CR évènement "rencontre des adhérents de l'AFNOR" sur le Cloud Computing et la normalisation

Gérard Peliks - Cassidian

Vendredi 25 mars à l'AFNOR, j'ai assisté à un évènement qui traitait, sous divers aspects, le Cloud Computing et la normalisation.

L'AFNOR est la communauté nationale qui porte la voix de la France auprès de l'ISO pour l'établissement des normes. Une norme, établie par une organisation de normalisation d'un pays ou d'un groupe de pays est à ne pas confondre avec un standard qui est une spécification technique élaborée par un consortium piloté par des industriels tel que le W3C, l'IEEE, l'IEC, la Cloud Security Alliance (CSA).

Frédéric Degon, responsable des relations de l'AFTEL (Association Française des Editeurs de Logiciels, regroupant 250 éditeurs) précise que le Cloud Computing est un des grands enjeux de cette association depuis 18 mois, avec un groupe de travail dédié à ce nouveau modèle économique qui semble encore vaporeux. Un livre blanc de l'AFTEL pose ce qu'est aujourd'hui le Cloud Computing et établit une feuille de route pour la France.

La définition du Cloud Computing dans WikiPedia date déjà de 4 ans. Quatre grands phénomènes gravitent autour du Cloud et entrainent une massification de la demande :

L'Internet et les réseaux ;

l'industrialisation massive des nouvelles technologies accompagnée de travaux de normalisation ;

Des technologies très efficaces qui ont mené à l'émergence du Cloud Computing ;

L'évolution de la demande des entreprises.

Il y a aujourd'hui convergence entre ce que fait l'utilisateur dans sa vie personnelle et ce qu'il fait dans son entreprise dont il utilise le même type de services. Plutôt qu'une innovation de rupture, le Cloud Computing représente une évolution des technologies.

Avec ses 4 modèles de déploiement, privé, communautaire, publique et hybride, et ses 3 couches de structuration, IaaS (Infrastructure), Paas (Plateforme), SaaS (Services), le Cloud Computing se caractérise par :

La fourniture de services à la demande ;

L'utilisation des ressources où qu'on soit (ubiquité) ;

Les données pouvant être localisées à l'extérieur de l'entreprise ;

Des infrastructures disponibles même pendant les pics de demande ;

Une facturation fonction de l'utilisation.

En résumé, le Cloud Computing est un concept désignant de nouvelles pratiques et services numériques qui reposent sur l'utilisation d'Internet et des réseaux étendus et sur la mise en

commun de ressources numériques. Aujourd'hui, la confidentialité des données est le principal enjeu, suivi de la garantie de services, de la qualité de services, des problèmes de réversibilité et de la dépendance aux fournisseurs.

Au schéma traditionnel de ventes de licences au client final, le Cloud Computing introduit une nouvelle chaine de valeur avec l'IaaS pour les hébergeurs, le PaaS pour les services intermédiaires et le SaaS pour les éditeurs de logiciels.

Le SaaS est la couche de services qui aura la plus forte croissance, suivi par l'IaaS. Sur le PaaS il y aura moins de compétition. Les politiques publiques, en particulier par le grand emprunt, en France, créent des enjeux industriels très forts et un nouveau modèle économique.

L'Union Européenne définit trois priorités :

Définir un cadre réglementaire pour la protection des données sur la vie privée ;

Assurer une assise technique avec des travaux de recherche sur la sécurité et les services ;

Développer le marché avec des projets pilotes dans le secteur public

Aux Etats-Unis, le Département d'Etat a demandé aux agences d'établir un plan détaillé de basculement vers le Cloud Computing (la doctrine est décrite en www.apps.com).

Les grands enjeux sont la normalisation et la standardisation, les cadres juridiques et réglementaires, le positionnement des différents acteurs (opérateurs télécom, SSII, éditeurs) et la demande des utilisateurs. Des normes sont attendues pour la sécurité du SaaS.

Olivier Cola, responsable de la normalisation chez Microsoft France présente le groupe de l'AFNOR qui travaille sur l'établissement de normes pour le Cloud Computing :

L'ISO IEC JTC1 SC38 définit le SOA

L'ISO IEC JTC1 SC27 définit la Privacy pour la protection des données personnelles

Il y a des liaisons internationales entre ces deux groupes et des liaisons nationales entre les groupes miroirs de ces groupes. La partie télécom est plutôt prise en charge par l'ITU. Aux USA, le NIST est assez avancé sur la normalisation du Cloud Computing.

