est que le Cloud n'est qu'un concept, et non une offre en tant que telle. Il s'inscrit dans la logique d'externalisation (et de dématérialisation progressive) du système d'information. Le Cloud Computing fait référence à des **ressources informatiques, utilisées par une ou plusieurs entreprises, à la demande, accessibles via Internet et reposant sur des infrastructures distantes, mutualisées et interconnectées entre elles.**

Les solutions Cloud Computing (comprenez « informatique en nuages ») se distinguent des applications informatiques traditionnelles en ce qu'elles apportent à l'utilisateur un **service à la demande**, assuré par des ressources IT distantes, mises en oeuvre par le fournisseur Cloud.

A la différence d'un modèle d'externalisation classique (outsourcing ou TMA), le Cloud offre plus de souplesse et de liberté : **l'entreprise utilisatrice accède au service quand elle le veut, pour le temps qu'elle veut.**



+20%

**CROISSANCE MARCHÉ DU
CLOUD EN FRANCE EN
2015***

CLOUD PUBLIC, PRIVÉ, HYBRIDE : QUELLES DIFFÉRENCES ?

Le Cloud Computing peut être déployé en trois modes distincts, chacun correspondant à des usages différents :

- le **Cloud Public** : il repose sur des ressources gérées par un prestataire externe et **mutualisées pour un usage partagé par un grand nombre d'utilisateurs**. Il convient aux entreprises pour des services très standards, comme la messagerie.
- le **Cloud Privé** : il est **utilisé en exclusivité par une seule entreprise** et peut être hébergé soit par l'entreprise, soit par un fournisseur externe. Il apporte en général des SLA sur mesure et plus forts.
- le **Cloud hybride** : c'est le fait d'utiliser un mixte Cloud Privé et Cloud Public pour son système d'information. C'est le modèle de plus en plus adopté par les entreprises aujourd'hui.

DE RÉELS AVANTAGES POUR LES ENTREPRISES

Economie budgétaire, maîtrise des coûts opérationnels, souplesse, agilité... Les **bienfaits du Cloud Computing** pour les entreprises sont potentiellement nombreux.

Réduction des coûts informatiques

L'un des principaux enjeux du Cloud Computing est, comme dans toute stratégie d'externalisation, d'ordre financier. Dès le départ, il exonère l'entreprise d'un investissement (parfois lourd) en achat de licences et de matériels : des **économies facilement et rapidement mesurables**.

Au-delà de l'investissement initial, la maîtrise du budget informatique est facilitée par le **lissage des coûts** et par la **visibilité de la dépense** sur le long terme. Plutôt que d'investir dans des immobilisations (CAPEX), l'entreprise concentre ses efforts sur ses dépenses opérationnelles (OPEX). L'imputation de l'informatique en OPEX libère des lignes de budget pour des **investissements plus centrés sur le coeur de métier**.

Accessibilité, agilité et productivité

L'accès aux applications Cloud nécessite une simple connexion Internet, permettant aux collaborateurs éloignés de l'entreprise de se connecter à distance sans difficulté. Le Cloud développe la mobilité et encourage le travail collaboratif des équipes en tout temps et en tout lieu. Il facilite la consultation des informations de l'entreprise, et augmente ainsi la productivité des collaborateurs et leur satisfaction au quotidien.

La productivité de l'entreprise se voit également largement optimisée grâce aux **temps d'implémentation** qui sont réduits par rapport aux solutions classiques. La souplesse offerte par l'abonnement permet d'adapter le périmètre fonctionnel choisi par l'entreprise en agissant sur les modules déployés, et d'ainsi **disposer d'une configuration sur mesure**. L'utilisation de nouveaux modules proposés par l'éditeur est quasi-immédiate après souscription, contrairement au mode traditionnel qui implique un nouveau cycle de déploiement.



Sécurité & confidentialité

En optant pour une solution en Cloud, les données sont hébergées au sein de **datacenters hautement sécurisés**, sous surveillance permanente. Les connexions sont contrôlées, les informations échangées sont chiffrées et les transferts de données sont surveillés. La confidentialité est également renforcée grâce à une politique de sécurité stricte passant par la gestion des identifiants, la clause de confidentialité du personnel, etc.

Parce que les données ne sont pas hébergées sur les serveurs de l'entreprise, elles ne dépendent plus de ce qui pourrait arriver au sein des locaux : en cas de sinistre, elles restent **en sécurité**, le fournisseur Cloud aura mis en place toutes les parades nécessaires permettant de restaurer le service & de garantir zéro perte de données (sauvegarde multi-sites, etc.).

