POLYTECH LYON

Veille Technologique

Livre Blanc

Mai 2012

La sécurité et la virtualisation

David GELIBERT
Farid SMILI
Jérôme DEROCK
Loïc RATSIHORIMANANA
Mickaël DREYER
Thomas GERVAISE

Sommaire

Table des illustrations

Introduction

Conquis par les capacités apportées par les outils de virtualisation, de nombreux responsables informatiques se tournent vers cette technologie. En effet, ce procédé permet de configurer une machine physique en y installant plusieurs machines virtuelles. Ainsi, on a la possibilité d'utiliser plusieurs systèmes d'exploitation sur une même machine. Mais c'est surtout pour les serveurs que cette technologie prend toute son importance en optimisant la capacité et la puissance. En réalité, ce n'est pas tant la virtualisation en elle-même qui attire ces entreprises, mais plutôt un nouveau concept : « l'informatique dans les nuages », couramment appelé « le cloud computing ». Ce principe offre à ses utilisateurs un moyen simple de stocker des données à la demande mais également d'effectuer des traitements informatiques lourds. La virtualisation n'est que le moyen de mettre au point une solution cloud.

Cependant aucun système n'est infaillible, surtout en informatique. Le premier frein à l'adoption du cloud a trait à la sécurité de leurs informations, comme on peut le voir à travers des exemples de failles aujourd'hui nombreux (Sony, Amazon…). Désormais, Il faut en plus penser aux problèmes concernant les contraintes d'accessibilité et la dépendance au réseau. Et au-delà de la notion de confiance qu'on accorde au cloud computing, le problème du regroupement et du cryptage des informations est, lui, bien réel.

Face à cette tendance à vouloir adopter le cloud computing, plusieurs questions peuvent être soulevées : comment peut-on définir le cloud computing ? Quels modèles et solutions existent ? Pourquoi la virtualisation et le cloud sont des outils attractifs pour les entreprises et quelles en sont les limites ? Comment assurer l'intégrité des données ? Comment fiabiliser l'accès et les échanges de données ?

Pour cela, nous allons dans un premier temps présenter en détail les concepts de la virtualisation et du cloud computing. Ensuite, nous aborderons en détail l'aspect sécurité et enfin nous analyserons les prospectives dans ce domaine.

Ce document rassemble donc de nombreux éléments permettant de comprendre ce qu'est le cloud computing, avec quelles technologies il fonctionne, la valeur ajoutée apportée aux entreprises mais également les risques liés à son utilisation. Il présente aussi les problématiques de sécurité et les solutions existantes.

Ce livre blanc a été rédigé en mai 2012 par un groupe d'étudiants en quatrième année d'informatique à l'école Polytech Lyon (http://polytech.univ-lyon1.fr/).

I – La virtualisation et le cloud computing

1) La virtualisation

Depuis quelques années, les entreprises s'intéressent de plus en plus aux technologies de virtualisation. Bien que ce concept ne soit pas nouveau, de nombreuses solutions sont actuellement mises en œuvre autour de la virtualisation.

a) Définition de la virtualisation

La virtualisation est un ensemble de techniques matérielles et/ou logicielles qui autorisent l'exécution de plusieurs applications indépendantes sur une même machine hôte. Grâce à la virtualisation, il est possible d'exécuter plusieurs systèmes d'exploitation (OS invité) sur un même serveur (**Figure 1**). Ainsi, il n'est plus nécessaire d'utiliser un serveur par application. On parle souvent d'environnement virtuel (*Virtual Environment* – VE) ou de serveur privé virtuel (*Virtual Private Server* – VPS) lorsqu'une machine exploite la virtualisation. Pour bénéficier de cette technologie, il suffit d'équiper une machine d'un logiciel de virtualisation permettant d'ajouter une couche de virtualisation, appelée hyperviseur. Cet hyperviseur masque les véritables ressources physiques de la machine afin de proposer des ressources différentes et spécifiques en fonction des applications qui tournent. Il y a donc une totale indépendance entre le matériel et les applications. Le logiciel de virtualisation simule autant de machines virtuelles que de systèmes d'exploitation souhaité. Chaque OS croit alors qu'il est installé seul sur une machine alors qu'en réalité, plusieurs OS peuvent fonctionner en parallèle en partageant les mêmes ressources.

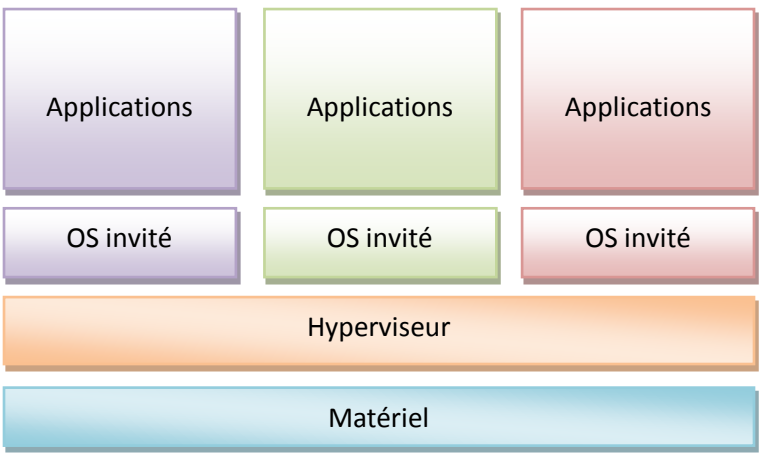

Figure 1 : Les différentes couches d'un serveur virtualisé

b) Les différents types de virtualisation

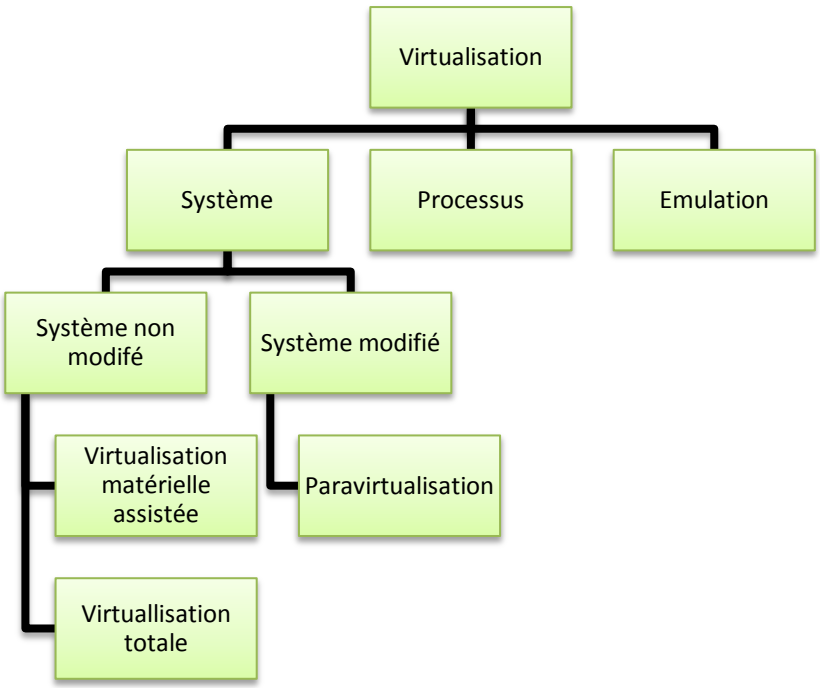

Figure 2 : Les différents types de virtualisation
Source : schéma inspiré du billet de blog http://www.antoinebenkemoun.fr

Le schéma (Figure 2) ci-dessus montre un aperçu des principaux types de virtualisation.

La virtualisation système a pour rôle de virtualiser un système d'exploitation. On peut distinguer deux catégories :

- Les systèmes non-modifiés : c'est le type de virtualisation le plus utilisé aujourd'hui. VMware, VirtualPc, VirtualBox et bien d'autres appartiennent à cette catégorie. On distingue la virtualisation matérielle assistée de la virtualisation totale car cette dernière est améliorée grâce aux processeurs Intel-V et AMD-V qui implantent la virtualisation matérielle dans leurs produits.
- Les systèmes modifiés : la virtualisation nécessite de modifier et d'adapter le noyau d'un système (Linux, BSD, Solaris). On parle alors de paravirtualisation.

Contrairement à la virtualisation système, la virtualisation processus ne virtualise pas l'intégralité d'un système d'exploitation mais uniquement un programme particulier au sein de son environnement.

Enfin, il y a l'émulation qui est une imitation du comportement physique d'un matériel par un logiciel.

c) Evolution de la virtualisation

Le concept de virtualisation est apparu autour des années 1960 lorsque des entreprises telles que IBM ont souhaité partitionner les ressources des mainframes (un mainframe ou ordinateur central est un ordinateur de grande puissance de traitement).

La virtualisation a perdu tout son intérêt dans les années 1980 – 1990 bien que certains projets comme Amiga, SideCar ou encore Enplant ont essayé d'exploiter cette technologie. En effet, durant cette période, les systèmes client-serveur sont à la mode. Mais les problèmes de protection en cas de panne ainsi que le coût important de la maintenance des serveurs et des stations clientes seront des limites pour cette architecture à deux niveaux.

Au milieu des années 1990, les émulateurs connaissent un réel succès (ordinateurs Atari, Amiga ; consoles NES).

Ce n'est qu'au début des années 2000 que la virtualisation devient célèbre grâce à la société VMware qui développe des logiciels pour des serveurs de type x86.

En 2003 apparait la para-virtualisation avec Xen.

A partir de 2005, les fabricants de processeurs Intel et AMD implantent la virtualisation matérielle dans leurs produits.

En 2007, les machines virtuelles KVM (*Kernel-based Virtual Machine*) débarquent sur Linux.

Jusqu'alors, la virtualisation était utilisée pour tester des systèmes d'information avant leur déploiement.

A partir de 2007 arrive la virtualisation 2.0. Cette seconde génération a pour objectif de consolider les applications de production.

En 2008, Microsoft met sur le marché son logiciel de virtualisation Hyper-V.

Depuis peu, le monde informatique connait une nouvelle mutation avec la virtualisation 3.0, utilisée principalement dans les technologies liées au cloud computing et à la gestion automatisée des déploiements internes.

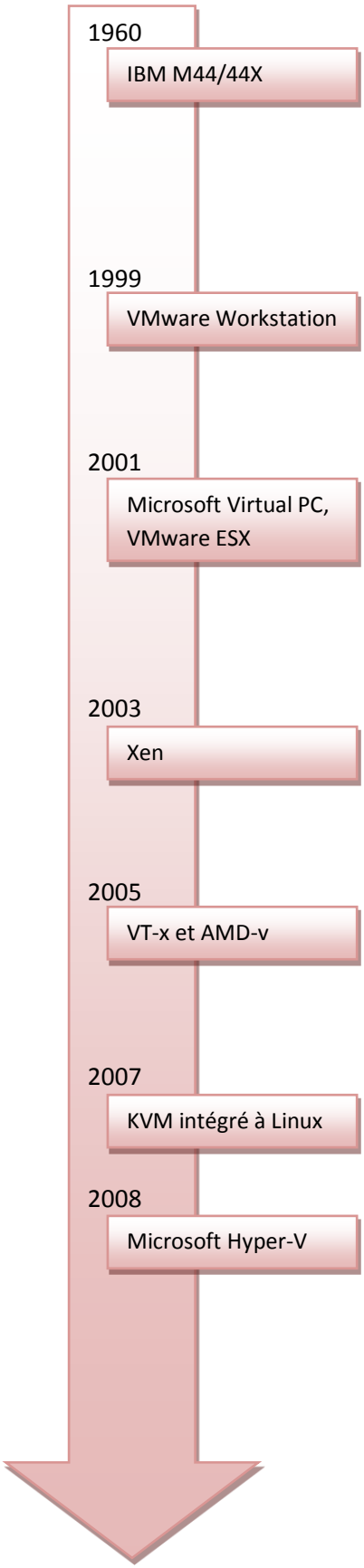

Figure 3 : Historique de la virtualisation

d) Les acteurs de la virtualisation

Actuellement, le leader mondial de la virtualisation est VMware avec plus de 65% de parts de marché grâce à ses solutions d'hyperviseurs comme ESX/ESXi et grâce à VSphere qui sert à déployer des infrastructures cloud de façon plus aisée. Le géant Microsoft ne se retrouve qu'en deuxième position, loin derrière VMware avec environ 27% de part de marché grâce à Hyper-V qui constitue sa solution de virtualisation intégrée de base à Windows server 2008 R2. Avec 6% de parts de marché, Citrix se place en troisième position derrière Microsoft, sa solution quant à elle est l'hyperviseur XenServer qui diffère des deux solutions suscitée car elle repose sur la technologie de la para-virtualisation au lieu de reposer sur la virtualisation totale. Il y a également d'autres acteurs comme Parallels ou Red Hat. Spécifions à présent les fonctionnalités des deux principaux acteurs en commençant par la solution de VMware.

