



VOUS PILOTEZ UNE STRATÉGIE MULTI-CLOUD ? **FREIN POUR LA SÉCURITÉ.**

Comment assurer la viabilité de votre projet multi-Cloud et la sécurité de vos données



SOMMAIRE

- 3** Le chemin vers le multi-Cloud débute ici
- 4** Le carrefour vers trois obstacles
- 5** Bâtir une route sécurisée vers l'avenir
- 7** En route pleins gaz entouré des bons partenaires
- 8** À propos de Snowflake

LE CHEMIN VERS LE MULTI-CLOUD DÉBUTE ICI

Souvenez-vous : il y a quelques années encore, tout le monde dans les départements informatiques se demandait *s'il fallait passer au Cloud*. Depuis, de l'eau est passée sous les ponts. Aujourd'hui, la plupart des grandes entreprises ont emprunté la voie du Cloud et se demandent plutôt *combien de Clouds elles doivent utiliser*.

S'il n'y a pas qu'une seule manière de répondre à cette question, sachez que les grandes entreprises utilisent en moyenne 4,8 Clouds publics et privés, d'après le rapport sur l'état du Cloud 2018 de RightScale.¹ Cette stratégie, connue sous le nom de « stratégie multi-Cloud », présente des avantages indéniables. En effet, elle crée des redondances au niveau des données afin de réduire ou d'empêcher la perte de données et les temps d'arrêt. Elle apporte également de la flexibilité dans les processus, permet d'harmoniser les offres du Cloud avec les besoins des départements informatiques, et évite la dépendance vis-à-vis d'un seul fournisseur Cloud. L'immense

majorité des grandes entreprises (81 %) a déclaré en 2018 avoir justement opté pour une stratégie multi-Cloud.

Ces entreprises sont également en demande d'une stratégie multi-Cloud auprès de leurs fournisseurs de services SaaS. Le recours à un seul fournisseur Cloud ne suffit plus pour assurer une haute disponibilité.

Alors que les dirigeants insistent auprès des cadres de direction pour qu'ils développent et améliorent leur stratégie multi-Cloud dans un délai d'un ou deux ans, les entreprises doivent également peser les risques de sécurité qui découlent d'une telle approche. La prise en charge de données et d'applications localisées sur différents Clouds n'est pas une sinécure, et il n'y a pas de formule magique pour sécuriser les processus. Cette mutation entraîne son lot de casse-têtes inédits pour les CISOs, les DSI, les CTOs et les équipes DevOps.

Nous sommes passés par là. Chez Snowflake, nous avons récemment annoncé notre partenariat avec GCP, complétant ainsi notre présence sur AWS. Passer au multi-Cloud représentait un projet ambitieux et qui s'inscrivait sur la durée, car nous

voulions opérer dans les règles de l'art. Notre objectif était de proposer le même service et de devenir agnostique en matière de plate-forme Cloud, tout en répondant aux problèmes de sécurité qu'impliquait le passage au multi-Cloud.

Dans cet ebook, vous découvrirez les problèmes de sécurité auxquels se heurtent les entreprises lorsqu'elles décident d'adopter une stratégie multi-Cloud. Vous y trouverez également des recommandations sur la manière de travailler avec les fournisseurs et les partenaires afin de surmonter ces difficultés et réussir dans un environnement multi-Cloud.

¹ 2018 State of the Cloud Report™, RightScale. <https://bit.ly/2xRsaoE>

LE CARREFOUR VERS TROIS OBSTACLES

Pour illustrer les difficultés posées par une stratégie multi-Cloud, observez la scène qui suit : Toute votre vie, vous avez emprunté les routes d'Amérique du Nord, installé sur le siège gauche du conducteur, toujours sur la file de droite. Imaginez le stress que vous pourriez ressentir en passant de l'autre côté de la voiture, et de l'autre côté de la route sur laquelle vous avez toujours roulé. Tous vos repères, apprentissage et expérience, seraient brouillés, vous qui aurez passé toute votre vie à gauche côté conducteur, et à droite sur la route. La moindre manœuvre, ne serait-ce pour tourner à droite, deviendrait difficile et contre nature le temps que votre cerveau s'habitue.

