// Syntec numérique

LIVRE BLANC
SÉCURITÉ DU CLOUD COMPUTING
Analyse des risques, réponses et bonnes pratiques

Syntec numérique

AVERTISSEMENT AU LECTEUR

Cet ouvrage vient compléter et détailler le premier livre blanc Cloud Computing édité par Syntec Numérique en avril 2010.

Apprendre en avançant

L'informatique, comme de nombreux domaines innovants, apprend en avançant. Ceci est vrai pour le Cloud Computing, dont les offres se définissent un peu plus précisément chaque jour. Ceci est tout aussi vrai pour les problématiques sécuritaires des TIC en général, et du Cloud Computing en particulier ! Cet ouvrage constitue donc une « photographie » des risques et solutions connus, traités et utilisés au moment de la rédaction de cet ouvrage (août à novembre 2010).

Cloud Computing &/ou Cloud Storage

Ce livre Blanc concerne principalement, et à dessein, le Cloud Computing (sécurité des données contenues dans les instances sur le Cloud). Seuls quelques paragraphes abordent explicitement les problématiques sécuritaires du « Cloud Storage » (traitement des données stockées sur des plates-formes distribuées).

Décideurs

Dans les lignes qui suivent, nous avons privilégié une approche pratique en ayant pour objectifs, non pas d'éduquer les RSSI sur la question, mais d'apporter des réponses simples et concrètes aux décideurs : DSI en particulier. Ceci explique :

- La rédaction d'un 2ème sommaire (thématique) répondant aux interrogations légitimes les plus courantes des DSI
- La mise en exergue, dès le chapitre 1, des 9 risques-majeurs liés à la sécurité des différents Clouds
- Les paragraphes traitant des aspects juridiques – et non pas uniquement techniques -de certains sujets
- La construction de l'ouvrage – pouvant parfois entraîner des redondances et concerner également des modèles plus traditionnels que le Cloud Computing –visant à aborder didactiquement la sécurité sur les aspects « physique », « logique » et « données » du Cloud.

La rédaction

EDITORIAL

"*Une méta-virtualisation de l'informatique par elle-même*", ainsi pourrait-on définir le Cloud Computing.
Il ne s'agit donc pas d'une technologie émergente - avec les errements et aléas indissociables que cela sous-entend - mais d'une abstraction, d'un concept de « présentation » qui ouvre la porte, pour ses usagers et clients, à de très nombreux avantages (*).

Pour l'industrie numérique elle-même, je retiendrai la compétition que le Cloud Computing suscite : les acteurs monolithes et dominants d'hier voient les cartes se rebattre à toute vitesse. Nouveaux entrants, nouveaux modèles économiques, nouvelles demandes, nouvelle « consommation » des TIC... les lignes bougent enfin, rendant ces moments d'autant plus exaltants !

Pour autant, cela ne doit pas inquiéter les entreprises clientes, et notamment les DSI. En effet, cette nouvelle redistribution des rôles précipite les alliances inédites, synonymes d'émulation, de créativité, d'ouverture, de standardisation, d'offres compétitives...

Observons le parcours sécuritaire de l'argent - lingots, bijoux et monnaie-or faciles à détrousser - remplacé au fil des... siècles par sa forme la plus abstraite actuelle : la carte bancaire, dont on aura noté le niveau élevé de sécurité. Une trentaine d'années aura suffi aux TIC pour que nos centres informatiques « Fort Knox » et leurs richesses se dématérialisent en Cloud Computing, gagnant tout autant en sécurité !

Sans tomber dans l'angélisme, nous pouvons affirmer qu'en matière de sécurité, le Cloud Computing n'est pas un agent « anxiogène » supplémentaire ! Ce deuxième livre blanc, entièrement consacré à cette thématique, en fait la preuve par 9 (comme les 9 risques-clés – et leur prévention - abordés dans les pages qui suivent).

Excellente lecture !

Philippe Hedde
Président du Comité Infrastructures
Syntec numérique

(*) Le premier livre blanc publié en début d'année par Syntec numérique avait su décrire parfaitement les concepts, atouts et limites du Cloud Computing (en libre téléchargement sur le site www.syntec-numerique.fr).

SOMMAIRE

SOMMAIRE CONTEXTUEL

INTRODUCTION

SUR LE CLOUD COMPUTING EN GÉNÉRAL

Avec l'apparition dans les années 1980 de la virtualisation, de l'infogérance et de l'externalisation ; avec la démocratisation de l'informatique dans les années 90 ; et - au cours de la dernière décennie - avec la généralisation d'Internet, le développement des réseaux à haut débit, la location d'application, le paiement à l'usage et la quête sociétale de mobilité… on peut expliquer à rebours l'avènement du Cloud Computing (CC).
Celui-ci consiste en une interconnexion et une coopération de ressources informatiques, situées au sein d'une même entité ou dans diverses structures internes, externes ou mixtes. Et dont les modes d'accès sont basés sur les protocoles et standards Internet.
Les solutions Cloud reposent sur des technologies de virtualisation et d'automatisation. Trois caractéristiques clés du Cloud le différencient de solutions traditionnelles :

- Services à la place de produits technologiques avec mise à jour en continu et automatiquement
- Self-service et paiement à l'usage (en fonction de ce que l'on consomme)
- Mutualisation et allocation dynamique de capacité (adaptation élastique aux pics de charge).

Vu des entreprises utilisatrices (du grand compte multinational à la PME locale), le Cloud Computing peut se définir comme une approche visant à disposer d'applications, de puissance de calcul, de moyens de stockage, etc. comme autant de « services ». Ceux-ci seront mutualisés, dématérialisés (donc indépendants de toutes contingences matérielles, logicielles et de communication), contractualisés (en termes de performances, niveau de sécurité, coûts…), évolutifs (en volume, fonction, caractéristiques…) et en libre-service.
Avec le CC, où passent donc les progiciels applicatifs, les bases de données, les serveurs et autres systèmes physiques de distribution, de communication, de sauvegarde et de stockage ?
Les machines, applications et données pourront être disséminées ou centralisées dans un, ou dans différents sites internes, chez des prestataires, dans un data center situé à l'autre bout de la planète ou sur une myriade de serveurs appartenant à un même « nuage ».
Partant de ces capacités d'abstraction et du paradigme des « services », le Cloud Computing peut être représenté en trois composantes principales – dont il est indifféremment l'une, les deux ou les trois combinées :

- **SaaS** (Software as a Service) : concerne les applications d'entreprise : CRM, outils collaboratifs, messagerie, BI, ERP,… Le modèle SaaS permet de déporter une application chez un tiers. Ce modèle convient à certaines catégories d'applications qui se doivent d'être globalement identiques pour tout le monde, la standardisation étant un des principes du cloud. Le terme SaaS évoque bien un service dans le sens où le fournisseur vend une fonction opérationnelle, et non des composants techniques requérant une compétence informatique
- **PaaS** (Platform as a Service) : concerne les environnements middleware, de développement, de test,… Le modèle PaaS consiste à mettre à disposition un environnement prêt à l'emploi, l'infrastructure étant masquée. Une plate-forme PaaS permet par exemple d'avoir un environnement de développement immédiatement disponible
- **IaaS** (Infrastructure as a Service) : concerne les serveurs, moyens de stockage, réseau, … Le modèle IaaS consiste à pouvoir disposer d'une infrastructure informatique disponible via un modèle de déploiement cloud computing. L'accès à la ressource est complet et sans restriction, équivalent de fait à la mise à disposition d'une infrastructure physique réelle. Ainsi une entreprise pourra par exemple louer des serveurs Linux, Windows ou autres systèmes, qui tourneront en fait dans une machine virtuelle chez le fournisseur de l'IaaS.

DIFFÉRENTS MODÈLES DE CLOUD COMPUTING

Si, pour le grand public, l'informatique « dans les nuages » fait référence globalement et sans autre précision à Internet, pour les entreprises il n'en est pas de même. Différents modèles de Cloud co-existent.

- **Cloud privé/privatif** : Il peut s'agir d'un « nuage » interne à la DSI (propriétaire des infrastructures) ou d'un Cloud entièrement dédié et accessible via des réseaux sécurisés, hébergé chez un tiers, mutualisé entre les différentes entités d'une seule et même entreprise. Ouvert aux partenaires privilégiés de l'entreprise (fournisseurs, bureaux d'études, grands clients, institutions financières, prestataires-clés…) voire à un groupement professionnel, le Cloud peut être également de type « communautaire ».
- **Cloud privé externalisé :** plate-forme de Cloud Computing qui vise à fournir, de manière externalisée, les garanties équivalentes à celles offertes par un Cloud Privé interne- avec, notamment, un accès à la plate-forme par des infrastructures privées (pas d'accès via Internet) – mais avec un niveau de mutualisation moindre que pour les plates-formes de Cloud Public, ce qui positionne économiquement ces offres entre le Cloud Public et le Cloud Privé.
- **Cloud public :** Il est externe à l'organisation, accessible via Internet, géré par un prestataire externe propriétaire des infrastructures, avec des ressources partagées entre plusieurs sociétés.
- **Cloud hybride :** Ici, il s'agit de la conjonction de deux ou plusieurs Cloud (public+privé) amenés à « coopérer », à partager entre eux applications et données.