VMware ESX/ESXi:

Fonctionnalité	VMware ESX 4.1	VMware ESXi 4.1	ESXi 5.0
Console de service	Oui	Suppression	Suppression
Admin/config. des CLI	COS + vCLI	PowerCLI + vCLI	PowerCLI + vCLI (améliorée)
Dépannage avancé	COS	Mode prise en charge technique	ESXi Shell
Installation au moyen de script	Prise en charge	Prise en charge	Prise en charge
Démarrage à partir du SAN	Prise en charge	Prise en charge	Prise en charge
SNMP	Prise en charge	Prise en charge (restrictions)	Prise en charge
Active Directory	Intégrée	Intégrée	Intégrée
Contrôle du HW	Agents tiers dans COS	Fournisseurs CIM	Fournisseurs CIM
Connectivité des ports série	Prise en charge	Pas de prise en charge	Pas de prise en charge
Trames étendues	Prise en charge	Prise en charge	Prise en charge
Déploiement rapide et gestion centrale des hôtes via Auto Deploy	Pas de prise en charge	Pas de prise en charge	Prise en charge
Création et gestion d'images personnalisées	Pas de prise en charge	Pas de prise en charge	Prise en charge
Fonctionnalité syslog sécurisée	Pas de prise en charge	Pas de prise en charge	Prise en charge
Pare-feu d'interface de gestion	Prise en charge	Pas de prise en charge	Prise en charge

Figure 4 : Comparaison des fonctionnalités des versions d'ESX
Source : http://www.vmware.com/fr/products/datacenter-virtualization/vsphere/esxi-and-esx/compare.html

Microsoft Hyper-V R2:

	Virtualization Needs	Microsoft Hyper-V Server 2008 R2	Windows Server 2008 R2 Standard	Windows Server 2008 R2 Enterprise	Windows Server 2008 R2 Datacenter
Scenarios	Server Consolidation	✔	✔	✔	✔
	Test and Development	✔	✔	✔	✔
	Branch Server Consolidation	✔	✔	✔	✔
	Virtual Desktop Infrastructure (VDI)	✔		✔	✔
	Mixed OS virtualization (Linux and Windows)	✔	✔	✔	✔
	Dynamic Data Center			✔	✔
Features	Host Clustering	✔		✔	✔
	Live Migration	✔		✔	✔
	Large Memory support (Host OS) > 32GB	✔		✔	✔
	Support for >4 Processors (Host OS)	✔		✔	✔
	Local Graphical User Interface		✔	✔	✔
	Ability to Add Additional Server Roles		✔	✔	✔
	Guest Virtualization Rights Included in Host Server License		✔	✔	✔
	Application Failover			✔	✔

Figure 5 : Comparatif des fonctionnalités de virtualisation pour les différentes versions de Windows Server 2008
Source : http://www.microsoft.com

e) Les objectifs de la virtualisation

L'un des objectifs clés de la virtualisation est la réduction des coûts. Cette réduction s'explique par la mutualisation des ressources qui permet de diminuer d'une part les besoins en matériel et de réduire d'autre part la consommation d'énergie électrique. De plus, le regroupement de plusieurs serveurs sur une même machine physique est sans perte de performance. En effet, la plupart des serveurs en entreprise n'exploitent qu'environ 10 à 15 % des ressources matérielles (**Figure 6**). La virtualisation offre également un déploiement et une migration facile des machines virtuelles d'une machine physique à une autre. L'administration des serveurs et des postes de travail devient aussi plus aisée.

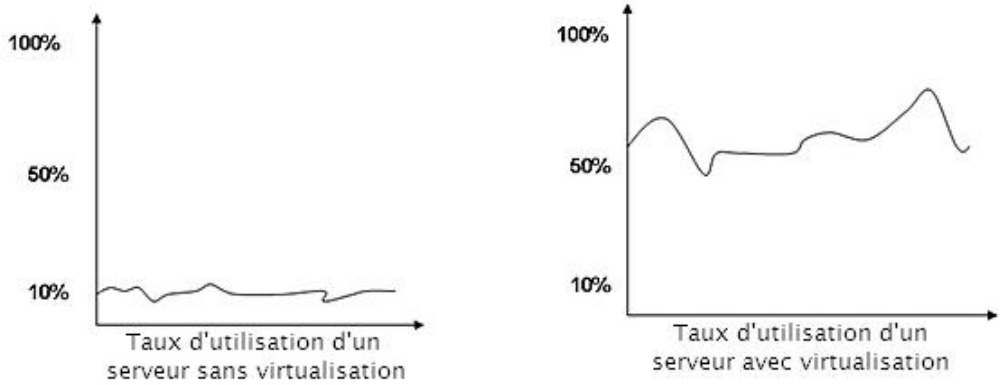

Figure 6 : Taux d'utilisation des serveurs
Source : http://magicgg.fr/blog/article-virtualisation-156

2) Le cloud computing

a) Définition du cloud computing

L'informatique dans les nuages, connue sous le nom de « cloud computing » est un concept informatique récent qui vise à décrire un ensemble de techniques utilisées pour délivrer des capacités informatiques en tant que services.
Ce procédé interconnecte et met en coopération des ressources informatiques au sein d'une même entité, ou bien au sein de structures externes comme une solution de serveur mail que l'on aurait externalisée et qui serait gérée par un tiers.
Pour fonctionner, le cloud s'appuie sur les technologies de la virtualisation et d'automatisation. Les protocoles et les standards Internet sont utilisés comme base pour les modes d'accès.

Après les mainframes dans les années 1970, le concept Client-Serveur dans les années 1980, le Web en 1990 et l'architecture orientée services en 2000 le cloud computing devient la cinquième génération d'architecture informatique.

b) Les caractéristiques d'un cloud

Une architecture dite cloud possède plusieurs caractéristiques principales :

- Elle offre un service mesuré qui peut être facturé à l'usage, en fonction de ce que l'on consomme. C'est donc un libre-service à la demande.

- Elle offre une accessibilité via le réseau par des clients variés, c'est à dire par des architectures hétérogènes.

- Elle offre une mise en commun des ressources, si deux services d'une entreprise utilisent le même logiciel de comptabilité, ils partageront le service cloud « comptabilité » de l'entreprise. Cette ressource sera donc mise en commun entre plusieurs utilisateurs.

- Elle offre une élasticité permettant d'adapter facilement le service, que ce soit en taille de stockage ou bien en puissance. En effet, il y a mutualisation et allocation dynamique de capacité (adaptation flexible aux pics de charge).

- Elle offre des services au lieu de logiciels techniques avec une mise à jour régulière et automatique.

c) Les différents modèles de service du cloud

Le cloud computing est divisé en quatre grands modèles de services :

- Le **Software-as-a-Service** (SaaS) fournit un logiciel à la demande mais ce dernier reste sur le cloud. Par exemple, on peut mettre une suite bureautique sur le cloud.
  Par exemple : Google Apps, Office 365, Salesforce.com, etc…

- Le **Platform-as-a-Service** (PaaS) fournit une plateforme logicielle qui va servir à développer une solution cloud computing. Par exemple, un serveur d'application web que l'on aurait porté sur le cloud.
  Par exemple : Microsoft Azure, Google App Engine, etc…

- L'**Infrastructure-as-a-Service** (IaaS) fournit une infrastructure qui va servir à développer des solutions cloud computing. Il peut s'agir d'un hébergeur de site web, une entreprise qui va se charger de faire fonctionner le site pendant que le propriétaire du site se chargera du contenu.
  Par exemple : Microsoft Azure, les hébergeurs de systèmes, les fournisseurs de machines virtualisées, etc…

- Le **Data-as-a-Service** (DaaS) fournit une solution de stockage à distance.
  Par exemple : Google Docs, iCloud, etc…

d) Les différents modèles de déploiement du cloud

Quatre grandes familles de cloud existent en fonction du mode de déploiement :

- Le **cloud privé** est réservé pour un usage interne. Soit la solution cloud est interne, dans ce cas, l'entreprise est propriétaire. Soit la solution cloud est basée sur une location entre l'entreprise et le fournisseur.

- Le **cloud public** est réservé pour un usage externe. La solution est fournie à toute catégorie d'utilisateur. L'infrastructure quant à elle reste à la charge de l'entreprise qui propose les services.

- Le **cloud communautaire** est une solution cloud partagée entre plusieurs organisations d'une même communauté (un Etat par exemple). Cette solution peut être gérée en interne ou bien en externe, via un tiers.

- Le **cloud hybride** est une solution formée à partir de deux ou plusieurs modèles de déploiement cloud.

e) Les avantages offerts par le cloud

En adoptant le cloud computing, une entreprise peut retirer de nombreux avantages technologiques.

- Déploiement facilité : les responsables d'applications ont accès à des plateformes en libre-service afin d'approvisionner leur infrastructure en seulement quelques clics de souris. Ils peuvent également répartir la charge entre les serveurs de manière simple et rapide.

- Gestion facilitée et évolutivité améliorée : le cloud computing permet aussi une certaine évolutivité dynamique. Par exemple, il est tout à fait envisageable d'ajouter à chaud un processeur et d'augmenter de la mémoire sur une machine virtuelle. Il est également possible de faire migrer à la volée une machine virtuelle d'un hôte vers un autre.

3) L'utilisation des technologies du cloud

a) Qui utilise le cloud computing ?

D'après une étude réalisée par la société Management Insight Technologies en décembre 2010, il ressort que plus de 85% des entreprises utilisent au moins un service du cloud computing (Figure 7). Cette étude a été menée auprès des entreprises américaines et européennes. Ces entreprises utilisent également en moyenne six services différents du cloud computing.

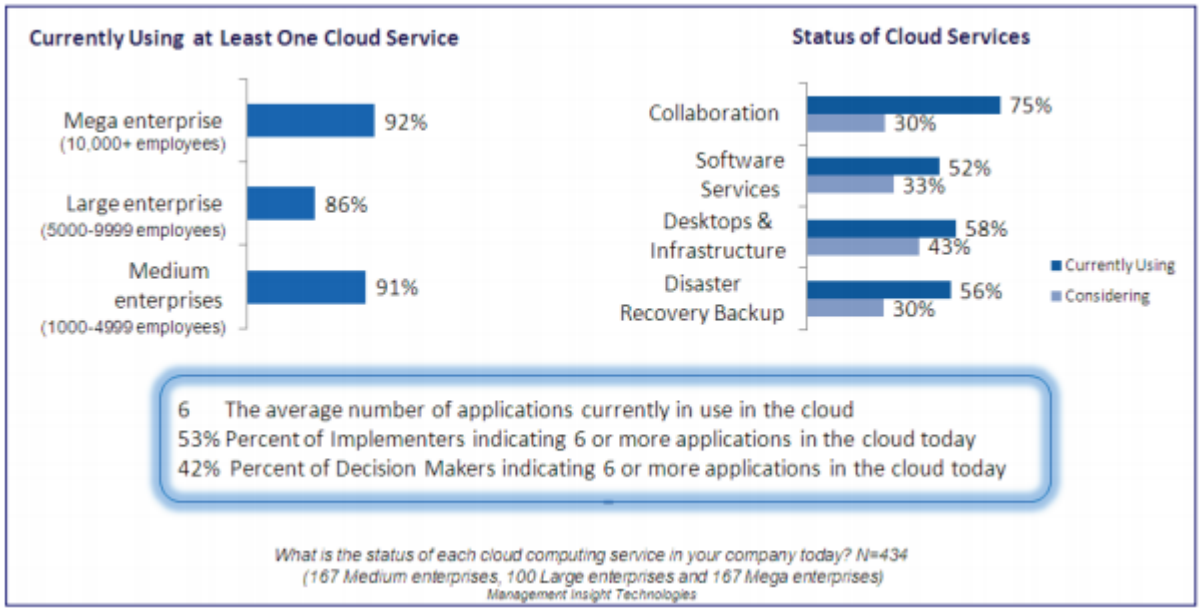

Figure 7 : L'utilisation du cloud computing en 2010
Source : http://www.ca.com/~/media/Files/whitepapers/the_arrival_of_cloud_thinking.pdf

Toujours d'après cette étude, presque un responsable informatique sur deux déclare avoir investi dans le cloud computing pour son entreprise dans le but de réduire les coûts. Pour 68% d'entre eux, la sécurité des informations demeure un frein majeur pour cet investissement.

b) Les parts de marché de la virtualisation

En octobre 2008, le cabinet Gartner a diffusé ses chiffres sur le marché de la virtualisation (**Figure 8**). VMware domine le marché avec 89% des parts du marché. Microsoft qui est pourtant un géant de l'informatique ne possède que 7% des parts de marché avec son logiciel Hyper-V. Suivent derrière d'autres logiciels tels que Citrix, Oracle ou Virtual Iron.

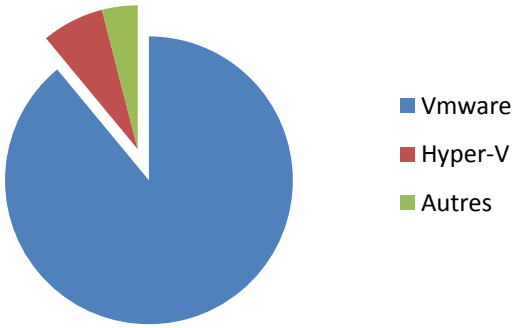

Figure 8 : Répartition de la part de marché des hyperviseurs en 2008
Source : http://www.gartner.com

A la fin du second semestre de l'année 2011, les plateformes open-source de cloud computing BitNami, Cloud.com et Zenoss ont réalisé ensemble une enquête à propos du cloud. Concernant l'usage des logiciels de virtualisation (**Figure 9**), 61% des directeurs de systèmes d'information utilisent l'hyperviseur VMware. Hyper-V est utilisé à hauteur de 14%. Des logiciels open sources comme Xen ou KVM sont également de plus en plus utilisés dans les entreprises.

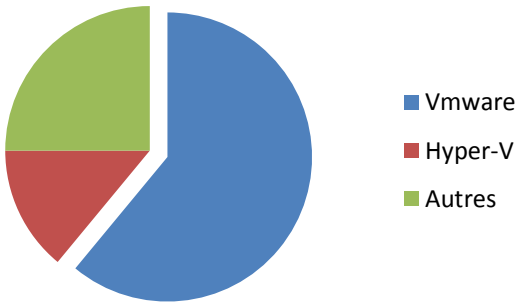

Figure 9 : Répartition de la part de marché des hyperviseurs en 2011
Source : http://www.cloud.com

c) Le SaaS : un modèle de service qui plait aux entreprises

Afin de savoir quel modèle de service du cloud computing est privilégié par les entreprises, le cabinet d'études Markess International a réalisé un sondage en mars 2011 auprès de 75 entreprises françaises. Les chiffres indiquent une demande importante du Software-as-a-Service (SaaS) de la part des entreprises (**Figure 10**) et en particulier des petites et moyennes entreprises (PME) et des très petites entreprises (TPE).

