Définir une bonne stratégie de migration vers le Cloud

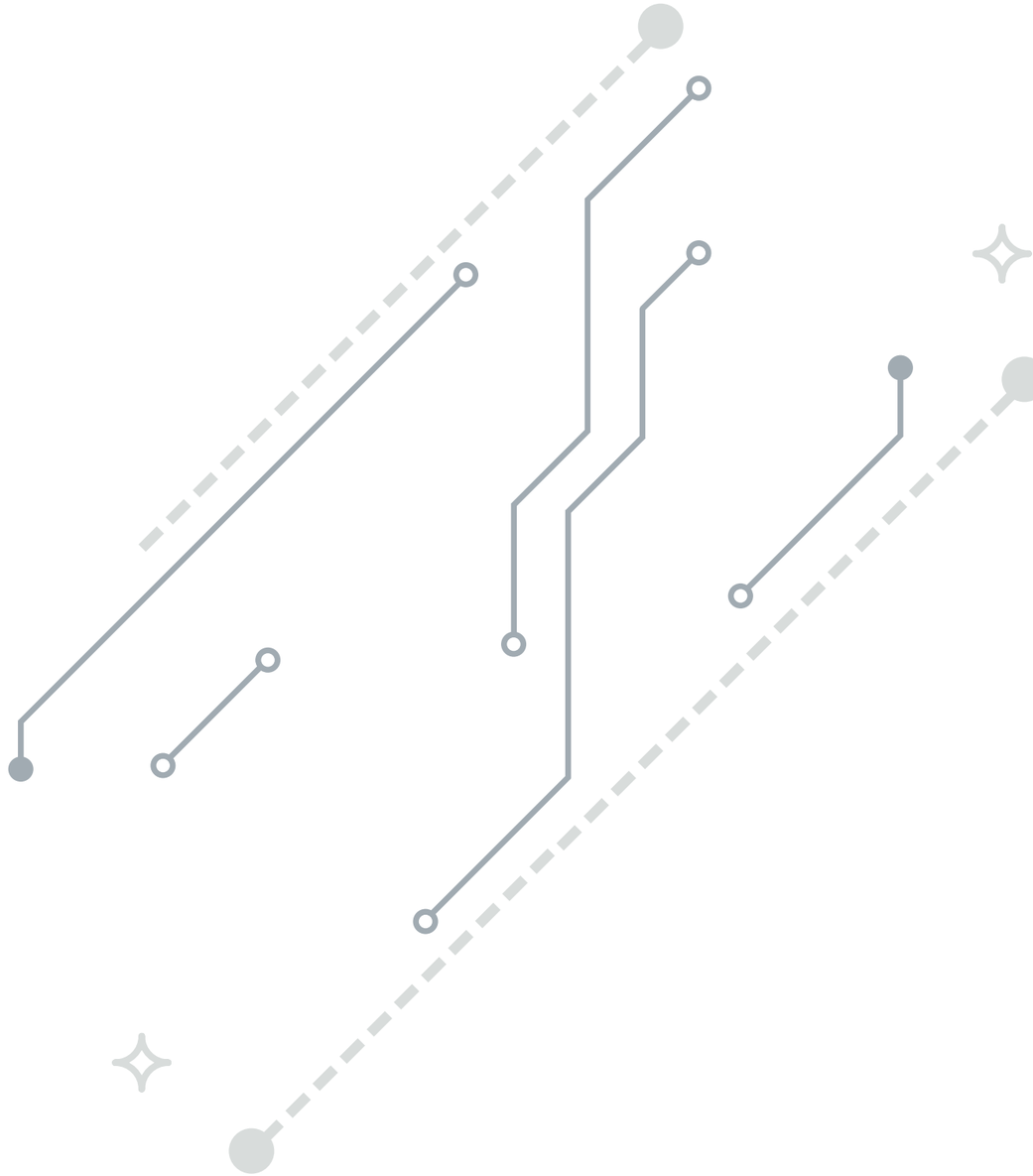
Des conseils pour obtenir une visibilité complète sur les opérations, la sécurité et la gestion des coûts, avant, pendant et après la migration

