Le cloisonnement logique sur AWS

S'affranchir de l'isolement physique à l'ère du cloud computing

Juillet 2020

Remarques

Il incombe aux clients de procéder à leur propre évaluation indépendante des informations contenues dans ce document. Ce document : (a) est fourni à titre informatif uniquement, (b) couvre les offres et pratiques actuelles des produits AWS qui peuvent être modifiées sans préavis, et (c) ne crée aucun engagement ou aucune garantie de la part d'AWS et de ses sociétés apparentées, fournisseurs ou concédants de licence. Les produits ou services AWS sont fournis « tels quels », sans garantie, engagement ou condition d'aucune sorte, qu'elle soit expresse ou implicite. Les responsabilités et obligations d'AWS vis-à-vis de ses clients sont régies par les contrats AWS. Le présent document ne fait partie d'aucun contrat et ne modifie aucun contrat entre AWS et ses clients.

Sommaire

Résumé

Ce document porte sur le cloisonnement logique pour les clients d’Amazon Web Services (AWS). Il présente une approche à plusieurs volets, incluant l'utilisation de la virtualisation, du chiffrement et des politiques de sécurité, pour créer des mécanismes de sécurité logiques qui égalent et souvent surpassent les performances de sécurité du cloisonnement physique et d'autres approches de sécurité traditionnellement déployées dans les datacenters privés. Les organisations commerciales et du secteur public du monde entier peuvent tirer parti de ces mécanismes pour migrer en toute confiance des applications sensibles vers le cloud sans avoir besoin d'une infrastructure physiquement dédiée.

Introduction

La technologie cloud est un levier essentiel de la transformation de l'informatique. Une technique fondamentale consiste à offrir des services mutualisés qui placent les applications et les données de plusieurs clients sur la même infrastructure physique. Cette architecture permet aux fournisseurs de services cloud comme AWS (CSP) de maximiser l'utilisation des ressources physiques, afin de proposer ces ressources à un coût moindre pour les clients. Elle permet également aux clients de mettre à jour leurs applications et de les migrer facilement et avec un minimum d'interruption vers la technologie en constante évolution du CSP. Ce choix architectural est rendu possible par le développement de contrôles de sécurité logiques puissants et flexibles qui créent des frontières d'isolement solides entre les clients. Depuis le lancement de ses premiers services cloud en 2006, AWS n'a cessé d'améliorer ses fonctions et ses contrôles, pour que les clients atteignent le niveau de sécurité requis pour répondre à leurs besoins de classification des données. Les clients constatent généralement que les CSP comme AWS leur permettent d'optimiser plus efficacement les configurations de sécurité dans le cloud que leurs solutions sur site.

Les clients qui utilisent AWS bénéficient d'un environnement physique, d'un réseau et d'une architecture logicielle conçus pour répondre aux exigences des organisations les plus sensibles à la sécurité au monde. AWS fournit des services hautement disponibles et met en œuvre une combinaison de mécanismes de sécurité traditionnels et nouveaux au cœur de la conception et du fonctionnement de ses services.

AWS offre aux clients un contrôle étendu sur leur contenu et leur fournit des outils pour déterminer où il sera stocké et comment il sera protégé. Les services AWS offrent aux clients la possibilité de sécuriser leur contenu en transit et au repos, de contrôler étroitement l'accès de leurs utilisateurs aux services et ressources AWS, et de surveiller l'accès, ainsi que l'état de leurs systèmes. Les clients d'AWS conservent le contrôle total de l'accès à leur contenu, l'architecture empêchant ainsi les utilisateurs non autorisés d'accéder aux données des clients. Tout se passe dans un cadre de services mutualisé avec isolement logique strict. L'isolement logique entre les environnements des clients, fourni par AWS peut être plus efficace et plus fiable que la sécurité observée dans une infrastructure physique dédiée.

