# Accélérez votre **initiative de supervision multicloud**

splunk> turn data into doing™

# L'avènement **du multicloud**

Les migrations vers le cloud ont le vent en poupe, à tel point que Gartner prédit que 80 % des entreprises auront intégralement abandonné les infrastructures locales d'ici 2025. Le dernier développement en matière de cloud computing est l'avènement du multicloud, une stratégie qui consiste à utiliser au moins deux services cloud au sein d'une même architecture ; autrement dit, différentes piles cloud pour différentes tâches, comme Google Cloud Platform pour les applications internes et Amazon Web Services (AWS) pour les applications destinées aux clients. Ce type d'approche a acquis une telle popularité que plus de 80 % des entreprises l'utilisent aujourd'hui.

Différents types de solutions cloud peuvent permettre de composer un environnement multicloud. Parmi les services cloud publics, citons, d'une part, AWS, Microsoft Azure, Google Cloud Platform et autres services proposés par des fournisseurs tiers. Les clouds privés, d'autre part, limitent l'accès à certaines entreprises. Les services et les infrastructures sont maintenus sur un réseau privé, pour offrir une sécurité et un contrôle accrus par rapport aux cloud publics.

# Différentes piles
# **pour différentes tâches**

**Pourquoi les entreprises utilisent plusieurs cloud publics**


**AWS pour le développement**
Microservices
Conteneurs
EC2, VM, stockage

**GCP pour les services internes**
G Suite, Workday, Salesforce

**Azure pour Lift and Shift**
Réduction des coûts
Récupération en cas de sinistre

# Comprendre les **environnements multicloud**

Il est également intéressant de définir les termes « cloud hybride » et « multicloud ». Une solution cloud hybride permet à une entreprise d'utiliser une combinaison d'infrastructure locale, en cloud public et en cloud privé, tandis que le multicloud désigne une pratique consistant à utiliser différents fournisseurs cloud pour plusieurs déploiements du même type (pour utiliser les clouds publics de différents fournisseurs par exemple). Chaque équipe a des besoins spécifiques et va donc choisir le fournisseur qui satisfait le plus ses critères.

## Quelle est la différence ?

| Multicloud | Cloud hybride |
|---|---|
| Les applicatifs peuvent être délégués à des plateformes cloud sans interopérabilité entre les fournisseurs | Applicatifs distribués sur de multiples environnements cloud et locaux, environnement hautement portable et interchangeable. |
| **Exemple :** deux clouds publics, AWS et Azure | **Exemple :** un cloud public ET une infrastructure de datacenter locale maintenue par le client |

## Pourquoi les entreprises adoptent-elle une approche multicloud ?

**Optimisation des performances :** en cas de défaillance ou de problèmes de performance sur un cloud primaire, un cloud passif peut servir de solution de secours. Cette stratégie a pour effet de réduire les interruptions, voire de les éliminer, jusqu'au rétablissement du cloud principal.

**Réduction des coûts :** la fiabilité accrue combinée à l'optimisation des performances permet à l'entreprise de réaliser des économies. Dans une banque, une interruption de service entraîne des pertes de revenus ; dans un hôpital, cela met également des vies en danger. Quel que soit le scénario, maintenir le bon fonctionnement des réseaux est indispensable pour le succès à long terme de toute entreprise.

**Flexibilité :** une approche multicloud permet à une entreprise de conserver une certaine liberté vis-à-vis des fournisseurs en évitant de dépendre exclusivement de l'infrastructure et des services d'un prestataire ; elle échappe ainsi également à des frais importants et à des contraintes significatives en cas de changement de fournisseur. Faire appel à une multiplicité de fournisseurs permet également d'optimiser les performances en choisissant une combinaison de services répondant spécifiquement à ses besoins. Une entreprise utilisera par exemple les outils Microsoft pour un scénario d'utilisation, puis Google ou AWS pour d'autres (infrastructure et développement par exemple).

**Fiabilité accrue**

**Optimisation des performances**

**Économies**

**Indépendance vis-à-vis des fournisseurs**

**Évolutivité**

# Défis clés des **environnements multicloud**

Si la stratégie multicloud offre de nombreux avantages, elle présente également des défis non négligeables. Les fonctionnalités qui permettent de gagner en flexibilité et en fiabilité sont aussi celles qui créent des risques de sécurité supplémentaires et des défis IT.

Toutes les difficultés rencontrées par les équipes IT avec le cloud computing sont amplifiées dans les environnements multicloud, où il est encore plus délicat d'identifier, investiguer et résoudre les problèmes critiques ; la multiplication des services augmente la complexité et les systèmes en silos empêchent la mise en place d'une supervision véritablement holistique.