	Demande soutenue de SaaS	**Demande moyenne de SaaS**	**Demande faible de SaaS**
Grandes entreprises (supérieur à 5000 employés)	31%	61%	8%
Entreprises de taille intermédiaire (250 à 5000 employés)	39%	57%	4%
PME (10 à 249 employés)	49%	49%	2%
TPE (moins de 10 employés)	44%	35%	21%

Figure 10 : Perception vis-à-vis de la demande des entreprises françaises en SaaS en 2011
Source : http://www.markess.fr

En ce qui concerne le Platform-as-a-Service (PaaS) et l'Infrastructure-as-a-Service (IaaS), ce sont les grandes entreprises qui ont le plus recourt à ces services (**Figure 11**). Les TPE sont ceux qui accordent le moins d'intérêt à ce modèle de service. En effet, les TPE privilégient davantage les solutions SaaS du cloud computing.

	Demande soutenue	**Demande moyenne**	**Demande faible**
Grandes entreprises (supérieur à 5000 employés)	33%	59%	8%
Entreprises de taille intermédiaire (250 à 5000 employés)	23%	71%	6%
PME (10 à 249 employés)	26%	51%	23%
TPE (moins de 10 employés)	19%	19%	61%

Figure 11 : Perception face à la demande des entreprises françaises en IaaS et PaaS en 2011
Source : http://www.markess.fr

d) Les enjeux du cloud computing

Les enjeux du cloud computing sont importants : plus d'un cinquième du budget informatique serait consacré à lui dans les entreprises en 2012. De plus, il donne à tous des avantages compétitifs non négligeables dans plusieurs domaines.

Le cloud étant une technologie encore jeune, beaucoup voit en lui de nouvelles occasions d'innover et de changer la vision de leur travail. D'après un sondage de KPMG en décembre 2011 : « *88 % des entreprises interrogées pensent que le cloud va transformer leur business et la façon dont elles exercent leurs activités : 50 % d'entre elles estiment que cela va permettre de réduire leurs coûts, 39 % que cette technologie va modifier leurs interactions avec leurs clients et leurs fournisseurs et 32 % que cela va changer fondamentalement leur modèle économique.*»

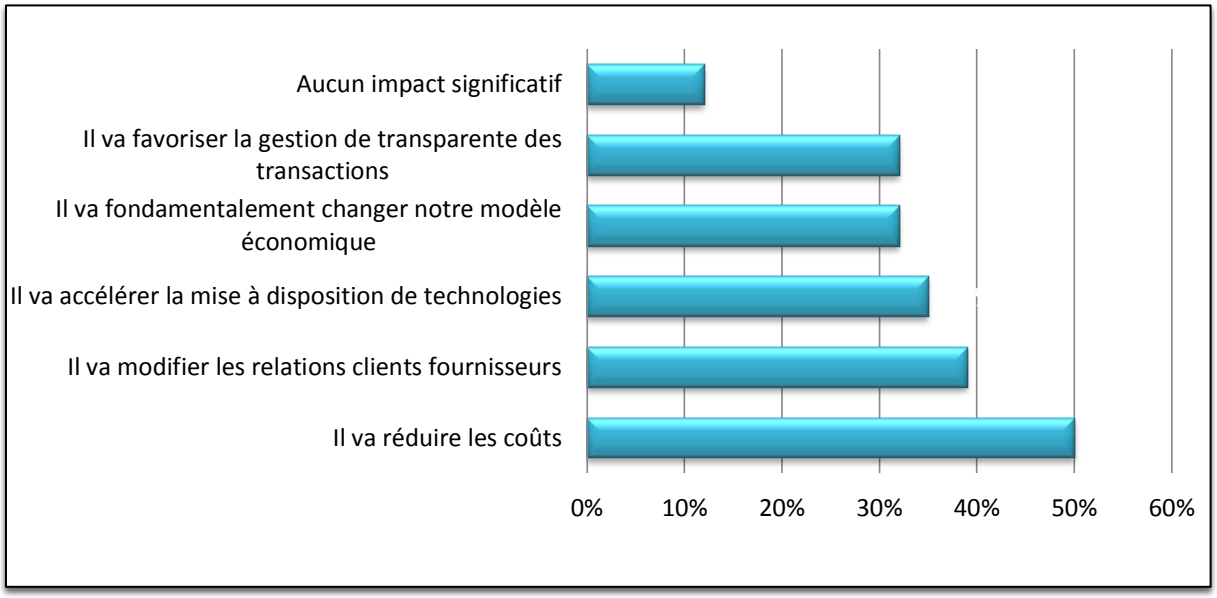

Figure 12 : L'impact du cloud sur le modèle économique des entreprises
Source : http://www.widoobiz.com/actualites/les-entreprises-ont-les-pieds-sur-terre-et-l%E2%80%99informatique-dans-les-nuages/13178

La majeure partie du temps, le cloud évoque dans les entreprises la rapidité, l'accessibilité, les multiples fonctionnalités que cette nouvelle technologie peut apporter (83% des entreprises françaises et 80% en général). Les économies d'échelles sont également un sujet principal selon 74 % en France et 76 % dans le monde, des prestataires de services et des autres fonctions interrogées. Enfin, la rationalisation des processus dans les entreprises va être considérablement augmentée (86 % France et 76 % monde).

Pour finir, nous allons parler d'énergie. L'opérateur téléphonique américain AT&T a cherché à les calculer pour promouvoir ses solutions de cloud computing (informatique mutualisée en nuage). Une économie de 830 millions d'euros par an d'ici 2020 pourrait être faite si le cloud computing était adopté dans les 215 plus grandes entreprises françaises. L'émission de 1,2 million de tonnes de carbone par an pourrait également être évitée. Selon AT&T, l'informatique en nuage permet d' « *éviter d'immobiliser des capitaux importants dans les infrastructures, d'offrir une meilleure flexibilité, d'éviter la maintenance continue et de diminuer le temps nécessaire de mise sur le marché - un nouveau serveur peut être activé en quelques minutes* ». (**Source : http://www.usinenouvelle.com/article/le-cloud-computing-source-d-economies-pour-les-groupes-francais.N162350**)

e) La législation

Avec la venue du cloud computing, une entreprise ne peut plus se contenter d'un simple pare-feu pour protéger ses données et ses services. En effet, dès lors qu'on fait appel à un fournisseur comme Amazon ou Microsoft, de nouveaux risques de conformité voient le jour. Aujourd'hui, le cloud computing n'est pas juridiquement bien encadré, pour ce qui est de la disponibilité, la conformité légale, la confidentialité et la sécurité des données.

Les services proposés par un fournisseur de cloud computing incluent forcément le traitement de données personnelles dans un cadre régional, national ou international. Le client doit donc définir le régime exact de protection des données personnelles qui lui sera applicable. Aussi, les informations confiées au fournisseur cloud peuvent nécessiter de la confidentialité, d'où l'importance d'une clause ou d'un accord de confidentialité ainsi que du niveau d'engagement attendu.

Mais si tout cela n'est pas respecté, qu'adviennent les données du cloud ? Des sanctions sont-elles appliquées ?

Afin de faire face à ces nouveaux types de problème, la vice-présidente de la Commission européenne en charge de la Justice, Viviane Reding, a présenté le 26 janvier 2012 une nouvelle directive européenne sur les données personnelles. Le but est d'avoir un contrôle plus précis sur les données personnelles qui transitent sur Internet. Ce projet prévoit notamment un « droit à l'oubli numérique », qui imposerait aux réseaux sociaux tels que Facebook de supprimer définitivement les données personnelles des individus qui en feront la demande. Les entreprises doivent également être en mesure de notifier les clients lors de l'utilisation de leurs données et prévenir de toute fuite de données. En cas de non-respect, des sanctions et des amendes sont prévues à l'encontre des entreprises. En France,

c'est la Commission Nationale Informatique et Libertés (CNIL) qui aura la charge de veiller au respect de la nouvelle législation.

Cette réforme est devenue essentielle, suite à de nombreux incidents comme la récolte des données de Google Street View ou encore les fuites de données du groupe Sony. Cette réforme permettra également de simplifier les règles en matière de législation. En effet, il y a actuellement 27 législations différentes. L'harmonisation permettra non seulement de faciliter le traitement et le contrôle des données mais aussi de faire des économies sur les démarches administratives («de l'ordre de 2,9 milliards d'euros par an pour les entreprises» selon Viviane Reding).

Ce qui est certain, c'est qu'après l'étude « BSA Global Cloud Scorecard » réalisée par la Business Software Alliance (BSA) sur « les contextes politiques et législatifs les plus favorables à la croissance du cloud computing », il en ressort que la France est classée cinquième sur les 24 pays audités. La France est bien classée car elle « impose une protection renforcée des services cloud ». On note toutefois que même si la législation française protège la vie privée, les déclarations sont encore complexes et peuvent être simplifiées.

4) Les nouveautés du cloud et de la virtualisation au 1er trimestre 2012

Dans cette partie nous allons parler des différentes évolutions constatées à la fois au niveau des solutions d'hyperviseurs et des solutions de services cloud proposés par les différents fournisseurs du marché. Nous allons spécifier les types de solutions en séparant les services cloud offerts aux entreprises des services cloud offerts aux particuliers ou bien orienté ordinateur personnel comme les VDI (*Virtual Desktop Infrastructure*). Le VDI est le déploiement de machines virtuelles destinées à être exécutées sur des postes clients. Cela permet de mettre à disposition des employés d'une entreprise une même machine virtuelle directement paramétrée et donc de diminuer les coûts de maintenance. Tout d'abord, intéressons-nous au monde des hyperviseurs avec l'annonce de l'arrivée d'Hyper V-3.

a) Etat actuel du marché des hyperviseurs

Dressons tout d'abord un bref récapitulatif des solutions d'hyperviseurs actuellement présentes sur le marché et commençons par VMware.

Le leader VMware propose son hyperviseur ESXi actuellement dans sa version 5. Ce système est extrêmement léger et permet l'intégration de toutes les solutions VMware notamment les logiciels de sécurité, les logiciels de gestion. Ce système est extrêmement léger car il ne contient que le kernel de l'hyperviseur. La gestion de l'hyperviseur est faite à distance. La tarification des solutions VMware est fonction du nombre de VM qui est amené à être exécuté sur l'hyperviseur. Les capacités des hyperviseurs ESXi sont actuellement les plus intéressantes sur le marché. En effet ils offrent des fonctionnalités beaucoup plus intéressantes que les hyperviseurs Hyper-V notamment au niveau de la gestion de la mémoire grâce à des techniques avancées telles que le balooning. La gestion des drivers est aussi beaucoup plus sure chez VMware car les pilotes passent par une importante série de tests afin de certifier à 100 % une intégration parfaite avec ESXi. (**Figure 13**)

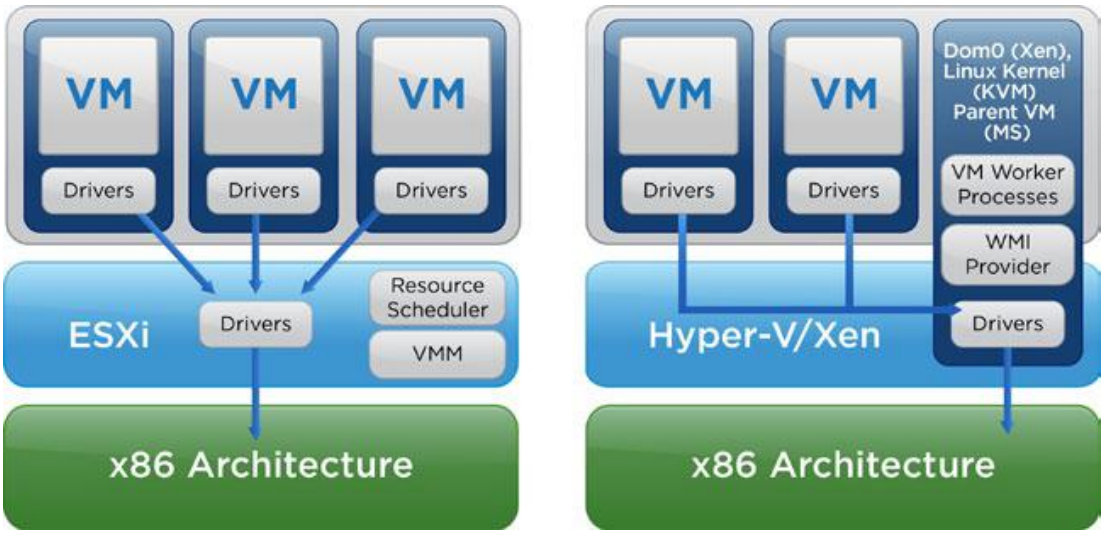

Figure 13 : Comparaison des architectures

Source : http://www.vmware.com/files/pdf/vmware_advantage.pdf

Passons à présent à la solution de Microsoft : Hyper-V. Cet hyperviseur est intégré par défaut au sein du système Windows server 2008 R2. L'avantage est qu'il n'est pas nécessaire d'acheter une licence logicielle supplémentaire. L'inconvénient est que les pilotes ne sont pas forcément les plus adaptés à la virtualisation, ce qui peut provoquer des bugs et d'autres problèmes de fiabilité. La gestion de la mémoire est moins efficace que celle de VMware car elle repose sur les algorithmes de pagination d'un système d'exploitation qui ne sont pas forcément prévus pour les architectures virtuelles.

b) Les nouveautés de la virtualisation

Microsoft Hyper-V

Concernant la virtualisation pure, il y a eu peu de nouveautés. La grande majorité des SSII fournissent des solutions cloud basées sur des solutions existantes, néanmoins Microsoft s'apprête à sortir une évolution de son hyperviseur. Microsoft Hyper-V 3 est en effet une évolution importante de l'hyperviseur Hyper-V. On peut y voir une volonté ferme de la part de la firme de Redmond de se placer en véritable concurrent de VMware au lieu de rester un outsider.