CEGID CLOUD SERVICES & SOFTWARE

Cegid développe des bouquets de services innovants sur le marché du Cloud Computing. Elle investit depuis de nombreuses années pour se doter des moyens techniques et humains nécessaires pour opérer ses applications en mode SaaS. Cette stratégie permet aujourd'hui à Cegid d'offrir à ses clients des solutions en ligne performantes, bénéficiant d'un mode d'utilisation simple, ouvert et sans contrainte.

Le groupe Cegid compte ainsi parmi les acteurs les plus dynamiques du marché du SaaS et du Cloud Computing.

SÉCURITÉ : LES 10 BONNES QUESTIONS À SE POSER

Alors que le recours à des solutions SaaS s'impose de plus en plus dans les habitudes des entreprises, quels points vérifier avant de se lancer ? Quelles sont les questions à se poser et quelles garanties vérifier avant de choisir son fournisseur ? Pour vous aider dans votre réflexion, nous vous donnons ci-dessous les points clés à vérifier auprès des prestataires de services Cloud...

COMMENT SONT GÉRÉES MES DONNÉES ?

En fonction de la nature des données confiées au prestataire SaaS (données personnelles, sensibles, stratégiques, etc.), l'exigence en termes de sécurité ne sera pas la même.

Les principaux points qui seront à vérifier et pour lesquels l'éditeur devra apporter des réponses précises seront les suivants :

Où seront localisées vos données ?

L'entreprise qui envisage de souscrire un abonnement SaaS devra en amont s'assurer du lieu exact où sont localisées ses données, surtout s'il s'agit de données stratégiques, et vérifier que le prestataire ne les transfère pas à l'étranger sans son accord. Cela évitera la mauvaise surprise d'une réquisition judiciaire des données par des autorités étrangères ou l'hébergement dans des pays dans lesquels les niveaux de sécurité ne sont pas optimums. **La localisation des données et des équipes de production doit donc être précisés contractuellement.**

Soyez par exemple vigilants avec les « cloud publics » pour lesquels il n'y a généralement que peu d'engagement sur la localisation des données.

Comment la confidentialité des données est-elle gérée ?

Le fournisseur Cloud doit être en mesure de garantir, de manière contractuelle, la confidentialité des données qui lui sont confiées et qu'il n'utilisera pas vos données à d'autres fins que celles prévues dans votre le contrat.



23 millions

D'EMPLOYÉS DANS LE MONDE
UTILISENT LE CLOUD*

La restitution des données est-elle cadrée contractuellement ?

La restitution des données est la possibilité de pouvoir obtenir une copie de l'intégralité des données dans un format du marché qui permet au client de **pouvoir changer de solution sans perte d'information.**

Qu'advient-il des données à l'issue du contrat ?

Afin de garantir la sécurité de ses données, l'entreprise doit vérifier la durée de conservation de ses données à l'issue de son contrat ainsi que la destruction effective et sécurisée de celles-ci.

Chez Cegid par exemple, les données sont conservées 60 jours après la fin du contrat puis elles sont effacées.

*Cloud Adoption and Risk Report 2015

COMMENT EST ASSURÉE LA SÉCURITÉ DES DONNÉES ET DES LOCAUX ?

Il est essentiel que les locaux où seront stockées vos applications et vos données soient eux-mêmes sécurisés : sécurité des accès, résilience des infrastructures, réplication des données (DRaaS) et plan de continuité d'activité (PCA).

Vérifiez également que l'ensemble des éléments du datacenter sont redondés. Très concrètement, cela signifie que tout problème technique rencontré aura immédiatement une solution grâce à un autre élément qui viendra prendre la relève de l'élément défectueux et cela, sans perturber l'utilisation du service. En effet un élément non redondé constitue une faille de sécurité pour l'ensemble du data center : on parlera ainsi de **politique « No SPOF » (No Single Point Of Failure)**.

PCA, DRaaS et NO SPOF sont notamment des politiques appliquées dans les datacenters qui hébergent les solutions SaaS du groupe Cegid.

Les niveaux de sécurité peuvent varier en fonction des prestataires, voire des datacenters d'un même prestataire. C'est pourquoi il est essentiel de **vérifier les garanties que présente le fournisseur cloud** afin que l'infrastructure du data center ne puisse constituer en elle-même une potentielle faille de sécurité : protection du site et sécurité des accès, sécurité électrique et système de climatisation, protection du réseau (pare-feu, antivirus, détection d'intrusion, etc.)...