LES PROBLÉMATIQUES SÉCURITAIRES ASSOCIÉES AU CLOUD COMPUTING

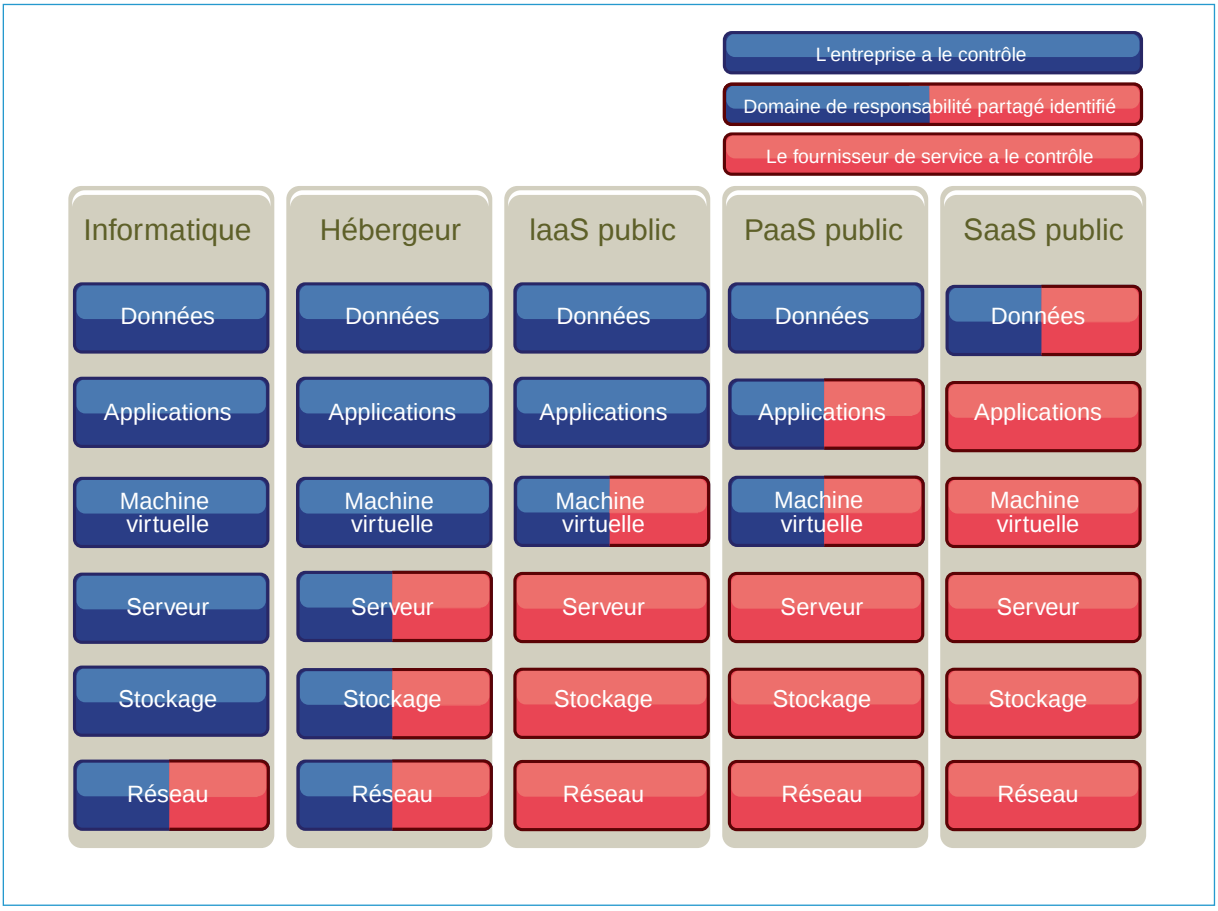
La « sécurité » est souvent citée comme le frein principal à l'adoption des services Cloud. Qu'en est-il réellement ? L'accès aux données hébergées dans le Cloud présente en général un haut niveau de sécurité en raison des mécanismes d'authentification mis en place par les fournisseurs de service. Ces mécanismes peuvent d'ailleurs être renforcés par les solutions Corporate clients, de gestion d'identités, qui sont alors placées en amont d'un lien unique avec le fournisseur de solutions Cloud ; notons cependant que certains fournisseurs seulement acceptent une telle architecture. Les entreprises clientes doivent toutefois 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 ?
- Quels sont les mécanismes de sécurité qui garantissent la confidentialité des données de l'entreprise au sein du cloud public ?
- Comment les données sensibles doivent-elles être envoyées et comment sont-elles accessibles? En clair ou en cryptant certaines d'entre elles ?

D'autres problèmes spécifiques au Cloud restent posés, notamment :

- Difficulté d'obtenir que certaines données restent localisées dans un pays désigné, le Cloud ne connaît pas de frontières ! Il faut alors être prêt à ce que le fournisseur doive se conformer à des réglementations comme la Directive Européenne de Protection des Données ou le USA Patriot Act, qui peuvent autoriser les autorités locales à prendre connaissance des données (cette possibilité est toutefois largement théorique)
- Impossibilité d'assurer la traçabilité des données, par exemple en vue des certifications SAS 70, Sarbanes Oxley ou autres, qui doivent garantir que nul n'a pu modifier des données sans qu'il en reste une trace. A noter : certains prestataires de services Cloud sont d'ores et déjà certifiés SAS 70 (type II).

Ces problèmes peuvent être en partie contournés par des architectures applicatives adaptées (*encryption* ou occultation de la propriété des données, et ségrégation des données contractuellement auditables).



Qui a le contrôle ?

ANALYSE DES RISQUES

L'inventaire des menaces et une analyse de risques sont préalables à tout projet informatique.
Cela permet de mieux appréhender le contexte d'utilisation du système d'information mis en œuvre.
Si l'apport du Cloud est indéniable, notamment en terme de flexibilité d'accès à des ressources informatiques, la concentration accrue des données et le transfert de certaines responsabilités nécessitent d'analyser les grandes familles de risques induits. On peut ainsi définir quatre catégories de risques à évaluer :

- les risques spécifiques liés aux aspects organisationnels, techniques et juridiques du Cloud
- les autres risques qui ne sont pas spécifiques au Cloud mais qui se retrouvent dans tout projet informatique.

Lors d'une analyse de risques, et à plus forte raison dans le cadre du Cloud, il faut avoir à l'esprit trois éléments de contexte :

- un risque doit toujours être analysé dans un contexte global. Le risque pouvant être contrebalancé par d'autres enjeux (économies, gains, délais...)
- le niveau de risque peut varier de façon significative selon le type d'architecture de Cloud pris en considération
- lorsque les risques sont transférés à un prestataire de service de Cloud, la prise en compte de ces risques par le prestataire, sous forme de service à valeur ajoutée, doit être intégrée dans le contrat.

NEUF PRINCIPAUX RISQUES IDENTIFIÉS

Les risques liés à l'utilisation du Cloud Computing doivent être pris en considération comparativement aux risques encourus par les environnements « traditionnels ».

RISQUE 1 : LA PERTE DE MAÎTRISE ET/OU DE GOUVERNANCE

Criticité : ***
Concerne : Cloud externe

Comme dans toute externalisation informatique traditionnelle, l'utilisation de services d'un prestataire Cloud se traduit d'une certaine manière par :

- un renoncement au contrôle sur son infrastructure
- la perte de la maîtrise directe du système d'information
- une gestion et une exploitation opaques.

RISQUE 2 : DES DÉFICIENCES AU NIVEAU DES INTERFACES ET DES APIs

Criticité : *
Concerne : Cloud interne et Cloud externe

Le niveau de portabilité actuel des services, des applications et surtout des données est encore peu probante : il y a peu de garanties sur les outils, les procédures, les formats de données et les interfaces de services. En cas de réversibilité ou de migration vers un autre fournisseur de services Cloud, les opérations peuvent être rendues très complexes, longues et coûteuses. En cas d'impossibilité de pouvoir revenir en arrière, le risque est élevé de se trouver captif d'une offre particulière.
D'autre part, le manque de clarté des spécifications des interfaces de programmation (APIs), leur pauvreté et le peu de contrôle à portée des clients sont autant de facteurs de risques supplémentaires. Les risques de compromissions liés à un dysfonctionnement des interfaces ou à des altérations de données sont donc à prendre en considération.
Les fournisseurs de services du Cloud proposent un ensemble d'API dont les clients se servent pour gérer et interagir entre leur SI et les services dans le Cloud. L'approvisionnement, la gestion, l'orchestration et le contrôle sont tous réalisés par le biais de ces interfaces.
La sécurité et la disponibilité des services du Cloud dépendent de la sécurité de ces APIs et de la qualité de l'intégration.
Toute API implique un risque potentiel de sécurité et même de rupture. Un problème au niveau de ces interfaces conduit à une perte totale ou partielle de service pour le client.
Ceci est vrai pour les Cloud publics et hybrides, car le SI de l'entreprise est à la fois en interne et dans le Cloud.

