

Réseau, fonctionnera ou ne fonctionnera pas ?

De nouvelles approches pour réussir la connexion de votre entreprise dans le cloud.

Si la sécurité technique peut s'obtenir moyennant les efforts adéquats, les législations et réglementations nationales constituent souvent un problème. Le "Private Cloud" est une alternative permettant aux services du cloud de répondre à certaines exigences en matière de sécurité. Ici, le défi réside plus dans l'infrastructure existante de l'entreprise qui, souvent, ne répond pas aux nouvelles exigences. Une solution envisageable, qui fournit un niveau supplémentaire d'intelligence est le SMART MPLS.

1. Cloud computing et la sécurité

Depuis quelque temps, l'informatique dans le cloud est un sujet dont on parle beaucoup. Ce nouveau paradigme apparaît régulièrement comme la panacée pour tous les problèmes IT, la complexité croissante des systèmes, la consommation énergétique des centres informatiques, l'espace occupé par les serveurs, mais aussi le besoin perpétuel de diminuer les coûts au sein du département informatique, bien qu'il ne s'agisse pas d'une technologie révolutionnaire, mais d'un modèle alternatif pour l'application de solutions IT. Quoi qu'il en soit, les avantages pour les entreprises sont manifestes: la concentration de services et la portée virtualisée, indépendante du lieu, des solutions IT sont à l'origine d'économies d'échelle et de synergies.

Puisque au jour d'aujourd'hui plus de bande passante est disponible, cette méthode peut être utilisée pour les applications standards telles que l'email, les plateformes de médias sociaux, mais aussi pour les moteurs de recherche. Ce n'est plus le rôle de l'utilisateur privé d'intégrer et de gérer son propre serveur ; Grâce au cloud, il peut utiliser les applications dans son propre environnement. Ceci pourrait ne pas satisfaire à toutes les exigences techniques, mais pour des raisons économiques, il est souvent plus intéressant quand il n'y a pas de pré-investissements à faire. En attendant, un portefeuille complet d'applications cloud est disponibles pour les entreprises, notamment Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) et Infrastructure-as-a-Service (IaaS). Les offres de fournisseurs de cloud comprennent la disponibilité d'espaces jusqu'au développement complet d'applications ERP.

Cependant les exigences des entreprises, par rapport au secteur résidentiel, sont beaucoup plus strictes. La question de la sécurité en particulier est perçue comme un point critique. Apparemment, de nombreux responsables en informatique estiment le transfert de leurs propres données vers le "cloud" trop risqué. Le fait d'être prudent quant au battage médiatique est facile à comprendre. Dans un monde digital le bien-être de chaque entreprise dépend de l'intégrité et de la confidentialité de ses données.

Lorsque l'on s'interroge sur la sécurité, il faut faire la distinction entre les aspects techniques et juridiques. En termes purement techniques, il y a clairement un risque, puisque c'est un canal externe où interagissent différents processus. Une connexion isolée est sans danger, mais complètement irréaliste. Aucune entreprise ne peut à base d'une propre connexion contrôler le trafic extérieur, ainsi que la

communication avec sa propre clientèle. Bien sûr, les connexions sont désormais protégées efficacement. Le blocage de l'accès non autorisé fait partie du quotidien de la sécurité informatique et n'est en rien une innovation dans l'environnement du « Cloud ». Le fait que les fournisseurs de cloud traitent simultanément les données de différentes entreprises ne change rien à la sécurité en tant que telle. Par ailleurs, l'extrême réduction des risques entraîne des coûts très élevés. La sécurité informatique est devenue un sujet très complexe qui demande beaucoup de savoir-faire et d'expérience. Les grandes entreprises disposent généralement des experts requis pour le bon fonctionnement de l'infrastructure informatique. Toutefois, ce sont les petites et moyennes entreprises qui ont du mal à suivre l'évolution rapide des technologies. Elles ont avantage à confier leur infrastructure aux fournisseurs spécialisés.