Préoccupations conduisant à des exigences de cloisonnement physique

Les exigences relatives aux environnements physiquement dédiés sont principalement motivées par des préoccupations d'accès des tiers ou d'accès non autorisé aux systèmes, aux applications ou aux données. Beaucoup croient à tort que les environnements physiquement séparés offrent une meilleure protection que les environnements cloud multi-clients logiquement séparés contre la divulgation involontaire d'informations ou de systèmes, la falsification et l'accès non autorisé. En réalité, si l'on examine les vecteurs d'attaque les plus courants liés à l'accès non autorisé – comme l'exploitation à distance, l'erreur humaine et la menace interne –, un environnement physiquement séparé ne réduit pas le profil de risque. En réalité, pour tout système accessible par un réseau ou par Internet, le cloisonnement physique – par exemple placer les environnements dans une cage verrouillée ou dans un centre de données séparé – ne renforce pas intrinsèquement la sécurité ou le contrôle sur les formes d'accès les plus importantes.

En outre, les environnements physiquement séparés de petite taille ne peuvent être comparés aux environnements cloud disponibles à très grande échelle. Par conséquent, toute exigence de cloisonnement physique peut limiter ou retarder la capacité d'un client à tirer parti d'investissements innovants (notamment des innovations dans les fonctions de sécurité) réalisés pour tous les clients utilisant les services AWS. Parmi les inconvénients potentiels, une structure de coûts moins avantageuse, des délais de mise en conformité importants et des options et fonctions de redondance limitées par rapport à la diversité géographique des régions de centres de données commerciaux.

AWS répond aux préoccupations qui motivent les exigences de cloisonnement physique par les fonctionnalités de sécurité logique fournis aux clients par des contrôles de sécurité destinés à protéger leurs données. La force de cet isolement, combinée à l'automatisation et à la flexibilité qu'elle procure, est équivalente ou supérieure aux contrôles de sécurité des environnements traditionnels physiquement séparés.

Cloisonnement logique et cloisonnement physique

Les clients peuvent bénéficier de tout ou partie des capacités AWS ci-dessous pour satisfaire aux exigences de sécurité de leur séparation physique sur site, voire les surpasser.

- **Authentification et autorisation unifiées** – Un modèle d'authentification et d'autorisation robuste et détaillé commun à tous les services AWS qui s'intègre aux systèmes de gestion interne des identités des utilisateurs du client.
- **Surveillance et journalisation étendues** – Services de journalisation détaillés et étendus pour bénéficier d'une visibilité sur tous les appels d'API et l'état des ressources dans les services AWS. La configuration courante et les événements liés aux applications sont consignés de manière centralisée, afin de comprendre rapidement la posture de sécurité actuelle, ainsi que les états précédents de la configuration.
- **Virtual Private Cloud (VPC) et fonctions associées** – Un VPC est un réseau défini par logiciel qui permet aux clients de créer des domaines réseau segmentés ou micro-segmentés, afin d'isoler le flux de trafic entre les différents environnements de calcul et les services AWS, et de relier des segments en cas de besoin, de manière ciblée et sûre.
- **Chiffrement des données au repos et en transit** – Options de chiffrement pour tous les services de stockage AWS, puissantes fonctions de création et de gestion du cycle de vie de certificats pour le chiffrement des données en transit. Gestion des clés via AWS Key Management Service (AWS KMS) ou utilisation éventuelle d'AWS CloudHSM pour la génération et le stockage des clés.
- **Isolement de l'hôte et de l'instance** – Options d'architectures dédiées basées sur un hyperviseur ou matériel nu permettant au client de maintenir les données sur un hôte de calcul physique non partagé.
- **Architecture sans serveur (« serverless ») et conteneur** – Les environnements d'exécution isolés offrent un environnement d'exécution plus petit et éphémère qui simplifie les contrôles de sécurité.

