Sécurité à l'échelle : gouvernance dans AWS

Analyse des fonctions AWS susceptibles d'alléger les défis sur site

Octobre 2015

(Veuillez consulter https://aws.amazon.com/compliance/aws-whitepapers/ pour obtenir la dernière version de ce document)

Table des matières

Résumé

Vous pouvez exécuter dans AWS pratiquement tout ce que vous exécuteriez sur site : sites Web, applications, bases de données, applications mobiles, campagnes d'e-mail, analyse de données distribuées, stockage de média et réseaux privés. Les services fournis par AWS sont conçus pour fonctionner ensemble afin que vous puissiez créer des solutions complètes. Un autre avantage souvent négligé de la migration des charges de travail vers AWS réside dans la capacité à atteindre un niveau de sécurité plus élevé, à l'échelle, en utilisant les nombreuses fonctions permettant la gouvernance qui sont disponibles. Pour les mêmes raisons que la fourniture de l'infrastructure dans le cloud offre des avantages par rapport à sa fourniture sur site, la gouvernance basée sur le cloud propose des frais d'entrée réduits, des opérations plus aisées et une meilleure agilité grâce à une vision, un contrôle de sécurité et une automatisation centrale accrus. Ce document décrit comment atteindre un niveau élevé de gouvernance de vos ressources informatiques à l'aide d'AWS. Conjointement avec le livre blanc AWS sur les risques et la conformité et le livre blanc de la liste de contrôles d'audit de sécurité, ce document vous aide à comprendre les fonctions de sécurité et de gouvernance qui régissent les services AWS en vue d'incorporer des atouts de la sécurité et des bonnes pratiques dans la conception de votre environnement intégré à AWS.

Introduction

L'industrie et les organismes de réglementation ont créé un ensemble complexe de lois et de règlements nouveaux et hérités qui impose un grand nombre de mesures de sécurité et de gouvernance des organisations. Dès lors, des firmes de recherche estiment que de nombreuses sociétés consacrent jusqu'à 75 % de leur budget informatique à la gestion de l'infrastructure contre 25 % seulement pour des aspects informatiques directement liés à l'activité de la société. Un des éléments clés pour améliorer ce rapport consiste à répondre efficacement aux principaux besoins de gouvernance informatique. Un moyen facile et efficace d'y parvenir consiste à exploiter les fonctions de gouvernance prêtes à l'emploi d'AWS.

Au vu de l'étendue de l'offre AWS en termes de fonctions de gouvernance informatique, il peut s'avérer difficile de détermine par où commencer et quoi mettre en œuvre. Ce document présente les domaines de gouvernance informatique courants à l'aide de cas d'utilisation (ou de défi sur site), les fonctions AWS et les propositions de valeur de gouvernance associées pour utiliser ces fonctions. Ce document est conçu pour vous aider à réaliser les objectifs de chaque domaine de gouvernance informatique[1].

Ce livre s'inspire de l'approche des principaux domaines des cadres de travail de gouvernance informatique communément mis en œuvre (tels que CoBIT, ITIL, COSO, CMMI, etc.) ; cependant, les domaines de gouvernance informatique sur lesquels s'articule ce livre sont génériques, ce qui permet à chaque client de l'utiliser pour comparer les fonctions de gouvernance d'AWS avec ce qui peut être obtenu à l'aide de vos ressources et outils sur site. Les domaines de gouvernance informatique suivants sont décrits à l'aide d'une approche de « cas d'utilisation » :

[1] Bien que la liste des fonctions permettant la gouvernance présentée dans ce document soit longue, elle n'inclut pas toutes les fonctions disponibles, car nous en développons constamment des nouvelles. Des didacticiels, outils de développement et documentations supplémentaires sont disponibles à la page http://aws.amazon.com/resources/.

Je souhaite améliorer la...

Gestion des ressources informatiques

Gestion des biens informatiques

L'identification et la gestion de vos ressources informatiques constitue la première étape d'une gouvernance efficace de l'informatique. Les ressources informatiques peuvent inclure des routeurs haut de gamme, commutateurs, serveurs, hôtes et pare-feux vers les applications, mais aussi des services, systèmes d'exploitation et autres ressources logicielles déployées dans votre réseau. Une mise à jour de l'inventaire des ressources matérielles et logicielles est vitale pour les prises de décision relatives aux mises à niveau et aux achats, le suivi des garanties, le dépannage et la sécurité. D'un point de vue professionnel, il devient impératif de disposer d'un inventaire précis des ressources pour pouvoir fournir des rapports détaillés et des vues à la demande. Des inventaires de ressources détaillés sont parfois aussi spécifiquement requis par certaines réglementations relatives à la conformité. FISMA, SOX, PCI DSS et HIPAA, par exemple, incluent tous dans leurs exigences des inventaires de ressources précis. Cependant, la nature même des ressources sur site reconstituées peut rendre le maintien à jour d'une telle liste difficile, voire impossible dans le pire des cas. Les organisations doivent souvent utiliser des solutions tierces pour automatiser la création de listes d'inventaire des ressources et même dans ce cas, il n'est pas toujours possible d'obtenir un inventaire détaillé de chaque type de ressource présent sur une seule console.

