Les environnements cloud

1. Qu'est-ce que le cloud computing ?

a. Ce que nous savons

Le cloud computing, ou tout simplement « le cloud », selon les personnes, c'est un peu tout et rien.

Pourquoi tout ? Parce que tout est « cloud » de nos jours. Dans certains salons technologiques, il m'est arrivé de voir qualifié de technologie « cloud » le fait d'effectuer une connexion à distance vers un serveur.

Pourquoi rien ? Simplement parce qu'en fait le périmètre de ce qu'est le cloud est en fait souvent mal compris (voire mal défini).

Alors que fait-on ? Le terme de « cloud » est en fait vague et tire son origine, dit-on, d'un ingénieur de chez IBM présentant une infrastructure de sauvegarde et réplication de stockage. Quand une personne de l'auditoire voulut savoir où se situaient les données (principales), l'ingénieur, gêné de ne pouvoir répondre précisément aurait répliqué : « it's in the cloud ! » - c'est dans le nuage - (Internet étant souvent représenté par un nuage représentant une multitude d'interconnexions sur lesquelles nous n'avons pas ou peu de maîtrise).

Est-ce une anecdote vérifiée ? Cela n'a que peu d'importance en fait, mais cela nous fera retenir une chose : une des caractéristiques des architectures pensées pour le cloud computing est le fait que les données peuvent se trouver n'importe où.

Nous n'avons pas nécessairement la connaissance précise de la situation de nos données à un instant donné. Le fait de pouvoir y accéder suffit.

Peut-on donc parler d'un ensemble de technologies de cloud computing ? Oui, c'est tentant, surtout quand on sait que le cloud permet d'obtenir des ressources informatiques très rapidement, et qu'en plus on pratique de la location et du paiement à l'utilisation. Cependant, le cloud ne peut être réduit à un empilement de technologies.

b. La définition du cloud computing

Il existe plusieurs (tentatives de) définitions du cloud computing. Certaines se rejoignent et posent un cadre assez précis sur ce qu'on sous-entend quand on parle de cloud.

Selon l'éditeur/constructeur Cisco :

Dans un environnement de cloud (computing) :

« Les **ressources informatiques** et les **services** sont **abstraits de l'infrastructure sous-jacente** et sont fournis **à la demande** et **à l'échelle** dans un **environnement partagé**. »

Si l'on s'attarde un peu sur les termes en gras :

Les ressources informatiques : on parle principalement de puissance de calcul ainsi que la mémoire nécessaire voire même du stockage. Il est difficile de dissocier puissance de calcul et mémoire vive bien qu'on puisse en général moduler la demande (plus ou moins de processeurs, une quantité de mémoire correspondant aux calculs à effectuer). Il est courant pour les fournisseurs de proposer des catégories établies selon les ensembles de demandes les plus courants. Voici un exemple de classification des machines proposées par un fournisseur de ressources informatiques (cloud computing) :

© Editions ENI – Tous droits réservés – Copie personnelle de Dirane Willy TAFEN

Type de machine	Processeur (nombre)	Mémoire vive (Go)	disque (Go)
Serveur - Bronze	1	2	40
Serveur - Silver	2	4	60
Serveur - Gold	4	8	80
Serveur - Platinum	4	16-32	100

Dans cet exemple, chaque type de serveur peut être proposé à prix compétitifs car simple à déployer. Cela n'enlève pas la possibilité de louer des machines de configuration matérielle différente dont les prix seront calculés selon le tarif unitaire du processeur virtuel, du gigaoctet de mémoire vive, du gigaoctet de stockage...

Les modèles de tarifs présentent plusieurs dimensions :

Pour les processeurs et la mémoire, on peut demander des ressources réservées ou mutualisées. En ce qui concerne le stockage, il est aussi possible d'éviter la mutualisation avec d'autres environnements. La partie stockage présente une complexité supplémentaire car il est question d'allocation / de réservation d'espace (giga, téraoctets).