Authentification unifiée et mécanismes d'authentification

Les mécanismes de sécurité qui définissent et gèrent la gestion des identités et des accès sont des éléments critiques d'un programme de sécurité informatique. Ils servent à garantir que seuls les principaux authentifiés (utilisateurs, rôles, groupes, applications et autres identités) sont autorisés à accéder à la ressource ciblée de la manière prévue et avec les moindres privilèges. Une fonction majeure que de nombreuses organisations s'efforcent d'obtenir est l'authentification unifiée à travers les services de l'entreprise. Cette fonction permet de

mettre en place une validation d'identité applicable à l'ensemble du portefeuille de services. L'exécution de cette fonction est difficile, surtout lorsqu'il s'agit de systèmes hétérogènes exigeant des formats d'autorisation personnalisés ou dotés de modèles d'autorisation incompatibles.

Avec AWS, les clients bénéficient d'une authentification et d'une autorisation unifiées pour tous les services AWS, afin d'appliquer le principe du moindre privilège. AWS Identity and Access Management (IAM) permet aux clients de s'authentifier auprès de n'importe quel service AWS en utilisant le même format d'autorisation. IAM prend en charge plusieurs moyens d'authentification, notamment les clés d'accès API, les mots de passe des utilisateurs dans la console et la fédération à l'aide de fournisseurs d'identité externes. Les clients peuvent configurer les modes d'authentification dans IAM pour exiger une authentification multifactorielle. AWS permet aux clients de contrôler l'accès à leurs ressources dans les services AWS à l'aide de mécanismes d'authentification basés sur des politiques. Chaque politique est définie soit par le client, soit par AWS si le client s'appuie sur des politiques gérées par AWS, avec des définitions qui se combinent pour créer des autorisations ou des interdictions d'actions détaillées et conditionnelles s'appliquant sur des ressources données. Les clients peuvent partager ou réutiliser les politiques entre les identités au sein d'un même compte et entre les comptes, indépendamment de la manière dont ces identités sont authentifiées. Grâce à la robustesse de ces fonctionnalités, les clients peuvent concevoir un large éventail de mécanismes d'isolement et de contrôle des ressources cloud et des éléments au niveau des applications. Pour ce faire, ils peuvent utiliser des méthodes de contrôle d'accès basées sur des rôles (RBAC) ou sur des attributs (ABAC), ou les deux.

Les clients peuvent utiliser les politiques de plusieurs façons, notamment 1) en contrôlant les ressources auxquelles un ensemble d'utilisateurs peut accéder, 2) en contrôlant quels utilisateurs peuvent accéder à une ressource donnée, 3) en contrôlant les services AWS qui peuvent être utilisés et 4) en contrôlant les utilisateurs qui sont autorisés à modifier les politiques. Toutes les politiques permettent d'utiliser des conditions pour élargir l'accès. Par exemple, un client pourrait appliquer une politique qui n'autorise l'accès au contenu d'un compartiment Amazon Simple Storage Service (Amazon S3) que si l'utilisateur a également accès à la clé de déchiffrement gérée dans AWS Key Management Service et que la demande est faite sur un VPC spécifique. Toute possibilité de modifier une telle politique pourrait être réduite à un ensemble limité de modifications réservées à un groupe d'administrateurs privilégiés devant tous s'authentifier en utilisant plusieurs facteurs. Les politiques peuvent être appliquées à plusieurs comptes en utilisant AWS Organizations.

Ce niveau de contrôle, d'intégration profonde et d'interopérabilité étendue serait extrêmement difficile à mettre en œuvre et à gérer dans un environnement d'entreprise traditionnel sur site avec des systèmes physiquement séparés et hétérogènes. La plupart des organisations utilisent une combinaison de solutions de gestion des accès et des identités qui varient selon les équipes et les applications, mais aussi selon les différentes couches de la « pile » de l'infrastructure : périphériques réseau, virtualisation, systèmes d'exploitation et applications. Il en résulte un vaste ensemble de services d'identité qui doivent être liés entre eux et gérés de manière unifiée. Ce qui rend la gestion encore plus complexe, c'est que l'intégration de ces systèmes nécessite généralement un travail manuel important, associé à une attention et à une vigilance constantes à chaque fois que d'autres parties du portefeuille de services sont incluses. Enfin, il reste encore à élaborer des politiques d'accès uniformes pour garantir une application en cascade aux niveaux des systèmes et des données dans toute l'entreprise.