L'ISO IEC JTC1 SC38 a tenu sa première réunion plénière à Pékin en mai 2010.

La présidence est US pour le groupe de travail WG1 : Web Services et Chinoise.

Dans le WG2 : SOA, Il y a un sous groupe qui s'occupe spécifiquement du Cloud Computing sous présidence coréenne et le secrétaire est chinois. Il y a des membres venant de Chine, Canada, Finlande, France, Allemagne, Japon, Corée, Suède, UK et USA, avec entre 60 et 80 participants. Alors que la Chine et les US alignent 15 personnes, la France n'en aligne que 2 ou 3.

La prochaine session plénière se tiendra à Paris.

A noter aussi que le W3C a obtenu, pour faire avancer les normes dans les Web Services, le statut de "PAS (Public Available Specification) submitter", c'est-à-dire qu'il peut présenter des travaux de normalisation à l'ISO en tant qu'organisme, comme le fait un pays (l'AFNOR par exemple pour la France).

Le W3C pousse les protocoles interopérables pour des échanges sécurisés et fiables dans un système à couplage faible.

Voici quelques domaines où les normes pour le Cloud Computing sont en phase d'analyse : Data Services lock in, QoS, Security, Data Confidentiality and Availability, Data ownership, Privacy, Software Licensing, Legal. Le Cloud Computing donnera l'illusion du passage d'une chaine infinie CAPEX (budget d'investissement) vers OPEX (budget de fonctionnement) et éliminera le besoin de planifier sa consommation.

Un format de données pour les machines virtuelles, porté par l'ANSI (organisme représentant les Etats-Unis auprès de l'ISO) est en phase Fast Track. Le vote devrait être arrété en juillet. Une interface de gestion CDMI (Cloud Data Management Interface) devrait être proposée par le consortium SNIA. Une API de management pour le stockage des données existe mais n'est pas encore soumise.

La Commission Nationale mirroir du SC38 tiendra sa troisième session plénière à Paris en avril; Le focus de la France porte sur la sécurité et la privacy. De grands acteurs sont impliqués et quelques PME qui donnent un aperçu des problèmes quotidiens qu'elles recontrent.

Marc Flammante (IBM) vice président de la CN38 et co éditeur des standards sur la SOA (Architectures Orientées Services) prend la parole.

Dans le CN38, les Web Services sont très murs et s'appuient sur les catalogues du W3C et d'OASIS. Le SOA est à un degré de maturité moindre. La Chine est très active sur la normalisation du SoA et va imposer le résultat de ses travaux à tous les opérateurs qui opèrent dans ce pays. il y a là un réel danger d'hégémonie et de rigidité que les autres pays essaient de tempérer.

l'ISO/IEC WD TR30102 de la CN38 développe un document "General Technical Principles of Services Oriented Architecture", dont Marc Flammante est co éditeur. Beaucoup de domaines y sont décrits et un travail de revue et d'amélioration est mené. La Chine a fournit des diagrammes et des définitions, le Canada la table des matières et la Norvège sa vision engineering. Le travail est lent et se heurte à beaucoup de négociations.

Côté SOA, OASIS est le groupe qui avance le plus vite. On insiste sur la nécessité de bien définir le vocabulaire. Ainsi le mot "Service" prète à confusion. Le service SOA est une fonction programmatique alors que le service IT ne comprend pas de fournitures. L'ISO 20000 voit le service au niveau de la maitrise d'ouvrage alors que le SC38 le voit au niveau de la maîtrise d'œuvre.

Revenons à la Chine. Ils viennent nombreux dans les groupes oeuvrant sur les normes du Cloud Computing et ont des avis très tranchés tout en gardant une attitude ouverte. Ils ont peu de maturité car les participants chinois ont une moyenne d'âge d'environ 25 ans. Il faut faire attention mais la Chine représente un immense marché et c'est une bonne chose qu'ils s'impliquent dans les mouvements de normalisation.

La commission nationale (CN38) française est composée de grands acteurs, Microsoft, Thales, Hitachi Data Systems, EDF, et de deux PME (des SSII impliquées dans le Cloud).La prochaine réunion plénière se tiendra en Corée en septembre.