Sur le plan de la sécurité, de récentes études mettent en évidence un lien entre le nombre de services cloud utilisés et la probabilité d'une attaque. Une étude de 2019 menée par Nominet a découvert que 52 % des environnements multicloud avaient subi des violations au cours de l'année écoulée, contre 24 % des infrastructures hybrides et 24 % des systèmes à cloud unique. Les environnements multicloud sont également plus susceptibles de subir des failles à répétition : 69 % des entreprises utilisant cette approche signalent 11 à 30 failles, tandis que seulement 19 % des entreprises exploitant un cloud unique et 13 % des entreprises utilisatrices de systèmes hybrides rapportent de tels chiffres.

# Les difficultés présentées par les environnements multicloud affectent les équipes IT et de sécurité de différentes manières.

**La multiplication des systèmes crée des silos :** une approche multicloud peut améliorer la sécurité et la fiabilité des systèmes parce que les services sont distribués sur plusieurs solutions cloud. Mais elle peut également générer des risques en empêchant les entreprises d'avoir facilement une bonne visibilité sur l'ensemble de leurs hôtes et services.

Parce qu'elles utilisent différentes solutions cloud ayant chacune leurs propres outils de supervision et de sécurité, les équipes IT ne peuvent pas avoir une image globale de l'intégralité de la pile et déterminer si une dégradation ou une interruption est due à un service particulier, ou si le système fonctionne comme prévu.

Les fondements traditionnels de la cybersécurité ne s'appliquent pas nécessairement aux environnements multicloud. Une entreprise peut utiliser plusieurs solutions pour superviser ses services cloud, mais cette méthodologie ralentit les équipes et provoque des retards coûteux en cas de problème urgent.

**Augmentation du temps moyen de résolution (MTTR) :** rassembler des informations sur une interruption de service ou une faille à l'échelle d'un système multicloud peut s'avérer très complexe pour les équipes IT et de sécurité, et avoir un coût important pour l'entreprise en termes de temps, d'argent, de satisfaction des clients et de confiance.

En raison de la visibilité réduite sur la pile, les équipes passent beaucoup plus de temps à déterminer où et pourquoi une panne se produit, parce qu'elles doivent basculer entre différents systèmes de supervision pour corréler et analyser les données d'événement afin d'obtenir une compréhension complète du problème. Chaque minute compte en cas d'interruption de service ou d'attaque malveillante, et la complexité ajoutée par un environnement multicloud exerce un impact direct sur les revenus.

**Gouvernance des données, conformité et vulnérabilité de l'infrastructure :** de plus, du fait du manque de visibilité sur les différentes piles, il devient plus difficile de satisfaire les obligations de conformité et de repousser les pirates qui parviennent plus aisément à détecter et à exploiter les vulnérabilités dans l'infrastructure distribuée de l'entreprise. En bref, chaque service cloud supplémentaire augmente le nombre de points d'accès à un réseau.

Les problèmes de visibilité génèrent également des problèmes de gouvernance et de conformité. Une multiplicité de clouds apporte un supplément de flexibilité mais crée aussi des défis réglementaires. Par exemple, une entreprise peut accidentellement exécuter une application dans un environnement non agréé et enfreindre le règlement général sur la protection des données (RGPD). La violation de ces directives et d'autres expose à des amendes importantes.

# Effectuer une supervision à l'aide **d'outils cloud différents crée :**

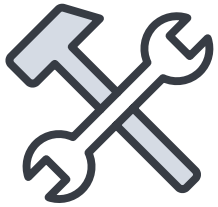
- **des vues en silos ;**
- **des équipes en silos ;**
- **des données en silos.**

## Les équipes parviennent difficilement à identifier, à investiguer et à résoudre les problèmes critiques dans le cloud.

### Manque de visibilité

Impossibilité de savoir si une dégradation ou une interruption de service est liée aux services cloud

### Un arsenal d'outils complexe



L'utilisation de multiples services cloud empêche de mettre en place une stratégie de supervision unifiée

### Un MTTR médiocre

Trop de temps perdu à déterminer où et pourquoi une interruption de service se produit