2. Le problème structurel du « Cloud Computing »

La protection technique n'est pas spécifiquement le problème clé. Les abus réels sont rares et peuvent être tracés. Ces problèmes sont liés non pas au cloud, mais à l'informatique proprement dite.

Le véritable problème, c'est l'incertitude juridique qui découle de l'existence de législations et réglementations nationales disparates en matière de fourniture de services internationaux. Le "cloud computing" est, dans les faits, indépendant de l'emplacement. Les fournisseurs qui le proposent réduisent leurs coûts sur la base de critères de rentabilité, et doivent avoir accès à un réseau de distribution aussi large que possible dans le cadre du "disaster recovery". De ce fait, les ressources sont soumises à des législations et réglementations nationales ou régionales hétéroclites, ce qui provoque un problème structurel pour le cloud.

Cela ne signifie pas que les données ne peuvent pas être fortement protégées hors d'Europe, mais qu'il peut exister une réglementation ou une législation régionale aux termes desquelles le fournisseur de service est tenu de permettre aux autorités locales d'accéder aux données (par exemple aux Etats-Unis) alors que ce n'est pas autorisé dans le pays où est basé le client. Ce qui pose problème à la fois pour le fournisseur et le client. Ainsi, le transfert de données personnelles vers des pays hors de l'Europe n'est permis que sous d'importantes restrictions, voire même pas du tout. La régulation financière Suisse par exemple défend certaines informations de quitter le pays. De telles mesures ne sont qu'un prétexte pour ne pas froisser les sensibilités nationales en terme de confidentialité, mais en réalité elles cachent bien d'autres intérêts plus tangibles. Prenons également l'exemple des sociétés américaines qui peuvent difficilement accepter la publication de leurs données par les autorités chinoises, alors que cela est fait en pleine conformité avec les lois et réglementations locales.

Ce problème structurel ne trouvera pas de solution tant qu'il n'y aura pas une législation et une réglementation internationales. C'est pourquoi, spécifiquement pour les applications critiques en entreprise, le cloud computing n'est pas une priorité, du moins pour autant qu'il soit interprété comme un "cloud public". D'autres questions dans le cadre du cloud computing, telles que la suppression de données après l'expiration du contrat ou la procédure en cas de faillite d'un fournisseur, peuvent toutefois être résolues. Malgré ce dilemme, les avantages techniques et économiques de ce modèle persistent. Tout dépend de ce que l'on veut atteindre grâce au cloud computing.

3. Le Cloud Privé par rapport au Cloud Public

Le « Cloud Privé » permet de combiner les avantages d'un réseau d'entreprise et du cloud computing, car le fournisseur met à disposition des ressources spécifiques. Utiliser le mot «Cloud Privé» peut être source de malentendus, puisque le terme suggère des données et applications privées. Il est plus approprié de parler de «Cloud dédié» ou «Services Enterprise Cloud". Il s'agit ici d'une séparation physique entre les ressources des différentes données des clients. Les demandes de plusieurs clients ne sont pas conservées sur le même serveur. Les clients savent toujours où leurs données sont stockées et peuvent facilement remplir leurs besoins individuels.

Puisque la sécurité dans le cadre du cloud privé est transparente pour les entreprises, c'est aux clients et aux fournisseurs de se mettre d'accord sur un niveau de sécurité, ce qui est impossible dans le cas du cloud public. Ici le fournisseur prévoit un modèle de sécurité par défaut pour tous les utilisateurs.

L'exemple suivant illustre ce problème. Afin de pouvoir utiliser des services externes, l'accès moyennant des codes est normalement protégé. Si le client dans l'intégration d'un service de cloud public n'a pas requis les contrôles techniques et organisationnelles nécessaires, ces codes peuvent être craqués par des pirates. Même si le service requiert des mots de passe complexes et une connexion sécurisée, l'ensemble de la chaîne de sécurité court des risques, ainsi que les données d'autres utilisateurs. Le risque augmente par rapport à la croissance du nombre d'utilisateurs de services de cloud public.