AWS met à votre disposition de nombreuses fonctions pour obtenir rapidement et facilement un inventaire précis de vos ressources informatiques AWS. Ces fonctions, associées à des conseils de type « procédure » et des liens pour en savoir plus sur ces fonctions sont énumérés ci-après :

Fonction AWS permettant la gouvernance	Comment la sécurité à l'échelle est-elle obtenue
Page d'activité du compte	Fournit une liste résumée des ressources informatiques en détaillant l'utilisation de chaque service par région. En savoir plus.
Inventaire du coffre Amazon Glacier	Fournit un inventaire des données Glacier qui répertorie toutes les ressources informatiques dans Glacier. En savoir plus.
AWS CloudHSM	Assure le contrôle virtuel et physique des clés de chiffrement en fournissant des HSM dédiés au client pour le stockage des clés. En savoir plus.
Exécuteur de tâches AWS Data Pipeline	Assure le traitement automatisé des tâches en interrogeant AWS Data Pipeline au sujet des tâches, puis en exécutant et en créant des rapports d'état sur ces tâches. En savoir plus.
AWS Management Console	Fournit un inventaire en temps réel des ressources et des données, en répertoriant toutes les ressources informatiques utilisées dans AWS, par service. En savoir plus.
API AWS Storage Gateway	Permet de créer par programmation des inventaires de ressources et de données en programmant des interfaces, des outils et des scripts pour gérer des ressources. En savoir plus.

Contrôle des coûts informatiques

La compréhension du coût de vos services informatiques vous permet de mieux contrôler vos frais informatiques et d'acquérir des ressources de la manière la plus rentable possible. Cependant, la gestion et le suivi des coûts et du retour sur investissement liés aux dépenses en ressources informatiques sur site peuvent s'avérer difficiles et imprécis en raison de la complexité des calculs ; planification de capacité, prévisions d'utilisation, coûts d'achat, amortissement, coût du capital et coût des installations comptent parmi les éléments qui compliquent le calcul du coût total de possession.

AWS met à votre disposition plusieurs fonctions pour comprendre et contrôler facilement et avec précision les coûts de vos ressources informatiques. Grâce à AWS, vous pouvez réaliser des économies de coût allant jusqu'à 80 % par rapport à des déploiements équivalents sur site[2]. Ces fonctions, associées à des conseils de type « procédure » et des liens pour en savoir plus sur ces fonctions sont énumérés ci-après :

Fonction AWS permettant la gouvernance	Comment la sécurité à l'échelle est-elle obtenue
Page d'activité du compte	Fournit un aperçu à tout moment des dépenses en ressources informatiques, en répertoriant les ressources utilisées par service. En savoir plus.
Lancement d'instance idempotente Amazon EC2	Contribue à empêcher le lancement erroné de ressources et la génération de frais supplémentaires en évitant que des instances supplémentaires soient lancées par des délais d'attente ou des erreurs de connexion. En savoir plus.
Balisage des ressources Amazon EC2	Fournit une association entre des dépenses de ressources et des unités d'activité en appliquant des intitulés personnalisés détectables à des ressources de calcul. En savoir plus.
Facturation de compte AWS	Fournit des fonctions de facturation simples pour vous aider à surveiller et à payer vos factures en détaillant les ressources utilisées et les frais de calcul réel associés encourus. En savoir plus.
AWS Management Console	Fournit une vue de type « guichet unique » des facteurs de coût, en répertoriant toutes les ressources informatiques utilisées dans AWS par service, y compris les coûts réels et les projections. En savoir plus.
Tarification des services AWS	Sensibilise irrévocablement le client sur le prix des ressources informatiques d'AWS en mentionnant la tarification de chaque produit AWS et les caractéristiques de tarification spécifiques. En savoir plus.
AWS Trusted Advisor	Favorise l'optimisation du coût des ressources informatiques en identifiant les ressources inutilisées et inactives. En savoir plus.
Alarmes de facturation	Fournit des alertes proactives à propos des dépenses en ressources informatiques en envoyant des notifications sur l'activité de dépense. En savoir plus.
Facturation consolidée	Assure le contrôle centralisé des coûts et la visibilité des coûts entre comptes en regroupant plusieurs comptes AWS sur une seule facture. En savoir plus.

