

# Cloud Computing – Eclaircies ou couvert ?

---

Des solutions pour répondre aux impératifs de continuité des activités

Ontrack®

- 2 Introduction
- 2 Le cloud computing : conçu pour combattre vents et marées
- 3 Le cloud computing pris dans la tempête
- 4 Conseils de protection pour le cloud computing
- 5 Beau fixe sur le cloud computing

## Introduction

Si vous demandez à un utilisateur d'ordinateur lambda de vous décrire le cloud computing, il y a fort à parier qu'il vous retournera un regard interrogatif. Le marketing a réussi à informer les internautes de l'existence du cloud computing, mais peu d'utilisateurs sont capables d'expliquer ce que ce concept représente ou ce qu'il implique pour eux. Pratiquement tous les internautes ont un lien avec les technologies de cloud computing sans même le savoir. Vous avez déjà utilisé un site d'hébergement de photos ? Alors vous avez déjà utilisé le stockage basé sur le cloud computing. Vous utilisez un site de réseau social interactif ou des applications bureautiques depuis votre navigateur ? Alors vous utilisez des logiciels basés sur le cloud computing.

L'industrie du cloud computing entre dans ses années d'apprentissage et peut désormais proposer des solutions aux entreprises qui cherchent à limiter leurs coûts et investissements dans les nouvelles technologies. La technologie de virtualisation, c'est-à-dire un logiciel qui émule le matériel informatique, constitue le fondement de toutes les offres de services du cloud computing.

Le cloud computing offre trois services : les **logiciels en tant que service (SaaS)**, **plate-forme en tant que service (PaaS)**, et **l'infrastructure en tant que service (IaaS)**. L'IaaS est la plus établie des offres de services basées sur le cloud computing, car elle permet aux entreprises d'utiliser uniquement ce dont elles ont besoin pour leurs systèmes informatiques ; par exemple, l'IaaS permet aux clients d'avoir accès à des ordinateurs virtualisés hors site sans devoir payer les coûts matériels associés ou les dépenses liées aux installations.

Les SaaS sont les plus accessibles des offres de services basées sur le cloud computing, car ils offrent des fonctionnalités d'application complètes via une interface internet. Le nombre d'applications qui ont été développées pour les navigateurs internet est impressionnant. Par exemple, il existe des applications de productivité bureautique complètes qui sont disponibles simplement via un navigateur internet et une connexion à internet.

La PaaS est destinée au développement rapide d'applications et exploite les deux services de cloud computing précédemment mentionnés. Considérez la PaaS comme l'intermédiaire entre les SaaS et l'IaaS ; ce service de cloud computing pourrait être plus proche de l'adoption que ce qu'on pensait<sup>1</sup>, car il favorisera d'autres fonctionnalités de SaaS.

Gartner Research signale que l'adoption de l'infrastructure en tant que service (IaaS) commence à susciter de l'intérêt sur la place de marché. Gartner prévoit ainsi que le marché mondial du cloud computing représentera 10,5 milliards de dollars en 2014, contre 3,7 milliards aujourd'hui, soit une hausse impressionnante de l'adoption sur le marché au cours des trois prochaines années<sup>2</sup>.

L'acceptation des services de cloud computing par les consommateurs par le biais des applications pour téléphone mobile démontre que la technologie offre un modèle économique dans lequel de plus en plus d'entreprises investissent. D'après comScore, Inc., société spécialisée dans le traitement analytique des médias numériques aux États-Unis, 69,5 millions d'individus possèdent un smartphone aux États-Unis et, à la fin 2010, près de la moitié de ces utilisateurs accédaient à leurs comptes bancaires, de crédit ou de courtage au moyen de leur appareil mobile<sup>3</sup>.