splunk> turn data into doing™

Obtenez une visibilité complète

En bref

- **Lorsque vous migrez des charges de travail vers AWS** et d'autres infrastructures cloud, il est indispensable de surveiller les performances de l'ensemble des architectures hybrides à l'aide d'outils qui recueillent et corrèlent les données provenant de toutes les sources.
- **N'attendez pas la fin de la migration pour surveiller vos services** de bout en bout. Optez sans délai pour une solution qui établira des valeurs de référence pré-migration, fournir des renseignements pendant la migration, et garantir la réussite post-migration.
- **Seules les solutions de supervision de bout en bout** recueillant facilement les fichiers-journaux des fournisseurs de cloud public peuvent localiser avec précision les vulnérabilités, menaces et violations.
- **Des outils de gestion des coûts** fournissent des informations sur l'utilisation historique et temps réel des instances, mettant ainsi en évidence les ressources sous-exploitées. Mais il est indispensable de mettre en place une économie d'infrastructure exhaustive afin de produire de solides prédictions d'utilisation des ressources, et de prendre des décisions de migration intelligentes.



Le paysage change

Chaque jour, les leaders de l'industrie sont confrontés à des start-ups qui développent intégralement leur activité dans le cloud.

Pour rester à la hauteur, les entreprises numérisent tous les aspects de leurs opérations et cherchent à tirer de l'agilité et des renseignements de leurs données et analyses. Cet effort de transformation consiste notamment à migrer des charges de travail vers AWS et d'autres infrastructures cloud alors que ces charges n'étaient jusqu'ici pas déployées en tant qu'applications compatibles avec le cloud.

pour rester à la hauteur, les entreprises numérisent tous les aspects de leurs opérations et cherchent à tirer de l'agilité et des renseignements de leurs données et analyses. Cet effort de transformation consiste notamment à migrer des charges de travail vers AWS et d'autres infrastructures cloud alors que ces charges n'étaient jusqu'ici pas déployées en tant qu'applications compatibles avec le cloud.

Mais l'infrastructure numérique des entreprises est aujourd'hui devenue plus complexe et englobe des plateformes de cloud hybride comprenant des mainframes, des serveurs clients, de la virtualisation, des architectures sans serveur, des conteneurs et des microservices. Les responsabilités des services IT, en revanche, n'ont pas changé : l'infrastructure doit constamment être surveillée et évaluée. Comment obtenir une visibilité sur l'infrastructure et des renseignements sur les charges de travail lorsque les données de performances concernent divers environnements ?

Et le service IT n'est pas le seul à ressentir les défis dus à la mise en place d'une stratégie cloud. Les services de sécurité doivent maintenir la position de sécurité d'une infrastructure qu'ils ne contrôlent plus directement, et les partenaires commerciaux IT doivent apporter la preuve par retour sur investissement qu'il était rentable d'abandonner la possession pour la location de l'infrastructure.

