Position RSSIC CNRS sur le cloud – version du 29 juin 2012.

Définitions

Le Cloud computing désigne un service où les données manipulées sont stockées sur le réseau (métaphoriquement le nuage) et accessibles dans le cadre d'une offre qui fournit de l'énergie informatique à la demande (pas de serveur dédié a priori).

Le Cloud computing utilise de façon intensive la technologie basée sur les machines virtuelles qui permet de modifier plus aisément l'architecture et les capacités de l'offre de service indépendamment de son implantation physique (nombre et localisation des machines physiques).

On distingue principalement 3 formes de Cloud :

- Public (fourni par un prestataire privé et accessible via une offre publique)
- Privé (fourni par une entité au bénéfice de ses utilisateurs)
    - Privatif (infrastructure hébergée et gérée par l'entité)
    - Hébergé (infrastructure hébergée et/ou gérée par un tiers)
- Communautaire (fourni par une ou plusieurs entités au bénéfice d'une communauté de travail).

Les services offerts via une offre Cloud sont principalement :

- SaaS : l'utilisateur utilise une application
    - Ex : application bureautique, BAL de messagerie, Site Web, etc.
- PaaS : l'utilisateur peut paramétrer des logiciels
    - Ex : Gestionnaire de Site Web, Gestionnaire de messagerie, etc.
- IaaS : l'utilisateur peut installer son OS et/ou ses logiciels
    - Ex : Machine virtuelle, Réseau VPN virtuel, etc.

Mais les définitions et typologies sont encore instables, quelques références ci-dessous pour aller plus loin :

- http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf définitions et typologie courtes et synthétiques par le NIST (2 pages)
- http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000022309303 traduction officielle de « cloud computing » par « informatique en nuage »

Etudes sur la sécurité du cloud

Un système d'information basé sur le Cloud computing reste un système d'information.

Les principes majeurs de ce type d'offre de service ne sont pas nouveaux et peuvent se rencontrer dans d'autres systèmes plus anciens :

- Concentration des données
- Mutualisation des ressources
- Accès exclusif via le réseau étendu
- Utilisation de technologies complexes (virtualisation dans le cas du Cloud)
- Externalisation des données (avec plusieurs niveaux en fonction des types de Cloud)

Au début des années 2000 le SaaS s'appelait ASP (Application Service Provider). Le *cloud computing* peut être considéré comme le stade ultime de l'externalisation (dans le cas du Cloud public).

Les problématiques liées à cette externalisation sont :

- Localisation (ou plutôt non localisation) des données.
- Pérennité du fournisseur
- Cadre légal, réglementaire
- Garanties en matière de disponibilité, intégrité, confidentialité et preuve de l'information
- Réversibilité
- Coût actuel et futur

De là on peut déduire qu'en fonction des types de Cloud le risque est plus ou moins difficile/couteux à maîtriser :

Risque faible	Risque moyen	Risque moyen à fort	Risque très fort
Cloud privé privatif	Cloud privé hébergé	Cloud communautaire	Cloud public

En fonction de la sensibilité des données que l'on veut traiter et des mesures de protection que l'on peut mettre en place (avec la capacité de vérifier leur application) il est manifeste que l'on ne peut utiliser n'importe quel type de Cloud.

Quelques références ci-dessous pour aller plus loin :

- http://www.syntec-numerique.fr/content/download/380/1220/version/1/file/Livre_Blanc_Cloud_Computing_Securit%C3%A9.Vdef.pdf Livre blanc sur la sécurité du cloud computing par le Syntec numérique (une vingtaine de pages en français).

- http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf Guidelines on Security and Privacy in Public Cloud Computing (un rapport du NIST)
- http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport Cloud Computing Risk Assessment (une étude de l'ENSA sur les risques associés au *cloud computing*).
- https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf Sécurity Guidance for Critical Areas of Focus in Cloud Computing (des recommendations de Cloud Computing Alliance)
- http://www.clusif.asso.fr/fr/infos/event/archive2010.asp (aller au 14 avril 2010) Sécurité du Cloud computing et de la virtualisation (présentations et vidéos).
- Cloud computing : les conseils de la CNIL pour les entreprises qui utilisent ces nouveaux services, recommandations détaillées, synthèse des réponses à la consultation

Risques juridiques principaux du Cloud computing public (basée sur une analyse de la DAJ du CNRS) :

1° Contrat d'adhésion :

Les contrats proposés par les sociétés prestataires sont des contrats dits d'adhésion. Autrement dit, ils n'offrent aucune marge de négociation quant à leurs clauses. En effet, afin de bénéficier de ce service de stockage, l'utilisateur ou client doit accepter les « conditions générales d'utilisation » : le client ne peut pas le négocier et doit l'accepter ou non d'un simple clic (« click-wrap »).