Avec AWS, la gestion de la sécurité basée sur des politiques offre aux clients plusieurs avantages. Les politiques de sécurité peuvent être conçues pour être lisibles par l'homme et par la machine. Ainsi, avec ce traitement des politiques de sécurité comme du code (« policy as code »), la gestion de la sécurité s'insère pleinement dans la gouvernance, la gestion des risques et la conformité. Cela améliore considérablement la clarté, la précision et la transparence en permettant aux parties prenantes de voir facilement les actions possibles ou impossibles, tout en pouvant exécuter cette politique directement dans le service. Les politiques peuvent être créées par programme et gérées dans un pipeline sous forme de code. Il est ainsi possible d'appliquer le même contrôle de la gestion de la configuration des politiques que celui dont dispose une organisation pour son code d'application. Un autre avantage distinct est la possibilité d'automatiser des tests dans un pipeline, comme on le ferait pour le développement de logiciels, afin de vérifier et de valider que les politiques fonctionnent correctement. Par exemple, IAM Access Analyzer permet aux clients d'évaluer en permanence les autorisations accordées dans les politiques, afin d'identifier les ressources auxquelles il est possible d'accéder en dehors du compte AWS du client. IAM Access Analyzer utilise un raisonnement automatisé qui applique la logique et l'inférence mathématique pour évaluer en quelques secondes des centaines, voire des milliers de politiques dans l'environnement d'un client.

Contrôle et journalisation étendus

L'une des pierres angulaires de la détection et de la protection de l'environnement et des données d'une entreprise est la capacité à surveiller de manière détaillée les configurations dans l'ensemble de l'entreprise et la journalisation robuste des activités qui se produisent dans une infrastructure informatique. La visibilité et la traçabilité dans les environnements informatiques sont souvent difficiles à obtenir pour les grandes opérations sur site qui se concentrent sur les contrôles de sécurité basés sur le cloisonnement physique. Cette conception peut entraîner une fragmentation des vues opérationnelles en raison du manque d'intégration entre les services. Dans ce cas, la détection des menaces et l'analyse des causes premières devient difficile. AWS crée des services de sécurité de base hautement intégrés au sein des services AWS, notamment la surveillance et la journalisation. AWS CloudTrail, Amazon CloudWatch, VPC Flow Logs et AWS Config s'intègrent avec les offres de services AWS, fournissant des enregistrements et des activités claires, ainsi que des modifications de configuration. Les informations fournies par ces services présentent une vue pluridimensionnelle de l'état opérationnel des systèmes et des données, sous l'angle fonctionnel, des performances et de la sécurité. Cette visibilité complète peut aussi être obtenue à moindre coût par rapport aux systèmes métier sur site.

AWS CloudTrail permet aux clients de journaliser les requêtes d'API AWS, indépendamment du fait que les requêtes ont été effectuées via la console de gestion AWS, les kits SDK AWS, les outils de ligne de commande, ou d'autres services AWS au nom du client. Chaque évènement de journal identifie l'appelant et l'API AWS appelée, l'adresse IP source de l'appel, lorsque l'appel a été émis, ainsi que d'autres paramètres propres à l'API. Les journaux peuvent être intégrés à un système local de gestion des informations et évènements de sécurité (SIEM) à des fins d'analyse, ou envoyés à d'autres services d'analytique, par exemple CloudWatch Logs Insights. Les journaux AWS CloudTrail sont signés numériquement afin d'empêcher qu'ils soient falsifiés avant leur stockage dans Amazon S3 à des fins d'accès par les clients. Les journaux peuvent également être conservés à l'aide du verrouillage d'objet S3, en vue de créer des politiques robustes qui rendent l'objet impossible à supprimer pour tous les utilisateurs, y compris les utilisateurs racines. Les journaux sont chiffrés au stockage, facultativement protégés par des clés gérées par le client dans AWS KMS.