### Une évolution difficile

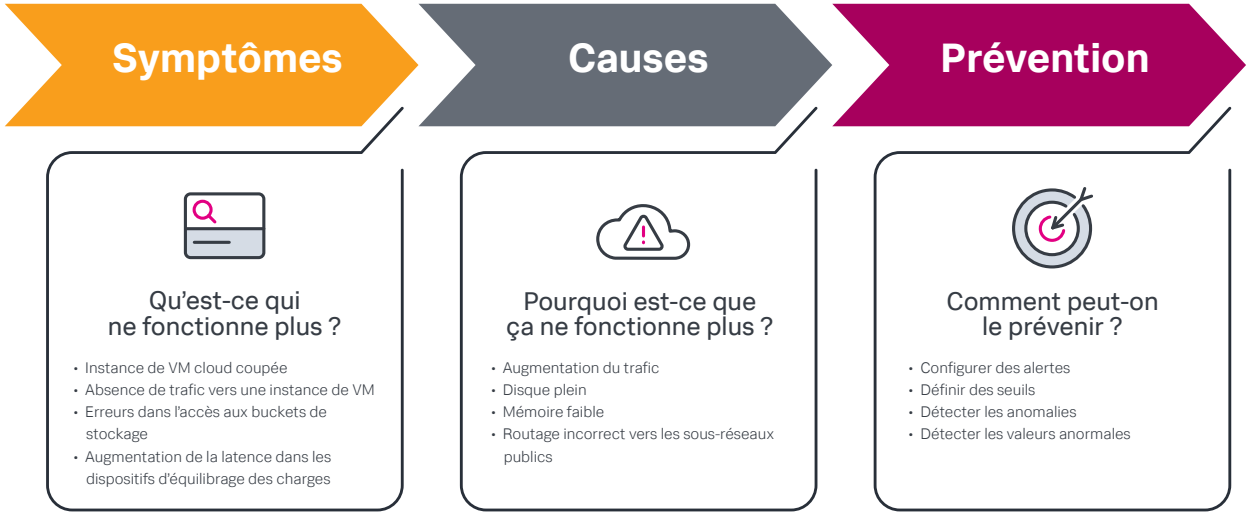
Difficulté à collecter des données sur des environnements multicloud combinant différents comptes et répartis sur plusieurs régions

# Comment aborder la **supervision du cloud**

Comment une entreprise peut-elle relever ces défis ? Les infrastructures cloud augmentent en taille et en complexité, et il devient crucial pour les entreprises de mettre en place des solutions et des stratégies de supervision complètes, capables de répondre aux besoins du multicloud et d'en relever les défis.

Face à la complexité croissante des infrastructures IT modernes, il est désormais essentiel de mettre en œuvre une méthode centralisée de supervision et de résolution des problèmes, couvrant les environnements multicloud. Sans une solution adaptée, l'entreprise d'aujourd'hui aura plus de difficultés à observer et à exploiter les données requises pour prévenir et gérer correctement les interruptions de service et les incidents.
Les entreprises qui investissent dans des outils IT et DevOps modernes peuvent créer des expériences clients positives et maximiser leurs capacités d'innovation et leurs revenus.

## Une voie pour alléger le fardeau de la supervision



# Splunk Infrastructure **Investigation and Monitoring**

Les outils cloud s'accompagnent souvent de leurs propres outils et services de supervision et de dépannage. Mais la transformation des entreprises exige une solution qui fonctionne sur plusieurs clouds et services en temps réel pour offrir une vision globale de la situation et une plateforme centrale pour passer à l'action.

C'est là qu'intervient Splunk Infrastructure Investigation and Monitoring (IIM). Elle offre une solution de supervision unifiée de l'infrastructure IT, pour remplacer la multitude d'outils de supervision et de dépannage. Employer des outils différents pour la supervision et la résolution des problèmes ajoute une complexité inutile et ralentit les équipes face aux problèmes critiques. Rassembler les deux fonctions dans une même solution peut considérablement simplifier les processus et alléger la pression sur les ressources. Cette approche réduit également les frictions dans l'obtention des données en permettant leur collecte auprès de plusieurs fournisseurs cloud, et en les mobilisant au sein d'une même vue. Cela donne aux entreprises les moyens d'assurer le suivi de leurs opérations, de leur sécurité et de leurs coûts sur l'ensemble de leurs environnements cloud, en temps réel.

Splunk y parvient en effectuant une supervision en temps réel de toute la pile cloud qui offre visibilité et contrôle en exploitant les données de toutes les sources, quelle que soit l'échelle, ainsi que des analyses basées sur l'IA en temps réel. Bénéficiez d'une meilleure compréhension de votre infrastructure cloud, de MTTD et MTTR réduits, et de la flexibilité à grande échelle requise pour appuyer la croissance de l'entreprise dans toutes les étapes de son parcours cloud.

## Découvrez comment.

La supervision des environnements multicloud peut être un défi, mais les entreprises n'ont pas besoin d'un arsenal complet d'outils pour suivre ce qui se passe dans leur infrastructure cloud.

Testez les capacités d'investigation et de supervision de l'infrastructure de Splunk. Inscrivez-vous pour essayer gratuitement **Splunk Infrastructure Monitoring**.

Vous pouvez également contacter **le service commercial** pour découvrir comment accélérer et optimiser vos initiatives multicloud avec un maximum d'efficacité.



20-13200-SPLK-FastTrackYourMulticloudMonitoringInitiative-117-EB

splunk> turn data into doing™