[2] Consultez le livre blanc sur le coût total d'appartenance pour en savoir plus sur les économies de coût globales à réaliser avec AWS

Tarification à l'utilisation	Fournit des services et des ressources de calcul pour créer en quelques minutes des applications en tarification à l'utilisation sans frais d'achat initial ou frais de maintenance réguliers, en dimensionnant automatiquement plusieurs serveurs en cas d'augmentation de la demande pour votre application. En savoir plus.

Gestion de la sécurité informatique

Contrôle de l'accès physique aux ressources informatiques

La gestion de l'accès physique est un élément clé des programmes de gouvernance informatique. Outre les verrous, alarmes de sécurité, contrôles d'accès et vidéos de surveillance qui constituent les éléments de sécurité physique traditionnels, les contrôles électroniques de l'accès physique sont également essentiels pour assurer une sécurité physique efficace. L'industrie de la sécurité physique traditionnelle évolue rapidement et les domaines de spécialisation qui émergent rendent la sécurité physique extrêmement plus complexe. Les aspects et les contrôles de la sécurité physique sur site deviennent plus complexes. Nous avons donc besoin d'un nombre accru de professionnels spécialisés et spécifiquement qualifiés en sécurité informatique pour gérer l'effort significatif que nécessite le contrôle physique efficace des informations d'identification d'accès aux cartes/lecteurs de carte, contrôleurs et serveurs système qui hébergent les données relatives à la sécurité physique.

AWS vous permet de confier facilement et efficacement les contrôles de la sécurité physique de votre infrastructure AWS à des spécialistes AWS disposant des compétences et des ressources nécessaires pour sécuriser l'environnement physique. AWS fait appel à plusieurs auditeurs indépendants différents pour valider la sécurité physique des centres de données au cours de l'année ; ces auditeurs certifient la conception et testent en profondeur l'efficacité de nos contrôles de sécurité physique. Pour en savoir plus sur les programmes d'audit AWS et les contrôles de sécurité physique associés, consultez les références ci-dessous :

Fonction AWS permettant la gouvernance	Comment la sécurité à l'échelle est-elle obtenue
Contrôles d'accès physique AWS SOC 1	Assure des contrôles transparents aux endroits interdisant l'accès non autorisé aux centres de données. Les contrôles sont conçus, testés et analysés adéquatement par une firme d'audit indépendante. En savoir plus.
Contrôles d'accès physique AWS SOC 2-Security	Assure des contrôles transparents aux endroits interdisant l'accès non autorisé aux centres de données. Les contrôles sont conçus, testés et analysés adéquatement par une firme d'audit indépendante. En savoir plus.
Contrôles d'accès physique AWS PCI DSS	Assure des contrôles transparents aux endroits interdisant l'accès non autorisé aux centres de données, en accord avec la norme de sécurité des données (Data Security Standard ou DSS) dans le secteur des cartes de paiement (PCI, Payment Card Industry). Les contrôles sont conçus, testés et analysés adéquatement par une firme d'audit indépendante. En savoir plus.

Contrôles d'accès physique AWS ISO 27001	Assure des contrôles et des processus transparents aux endroits interdisant l'accès non autorisé aux centres de données, en accord avec la norme ISO 27002 relative aux bonnes pratiques de sécurité. Les contrôles sont conçus, testés et analysés adéquatement par une firme d'audit indépendante. En savoir plus.
Contrôles d'accès physique AWS FedRAMP	Assure des contrôles et des processus transparents aux endroits interdisant l'accès non autorisé aux centres de données, en accord avec la norme NIST 800- 53 relative aux bonnes pratiques. Les contrôles sont conçus, testés et analysés adéquatement par une firme d'audit indépendante et accréditée auprès du gouvernement. En savoir plus.

Contrôle de l'accès logique aux ressources informatiques

Un des principaux objectifs de la gouvernance informatique consiste à gérer efficacement l'accès logique aux systèmes informatiques et aux données. De nombreuses organisations peinent néanmoins à dimensionner leurs solutions sur site pour faire face à la croissance et à l'évolution constante du nombre de considérations et de complexités relatives à l'accès logique, y compris la capacité à établir une règle du moindre privilège, gérer les autorisations aux ressources et faire face aux changements de rôles, aux besoins d'informations et à la multiplication des données sensibles. Les principaux défis persistants de la gestion de l'accès logique dans un environnement sur site consistent à fournir aux utilisateurs un accès basé sur :

- le rôle (utilisateurs internes, sous-traitants, personnes extérieures, partenaires, etc.)
- la classification des données (confidentielles, à usage interne uniquement, privées, publiques, etc.)
- le type de données (informations d'identification, données personnelles, données de contact, données professionnelles, certificats numériques, mots de passe cognitifs, etc.)