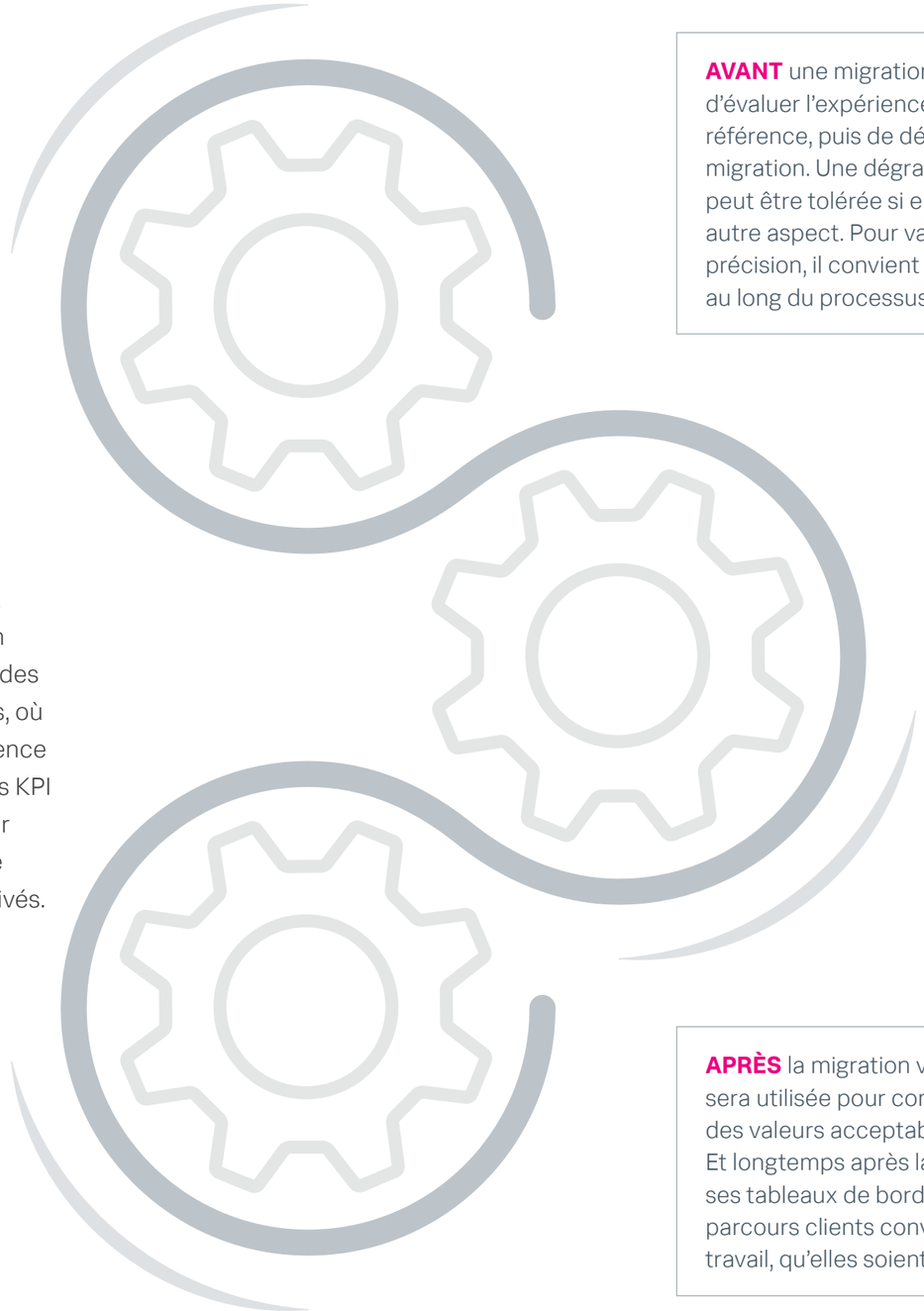
Il est plus que jamais indispensable de superviser les performances de l'ensemble des architectures hybrides à l'aide d'outils qui recueillent et corrèlent les données provenant de toutes les sources. Les solutions de supervision multiples et fragmentées n'offrent pas la visibilité et l'intelligence nécessaires pour atteindre les objectifs commerciaux, de sécurité et IT.

Le point de vue des Opérations Informatiques

Réussir votre migration : avant, pendant et après

Lorsqu'une entreprise migre vers le cloud, elle doit impérativement disposer d'une visibilité de bout en bout sur ses opérations avant, pendant et après le changement, pour conserver en permanence un aperçu clair de ses performances et répondre aux inquiétudes associées à la perte de contrôle sur l'infrastructure. Cette visibilité permet également d'éviter de chercher des coupables lorsque les KPI ne sont pas respectés et que la réputation du service IT est en jeu.

Et comment se traduit la visibilité opérationnelle dans un environnement cloud hybride ? Par une vue de bout en bout des performances de l'ensemble des charges de travail et des microservices, où qu'ils se trouvent. Elle apporte l'intelligence nécessaire pour surveiller et évaluer les KPI et offre donc une expérience utilisateur convaincante lorsqu'une infrastructure s'étend sur des domaines publics et privés.