Toujours concernant le stockage, la capacité et la durée ne suffisent pas à établir le montant que cela coûtera, il faut aussi prendre en compte les performances en débit et en entrées/sorties par seconde (IOPS : Input/Output Per Second). Selon le type de données stockées, les performances sous-jacentes doivent être adaptées afin d'optimiser les coûts : par exemple, il ne viendrait pas à l'idée de stocker des sauvegardes de machines / de fichiers sur des SSD...

Les services : la notion de service est plus complexe que celle de ressource informatique. La partie service comporte évidemment des ressources, mais aussi et surtout les composants logiciels à même de permettre certaines actions et/ou traitements au client.

Leur mise en place se fait à plusieurs niveaux :

- Installation et configuration (déploiement) des systèmes d'exploitation.
- Installation des applications.
- Configuration des applications.
- Personnalisation des applications afin de fournir le service demandé.
- Mise à disposition selon des paramètres les moins contraignants possible (en matière de configuration du poste de travail du client qui va utiliser les services demandés).
- Et surtout : définition, durée, conditions d'utilisation, accords de qualité de service (SLA).

Le service demandé peut être constitué d'une série d'actions et de traitements que le client doit pouvoir effectuer. Les formats d'entrée et de sortie des données font partie du cahier des charges du service demandé. La préparation de l'environnement nécessaire demande bien plus de compétences et de temps que la fourniture de ressources informatiques simples, car les applications qui ne représentent qu'un *moyen* de fournir le service doivent être maintenues et le plus possible, invisibles pour le client.

Abstraits de l'infrastructure sous-jacente : la ressource demandée n'est pas directement liée à l'infrastructure sous-jacente, et surtout le client n'en a pas connaissance. En fait, c'est assez simple à concevoir pour des professionnels de l'informatique mais il n'y a pas de lien direct entre ce qu'on peut obtenir et les produits utilisés. Il n'y a aucun besoin de connaître les technologies, les éditeurs et constructeurs pour utiliser les services offerts basés sur cette infrastructure.

En fait, l'abstraction des ressources présente un certain nombre d'avantages. Mais attention, cela entraîne

© Editions ENI – Tous droits réservés – Copie personnelle de Dirane Willy TAFEN

quelques ajustements dans notre manière de penser :

Par exemple, le fait de « louer de l'espace de stockage ». Ce cas est très répandu : on paie une somme (souvent dérisoire) par mois pour pouvoir disposer d'un espace de stockage « en ligne », sur des serveurs distants et accessibles grâce à une connexion Internet. Dans certains cas, l'accès est même gratuit !

Bien que ceci ne soit qu'un avis personnel, un service purement et simplement gratuit ne coïncide que rarement avec les intérêts des sociétés commerciales dont le but est de manière très basique le gain financier. Fournir un produit gratuit a souvent pour but (légitime) de vous donner l'envie de poursuivre et d'acheter une licence pour plus de fonctions. Dans certains autres cas, un accès complètement gratuit à du stockage ou des produits/services peut cacher un but exprimé beaucoup moins clairement : la récupération d'informations (personnelles) et de statistiques. À l'heure du Big Data, méfions-nous car très souvent nous sommes le produit !

Revenons à nos octets : un client - particulier - qui loue 50 Go d'espace disque paiera (environ 1 € par mois) pour conserver le bénéfice de ce service. Il est évident que les 50 Go d'espace sont ce qui est vendu - et obtenu, enfin plus précisément perçu du côté client. En fait, du côté de l'infrastructure, il y a déduplication et compression à l'échelle de centaines (de milliers) de clients et donc des millions voire des milliards de fichiers. Considérons que nous stockons pour la plupart les mêmes types de fichiers et il devient aisé de se rendre compte que l'espace vu par le client n'a pratiquement rien à voir avec l'espace vraiment consommé dans les centres de données du fournisseur. Pour s'approcher de la réalité, les limites de taille de fichiers, des connexions Internet et la bande passante utilisée (que ce soit au niveau du centre de données fournisseur ou de l'accès Internet client) font qu'en fait un particulier n'utilise en général que 40 à 50 % de l'espace dont il dispose.