Le cloud privé ou d'entreprise offre un niveau de sécurité beaucoup plus élevé, mais ne peut égaliser les avantages financiers du cloud public. Quoi qu'il en soit, la plupart des utilisateurs sont plus préoccupés par le gain en flexibilité et en évolutivité que par le coût. Dans ce cas-ci la sécurité est adaptée aux besoins du client respectif. Les clients doivent avoir une idée claire du résultat souhaité à l'aide des systèmes et selon les risques que cela entraîne, ce qui permet d'initialiser les contrôles et rapports adéquats, ainsi que les certifications appropriées. Le cloud privé se réfère à une solution individuelle, qui dépend fortement de la coopération étroite entre le client et le fournisseur, exigeant du fournisseur une gestion correcte des processus de l'entreprise.

Divers fournisseurs de services, tels que par exemple Easynet, sont certifiés selon les niveaux de sécurité internationale ISO 27001 et ISO 9001 en termes de gestion de qualité, de collaboration avec les clients et de réalisations d'audits. D'autres attestations qui s'appliquent à l'environnement cloud comprennent par exemple: ISAE3402 ou SSAE16. Ces certifications sont essentielles quand il s'agit d'informations sensibles et critiques pour l'entreprise, comme le traitement de carte de crédit. Ce qui autorise l'utilisation du service cloud privé de gérer de l'information critique est donc bien la séparation physique entre les ressources des différents clients.

4. L'importance du réseau

Une enquête réalisée en début d'année parmi des CIO's a révélé que, tandis que la moitié prévoyait d'augmenter leurs investissements dans le cloud, à peine un CIO sur cinq perçoit le réseau comme un élément crucial dans la formulation de la stratégie du cloud. Cela signifie que les entreprises ne connaissent pas suffisamment en détail les implications du cloud, ainsi que son effet sur le réseau. Auparavant les données étaient limités au LAN (local area network), aujourd'hui elles traversent le réseau de l'entreprise, voire même l'Internet public, ce qui peut entraîner des tensions importantes sur le réseau. Dès lors les utilisateurs peuvent rencontrer des problèmes de performance majeurs pour des tâches relativement banales.

Justin Fielder, CTO, Easynet Global Services : "Je suis convaincu que les experts du réseau jouent un rôle important dans leur démonstration par rapport à la planification d'urgence et le design intelligent du réseau permettant d'atténuer certains de ces problèmes"

Le cloud résout, grâce à la structure fortement distribués et virtualisés, un grand nombre de problèmes de continuité. Toutefois, la dépendance du réseau joue encore un rôle trop important en tant que point unique de défaillance, ce qui signifie qu'il en faut peu pour totalement exclure un bureau régional du service. Dans la plupart des cas, une connexion redondante (basée sur l'ADSL ou l'ISDN) serait une réponse évidente pour assurer la connectivité, mais est-ce suffisant pour gérer les exigences du cloud et tout ce qui traverse le réseau, telles que la téléphonie?

Avec l'application largement répandue de services basés sur le cloud, on observe un accroissement de la demande de nouveaux produits qui viennent compléter les activités existantes, non seulement dans la technologie de réseaux sous-jacents (passer à une connexion fibre moins cher), mais aussi dans l'utilisation double de la bande passante.

Une approche que beaucoup d'entreprises choisissent pour résoudre ce défi consiste à recourir à ce que l'on nomme l'utilisation 'actifs-actifs' du réseau. Le principal avantage de cette nouvelle solution est qu'elle est basée sur deux connexions réseaux séparées, qui coopèrent en situation normale : l'une donne la priorité aux données vocales, à l'intranet, à l'ERP etc., et l'autre gère le trafic non-critique pour l'entreprise - internet, médias sociaux, extranet etc. Le principal est que lorsqu'une connexion primaire ou secondaire est coupée, l'entreprise doit disposer d'un réseau MPLS suffisamment intelligent pour donner la priorité au trafic critique.