## Le cloud computing : conçu pour combattre vents et marées

Jason Baker, directeur de la technologie à Visi, Inc., prestataire de services d'IaaS et d'hébergement de centres de traitements, indique que la technologie de cloud computing est "conçue pour résister aux défaillances" grâce à sa conception intrinsèque de distribution et de redondance. Il rappelle que "le déploiement d'applications traditionnel [...] se passait sur le serveur internet, le serveur d'applications et le serveur de bases de données. Le cloud computing supprime tout cela et permet aux entreprises de se

Les SLA et les obligations contractuelles n'offrent pas forcément une protection complète aux utilisateurs du cloud computing en cas de perturbation des activités.

<sup>1</sup> <http://www.businesswire.com/news/home/20110314006630/en/Gartner-2011-Year-Platform-Service>

<sup>2</sup> <http://www.businesswire.com/news/home/20110407005575/en/Gartner-Maps-Rapidly-Evolving-Market-Cloud-Infrastructure>

<sup>3</sup> [http://www.comscore.com/Press\\_Events/Press\\_Releases/2011/4/comScore\\_Reports\\_February\\_2011\\_U.S.\\_Mobile\\_Subscriber\\_Market\\_Share](http://www.comscore.com/Press_Events/Press_Releases/2011/4/comScore_Reports_February_2011_U.S._Mobile_Subscriber_Market_Share)

<http://www.creativedepartment.com/news/mobile/use-mobile-banking-apps-rose-sharply-fourth-quarter-183600>

concentrer soit sur les couches d'applications, soit sur les couches orientées web". La couche physique (le matériel) est fournie par la technologie de virtualisation.

À mesure que la demande pour le cloud computing augmentera, les applications et services de cloud computing se banaliseront. Pourtant, ce qui importera le plus aux clients du cloud computing sera la pérennité du prestataire et sa réputation. "La confiance est essentiellement ce qui portera les prestataires de services de cloud computing dans les années à venir", estime Harold Moss, directeur de la technologie en charge de la stratégie de sécurité du cloud computing d'IBM. "Le domaine des services se développera, avant de rétrécir. Seuls les prestataires proposant des solutions complètes aujourd'hui seront encore présents à l'avenir." Harold Moss explique que les prestataires de services pourraient diluer leurs solutions en externalisant leurs propres services à un autre prestataire de services afin de rester compétitifs au niveau des prix. On en arrive à un "contrat de niveau de service composé", indique-t-il, et c'est tout le service du prestataire qui est dévalorisé parce que lui aussi a utilisé le cloud computing pour fournir les ressources informatiques. Chacun de ces SLA devient dépendant d'un autre prestataire.

## Le cloud computing pris dans la tempête

Les fournisseurs de cloud computing sont censés adhérer aux politiques de gouvernance de la responsabilité, la sécurité et la conformité. Malheureusement, les certificats et les évaluations d'audit ne révèlent pas comment un prestataire de services de cloud computing réagira en cas de perturbation des activités<sup>4</sup>.

Or, des turbulences dans le cloud computing peuvent être désastreuses pour les utilisateurs finaux, comme en témoigne la mésaventure survenue à un prestataire de services informatiques au Canada. Celui-ci avait une appliance de stockage NetApp® de 40 To qui contenait des unités logiques virtuelles, ou fichiers iSCSI au niveau du volume NetApp. À l'intérieur de ces fichiers iSCSI figuraient des volumes VMware® ESX. Ces volumes ESX contenaient les fichiers de disque virtuel pour les serveurs du prestataire de services informatiques et des machines virtuelles IaaS de certains de ses clients. La tempête essuyée par cette entreprise n'était pas externe mais interne.

Un employé mécontent a lancé la commande "Supprimer les volumes" au niveau de l'unité de stockage. Cette unité de stockage en question employait la technologie d'instantané des blocs de NetApp, laquelle aurait été suffisante pour sauvegarder les données si l'employé malveillant s'était arrêté là. Malheureusement, cet employé savait comment la fonction d'instantané du classeur fonctionnait. L'horloge système du classeur a été retardée d'une heure juste avant de supprimer les volumes NetApp, si bien que la réplication d'instantané a copié les métadonnées de volumes vides. Une fois le mal accompli, l'employé a remis l'horloge système du classeur à la bonne heure avant de quitter le centre de traitements de l'entreprise. Le classeur NetApp a continué à prendre des instantanés des volumes, comme prévu, remplissant toute la liste d'instantanés de blocs vides. Lorsque les autres administrateurs ont découvert l'ampleur des dégâts, il n'y avait aucun point de récupération valable auquel revenir.