En environnement cloud, nous n'achetons rien - en cas de fermeture du service, dans les cas favorables, le client est prévenu à l'avance et avant la fermeture effective, voire des chemins de transitions sont offerts comme la migration vers un autre prestataire partenaire, et dans d'autres, le service ferme brusquement et le temps est très limité pour récupérer ses données.

Finalement, dites-vous que quand vous payez 1 € par mois pour 50 Go, le fournisseur gagne de l'argent sur le service !

Attention : comme tout service, le fournisseur peut changer les conditions d'utilisation, ce qui a été le cas avec Microsoft Onedrive : l'espace de stockage gratuit passe de 15 go à 5 go, et l'option de stockage illimité disparaît au début 2016 comme annoncé le 2 novembre 2015 : https://blog.onedrive.com/onedrive_changes/

À la demande : la ressource est louée et disponible immédiatement pour un temps donné, à propos duquel on contracte avec le fournisseur au départ et qui peut bien sûr être prolongé et ajusté selon l'utilisation requise.

L'investissement logiciel et matériel est réduit à son minimum car une machine dotée d'un système d'exploitation moderne et une connexion Internet suffisent. La partie infrastructure et services est gérée par le fournisseur.

Le système moderne est très important : ceci est plus précisément lié au navigateur web qui est utilisé pour accéder aux interfaces d'utilisation et d'administration le cas échéant. Les prérequis en matière de sécurité conduisent à ne supporter que les navigateurs gérant les derniers algorithmes de chiffrement ainsi que les systèmes plus généralement à jour côté sécurité. Certains plug-ins et clients (tels que le Citrix Receiver) ne pourront s'installer que sur des systèmes récents. Accéder au cloud n'est pas (trop) contraignant, mais mettez les Windows XP (et 2003) à la retraite !

À l'échelle : que peut bien signifier ce terme ? Il signifie simplement qu'on peut obtenir tous les services demandés, peu importe la taille de l'environnement. Cela paraît évident (en tout cas je l'espère) mais précisons tout de même : j'ai quatre serveurs (virtuels) pour lesquels j'ai besoin d'une tolérance de panne très importante, ainsi que de la sauvegarde régulière, de la réplication et pour finir un plan de reprise sur un site distant. Je peux obtenir ce service pour mes quatre machines virtuelles (elles seront virtuelles, car c'est plus simple de fournir tous ces services), voir même pour une seule machine. La facture sera proportionnelle à la consommation de ressources

© Editions ENI – Tous droits réservés – Copie personnelle de Dirane Willy TAFEN

et au nombre et types de services que j'y associerai en tant que client.

Imaginez juste devoir acheter des produits tels que la partie hyperviseur (vSphere ESXi), la partie gestion (vCenter), le tout en licence Enterprise plus (pour la réplication, l'équilibrage de charge automatique...) ainsi que le produit VMware Site Recovery Manager sans compter la surveillance (vRealize Operations Manager), la gestion et corrélation des logs (vRealize LogInsight), etc.

En grossissant volontairement le trait, nous obtenons là un ticket d'entrée très élevé pour quelques machines virtuelles. Alors bien sûr, il convient de chiffrer le préjudice en cas d'incident si lesdites machines n'étaient pas protégées. Cependant pour une petite entreprise, déléguer la mise en place et la gestion de l'environnement sous-jacent à un spécialiste peut être assez rapidement intéressant.

De plus, le client peut théoriquement étendre le périmètre des services demandés par simple demande (enfin presque - il convient de choisir un prestataire proposant un catalogue de services afin d'éviter que toute demande soit traitée comme un cas particulier). En gros, le client a l'impression que les ressources du fournisseur sont infinies ! Est-ce vraiment le cas ? Nous répondons à cela de manière un peu abrupte certes, mais **ce n'est pas le problème du client**.