Tout d'abord au niveau des performances de l'hyperviseur, on note une nette amélioration au niveau de la mémoire allouable à une machine virtuelle, celle-ci passant de 64 giga-octets à 512 giga-octets ; également au niveau du nombre de processeurs virtuels que l'on peut allouer par VM, on passe de 4 à 32. Au niveau de la création des clusters de serveurs, on peut maintenant allouer 160 processeurs logiques (processeurs que verront les applications) par nœud du cluster (nombre de machine) contre 64 précédemment. Ces mêmes serveurs peuvent disposer désormais d'une capacité physique de 2 téra-octets pour leur mémoire vive contre 1 téra-octet auparavant. La taille maximale d'un cluster est également revue à la hausse. En effet, elle passe de 16 nœuds à 63 nœuds. Enfin, le nombre de VM dans un cluster est multiplié par 4, on passe en effet de 1000 VM à 4000 VM.

Maintenant attachons nous à voir quelles évolutions sont proposées par Microsoft au niveau des fonctionnalités de son hyperviseur. Tout d'abord Hyper-V 3 offre la possibilité de gérer les échanges entre VM et machines physiques à l'aide d'une nouvelle version de leur switch virtuel. Ce switch virtuel permet d'améliorer la granularité des échanges sur le switch entre VM. Le problème majeur de la gestion et du contrôle des échanges réseaux venant du fait que l'on ne puisse pas gérer le trafic de données entre VM depuis la machine hôte car cette dernière ne voyait pas les données que s'échangeaient les VM. Le gros avantage de ce switch est qu'il va permettre aux partenaires de Microsoft d'étendre les fonctionnalités de leurs logiciels en ajoutant des plugins qui utilisent les API ouvertes de WFP (*Windows Filtering Platform*). Ces derniers ont d'ailleurs commencé à développer ces plugins et logiciels.

Ensuite Microsoft offre la possibilité de définir des ACL (Access Control List) prenant en compte des VM. En effet, il est désormais possible de définir des autorisations pour des VM soit en passant par les adresses MAC soit en passant un intervalle IP. On peut noter ensuite les fonctionnalités de PVlans (*Private Vlans*) qui permettent d'isoler des VM partageant le même scope IP sur un réseau virtuel. Ensuite on peut citer le NIC Teaming (*Network Interface Controller*) qui permet de créer des agrégats de cartes réseau pour améliorer la bande passante. Les volumes CSV (*Cluster Shared Volume*) seront encryptés grâce à Bitlocker ce qui améliore la sécurité.

Une nouveauté importante consiste en l'intégration d'un utilitaire de migration à chaud de machines virtuelles. Auparavant à la charge du logiciel DPM 2010, la migration asynchrone de machines virtuelles sera désormais intégrée nativement à Hyper-V 3. Au niveau de la réplication de données, l'hyperviseur gérera le *failback* (capacité de retransférer les requêtes du serveur de réplication vers le serveur principal une fois que ce dernier est de nouveau disponible) et le *failover* (transfert des requêtes vers un autre serveur une fois que le serveur principal est trop surchargé de demandes). On note également la possibilité d'effectuer des migrations de disques durs virtuels et non plus seulement des machines virtuelles. Ce récapitulatif regroupe les principales nouveautés mais ne présente pas la totalité de ces dernières. Nous détaillerons par la suite les nouvelles fonctionnalités liées à la sécurité.

c) Les nouvelles offres cloud

Le cloud entreprise

De nombreux acteurs se lancent dans le cloud computing et certains proposent des services très innovants portant sur des tâches exportables sur des serveurs distants. Parmi ces nouveaux acteurs, il y a ceux qui fournissent des solutions généralistes comme Xerox et Powercloud qui offrent des services cloud aux PME. HP et SFR se sont associés afin de fournir des solutions cloud IaaS adaptées aux PME avec notamment des services d'archivage, de sauvegarde, de partage de données et de sécurité. Les passerelles cloud permettant d'améliorer la gestion d'applications existantes sont aussi en pleine expansion. Ainsi Vordel, une société fournissant ce genre de passerelles, permet de gérer une solution Microsoft Sharepoint via son service Vordel Sharepoint. IBM lance également une offre permettant de créer de façon automatisée des solutions cloud prêtes à l'emploi. Elle permet de plus de les gérer et de les administrer une fois qu'elles sont créées. Les solutions de gestion de cloud à travers un portail informatique telles que celles d'Enovance commencent elles aussi à émerger au regard de la difficulté croissante d'administrer efficacement de grosses infrastructures cloud.

Parmi les nouveaux services évoqués plus tôt, on peut citer le *Compute as a Service* (CaaS) qui consiste à offrir de la puissance de calcul à des entreprises ou à des particuliers qui en ont besoin. Parmi ces services on peut citer celui de Dimension Data qui va offrir des solutions de stockage et de CaaS aux entreprises et aux particuliers de la ville de Sydney en Australie. Enfin un nouveau service très axé sur la sécurité a vu le jour avec Nscaled qui fournit une solution cloud dite de RaaS (*Recuperation as a Service*). C'est un système permettant une reprise après sinistre, de l'archivage et de la sauvegarde.

VDI et cloud pour particulier

Des acteurs comme Gosis favorisent le retour de la virtualisation de poste de travail pour le cloud en insistant sur les VDI. On a aussi pu voir la création d'offre cloud open source comme Open Stack. Il s'agit en effet une solution adaptable à tous les hyperviseurs du marché pour concevoir une solution cloud qui se veut très compétitive par rapport à celles déjà présentes sur le marché.

Telefonica va fournir un service baptisé Dual Persona qui vise l'association d'un téléphone mobile et professionnel dans le même smartphone. Ce service sera géré dans le cloud et permettra de résoudre le problème de la conciliation de ces deux univers.

En conclusion, on peut dire qu'il y a de nombreux services qui émergent à cause de la jeunesse des technologies cloud et de l'engouement suscité. Les fournisseurs de solutions de virtualisation fournissent eux aussi des solutions qui tendent à s'adapter de plus en plus à la mouvance actuelle du cloud computing, la sortie prochaine de Hyper-V le montre bien. Regardons dès à présent comment sécuriser une infrastructure cloud.

II – La sécurité

Comme de nos jours les systèmes d'information prennent une place primordiale au sein des entreprises, la sécurité est bien évidemment un point majeur à travailler. Dans cette partie, on exposera la sécurité en général avec ses principes et les différents types d'attaques usuels, puis la sécurité dans la virtualisation et le cloud, et enfin les différentes solutions de sécurité.

1) La sécurité en général

Rendre vulnérable un système d'information reviendrait à rendre vulnérable l'activité voir la pérennité de l'entreprise. Les compagnies de transport, les banques ou toute autre organisation en dépendent. Ainsi, assurer la sécurité informatique est une priorité vitale. Les menaces contre les systèmes sont nombreuses : destruction, falsification, usurpation des données, ou usage frauduleux d'un réseau. Avec l'avancée d'Internet, la sécurité informatique couvre de nombreux domaines qu'ils soient juridiques, sociaux ou organisationnels.

Concernant les problèmes techniques de la sécurité, on peut distinguer deux catégories :

- La sécurité concernant l'ordinateur proprement dit, système d'exploitation serveur ou poste de travail.
- La sécurité des réseaux.

a) Les principes de la sécurité informatique

De ce fait, l'essor d'Internet a permis la combinaison de ces deux catégories et a pu ainsi multiplier les problèmes de sécurité en rendant vulnérable les serveurs et les postes de travail. On peut donc définir quelques principes de base qui permettent de faire face à certaines vulnérabilités.

Définition des risques et objets à protéger

Tout d'abord, il est essentiel de définir les risques et les objets à protéger. Pour cela, on définit un périmètre de sécurité au niveau physique tel que le matériel, les réseaux, les lieux. Mais cette mesure trouve ces limites avec les ordinateurs portables qui peuvent provenir de l'extérieur et s'introduire dans le périmètre de sécurité.

Authentification

Ensuite, il est nécessaire d'assurer une authentification des utilisateurs lors des accès aux ressources et aux systèmes et de veiller à la bonne définition des droits. En dépit de cela, la lecture des données n'est pas restreinte aux seuls authentifiés et peut donc être interceptée par un tiers. Il est donc important de chiffrer les données et de s'authentifier.

Pare-feu

Ces solutions ne sont pas encore suffisantes, il faut empêcher les intrusions venues de l'extérieur. Une technique classique consiste à installer un pare-feu qui va filtrer les communications réseaux. On pourra donc rendre les machines internes invisibles de l'extérieur et réduire certains services ou dialogues réseaux. Pour établir une zone accessible pour les personnes venant de l'extérieur (serveur Web, messagerie …), il est fréquent d'utiliser une zone démilitarisée (DMZ).

Sauvegarde des données

Un autre principe paraissant assez trivial est la sauvegarde des données. En effet, pour chaque type de donnée, on définit une périodicité de sauvegarde en fonction de leur utilisation. On veillera à ce que les supports de sauvegarde soient à l'abri de sinistre ou vers un site externe. On peut alors simuler une panne générale du système d'information qui va pouvoir déceler des failles organisationnelles.

Il existe encore d'autres aspects que nous ne verrons pas ici. Mais nous remarquerons que ces problématiques sont aussi valables dans le domaine matériel que virtuel.

b) Les types d'attaques usuels

Parmi les différents problèmes de sécurité réseau, on peut recenser quatre types d'attaques qui peuvent affaiblir un système d'information : les attaques d'accès, de modification, de déni de service et de répudiation.

Attaques d'accès

Les attaques d'accès représentent les tentatives d'accès au système par une personne non autorisée. Ainsi la confidentialité des données est mise en cause. On peut citer par exemple le *sniffing*, qui grâce à un logiciel permet de capturer des paquets réseaux. On

peut ainsi observer les sessions ftp en cours ainsi que les personnes connectées sur le réseau. Les chevaux de Troie sont également des outils fréquemment utilisés par les pirates. Ce sont des programmes cachés derrière des programmes qui permettent ainsi d'installer des portes dérobées. Une porte dérobée est un moyen au pirate d'accéder au système sur lequel il s'est déjà introduit sans refaire toutes les manipulations d'intrusion. Cela s'illustre par la création d'un nouveau compte administrateur et la modification des règles de pare-feu. Il existe un autre moyen de récupérer des mots de passe, qui est appelé l'ingénierie social. Ce n'est pas vraiment une attaque mais une ruse. Il consiste à demander des renseignements personnels en prétextant un motif (plantage, migration…) par e-mail ou téléphone. On a également la méthode traditionnelle de craquage de mot de passe qui peut se faire soit par la méthode brute (l'essai de toute les combinaisons possibles) ou l'utilisation de dictionnaire contenant une banque de mots de passe les plus utilisés. Les attaques d'accès n'étant pas négligeables, elles doivent être anticipées.

Attaques de modification

Les attaques de modification sont quant à elles prévues pour modifier l'information. Elles se traduisent par des virus, des vers (programmes malveillants qui se propagent et se multiplient par le réseau) ou des chevaux de Troie. Elles modifient des informations système, voire l'affichage. De ce fait, des données peuvent être détruites et rendre le système défaillant. De plus, cela provoque un ralentissement du réseau.

Attaques par saturation

Les attaques par saturation (ou déni de service) consistent à envoyer des milliers de messages sur un serveur (par exemple : le Web) en provenance de plusieurs stations différentes. Ainsi, le site web se voit paralyser, son accès est impossible et cela permet au hacker de s'y introduire en profitant de la saturation. On peut citer notamment le *flooding* qui consiste à envoyer des paquets IP de grosse taille jusqu'à ce que la machine cible se déconnecte du réseau. Il y a aussi le « *smurf* » qui par une requête *ping* peut aussi faire saturer une station. Imaginons une machine A se faisant passer pour une machine B en utilisant son adresse IP. La machine A va envoyer une requête *ping* sur plusieurs serveurs de *broadcast*. Chaque serveur va renvoyer ainsi vers la machine B autant de réponses que le serveur possède de machines. Soit un méga-octet la taille d'une requête *ping*, si un serveur *broadcast* possède mille machines, alors on a un méga-octet de données reçu. Mais supposons que le *ping* a été envoyé à dix serveurs, cela reviendrait à recevoir un giga-octet de données.

Attaques par répudiation

Pour terminer, les attaques par répudiation s'illustrent par la tentative de donner des informations erronées ou de nier une transaction ou un évènement qui a eu lieu. Ainsi, on met en cause la responsabilité de l'origine de l'action effectuée. Cela s'illustre par une usurpation d'identité par exemple lors d'un échange mail. Un mécanisme de cryptage peut être mis en place afin d'éviter ce genre d'incidents.

Ainsi, maintenir la sécurité informatique est une question vitale car cela peut affecter voir paralyser le fonctionnement d'une entreprise. Une faille de sécurité peut ainsi entrainer de fortes pertes financières. On doit ainsi tout mettre en œuvre pour préserver son système des différentes attaques et garantir la préservation des données, de leur intégrité et de leur confidentialité. Dans cette partie, nous avons survolé les principaux défis de la sécurité informatique. Cette dernière ne concerne pas seulement le domaine matériel mais aussi le domaine des technologies virtuelles. Ainsi, on retrouvera les mêmes défis et contraintes dans la virtualisation des systèmes et donc dans l'univers du cloud.

2) Sécurité de la virtualisation et du cloud

a) La sécurité dans la virtualisation

Prenons encore le cas concret de la solution VMware. Nous allons aborder les solutions pour pallier les problèmes de sécurité vus dans la partie précédente. Voici un extrait de la présentation « La virtualisation : des failles biens réelles ou virtuelles » de David Girard Expert conseil sécurité BPR-TIC (**voir Annexe 1**).

