LE CLOUD COMPUTING

Définition

De (trop) nombreuses définitions du Cloud Computing existent, fournies par des instances de normalisation telles que le NIST aux Etats-Unis, des cabinets de conseil spécialisés ou des groupes d'utilisateurs ou de fournisseurs du métier de l'informatique.

Toutes ces définitions s'articulent autour de quelques grands thèmes sur lesquels tous les observateurs s'accordent : le Cloud Computing représente une nouvelle façon d'utiliser et de fournir l'informatique aux entreprises et aux particuliers, une façon qui certainement prévaudra sur le long terme. En quelque sorte, le Cloud Computing représente l'informatique de demain.

Le rôle de l'Internet est central dans sa mise en œuvre. Dans le grand public, on se réfère souvent à l'Internet comme un moyen d'accéder à de l'information au travers de pages qui s'affichent dans un navigateur. Mais ces 15 dernières années, Internet a suivi des évolutions majeures, qui en font aujourd'hui une plate-forme d'échange et d'intelligence à grande échelle, permettant certes la communication entre un utilisateur et une application, mais aussi et surtout la dissémination d'applications au sein du réseau, et leur mise en communication au sein d'architectures très modulaires.

C'est bien ce deuxième attribut qui permet aujourd'hui de parler de Cloud Computing. En effet, l'idée qui prévaut est d'utiliser l'Internet comme l'épine dorsale de l'informatique, en permettant à un utilisateur d'informatique de disposer de ressources mutualisées, prêtes à être utilisées, activables automatiquement et payables à l'usage.

A la clé figurent plusieurs promesses :

- Ne payer l'informatique qu'à l'usage, la mutualisation des ressources permettant de plus d'atteindre des économies d'échelle abaissant le coût global du service,
- Ne plus avoir à concevoir, installer et gérer des équipements et des applications, mais en disposer dynamiquement en mode service,
- Disposer d'une puissance de calcul potentiellement illimitée, permettant le cas échéant de mettre en œuvre des applications qui sans cela ne seraient pas viables économiquement.

Définition du NIST (National Institute of Standards and Technology), version 15 : le Cloud Computing est un modèle permettant un accès simple, à la demande, à des ressources informatiques partagées et configurables, au travers du réseau. Ces ressources peuvent être des équipements de réseau des serveurs, du stockage, des applications ou des services. Elles peuvent être rapidement mise à disposition et ensuite libérées avec un effort de gestion minime au travers d'une interaction limitée avec le fournisseur de service.

Exemples

D'innombrables applications de Cloud Computing existent sur le marché.

L'un des services les plus connus mondialement est celui d'Amazon Web Services, qui offre une puissance de traitement (EC2) ou de stockage (S3) à la demande. Il s'agit essentiellement d'une offre de catégorie IaaS (Infrastructure as a Service), constituée d'une infrastructure informatique virtuelle configurable et activable à la demande. L'utilisateur ne paye que la puissance utilisée, pour la période pendant laquelle elle a été mobilisée.

Salesforce.com offre des applications de gestion de la relation client, qui permettent de gérer l'ensemble des informations commerciales d'une entreprise. Cette fois-ci, le modèle est celui du SaaS (Software as a Service), où une application complète est mise à disposition de l'utilisateur au travers du réseau Internet.

Cibles

Le marché ciblé par le Cloud Computing est très large. La plupart des usages de l'informatique professionnelle sont disponibles via un service en mode Cloud Computing, aussi le marché représente potentiellement l'ensemble des entreprises, petites ou grandes, qui utilisent l'informatique.

Mais le marché du Cloud Computing est aussi celui du grand public : de très nombreux services accessibles de façon ouverte, et souvent gratuite, sont aujourd'hui disponibles, que ce soit pour la messagerie, la collaboration ou la gestion de documents entre particuliers.

Cadre réglementaire

Il n'existe fondamentalement pas de cadre réglementaire régissant les services du Cloud Computing, et de nombreux débats existent aujourd'hui sur l'applicabilité des cadres réglementaires existants au Cloud Computing, qui par nature rend virtuelles les ressources informatiques, abolit les frontières et pose des questions de souveraineté. C'est souvent à l'entreprise de s'assurer que les règlements auxquels elle est soumise seront respectés quand elle recourra aux services d'un fournisseur de Cloud Computing, que ce soit, notamment, pour la protection des données individuelles ou pour les règles de gouvernance telles que Bâle II ou Sarbanes Oxley.

Evaluation des risques

Dès lors que l'on applique les principes essentiels du Cloud Computing, on s'aperçoit que de nombreuses problématiques de sécurité vont se poser. Certaines seront résolues facilement par l'état de l'art technologique, d'autres demanderont que de nouvelles technologies soient mises en œuvre dans les années qui viennent.

De façon globale, la sécurité est aujourd'hui vue comme le principal frein à l'adoption du Cloud Computing par les entreprises, voire par les particuliers.