Maintenant, imaginez-vous aller et revenir continuellement entre ces deux modes de conduite. Une minute, vous conduisez en

Amérique, et la minute d'après, vous conduisez en Australie. Savoir de quel côté de la route vous devez rouler et comment changer de voie ou prendre des virages constitueraient des opérations douloureuses.

Cette situation est semblable à celle que vit votre équipe DevOps lorsqu'elle est formée sur un fournisseur Cloud et que vous lui demandez ensuite de travailler sur un autre prestataire. Les concepts de base sont certes identiques, mais leur exécution a une saveur totalement différente. Voici pourquoi.

TERMINOLOGIE

Chaque fournisseur Cloud a créé ou adopté sa propre terminologie, que l'on pourrait apparenter à une véritable langue vivante. Par exemple, lorsque vous échangez avec des clients ou des équipes d'ingénierie sur AWS, vous parlez de VPC, pour « Virtual Private Clouds ». Sur Azure, en revanche, vous discutez « réseaux virtuels » (VNET). Les distinctions sont subtiles, mais si vous connaissez leurs différences et si vous savez parler le bon dialecte en toutes circonstances, alors vous établissez votre crédibilité et prouvez votre expertise dans le domaine.

Cet exemple n'est que la partie immergée de l'iceberg terminologique. Les infrastructures sont différentes, et tout, des concepts de base jusqu'à la technologie propriétaire, s'énonce avec des mots différents. AWS a construit son infrastructure d'autorisation et d'authentification (basée sur des rôles, des utilisateurs IAM, des politiques de service, etc.) tandis que celle d'Azure repose sur Active Directory. De ce fait, tous les manuels, outils et scripts de chaque fournisseur Cloud sont écrits à l'aide d'une terminologie particulière, et aucun espéranto du Cloud n'est là pour les connecter.

TECHNOLOGIE

Alors que la terminologie est distinctive, la technologie sous le capot est encore plus compliquée. Travailler au sein de deux infrastructures disparates ou plus nécessite de la formation pour comprendre et gérer les mêmes fonctionnalités à travers plusieurs Clouds. Cela est envisageable, mais difficile. Et agir ainsi de manière sécurisée, évolutive, et conforme aux exigences de certification, demande d'avoir clairement les reins solides. Développer son expertise prend du temps.

Une fois que vous avez une vision claire de ces technologies, votre équipe DevOps doit encore trouver des moyens de faire la différence entre les fournisseurs Cloud et de toujours avoir une idée claire de leurs spécificités. De plus, elles doivent trouver des parallèles afin de créer des efficacités et affronter les questions de sécurité. Ce n'est pas rien, surtout lorsque tous les processus, des connexions aux rôles en passant par les écritures et le chiffrement, sont traités différemment.

ÉQUIPE

Face à une courbe d'apprentissage abrupte et les complexités associées aux aller-retours entre plusieurs Clouds, vous avez peut-être songé à monter des équipes DevOps distinctes, chacune étant consacrée à un fournisseur Cloud spécifique. L'idée semble judicieuse, car vous mettez les différents Clouds entre les mains d'experts, sans créer la confusion.

Cependant, cette approche génère des silos de données cloisonnées, ce qui va à contre-courant d'une organisation intelligente. Aujourd'hui, la plupart des entreprises redoublent d'efforts pour fluidifier les échanges. La dernière chose à faire est d'ériger de plein gré de nouveaux murs à l'intérieur de votre équipe DevOps. Cette solution court-terme finira par créer des problèmes de croissance, d'alignement de stratégies, de standardisation, et vous empêchera d'apporter les réponses que vos clients s'empressent de recevoir.



BÂTIR UNE ROUTE SÉCURISÉE VERS L'AVENIR

En matière de sécurité, le multi-Cloud en est encore à ses balbutiements. Très peu d'entreprises ou fournisseurs de services SaaS se sont attelés à la difficile tâche de trouver des moyens d'établir des connexions entièrement sécurisées entre les différents fournisseurs Cloud. C'est la mauvaise nouvelle.

La bonne nouvelle, c'est que Snowflake compte parmi les très rares organisations qui ont construit une plate-forme multi-Cloud sécurisée, et qui sont capables et prêtes à partager leur expertise. Les recommandations suivantes vont vous aider à formuler et à mettre en œuvre votre propre stratégie multi-Cloud.

