Introduction

Vous pouvez trouver des technologies cloud et leurs applications pratiques dans plusieurs domaines d'activité. Avec chaque année qui passe, de plus en plus d'organisations les utilisent dans leur travail. L'avenir appartient à ces solutions cloud et elles connaissent un succès commercial.

La migration vers le cloud est le processus de déplacement des applications, des données ou même de l'ensemble de l'infrastructure informatique de l'entreprise vers les installations de serveur distant et un environnement virtuel. Les avantages de la migration vers le cloud sont notables. L'architecture cloud permet d'accepter n'importe quelle charge de travail, et la facilité d'inclure de nouveaux services offre une chance de répondre rapidement à l'évolution des besoins de l'entreprise.

En raison de problèmes de fiabilité et de sécurité, plusieurs organisations retardent encore leur migration vers le cloud. Sinon, ils pourraient ne pas trouver cela bénéfique. Néanmoins, le monde se transforme et à l'heure actuelle, les technologies cloud sont incontournables.

4.5.1. Détérioration du service à la clientèle et du service qualité.

Solutions d'infrastructure cloud tierces présentes un risque pour le service à la clientèle et la qualité globale du service pour gestionnaires de support, ingénieurs de support et service client Personnel. Les responsables de l'assistance et les ingénieurs risquent de devenir dépendant d'un fournisseur de services cloud qui ils n'ont aucun contrôle sur et risquent d'exiger des ressources supplémentaires pour effectuer la migration et gérer les problèmes à court terme qui surviennent à la suite de la migration (par exemple, des lacunes dans les connaissances sur les opérations cloud entraînant tâches prenant temporairement plus de temps à accomplir). Soutien les managers et les ingénieurs risquent plus particulièrement de devenir dépend d'un fournisseur de services cloud pour la résolution problèmes de matériel et de réseau. C'est un risque car cela pourrait entraîner la détérioration de la qualité de service que le responsable du support ne serait pas en mesure de contrôler. Soutien les gestionnaires risquent également d'avoir temporairement besoin de plus de ressources faire face à la migration et aussi le manque relatif des connaissances et l'expérience détenues par le personnel de soutien concernant systèmes en nuage. Il s'agit d'un risque car le personnel peut initialement besoin de plus de temps pour effectuer les mêmes tâches en raison de pour apprendre à effectuer des tâches dans l'environnement cloud qui pourrait compromettre la qualité du service et le client service. Le personnel du service à la clientèle risque également de ne pas pouvoir offrir les niveaux de service à la clientèle existante, car cela peut prendre plus de temps pour résoudre les questions des clients que la coopération avec des prestataires de services externes peuvent devenir nécessaire. C'est un risque car les temps de réponse pour traiter avec le client les requêtes peuvent augmenter, entraînant des arriérés et des cascades de travail supplémentaire car le client rappelle pour l'avancement mises à jour et se traduira par le personnel de service à la clientèle insatisfaction.

4.5.2. Diminution de la satisfaction.

les implémentations d'infrastructures du cloud présentent un risque de diminution de la satisfaction au travail des ingénieurs de support, des ventes et personnel de marketing et personnel de service à la clientèle. Soutien des ingénieurs risquent de diminuer la satisfaction au travail car le travail peut passer d'un rôle technique pratique à un rôle de rapport et de rechercher des problèmes avec des fournisseurs de services du cloud. Les ingénieurs de support deviendront dépendants du réactivité des fournisseurs de services tiers pour résoudre les problèmes réduisant ainsi le niveau de prise en charge du contrôle.les ingénieurs ont plus de problèmes à résoudre. Il s'agit d'un risque pour soutenir la satisfaction des ingénieurs car ils tirent satisfaction des aspects techniques du travail et résolution rapide des problèmes à la satisfaction du client. Les ventes et le personnel de marketing risque de diminuer la satisfaction au travail si on leur fixe des objectifs irréalistes concernant la vente des nouveaux services basés sur le cloud. Il s'agit d'un risque pour les ventes et la satisfaction du marketing car ils tirent satisfaction d’atteinte des objectifs de ventes et de parts de marché. Le service client et le personnel risque également de diminuer sa satisfaction au travail parce que son capacité à accomplir leur travail dépendra de tiers parties hors de leur contrôle entraînant un plus grand décalage entre les requêtes des clients et la résolution

4.5.3. Réduction des effectifs départementaux.

les implémentations d'infrastructures du Cloud tiers présentent un risque de réduction des effectifs aux départements de support informatique. Support Informatique les départements risquent de réduire leurs effectifs si la majorité de leur travail comprend le support matériel et réseau. Cette est un risque car les fournisseurs de cloud seront responsables de le maintien de ces aspects de soutien rendant la capacité inutile au sein du service de support informatique.