Eric Caprioli, **vice président de la FNTC** (Fédération Nationale des Tiers de Confiance) et avocat aux barreaux de Paris et de Nice, parle des enjeux juridiques du Cloud Computing et déclenche de nombreuses et vives remarques. Il commence par faire remarquer que lui, prend soin de mettre un soleil près du cloud, qui symbolise l'encadrement juridique qui doit

éclairer la relation entre les fournisseurs et les clients. Pour définir ce qu'est le Cloud, il s'appuie sur les quatre critères clés intervenant dans la définition faite par le Syntec :

La mutualisation des ressources

Le paiement à l'usage

La modularité

La standardisation des fonctions proposées.

En postulat, c'est au client de déterminer les données qu'il va confier au Cloud, avec les droits d'accés et le périmètre des données à externaliser. Il négocie le contrat avec le prestataire de services qui détermine avec le client le SLA (Service Level Agreement) proposé. En contrepartie des services, le client paye. C'est une abération pour le client de négocier le contrat d'abord et de s'occuper des addendum ensuite. Il ne faut signer que sur un "paquet cadeau" où rien n'est oublié, en particulier des clauses de pénalité si le SLA n'est pas respecté

Par exemple un opérateur d'importance vitale ou une banque doit prendre en compte certaines contraintes, comme les délais sur les requêtes. Il doit s'assurer qu'un PCA (plan de continuité d'activités) est mis en place par le prestataire. La convention de services doit reprendre les exigences fixées pour les opérateurs d'importance vitale par l'ANSSI.

La clause de réversibilité est fondamentale, le manque de réversibilité doit être inacceptable. Le client doit être en mesure de rapatrier chez lui, dans un délai raisonable, toutes les données confiées, sinon il peut se mettre en infraction avec les lois t les réglements, comme ceux définis par la CRBF 9702. La clause de réversibilité est importante également pour changer de prestataire. Bien sûr, à cette clause est associé un coût.

Le client doit savoir où ses données se trouvent dans le nuage …

Cette remarque entraine dans la salle de l'AFNOR de nombreuses interjections car le Cloud Computing ne rend pas cette obligation possible.

Maitre Caprioli répond que le Cloud a son comportement, mais la loi en a un autre, en particulier, lelle s'applique à l'intérieur des frontières d'un pays, donc les règles sont celles du pays où est basé le serveur qui contient les données. Si on ne sait pas où sont les données, on ne sait pas quelles lois s'appliquent et ça peut réserver de bonnes ou de beaucoup moins bonnes surprises, et les avovats ne vont pas manquer de travail concernant les problèmes qui vont se poser.

Les 27 états européens ont l'obligation de demander où se trouvent les données confiées au Cloud, et de s'assurer auprès des prestataires et des clients que les données des clients européens se trouvent bien en Europe. Dans une action judiciaire, un tribunal a une compétence territoriale, alors comme le droit est local, si vous vous demandez si vos données peuvent être hébergées n'importe où, les structures juridiques vont répondront : NIET !

D'autre part, juridiquement parlant, ce n'est pas parce qu'on mutualise ses données avec les données d'un autre client qu'on peut les mélanger alors attention à aux problèmes d'étanchéité dans un cloud mutualisé ! Concernant les formats d'échanges des données, une demande de normalisation pour définir des champs où les données ne peuvent pas aller doit être soumise pour établir une norme.

Les articles 34 et 35 de la loi Informatique et Libertéimposent de prendre toutes les précautions pour que les transferts de données respectent le cadre légal. Un manquement à

ces obligations constitue un déli pénal pouvant être puni d'une peine de 5 ans de prison (mais pas encore appliqué par les juges). Un cloud doit pouvoir rester national ou européen voire même localisé.

Des zônes où les données peuvent se trouver parce que les pays sont reconnus comme prenant des précausions suffisantes pour les données qu'ils hébergent ont été définies, ce sont les Safe Harbors. Par exemple Israël vient d'obtenir le statut de Safe Harbor.

Autres précaution qui doivent être prises d'un point de vue légal est la confidentialité des données (il faut par exemple chiffrer les données dans les serveurs de sauvegardes) et leur sécurité (il faut s'assurer que le prestataire gère bien ses systèmes d'information conformément aux normes de la famille ISO27000).

Les licences des logiciels utilisées par les prestataires de service de Cloud peuvent avoir leur importance d'un point de vue juridique. Par exemple, il faut s'assurer que le prestataire n'utilise pas pour les traitements, des logiciels "open source" dont la licence ne contamine pas les autres briques logicielles utilisées et les données manipulées.