RISQUE 3 : CONFORMITÉ(S) ET MAINTIEN DE LA CONFORMITÉ

Criticité : **

Concerne : Cloud externe

Le contexte protéiforme du Cloud génère de nombreuses questions liées aux aspects règlementaires et juridiques. Et notamment :

- la responsabilité des données et des traitements
- la coopération avec les entités légales et de justice (des différents pays)
- la traçabilité de l'accès aux données aussi bien dans le Cloud, que lorsque ces données sont sauvegardées ou archivées
- la possibilité de réaliser des contrôles et des audits sur le respect des modes opératoires et des procédures
- le respect d'exigences réglementaires métiers.

De plus, lorsque des investissements initiaux ont été réalisés, lorsque des certifications ont été acquises ou des seuils de conformité atteints avant le passage sur le Cloud, toute dérive doit être détectée et une remise en conformité doit être recherchée. L'impossibilité d'effectuer des contrôles, voire des audits formels (ou leur non réalisation) risque alors de devenir problématique.

De plus, certains types d'infrastructure rendent impossible le respect de critères normatifs (PCI DSS et Cloud public).

RISQUE 4 : LOCALISATION DES DONNÉES

Criticité : ***

Concerne : Cloud externe

La dématérialisation des données sur des sites physiques de stockage différents peut conduire à un éclatement des données et une répartition dans différents pays. Un manque de maîtrise de cette répartition géographique est susceptible de provoquer le non-respect de contraintes réglementaires liées à la localisation des données sur le territoire d'un Etat.

RISQUE 5 : SÉGRÉGATION / ISOLEMENT DES ENVIRONNEMENTS ET DES DONNÉES

Criticité : ***

Concerne : Cloud externe

La mutualisation des moyens est l'une des caractéristiques fondamentale du Cloud. Mais les risques afférents sont nombreux, souvent liés aux mécanismes de séparation :

- L'étanchéité entre différents environnements utilisateurs ou clients est une condition sine qua non afin de garantir, a minima, la confidentialité des traitements
- L'isolation des données sous leurs différentes formes (stockage, mémoire, transmission et routage, ...) : elle est réalisée au moyen de différents services de sécurité ou techniques de sécurisation, telles que le contrôle d'accès et le chiffrement
- L'allocation des ressources : la monopolisation de ressources matérielles par un environnement utilisateur ou client ne doit pas être possible au détriment de la disponibilité ou, à moindre échelles, de la diminution des performances des environnements voisins.

Dans le cas d'un environnement partagé entre plusieurs "clients locataires", deux sortes d'attaque sont possibles, de type "*guest-hopping*" et contre les hyperviseurs.

LES VERTUS DE LA CERTIFICATION SAS 70

Créée par l'American Institute of Certified Public Accountants, la norme SAS 70 concerne les entreprises qui font appel à des fournisseurs spécialisés pour externaliser leurs services. Elle se caractérise par des audits indépendants réalisés par des tiers et des vérifications des processus sur site.

SAS 70 comporte deux niveaux (Type I et type II). Le premier porte sur la description des activités de la société et sur la pertinence des contrôles. Le deuxième niveau évalue leur efficacité à travers des tests dont les résultats sont publiés dans le rapport SAS 70 (type II).

Avantage-clé pour le fournisseur : éviter de multiples audits réalisés régulièrement par ses différents clients. C'est également un moyen important de différenciation commerciale.

Pour les entreprises-clientes, et en particulier celles soumises à la loi Sarbanes-Oxley, la certification SAS 70 garantit notamment la conformité et le « bon ordre » de leurs fournisseurs.

(source : Wikipedia)

RISQUE 6 : PERTE ET DESTRUCTION MAÎTRISÉE DE DONNÉES

Criticité : ***

Concerne : Cloud externe

Les pertes de données ne sont pas spécifiquement liées au Cloud, et les deux grandes familles de risques sont :

- les pertes liées à des problèmes lors de l'exploitation et la gestion du Cloud ;
- un défaut de sauvegarde des données gérées dans le Cloud.

S'ajoutent des risques liés à la non suppression de données (celles à ne pas conserver). En effet, une donnée peut exister logiquement sous les quatre formes suivantes – et bien plus au niveau physique – : les données en ligne (on-line) ou hors ligne (off-line), et les données sauvegardées (souvent en plusieurs versions) ou archivées (parfois en plusieurs versions).

Lorsqu'une demande de suppression d'une donnée située dans le Cloud est émise, cela doit se traduire par une suppression réelle, mais pas nécessairement sous toutes ses formes. En revanche, lorsqu'une demande de suppression définitive d'une donnée est émise, suite à une rupture contractuelle par exemple, ou pour des raisons légales, la suppression doit être effectuée sur toutes les formes que peut prendre cette donnée. Avec la répartition/dissémination des données il est nécessaire de retrouver toutes les instances de cette donnée, ce qui peut s'avérer être une tâche complexe dans le cas de multiples localisations et de la réutilisation des ressources matérielles. Lors d'une suppression sur disque, les données doivent être non seulement désallouées, mais aussi nettoyées (écrasement par motif), ceci afin de ne pas révéler ces anciennes données en les rendant accessibles au suivant à la prochain réallocation de disques au sein du Cloud.

RISQUE 7 : RÉCUPÉRATION DES DONNÉES

Criticité : *

Concerne : Cloud externe, Cloud interne

Il est indispensable d'avoir la garantie de disposer des moyens pour la récupération de données en cas de problèmes autres que les cas de non-disponibilité. La récupération doit pouvoir s'effectuer dans conditions de délais respectant les contraintes exprimées et les besoins métiers. La dissémination des données doit toutefois être effectuée de façon transparente pour l'utilisateur du Cloud.

RISQUE 8 : MALVEILLANCE DANS L'UTILISATION

Criticité : **

Concerne : Cloud externe, Cloud interne

Les architectures de type Cloud sont gérées et exploitées par des personnes disposant de privilèges élevés et qui sont donc à risque élevé. Des dommages peuvent être causés par ces spécialistes techniques. Les risques d'accès non-autorisés aux données ou d'utilisation abusive doivent être pris anticipés. Les dommages causés par des administrateurs système du Cloud - même s'ils sont rares - s'avèrent plus dévastateurs que dans un environnement informatique classique. Des procédures et des moyens sont nécessaires tant pour les phases de prévention et de détection, que pour les phases de protection et de réaction.

RISQUE 9 : USURPATION

Criticité : ***

Concerne : Cloud externe, Cloud interne

Les risques d'usurpation d'identité sont de deux natures :

- L'usurpation de service offert par l'architecture Cloud : il peut s'agir de services similaires, voire identiques, offerts par d'autres offreurs ou en d'autres points du Cloud pour d'autres clients. A l'extrême, on peut se retrouver confronté à des problématiques telles que celle du phishing (hameçonnage).
- L'usurpation d'identité d'utilisateurs ou de clients des services du Cloud : il peut s'agir d'attaques liées au vol de l'identité d'utilisateurs de services suite à des déficiences dans les mécanismes d'authentification. De faux clients utiliseraient de façon indue des ressources, voire accèderaient aux données des clients légitimes.

Dans les deux cas, la faiblesse de l'identification et de l'authentification laisserait la porte ouverte à ces attaques.

LIMITES DU TRANSFERT DE RISQUE

Le transfert de risque du client au prestataire de services de type Cloud ne peut pas être total. Si un risque conduit à la disparition d'une entreprise, à des atteintes sérieuses à sa réputation ou à des conséquences juridiques graves, il sera difficile voire impossible, pour quelque partie que ce soit, de compenser ces dommages. En définitive, on peut déléguer la responsabilité, mais pas s'en décharger complètement.

SECURITE PHYSIQUE

Le Cloud Computing, par nature, est associé à une sorte de « dématérialisation » de l'hébergement (le nuage). En effet, le lieu d'hébergement du Cloud est généralement multiple, et réparti sur plusieurs data centers, en France et/ou à l'étranger. Dans le cas du Cloud public, le client ne connaît donc pas avec précision le ou les lieux d'hébergement du Cloud.
Cette caractéristique, gage de disponibilité du Cloud, entraîne un changement important pour le client dans le mode de sélection de l'hébergeur.
Une visite de data center ne suffit plus pour évaluer le niveau d'hébergement garanti par un fournisseur de Cloud. Ce dernier doit être en mesure d'apporter des garanties sur les conditions d'hébergement associées à son offre.
Un certain nombre de certifications et/ou de classifications existent à ce sujet, sont reconnues et adoptées par l'ensemble des hébergeurs. L'une des plus représentatives étant la classification « Tier » de l'Uptime Institute .

ACCÈS PHYSIQUE

L'accès physique d'une seule personne mal intentionnée qui possède une excellente connaissance de l'implémentation physique du CC et de ses points névralgiques peut suffire à mettre hors service le Cloud, provoquant une rupture dans la continuité du service et empêchant tout accès externe au Cloud.
Les conséquences d'une telle intrusion peuvent être désastreuses :

- isolement complet ou partiel du service dans le cas de coupure des liaisons d'accès
- perte des données en production mais aussi des données sauvegardées, sans aucune possibilité de récupération si celles-ci sont détruites ou détériorées, hors des données déjà sauvegardées (externalisation et/ou réplications).
- risque d'incendie élevé ou d'inondation...