Voici les solutions qui sont proposées :

Comment se protéger
1. Gestion des accès (rôles) et de l'authentification serré.
2. Définir des serveurs ESX pour des tâches différentes et des niveaux de sécurité différents.
3. Sécurité de la persistance « Storage ».
4. Sécuriser la console
5. Séparation des tâches entre les administrateurs.
6. Mettre à jour les composants.
7. Sécuriser les réseaux physiques et virtuels.
8. Mettre place une infrastructure de journalisation et de surveillance adéquate.
9. Implanter une solution de sécurité qui tire profit de VMSafe ou l'équivalent.
10. Durcir et protéger les VM elles-mêmes.
11. Effectuer le durcissement de l'environnement virtuel
12. Balayer les environnements virtuels avec des scanneurs de vulnérabilité régulièrement.

Source : La virtualisation : des failles biens réelles ou virtuelles de David Girard
Disponible sur http://asiq.org/documents/conferences/2012/ASIQ-201201.pdf

Ainsi, la partie sécurité est aussi à assurer tant au niveau virtuel que matériel.

Il est nécessaire d'assurer l'isolement de la machine virtuelle et de la machine hôte. Il faut éviter qu'il y ait un accès au support physique. Au niveau de la répartition des machines, on doit veiller à ne pas surcharger la machine hôte de serveurs virtuels de crainte d'augmenter sa criticité. La panne de la machine hôte induirait l'arrêt total de l'ensemble des serveurs. L'accès au serveur de machines virtuelles doit être contrôlé. Un utilisateur ayant les droits d'accès lui permettrait de copier les machines virtuelles et de récolter des informations confidentielles. Il suffirait même qu'il reboote de manière non-intentionnelle ou modifie les paramètres de configuration. La performance de la machine hôte peut être affaiblie dans le cas où un programme malveillant tel qu'un vers serait introduit. La charge serait ainsi affectée et affaiblirait les performances du réseau et de l'ensemble des machines virtuelles.

Pour anticiper l'ensemble des risques, il est donc important d'instaurer une supervision de ces infrastructures. Il faut évidemment veiller à la mise en place de système de *clustering* pour les serveurs en cas de panne. Enfin, on doit effectuer une gestion de la sécurité de manière rigoureuse.

b) La sécurité dans le cloud

Gérant une grande quantité de données et de flux, le cloud est sensible aux problèmes de sécurité. On identifiera les risques et les points cruciaux pour mettre en place une politique de sécurité solide et pérenne.

Identification des risques de sécurité

Nous pouvons identifier neuf risques d'après SYNTEC numérique sur lesquels on doit porter notre attention. Nous commençons avec la perte de maîtrise, c'est-à-dire le transfert de charge des données par l'hébergeur du cloud, qui fait perdre à l'entreprise le contrôle du système. Ensuite, nous avons le risque de déficiences au niveau des interfaces et des APIs : le cloud étant en émergence, la technologie n'est pas encore mature et a besoin encore d'évolution. Il y a également le risque de conformité et de maintenance de conformité sur l'aspect juridique des données ainsi que sur la traçabilité. On peut parler aussi du risque de la délocalisation des données qui provoque une maîtrise plus faible de celle-ci. Puis, il y a le risque d'isolement des environnements de données sur l'étanchéité entre les différents utilisateurs, l'isolation des données en différentes formes et la monopolisation des ressources par un environnement utilisateur. Enfin nous passons aux derniers risques plus simples : la perte de données, leur récupération, l'usurpation expliquée précédemment et la malveillance dans l'utilisation (par administrateur).

Sécurité physique

La dématérialisation des données permet donc d'avoir de multiples datacenters où peuvent être stockées ces données. Il faut un contrôle et une traçabilité d'accès dans le but de prévenir tout dommage sur le matériel. Faire attention au va-et-vient dans certaines zones, protéger l'accès à certaines salles et même les interdire d'accès peuvent être un bon moyen de protection. Il est impératif de protéger également certaines zones plus que les autres contre les incendies et autres risques environnementaux, ainsi que bien les climatiser (**Figure 14**).

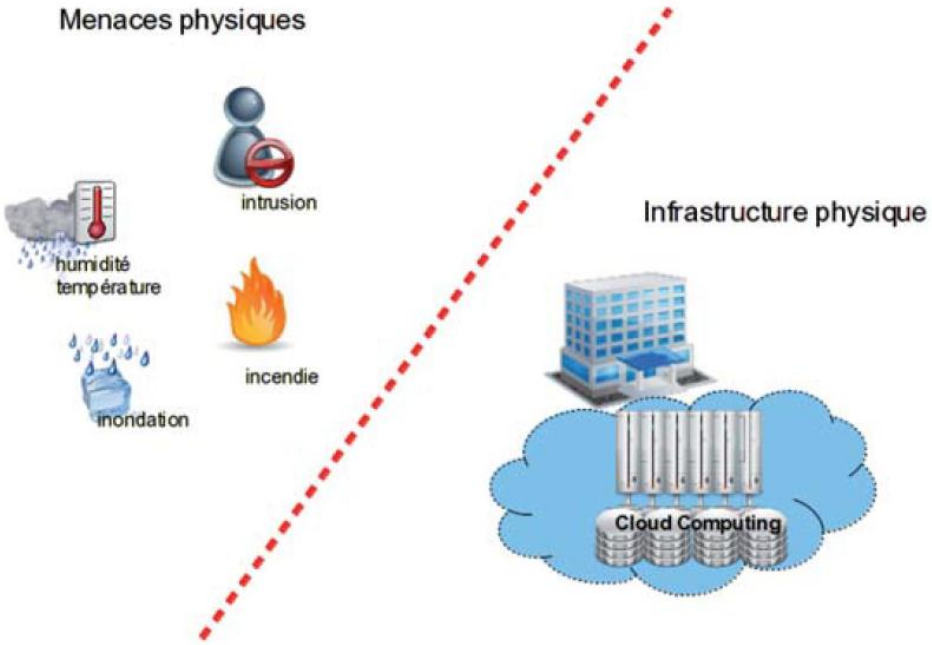

Figure 14 : La sécurisation de l'environnement
Source : http://www.syntec-numerique.fr/content/download/380/1220/version/1/file/Livre_Blanc_Cloud_Computing_Securit%C3%A9.Vdef.pdf

Les redondances matérielles sont également très utilisées pour garantir l'accès au service en très haute disponibilité avec des performances optimales. Penser à la réplication de configuration entre les équipements et également à une redondance avec une sélection d'équipements différents (exemple : constructeur différent) permet de prévenir plusieurs problèmes importants.

Enfin, il est possible de mettre en place comme sécurité géographique, un système de secours géographiquement éloigné, au cas de la perte totale de l'infrastructure. Il permet de réaliser un PCA (plan de continuité d'activité) sans interruption.

Sécurité logique

La sécurité que l'on souhaite intégrer est destinée à des plateformes virtualisées. Il faut cependant appliquer les mêmes règles de sécurité que dans une architecture physique. Mais il faut en plus s'intéresser aux problématiques de sécurité spécifiques au cloud (multi-location). En effet la colocation et le partage de l'infrastructure entre plusieurs utilisateurs imposent des règles strictes de sécurité.

La sécurité et la confidentialité des données peuvent être gérées de différentes façons d'un point de vue logique : la segmentation réseau sera ainsi sécurisée par des équipements de filtrage (pare-feu, proxy, sondes IPS/IDS…) et des solutions antivirus. Le but est ici de contrôler les requêtes entrantes. Un processus d'authentification est par ailleurs nécessaire. Il faut également insister sur deux bonnes pratiques de sécurisation logique dans un environnement cloud. Tout d'abord, il faut paramétrer le système d'exploitation des machines virtuelles pour les sécuriser comme le conçoit l'éditeur de la solution de virtualisation. La deuxième bonne pratique consiste à bien isoler le trafic réseau en fonction des besoins lors de la conception du réseau virtuel.

Sécurité des données

Pour la sécurité des données, on peut naturellement se diriger vers des solutions de chiffrement. Notamment la méthode classique consistant à créer un couple clé publique/clé privée où seul le destinataire est en mesure de déchiffrer les données qui lui sont destinées grâce à sa clé privée. Il est important de mentionner que même le fournisseur de cloud ne détiendra pas la clé privée. Cette solution permet de bien sécuriser les données (selon la taille de la clé) et le client à la possibilité de ne chiffrer qu'une partie de ses données. La méthode pose cependant certaines problématiques d'implémentation. Lors de certains traitements tels que la sauvegarde ou l'indexation, il peut s'avérer nécessaire de manipuler des données décryptées.

3) Les solutions de sécurité du cloud et de la virtualisation

a) Les solutions de sécurité : outils non techniques

Sans entrer dans un premier temps dans les aspects techniques, nous allons lister les problèmes importants et leur résolution en termes de sécurité des données, afin de limiter les risques. Voici ce que le client et le provider devraient prendre en compte et ce sur quoi ils devraient s'engager :

Les entreprises clientes doivent considérer les points suivants :

Quels types d'informations sont accessibles dans le cloud ? Qui peut y accéder et comment sont-elles isolées des éléments non sécurisés ? Qui dispose de droits pour envoyer et recevoir des données sensibles en dehors du périmètre de l'entreprise ? Quelles sont les données qui ne doivent pas sortir de l'entreprise ? Comment les données sensibles doivent-elles être envoyées ? En clair ou en cryptant certaines d'entre elles ?

Le fournisseur devrait formaliser avec le client les procédures de réponse aux incidents :

Réaliser des enquêtes dès qu'une violation a eu lieu, atténuer une violation et y remédier, aviser rapidement le client (dans des temps convenus), fournir des rapports écrits et faire régulièrement le point sur l'incident, conserver certaines informations qui pourraient être pertinentes (logs, documents de planning, journal d'audits, enregistrements et rapports, etc.) et documenter les mesures correctives.

En ce qui concerne l'obligation de préserver les données :

Le client devrait également essayer d'obtenir le droit d'effectuer ses propres enquêtes judiciaires et procédures de préservation sur les systèmes du fournisseur.

En ce qui concerne les droits d'expertise judiciaire :

Il peut y avoir des limites relatives aux fournisseurs de cloud tiers, ainsi, il faudrait limiter le recours à un fournisseur tiers pour le stockage de ses données et obliger le fournisseur à au moins avertir son client en cas de transfert vers un fournisseur tiers. Ou alors, obliger le fournisseur principal à appliquer les mêmes mesures vis-à-vis de ses fournisseurs tiers que ses clients.

En ce qui concerne les risques de pertes suite à une violation de données *:*

Il faudrait préciser dans le contrat qui devra assumer la perte. Les clients devraient négocier des modalités contractuelles qui transfèrent ce risque de perte au fournisseur de cloud victime de la violation. Il faut préciser des clauses d'indemnisation (frais divers, avocat, etc…), des clauses de limitation de responsabilité côté fournisseur (peut être utilisé pour faire valoir une rupture de contrat). Les fournisseurs proposent des assurances.

En ce qui concerne la question des employés :

Les frontières de l'entreprise n'existent plus (mobiles, tablettes, Facebook, etc…), la sécurité passe de plus en plus par les employés (75% des incidents de sécurité ont une origine interne et humaine). Le travail se poursuit au domicile, où les conditions ne sont pas les mêmes. Il faut considérer une approche globale de la sécurité (Sécurité 2.0). Ainsi, l'employé n'est plus la source des problèmes mais une composante indispensable d'une politique de sécurité efficace (sécurité collective).

Pour résumer, il faut penser à la viabilité du contrat, à l'auditabilité des procédures de sécurité et à la transparence des informations.

Cela en plus des aspects techniques à prendre en compte pour le stockage, la sauvegarde, l'intégrité et la restauration des données car du point de vue technique, la protection des données, c'est :

- La classification et la gestion des droits à la création
- Le transfert : réseaux privés/chiffrement/authentification forte
- Le stockage : contrôle d'accès/gestion des droits/chiffrement
- L'utilisation : contrôle logique/suivi des activités
- L'archivage : chiffrement/ gestion des biens
- La destruction : effacement sécurisé

b) Les solutions de sécurité : outils techniques

Politique d'authentification

Aspect essentiel dans la protection des données, des solutions d'authentification sécurisée sont proposées sur le marché.

Intel Cloud SSO (S*ingle Sign-On*) est une solution pour automatiser l'accès aux services dans le cloud en mode SaaS. Ce service permet à la fois de s'authentifier pour accéder à un service cloud, mais permet aussi de gérer les autorisations. L'éditeur de logiciel ILEX propose Sign&go 5.0 et implémente le standard OAuth 2.0 dans une solution IAM (*Identity and Access Management*) qui permet d'unifier les modes d'authentification. Google a renforcé la sécurité de ses services hébergés avec l'authentification basée sur les certificats. Ainsi, la requête d'une application Web au service Google Cloud Storage pourra par exemple être authentifiée par un certificat au lieu d'une clé partagée.

Politique de pare-feu et de détection des intrusions

De nombreuses organisations désirent un cloud intelligent qui détecte les menaces de manière autonome. L'armée américaine par exemple cherche à définir des modèles de fonctionnement normal de son cloud. Ainsi, si un évènement arrive et qu'il ne correspond pas à un des modèles connus, alors il s'agit probablement d'une attaque. Il existe plusieurs solutions pour bloquer les intrusions avec des politiques de pare-feu et de détection.