Un bon indicateur quant à la qualité des process est l'existence de **certifications de type ISO 27001**, qui établit des spécifications de pointe concernant la sécurité des Systèmes d'Informations.

UN OBJECTIF : SÉCURISER VOTRE ACTIVITÉ

Choisir un partenaire pérenne, s'assurer qu'il sera en mesure de vous garantir la sécurité de vos données et de l'infrastructure qui les protège sont des préalables essentiels. **C'est l'assurance de ne pas risquer d'arrêt d'exploitation dans l'utilisation de votre solution qui pourrait pénaliser votre activité.**

Mais quelles que soient les garanties qui vous sont données, vous accédez à votre solution au travers de votre propre infrastructure Télécom. C'est donc un des points de vigilance important. L'exploitation d'une solution de production « cœur de métier » doit disposer entre autres

de la bande passante nécessaire et ne pas risquer d'être ralenti par d'autres flux internet quotidiens (visionnages de vidéos, mails, téléchargements...).

Le prestataire doit vous fournir les prérequis techniques nécessaires au bon fonctionnement de la solution, et vous communiquer les débits minimums et la latence recommandés. De l'ultra performant VPN à la ligne ADSL, l'infrastructure télécom devra être déterminée en fonction de la criticité des données hébergées, de la typologie d'application utilisée, ou du nombre d'utilisateurs.

Autant de mesures au service de la sécurisation de vos données et de votre activité.



Les bonnes questions à se poser et à poser à son fournisseur Cloud

1. La localisation des données est-elle bien précisée ?
2. La propriété des données est-elle bien encadrée ?
3. La confidentialité de mes données est-elle garantie ?
4. La restitution des données est-elle cadrée ?
5. Quelles sont les mesures de sécurité et de résilience mises en place ?
6. Quelles sont les certifications du fournisseur Cloud ?
7. Le fournisseur Cloud a-t-il un PCA / un Draas ?
8. Quelle est l'expérience de mon fournisseur Cloud ?
9. Quels sont les prérequis techniques ?
10. Alors... Quand est-ce que je me lance ?

CLOUD PRIVÉ CEGID



**DATACENTER
TIERS 3+
LOCALISÉS EN FRANCE**



**INFRASTRUCTURE
CERTIFIÉE ISO 27001**

99%



**TAUX DE DISPONIBILITÉ
GARANTI**

SÉCURISEZ VOTRE ACTIVITÉ



+400%

de **données perdues** depuis 2012.

64% des entreprises ont subi **une perte de données** ou une **interruption d'activité** en 2014 au niveau mondial.



60% des entreprises qui perdent leurs données cessent leur activité dans les 6 mois suivant le sinistre.

PROFITEZ DE SAUVEGARDES FIABLES

42% des entreprises ont une fréquence de sauvegarde de leurs données d'une fois par an.



34% des entreprises **ne testent pas leurs sauvegardes** sur bande.

77% découvrent des **échecs de sauvegardes** après des tests de sauvegardes



ANTICIPEZ LES RISQUES



En 2015, les **cyberattaques** ont progressé en France de

51%

En 2015, les entreprises françaises ont subi en moyenne

21 incidents/jour



Augmentation de **28%** de **pertes financières** estimées, imputables à ces incidents en 2015

FAIRE FACE À L'EXPLOSION DU VOLUME DE DONNÉES

90% des données créées dans le monde l'ont été durant **les 2 dernières années.**



010101
001010
010101
001010

x30 le volume de données d'ici 2020 pour atteindre **35 zettaoctets** au total, au niveau mondial.

Selon **63%** des entreprises, ce flux massif de données apporte une pression supplémentaire sur leurs infrastructures.



LES ATOUTS DU CLOUD #CEGID/IBM



SÉCURITÉ

- Garantie de ne plus perdre ses données
- Accès à un niveau de sécurité que seul un industriel peut atteindre
- Infrastructure certifiée ISO 270001
- Surveillance 24/7 des datacenters



SAUVEGARDES

- Sauvegardes redondantes et sécurisées quotidiennes
- Tests de restauration réguliers



CONFIDENTIALITÉ

- Respect de la confidentialité de vos données
- Garantie de localisation des données



DISPONIBILITÉ

- Élimination des pertes business dues aux indisponibilités de votre SI
- Meilleur ROI

Sources : Cabinet Vanson Bourne pour le compte de l'entreprise EMC
EMC-IDC - PwC - IBM

Découvrez nos offres // www.cegid.fr
Site corporate // www.cegid.com
Portail clients // www.cegidlife.com
Boutique en ligne // www.cegidstore.com