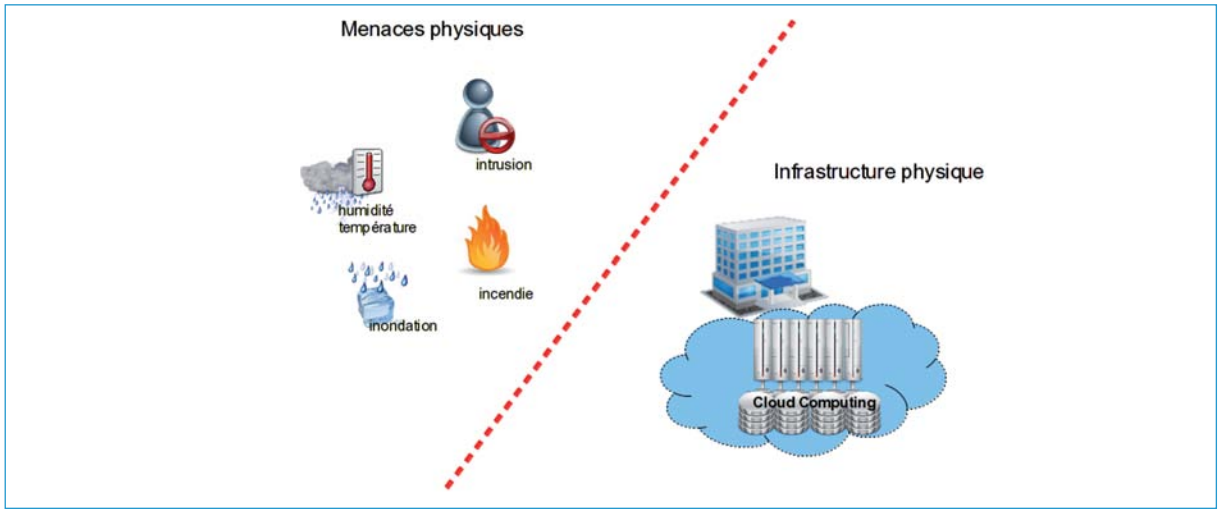
CONTRÔLE ET TRAÇABILITÉ DES ACCÈS

Point critique de la sécurité physique, le contrôle des accès doit être maitrisé, que l'on soit dans un contexte de cloud privé, public ou privé externalisé. Dans ces deux derniers cas, c'est au client final de s'assurer que les bonnes pratiques sont mises en œuvre chez son prestataire de service/opérateur de cloud.

Concrètement, les va-et-vient du personnel interne et des prestataires externes (informatique et télécoms, société de maintenance, de nettoyage, …) sont nombreux dans une salle informatique ou dans les locaux techniques.

Ce flux représente une source potentielle de dysfonctionnements, volontaires ou non.

Il convient de bien délimiter les zones les plus sensibles et de mettre en place des garde-fous suffisamment efficaces pour retrouver, le cas échéant, l'origine d'un incident. L'accès aux zones sensibles (serveurs, réseau...) sera interdit et le passage dans les zones intermédiaires sera limité. Le personnel autorisé devra être informé du caractère sensible des zones dans lesquelles il est amené à intervenir.



Sécurisation de l'environnement

BONNES PRATIQUES DE LA SÉCURITÉ PHYSIQUE

• Découper les locaux informatiques en zones de sécurité concentriques, regrouper le matériel le plus sensible dans les zones les mieux protégées
• Déporter à l'extérieur des locaux les accès de maintenance ordinaire (eau, électricité, ascenseurs...)
• Eloigner les supports de sauvegarde (bandes, cassettes, CD...) des locaux, si possible du bâtiment. La répartition du système de stockage sur plusieurs data centers permet de limiter les risques de perte totale du service en améliorant la tolérance de panne.
• Contrôler l'accès par des systèmes à clé, cartes, digicodes..., faciles à utiliser et dont les listes d'accès sont actualisées en permanence
• Installer des systèmes de surveillance extérieure permanente (caméras, détecteurs de présence...)
• Enregistrer en vidéo les entrées et sorties (très dissuasif). L'enregistrement doit pouvoir durer entre le moment d'une intrusion et le moment de la constatation d'une malveillance, y compris pendant les congés tout en respectant les réglementations de protections liées à l'utilisation des données personnelles (en France, la CNIL)
• Mettre en œuvre de bonnes pratiques pour accompagner durant leur venue les visiteurs. On les adaptera selon le niveau de criticité :
- établir une politique d'accès générale comprenant toutes les exceptions
- y soumettre tous les utilisateurs du site
- identifier clairement les visiteurs par un badge spécial à durée limitée
- installer des sanitaires/vestiaires pour les visiteurs
- ne jamais laisser un visiteur seul se promener dans le bâtiment
- tout visiteur doit avoir une autorisation d'accès délivrée par un responsable (maintenance, entretien, visites, réunions, …)
- concevoir le data center de façon à ce que la présence d'équipes de nettoyage ne soit pas nécessaire dans la salle des serveurs (mobilier anti-statique, filtres à particules, …).

Au-delà des contrôles d'accès et de la sécurité physique, il est tout aussi important de porter attention à la « conception sécurisée » des data center- centres d'hébergement d'un cloud privé ou public.
Les bonnes pratiques décrites ci-après constituent autant de points de vigilance pour la mise en œuvre d'une solution privée, ou pour le choix d'un prestataire de cloud public.

L'emplacement d'une salle informatique doit être adapté et réfléchi en fonction de :
• de l'environnement (vigilance sur les zones à risques)
• des types de risques déterminés
• des charges au sol…

La sécurisation de la **partie énergie** :
• Energie de haute qualité
- Onduleurs ou chaîne d'onduleurs
- Source dédiée uniquement à la salle informatique
• Secours
- Deux ou plusieurs arrivées d'alimentation
- Autonomie en cas de perte du réseau
- Redondance des onduleurs
- Groupe électrogène (autonomie définie par la capacité de la cuve de fioul, idéalement 72h)
• Dimensionnement des sources
- Bilan de puissance des machines installées et estimées dans le futur
• Distribution
- Deux ou plusieurs MT/BT en fonction du nombre d'arrivées d'alimentations (inductions électriques)
- Armoires divisionnaires
- Alimentation des baies et machines : deux ou plusieurs départs par baie, alimentées depuis des armoires distinctes ; alimentation personnalisée pour des matériels spécifiques (SAN, stockage…)

Pour la **climatisation**, on préconise :
• Une solution dédiée à la salle à refroidir
• Une redondance des climatiseurs
• Un groupe électrogène spécifique pour les climatiseurs
• Une urbanisation de la salle alternant allées chaudes et allées froides

La **sécurité incendie** nécessite :

- Des systèmes de détection optique/ linéaires par faisceau laser/ de flamme/ d'analyse de particules
- Une extinction automatique et non destructrice (ex gaz inibiteurs type FM200).

Tout au long de la durée d'exploitation, l'ensemble de ces systèmes doivent être maintenus et supervisés, afin d'identifier les alarmes techniques liées à d'éventuels dysfonctionnements sur ces équipements (surveillance multi-technique).

REDONDANCE MATÉRIELLE

L'architecture Cloud Computing doit garantir un accès au service en très haute disponibilité avec des performances optimales. La seule défaillance d'un équipement matériel peut engendrer une dégradation ou une coupure du service voire une perte de données. Pour limiter les risques d'arrêt de service liés à la défaillance d'un équipement, il est nécessaire de le redonder.

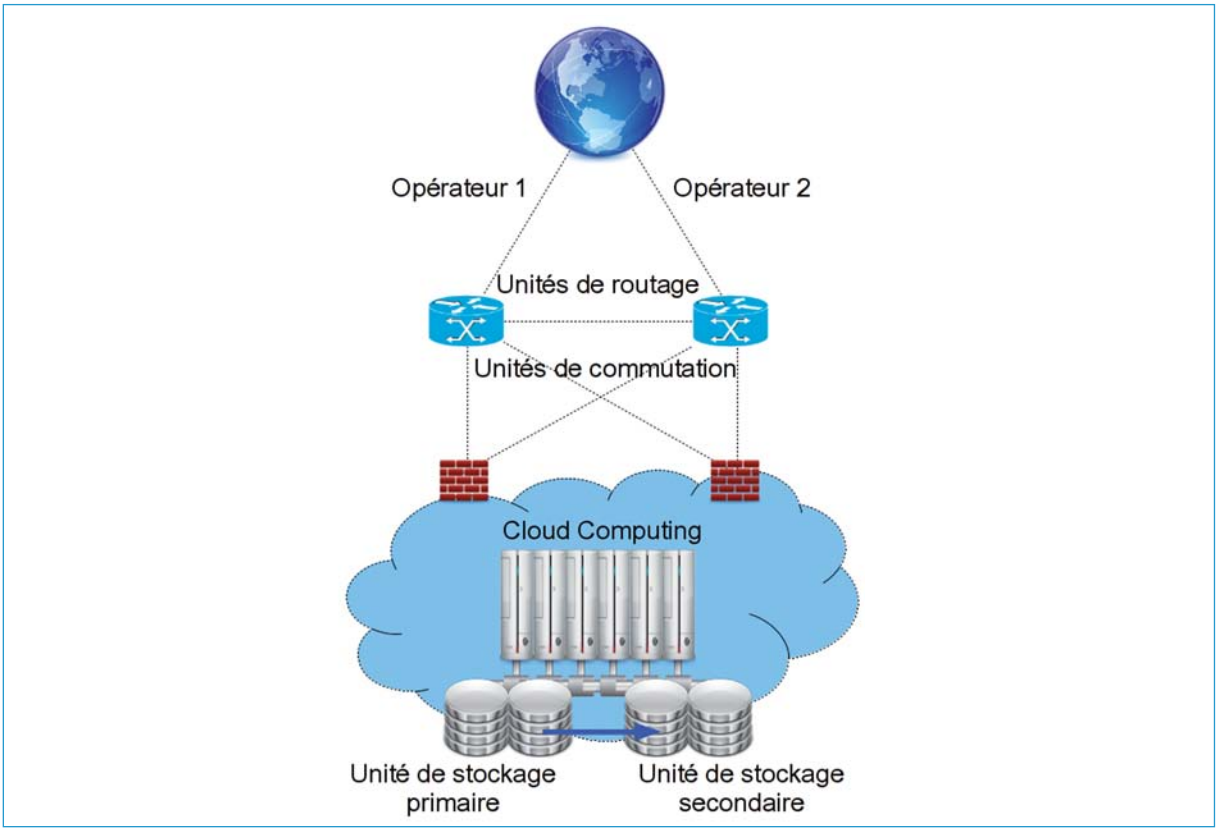
Une réplication des configurations entre les équipements peut faciliter la bonne prise en charge de la redondance et ainsi augmenter la haute disponibilité du service. La mise en œuvre d'une redondance différentielle avec une sélection d'équipements de natures différentes (ex : différents constructeurs, composants d'origines différentes ...), permet de se protéger d'un problème survenu à un équipement donné.