Ce sinistre a vite pris l'allure d'une catastrophe, non seulement parce que certains des systèmes IaaS de leurs clients avaient disparu, mais aussi parce que le prestataire de services n'avait même plus ses propres données opérationnelles. Pire encore, il n'existait aucune sauvegarde pertinente des données d'origine.

Ce prestataire de services avait promis un temps de disponibilité de 99,99 % pour son centre de traitements et une connectivité à internet de niveau 1. Durant toute l'interruption des activités, le temps de disponibilité et la rapidité de connexion ont été maintenus, conformément aux SLA stipulés. Comme les clients de ce service de cloud computing l'ont vite découvert, la connectivité et le temps de disponibilité des systèmes n'ont rien à voir avec la disponibilité des données.

Le prestataire de services informatiques canadien a été obligé d'engager un prestataire de services de récupération de données pour récupérer ses propres données, ainsi que les systèmes virtuels IaaS de ses clients. Durant cette perturbation des activités, l'entreprise s'est efforcée de prendre soin de

À mesure que la demande pour le cloud computing augmentera, les applications et services de cloud computing se banaliseront. Pourtant, ce qui importera le plus aux clients du cloud computing sera la pérennité du prestataire et sa réputation.

<sup>4</sup> Pour les besoins de cet article, une perturbation des activités est tout ce qui empêche le travail quotidien d'être accompli, notamment une coupure d'électricité, un dérangement des lignes téléphoniques, etc. La perte de données se produit lorsque des données sont altérées ou inaccessibles. La perte de données est donc un sous-ensemble de la perturbation des activités.

ses clients. Toutefois, certains clients ont été informés que s'ils n'avaient pas acheté une réplication supplémentaire ou ne possédaient pas de sauvegarde de leurs données, ils devraient payer leur propre récupération via le même prestataire de services de récupération de données. Cette révélation a choqué les clients qui pensaient que leur SLA couvrait la disponibilité des données.

Cet exemple montre que les SLA et les obligations contractuelles n'offrent pas forcément une protection complète aux utilisateurs du cloud computing en cas de perturbation des activités. Tout aussi risqué : ne pas avoir de clause relative à la récupération des données dans un contrat passé avec un fournisseur de cloud computing. Croire à tort que le matériel de stockage se rétablira par lui-même ou sera redondant à 100 % est naïf et peut coûter cher. La réplication de données synchrone est onéreuse et n'empêche pas les conséquences d'une erreur humaine ou d'une destruction malveillante des données.

## Conseils de protection pour le cloud computing

Des tempêtes ont éclaté début 2011, causant des interruptions de service pour quelques-uns des plus grands noms dans les services de cloud computing<sup>5</sup>. Ces événements chaotiques n'avaient pas de lien entre eux ; toutefois, ces perturbations ont rendu des sites internet inaccessibles, affectant les internautes. Les abonnés à ces services se sont heurtés au même message : "Ce service est momentanément indisponible". Comme les services de cloud computing sont relativement nouveaux, un client peut ignorer les limitations d'un SLA tant qu'une perturbation des activités n'a pas eu lieu. Par exemple, quelle compensation ou quel remboursement le SLA prévoit-il en cas d'interruption de service, ou comment la procédure de récupération du prestataire de services rétablira-t-elle les services manquants ? Les clients du cloud computing peuvent réaliser trop tard qu'ils ont besoin d'une plus grande résilience dans leurs contrats de cloud computing<sup>6</sup>.