Notons dans ces clauses non négociables :
- la possibilité pour le Prestataire de modifier ou d'arrêter le service de manière temporaire ou permanente avec ou sans préavis, à tout moment ;
- un désengagement de toute responsabilité du Prestataire se décharge de toute responsabilité quant l'accès et l'utilisation du service ayant provoqué tout dommage subi par le matériel, toute perte ou corruption des données du client.

2° Propriété intellectuelle :

A titre liminaire, il convient de relever que le contrat d'adhésion stipule que le client est présumé titulaire des droits de propriété sur les données qu'il va stocker. Par conséquent, avant de stocker toute donnée, le chercheur doit s'assurer d'être titulaire des droits sur cette donnée. En théorie, il ne peut donc pas stocker un résultat issu des travaux menés au sein du laboratoire.

Le contrat octroie à la société prestataire une licence non exclusive d'utilisation pour l'ensemble des données stockées et ce, pour les besoins du service ; autrement dit, un droit de reproduction et de modification sur les données (notamment pour le stockage dans d'autres serveurs).

Par ailleurs, le service propose à l'utilisateur des zones de stockage publiques (zones publiques / dossiers publics). Si le chercheur dépose des données dans ces zones ou dossiers, il concède automatiquement à la société prestataire et à l'ensemble des autres utilisateurs du service, une licence universelle, libre de droit et non exclusive d'utilisation, de distribution, de reproduction, de modification, d'adaptation, de publication, de traduction, de représentation et d'affichage publics du contenu. Il est donc vivement recommandé d'éviter d'utiliser ces zones, d'autant plus pour des données sensibles.

3° Confidentialité, sécurité et intégrité des données non garanties

Les caractéristiques propres du cloud computing ne permettent pas de garantir une confidentialité, une intégrité et une sécurité totales des données stockées. En particulier, la localisation des serveurs de stockage est méconnue du client et très vraisemblablement en dehors du territoire, voire même des États Membres de l'UE.

Les sociétés prestataires se déchargent de toute responsabilité quant à l'accès et l'utilisation du service ayant provoqué tout dommage subi par le matériel, toute perte ou corruption des données du client. Elles ne garantissent pas la sécurité des données.

De plus certains Etats peuvent demander aux sociétés soumises à leur juridiction, même si elles hébergent des données en territoire Français, de fournir les données hébergées dans le cadre de perquisitions soit sous le contrôle d'un juge soit hors de son contrôle, ces actions pouvant demeurer secrètes pendant une durée indéterminée.

4° Risque spécifique en cas de stockage de données à caractère personnel

Dans le cas où le chercheur installé en France utiliserait le service pour stocker des données à caractère personnel, il se retrouve sous le coup de la loi Informatique et libertés modifiée du 6 janvier 1978. En effet, le contrat d'adhésion prévoit qu'il est responsable du traitement de données à caractère personnel. Cela implique qu'il devra respecter les obligations de la loi, en particulier, les formalités auprès de la CNIL.

Prises de position de l'état sur le cloud

Toute décision de transférer un service, des données dans le cloud, doit être précédée d'une appréciation des risques et il est essentiel de bien négocier le contrat d'externalisation.

Dans le cas du cloud « gratuit » on est face à un contrat d'adhésion où il n'est possible de changer les clauses. De plus il faut se demander quel est la contrepartie à cette gratuité.

Pratiquement il n'est pas possible d'utiliser un cloud public a fortiori gratuit pour stocker ou traiter des informations ayant une quelconque sensibilité (toute information dont la diffusion sur Internet aurait des conséquences dommageables).

- http://www.ssi.gouv.fr/IMG/pdf/2010-12-03_Guide_externalisation.pdf guide de l'externalisation de l'ANSSI (le cloud est bien évidemment une forme d'externalisation).
- http://media.enseignementsup-recherche.gouv.fr/file/Formations_et_diplomes/48/0/Guide_IE_210480.pdf guide de l'intelligence économique pour la recherche (chapitre sur la PSSI : « le refus d'utilisation de services hébergés dans le nuage informatique » et « Contrôler et réglementer l'utilisation du *cloud computing* et l'externalisation des données du chercheur »).

Position du CNRS sur le Cloud

Le Cloud computing public présente des risques importants pour le chercheur mais aussi pour le CNRS et les autres tutelles du laboratoire, si le chercheur devait l'utiliser pour stocker des données professionnelles.

Le CNRS développe des offres de service de type Cloud privé hébergé afin d'éviter le risque du Cloud public, notamment les offres suivantes :

- Messagerie unifiée et Espaces Collaboratifs CORE
- Plates-formes de gestion de contenu Web
- Machines virtuelles packagées.