Maitre Caprioli conclut en disant que la confiance entre le client et le prestataire ne peut s'établir que par la transparence sur le plan juridique et donc que le nuage doit être transparent pour que, en parodiant Beaudelaire, le ciel ne soit pas bas et lourd, et ne pèse pas comme un couvercle.

Bertrand Paihès du service d'expertise de la CNIL nous parle de la protection des

données personnelles.

La CNIL danoise a imposé à une municipalité de ne pas utiliser Google Apps pour traiter ses données sensibles. En France, la CNIL n'a pas encore de position officielle publiée sur l'externationalisation des données. Bertrand Pailhès rappelle que les principaux freins au Cloud Computing sont la sécurité, la réversibilité et la mise en conformité règlementaire. Il définit le Cloud Computing comme étant une infrastructure virtuelle, avec des services à la demande et accessibles de n'importe où avec une flexibilité dans les capacités de stockage.

Google Apps est utilisé aujourd'hui par plus de trois millions de clients, et on observera dans l'avenir un passage du Cloud privé au Cloud public avec des offres standards qui seront hélas difficiles à négocier.

Il est important de bien qualifier qui sont les intervenants. En France, il n'y a, pour chaque client, qu'un seul responsable des traitements mais qui peut faire éventuellement appel à des sous traitants. Le marché est concentré sur de gros acteursqui ont tendance à imposer leur offre de services (en contrepartie bien sûr que ces services ne sont pas coûteux).

En cas de problème, qui est responsable ? client ou prestataire ?

Le client est seul responsable des ses données (durée de conservation, destruction, …)

Le prestataire est responsable de leur traitement.

Les transferts de données sont interdits en dehors de l'Union Européenne, sauf vers les pays considérés comme ayant une protection adéquate des données (les Safe Harbors qui se sont engagés auprès de l'Union Européenneà respecter les données qui leur sont confiées).

L'envoi de données à caractère personnel, par exemple vers l'Iran qui n'est pas un "safe harbor", est soumis à autorisation de la CNIL.

La CNIL reconnait aussi la notion de BCR (Binding Corporate Rules) au sein d'un groupe international mais uniquement pour le transferts de données entre ses filiales.

Pour la CNIL, l'avenir du Cloud impose de :

Redonner du pouvoir aux clients qui sont responsables de leurs données

Impliquer les industriels et les prestataires

Développer des standards internationaux, en particulier dans le domaine de la sécurité et du format des données (champs rellatifs à la localisation, à la durée de conservation, …)

Utiliser le chiffrement côté client.

Des questions sont posées sur le pouvoir réel de la CNIL face aux grands groupes US, sur la compatibilité entre le Safe Harbor qui donne des obligations aux USA de repecter la confidentialité des données européennes et le Patriot Act qui leur permet d'en prendre connaissance.La CNIL répond qu'elle est en phase de réflexion pour établir un cadre et qu'elle ne souhaite pas être dans l'obligation de dire "ne faites pas cela".

Jamel Chawki, vice président de l'ITU-T focus group sur le Cloud Computing trace un historique de l'avant cloud, avec les ISP dans les années 80-90, les ASP dans les années 2000, le SaaS sur l'Internet vers 2005 et le Cloud Computing arrivant en 2008.

Son groupe présidé par un Russe existe depuis juin 2010. Deux groupes de travail sont actifs. Le WG1 qui définit les bénéfices et les demandes du Cloud et le WG2 qui réfléchi sur l'intégration entre services et réseuax et sur les métiers opérés.

Quatre documents seront discutés dans un workshop en avril à Genève :

Ecosystem taxinomy

Requirements

Cloud security

Cloud SDO analysis

La grande question qu'ils se posent est : les réseaux vont-t-ils tenir face aux flux de données qui vont grandissants ? Ce qui peut devenir problématique n'est pas les flux en période normale, mais les pics de flux.

Christian Perez de l'INRIA rappelle que le modèle SaaS et les hébergeurs de sites Web existaient bien avant le Cloud. Le modèle IaaS introduit des liens de plus en plus forts entre les fonctions demandées et les ressources offertes. Les recherches de l'INRIA concernant le Cloud Computing portent sur l'adaptabilité des applications qui tournent sur plusieurs machines avec des temps d'instabilité de l'ordre de la micro secondeet une adaptation en fonction de la charge.