Les fournisseurs de cloud computing qui n'ont pas de spécialistes en récupération internes ou tiers disponibles pour les aider à surmonter la perturbation des activités n'offrent pas le niveau de confiance attendu par leurs clients. Pendant une interruption de service, tout le personnel informatique est à pied d'œuvre, travaillant d'arrache-pied à rétablir les services, remplacer le matériel, restaurer les sauvegardes et accomplir les analyses des causes premières et autres tâches d'investigation motivées par le besoin de la direction de comprendre ce qui a déclenché l'événement. Les fournisseurs de cloud computing qui tentent de tout conserver en interne s'aperçoivent rapidement qu'un personnel informatique déjà surchargé approche du point de rupture lors d'une interruption de service.

Une interruption de service dans le cloud computing peut venir d'une panne du réseau, d'un remplacement du matériel, d'une attaque réseau venue de l'extérieur ou d'un bug logiciel, pour citer des causes courantes. De plus, malgré les progrès dans la technologie de stockage des données, le cloud computing est sujet à des pertes de données, lesquelles peuvent contribuer à une interruption de service. Les prestataires de services de récupération de données récupèrent les données des systèmes de stockage qui ont subi une panne, ont été mal gérés à cause d'une erreur humaine, ou ont été victimes d'un sabotage en bonne et due forme. Les services de récupération sont utilisés par les consommateurs du stockage uniquement après qu'ils aient perdu l'accès à leurs données. Personne ne croit vraiment qu'une défaillance du stockage ou une perte de données lui arrivera. Pourtant, quand c'est le cas, un fournisseur de cloud computing (ou client) qui n'a pas entièrement sauvegardé ses données immédiatement avant le sinistre peut collaborer avec un prestataire de services de récupération de données pour récupérer ses données d'origine.

La technologie de virtualisation du stockage dans le cloud computing ajoute une couche complexe supplémentaire au processus de récupération de données. En raison de la double organisation de système de fichiers du serveur hôte et du système d'ordinateur virtuel, la fragmentation des données est multipliée par deux. Comme évoqué précédemment, la technologie de virtualisation favorise les

La connectivité et le temps de disponibilité des systèmes n'ont rien à voir avec la disponibilité des données.

<sup>5</sup> [http://www.computerworld.com/s/article/9216064/Amazon\\_gets\\_black\\_eye\\_from\\_cloud\\_outage](http://www.computerworld.com/s/article/9216064/Amazon_gets_black_eye_from_cloud_outage), <http://www.pcmag.com/article2/0,2817,2384214,00.asp>, [http://www.computerworld.com/s/article/9211798/Update\\_Google\\_Gmail\\_outage\\_leaves\\_thousands\\_of\\_users\\_without\\_e\\_mail](http://www.computerworld.com/s/article/9211798/Update_Google_Gmail_outage_leaves_thousands_of_users_without_e_mail), [http://news.cnet.com/8301-31001\\_3-20046091-261.html](http://news.cnet.com/8301-31001_3-20046091-261.html)

<sup>6</sup> Pour les besoins de cet article, une perturbation des activités est tout ce qui empêche le travail quotidien d'être accompli (coupure d'électricité, dérangement des lignes téléphoniques...) La perte de données se produit lorsque des données sont altérées ou inaccessibles. La perte de données est donc un sous-ensemble de la perturbation des activités.

services de cloud computing et offre une incroyable flexibilité pour la croissance à grande échelle. La couche de stockage peut devenir un maillon faible du fait que la virtualisation repose fortement dessus. La meilleure protection lors de l'adoption de la technologie de cloud computing est d'exiger de votre prestataire de services de cloud computing qu'il collabore avec un spécialiste de la récupération de données renommé et offrant une gamme de services complète. Vous minimiserez ainsi le temps d'arrêt causé par des défaillances du stockage des données.