Les gestionnaires de support et les ingénieurs de support seront touchés car les ingénieurs de support peuvent perdre leur emploi et les gestionnaires de support peuvent perdre de l'influence car ils ont un petit département

4.5.4. Incertitude avec les nouvelles technologies.

les implémentations d'infrastructure cloud présentent un risque pour le personnel des finances/développement des affaires, car cela peut ouvrir l’organisation à la volatilité à long terme dérivée des forces du marché associées aux coûts d'utilisation d'un cloud et les frais de transfert des données. Il s'agit d'un risque à moyen et à long terme la viabilité d'une solution cloud versus la solution d’hébergement interne est incertaines. De plus, le passage à l'externe hébergement diminue la certitude et l'enfermement du client dans les termes des contrats de support logiciel est maintenu à l'extérieur et donc l'entreprise peut ne prétendez plus qu'il offre un "tout-en-un". le contrat de maintenance qui évite d'avoir affaire à plusieurs contacteurs. Une autre considération est la perte de l’expertise interne entraînant des obstacles supplémentaires à ramener le système en interne si le fournisseur de cloud est inadéquat.

4.5.5. Manque de ressources de soutien.

les implémentations d'infrastructures Cloud présentent une ressource de risque de la rareté des départements de supp+ort informatique et de vente/marketing. Il existe un risque d'augmentation temporaire des départements du support informatique pour faire face à la migration. le manque de connaissances et d'expérience a tenir le soutien des ingénieurs concernant les systèmes cloud. C'est un risque car le personnel peut initialement avoir besoin de plus de temps pour effectuer la même tâches en raison de devoir apprendre à le faire dans l’environnement du cloud. Il y a un risque d'augmentation temporaire des effectifs commercial/marketing pour faire face à la création et au lancement de nouveaux produits/services basés sur le cloud. C'est un risque car le personnel des ventes et du marketing devra développer des stratégies et du matériel pour s'assurer que le marché est au courant de l'offre de produits.

En résumé, ces résultats illustrent que si les analyses financières et technologiques sont certainement importante, la dimension organisationnelle doit également être considéré. Ceci doit être particulièrement pris en compte à partir de la perspective de la qualité du service et du service à la clientèle, et la gouvernance organisationnelle et les implications de risque d'être si fortement dépendant d'un tiers pour le produit/service de livraison aux clients. Dans certains cas, les finances la dimension n'est peut-être même pas la principale considération pour les applications critiques pour l'entreprise. Ces constatations sont renforcée par le fait qu'actuellement la majorité de la direction de l'organisation est réticente à mettre en œuvre le changement au-delà d'un environnement de test malgré les incitations financières car les risques sont perçus comme supérieurs des économies perdues.

Parmi les scénarios possibles qui peut se produire :

1. Latence indésirable.

La latence supplémentaire est un risque de migration vers le cloud qui est souvent sous-estimé (ex : la validation du service d’achat est ralenti). Un retard de quelques secondes de votre application peut sérieusement nuire à votre entreprise. Non seulement la latence est une cause de frustration pour les clients, mais elle peut également avoir un impact grave sur la réputation de votre marque. Il existe un certain nombre de solutions possibles aux problèmes de latence, mais si ces méthodes ne fonctionnent pas ou sont trop coûteuses, il peut être judicieux de conserver certaines de vos données sur site.

Pour se débarrasser des problèmes de latence, vous devez d'abord comprendre ses causes : une QoS (Quality of Service) mal configurée et la distance géographique entre les serveurs et les appareils clients. Il existe de nombreuses façons de résoudre les problèmes de latence :

Diviser les flux de trafic

Optimiser et localiser le réseau

Déchargez Internet à la fin

Créer une connectivité multicloud

Connectez-vous avec des écosystèmes et des partenaires commerciaux pour des affaires en ligne ou des échanges de données.