Ainsi, Barracuda Networks NG Firewall propose un pare-feu et une interface pour gérer les politiques de sécurité de l'infrastructure réseau (Internet, WAN). Cisco présente un pare-feu contextuel avec sa plate-forme ASA SecureX ayant des fonctionnalités de contrôle d'accès, de filtrage réseau et de prise en charge des environnements virtuels. Dell a également renforcé sa position sur le segment de la sécurité IT adressée aux PME (pare-feu, gestion unifiée des menaces…) en rachetant SonicWall ce qui renforce ses offres SecureWorks, solutions cloud et chiffrement des données, ainsi que la gamme Kace (gestion des vulnérabilités et gestion des correctifs). Le SaaS MetaFlows Security System propose une plateforme pour unifier la sécurité réseau avec un système de détection des intrusions, la surveillance du trafic sur le réseau, des historiques. La startup propose également un forfait pour la mise en place d'un client « honeypot » qui agit comme un leurre pour les menaces (détection et analyse).

Protection des infrastructures virtuelles

La sécurité des environnements virtuels est primordiale : les attaques sont nombreuses sur les instances de Machines Virtuelles (application, système d'exploitation). La signature future de VM identifiable par un catalogue de VM de l'entreprise (pour ne pas se les faire voler) pourrait constituer une bonne solution. En attendant, plusieurs solutions sont proposées sur le marché :

Symantec Corp. s'est associé à VMware pour proposer des solutions de protection des infrastructures virtuelles basées sur VMware (VMware Cloud Infrastructure). L'objectif est de recentrer la sécurisation de l'information quel que soit l'environnement de travail, qu'il soit physique ou virtuel. La plate-forme Symantec O3 fournit plusieurs couches de sécurité pour le cloud (contrôle d'accès, protection des identités). Trend Micro propose Deep Security 8.0, une plate-forme de sécurité pour le datacenter avec des modules de protection pour les environnements physiques, virtuels et cloud (surveillance de l'intégrité des fichiers), adressé au PME. Dell a amélioré la sécurité de son cloud public avec Trend Micro SecureCloud Solutions (services de cryptage de données pour le cloud Dell avec VMware vCloud Datacenter Service). CloudPassage améliore la sécurité des serveurs élastiques dans le cloud avec une nouvelle version de ses outils de sécurité SaaS Halo appelée NetSec. L'idée est de sécuriser l'image de base et que celle-ci s'adapte automatiquement, donc de manière élastique lorsque le nombre d'instance augmente ou diminue.

Protection de la messagerie

Dans les entreprises, la messagerie est souvent l'un des premiers éléments externalisés dans le cloud. Néanmoins, les informations circulant dans les mails sont loin d'être anodines, c'est pourquoi des solutions de sécurité de messagerie sont proposées :

Vade Retro propose une solution de sécurité de messagerie dans le cloud qui permet de définir une politique de sécurité pour les fournisseurs de services de messagerie (filtrage des mails, outils de gestion, de reporting …). OpenText Managed File Transfer est une solution pour gérer les échanges de fichiers volumineux de l'entreprise de manière sécurisée. Elle s'intègre à Microsoft Outlook et simplifie les questions liées à la taille des pièces jointes. Elle fournit une plate-forme pour l'échange sécurisé et la vérification de tous contenus numériques, y compris les informations sensibles liées à la propriété intellectuelle, entre les collaborateurs, les partenaires et les clients.

Les autres offres de sécurité dans le cloud

- In-Webo et InterCloud propose une offre conjointe de sécurisation des accès au cloud computing.

- BitDefender propose deux solutions : Cloud Security for Endpoints et Security for Virtualized Environments (SVE) et se positionne également avec un service de sécurité en mode SaaS.

- La firme eNovance présente une solution de sécurisation multi-cloud.

- Après Google Bouncer et sa solution de scan de logiciels malveillants sur Android Market, Micro Trend propose aussi une solution cloud appelée Mobile App Reputation permettant d'analyser les applications mobiles fonctionnant sous Android et Symbian.

- PerspecSys Inc propose PerspecSys PRS Adapter pour Oracle CRM On Demand. Cet adaptateur permet d'assurer une solution de protection des données dans le cloud.

c) Les solutions de sécurité au niveau « hyperviseur »

Les attaques sur les hyperviseurs se sont développées, ceux-ci présentent donc des solutions de sécurité. Nous rappelons ci-dessous les caractéristiques sur l'aspect sécurité du dernier hyperviseur de Microsoft : Hyper-V3.

Sur l'aspect sécurité, Hyper-V3 intègre un switch virtuel Microsoft avec un firewall intégré en analogie avec la solution v-Shield de VMware. Une fonction de sécurité au niveau DHCP existe également, pour se prévenir des utilisateurs malveillants.

Fonctionnalités disponibles :

- Protection contre l'usurpation d'adresse MAC via filtrage des annonces *Address Resolution Protocol* (ARP).
- Protection contre la mise en œuvre du service DHCP via filtrage des annonces *Dynamic Host Configuration Protocol* (DHCP).
- Protection contre la modification des tables de routage via filtrage des annonces de routeurs (RIP, RIPv2).
- Surveillance (monitoring) du trafic au niveau du port utilisé par une machine virtuelle.
- Administration simplifiée avec PowerShell et WMI.
- La sécurité « *snapshot* » permet de réaliser chaque jour une image pour la sauvegarde : en cas de plantage, il est facile de revenir sur une version antérieure et stable.

d) Les solutions de sauvegarde, back-up, restauration

De nombreuses entreprises et de nombreux particuliers utilisent des solutions de stockage cloud tels que MegaUpload, OVH, Amazon, Apple... Cependant, en cas d'arrêt voir de fermeture brutale comme MegaUpload, la question est de savoir comment récupérer ses données. Pour faire face à ces problèmes, il est essentiel de classer les données externalisables des données indispensables, confidentielles, nominatives et sensibles. En effet, il faut être extrêmement vigilant avec la deuxième catégorie de données pour la reprise de l'activité en cas d'arrêt ou de fermeture brutale d'un fournisseur de stockage cloud. Pour cela, des moyens existent comme la copie et la sauvegarde régulière de ces données importantes.

La sauvegarde des données dans un but de back-up et de restauration constitue un point essentiel car si le back-up ne constitue pas une protection en amont, il permet une copie de sauvegarde des données pour en assurer la pérennité. Ainsi le back-up constitue le dernier recours en cas de perte de données dans le cloud. Le choix de la solution est

important de par plusieurs critères (fiabilité, accessibilité, rapidité, sécurité, problématique de stockage …).

En effet, de nombreuses solutions sont proposées sur le marché, néanmoins les offres diffèrent en s'adressant généralement à des cibles différentes : si Dropbox permet à un particulier de sauvegarder ses fichiers dans le cloud, les PME se tourneront vers des solutions de sauvegarde qui leur sont adressées : Western Digital a par exemple annoncé que tous ses clients utilisateurs du WD Sentinel DX4000 (destiné aux PME) pourraient accéder gratuitement à un service de stockage dédié hors site. De même, la solution de sauvegarde et restauration de Quest Software, NetVault Backup Capacity Edition s'adresse aux PME en se voulant hétérogène et multiplateforme, tant sur les environnements physiques que virtuels. De même, Symantec Corp. présente les solutions de sauvegarde Symantec NetBackup 7.5 et Backup Exec 2012 qui intègrent un support pour le stockage dans le cloud proposé par AT&T, Amazon Web Services et Rackspace et qui fournissent la possibilité d'effectuer des sauvegardes de machines virtuelles Microsoft et VMware et de restaurer des VM corrompues à partir de ces sauvegardes (*bare-metal*). Il faut également regarder du côté d'IBM et de son logiciel Tivoli (application de gestion de stockage, sauvegarde et restauration destinée aux entreprises) qui présente des avantages au niveau de la réduction du temps d'allocation des ressources.

e) Les solution futures de cryptage et de chiffrement

Des recherches actuelles permettront sans doute d'utiliser des données cryptées avec des applications dans le cloud. En effet, aujourd'hui, les données doivent être en clair pour pouvoir être utilisée par des applications sur le cloud. Si les données sont chiffrées, le résultat sera lui aussi chiffré (exemple d'une requête SQL qui retournera un résultat chiffré). L'utilisation d'une clé n'est pas possible ici, car sinon, elle sera publiée sur Internet (**Figure 15**).

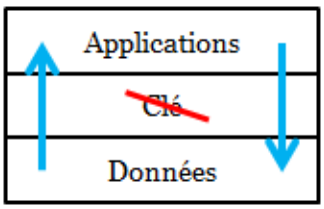

Figure 15 : Principe de chiffrement sans clé

On peut stocker ou archiver des données cryptées, mais une application cloud ne peut pas travailler sur des données cryptées. Les recherches pour remédier à ce problème ont mené à essayer de mettre en place une solution pour utiliser des données cryptées malgré tout (Cf. les recherches de Craig Gentry). La méthode consiste à mettre en place un

algorithme totalement homomorphique. Ce dernier fonctionne pour des opérations d'additions : il va à présent falloir faire en sorte de pouvoir appliquer l'algorithme à des opérations de multiplication. Les plus avancées dans ces recherches sont les chercheurs de l'ENS Lyon, et une partie de leur travail va aussi consister à améliorer la complexité de l'algorithme qui est un réel problème lorsque la clé devient très grande. Ces recherches pourraient constituer l'avenir de la sécurité du cloud computing.

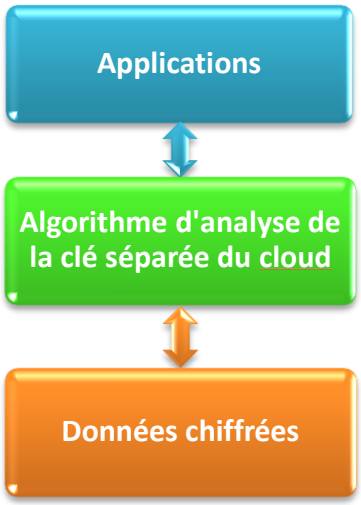

Figure 16 : Fonctionnement cloud sur des données chiffrées sans clé de sécurité

On peut donc voir que l'algorithme d'analyse (**Figure 16**) va pouvoir donner la possibilité aux applications de travailler sur les données chiffrées.

f) Les autres approches

On voit apparaitre aujourd'hui des cloud spécifiques à des besoins fonctionnels comme le cloud d'archivage ou le cloud poste de travail avec donc pour chacun, une sécurité adaptée à leurs fonctions. Il faut donc penser à une approche de sécurité adaptée en fonction du service cloud également comme par exemple l'IaaS avec une gestion de sécurité de l'infrastructure et des identités forte ou encore le PaaS centrée sur l'application et ses données.

Les considérations à prendre en compte pour adopter une solution de sécurité sont donc nombreuses et complexes. Ce qui est sûr, c'est que cloud a permis de faire évoluer la sécurité dans de multiples domaines comme l'évolution de la gestion des logs, la « fédération d'identité » et le « multiple login ».

III – La prospective du cloud et de la virtualisation

1) La tendance

Aujourd'hui, le cloud est adopté non seulement par les entreprises, mais aussi par le grand public. On constate un réel engouement et une multiplication des services proposés. De nombreuses offres SaaS répondent aux besoins des fonctions supports dans les entreprises comme les ressources humaines, la gestion, ou encore la finance. Quant au grand public, le cloud attire des utilisateurs autour d'applications telles que Dropbox ou iCloud, qui permettent de partager des ressources sur différents supports (ordinateur, tablette, Smartphone….).

Les géants de l'informatique ont compris que le cloud computing est le nouvel eldorado de l'informatique. Chacun essaye de s'imposer sur ce vaste marché en plein essor, en essayant de proposer ses solutions (par exemple : VMware vs Microsoft, iCloud vs S-Cloud, Orange vs SFR, …). Ainsi, dans les trois prochaines années, le cloud va être l'une des principales valeurs d'investissements.

2) L'impact économique

Le marché du cloud computing est actuellement en plein essor avec un taux de croissance annuel moyen de 30% pour l'année 2011. En effet, de nombreuses entreprises tentent de tirer leurs épingles du jeu en proposant leurs solutions. D'après une étude EMC, les entreprises qui adopteraient le cloud devraient faire des économies à hauteur de 26 milliards d'euros entre 2010 et 2015.

Selon une étude menée par Microsoft, 14 millions d'emplois seraient créés dans le monde d'ici 2015 (**voir Annexe 2**), plus particulièrement 190 000 en France. On chiffre également à 4,6 millions d'emploi pour la Chine ainsi que 2,1 millions pour l'Inde. Contrairement aux idées reçues, le cloud sera bien à l'origine de création d'emploi. Le cloud va représenter plus de 10% des d'investissements mondiaux pour 2013.

Le cloud computing possède de réels avantages en matière d'économie. En investissement de départ, il ne nécessite pas le déploiement du réseau et des serveurs. On obtient ainsi un gain non négligeable sur ce temps de déploiement. Les offres disponibles requièrent peu de paramétrages et un temps d'installation court. Le cloud permet aussi de gérer les coûts dans la maintenance des systèmes d'information ainsi que l'allocation dynamique de ressources.

C'est pourquoi le cloud computing demeure attractif de par ses avantages économiques et sa flexibilité d'utilisation. Les prix des offres cloud ne cessent de diminuer comme on a pu le constater durant ce début d'année 2012. Cela accélère son adoption.

Ainsi, avec une forte croissance dans les prochaines années à venir (**Figure 17**) et un développent rapide, le cloud va donc directement s'imposer comme un nouveau modèle économique important.