Il ne s'agit pas seulement de prévoir un stockage hors site, la réplication synchrone/asynchrone ou des sauvegardes sur bandes dans le SLA (que tous les fournisseurs de cloud computing devraient offrir, au minimum). Un fournisseur de cloud computing qui collabore avec un prestataire de services de récupération de données réputé montre que la disponibilité des données est plus importante que l'accessibilité ou le temps de disponibilité des systèmes. Un tel fournisseur gagne la confiance d'un client envers son offre de services en ayant un plan de continuité des activités complet pour protéger les données de l'abonné.

La récupération des données n'est qu'un aspect de la discussion à avoir au sujet du cloud computing. La destruction des données est tout aussi importante. Comprendre ce qu'il advient de vos données lorsque le contrat de cloud computing arrive à

échec fait partie intégrante de la sélection des fournisseurs de cloud computing. Les grands centres de traitements auront des contrats de services d'OEM pour assurer la maintenance du matériel de stockage et faire détruire ou démagnétiser les disques défaillants avant qu'ils ne quittent l'environnement sécurisé. Il est facile de supposer que les données supprimées seront rapidement écrasées par les opérations d'écriture incessantes du stockage ultérieur. Toutefois, la destruction complète des données nécessite que les fichiers du client passent par un processus d'effacement. Les fichiers sensibles sont alors écrasés par des données pseudo-aléatoires, avant d'être supprimés du volume.

## Beau fixe sur le cloud computing

Pour avoir une vue dégagée sur vos stratégies de cloud computing, il faut pouvoir identifier tous les obstacles. Certains de ces obstacles viendront du prestataire de services et d'autres du budget et de la stratégie du projet. Il est essentiel de savoir où se terminent les obligations du prestataire de services et où commencent les vôtres quant à la protection des données afin d'assurer la disponibilité de vos applications et infrastructures pour vos clients.

Kroll Ontrack recommande les considérations suivantes pour garantir à votre entreprise un ciel radieux.

Le déluge technique : les points à prendre en compte	Pourquoi c'est important
<ul style="list-style-type: none"> <li>• Les protocoles et systèmes de sauvegarde sont-ils alignés sur vos propres standards de sauvegarde internes ?</li> <li>• Votre fournisseur de cloud computing a-t-il une réputation de fiabilité technique apte à satisfaire vos besoins ?</li> </ul>	<p>Par exemple, le matériel suspect, les fichiers fragmentés et les niveaux de RAID inappropriés peuvent compromettre la disponibilité des données.</p>
<ul style="list-style-type: none"> <li>• Vos données sont-elles stockées sur des systèmes de stockage fiables ?</li> <li>• Les différents types de données et d'applications sont-ils gérés de manière appropriée ?</li> <li>• Votre fournisseur de cloud computing a-t-il un spécialiste de la récupération de données identifié dans son plan de reprise après sinistre/continuité des activités ?</li> <li>• En cas de perte de données, il est impératif de respecter une procédure de réponse rapide.</li> <li>• Comment le fournisseur prouve-t-il qu'il respecte les lois sur la conservation des données ?</li> <li>• Quels sont les contrats de niveau de service eu égard à la récupération de données, la responsabilité en cas de perte, l'application de résolutions et les résultats opérationnels ?</li> </ul>	<p>Le temps de découvrir comment le fournisseur de cloud computing traite ces questions, il peut être trop tard pour réagir en cas de temps d'arrêt.</p> <p>Ne supposez pas qu'un SLA supplémentaire peut compenser une perte de données. Si le fournisseur de cloud computing n'a pas de partenaire en récupération de données, trouvez-en un pour qui c'est le cas.</p>