AWS propose de nombreuses fonctions de contrôle pour gérer efficacement votre accès logique s'articulant sur une matrice de cas d'utilisation basés sur le moindre privilège. Ces fonctions, associées à des conseils de type « procédure » et des liens pour en savoir plus sur ces fonctions sont énumérés ci-après :

Fonction AWS permettant la gouvernance	Comment la sécurité à l'échelle est-elle obtenue
Listes de contrôle d'accès (ACL) Amazon S3	Fournit des autorisations centrales et des conditions en ajoutant des conditions particulières pour contrôler la manière dont un utilisateur peut utiliser AWS, notamment l'heure du jour, l'adresse IP d'origine, l'utilisation ou non de SSL, l'emploi ou non d'un dispositif d'authentification multi-facteurs pour authentifier l'utilisateur. En savoir plus ici et ici.
Stratégies de compartiment Amazon S3	Permet de créer des règles conditionnelles pour gérer l'accès aux compartiments et aux objets en vous autorisant à restreindre l'accès sur base du compte ainsi que des attributs sur demande tels que le référent HTTP et l'adresse IP. En savoir plus.

Authentification par chaîne d'interrogation Amazon S3	Permet de donner l'accès HTTP ou par navigateur à des ressources qui nécessitent en principe une authentification par signature dans la chaîne d'interrogation pour sécuriser la requête. En savoir plus.
AWS CloudTrail	Permet de journaliser des actions de console ou API (modification d'une stratégie de compartiment, arrêt d'une instance, etc.), ce qui favorise la supervision avancée. En savoir plus.
AWS IAM Multi-Factor Authentication (MFA)	Renforce MFA dans toutes les ressources en exigeant un token pour la connexion et l'accès aux ressources. En savoir plus.
Stratégie de mot de passe AWS IAM	Pour gérer la qualité et les contrôles des mots de passe de vos utilisateurs, vous pouvez définir une stratégie applicable aux mots de passe employés par des utilisateurs IAM dans laquelle vous spécifiez que les mots de passe doivent avoir une longueur déterminée, doivent inclure certains caractères, etc. En savoir plus.
Autorisations AWS IAM	Facilite la gestion des autorisations en vous permettant de spécifier qui peut accéder aux ressources AWS et quelles actions peuvent être effectuées dans ces ressources. En savoir plus.
Stratégies AWS IAM	Assure la gestion détaillée de l'accès avec les privilèges les plus faibles en vous permettant de créer plusieurs utilisateurs à l'intérieur de votre compte AWS, de leur affecter des informations d'identification de sécurité et de gérer leurs autorisations. En savoir plus.
Rôles AWS IAM	Permet de déléguer temporairement l'accès à des utilisateurs ou des services qui n'ont en principe pas accès à vos ressources AWS en définissant un ensemble d'autorisations pour accéder aux ressources dont un utilisateur ou un service a besoin. En savoir plus.
AWS Trusted Advisor	Permet d'évaluer la gestion de la sécurité de manière automatisée en identifiant et en remontant des éventuels problèmes de sécurité et d'autorisation. En savoir plus.

Sécurisation des ressources informatiques

La sécurisation des ressources informatiques est la pièce maîtresse des programmes de gouvernance informatique. Cependant, dans les environnements sur site, la mise en ligne d'un nouveau serveur nécessite la mise en œuvre d'une panoplie de mesures de sécurité. Il faut notamment mettre à jour les stratégies de pare-feu et de contrôle d'accès, vérifier si l'image du nouveau serveur créé est conforme à la stratégie de sécurité et actualiser tous les packages logiciels. À moins que ces tâches de sécurité soient automatisées et réalisées en tenant compte des besoins ultra-dynamiques de l'activité, les organisations qui utilisent exclusivement des approches de gouvernance traditionnelles risquent de voir des utilisateurs confrontés à des problèmes de contrôle de sécurité ou d'accuser des retards d'activité onéreux.