Amazon CloudWatch permet de contrôler les ressources et applications AWS en quasi-temps réel. Le service peut collecter, suivre et envoyer des alertes en fonction de métriques accessibles via des tableaux de bord ou des API personnalisables. Les données CloudWatch sont chiffrées en transit et au repos. Par ailleurs, Amazon EventBridge fournit aux clients un flux

quasi-temps réel d'évènements système qui décrivent les modifications apportées aux ressources AWS. Les clients peuvent ainsi définir des alarmes de manière à être informés de tout accès potentiellement non autorisé. Les règles peuvent être implémentées en fonction des évènements et acheminées vers un ou plusieurs flux ou fonctions cibles afin de renforcer la surveillance, voire d'exécuter des actions correctives. Par exemple, les règles peuvent permettre d'examiner les événements entrants, d'analyser les valeurs entrantes et d'acheminer correctement les événements vers différentes cibles, telles que des adresses e-mail ou des appareils mobiles, des files d'attente de tickets et des systèmes de gestion des problèmes.

La gestion des configurations est au cœur du contrôle des modifications apportées à un environnement. Les configurations qui s'écartent de leur état prévu présentent un risque pour la posture de sécurité d'un système. En général, la gestion et l'application des états de configurations sur un environnement sur site sont loin d'être une tâche facile, car les outils pour mesurer l'état actuel d'un système n'ont pas souvent suffisamment de points d'intégration pour offrir une vue holistique de l'entreprise. Chez AWS, les clients peuvent effectuer la gestion des configurations de plusieurs manières. L'une des solutions idéales est la migration de votre environnement vers un modèle IaC (infrastructure as Code).

Le modèle IaC vous permet d'allouer, de désallouer et de maintenir l'état de configuration de l'infrastructure de façon cohérente, réplicable et automatisée à l'aide du code. Cela inclut la possibilité d'utiliser des pratiques de gestion de code sécurisées et de tester l'automatisation directement sur les composants d'infrastructure. Un des moyens d'y parvenir avec AWS est d'utiliser AWS CloudFormation.

Les modèles AWS CloudFormation permettent de créer, de configurer et de gérer les ressources via JSON (JavaScript Object Notation) ou YAML. Vous gérez ces ressources déclarées dans les modèles dans des unités appelées piles AWS CloudFormation. Les piles sont composées de StackSets qui permettent de gérer les ressources entre les régions et les comptes à partir de modèles individuels ou d'ensembles de modèles. Du point de vue de la surveillance, CloudFormation s'intègre à CloudTrail afin d'enregistrer les actions exécutées par le service. Par ailleurs, CloudFormation peut détecter les écarts de configurations entre la configuration actuelle des ressources d'un StackSets et la configuration attendue déclarée dans le StackSets. Ce niveau de gestion des configurations permet de détecter les modifications non gérées. L'utilisateur peut ainsi appliquer à nouveau le modèle afin de retourner les ressources à l'état déclaré.

Des fonctionnalités de gestion des configurations plus vastes et plus profondes sont souvent nécessaires pour permettre aux clients de gérer les nombreuses façons dont les ressources AWS

peuvent être allouées, modifiées et gérées. AWS Config répond à ce besoin en fournissant une vue détaillée et continue de la configuration des ressources AWS dans les différents comptes AWS d'un client. Cet aperçu montre notamment la manière dont les ressources sont liées les unes aux autres ainsi que leurs configurations antérieures, de sorte qu'un client puisse observer l'évolution des configurations et des relations au fil du temps. AWS Config fournit un inventaire des ressources AWS, un historique des configurations et des notifications de modification de configurations entre les comptes et les régions. Ces fonctionnalités, combinées à l'interrogation avancée et aux règles personnalisables, permettent d'obtenir des informations de sécurité et de gouvernance ainsi que d'automatiser les flux pour les ressources AWS.