AVANT une migration vers le cloud AWS, il est important d'évaluer l'expérience utilisateur et les performances de référence, puis de définir les niveaux acceptables post-migration. Une dégradation d'un domaine de performances peut être tolérée si elle est compensée par l'amélioration d'un autre aspect. Pour valider la réussite d'une migration avec précision, il convient d'utiliser le même outil de supervision tout au long du processus.

PENDANT une migration vers AWS, les indicateurs de performances établis doivent être étroitement surveillés. Tout écart par rapport aux valeurs de référence est un signe avant-coureur de problème. Le tableau de bord et les alertes de la solution de supervision indiquent rapidement ces anomalies, bien avant la mise en production, ce qui permet de gagner du temps et d'économiser des ressources. Il est préférable d'identifier les défauts de performances pendant la migration, lorsqu'il est plus facile de suspendre le processus pour apporter des corrections.

APRÈS la migration vers AWS, la même solution de supervision sera utilisée pour confirmer que les indicateurs restent dans des valeurs acceptables, signe de la réussite de la migration. Et longtemps après la transition, la solution de supervision et ses tableaux de bord restent indispensables pour garantir des parcours clients convaincants pour l'ensemble des charges de travail, qu'elles soient sur site ou dans le cloud public.

Le point de vue de la sécurité

Une vue complète pour protéger votre entreprise, mais aussi vos clients

Pour assurer la sécurité d'un environnement cloud hybride, les entreprises ont besoin d'une visibilité de bout en bout sur l'identité et le comportement des utilisateurs, et ce à tous les points d'accès aux applications et bases de données. Cette vue met en évidence les accès non autorisés, la localisation des menaces et des attaques, ainsi que les changements d'autorisation. Elle fournit également des informations cruciales lorsque les points d'entrée sont dispersés sur différentes plateformes et régions.

Lors d'une migration vers AWS, les équipes IT et de sécurité restent responsables de la protection complète des données de l'entreprise et des informations des clients. Et pour les dirigeants des fonctions commerciales, désigner des coupables ou s'exposer à des poursuites est tout simplement inacceptable. Les équipes techniques doivent donc bénéficier d'une visibilité complète sur la position de sécurité de l'ensemble des architectures hybrides, réagir rapidement aux vulnérabilités et menaces et mener des audits en temps voulu.

Cela dit, l'ajout de charges de travail à un cloud public accroît la complexité du paysage de sécurité. Cette démarche augmente le nombre de points d'entrée pour les hackers et ajoute le personnel du fournisseur de cloud à la liste des menaces potentielles. Pour mener une supervision exhaustive de l'activité des utilisateurs à l'échelle de toute l'architecture hybride, il faut impérativement bénéficier d'un accès simplifié aux fichiers-logs AWS et aux outils chargés d'effectuer, de bout en bout, la collecte, la corrélation et l'analyse des comportements suspects.

Supervision des identités et des accès dans AWS

Les fichiers-logs et les outils de supervision d'AWS offrent une excellente visibilité et des analyses de l'activité des utilisateurs. Ils suivent l'identité des utilisateurs qui soumettent, modifient et suppriment des données, ainsi que le moment auquel ces événements se produisent. Ils révèlent également les tentatives d'accès non autorisées, les connexions simultanées depuis des sites disparates et les changements d'autorisation. Ils peuvent même permettre de détecter les modifications accidentelles d'informations.

Les tableaux de bord des outils de supervision d'AWS facilitent la visualisation de l'identité des utilisateurs et des événements d'accès, offrant ainsi une base pour l'analyse des tendances. Les alertes et rapports permettent une transition fluide d'une approche réactive à une approche proactive. De plus, certains outils produisent des analyses prédictives qui délivrent des renseignements de sécurité permettant d'offrir une vue complète de l'infrastructure AWS et de la posture de sécurité. De nombreux outils de supervision peuvent en outre établir des procédures d'audit et appliquer des contrôles de conformité pour garantir le respect des normes internes et industrielles. Grâce aux pistes d'audit, les équipes IT et de sécurité désamorcent rapidement les menaces avant qu'elles ne deviennent des violations de sécurité.