AWS fournit de nombreuses fonctions de sécurité pour sécuriser facilement et efficacement vos ressources informatiques. Ces fonctions, associées à des conseils de type « procédure » et des liens pour en savoir plus sur ces fonctions sont énumérés ci-après :

Fonction AWS permettant la gouvernance	Comment la sécurité à l'échelle est-elle obtenue
AMI Amazon Linux	Permet de déployer de manière cohérente une image « dorée » (renforcée) en développant une image privée à utiliser dans tous les déploiements d'instance. En savoir plus.
Instances dédiées Amazon EC2	Fournit un réseau virtuel privé et isolé et garantit que vos instances de calcul Amazon EC2 sont isolées au niveau matériel et lancées au sein d'un VPC. En savoir plus.
Assistant de lancement d'instance Amazon EC2	Permet un processus de lancement régulier en imposant des restrictions sur des images de machine disponibles au lancement des instances. En savoir plus.
Groupes de sécurité Amazon EC2	Assure un contrôle précis des trafics entrants et sortants en agissant comme un pare-feu qui contrôle le trafic pour une ou plusieurs instances. En savoir plus.
Archives Amazon Glacier	Fournit un service de stockage à long terme à coût réduit, sécurisé, durable et optimisé pour l'archivage et la sauvegarde des données en utilisant le chiffrement AES 256 bits par défaut. En savoir plus.
Chiffrement côté client Amazon S3	Permet de chiffrer vos données avant de les envoyer à Amazon S3 en créant votre propre bibliothèque pour chiffrer les données de vos objets sur le côté client avant leur téléchargement vers Amazon S3. AWS SDK pour Java peut aussi chiffrer automatiquement vos données avant de les télécharger vers Amazon S3. En savoir plus.
Chiffrement côté serveur Amazon S3	Assure le chiffrement des objets au repos et des clés gérées par AWS en utilisant le chiffrement AES 256 bits pour les données Amazon S3. En savoir plus.

Amazon VPC	Fournit un réseau virtuel ressemblant étroitement à un réseau traditionnel en service sur site, mais qui utilise avantageusement l'infrastructure évolutive d'AWS. Il vous est possible de créer des sections d'AWS isolées logiquement au sein desquelles vous pouvez lancer des ressources AWS dans un réseau virtuel que vous définissez. En savoir plus.
Isolation logique Amazon VPC	Assure l'isolation virtuelle des ressources en permettant d'isoler des images de machine des autres ressources mises en réseau. En savoir plus.
ACL réseau Amazon VPC	Assure l'isolation « de type pare-feu » des sous-réseaux associés en contrôlant les trafics entrants et sortants au niveau du sous-réseau. En savoir plus.
Adresses IP privées Amazon VPC	Contribue à protéger des adresses IP privées contre l'exposition à Internet en acheminant leur trafic via une instance NAT (Network Address Translation) dans un sous-réseau public. En savoir plus.
Groupes de sécurité Amazon VPC	Assure l'isolation « de type pare-feu » des instances Amazon EC2 associées en contrôlant les trafics entrants et sortants au niveau de l'instance. En savoir plus.
Modèles AWS CloudFormation	Permet de déployer de manière régulière l'image d'une machine particulière avec d'autres ressources et configurations en mettant l'infrastructure en service avec des scripts. En savoir plus.
AWS Direct Connect	Élimine la nécessité d'utiliser une connexion Internet publique à AWS en établissant une connexion réseau dédiée entre vos installations et le centre de données AWS. En savoir plus.
Connexions VPN Hardware/Software sur site	Assure un contrôle précis de la sécurité du réseau en autorisant des connexions sécurisées entre le réseau existant et AWS. En savoir plus.
Passerelles privées virtuelles	Assure un contrôle précis de la sécurité du réseau en fournissant un moyen de créer une connexion VPN Hardware à votre VPC. En savoir plus.

Gestion de la journalisation des ressources informatiques

La journalisation des ressources informatiques est un catalyseur clé pour la sécurité informatique. La journalisation est particulièrement importante pour la gouvernance informatique pour une variété de cas d'utilisation, y compris mais sans y être limité : la détection/le suivi de comportement suspect, la prise en charge d'analyses légales, le respect des exigences de conformité, l'assistance informatique/mise en réseau de la maintenance et des opérations, la gestion/réduction des frais de sécurité informatique, la supervision des niveaux de service ainsi que la prise en charge de processus d'activité internes. Les organisations dépendent toujours plus de la gestion efficace des journaux pour soutenir des fonctions de gouvernance clé telles que la gestion des coûts, la supervision d'application au niveau du service et du secteur d'activité ainsi que d'autres activités liées à la conformité et la sécurité informatique. SANS Log Management Survey révèle constamment que les organisations cherchent continuellement à exploiter davantage leurs journaux, mais se heurtent à des frictions lorsque des cas d'utilisation doivent collecter et analyser ces journaux en utilisant des ressources sur site. Avec la multiplication des types de journaux destinés à collecter et à analyser des données provenant de différentes ressources informatiques, les organisations doivent faire face à une surcharge manuelle liée à la normalisation des données de journal, disponibles dans de nombreux formats différents, ainsi qu'aux fonctionnalités de recherche, de corrélation et de création de rapports. La gestion des journaux est essentielle pour la supervision de la sécurité, la conformité et la prise de décision efficace concernant des dizaines, voire des centaines ou des milliers d'activités exécutées chaque jour.