Un environnement partagé : eh oui ! Rappelons-nous que certains services ne sont « pas chers ». En même temps n'oublions pas que tout se paie, et qu'une entreprise fournissant un service est censée gagner de l'argent avec (directement ou pas, cela dépend du modèle de l'entreprise).

Bien sûr, certains fournisseurs de services cloud pour entreprises disposent d'une ou plusieurs options permettant de dédier tout ou partie de l'infrastructure (puissance de calcul, réseau, stockage), mais dans ce cas le prix est à l'avenant.

2. Tentatives de standardisation du cloud computing

Pour que chacun puisse s'y retrouver lors de discussions (formations, réunions, etc.), plusieurs caractéristiques du cloud computing ont été définies et acceptées.

Dans le précédent paragraphe, il était question de la définition du cloud par Cisco. Le NIST (*National Institute of Standards and Technology*) américain a produit une définition très précise du cloud computing (informatique en nuage ou infonuagique au Québec) qu'on retrouve dans le document suivant :http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Au-delà des caractéristiques du cloud (qui correspondent à la définition qu'en fait Cisco), on peut y trouver les différentes catégories de services fournis :

SaaS : *Software as a Service*. C'est une catégorie très représentée et surtout, facile à concevoir pour qui n'est pas informaticien. En effet c'est assez couramment utilisé : un logiciel atteignable par un simple navigateur web... Vous utilisez le logiciel et c'est tout. La complexité sous-jacente permettant d'assurer la résilience de l'application ainsi que la conservation et la protection des données est masquée. On peut citer en exemple les produits Salesforce, utilisés par la majorité des éditeurs/constructeurs et distributeurs.

PaaS : *Platform as a Service*. Là aussi, c'est assez connu. Imaginez que vous deviez installer une application pour un service ou une catégorie d'utilisateurs. Seulement, cette application est prévue pour un accès sécurisé, authentifié, de l'extérieur de la société proposant le service. Pour prendre un exemple connu - et vécu - nous dirons que l'application nécessite une infrastructure Citrix XenApp (car compatible et certifiée pour). Connaissant bien l'application, vous demanderez à votre prestataire de vous installer et configurer la plateforme Citrix. Voilà un partage des tâches tout à fait sain : chacun effectue les tâches pour lesquelles il dispose des compétences requises. Nous sommes donc dans le cas ou la plateforme est prête pour accueillir l'application. La fourniture de la plateforme est un *service*.

© Editions ENI – Tous droits réservés – Copie personnelle de Dirane Willy TAFEN

IaaS : *Infrastructure as a Service*. On vous fournit des configurations de machines pouvant communiquer en réseau (via des VLAN et routage si demandé). C'est dans ce cas au demandeur d'installer et de préparer toutes les configurations nécessaires au fonctionnement des applications prévues (à installer aussi).

Les modes de déploiement, ou types de clouds :

Public : le plus connu - tout est en ligne, et ailleurs, par rapport aux infrastructures propres à l'entreprise le cas échéant. Ne confondons pas avec du cloud externe qui ne concerne que la localisation des infrastructures. On parle ici de service public, accessible et partagé par tous.

Communautaire : c'est une sorte de cloud public aussi, mais comportant une ou des restrictions assez intéressantes, car clivantes. Il s'agit de gérer des machines, applications correspondant à un certain type de données. Par exemple un environnement spécialisé pour héberger des données concernant la santé des personnes. Cela tombe bien, car ce n'est pas simple : des certifications et accréditations sont nécessaires !

Nuançons tout de même : un cloud accrédité pour un type de données n'est pas obligatoirement spécialisé mais il convient d'avoir des sections dédiées pour ces types de données.