De plus, une redondance des moyens de connexion, par la multiplication des liaisons, des opérateurs, et des chemins d'accès permet une accessibilité accrue au service en augmentant la tolérance aux pannes.

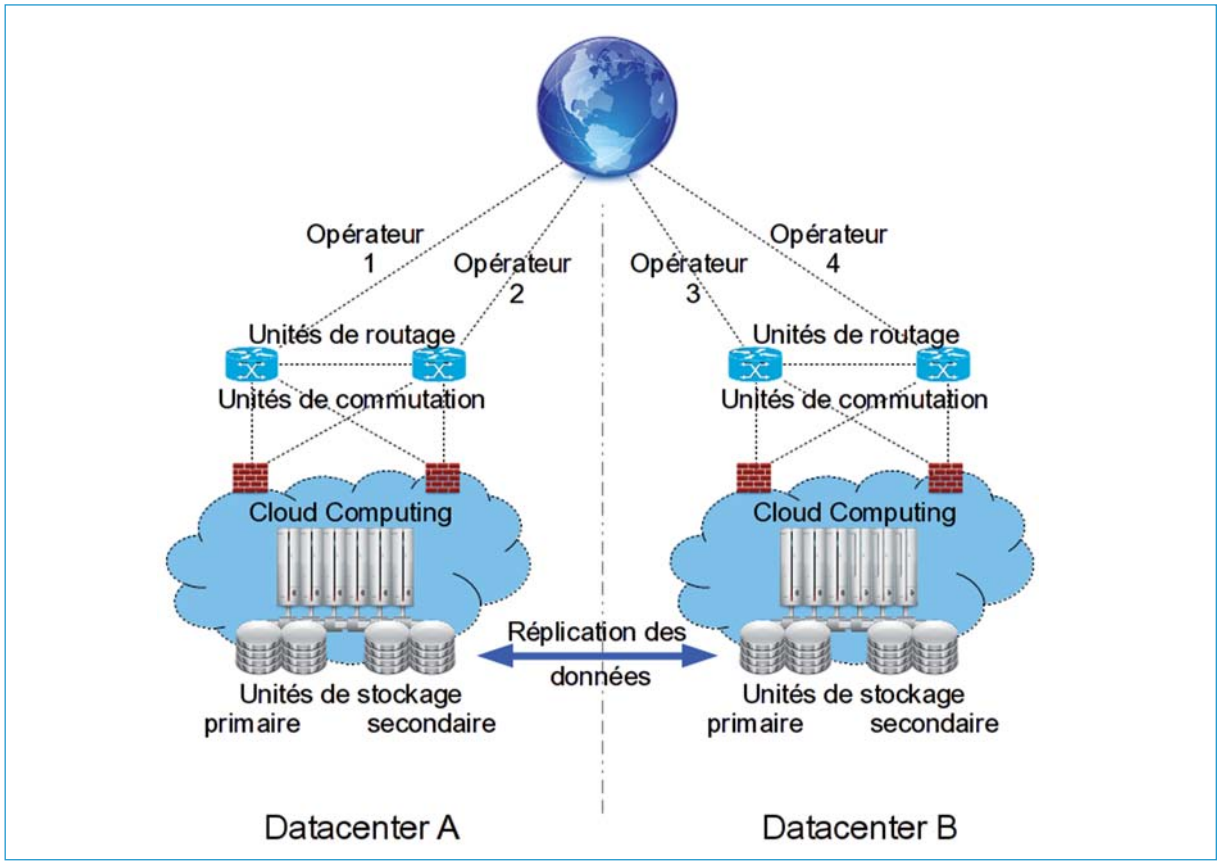
RÉSILIENCE

Une catastrophe d'origine humaine ou naturelle peut avoir des impacts radicaux sur le fonctionnement du Cloud Computing et amplifier une panne totale ou partielle du service. La perte totale de l'infrastructure du Cloud Computing pourrait entrainer une interruption de service d'une durée indéterminée et une perte de données irrémédiable sans possibilité de remise en service de l'infrastructure.

Une architecture de secours doit exister, sur un site géographiquement éloigné, avec des équipements redondants (voir chapitre redondance différentielle) et permettant de réaliser un PCA (plan de continuité d'activité) sans interruption de service.



Présentation d'une architecture mono-data center



Présentation d'une architecture multi-data center

SECURITE LOGIQUE

SÉCURITÉ DES SERVEURS VIRTUELS

Le Cloud Computing s'appuie fortement sur les technologies d'abstraction de services.
Dans le cadre d'un modèle IaaS, c'est la virtualisation de serveurs qui fournit cette abstraction ; l'élément de base, visible ou non, étant une machine virtuelle (VM) sur un hyperviseur. L'hyperviseur héberge également une VM particulière que nous appellerons de manière générique la « partition de gestion » (le vocabulaire varie selon le fournisseur). Elle permet d'administrer l'hyperviseur, de gérer le matériel et les ressources virtualisées.

Généralement on discerne les bonnes pratiques de sécurité liées à la virtualisation en deux familles. En premier lieu, il s'agit de sécuriser les systèmes en assurant une gestion des mises à jour de sécurité. La mise à jour de l'hyperviseur et de la partition de gestion, a priori à la charge de l'hébergeur, conduit dans la plupart des cas à un redémarrage du serveur. Pour éviter que les VM soient indisponibles durant l'opération, un mécanisme de déplacement automatique des VM vers un autre serveur est possible, voire recommandé.

La sécurisation des systèmes suppose également la réduction des surfaces d'attaque, en fixant au strict minimum les services de la « partition de gestion ». On protège également les fichiers des disques virtuels par du contrôle d'accès, de l'audit, voire du chiffrement. Idéalement, on agit conformément aux recommandations des fournisseurs de l'hyperviseur (configuration des disques virtuels, installation de composants d'intégration dans les VM, etc.) et des OS, en mettant en place un contrôle de conformité automatisé.

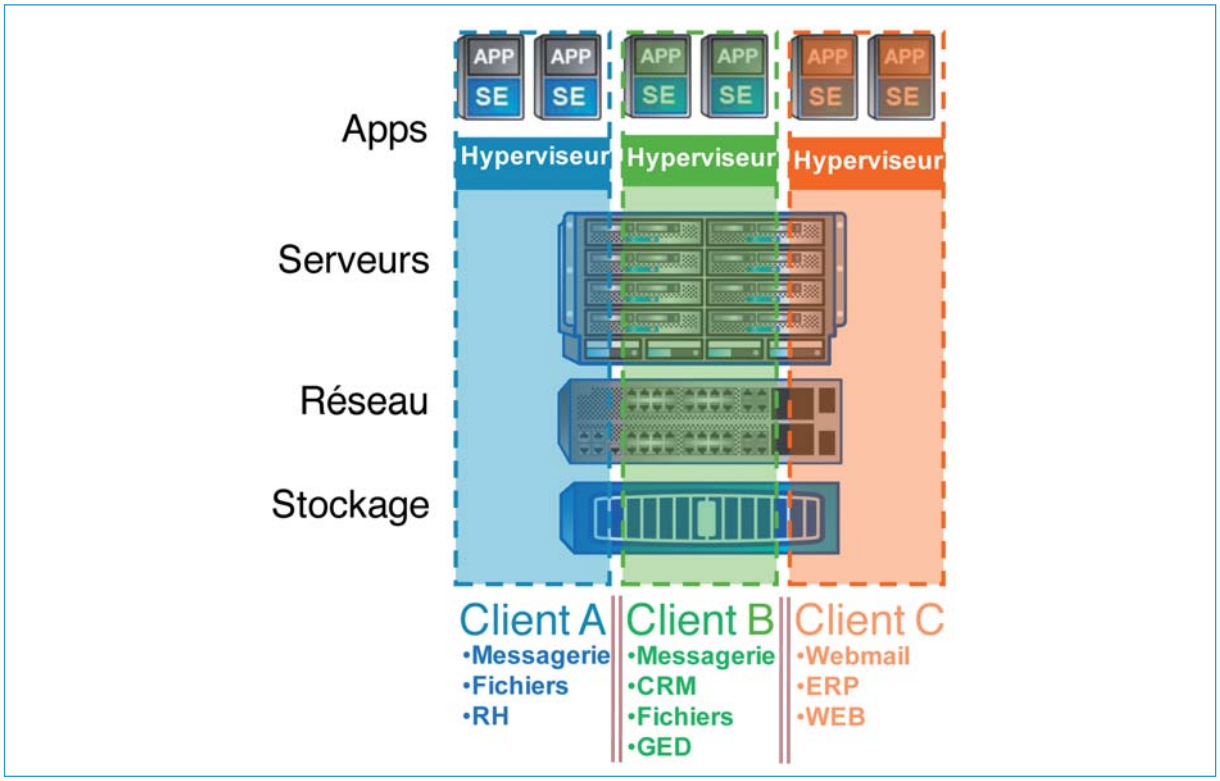
La seconde famille de bonnes pratiques concerne la notion d'isolation : isolation des flux réseaux, isolation des VM par niveau de sécurité, délégation de l'administration, affectation de quotas d'usage des ressources par les VM.
L'infrastructure de type cloud - pour être efficace et rentable - doit automatiser la plupart des contraintes évoquées précédemment, en plus des processus liées à l'administration, la supervision et l'allocation automatique de ressources.