Par exemple, une étude réalisée par Forrester en octobre 2010 indique que sur un échantillon d'entreprises réticentes à adopter le Cloud Computing, 66% disent être préoccupées par la protection

des données, 65% par les contrôles d'accès, et 60% à la fois pour la gestion des vulnérabilités et la disponibilité du service.

Un particulier pourra en effet hésiter, par exemple, à stocker des informations confidentielles le concernant auprès d'un prestataire au travers de l'Internet. Ses craintes seront de divers ordres :

- Mes informations seront-elles lisibles seulement par moi ? Un tiers ne pourrait-il pas les lire ?
- Mes informations ne risquent-elles pas d'être exposées de façon publique ?
- Mes informations ne risquent-elles pas de disparaître, ou d'être altérées, en cas de problème chez le fournisseur de service ?

A l'échelle d'une entreprise, les questions qui se posent vont être d'un ordre de magnitude encore supérieur.

Localisation des traitements
Je ne possède plus directement les ordinateurs, les applications, voire les données me concernant. Ces ressources sont désormais quelque part chez mon fournisseur de service, et j'y accède au travers de l'Internet.
Quelle est leur localisation ? Sont-elles protégées efficacement comme je le ferais si j'en étais encore « propriétaire » ? Sous quel régime juridique mes données sont-elles désormais régies ?

Certification des ressources
Mes ressources sont désormais gérées, souvent de façon virtuelle et dématérialisée, par mon fournisseur de service.
Comment puis-je contrôler que mes ressources sont bien celles que je comptais utiliser à l'origine ? Comment puis-je m'assurer qu'elles n'ont pas été altérées pour un usage qui n'est pas celui que j'entendais ? Puis-je alors signer, ou certifier ces ressources pour m'assurer de leur conformité à mes attentes ?

Sécurité des échanges et des données
Je n'accède à mes applications et mes données qu'au travers de l'Internet.
Comment puis-je garantir la confidentialité des données échangées sur le réseau, ou stockées sur les systèmes du fournisseur de service ?

Gestion des utilisateurs et des droits d'accès
Autrefois, je m'identifiais dans mon système d'information par mon nom d'utilisateur et mon mot de passe.
Comment vais-je m'identifier demain vis-à-vis de ces applications disponibles en mode Cloud Computing ? Devrai-je me ré-identifier à chaque fois ? Pourrai-je disposer d'un identifiant unique ?

Défense contre les attaques Internet
L'infrastructure de mon fournisseur de service est partagée entre de nombreux utilisateurs et mise à disposition au travers de l'Internet.
N'est-elle pas, par sa nature même, plus exposée aux attaques (virus, chevaux de Troie, attaques en déni de service, etc.) ? Quel est le degré de protection mis en œuvre par mon fournisseur de service ?

Conformité
Mon entreprise est sujette à des réglementations et des obligations au titre de la loi ou au titre des attentes de mes parties prenantes sur la Responsabilité Sociétale d' Entreprise.
En ayant recours aux services de fournisseurs de Cloud Computing, suis-je encore en mesure de garantir à mes instances de régulation ou à mes parties prenantes que je respecte le cadre de fonctionnement

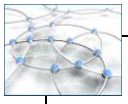
qu'ils attendent ? Pourrai-je auditer mon fournisseur d'accès et lui imposer certaines règles, de façon à garantir ma propre conformité ?

Moyens de protection

Les fournisseurs de service doivent mettre progressivement à disposition de leurs clients des outils de sécurité. De nombreuses solutions existent dès maintenant. Pour en citer quelques-unes, répondant point par point aux 6 défis listés ci-dessus :

- Certains fournisseurs de services établissent des plates-formes en Europe.
- Il est possible de certifier des ressources au travers de signatures électroniques.
- Il est possible de crypter des échanges et des données, en établissant des tunnels VPN entre utilisateur et fournisseur de services Cloud.
- Les identités peuvent désormais se gérer voire se fédérer à l'échelle de systèmes distribués.
- De nombreuses solutions de défense existent en matière de firewalls et d'équipements de réseaux.
- Et les fournisseurs de services, pour certains d'entre eux, peuvent d'ores et déjà se soumettre à des obligations contractuelles et réglementaires.

Bien entendu, le champ de la sécurité du Cloud Computing restera dans les années à venir un domaine d'innovation majeur pour l'industrie.



Liens utiles

Pour plus d'informations, se référer à la documentation disponible sur le sujet, et notamment les sites Internet suivants :

ENISA
http://www.enisa.europa.eu/activities/risk- management/files/deliverables/cloud-computing-risk-assessment/

http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds/

http://www.enisa.europa.eu/activities/application-security/test/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts

ANSSI
http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-de-l-externalisation/externalisation-et-securite-des-systemes-d-information-un-guide-pour-maitriser.html

CSA
https://cloudsecurityalliance.org/

SYNTEC NUMERIQUE
http://www.syntec-numerique.fr/Actualites/Livre-Blanc-Cloud-Computing-Securite