Un autre pilier de la surveillance et de la journalisation de pointe est la visibilité du flux de trafic. Les journaux de flux VPC sont une fonction qui permet aux clients de capturer des informations sur le trafic IP vers et depuis les interfaces réseau de leurs VPC. Les données de journaux de flux peuvent être publiées sous forme de registres vers Amazon CloudWatch Logs et Amazon S3 à des fins d'analyse avancée. Un journal de flux peut être créé pour un VPC tout entier, un sous-réseau ou une interface réseau unique. Outre les journaux de flux, un VPC permet également une capture intégrale en cas d'utilité ou de nécessité à l'aide de la fonction de mise en miroir du trafic. Ces deux fonctions fonctionnent correctement ensemble, les journaux de flux de VPC pour la journalisation réseau de routine, et l'activation temporaire de la mise en miroir du trafic lorsque les circonstances l'exigent.

Utiliser des données de journalisation volumineuses peut être fastidieux pour certains clients. Ainsi, plusieurs choisissent de simplifier la surveillance et l'analyse des journaux en utilisant Amazon GuardDuty, la solution gérée AWS de détection des menaces. GuardDuty est un service qui fournit la détection des menaces et la surveillance continue du trafic réseau en utilisant et en analysant nombre de sources de données mentionnées ici, notamment les journaux de flux et les journaux CloudTrail, en plus des journaux DNS AWS internes et des flux d'informations sur les menaces. GuardDuty applique le machine learning, l'analyse des anomalies de comportements et d'autres techniques de détection pour identifier les menaces sur l'ensemble de l'activité réseau.

VPC et fonctions associées

Amazon Virtual Private Cloud (Amazon VPC) permet de créer au sein du réseau Amazon Elastic Cloud Compute (Amazon EC2) une enclave réseau logiquement séparée capable d'héberger les

ressources de calcul et de stockage. Cet environnement peut être connecté à une infrastructure existante du client à travers différentes méthodes (notamment la connexion réseau VPN via Internet) ou via AWS Direct Connect, un service qui fournit la connectivité privée dans le Cloud AWS. L'utilisation d'un VPC fournit aux organisations flexibilité, sécurité et contrôle total de leur empreinte réseau dans le cloud. Les clients peuvent contrôler leur environnement privé, par exemple les adresses IP, les sous-réseaux, les listes de contrôle d'accès réseau, les groupes de sécurité, les pare-feu de systèmes d'exploitation, les tables de routage, les VPN et les passerelles Internet. Amazon VPC fournit une isolation logique robuste de toutes les ressources clientes, dont leurs chemins d'accès réciproques et leurs chemins d'accès aux services AWS.

Chaque flux de paquets du réseau est individuellement autorisé, conformément à une règle, pour valider la source et la destination appropriées avant la transmission et la livraison dudit flux. Il est ainsi tout à fait improbable que des informations puissent traverser des entités sans être spécifiquement autorisées par l'entité de transmission et celle de réception. Si un paquet est acheminé vers une destination sans une règle de correspondance, il est rejeté. Les adresses de réponse doivent être valides, sinon le paquet est rejeté. De plus, les paquets ARP (protocole de résolution d'adresse) déclenchent une consultation de base de données authentifiée, et ainsi ces paquets n'atteignent jamais le réseau, car ils ne sont pas indispensables à la détection de la topologie du réseau virtuel. Par conséquent, l'usurpation ARP est tout à fait improbable sur le réseau AWS. Par ailleurs, le mode promiscuité (« promiscuous mode ») ne révèle aucun trafic autre que le trafic vers et depuis le système d'exploitation du client. Les clients peuvent définir des règles précises pour le trafic entrant et sortant, qui optimisent la flexibilité de la connectivité ainsi que le contrôle client de la segmentation et du routage du trafic.