BONNES PRATIQUES DE CONFIGURATION DES MACHINES VIRTUELLES

- L'entreprise cliente sera attentive au fait que le Cloud provider devra :
- Utiliser des disques durs virtuels de taille fixe
- Protéger les disques durs virtuels et les snapshots par des ACL sur le disque
- Décider de la mémoire allouée à chaque machine virtuelle
- Imposer des limites sur l'utilisation du processeur
- Concevoir le réseau virtuel de façon à isoler le trafic réseau en fonction des besoins
- Limiter le nombre de disques durs virtuels en fonction des besoins
- Sécuriser le système d'exploitation des machines virtuelles selon les recommandations de l'éditeur
- Configurer les antivirus, pare-feu et logiciels de détection d'intrusion dans les machines virtuelles en fonction de leur rôle
- S'assurer que, avant sa (re)mise en production, une machine virtuelle est à jour en termes de versions et de mises à jour de sécurité de tous les composants logiciels qu'elle héberge
- Installer les composants d'intégration de l'hyperviseur, de façon notamment à s'assurer que les machines virtuelles ont une horloge juste (pour les audits)

LA COLOCATION SÉCURISÉE

La colocation sécurisée consiste en l'hébergement sur le Cloud des applications et données de multiples clients (sociétés, organisations, entités métier…) au sein d'une seule et unique infrastructure physique, mutualisée, tout en respectant la sécurité, notamment au sens de la confidentialité.
A juste titre, les sociétés-clientes du Cloud veulent être rassurées sur le fait que leurs données et traitements seront bien isolés et protégés des autres environnements hébergés sur l'infrastructure partagée. C'est souvent une obligation légale, par exemple lorsqu'une société stocke des numéros de cartes bancaires ou des données personnelles, médicales…
Comment essayer de satisfaire ces deux impératifs de confidentialité et d'efficacité pour les infrastructures Cloud, et à tous les niveaux : machines virtuelles, serveurs hôte, réseaux (Ethernet et SAN) et stockage ?
En plus d'appliquer rigoureusement les bases de la sécurité d'un système d'information mutualisé (planification rigoureuse des droits d'accès, des privilèges administrateurs, sécurisation des mots de passe, etc.…), certaines techniques ou architectures permettent de tendre vers ce but. En voici des exemples.



Colocation sécurisée

Le chiffrement

Le chiffrement est *a-priori* séduisant, notamment la méthode classique à base de clé publique/clé privée : seul le destinataire de l'information peut déchiffrer la donnée qui lui est destinée avec sa clé privée, connue de lui seul, mais pas du fournisseur de la solution Cloud et moins encore d'un autre colocataire. C'est une méthode très sécurisée (selon la taille de la clé) et sélective car on peut choisir de ne chiffrer que ce qui le nécessite.

Toutefois le chiffrement impose certaines réflexions quant à son implémentation. Notamment dans le cas où des traitements sont nécessaires (calcul, indexation, sauvegarde), pouvant obliger à la manipulation de données décryptées.

Solutions d'étanchéité logiques

Faire appel à des solutions d'étanchéité logiques permet de fournir les ressources à des groupes différents d'utilisateurs en toute sécurité.

Au niveau des VM, on peut utiliser un firewall virtuel sur la machine hôte qui cloisonne les VMS ; les VLANs permettent de cloisonner le trafic réseau sur Ethernet ; des partitions virtuelles de stockage apportent l'étanchéité dans la baie de stockage.

Différentes approches sont possibles : on peut retenir la solution la plus pertinente et mature sur chaque couche (selon une approche « best of breed » : la meilleure de sa catégorie), ce qui assure une certaine indépendance dans le choix de chaque solution, mais nécessite d'être certain de la qualité de l'intégration des différentes solutions de sécurisation de chaque couche. Comme souvent, ce n'est pas parce que chaque couche est sécurisée que l'ensemble le sera (attention au maillon faible et à l'interfaçage entre les différentes couches).

Une autre approche consiste à retenir une solution d'infrastructure sur étagère, proposée par un fournisseur unique ou un ensemble de fournisseurs. On perd en indépendance, car les différents composants (serveur, réseau, stockage) sont imposés, mais on gagne en intégration et en sécurisation. En effet, pour simplifier les déploiements de solutions mutualisées et pour en améliorer la confidentialité, certaines sociétés se sont alliés, ont co-réalisé et co-validé des solutions « tout-en-un » et/ou des guides de conception complets qu'ils mettent à disposition des fournisseurs de solution Cloud.

Avantage de cette dernière approche : l'étanchéité est assurée logiquement et de bout en bout, de l'application (la VM) aux disques (la baie de stockage mutualisée, cloisonnée en partitions virtuelles étanches), en passant par le réseau, afin de ne jamais mettre en danger les informations sensibles.

SEGMENTATION RÉSEAU

La segmentation réseau des machines virtuelles (VM) doit parer aux risques classiques de tout serveur, mais également à des risques liés à la colocation dans le cas d'un Cloud public.

Les risques classiques

Il faut appliquer les mêmes règles dans la virtualisation que dans une architecture physique :

- Cloisonner les différents rôles (serveurs frontaux, données, applications, pré-production …) sur des VM différentes via des VLAN différents (réseau dédié à une VM ou a un rôle) entre le serveur physique et l'infrastructure du client
- Mettre en place des briques de sécurité (firewall, reverse proxy …) qui assurent les rôles de :
  - Routage inter-VLAN : pour que les VM communiquent sur des ports applicatifs spécifiés
  - Filtrage (analyse port source/destination)
  - Sécurité applicative (vérification protocolaire)

Administrer ses VM via un réseau dédié pour superviser, mettre à jour et ainsi ne pas passer par le réseau frontal/public.

La politique de sécurité mise en place dans l'architecture Cloud doit être appliquée sur la durée avec un contrôle permanent et une mise en œuvre de bonnes pratiques au quotidien : procédures d'exploitation, tests d'intrusion …

Les risques accentués par le Cloud, liés à la multi-location :

La colocation et le partage de l'infrastructure entre plusieurs clients engendrent des risques accrus et nécessitent un renforcement de la politique de sécurité.

Chiffrer les sauvegardes : alors qu'il est naturel de penser à l'implémentation des protocoles de production chiffrés comme le passage en HTTPS pour les sites Web ou Intranet, il est moins commun de penser à la protection des tâches de plus bas niveau

Conflits et usurpation d'adressage : les machines étant virtuelles, il est plus facile dans ce contexte de générer des conflits d'adressage. Ainsi, une attention particulière doit être portée à la liste des personnes ayant un droit d'administration sur le Cloud. Cloner une instance déjà présente sans prendre en compte ces considérations peut être une source de problème

SÉCURITÉ DE L'INTERFACE D'ADMINISTRATION

L'accessibilité aux interfaces d'administration via une vulnérabilité applicative expose aux risques d'une coupure partielle ou totale du service ou à une perte irrémédiable des données. Par cet accès, l'introduction de virus ou de vers peut également détériorer les applications, faciliter la corruption des données ou nuire à l'image de marque du service.

Les solutions préventives consistent en la mise en place d'équipements de filtrage (pare-feu, proxy, sondes IPS/IDS...) et de solutions antivirus afin de contrôler la légitimité des requêtes entrantes et ainsi garantir l'intégrité des données hébergées. La planification de tests de vulnérabilités et d'intrusions doit être régulière et fréquente.

Le développement des applications doit être soumis à des audits de codes réguliers, et à l'implémentation de règles et contrôles des données.

Authentification

L'accès aux interfaces d'administration du Cloud Computing pourrait permettre à une personne mal intentionnée de provoquer une coupure de service ou de corrompre les données hébergées.