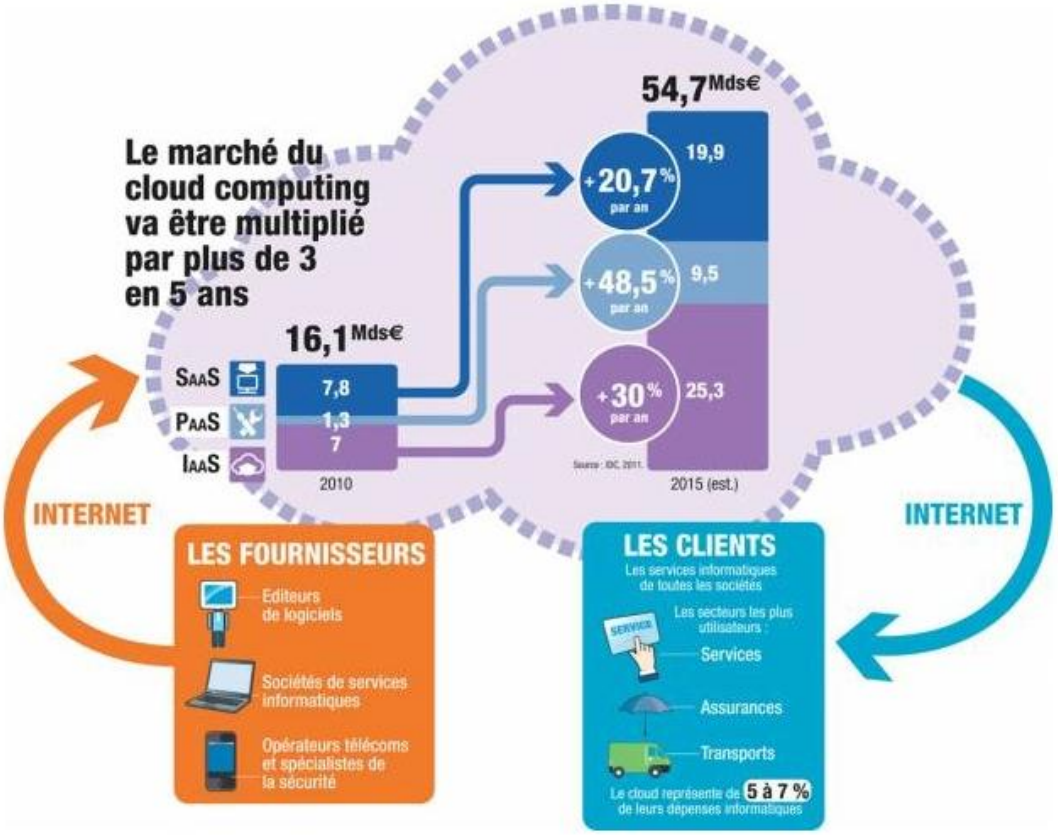

Figure 17 : L'évolution du cloud entre 2012 et 2015
Source : http://www.investir.fr/infos-conseils-boursiers/dossier/Le_cloud_La_nouvelle_revolution_technologique_a_jouer_en_Bourse/le-cloud-la-nouvelle-revolution-technologique-a-jouer-en-bourse-421520.php

3) Les améliorations à venir

Dans les prochaines années à venir, de nombreuses améliorations seront apportées dans le domaine du cloud computing, notamment sur la sécurité et la collecte de données.

Concernant les futures normes du cloud, une norme ISO (*International Standard Organisation* — Organisation internationale de normalisation) sur le cloud computing devrait voir le jour. Ce sujet a été abordé la première fois en octobre 2010. A cette date, les chinois et les sud-coréens ont décidé de se porter candidats pour l'hébergement des données et des applications. Depuis cette volonté asiatique de faire naître de nouvelles normes, ce projet est devenu un des enjeux mondiaux majeurs du cloud.

Cette future norme aura pour objectif de définir clairement la terminologie utilisée pour le cloud, mais également de définir les différents acteurs et leurs rôles (fournisseur, consommateur), les différentes architectures ainsi que des aspects importants comme la sécurité, la confidentialité ou encore l'interopérabilité.

En France, l'AFNOR (Association française de normalisation) possède une commission composée d'acteurs importants comme Microsoft, IBM, Thalès ou encore EDF. Cette commission sera en charge d'aller négocier auprès de l'ISO.

En termes d'authentification, Intel va proposer cet été une offre SSO (*Single Sign-On*) pour l'authentification dans le cloud. En effet, les fournisseurs de solutions de sécurité aimeraient mettre en place une signature unique SSO afin d'une part de s'authentifier dans le but d'accéder aux services cloud mais également de pouvoir gérer toutes les autorisations du compte en question. Ce procédé aura donc l'avantage d'automatiser la gestion des différents comptes qui se connectent pour les services SaaS.

4) Les futurs grands projets cloud français

Depuis quelques années, de nombreux projets cloud ont vu le jour. Il y a encore de nombreux projets à venir dans les prochaines années. En France, Andromède est un des projets majeurs du gouvernement. L'idée étant de créer un « cloud à la française ». En effet, concernant la territorialité, il est actuellement difficile de connaitre quelle loi régit les données d'un cloud. Par exemple, toute donnée stockée sur un serveur américain est potentiellement visible par l'autorité selon le Patriot Act américain. C'est entre autre pour cette raison que la France a décidé de lancer son propre cloud national, baptisé Andromède. Ce cloud permettra aux administrations et aux entreprises d'externaliser leurs données dans des serveurs situés en France et par conséquent soumis aux lois françaises. Ainsi, il n'y aura pas de problèmes liés à la territorialité des données. Il est fort probable que ce type de protection des données soit un avantage concurrentiel par rapport aux fournisseurs actuels de cloud.

Un autre projet majeur financé par l'état dans le cadre du Programme d'Investissements d'Avenir concerne UnivCloud, un cloud destiné aux universités françaises. L'une des particularités d'UnivCloud sera d'assurer une mutualisation de l'infrastructure des systèmes d'information des différentes universités françaises mais aussi des différentes collectivités. Ce projet porté par INEO sera de type cloud communautaire pour plus d'un demi-million d'utilisateur. Actuellement, quatorze universités participent à la première phase d'analyse des besoins. En 2013, une maquette sera réalisée et la construction pourra alors être démarrée.

Toujours dans le cadre du Programme d'Investissements d'Avenir du gouvernement français, en plus du projet UnivCloud, on peut citer :

- La plate-forme d'ingénierie logicielle de la société Orange Labs qui permettra un développement collaboratif et une gestion des applications plus aisée sur le cloud ;
- Les outils de portage d'applications de la PME Prologue qui permettront de rendre plus facile la migration des logiciels de toute entreprise vers le cloud ;
- Le projet d'infrastructure logicielle haute performance de la société Bull qui offrira des performances de calcul à la demande ;
- Le projet Nu@ge de la PME Non Stop Systems qui développera des solutions de mutualisation des infrastructures pour différentes PME dans le but de proposer des services toujours plus innovants.

5) Les perspectives de sécurité

Le cloud est encore une technologie nouvelle et les retours d'expérience sur la sécurité sont peu nombreux (ou non mentionnés afin de ne pas inquiéter les clients). Malgré les solutions de sécurité sorties ces derniers mois, aucune entreprise cloud ne garantit actuellement une sécurité fiable à 100%. Par exemple, le code de VMware ESX a été divulgué sur internet en avril 2012. Ainsi, on peut se poser la question de savoir si les infrastructures cloud bâties sur VMware sont vulnérables face à de futures attaques.

Selon certains experts, on pourrait s'attendre à de futures attaques sur le cloud dans l'avenir. D'après Fabrice Prugnaud, vice-président EMEA de LogLogic « *Cela ne sera probablement pas une attaque malicieuse mais vraisemblablement une attaque pour permettre de prouver que cela est réalisable. Cela soulignera notamment le fait qu'il est nécessaire d'actualiser les mesures de sécurité (politiques, pratiques et règles de conformité et de sécurité Cloud) dans les entreprises qui souhaitent que leurs données soient mieux protégées. Nous devrions également observer une demande croissante de la part des entreprises auprès de leurs fournisseurs afin que les solutions répondent aux normes ISO 27002, permettant de garantir la préservation de la confidentialité, de l'intégrité et de la disponibilité de l'information* ».

De ce fait, pouvoir atteindre une certaine maturité et une plus grande fiabilité en matière de sécurité cloud va nécessiter davantage de temps car ce sont des technologies récentes. Ainsi on peut s'attendre à de futures attaques majeures qui pourront peut-être ébranler le modèle cloud ou au contraire renforcer sa sécurité.

Conclusion

À travers ce document, nous avons pu développer le vaste sujet de la sécurité dans la virtualisation et dans le cloud computing.

Le cloud computing est donc un moyen de délivrer un service informatique ciblé et quantifié à une clientèle précise sans que cette dernière n'ait à investir dans un système d'information dédié à ce service. Selon cette définition, nous avons vu des modèles tels que le PaaS, SaaS, IaaS, DaaS. Ces modèles reposent sur des technologies de virtualisation qui permettent d'atteindre la flexibilité requise à la réalisation de ces modèles. La virtualisation est une technologie clé du cloud computing. Elle permet de mutualiser des ressources matérielles et logicielles comme nous l'avons vu en spécifiant les offres de VMware, Microsoft et des autres acteurs de ce marché.

La virtualisation permet d'assurer une très grande souplesse au niveau des ressources allouables à une solution ou à un client. L'indépendance des solutions matérielles et logicielles permet de donner toute la puissance requise à la bonne exécution du service.

Le cloud est une technologie jeune et innovante dont l'attractivité est en hausse. Ce procédé peut changer les méthodes de travail, réduire les coûts, modifier les interactions client/fournisseur ainsi que changer le modèle économique.

De nombreuses nouvelles solutions pour pallier aux problèmes de sécurité du cloud ont vu le jour ces derniers mois. La sécurité est un en effet un des enjeux primordiaux pour la continuité du développement du cloud computing. C'est pourquoi les fournisseurs doivent garantir une sécurisation suffisante des données (intégrité et confidentialité), et assurer la pérennité du service. D'autres points sensibles sont à envisager tels que les problèmes juridiques concernant la localisation des données (territorialité). Les coûts doivent être analysés avec précaution afin d'éviter une tarification inadaptée. Ces derniers ont besoin d'adapter leurs offres de logiciels de virtualisation selon les demandes parfois très différentes de leurs clients. Tous ces éléments doivent être pris en compte lors de l'adoption d'une solution cloud.

Le marché du cloud computing est encore en plein essor. Selon le cabinet Gartner, le marché du cloud computing a été de 68,8 milliards de dollars en 2010 et pourrait s'élever à 148,8 milliards de dollars en 2014. Une des raisons de ce succès est le fait que le marché se soit adapté, permettant aux fournisseurs de transmettre des services à travers le réseau. Ainsi il est important de prêter une attention particulière à ces technologies qui vont bouleverser la manière de gérer les systèmes d'information.

Bibliographie

Scott M. Fulton (Microsoft). Virtualization is not Cloud Computing [en ligne]. Disponible sur : <http://www.readwriteweb.com/cloud/2011/08/microsoft-virtualization-is-no.php> (publié le 29/08/2011)

Erik van Ommeren, Martin van den Berg. Maitrisez le cloud. [document PDF en ligne]. Disponible sur : < http://www.sogeti.com/upload/Looking%20for%20Solutions/Documents/Seize-theCloud-FR.pdf > (2011)

Philippe Bron. Les principes du Cloud Computing : « Etat de l'art et perspectives » [article en ligne]. Disponible sur <http://behind-cloud-computing.com/cloudcomputing/les-principes-du-cloud-computing%C2%A0-%C2%AB%C2%A0etat-de-lart-et-perspectives%C2%A0%C2%BB/> (publié le 24/01/2011).

Comparaison concurrentielle entre les solutions Cloud computing Microsoft® et VMware [en ligne]. Disponible sur < http://download.microsoft.com/download/D/6/1/D61B4B1F-9413-431D-8419-1BDC89F96DF9/Microsoft%20Cloud%20Compete%20White%20PaperFinal_fr-fr.pdf > (publié le 04.12.2011)

David Girard. La virtualisations : des failles biens réelles ou virtuelles [document PDF en ligne]. Disponible sur < http://asiq.org/documents/conferences/2012/ASIQ-201201.pdf >

Ariane Beky. Viviane Reding veut faire du « droit à l'oubli » un pilier juridique de la protection des données en Europe [en ligne]. Disponible sur < http://www.silicon.fr/viviane-reding-veut-faire-du-droit-a-loubli-un-pilier-juridique-de-la-protection-des-donnees-en-europe-70961.html >

KPMG International. Clarity in the cloud: A Global study of the business adoption of Cloud [en ligne]. KPMG International : 2011. Disponible sur : <http://www.kpmg.com/FR/fr/IssuesAndInsights/ArticlesPublications/Documents/Clarity-in-the-cloud-french.pdf>

Sources des illustrations

Figure 2 : Antoine Benkemoun. Les différents types de virtualisation [billet de blog en ligne]. Disponible sur < http://www.antoinebenkemoun.fr/2009/07/les-differents-types-de-virtualisation-classification/ > (publié le 15/07/2009)

Figure 4 : VMware. Comparaison des fonctionnalités des versions d'ESX . Disponible sur < http://www.vmware.com/fr/products/datacenter-virtualization/vsphere/esxi-and-esx/compare.html >

Figure 5 : Microsoft. Comparatif des fonctionnalités de virtualisation pour les différentes versions de Windows Server 2008. Disponible sur < http://www.microsoft.com >

Figure 6 : Guillaume Genet. Qu'est-ce que la virtualisation [article en ligne]. Disponible sur < http://magicgg.fr/blog/article-virtualisation-156 > (publié le 15/04/2011)

Figure 7 : Management Insight Technologies. The Arrival of Cloud Thinking [document PDF en ligne]. Disponible sur < http://www.ca.com/~/media/Files/whitepapers/the_arrival_of_cloud_thinking.pdf > (Novembre 2011)

Figure 8 : Gartner - http://www.gartner.com/technology/home.jsp

Figure 9 : BitNami , Cloud.com et Zenoss. Les tendances du Cloud Computing en 2011 [article en ligne]. Disponible sur < http://www.cloudactu.fr/infographie-les-tendances-du-cloud-computing-en-2011/ > (2010)

Figure 10 : Markess International - http://www.markess.fr/home.php

Figure 11 : Markess International - http://www.markess.fr/home.php

Figure 12 : Widoobiz. Les entreprises ont les pieds sur terre et l'informatique dans les nuages [en ligne]. Disponible sur : <http://www.widoobiz.com/actualites/les-entreprises-ont-les-pieds-sur-terre-et-l%E2%80%99informatique-dans-les-nuages/13178>

Figure 13 : comparaison des architectures [document PDF en ligne]. Disponible sur < http://www.vmware.com/files/pdf/vmware_advantage.pdf >

Figure 14 : Syntec numérique. Sécurité Du Cloud Computing [livre blanc en ligne]. Disponible sur < http://www.syntec-numerique.fr/content/download/380/1220/version/1/file/ Livre_Blanc_Cloud_Computing_Securit%C3%A9.Vdef.pdf > (novembre 2010)

Figure 17 : Le cloud, la nouvelle révolution technologique à jouer en Bourse [article en ligne]. Disponible sur < http://www.investir.fr/infos-conseils-boursiers/dossier/Le_cloud_La_ nouvelle_revolution_technologique_a_jouer_en_Bourse/le-cloud-la-nouvelle-revolution-technologique-a-jouer-en-bourse-421520.php > (publié le 11/04/2012)

Annexes

1) Failles de sécurité

a) Les failles connues

Lorsque l'on parle de sécurité du cloud, il est évident que des problématiques de sécurité au niveau de la virtualisation doivent être abordées.