Les options de connectivité VPC incluent la possibilité pour les clients de :

- se connecter à Internet à l'aide du mécanisme NAT (Network Address Translation) (sous-réseaux privés). Ici, des sous-réseaux privés peuvent être utilisés pour des instances ne devant pas avoir un accès direct à ou depuis Internet. Les instances d'un sous-réseau privé peuvent accéder à Internet sans exposer leur adresse IP privée, en acheminant leur trafic via une passerelle NAT (Network Address Translation) dans un sous-réseau public ;

- se connecter en toute sécurité au centre de données d'entreprise. Ainsi, l'ensemble du trafic sortant et entrant dans les instances d'un VPC peut être acheminé jusqu'au centre de données d'entreprise du client à travers une connexion VPN matériel IPsec chiffrée et conforme aux normes du secteur ;
- se connecter de manière privée à d'autres VPC. Appairez des VPC pour partager des ressources sur plusieurs réseaux virtuels au sein de multiples comptes AWS ;
- connecter de manière privée les services internes dans différents comptes et VPC au sein d'un AWS Organisation, simplifiant ainsi considérablement l'architecture réseau interne ;
- utiliser AWS Transit Gateway comme passerelle centrale unifiée et unique où vous pouvez créer des connexions vers plusieurs VPC et systèmes sur site tout en étant en mesure de gérer l'authentification et l'accès aux services avec AWS IAM ;
- utiliser des fonctions comme AWS PrivateLink pour créer des connexions privées aux ressources en dehors du VPC du client. Ces connexions privées ne traversent pas l'Internet public, et peuvent fournir une connectivité sécurisée entre les VPC, les services AWS et les applications sur site.

Par ailleurs, l'ensemble du trafic au sein d'un VPC et d'un appairage inter-région est chiffré de manière transparente lorsque vous utilisez les types d'instance pris en charge. Du point de vue de l'infrastructure, le chiffrement du réseau physique est utilisé par AWS pour chiffrer le trafic réseau sur n'importe quelle liaison hors du contrôle physique d'AWS, par exemple entre les centres de données.

Chiffrement des données au repos et en transit

AWS recommande le chiffrement comme solution de renforcement du contrôle des accès, en complément des contrôles d'accès orientés identité, ressources et réseau décrits ci-dessus. AWS fournit un certain nombre de fonctions qui permettent aux clients de simplifier le chiffrement de leurs données et la gestion de leurs clés. Tous les services AWS offrent la possibilité de chiffrer les données au repos et en transit. AWS KMS s'intègrent avec la plupart des services. Les clients peuvent ainsi contrôler le cycle de vie et les autorisations relatives aux clés utilisées pour chiffrer les données au nom du client. Les clients peuvent appliquer et gérer

le chiffrement sur les services intégrés à AWS KMS en utilisant des outils de politiques et de configuration.

L'utilisation du chiffrement côté serveur des services AWS est le moyen le plus simple pour les clients de garantir que le chiffrement est implémenté correctement et appliqué de manière cohérente. Les clients peuvent contrôler le moment où les données sont déchiffrées, l'identité de l'auteur ainsi que les conditions du déchiffrement, et ce au fil du passage de ces données vers et depuis leurs applications et leurs services AWS. Étant donné que l'accès à des fins de chiffrement et de déchiffrement aux données dans un service est contrôlé de manière indépendante par les politiques AWS KMS sous maîtrise du client, ce dernier peut isoler le contrôle de l'accès aux données du contrôle de l'accès aux clés. Ce modèle d'isolation est un puissant outil pour renforcer le contrôle du cloisonnement logique qui peut être appliqué sur l'ensemble de l'environnement AWS d'un client.

Outre le contrôle du chiffrement côté serveur dans les services AWS, les clients peuvent choisir de chiffrer leurs données dans leur propre environnement d'applications en utilisant AWS KMS avec le chiffrement côté client, ce qui évite ainsi d’inclure les services AWS de leur domaine de confiance. Le chiffrement au niveau des applications et côté client peut être utilisé pour garantir une posture de sécurité cohérente à mesure que les données transitent dans la propre architecture de services du client, que ce soit dans AWS, sur site ou dans un modèle hybride. L'utilisation d'AWS KMS pour gérer le cycle de vie et les autorisations relatives aux clés fournit un mécanisme homogène de contrôle d'accès pour toutes les clés de chiffrement, et ce indépendamment de l'emplacement où elles sont utilisées.

