Excellence opérationnelle du Cloud: maîtriser les erreurs de configuration

Les fondamentaux d'une architecture d'excellence

Le Cloud regorge d'avantages et vos équipes en sont conscientes. Ces avantages incitent votre entreprise à accélérer sa migration vers le Cloud. Néanmoins, mieux vaut prendre un certain recul pour faire de l'excellence opérationnelle une priorité.

Beaucoup pensent que cette excellence opérationnelle dans le Cloud ne requiert pas autant d'attention que pour les environnements traditionnels sur site. Pourtant, sur le terrain, plusieurs aspects doivent être pris en compte pour tenir cet objectif. Les enjeux et les opportunités sont plus importants que jamais pour mettre en œuvre des stratégies opérationnelles pertinentes. Ceci est d'autant plus vrai lorsque vous collaborez avec un fournisseur de services Cloud (CSP) : vous devez en effet assumer vos responsabilités dans le cadre du modèle de responsabilités partagées du CSP.

Un framework pour gagner en simplicité

Cette quête d'excellence opérationnelle s'initie par l'adhésion des architectes Cloud aux bonnes pratiques telle que définies par les frameworks Well-Architected d'AWS et de Microsoft® Azure™. Ces frameworks ont été conçus pour aider les architectes Cloud et les développeurs à bâtir des infrastructures sécurisées, performantes, résilientes et efficientes pour leurs applications.

L'excellence opérationnelle, un sujet majeur pour les deux frameworks, assure le bon fonctionnement des systèmes en production et offre une approche cohérente qui évalue les architectures et favorise leur évolutivité sur le long terme[1]. Votre architecture et vos workloads doivent être conformes aux bonnes pratiques et normes d'ingénierie pour garantir cette excellence sur le terrain[1]. Ces frameworks constituent un socle pour les entreprises souhaitant exploiter le Cloud plus efficacement et offrir davantage de valeur. Penchons-nous sur cette excellence opérationnelle qui aide à élaborer des architectures favorisant la réussite business.

Des garde-fous pour simplifier l'opérationnel

Si vous comptez mettre sur pied des Centres d'excellence Cloud et déployer des services partagés sur l'ensemble des environnements Cloud, vous devez garantir l'application permanente des bonnes pratiques. Ces garde-fous opérationnels aident les entreprises à atteindre l'excellence opérationnelle, permettant aux fonctions standards de s'exécuter de manière prévisible et cohérente sur l'ensemble du périmètre.

Avec ces contrôles, vous êtes assurés que :

- **Les données critiques stockées dans le Cloud bénéficient d'un contrôle de sécurité renforcé**
- **Les règles d'accès au réseau et les groupes de sécurité sont configurés de manière pertinente pour empêcher les accès prohibés**
- **Les autorisations de gestion des accès et des identités sont définies**

Les fonctions automatisées de contrôle s'assurent que les règles applicables aux services mutualisés sont déployées à grande échelle et dans le respect des bonnes pratiques, des réglementations en vigueur et de la gouvernance. Vous êtes plus serein en sachant que votre entreprise est mieux préparée aux attaques à venir.

Vous avez dit automatisation ?

Pour concrétiser les promesses d'agilité et d'économies du Cloud, l'automatisation s'impose. Tous les développeurs, même les plus aguerris, font parfois des erreurs.

Rendre votre infrastructure "programmable", via des scripts qui automatisent vos processus opérationnels, permet de réduire les erreurs humaines. En revanche, cette approche présente certains risques. Les développeurs travaillent souvent sous pression : ils doivent tenir des délais serrés et fournir des applications qui fonctionnent, même si cela implique parfois d'envoyer les bonnes pratiques de développement aux oubliettes. Ainsi, dans le rush de la sortie d'une nouvelle version logicielle, vos développeurs pourraient être tentés de ne pas configurer des autorisations IAM (gestion des identités et des accès) granulaires pour un serveur virtualisé. Les autorisations basées sur des rôles IAM offrent un niveau supplémentaire de protection puisque votre infrastructure connaît vos utilisateurs et qu'elle leur applique des autorisations sur mesure. Cependant, sans configuration appropriée, l'entreprise peut subir un incident majeur de sécurité. D'où l'importance d'adopter les bonnes pratiques tout au long du cycle de développement, même lorsque les délais sont serrés.

L'automatisation vous permet de tirer le meilleur parti de votre infrastructure Cloud, grâce à des fonctions d'auto-scaling, d'auto-restauration, de scripting, de reporting personnalisé, etc. Avec l'approche « Operations as Code », les architectes et les ingénieurs DevOps peuvent proposer des nouvelles versions de l'infrastructure applicative, au même titre que les développeurs assurent le versioning de leurs applications. Le déploiement et l'exploitation d'une architecture réactive et efficiente permet de supporter des applications adaptées à vos priorités métier.