Si les stratégies de migration vers le cloud susmentionnées sont coûteuses pour vous ou ne vous aident pas, envisagez de conserver ces applications sur site.

2. Dépenses excessives.

Les modèles de tarification des fournisseurs de cloud sont flexibles (ex : la stratégie de hébergement de l’application e-commerce n’est pas adaptées), mais ils peuvent souvent être difficiles à comprendre. Cela peut entraîner et entraîne parfois des dépenses inutiles pouvant atteindre 70 % des coûts du cloud.

Il existe différents frais impliqués dans le cloud computing, et chaque fournisseur proposera une gamme différente de services et de prix. Il peut être difficile de choisir la meilleure combinaison. Si vous ne faites pas les calculs nécessaires pour déterminer exactement ce dont vous avez besoin, vous risquez de perdre beaucoup d'argent.

Assurez-vous d'optimiser vos coûts - et si vous ne savez pas comment, engagez un expert pour le faire pour vous.

Vous devez optimiser vos coûts de cloud. Au cas où vous ne le sauriez pas, engagez des experts pour vous aider. Certaines pratiques courantes d'optimisation des coûts du cloud sont les suivantes :

Utiliser les remises

Effacer les instances sous-utilisées

Augmentez les instances ponctuelles pour les serveurs sans serveur et les éléments qui n'ont pas besoin d'une haute disponibilité

Administrez vos charges de travail

Dépenses en instances réservées

Profitez de l'autoscaling

Vérifiez si l'hébergement dans une autre région pourrait réduire les coûts

Correction des alertes pour franchir les seuils de dépenses prédéterminés

Déplacer le stockage à accès irrégulier vers des niveaux moins chers

3. Suppression incomplète des données.

Bien que la perte de données soit un réel problème (ex : la suppression des données répliquées peut engendrer des incohérences), il peut y avoir un autre problème à l'autre bout du spectre. Lorsque vos données sont réparties sur plusieurs périphériques de stockage, ce risque est encore plus préoccupant. Lorsque vous avez besoin de supprimer des données en temps opportun, mais que ces données sont enregistrées sur le même matériel que les données d'autres clients, ce n'est pas aussi simple que de simplement détruire le disque. De plus, étant donné que les procédures de suppression peuvent différer d'un fournisseur à l'autre, il peut être difficile de vérifier si vos données ont été supprimées de manière sécurisée et de s'assurer qu'il n'en reste rien. Plus vous utilisez de services CSP, plus cette menace devient importante.

Les principaux fournisseurs de services cloud comme AWS et Azure offrent une sécurité. Ils s'assurent de protéger vos actifs physiques contre tout accès non autorisé. Les fournisseurs de cloud maximum disposent d'un excellent portefeuille de services de conformité intégrant FIPS, CJIS, HIPAA, DISA, ITAR, etc. Ils dépensent beaucoup en sécurité pour protéger les données des clients contre les cybermenaces.

De plus, ils fournissent des solutions exclusives pour sécuriser les données de vos clients lors de la migration vers le cloud. Néanmoins, vous devez embaucher une équipe de sécurité expérimentée et des ingénieurs DevOps formés qui peuvent effectuer les configurations requises et garantir la sécurité des données à long terme dans le cloud :

Autoriser l'authentification multifacteur

Chiffrer les ressources de données en cours de migration et au repos

Établir des politiques d'accès des utilisateurs

Configurer un pare-feu

Former les autres sur les moyens de maintenir la sécurité dans le cloud

Exécuter les contrôles requis

Séparez les charges de travail individuelles pour réduire tous les dommages qui pourraient survenir à cause d'un attaquant

5. Perte de données.

Chaque fois que des données sont déplacées pour être stockées dans un nouvel emplacement,(ex : l’extension de la capacité du stockage en utilisant de nouveau périphériques) il y a toujours un risque qu'elles soient perdues. Que ce soit en raison de divers problèmes techniques ou en raison d'une erreur humaine, certains de vos fichiers peuvent être manquants, incomplets ou corrompus. Assurez-vous que votre CSP dispose d'options de sauvegarde, de restauration et de basculement des données. C'est une bonne idée de faire sauvegarder vos données par plus d'un fournisseur de cloud, de sorte que vous n'aurez pas à vous soucier des temps d'arrêt inattendus d'un fournisseur particulier. De plus, c'est une bonne idée de sauvegarder également toutes vos données importantes sur un disque.