Si l'accès authentifié n'est pas clairement identifié, alors il sera impossible de pouvoir tracer la connexion et la modification des données ou du service qui en résulte. L'authentification doit apporter une preuve de l'identité si on veut pouvoir enquêter sur d'éventuels accès suspects.

Une vulnérabilité provenant d'erreur, de faille « humaine » ou «d'hameçonnage» dans le processus d'authentification peut aussi être exploitée. Celle-ci pourrait donner des accès de type «administrateur » à l'architecture Cloud Computing et entraîner une corruption de la plate-forme.

Les bonnes pratiques en la matière sont :

- La mise en place de mécanismes d'authentification forte (reposant sur deux facteurs ou plus) : identifiant, mot de passe, accès par jeton, certificat électronique, contrôle biométrique ...
- L'identification de l'authentification afin de disposer d'une traçabilité des accès
- La journalisation des authentifications réussies ou échouées

• La stricte application d'une politique de sécurité : changement des mots de passe tous les mois, politique de mots de passe complexes, formation du personnel...

Sécurisation des accès

Pour maitriser la sécurité de bout en bout, il faut sécuriser les éléments constituant la plate-forme Cloud, mais également l'accès à cette plate-forme.

Dans le cas d'un accès aux services hébergés sur le cloud par internet, le serveur (VM) est nativement vulnérable puisqu'il est directement exposé sur la Toile. Deux solutions de sécurisation peuvent être appliquées :

• inclure des briques de sécurité type Firewall (ouvre les ports applicatifs nécessaire), IPS ou IDS (détection et protection d'intrusion) entre l'infrastructure cloud et le client mais aussi éventuellement au sein de l'architecture serveur, entre serveurs front office et serveurs back office. (cette dernière solution n'est possible que dans les environnements de cloud privés dans lesquels les serveurs n'ont pas d'adresse IP publique)
• sécuriser chaque serveur virtuel par un firewall applicatif installé sur l'OS (ou IPS, IDS applicatif). Cela suppose néanmoins une gestion lourde des règles d'accès avec internet et entre serveurs virtuels.

Ce type d'accès n'est envisageable que pour des serveurs hébergeant des données publiques (serveur FTP public, site web …) peu sensibles pour l'entreprise.

Si le serveur héberge des services privés de l'entreprise (ERP, CRM, intranet …) et constitue alors une extension du SI, le serveur ne doit pas être visible d'internet et des solutions de connexions dédiées doivent impérativement être envisagées, telles que :

• Connexion VPN privée : l'accès aux serveurs du cloud se fait via des liaisons dédiées (fibre, xDSL, multi-opérateur …) entre le cloud et l'utilisateur

• Connexion VPN internet : l'accès aux serveurs du cloud se fait via une connexion sécurisée par des mécanismes de chiffrement et d'identification (IPSEC ou TLS) montée entre le cloud et l'utilisateur, via le transit internet.

Accessibilité

Quel que soit le type de connexion au cloud, dédiée ou via Internet, il faut s'assurer que le service hébergé reste joignable par les utilisateurs. L'accessibilité aux serveurs doit être ajustée au niveau de disponibilité de ceux-ci. Tout comme la redondance offerte par les offres cloud, la joignabilité de ceux-ci doit donc être renforcée par une redondance à tous niveaux. En effet, une infrastructure cloud ultra-disponible ne sert à rien si l'accès ne l'est pas :

• Pour des connexions via internet :
  - Il faut s'assurer que le fournisseur de l'offre cloud dispose d'une présence internet redondée sur plusieurs sites
  - Et que ces accès internet sont fournis par plusieurs opérateurs ou points de peering
• Pour des connexions dédiées :
  - Il faut privilégier une connexion multi-opérateur qui permet de basculer d'un opérateur à l'autre en cas de défaillance
  - Idéalement, chaque lien devrait être supporté par une technologie différente xDSL, fibre, BLR …
  - La collecte des flux doit se faire sur au moins deux data center : en cas de défaillance du premier, l'accès aux machines est toujours assuré par le data center secondaire.

Les briques de sécurité (firewall de constructeurs différents par exemple …) doivent être également redondées. Il en va de même pour les briques de publication de services (répartition de charge, …) .

Les administrateurs du Cloud Computing doivent être certains de se connecter sur les bons serveurs pour exécuter leurs taches d'administration, sans quoi des informations sur la sécurité de l'infrastructure pourraient être récupérées et utilisées à mauvais escient. Pour se prémunir de ces risques, il convient de :
• Mettre en place d'un protocole de sécurisation du transport des données avec un chiffrage de celles-ci (ex : TLS)
• Instaurer un procédé d'identification du serveur (ex : certificat électronique)
• Filtrer les accès, par un équipement de sécurité type pare-feu à inspection de paquets.

• Rédiger une charte d'utilisation du système informatique (ex : prise de conscience de l'outil informatique comme un point d'entrée dans l'entreprise)
• Appliquer une politique de contrôle stricte des utilisateurs (ex : contrôle de l'installation de logiciel tiers sur la plate-forme, surveillance des accès, journalisation des actions ...).
• La performance des VM peut être altérée si les équipements saturent à cause d'un utilisateur, impactant aussi sur les autres utilisateurs. Pour éviter cela, il faut adapter le dimensionnent nominal des environnements sur le Cloud. Si l'application peut dès le début supporter une croissance horizontale, c'est-à-dire une multiplication des machines qui traitent le flux (comme de la répartition de charge par exemple) alors il est préférable d'avoir dès le début deux petites machines plutôt qu'une grosse. Ces instances ne seront probablement jamais sur un même socle physique. Ainsi, si un pic de charge local dans le cloud vient affecter une instance, la seconde sera la plupart du temps épargnée. Par ailleurs cette topologie permettra - en cas de forte charge - de multiplier les instances en fonction du besoin. Les prestataires proposent ici des solutions de publication des applications clefs en main.

Adaptabilité aux pics de charge

Une forte charge non prévue sur un des services hébergés sur l'infrastructure Cloud Computing risque d'entrainer une dégradation des performances de ce service. Pour éviter cela, on met en œuvre un mécanisme de flexibilité des ressources permettant d'adapter la plate-forme aux besoins en un minimum de temps et d'efforts.

Impact de la gestion des mises à jour de sécurité sur la certification

La gestion des mises à jour de sécurité est nécessaire pour certains types de certification. Ne pas les installer équivaudrait plutôt à perdre une telle certification.
Par exemple, les solutions d'IaaS privées incluent obligatoirement une gestion automatisée des mises à jour. De même, un des avantages des offres de SaaS publics est justement de déléguer au fournisseur la gestion des mises à jour, et celui-ci doit s'engager sur cette gestion et les délais d'application des mises à jour.
Toute modification du socle technique sur lequel repose la solution Cloud doit être communiquée aux clients, pas forcément en temps réel mais avec une périodicité bien établie.
En cas de modification majeure d'un élément logiciel (remplacement d'une brique par une autre), l'homologation doit être repassée. En revanche, en cas de montée de version ou d'installation de patch, sur une solution logicielle donnée, cette opération ne nous semble pas obligatoire.
Rappelons quand même qu'une homologation est généralement accordée pour une durée bien précise. Le client vérifiera que son fournisseur reste bien à jour de ses homologations.

SECURITE DES DONNEES

RESPONSABILITÉ JURIDIQUE DE LA SÉCURITÉ ET DE LA CONFIDENTIALITÉ DES DONNÉES DANS LE CLOUD

Le Client est juridiquement responsable de ses données et de leur utilisation, notamment de tout ce qui concerne leur conformité aux obligations juridiques.
Le Prestataire est soumis à des obligations techniques et organisationnelles. Il s'engage à préserver l'intégrité et la confidentialité des données, notamment en empêchant tout accès ou utilisation fraudeuse et en prévenant toutes pertes, altérations et destructions. Sa responsabilité juridique peut être engagée dans le cas où il aurait transféré les données de son client en dehors de l'UE sans l'en prévenir et sans s'assurer que les déclarations nécessaires ont été faites.

De façon générale, plus l'infrastructure est confiée au fournisseur Cloud, plus sa responsabilité est importante. Dans les cas de PaaS et de SaaS, le client ne contrôle que le contenu de ses données (et encore partiellement en SaaS où la responsabilité est partagée avec le fournisseur). En fonction du service fourni au client, le fournisseur peut être en charge (et donc responsable) de la sauvegarde, d'un niveau bien défini de disponibilité du service, et de la confidentialité des données. Même dans ce cas, le client final n'est pas affranchi de toutes responsabilités : il doit par exemple sécuriser les mots de passe ou les certificats qui lui servent à accéder à son environnement Cloud, ne pas laisser d'accès ouvert au service via son propre réseau. Les conséquences d'une négligence avérée du client final ne sauraient être imputées au fournisseur.

Le contrat de service doit aborder le domaine des responsabilités de chaque partie. Si le client doit exiger de la part de son prestataire des engagements de confidentialité et les moyens de contrôle afin de surveiller que le prestataire respecte ses engagements, il est évident que ce dernier ne peut assumer pleinement la confidentialité des données confiées dans le système de stockage du Cloud. Il est nécessaire que les parties, chacune de leur côté, puissent maitriser leur propre sécurité, et d'autre part, contrôler le domaine tiers. Faute de contrats formalisant ces points de partage des responsabilités, et des outils de contrôle et d'enregistrement, des procédures en cas de litiges peuvent être longues et laborieuses... surtout dans un domaine où la jurisprudence est rare.