La sécurité dans le monde de la virtualisation doit être assurée autant que dans les infrastructures matérielles. La « sensation de virtuel » peut nous faire oublier certaines problématiques qu'on aurait en temps normal.

Prenons un cas concret : la solution VMware.

Voici un extrait de la présentation « La virtualisation : des failles biens réelles ou virtuelles » de David Girard, Expert conseil sécurité BPR-TIC

1. Attaques sur l'infrastructure de gestion (XSS, DoS, etc) ;
2. Attaques sur les machines virtuelles (une VM ou de ou VM à VM «VM hopping »
3. Side channel attack. L'hyperviseur envoi des informations à une VM qui expose des secrets à une autre VM. Survient si le réseau virtuel est mal configuré : promiscues mode enabled.
4. Attaques sur le réseau virtuel
5. Sabotage de la part de l'administrateur de l'infrastructure virtuelle.
6. Attaque sur les fichiers de logs. Log Abuse. DoS.
7. Fausses mises à jour.
8. Exploiter des VM ou des vSwitch mal isolées.
9. Attaquer la console.

Source : La virtualisations : des failles biens réelles ou virtuelles de David Girard
Disponible sur http://asiq.org/documents/conferences/2012/ASIQ-201201.pdf

Un des principaux défis du cloud est de garantir la sécurité et l'intégrité des données. En effet, des données mal sécurisées peuvent être interceptées durant leurs transmissions vers le nuage. Mais des données piratées au sein même du cloud seraient également un grand danger pour certaines entreprises qui utiliseraient des données confidentielles. Nul n'est à l'abri d'attaques virales.

Nous pouvons prendre exemple sur Amazon Web Services (AWS) qui a eu deux problèmes de ce type. Le premier a été Zeus. Un hacker avait réussi à introduire un cheval de Troie du nom de Zeus sur le cloud. Ce cheval de Troie est spécialisé dans le vol de

données sensibles (données bancaires, mots de passe, etc..). Ayant piraté un site web hébergé par Amazon pour pénétrer son infrastructure, il a réussi à héberger et faire tourner le module de commande centrale du « cheval de Troie » Zeus.

b) Les failles les plus récentes

Mais le cloud a plus récemment connu d'autres problèmes de sécurité. Nombreuses ont été les failles ces derniers mois et nous verrons que les causes de problèmes de sécurité au niveau du cloud peuvent provenir de diverses raisons.

Ainsi, au mois de février dernier, la solution « SaaS for Total Protection » de McAfee, censée lutter contre les malwares, a présenté une faille qui transformait les PC en relais de spam. Cette faille a été repérée par des utilisateurs dont les adresses mails ont été bloquées par leur F.A.I après détection d'envoi massif de mail.

C'est aussi au mois de février dernier que l'on a pu entendre parler d'une faille sur la plateforme de téléchargement d'Apple : iTunes. Un forum de consommateurs recenserait 71 pages de plaintes pour cette faille, qui serait présente et toujours pas corrigée depuis près d'un an. Des comptes iTunes ont ainsi été piratés et des comptes PayPal ont été débités à tort, pour des montants souvent faibles, mais pouvant tout de même atteindre 500$.

Mais la faille ayant incontestablement fait le plus parler d'elle ces derniers temps est la panne du cloud de Microsoft. En effet, le 29 février 2012, Azure a subit une panne mondiale pendant de nombreuses heures. Cette panne a touché pas moins de 4% des utilisateurs de ce cloud, principalement en Amérique du nord et en Europe. Il a d'abord été annoncé que la panne provenait d'une mauvaise gestion de la date pour les années bissextiles. Nous avons appris par la suite que la panne provenait d'un problème d'expiration des certificats de sécurité dans les machines virtuelles. En effet, à chaque redémarrage d'une machine virtuelle, un certificat d'un an est émis à partir de la date actuelle. Or, l'ajout d'une année au 29 février 2012 a fait désordre car il n'y a pas de 29 février 2013. Un correctif a été évidemment déployé très rapidement afin de corriger le problème. Cela aura été néfaste pour le cloud de Microsoft qui peine à s'implanter.

2) Le cloud computing : générateur d'emploi dans le monde

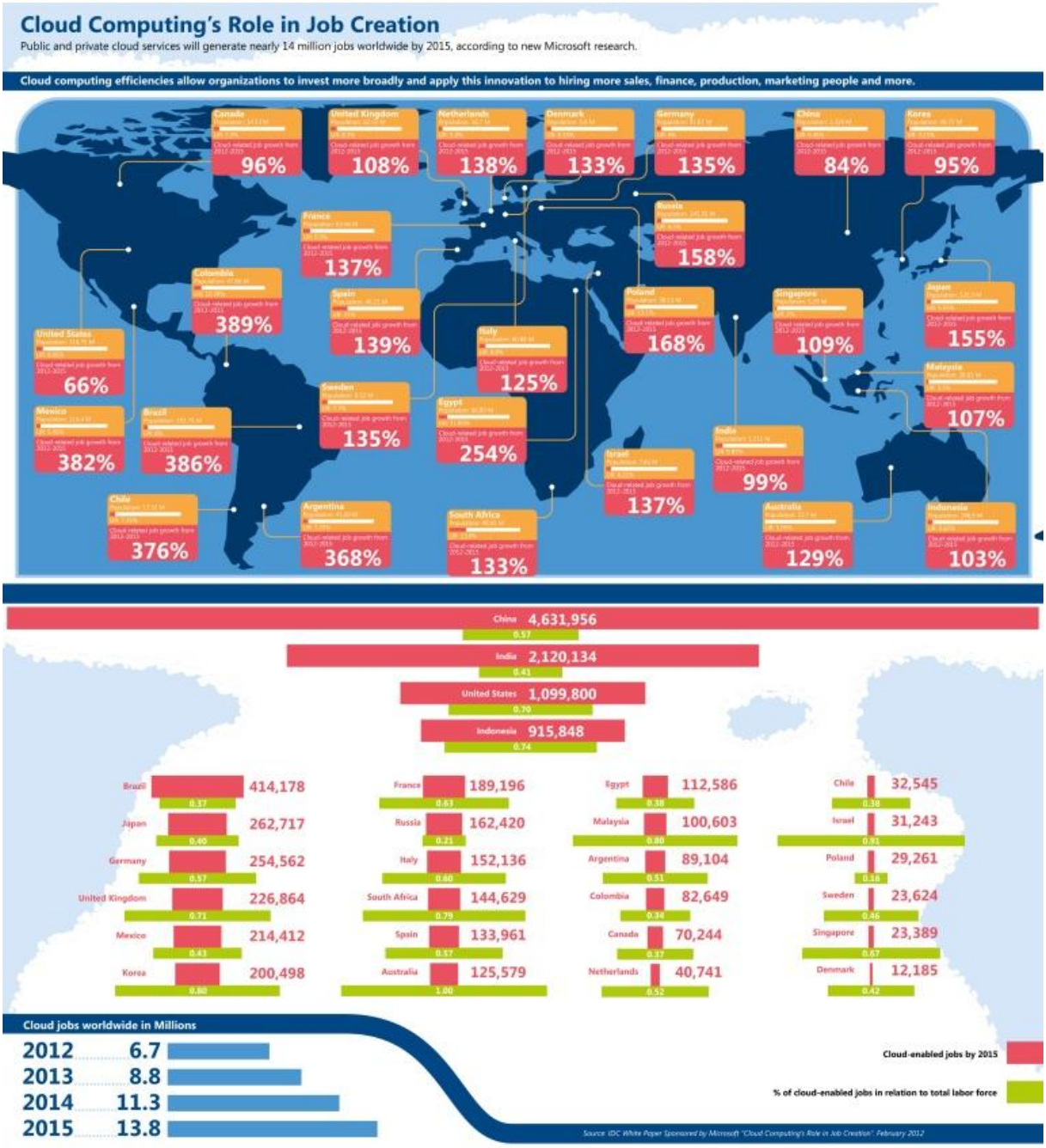

Figure 18 : Création d'emploi dans le cloud
Source : http://www.microsoft.com/presspass/images/features/2012/03-05CloudJobs_lg.jpg

3) Des outils d'accompagnement

Dans cette partie nous allons parler des différentes solutions d'accompagnement que peuvent utiliser les utilisateurs de services cloud. Les types de services que ces logiciels d'accompagnements fournissent sont assez variés.

a) Gestion, maintenance et migration

IBM a annoncé des fonctionnalités supplémentaires sur sa solution Tivoli, celle-ci étant un moyen extrêmement fiable de gérer les différents espaces de stockage. Celle-ci permet de gagner un temps conséquent sur la gestion du stockage car elle réduit le temps d'allocation des ressources.

Nimbula sort Nimbula director 2.0 qui se veut une solution d'aide au déploiement et à la gestion de solutions cloud basées sur l'offre VMware.

Egenera Pan Manager est un logiciel facilitant la migration des données vers une infrastructure VMware, la dernière version de ce logiciel améliore encore la flexibilité des clients qui désire migrer leur infrastructure sur des systèmes VMware.

Au niveau de la gestion des clusters sur lesquels reposent certaines solutions cloud, Caringo apporte une solution de gestion avec CAStor qui permet la création de fichiers de très grande taille de quatre téra-octets tout en étant plus performante que des solutions raid classiques.

Au niveau de la migration de cluster, Hitachi a conçu une solution permettant une gestion facilitée de la migration de clusters physiques Hitachi vers un cluster virtuel. Cela permet de limiter les risques lors de la mise en place de solutions cloud car ces dernières auront directement un espace de stockage virtualisé.

Au niveau des outils pour les développeurs on peut citer Cloud 9 qui est un IDE conçu pour développer sur la plateforme Microsoft Azure.

Toujours dans le monde Microsoft, Citrix permet d'accélérer la migration vers Windows Seven en fournissant des images personnalisées de machines fonctionnant avec ce système d'exploitation.

Si l'on se place du côté de l'utilisateur, il apparaît qu'il existe une multitude de solutions cloud qui disposent chacune d'une interface de gestion. Pour régler ce problème de complexité de gestion le consortium Apache en est venu à développer DeltaCloud qui est une interface de gestion normalisée pour tout type de cloud à travers des API.

b) Du nouveau côté matériel

Paul Maritz (PDG de VMware) évoque l'ère post-PC. En 2011, les ventes de Smartphones et de tablettes ont éclipsé le PC. Les fournisseurs de cloud et de virtualisation intensifient la tendance de remplacement de l'informatique orientée matériel par l'informatique en tant que service (IaaS) avec des entreprises « connectées » qui doivent gérer des terminaux et autres équipements mobiles (Il existe des services cloud comme Xerox pour gérer ces différents appareils utilisés à des fins professionnelles.

Le cloud grandissant, le matériel s'est adapté en conséquence et des associations se créent entre fabricants hardware et fournisseurs software (offres packagés), voici ce que nous avons observé :

Coté serveur :

Répondant à la croissance du trafic des données par le cloud, Intel présente sa famille de processeurs Intel Xeon E5-2600 pour les serveurs de cloud computing et les échanges de données entre appareils mobiles connectés. Ces processeurs fournissent des performances élevées, des innovations d'entrées/sorties ainsi que des fonctions de sécurité matérielle.

L'association d'Intel avec Maxthon Labs donnera naissance à une expérience de navigation accélérée par GPU améliorée pour les expériences web riches en contenu multimédia, notamment les services de cloud computing, jeux et vidéo.

IBM propose aussi une gamme de solutions serveurs, notamment à travers la ligne de produits x86 qui offre plus de puissance pour les machines virtuelles permettant un transfert rapide des données, nécessaire pour le cloud et l'analytique.

L'entreprise Silicon Graphics sort SGI InfiniteStorage modulaire JBOD : une plate-forme à haute densité d'extension de stockage qui peut être une solution viable pour le montage de gros nuages dans les espaces restreints.

Teradici propose une carte matérielle add-in (APEX 2800) pour améliorer les performances des implémentations VDI. Elle se branche dans n'importe quel emplacement PCIe et exécute certains pilotes logiciels communiquant avec VMware vSphere et ESX-i. En déchargeant l'encodage de l'image vers une carte d'encodage matériel, 50 % de la capacité du processeur peut être récupérée.

Coté client :

HP propose une solution de PC orienté terminal **:** ce type d'ordinateur fournit la puissance requise à la connexion et au pilotage d'un ordinateur distant (serveurs virtualisés). En cible : les administrations américaines du fait que leurs systèmes d'information soient orientés cloud. Un programme de client SafeBook léger pour Dell est aussi proposé par Devon IT.