AWS propose plusieurs fonctions de journalisation pour consigner et suivre efficacement l'utilisation de votre ressources informatiques. Ces fonctions, associées à des conseils de type « procédure » et des liens pour en savoir plus sur ces fonctions sont énumérés ci-après :

Fonction AWS permettant la gouvernance	Comment la sécurité à l'échelle est-elle obtenue
Journaux d'accès Amazon CloudFront	Fournit des fichiers journaux contenant des informations relatives à l'accès de l'utilisateur final à vos objets. Des journaux peuvent être distribués directement à un compartiment Amazon S3 spécifique. En savoir plus.
Journaux de base de données Amazon RDS	Fournit un moyen de surveiller un certain nombre de fichiers journaux générés par vos instances DB Amazon RDS. Ils sont utilisés pour diagnostiquer, dépanner et résoudre des problèmes de performance et de configuration de base de données. En savoir plus.
Expiration d'objet Amazon S3	Assure l'expiration automatisée des journaux en programmant la suppression d'objets après une période de temps définie. En savoir plus.
Journaux d'accès du serveur Amazon S3	Fournit des journaux de demandes d'accès contenant des détails relatifs aux demandes, tels que le type de demande, la ressource avec laquelle la demande a été effectuée ainsi que l'heure et la date de traitement de la demande. En savoir plus.
AWS CloudTrail	Fournit des journaux sur les actions de sécurité effectuées via AWS Management Console ou des API. En savoir plus.

Gestion des performances informatiques

Supervision et réponse aux événements

La gestion et la supervision des performances informatiques sont devenues des composantes stratégiques importantes de tout programme de gouvernance informatique. La supervision informatique est un élément essentiel de la gouvernance qui vous permet d'éviter, détecter et corriger des problèmes informatiques susceptibles d'influencer des performances et/ou la sécurité. Le principal défi de la gouvernance en termes de gestion des performances informatiques dans les environnements sur site est la mise à disposition de multiples systèmes de supervision pour gérer chaque couche de vos ressources informatiques. Ce mélange d'outils de gestion propriétaire et de processus informatiques engendre un niveau de complexité systémique tel que dans le meilleur des cas il ralentit les temps de réponse, mais dans le pire des cas, il altère l'efficacité de la gestion et de la supervision de vos performances informatiques. De plus, l'augmentation de la complexité et de la sophistication des menaces de sécurité implique que les capacités de réaction et de supervision d'événements doivent évoluer constamment et rapidement afin de résoudre les menaces émergentes. Dès lors, la gestion des performances sur site est continuellement confrontée à des défis grandissants en termes d'acquisition d'infrastructure, d'évolutivité, de capacité à simuler des conditions de test entre plusieurs zones géographiques, etc.

AWS propose de nombreuses fonctions de supervision pour surveiller et gérer facilement et efficacement vos ressources informatiques. Ces fonctions, associées à des conseils de type « procédure » et des liens pour en savoir plus sur ces fonctions sont énumérés ci-après :

Fonction AWS permettant la gouvernance	Comment la sécurité à l'échelle est-elle obtenue
Amazon CloudWatch	Fournit des données statistiques pour consulter, analyser et définir des alarmes relatives au comportement opérationnel de vos instances. Ces mesures incluent l'utilisation des UC, le trafic réseau, les E/S et la latence. En savoir plus.
Alarmes Amazon CloudWatch	Il est possible de déclencher des alarmes cohérentes pour des événements critiques via des mesures personnalisées, des alarmes et des notifications d'événement. En savoir plus.
Statut d'instance Amazon EC2	Fournit des contrôles de statut d'instance qui résument les résultats des tests automatiques et donnent des informations sur certaines activités programmées pour vos instances. Utilisez ces contrôles automatisés pour détecter si des problèmes spécifiques concernent vos instances. En savoir plus.
Équipe de gestion d'incident Amazon	La détection, la supervision et la gestion continue des incidents, 24 heures sur 24, 7 jours sur 7 pendant toute l'année sont assurées par des équipes d'opérateurs qui vous aident à détecter, diagnostiquer et résoudre certains événements de sécurité. En savoir plus.
Confirmation sélective TCP Amazon S3	Permet d'améliorer le temps de récupération après un nombre important de pertes de paquets. En savoir plus.