Pour exemple, vous pouvez consulter le site du groupe Diademys, qui a obtenu l'agrément permettant d'héberger des données de santé officialisé le 5 novembre 2015 : http://www.diademys.com/agrement-asip/

Plus généralement, voici la liste des hébergeurs agréés de données de santé à caractère personnel (en général à des fins de suivi médical) : http://esante.gouv.fr/services/referentiels/securite/hebergeurs-agrees

Privé : le cloud privé. C'est tout simplement toute une infrastructure de cloud computing avec tous les services associés qui est restreinte à une entreprise ou plus généralement à un groupe dont les filiales se servent selon leur activité.

Hybride : le fameux hybride, celui dont tout le monde parle. Si vous avez suivi les annonces des fournisseurs d'infrastructures, produits et solutions technologiques liées au cloud computing, vous avez sans doute remarqué que l'interopérabilité est le sujet principal de ces derniers temps. Pourquoi ? Sans prétendre pouvoir tout expliquer, les modèles de cloud public et cloud privés sont souvent perçus comme antinomiques. Cependant, c'est loin d'être le cas, ne serait-ce que pour utiliser les avantages des deux types de clouds : un privé pour les données et services de l'entreprise et une utilisation de cloud public pour héberger des services proposés à des partenaires, pour manipuler des données à caractère non confidentiel, ou enfin pour faire face à un pic d'activité. Le cloud public peut aussi servir de dernier recours pour un plan de reprise d'activité.

Depuis, les services ont évolué et on voit apparaître d'autres types de services :

MSaaS : *Managed Security as as Service*.

STaaS : *Storage as a Service* (par exemple l'offre glacier chez AWS - *Amazon Web Services*).

DaaS : *Desktop as a Service* : bureau virtuel fourni grâce aux produits de type VDI tels que Citrix XenDesktop, Oracle Secure Global Desktop ou VMware View.

Et même **BADaaS** : *Business Automation and Development as a Service*, pour la création automatisée de plateformes de développement. Pour plus d'informations, consultez la page suivante : https://community.servicenow.com/community/blogs/blog/2013/12/19/2623

En ce qui concerne les types de clouds, l'avenir est clairement dans le cloud hybride qui finalement est pour beaucoup d'éditeurs le seul type de déploiement à même de répondre aux problématiques business, de sécurité, d'utilisation (au sens large) des entreprises. On évite aussi le « vendor lock-in », soit le fait de s'enfermer dans les technologies provenant d'un seul éditeur.

© Editions ENI – Tous droits réservés – Copie personnelle de Dirane Willy TAFEN

Le vendor lock-in, qu'on peut traduire par verrouillage éditeur, est en fait une notion connue. On essaie de l'éviter dans la mesure du possible même si les éditeurs proposent de plus en plus de technologies et services interopérables. Il n'est pas rare de trouver des plateformes opérées par les technologies d'un éditeur en majorité (par exemple Microsoft Hyper-V pour la virtualisation de serveurs, Microsoft VDI pour la virtualisation de poste de travail, Microsoft SQL pour les bases de données, Microsoft Dynamics pour le CRM - Customer Relationship Management et L'ERP - Enterprise Resource Planning. Le vendor lock-in représente aussi l'impossibilité de changer certaines briques technologiques du fait des adhérences avec les autres (provenant du même éditeur).

Considérez d'autres types de service, clairement pas standards, mais non moins intéressants :

HaaS : *Hacking as a Service* : malheureusement, il s'agit bien de ce que vous pensez en lisant cela, des services proposés permettant de s'attaquer à des entreprises. Le but étant souvent d'obtenir des informations ayant une valeur pécuniaire, en général sur le « darknet ».

DDoS as a Service : *Distributed Denial of Service* - comme service. Il s'agit d'attaques distribuées de déni de service, dont le but est de bloquer certains sites ou services en utilisant des flux de requêtes simultanées. Le but étant de paralyser un système (un exemple de la vie courante est l'attaque des services Playstation Network et Xbox Live en décembre 2014).

Le cloud a apporté son lot de commodités qui sont utilisées par les entreprises, les particuliers, mais n'oublions pas que les pirates en profitent aussi.

Les challenges d'aujourd'hui portent sur la sécurisation des environnements cloud computing.