Le point de vue des Opérations

Prédire et gérer les coûts grâce à l'analyse

La migration vers le cloud peut s'accompagner d'économies considérables puisqu'elle réduit le nombre de serveurs à posséder et gérer. Mais si les projections de coût d'AWS s'avèrent incorrectes, c'est tout l'argumentaire commercial du cloud qui peut être compromis. Le retour sur investissement décline, le délai d'amortissement se prolonge, et le service IT se retrouve accusé d'avoir établi de mauvaises projections de capacités. On peut alors observer un écart important entre les dépenses réelles et le budget le plus soigneusement établi.

Un remède à ce risque : une visibilité et de solides projections sur les coûts du fournisseur de cloud. Une fois appliqués aux charges de travail cloud existantes, les outils de supervision contribuent à l'amélioration des prévisions concernant le prochain groupe d'applications à migrer. Grâce aux analyses d'utilisation et de coût, ils indiquent à quel moment déplacer des charges de travail vers le cloud ou préconisent leur maintien en local jusqu'à un changement des structures de coût.

Le machine learning au service de la réduction des coûts

Les analyses effectuées par les outils de supervision du cloud permettent d'optimiser les coûts parce qu'elles suggèrent aux utilisateurs d'acheter des instances à l'avance, à un prix inférieur. En appliquant des algorithmes machine learning aux données d'utilisation des charges de travail existantes, le service IT obtient des prévisions plus précises et peut les ajuster en fonction des pics de demande attendus. Les actifs de l'entreprise sont mieux exploités, ce qui a un impact positif sur les marges. Les prévisions défaillantes mettent en revanche en danger la réputation du service IT ; elles incitent les équipes commerciales à ignorer ses recommandations et à gérer elles-mêmes leurs achats, hors de la visibilité fournie par les outils de supervision.

Plus les choses changent, plus elles se ressemblent

Il est toujours frustrant de ne pas connaître la source d'un problème de performances d'une infrastructure ou d'une menace de sécurité, en particulier au moment critique de la migration d'une charge de travail. Les solutions de supervision diverses et segmentées ne font qu'aggraver le problème en fournissant une image fragmentée d'une infrastructure déjà stratifiée.

Mais une solution de supervision unique, qui propose des tableaux de bord adaptés à différents publics à partir des mêmes données, facilite la compréhension entre les équipes et rend la transition vers le cloud aussi fluide que possible.

Dans la gestion d'un environnement hybride, les objectifs du service IT, sécurité et des fonctions commerciales sont toujours les mêmes. Par exemple :

- Les KPI dont le service IT aura besoin pour surveiller le redimensionnement des instances en fonction des charges de travail sont aussi ceux qui permettent de surveiller les charges locales – et le service IT devra associer ces données aux indicateurs des applications pour mener une supervision globale.
- La sécurité a besoin d'une image complète de toute l'infrastructure – nœuds de cloud, transactions, utilisateurs – pour garantir la posture de sécurité et la protéger face aux menaces potentielles.
- Pour gérer les coûts et calculer le retour sur investissement, les équipes commerciales ont besoin de savoir ce qui a été déployé dans AWS, one source prevents quel est le taux d'utilisation, et si des appareils ont été déconnectés ou abandonnés. Lorsque ces trois services appuient leurs analyses sur une même source, les responsabilités sont plus claires et les silos disparaissent.

Il est plus que jamais indispensable de surveiller les performances de l'ensemble des architectures hybrides à l'aide d'outils qui recueillent et corrèlent les données provenant de toutes les sources. Un outil de supervision de bout en bout couvrant l'ensemble de l'environnement cloud hybride rend service aux trois équipes : IT, sécurité et gestion des coûts. Mais lorsque ces trois équipes travaillent sur les mêmes données, c'est toute l'entreprise qui en tire les bénéfices.

Migrer vers le cloud sans perdre en visibilité

En savoir plus

20-XXXX-SPLK-How-To-Cloud-Migration-Strategy-FR-102-EB

splunk> turn data into doing™