Amazon Simple Notification Service	Assure le déclenchement d'alarmes cohérentes pour des événements critiques et transmet les messages aux clients ou points de terminaison abonnés. En savoir plus.
AWS Elastic Beanstalk	Permet de surveiller des détails de déploiement d'application tels que la mise en service de capacité, l'équilibrage des charges, l'auto-scaling et la supervision la santé des applications. En savoir plus.
Elastic Load Balancing	Permet de répartir automatiquement votre trafic d'applications entrant entre plusieurs instances Amazon EC2 en détectant les instances qui sont surchargées et en réacheminant le trafic vers celles qui sont sous-utilisées. En savoir plus.

Obtention de la résilience

La protection des données et la planification de la reprise après sinistre doivent être des priorités de la gouvernance informatique pour toutes les organisations. La valeur de la DR n'est sans doute pas concernée, mais bien l'aptitude de l'organisation à se redresser et à reprendre son activité après un événement grave ou une catastrophe. Cependant, la mise en œuvre de la gouvernance au niveau de la résilience des ressources informatiques peut être onéreuse, complexe, fastidieuse et laborieuse. Les organisations sont confrontées à un nombre croissant d'événements susceptibles de provoquer des immobilisations imprévues ou des blocages opérationnels. Ces événements peuvent être dus à des problèmes techniques (virus, corruption de données, erreur humaine, etc.) ou à des phénomènes naturels (incendie, inondation, panne de courant, interruptions dues à la météo, etc.). Les organisations sont ainsi confrontées à une augmentation des coûts et de la complexité de la planification, des tests et de la mise en service des sites de basculement sur site à cause de la croissance continuelle des données.

Face à ces défis, la virtualisation du serveur de cloud computing rend les programmes de résilience de qualité réalisables à moindre coût. AWS propose de nombreuses fonctions pour assurer facilement et efficacement la résilience de vos ressources informatiques. Ces fonctions, associées à des conseils de type « procédure » et des liens pour en savoir plus sur ces fonctions sont énumérés ci-après :

Fonction AWS permettant la gouvernance	Comment la sécurité à l'échelle est-elle obtenue
Instantanés Amazon EBS	Fournit des volumes de stockage prévisibles à hauts niveaux de disponibilité et de fiabilité avec contrôle des sauvegardes incrémentielles à un instant donné des données du serveur. En savoir plus.
Déploiements multi-AZ Amazon RDS	Fournit un moyen de sauvegarder vos données en cas de défaillance grâce aux contrôles de disponibilité automatisés et à l'architecture résiliente homogène. En savoir plus.
AWS Import/Export	Permet de déplacer localement des quantités importantes de données en créant rapidement des tâches d'import et d'export avec le réseau interne à grande vitesse d'Amazon. En savoir plus.

AWS Storage Gateway	Assure l'intégration sûre et transparente entre votre environnement informatique sur site et l'infrastructure de stockage d'AWS via la planification d'instantanés stockés par la passerelle dans Amazon S3 sous la forme d'instantanés Amazon EBS. En savoir plus.
AWS Trusted Advisor	Assure la gestion automatisée des performances et le contrôle de disponibilité en identifiant des options permettant d'augmenter la disponibilité et la redondance de votre application AWS. En savoir plus.
Solutions tierces étendues	Permet le stockage de données sécurisé et le contrôle de disponibilité automatisé en vous connectant facilement à un marché d'applications et d'outils. En savoir plus.
Services de base de données SQL/non SQL AWS gérés	Fournit un stockage de données sécurisé et durable en répliquant automatiquement des éléments de données entre plusieurs zones de disponibilité dans une région pour assurer le haut niveau de disponibilité et la durabilité des données intégrées. En savoir plus : • Amazon Dynamo DB • Amazon RDS
Déploiement sur plusieurs régions	Assure la géo-diversité des emplacements de calcul, réseaux électriques, lignes défectueuses, etc. en fournissant une variété de lieux. En savoir plus.
Vérifications de l'état et basculement DNS avec Route 53	Surveille la disponibilité des données de sauvegarde stockées en vous permettant de configurer le basculement DNS dans des configurations actives-actives, actives-passives ou mixtes pour améliorer la disponibilité de votre application. En savoir plus.