3. Des exemples de plateformes

Les plateformes de cloud computing sont basées sur les produits suivants :

VMware

vCloud Director

C'est le premier produit de gestion d'environnement cloud de l'éditeur VMware. Aujourd'hui il est réservé aux fournisseurs de services. Pour tous les autres cas (notamment les entreprises qui n'utilisaient pas vCloud Director) vRA est le produit à utiliser.

vRealize Automation, ou vRA, est le nouveau nom de vCAC ou vCloud Automation Center. vRA est compatible avec les configurations multihyperviseurs et les outils de configuration tels que Puppet et Chef.

vCloud Air : anciennement vCloud Hybrid Service. C'est la plateforme de cloud public de VMware. Qui vient d'être racheter par OVH (avril 2017).

Amazon Web Services

EC2 : *Elastic compute cloud*. C'est le service d'hébergement de machines et plateformes d'Amazon. Il est possible d'exécuter différentes applications et de contrôler leur coût et leur localisation grâce aux différentes « régions » où sont situés les centres de données du service.

S3 : *Simple Storage Service*. Il s'agit des services de stockage en ligne d'Amazon Web Services. Les espaces de stockage sont la plupart du temps utilisés par d'autres éditeurs et fournisseurs de services, comme par exemple Citrix proposant Sharefile - un service de stockage et synchronisation de fichiers en ligne - qui s'appuie sur S3.

Les services d'Amazon Web Services sont spécialisés dans le cloud public. La plupart des autres produits et

© Editions ENI – Tous droits réservés – Copie personnelle de Dirane Willy TAFEN

infrastructures de cloud (privé) utilisent les API et connecteurs mis à disposition afin d'étendre leur compatibilité vers AWS.

Microsoft

Azure permet, comme les autres services de cloud, de faire fonctionner une partie de l'IT directement dans le nuage et l'interconnexion avec l'infrastructure interne. Les applications en SaaS étaient fournies à l'aide de RemoteApp, mais à partir de septembre 2017 c'est le produit Citrix XenApp Express et donc le protocole de déport d'affichage ICA /HDX de Citrix qui sera utilisé dans le cloud public de Microsoft : http://www.silicon.fr/microsoft-azure-remoteapp-citrix-xenapp-express-155635.html

Azure pack : permet de proposer un portail de gestion et d'accès aux ressources en libre-service au sein du datacenter de l'entreprise.

System Center : la plateforme System Center, couplée à Hyper-V, permet de créer et d'opérer du cloud privé.

Google

Cloud Platform : https://cloud.google.com. La plateforme de Google permet, en plus des outils similaires aux autres plateformes, d'utiliser leur API de traduction et comporte un service spécialisé dans les conteneurs pour applications web.

Apache

Cloudstack : https://cloudstack.apache.org

Apache Cloudstack est une plateforme de cloud public, privé et hybride (via la compatibilité avec Amazon EC2).

Citrix propose avec Cloud Platform une implémentation d'Apache Cloudstack permettant de gérer des infrastructures de cloud privé/hybrides.

Openstack : http://www.openstack.org

Openstack est un ensemble de projets liés permettant d'opérer des infrastructures IaaS. Une fondation (organisation non commerciale) a été créée afin d'aider et supporter les développements. De nombreuses sociétés font partie de la fondation Openstack : Intel, VMware, NetApp, Cisco, HP, Dell, Red Hat...

La compatibilité avec Amazon EC2 et S3 est assurée via des API permettant des adaptations rapides des applications d'une plateforme à l'autre.

Openstack est utilisé aussi bien pour les clouds publics que privés. VMware propose une distribution Openstack, nommée VIO pour *VMware Integrated Openstack* qui contient les connecteurs et pilotes afin de mettre en relation les projets Openstack et les produits et services VMware : https://www.vmware.com/support/pubs/integrated-openstack-pubs.html

© Editions ENI – Tous droits réservés – Copie personnelle de Dirane Willy TAFEN