POSEZ DES QUESTIONS

Que vous soyez un fournisseur de services SaaS dont les clients recherchent la redondance du multi-Cloud, ou un CISO, un DSI ou un CTO attiré par les avantages que le multi-Cloud pourrait apporter à son organisation, posez-vous, au minimum, les questions suivantes :

Intégration

- Quelle est votre stratégie multi-Cloud globale ? Où en êtes-vous aujourd'hui dans votre projet de stratégie multi-Cloud ?
- Comment votre entreprise fait-elle le pont entre les différents Clouds ?
- Quelles techniques mettez-vous en place pour faciliter l'intégration ?
- Comment partagez-vous les données d'un Cloud à un autre ?
- Mélangez-vous les Clouds ? Si oui, de quelle manière ? Accordez-vous une place plus importante à un fournisseur Cloud par rapport aux autres ?
- Dans quelle mesure authentifiez-vous et gérez-vous efficacement les comptes d'utilisateurs entre les Clouds ?

Sécurité

- Quelle est votre stratégie multi-Cloud en matière de sécurité ?
- Comment vous organisez-vous pour appliquer la même configuration et la même efficacité à l'ensemble de vos fournisseurs Cloud sur le plan de la sécurité ?

- Comment recueillez-vous des événements et des logs auprès de chaque fournisseur Cloud ? Différentes règles sont-elles définies ? Comment les surveillez-vous ?
- Centralisez-vous les événements et les logs à un emplacement unique afin d'y avoir accès plus facilement ? Avez-vous automatisé ce processus ?
- Comment faites-vous pour que le chiffrement tienne compte des différences de gestion de clés entre les différents fournisseurs Cloud ? Différentes règles sont-elles définies ?

Équipe

- Comment votre équipe DevOps fonctionne-t-elle ?
- Vos employés DevOps travaillent-ils avec plusieurs fournisseurs Cloud ? S'expriment-ils à l'aide de la terminologie officielle de chaque fournisseur ?
- Comment gèrent-ils les différences d'infrastructures ?
- Peuvent-ils créer des outils d'automatisation efficaces ? Quel volume de leur travail est encore représenté par des tâches manuelles ?

Ces questions vont vous permettre de comprendre la manière dont les Clouds sont connectés entre eux, d'identifier les systèmes et les outils utilisés, et dans quelle mesure votre équipe DevOps sécurise votre infrastructure multi-Cloud. Dès que vous avez recours à différentes infrastructures, vous devez les rapprocher les unes des autres. **Lorsqu'il y a convergence de technologies, il y a risques de sécurité.** Les mauvaises configurations peuvent souvent être à l'origine de failles de sécurité potentielles.

Par exemple, un processus non automatisé est particulièrement dangereux. Les efforts manuels augmentent la probabilité d'erreur humaine, qui peut être exploitée par des entités non autorisées désireuses d'accéder aux données des clients. Reste que l'automatisation est un procédé complexe et lourd à mettre en place si on s'y attèle sérieusement. Pour fonctionner, la configuration doit être sophistiquée.

EXAMINEZ LES RAPPORTS DE SÉCURITÉ TIERS

Un PowerPoint ne peut pas répondre aux questions précédentes. Si un fournisseur de solutions SaaS l'utilise pour expliquer la manière dont il gère la sécurité vis-à-vis du multi-Cloud, alors c'est mauvais signe. Dans ce cas de figure, il y a fort à parier qu'il sous-estime les complexités et les différences qui existent entre les environnements Cloud.

Les fournisseurs multi-Cloud doivent documenter leurs sources et leurs mesures de sécurité. Pourtant, ne soyez pas étonné si vous vous rendez compte que très peu d'entreprises semblent prendre la sécurité au sérieux. Une source indépendante, comme un rapport SOC 2 ou tout autre rapport de source externe, doit impérativement détailler les différences entre les mises en œuvre AWS, Azure et/ou Google Cloud.

Par exemple, un rapport SOC 2 contient une section descriptive du système, dans laquelle les similarités et les différences entre les fournisseurs doivent être identifiées, tout comme la différence de traitement des différentes plateformes. Si ces informations ne sont ni mises en avant, ni spécifiques, alors le manque de transparence devrait être reconnu comme un signal d'alarme.