PROTECTION ET RÉCUPÉRATION DES DONNÉES

Il existe deux métriques qui permettent de mesurer l'efficacité d'un processus de protection des données. Le premier est le « Recovery Time Objective » ou RTO qui mesure le temps acceptable ou toléré de rétablissement du service lors d'une panne. Le second étant le « Recovery Point Objective » ou RPO qui mesure la quantité de données que l'on s'accorde ou tolère à perdre due à une panne ou au processus de restauration.
Une phase d'analyse est nécessaire pour identifier les applications et données critiques pour l'entreprise afin de mettre en place une politique de protection adaptée. Ainsi plus les données sont critiques pour l'entreprise plus la fréquence des copies doit être élevée avec un besoin d'accès et de performances plus important.
Par nature le « Cloud » repose sur une infrastructure, un socle mutualisé et il faut tenir compte de cette particularité en termes d'évolutivité, de flexibilité, de migration, de mobilité et de colocation sécurisée.
Mettre ses données dans un « Cloud » est une chose mais quelle garantie a-t-on sur l'intégrité et sur la disponibilité des données ? Faut-il continuer à sauvegarder et restaurer ses données ? Quel plan de secours mettre en œuvre en cas de sinistre ?
En réalité, il s'agit d'un déplacement des responsabilités vers l'hébergeur, fournisseur (ou « Cloud Provider »). Les SLAs (Service Level Agreements) définissant, pour chaque groupe consommant le « Cloud », les niveaux de services attendus.

Infrastructure « Always On »

Dans un environnement Cloud storage il ne peut y avoir d'arrêt (même planifié) pour des opérations de maintenance, de mises à jour ou pour garantir la performance définie par les SLAs. Que se passe-t-il lorsqu'on doit déplacer les applications et données complètes d'un locataire vers un nouveau système de stockage pour des raisons de répartition de charge ou pour optimiser les performances ?
La réponse est la mise en oeuvre d'un data center virtuel rompant avec le data center physique traditionnel. Ce data center virtuel permet un alignement approprié avec le bon tiers de stockage, la maintenance planifiée ou la migration vers une nouvelle plate-forme, le tout sans arrêt de service.

Sauvegardes et Snapshots

La protection des données passe par la mise en oeuvre de sauvegardes soit sur disques pour une restauration rapide et un RTO plus court soit sur bandes plus orientées long terme avec une externalisation. La copie sur disques de

snapshot permet des sauvegardes plus fréquentes que traditionnellement et répond aux besoins d'un RPO (Recovery Point Objective) strict.

Miroirs distants

En cas de sinistre, il est important de mettre en place une solution de miroir qui permet de protéger les données critiques. La réplication peut être synchrone ou asynchrone, en effectuant le cas échéant de la compression pour réduire le RPO. Des mécanismes doivent être en place pour garantir la cohérence des données répliquées (cohérence temporelle et sans transaction en cours).

Administration

Une administration à base de politique ou de règles est cruciale pour un « Provider ». L'automatisation des tâches est également un point important de la sécurité évitant les erreurs de configurations ou de manipulations. En environnement « Cloud storage » il est nécessaire de pouvoir gérer les relations entre les différents systèmes en miroirs et aussi de surveiller la bonne application des règles de protection mises en oeuvre à partir d'une interface unique.

INTÉGRITÉ DES DONNÉES (RBAC)

Pour un « Cloud » plus sûr il est important aussi de réfléchir au contrôle d'accès de ce même « Cloud » en implémentant la fonctionnalité de « Role Based Access Control » ou RBAC. C'est une méthode qui permet de définir un certain nombre d'actions que peut réaliser un utilisateur ou un administrateur au sein du « Cloud ». En fait il s'agit de la définition de plusieurs rôles qui auront chacun des permissions et des privilèges différents puis en associant des collaborateurs, des clients, des partenaires… à ces mêmes groupes selon leurs fonctions. C'est donc une fonctionnalité qui idéalement est présente sur l'ensemble de la chaîne « Cloud », des serveurs virtualisés, des équipements réseaux jusqu'aux entités virtualisées du stockage.

CHIFFREMENT LIÉ À LA DONNÉE

Les défis de la cryptographie dans le Cloud sont complexes, notamment lorsqu'il s'agit de protéger les données hébergées contre des accès non-autorisés de la part de l'hébergeur.

Des travaux sont en cours chez les grands offreurs de l'IT, pour la mise en œuvre d'un chiffrement adapté à ces situations et qui fournisse un équilibre satisfaisant entre sécurité, efficacité et fonctionnalité.

Un chiffrement requêtable permet de manipuler et d'effectuer des recherches sur des données chiffrées sans déchiffrer les données, ainsi que d'en vérifier l'intégrité.

DONNÉES DU CLOUD ACCESSIBLES AUX AUTORITÉS D'UN AUTRE PAYS

Tout pays a le droit légitime d'avoir accès, dans les conditions juridiques qui lui sont propres, aux données qui sont stockées sur son territoire, ou qui transitent par celui-ci. Ainsi, en France, dans le cadre d'une perquisition et conformément à l'article 97 du code de procédure pénale, l'hébergeur doit être en mesure d'extraire de son Cloud les éléments recherchés ou l'ensemble des informations concernant un client particulier, sans pour autant avoir à livrer l'ensemble des données des clients hébergés dans le Cloud.

La bonne pratique consiste à s'assurer contractuellement du (ou des) pays où seront physiquement installés les éléments d'infrastructures et de connaître, avant de s'engager dans un contrat de service Cloud avec un fournisseur, les juridictions compétentes.

RÉVERSIBILITÉ : CHANGER DE *CLOUD PROVIDER*

Il serait hasardeux de s'engager dans une solution Cloud sans savoir, a priori, comment on peut la quitter et comment on peut avoir l'assurance que les données, après récupération, seront bien effacées chez le premier prestataire.

Pour faciliter la migration entre Cloud, il existe plusieurs APIs Cloud émergentes sur le marché, proposées par des consortiums ou des sociétés privées. On privilégiera les APIs des organismes de standardisation dès lors que ces APIs auront commencées à être utilisées par un nombre significatif de fournisseurs Cloud. Ainsi CDMI ou SNIA's Cloud Data Management Interface dont l'objectif est de permettre la portabilité, la conformité, la sécurité des données et l'interopérabilité entre différents fournisseurs de Cloud.

De plus, il existe un standard OVMF (*Open Virtual Machine Format*) qui permet une exportation et une importation simplifiée entre les différentes plates-formes de Cloud Computing.

Le respect de standards assure la compatibilité entre les différentes architectures et permet de changer de Cloud provider beaucoup plus librement.

Quant aux données, le processus de réversibilité assure à un client du Cloud Computing qu'elles seront complètement écrasées (ainsi que les sauvegardes) après une période définie contractuellement.

POUR EN SAVOIR PLUS

SOURCES ET DOCUMENTS UTILES :

- Article : Searching an Encrypted Cloud http://www.technologyreview.com/computing/23929/?a=f
- Classification Tier de l'Uptime Institute : http://www.uptimeinstitute.org/
- http://securite-ti.com/?p=90
- http://www.integra.fr/securite/
- Hyper-V Security Guide
  http://www.microsoft.com/downloads/details.aspx?FamilyID=2220624b-a562-4e79-aa69-a7b3dffdd090&displaylang=en
- http://www.imaginevirtuallyanything.com/?cc=fr&REF_SOURCE=netappmicrosite
- http://www.netapp.com/fr/technology/secure-multi-tenancy-fr.html
- Cloud Cryptography : http://research.microsoft.com/en-us/projects/cryptocloud/
- Vidéo : Enhancing Cloud SLA with Security: A secure, Searchable, and Practical Cloud Storage System : http://research.microsoft.com/apps/video/default.aspx?id=103364

RÉDACTION DU LIVRE BLANC

Rédaction et rewriting : **Philippe Grange** - Faits et Chiffres
Chef de projet : **Céline Ferreira** - Integra
Chef de projet : **David Vandenborght** - Syntec numérique
Chef de production : **Claire Bès de Berc** - Syntec numérique

Ont contribué à l'élaboration, à la rédaction et à la relecture du Livre Blanc :

Rachid Boularas - NetApp France
Cédric Buot de l'Epine - Integra
Olivier Caleff - Devoteam
Thierry Del-Monte - Integra
Yassine Essalih - Aastra
Nolwenn Le Ster - Spie Communications
Magali Montagnon - VeePee
Pascal Saulière - Microsoft France
Cyril Van Agt - NetApp France

Ont également contribué au Livre Blanc :

Jean-Marc Boursat - Devoteam
Jérôme Brun - Atos Origin
Nicolas Koleilat - Sopra Group
Nicolas Pondemer – NextiraOne
Yannick Ragonneau – Devoteam
Serge Robert - Open

REMERCIEMENTS

Nous tenons à remercier Philippe Hedde, président, ainsi que tous les membres du Comité Infrastructures de Syntec numérique

SYNTEC NUMERIQUE
3, rue Léon Bonnat - 75016 Paris
Tel : 01 44 30 49 70 - Fax : 01 42 88 26 84
www.syntec-numerique.fr