Ceci présuppose non seulement un prestataire de services attentif, disposant des instruments de contrôle adéquats pour déterminer quand une connexion est coupée, mais aussi d'un réseau MPLS assez intelligent pour donner la priorité au trafic des données. Ce niveau technologique doit être soigneusement pesé, puisque les formes de «communication» sont bien différentes.

Toutefois, cela ne signifie pas que la gestion de la continuité des activités est la clé pour les entreprises engagées dans le problème du cloud. Le réseau doit répondre à de nouvelles exigences et dans de nombreux cas les infrastructures existantes en sont incapables. Vu l'évolution de données hébergées localement vers un hébergement à distance, il est raisonnable de supposer que les niveaux de service, de

performance et de bande passante d'une entreprise ne sont pas capables de répondre aux exigences souhaitées.

Nous savons que la conception d'un réseau MPLS pouvant répondre aux critères de performance pour des applications clés d'une entreprise, tout en maintenant les besoins quotidiens des utilisateurs finaux, n'est pas une tâche triviale. On ne peut certainement pas prendre de décisions basées sur les réclamations majeures des fournisseurs de services. Il est crucial que le fournisseur prenne le temps et fasse l'effort de comprendre où vos données se trouvent et comment elles se déplacent à travers le réseau, avant de conseiller un design de réseau approprié. Le marché est submergé de fournisseurs proposant des solutions MPLS qui à première vue semble simple. Ceci est davantage erroné, si vous voulez une stratégie cloud à votre avantage.

Le temps du "j'installe et puis j'oublie" du MPLS est maintenant terminé. Il faut choisir une solution dotée d'un niveau d'intelligence supplémentaire - ce qu'Easynet appelle un SMART MPLS. En cas de panne, le réseau recherchera automatiquement la source du problème et prendra des mesures correctives. Cette solution innovante garantit des connexions stables, un transfert rapide des services, sans préjudicier l'utilisation par les utilisateurs finaux.

En plus du SMART MPLS des configurations simples sont réalisables pour des performances optimales, comprenant des investissements peu élevés et une gestion facile. La principale différence entre le MPLS et le SMART MPLS est qu'au lieu du réseau MPLS, qui comprend et privilégie le trafic IP, il est capable de comprendre, de rapporter et, plus important encore, il est toujours en mesure de réagir sur les applications qui passent par le réseau.

Justin Fielder poursuit: «Le cloud impose des exigences de plus en plus élevées au réseau d'entreprise, et les entreprises attendent que ce réseau soit capable d'y faire face . Sans la flexibilité intégrée du service «actifs-actifs», ou l'intelligence du SMART MPLS, le risque pour les entreprises d'avoir une première expérience négative par rapport au cloud est bel et bien réel. J'espère me tromper».

A propos d'Easynet Global Services

Easynet Global Services est un fournisseur international de [réseaux administrés](#), [d'hébergement](#), et de services d'intégration à valeur ajoutée comme la [Télépresence](#). La société a des clients dans 50 pays et compte 900 salariés dans 25 bureaux dans le monde, dont ViaMichelin, FOX, Brinks, Transport for London, EDF, SAGE, Q-Park et Bridgestone. LDC (Lloyds TSB Development Capital) est la branche de private equity mid-market de Lloyds Banking Group, qui possède avec l'équipe de management de l'entreprise la totalité d'Easynet. Vous trouverez de plus amples informations sur www.easynet.com et vous pouvez également suivre Easynet via [@easynet](#) et [Easynet | LinkedIn](#).

Pour plus d'informations :

Laurence Van Doosselaere

Tél : +32 (0)2 402 37 58

E-mail : Laurence.VanDoosselaere@easynet.com