Qu'il s'agisse d'une violation de la sécurité ou d'une panne de courant dans un centre de données, tout peut entraîner une perte de données. Ainsi, si vous stockez les sauvegardes des bases de données dans le cloud ou sur un serveur, vous pouvez restaurer toutes les données rapidement.

De plus, si vous utilisez de nombreux fournisseurs de cloud, vous n'avez pas à vous inquiéter de l'échec soudain du service d'un fournisseur spécifique. Vous pouvez toujours distribuer une réplique indépendante de votre application sur l'infrastructure d'un autre fournisseur.

Assurez-vous de configurer la sauvegarde des données migrées pour économiser beaucoup de temps et d'argent. N'oubliez pas de sauvegarder votre ancien système afin de pouvoir retrouver tous les fichiers manquants si nécessaire.

´

4. Visibilité et contrôle réduits.

Le manque de visibilité dans le cloud public est un risque très réel de migration vers le cloud qui peut affecter les performances (ex : délégation de la gestion des données et réseau au hébergeur). Lorsque vos données sont stockées sur site, vous avez un contrôle total sur toutes vos ressources, politiques et infrastructure. Mais lors de la migration vers des services cloud externes, certaines de ces responsabilités sont transférées au fournisseur de services cloud (CSP), ce qui peut entraîner une visibilité réduite pour votre entreprise.

Désormais, plusieurs outils peuvent vous aider dans la surveillance des performances de l'application et du réseau. Les fournisseurs de sécurité tiers et les fournisseurs de services cloud proposent de nombreuses solutions pour cela. Voici quelques demandes pour des outils de surveillance efficaces :

Réponse automatique à certains types de menaces et d'alertes

Une courbe d'apprentissage abrupte

Périmètres de configuration des différents types d'alertes

Analyses solides

Une solution de monitoring doit s'intégrer simplement avec d'autres solutions

Capacités de surveillance fondamentales sans exigence de configuration manuelle

3. Risques de sécurité.

Ce sont probablement les plus grands risques auxquels sont confrontées les entreprises qui passent au cloud computing ( ex : la sécurité est assurée par l’hébergeur). La migration vers le cloud implique toutes sortes de risques de sécurité, des violations de conformité et des violations contractuelles aux API non sécurisées, aux erreurs accidentelles, aux logiciels malveillants, aux attaques externes, etc. Il est essentiel que, lors du passage au cloud, vous soyez conscient de ces risques et que vous vous armiez pour les gérer.

Lorsque vous choisissez un fournisseur de cloud, recherchez-en un avec un portefeuille de conformité solide. Dans le même temps, vous aurez besoin d'ingénieurs DevOps expérimentés et d'une équipe de sécurité capable de prendre des mesures pour assurer la sécurité à long terme de vos données dans le cloud. Cela inclut le chiffrement des données en transit et au repos, la configuration d'un pare-feu, l'isolement des charges de travail individuelles afin de minimiser les dommages potentiels et la formation des autres sur le maintien de la sécurité des données dans le cloud.

Les principaux fournisseurs de services cloud comme AWS et Azure offrent une sécurité. Ils s'assurent de protéger vos actifs physiques contre tout accès non autorisé. Les fournisseurs de cloud maximum disposent d'un excellent portefeuille de services de conformité intégrant FIPS, CJIS, HIPAA, DISA, ITAR, etc. Ils dépensent beaucoup en sécurité pour protéger les données des clients contre les cybermenaces.

De plus, ils fournissent des solutions exclusives pour sécuriser les données de vos clients lors de la migration vers le cloud. Néanmoins, vous devez embaucher une équipe de sécurité expérimentée et des ingénieurs DevOps formés qui peuvent effectuer les configurations requises et garantir la sécurité des données à long terme dans le cloud :

Autoriser l'authentification multifacteur

Chiffrer les ressources de données en cours de migration et au repos

Établir des politiques d'accès des utilisateurs

Configurer un pare-feu

Former les autres sur les moyens de maintenir la sécurité dans le cloud

Exécuter les contrôles requis

Séparez les charges de travail individuelles pour réduire tous les dommages qui pourraient survenir à cause d'un attaquant