RÉÉCRIVEZ LE CODE

Alors que l'industrie s'intéresse à la question de la sécurité d'une approche multi-Cloud, tout fournisseur de services SaaS ou toute équipe DevOps qui se respecte et qui propose des services de location d'espaces multi-Cloud doit construire

sa propre intégration. Ils devront passer des heures et des heures à chercher péniblement des manières de réécrire le code afin de connecter les différents fournisseurs Cloud de manière sécurisée.

C'est malheureusement une réalité. Les équipes DevOps doivent d'abord connaître la terminologie du nouveau fournisseur Cloud et son infrastructure, puis se heurter aux opacités des API. C'est seulement après qu'ils peuvent déterminer les différentes méthodes de configuration pour chaque fournisseur Cloud, et identifier comment effectuer le portage des éléments entre plusieurs Clouds.

Votre équipe devra écrire des applications ou des scripts d'orchestration d'infrastructure suffisamment complets pour reconnaître l'environnement dans lequel elle évolue, et de manière suffisamment souple pour exécuter un ensemble de code différent en fonction du fournisseur Cloud. Ce défi représente la meilleure manière de standardiser des fonctions et d'automatiser des processus.

FORMEZ VOS TROUPES

Alors que les ingénieurs agnostiques en matière de plate-forme Cloud se multiplieront demain, aujourd'hui, trouver des personnes DevOps capables de travailler à la fois sur AWS et Azure relève du parcours du combattant. Si vous connaissez un professionnel qui

parle les deux langues et qui maîtrise ces deux infrastructures, vous êtes tombé sur la perle rare à qui vous devrez proposer une rémunération particulièrement alléchante pour espérer la séduire. C'est ce que vous devez faire.

Pour la plupart des organisations, vous devrez consacrer du temps, de l'argent et des ressources afin de former vos ingénieurs DevOps pour qu'ils deviennent agnostiques en matière de plateforme Cloud. Dans l'idéal, plongez les membres de votre équipe sénior dans la plateforme Cloud qu'ils ne connaissent pas encore, certainement Azure ou Google Cloud. Non seulement vous développerez leurs compétences et les rendrez plus rares sur le marché du travail, mais cela vous aidera aussi à bâtir un environnement multi-Cloud sécurisé sans plus attendre.



EN ROUTE, PLEINS GAZ ! ENTOURÉ DES BONS PARTENAIRES

Qui arrivera à récolter les fruits du multi-Cloud ? Les entreprises et les fournisseurs de services SaaS qui comprennent comment gérer la question de la sécurité. Cette difficulté est permanente, et continue de s'aggraver à mesure que les entreprises sont de plus en plus nombreuses à adopter des stratégies multi-Cloud. Les entreprises capables de démontrer leur expertise au niveau de la sécurité y auront consacré du temps et des ressources.

Bien qu'il n'existe pas de solutions clés en main pour assurer la sécurité dans un milieu multi-Cloud, n'hésitez pas à profiter de l'expérience de fournisseurs qui sont déjà passés par là.

Si vous vous associez aux bons fournisseurs de services SaaS, vous avez une occasion unique de prendre une longueur d'avance. Certaines organisations, comme Snowflake, ont investi des ressources et du temps pour prendre en charge le multi-Cloud, et c'est ce type de partenaires qui assurera votre sécurité dans les années à venir.





À PROPOS DE SNOWFLAKE

Snowflake est la seule solution de data warehouse pensée et conçue pour le cloud. Snowflake apporte la performance, gestion de la concurrence sans équivalent et la simplicité requises pour stocker et analyser toutes les données existantes d'une organisation dans un même endroit. La technologie de Snowflake combine la puissance du data warehousing, la flexibilité des plateformes de big data, l'élasticité du cloud, et la capacité de partage de données en temps réel à une fraction du coût demandé par les solutions historiques traditionnelles.

Snowflake : Your data, no limits. En savoir plus sur <https://www.snowflake.com/?lang=fr>

À propos de l'auteur

Mario Duarte est vice-président de la sécurité chez Snowflake. Avec près de 20 années d'expérience en tant que professionnel de la sécurité, il a monté et géré ses équipes chargées de la sécurité, développé et mis en œuvre des programmes de sécurité et encadré des initiatives de conformité PCI, HIPAA et FedRAMP pour le compte de moyennes et de grandes entreprises.



© 2018 Snowflake. Tous droits réservés.