Infrastructure as Code = accélérer l'innovation

La préférence des entreprises pour l'automatisation, ainsi que l'adoption accélérée du Cloud computing et des pratiques CI/CD aboutissent à une infrastructure conçue, déployée et configurée de manière nouvelle. Le Cloud vous permet de mettre en œuvre et exploiter pratiquement tout ce dont vous avez besoin.

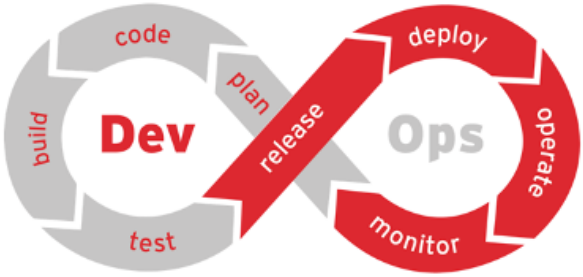
Dans le Cloud, vous pouvez :

- **Appliquer les processus d'ingénierie de votre code applicatif à l'ensemble de votre environnement Cloud.**
- **Définir et mettre à jour vos instances par programmation, à l'aide de templates**
- **Scripter vos procédures opérationnelles et les exécuter automatiquement par rapport à des évènements définis**

Terraform

AWS CloudFormation

Vous pouvez également renforcer l'automatisation à l'aide d'une approche IaC qui permet un provisioning et une gestion des ressources Cloud de votre infrastructure à l'aide de fichiers texte**.** **La gestion de la virtualisation avec l'automatisation** et l'utilisation d'outils d'automatisation (AWS CloudFormation ou Terraform notamment), est une bonne façon de procéder. CloudFormation permet de créer et d'activer, à l'aide d'un simple fichier texte, des ressources d'infrastructure Cloud comme les instances Amazon Elastic Compute Cloud (Amazon EC2). Ce fichier texte décrit un ensemble de ressources AWS devant être déployées et configurées.



IaC présente de nombreux avantages pour concevoir et déployer des projets : cohérence, rapidité et maîtrise des coûts. Cette méthode de déploiement efficace et avancé des infrastructures accélère les modifications au sein de vos environnements Cloud. Voilà qui semble idéal non? Et pourtant...

Des risques en matière de sécurité, de conformité et de performances peuvent être insérés aussi rapidement. Pour tirer parti de l'IaC en toute confiance, il existe des solutions pour tester vos scripts CloudFormation avant leur déploiement : ainsi, seuls les modèles les plus sécurisés sont migrés vers vos environnements. Les modifications pouvant potentiellement causer des dommages peuvent être inspectées simplement, avec la possibilité d'un roll back. Par exemple, si un bucket Amazon S3 (Amazon Simple Storage Service) est créé sans activation de la mise en logs des accès, une fonction AWS Lambda peut automatiquement déployer cette bonne pratique. D'autre part, les Cloud Builders apprécient de pouvoir évaluer les améliorations et la qualité des modèles CloudFormation sans avoir à exécuter le code au préalable.

Oui à la qualité et à la sécurité ! Mais en amont...

DevOps favorise une approche « fail fast, fail often » qui permet aux équipes d'innover et d'avancer rapidement. Si cette approche paraît séduisante, elle ne rassure pas d'un point de vue sécurité, à l'instar d'un bucket Amazon S3 non chiffré et pouvant entraîner une fuite de données.

Dans l'idéal, il vous faudrait des garde-fous à disposition des développeurs, dès les phases amont du pipeline CI/CD. Ces mesures préventives et automatisées ont été adoptées par les Cloud Builders les plus efficaces, pour assurer la sécurité et la conformité du développement des applications, avant que ces derniers ne soient déployés dans le Cloud. Voici quelques erreurs classiques de configuration :

- **Autoriser un accès public aux buckets Amazon S3 hébergeant des données sensibles**
- **Ouvrir trop de ports TCP au sein des groupes de sécurité Amazon EC2**
- **Permettre un accès libre via les NSG (Network Security Groups) d'Azure**
- **Autoriser les comportements malveillants sur Azure SQL**
- **Se tromper dans les autorisations accordées à des utilisateurs et rôles IAM**

Pour éviter l'impact des vulnérabilités de sécurité, des fuites de données Cloud et des problématiques de fiabilité et de performance sur votre environnement de production, vous avez besoin d'une solution qui :

- **Est capable de prédire un incident à venir et présente des solutions de remédiation en amont dans le cycle de développement : les problématiques sont traitées avant qu'elles ne se concrétisent.**
- **Valide vos instances par rapport aux règles en vigueur, avant la mise en production dans le Cloud. Chaque ressource est évaluée par rapport à des centaines de bonnes pratiques et normes : AWS Well-Architected Framework, CIS Microsoft Azure Foundations Security Benchmark, ISO 27001, HIPPA, PCI DSS et RGPD**

Positionner l'excellence opérationnelle, la sécurité, la gouvernance et la conformité dès les phases amont du pipeline CI/CD favorise une prévention automatisée et proactive des erreurs de configuration. D'autre part, ces validations et les capacités de restauration autonomes sont disponibles au sein des environnements Cloud en production. L'analyse de votre code pour évaluer le respect des bonnes pratiques aide votre entreprise à concevoir une architecture optimale.