Index des fonctions de gouvernance par service

Les informations ci-dessus sont présentées par domaine de gouvernance. À des fins de référence, le tableau suivant décrit un résumé des fonctions de gouvernance proposées par les principaux services AWS :

Service AWS	Fonction de gouvernance
Amazon EC2	Lancement d'instance idempotente Amazon EC2 Balisage des ressources Amazon EC2 AMI Amazon Linux Instances dédiées Amazon EC2 Assistant de lancement d'instance Amazon EC2 Groupes de sécurité Amazon EC2
Elastic Load Balancing	Distribution du trafic Elastic Load Balancing
Amazon VPC	Amazon VPC Isolation logique Amazon VPC ACL réseau Amazon VPC Adresses IP privées Amazon VPC Groupes de sécurité Amazon VPC Connexions VPN Hardware/Software sur site
Amazon Route 53	Jeux d'enregistrements de ressource de latence Amazon Route 53 Vérifications de l'état et basculement DNS avec Route 53
AWS Direct Connect	AWS Direct Connect
Amazon S3	Listes de contrôle d'accès (ACL) Amazon S3 Stratégies de compartiment Amazon S3 Authentification par chaîne d'interrogation Amazon S3 Chiffrement côté client Amazon S3 Chiffrement côté serveur Amazon S3 Expiration d'objet Amazon S3 Journaux d'accès du serveur Amazon S3 Confirmation sélective TCP Amazon S3 Mise à l'échelle des fenêtres TCP Amazon S3

Amazon Glacier	Inventaire du coffre Amazon Glacier Archives Amazon Glacier
Amazon EBS	Instantanés Amazon EBS
AWS Import/Export	AWS Import/Export bulk datano…
AWS Storage Gateway	Intégration AWS Storage Gateway API AWS Storage Gateway
Amazon CloudFront	Amazon CloudFront Journaux d'accès Amazon CloudFront
Amazon RDS	Journaux de base de données Amazon RDS Déploiements multi-AZ Amazon RDS Services de base de données SQL/non SQL AWS gérés
Amazon Dynamo DB	Services de base de données SQL/non SQL AWS gérés
AWS Management Console	Page d'activité du compte Facturation de compte AWS Tarification des services AWS AWS Trusted Advisor Alarmes de facturation Facturation consolidée Tarification à l'utilisation AWS CloudTrail Équipe de gestion d'incident Amazon Amazon Simple Notification Service Déploiement sur plusieurs régions

AWS Identity and Access Management (IAM)	AWS IAM Multi-Factor Authentication (MFA) Stratégie de mot de passe AWS IAM Autorisations AWS IAM Stratégies AWS IAM Rôles AWS IAM
Amazon CloudWatch	Tableau de bord AWS CloudWatch Alarmes Amazon CloudWatch
AWS Elastic Beanstalk	Supervision AWS Elastic Beanstalk
AWS CloudFormation	Modèles AWS CloudFormation
AWS Data Pipeline	Exécuteur de tâches AWS Data Pipeline
AWS CloudHSM	Stockage de clé CloudHSM
AWS Marketplace	Solutions tierces étendues
Centres de données	Contrôles d'accès physique AWS SOC 1 Contrôles d'accès physique AWS SOC 2-Security Contrôles d'accès physique AWS PCI DSS Contrôles d'accès physique AWS ISO 27001 Contrôles d'accès physique AWS FedRAMP

Conclusion

La gouvernance informatique s'articule essentiellement autour de la gestion des ressources, de la sécurité et des performances pour garantir un alignement stratégique de valeur sur les objectifs de votre activité. En raison de la croissance cadencée et de la complexité accrue de la technologie, les environnements sur site à l'échelle ont de plus en plus difficile à fournir les contrôles précis et les fonctions nécessaires à la gouvernance informatique de qualité à moindre coût. Pour les mêmes raisons que la fourniture de l'infrastructure dans le cloud offre des avantages par rapport à sa fourniture sur site, la gouvernance basée sur le cloud propose des frais d'entrée réduits, des opérations plus aisées et une meilleure agilité grâce à une vision et une automatisation accrues qui permettent aux organisations de se concentrer sur leurs activités.

Références et suggestions de lecture

Que puis-je faire avec AWS ? http://aws.amazon.com/solutions/aws-solutions/.

Comment puis-je commencer à utiliser AWS ? http://docs.aws.amazon.com/gettingstarted/latest/awsgsg-intro/gsg-aws- intro.html