Le courant dominant de la sécurité : les points à prendre en compte	Pourquoi c'est important
<ul style="list-style-type: none"> <li>• Vos données sont-elles bien protégées ? Quelles mesures le fournisseur prend-il pour réduire le risque d'une brèche de sécurité des données ? Par exemple, les données sont-elles cryptées ?</li> <li>• Savez-vous qui au sein de votre entreprise et chez le fournisseur de cloud computing peut accéder à vos données ?</li> <li>• Quelles sont leurs habilitations ?</li> </ul>	<p>Votre entreprise emploie les pratiques de l'industrie quant à la sécurité des données, y compris les employés. En comprenant comment votre partenaire en cloud computing gère son personnel et ses données, vous pourrez choisir un service parfaitement adapté à vos politiques existantes.</p>
<ul style="list-style-type: none"> <li>• En matière de propriété des données, vos données vous appartiennent-elles toujours une fois qu'elles sont dans le cloud computing ?</li> <li>• Vous appartiennent-elles une fois qu'elles quittent votre possession ?</li> <li>• Les données en fin de vie sont-elles effacées et démagnétisées ? Qui certifie que ces données ont bien été supprimées ? Ont-elles été effacées conformément aux normes de suppression spécifiques de votre pays ?</li> </ul>	<p>Le récent débat sur la sécurité d'un site de réseau social populaire suggère que la question mérite d'être examinée de plus près.</p>

Le brouillard juridique : les points à prendre en compte	Pourquoi c'est important
<ul style="list-style-type: none"> <li>• Le fournisseur de cloud computing conserve-t-il les données dans le respect de la politique de conservation des documents de votre entreprise ?</li> <li>• Le fournisseur de cloud computing offrira-t-il la garantie qu'il respecte les réglementations relatives à la protection des données ?</li> <li>• En cas de litige ou d'investigation, votre spécialiste externe en e-discovery ou vous-même pourrez-vous accéder et extraire ou préserver toutes les informations stockées sous forme électronique ?</li> </ul>	<p>En cas de cybercrime ou de brèche de sécurité au niveau des données, les spécialistes en recherche de preuves récupéreront tous les systèmes de stockage, et cela peut inclure vos données.</p> <p>Si les données sont partagées entre des services de cloud computing, cela peut compliquer l'enquête et laisser vos clients et vous-même sans aucun accès aux applications ou systèmes de stockage.</p>
<ul style="list-style-type: none"> <li>• Où vos données sont-elles stockées exactement ?</li> <li>• Sont-elles virtualisées avec les données d'autres entreprises ?</li> <li>• À quel endroit se trouve le centre de traitements ?</li> <li>• Les données seront-elles stockées dans des juridictions où elles peuvent faire l'objet d'une ordonnance de production par des tiers ?</li> <li>• Si vous mettez un terme à une relation avec un fournisseur de cloud computing, pouvez-vous récupérer vos données ? Sous quel format se présenteront-elles ?</li> <li>• Comment pouvez-vous être sûr que toutes les copies de vos données sont détruites une fois le contrat terminé ?</li> </ul>	<p>La mutualisation peut poser des problèmes pour la récupération de données et la production de données dans les litiges ou enquêtes. De plus, les considérations géographiques sont également importantes, car les retards dans l'extraction des données à des fins de récupération ou de collecte peuvent s'avérer extrêmement coûteux.</p> <p>C'est vous-même, et non le fournisseur de cloud computing, qui êtes responsable de la protection et la conservation des données de vos clients. Le fait de comprendre et surmonter les obstacles empêchera les désastres juridiques.</p>

# Ontrack®

France : 0 800 10 12 13  
[www.ontrack.fr](http://www.ontrack.fr)

Belgique : +32 (0)2 512 30 22  
[www.ontrackdatarecovery.be](http://www.ontrackdatarecovery.be)

Copyright © 2012 Kroll Ontrack Inc. Tous droits réservés. Kroll Ontrack, Ontrack et les autres noms de produits et de marques Kroll Ontrack cités dans ce document sont des marques de commerce ou des marques déposées de Kroll Ontrack Inc. et/ou de sa société mère, Kroll Inc., aux États-Unis et/ou dans d'autres pays. Tous les autres noms de produits ou de marques sont des marques de commerce ou des marques déposées de leurs détenteurs respectifs.