De (trop?) nombreux intervenants dans le processus

Les cycles modernes de développement logiciel présentent un défi majeur, celui de la multiplicité des équipes impliquées dans la phase de déploiement. Les développeurs, les opérationnels, les ingénieurs d'infrastructure et les business units ont tous un rôle à jouer dans une fourniture applicative performante. Coordonner ces différentes équipes n'est pas toujours chose aisée. Mais quelle que soit la structure de votre équipe, un objectif d'excellence opérationnelle répond à ce défi.

L'excellence opérationnelle, loin d'être une contrainte, peut s'inscrire dans une culture partagée par toutes les équipes et leurs membres lors du développement logiciel et du déploiement. Dans cette optique, vos équipes disposent d'un objectif vers lequel évoluer, ce qui est fondamental dans le cadre d'une collaboration pluridisciplinaire. Cette culture d'excellence opérationnelle aide à définir un référentiel de bonnes pratiques et un processus d'amélioration permanente des cycles de développement et des déploiements, pour contribuer, au final, à la réussite métier.[2]

Les temps changent... Et vous ?

Les fournisseurs de services Cloud proposent régulièrement de nouveaux services et bonnes pratiques. Si vos comptes ont été validés, il y a quelques semaines, comme étant optimisés, fiables, efficients et sécurisés, il n'y a aucune garantie qu'ils le sont toujours aujourd'hui.

Que diriez-vous de disposer d'une visibilité totale sur votre infrastructure ? Et quid d'une application automatiquement des bonnes pratiques de développement, de sécurité et de conformité ? Toute l'information deviendrait visible et vous pourriez faire évoluer votre infrastructure Cloud, jusqu'à l'optimiser. Vous disposez ainsi d'un levier qui encourage l'innovation et jette les fondamentaux de votre réussite en tant qu'entreprise.

L'excellence opérationnelle mise sur un processus d'amélioration continue qui assure une infrastructure parfaitement sécurisée, fiable, efficiente et économique. Chaque évènement ou problématique au niveau de l'opérationnel doit être perçu comme une opportunité d'améliorer votre architecture. Pour les développeurs et les équipes IT, la tâche peut être lourde, mais les équipes qui partagent une culture d'excellence opérationnelle sauront relever ce défi.

Prochaines étapes

Viser l'excellence opérationnelle en matière de Cloud pour atteindre vos objectifs d'innovation implique une solution qui offre :

- **Une visibilité en temps réel sur la sécurité et la conformité réglementaire/interne au sein de votre environnement multi-Cloud.**
- **Des centaines de processus de vérification, avec une fonction de restauration autonome, basée sur le framework well-architected des fournisseurs de services Cloud, l'application des bonnes pratiques et sur la conformité aux normes et réglementations du secteur.**
- **Un reporting capable d'exécuter des analyses selon différents filtres associés pour un audit intégral de votre infrastructure.**
- **Une intégration transparente avec votre pipeline CI/CD et vos workflows existants via des API, pour rendre cette intégration étroite et intuitive au sein de vos environnements de Cloud public.**
- **Des outils d'analyse de modèles lors du processus de coding pour assurer que vos équipes conçoivent une architecture qui prévient les vulnérabilités de manière automatisée et proactive.**

Trend Micro Cloud One™ – Conformity assure la sécurité, la conformité et le monitoring des plateformes SaaS. La solution vous permet de gérer les erreurs de configurations des ressources présentes dans le multi-Cloud. Avec Conformity, les Cloud Builders s'assurent d'une infrastructure Cloud conforme et capable d'accompagner leur croissance.

>> En savoir plus

Références :

1. Fitzsimons, P., B. C., Steele, J., & King, R. (2018). Amazon Web Services – Operational Excellence AWS Well-Architected Framework. Source : https://d0.awsstatic.com/whitepapers/architecture/AWS-Operational-Excellence-Pillar.pdf?ref=wellarchitected-wp
2. Tozzi, C. (2019, novembre 19). Operational Excellence and the Success of Software Deployments. Source : https://devops.com/operational-excellence-and-the-success-of-software-deployments/

TREND MICRO™ Securing Your Connected World