10 point importants avant de faire le pas vers le Cloud hybride

9

10 point importants avant de faire le pas vers le Cloud hybride

Les entreprises semblent adopter pleinement le cloud computing hybride. Mais comment y aller de la bonne façon ? Voici quelques grands points auxquels il faut faire attention dans la conception de ce type de projet.

1. Complexité de l'architecture et ressources adéquates

Un environnement de cloud computing hybride est une architecture informatique extrêmement complexe qui implique différentes combinaisons de cloud computing public et privé et d'informatique sur site. Il faut un personnel informatique aguerri pour structurer et gérer une infrastructure de bout en bout qui doit prendre en charge des transferts de données continus entre toutes ces plates-formes…[lire la suite]

2. Coordination des achats de cloud computing et des besoins des utilisateurs finaux

La pire façon de se lancer dans une stratégie de cloud computing hybride est de le faire au petit bonheur la chance. Ces situations se produisent lorsque les départements métiers et le département informatique souscrivent indépendamment à des services de cloud computing…[lire la suite]

3. Bien gérer la complexité de la gestion des données

De plus en plus d'entreprises utilisent des systèmes automatiques dans leurs centres de données pour acheminer les données vers différents niveaux de stockage (rapides, moyens ou rarement utilisés), et ce en fonction du type de données et des besoins d'accès aux données…[lire la suite]

4. Sécurité et confidentialité des données

La sécurité et la confidentialité des données s'améliorent dans le cloud, mais cela ne change rien au fait que le département informatique d'entreprise a un contrôle direct sur la gouvernance, la sécurité et la confidentialité des données que l'entreprise conserve dans son propre centre de traitements, alors qu'il n'a pas ce contrôle direct dans le cloud computing…[lire la suite]

5. Débit et latence, deux points critiques

L'accès au cloud computing peut se faire via un réseau privé sécurisé ou, plus souvent, via Internet. Cela signifie que la gestion du débit et le risque de latence pour les flux de données en temps réel et les transferts de données en masse deviennent plus risqués que lorsqu'ils se produisent au sein du propre réseau interne de l'entreprise…[lire la suite]

6. Reprise après sinistre et reprise à chaud

Les entreprises qui transfèrent des données et des applications vers le cloud computing doivent demander à voir les plans de reprise après sinistre et les engagements de reprise après sinistre et reprise à chaud des fournisseurs de cloud computing…[lire la suite]

7. Changement de fournisseur

Pourrez-vous facilement changer de fournisseur de cloud computing si tel est votre choix ? Si cette opération peut être facile sur le plan technique, elle pourrait être plus compliquée d'un point de vue contractuel ou de la coopération…[lire la suite]

8. Gestion des contrats et des licences sur site

Si vous transférez des applications sur site vers le cloud computing, la coordination sera optimale si vous parvenez à opérer cette transition au moment où vos licences logicielles sur site expirent. La migration vers le cloud n'est généralement pas un problème si vous conservez le même fournisseur, mais elle peut le devenir si vous quittez un fournisseur pour un autre…[lire la suite]

9. SLA des fournisseurs

De nombreux fournisseurs de cloud computing ne publient pas de contrats de niveau de service (SLA) et ne les incluent non plus dans leurs contrats. Si vous prévoyez de migrer vers un environnement de cloud computing public ou un environnement de cloud privé hébergé par un fournisseur extérieur, les SLA de base que vous devez exiger de la part de votre fournisseur concernent le temps de disponibilité, le délai moyen de réponse, le délai moyen de résolution des problèmes et le délai de reprise après sinistre…[lire la suite]

10. Gestion du risque et responsabilité du fournisseur

Quelle est la responsabilité du fournisseur en cas de sinistre (et de temps d'arrêt) d'un service qui nuit à votre entreprise ? Que se passe-t-il si le fournisseur n'a pas de contrôle sur les circonstances qui ont conduit au problème ? (Cela peut être le cas si le fournisseur de cloud ne possède pas ses propres centres de traitements et les loue à des tiers et que le problème provient d'un de ces centres de traitements.) Qu'en est-il si une brèche de sécurité touche vos données dans le cloud ?…[lire la suite]

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Cloud hybride : 10 points de vigilance à bien noter – ZDNet