Afin d'empêcher l'utilisation non autorisée des clés de chiffrement en dehors des limites d'AWS KMS, le service emploie des modules de sécurité matériel (HSM) pour protéger les clés de chiffrement du client pendant que celles-ci sont utilisées. Ces HSM sont validés en vertu de la norme FIPS (Federal Information Processing Standard) 140-2 avec des contrôles sur la résistance à l'effraction physique. Ces HSM sont conçus de telle sorte que les clés de texte en clair ne peuvent pas être utilisées par quiconque en dehors du module HSM, même les employés d'AWS. La seule façon dont ces clés peuvent être utilisées c'est lorsque le service reçoit une requête authentifiée et autorisée du client. En réponse à cette requête, AWS KMS permet que la clé du client puisse être utilisée dans le HSM pour une opération de chiffrement ou de déchiffrement. Les clés du client peuvent être utilisées uniquement dans la région AWS dans laquelle elle a été créée. Les HSM dans AWS KMS ont une conception multilocataire, car n'importe quelle clé de client peut être utilisée dans n'importe quel HSM dans la région. Comme les autres services AWS qui utilisent la multi-location, AWS KMS limite l'utilisation des clés uniquement au client qui possède les clés. Il n'existe aucun mécanisme permettant à un utilisateur non autorisé d'utiliser la clé d'un client. AWS KMS gère de manière transparente la durabilité et la disponibilité des clés des clients et peut être mis à l'échelle pour prendre en charge un nombre illimité de clés au rythme où les applications des clients doivent les utiliser. Les clients gèrent simplement le cycle de vie et les autorisations sur les clés à l'aide des mêmes contrôles d'authentification et d'autorisation disponibles pour tous les autres services AWS. Chaque demande faite à AWS KMS est enregistrée dans AWS CloudTrail pour fournir un audit sur le moment où et les circonstances dans lesquelles les clés ont été utilisées. AWS KMS est dans le champ d'application de tous les programmes d'accréditation pris en charge par AWS qui concernent la protection des données.

Pour les clients qui souhaitent gérer directement le dispositif HSM qui génère, stocke et utilise leurs clés de chiffrement, AWS CloudHSM est disponible en option. AWS CloudHSM offre un dispositif HSM dédié, validé FIPS 140-2 niveau 3, et la possibilité de s'intégrer aux applications des clients à l'aide d'API standard telles que les bibliothèques PKCS#11, Java Cryptography Extensions (JCE) et Microsoft CryptoNG (CNG). Il permet aux organisations d'exporter des clés vers la plupart des autres modules HSM disponibles dans le commerce pour les utiliser dans des architectures hybrides. AWS automatise les tâches administratives chronophages liées à ces modules HSM, telles que la mise en service de matériels, l'application de correctifs logiciels, le routage réseau et la création de sauvegardes chiffrées des magasins de clés. Les clients se chargent de la mise à l'échelle de leur environnement CloudHSM et de la gestion des comptes utilisateur cryptographiques et des informations d'identification dans le module HSM. Comme

AWS KMS, CloudHSM est conçu de telle sorte que les clés en clair ne peuvent pas être utilisées en dehors du module HSM par quiconque, y compris les employés d'AWS.

Les clients peuvent bénéficier de la facilité d'utilisation et de l'intégration aux services AWS offertes par AWS KMS avec AWS CloudHSM en utilisant l'option de magasin de clés personnalisé AWS KMS. Les clients attachent logiquement un cluster AWS CloudHSM à un identifiant de clé AWS KMS, de sorte que les demandes faites à la clé sont autorisées par AWS KMS, mais exécutées sur le CloudHSM dédié du client.

Pour protéger les données en transit, AWS encourage ses clients à utiliser une approche à plusieurs niveaux. Tout le trafic réseau entre les centres de données AWS est chiffré de manière transparente au niveau de la couche physique. Tout le trafic dans un VPC et entre les VPC appairés entre les régions est chiffré de manière transparente au niveau de la couche réseau lors de l'utilisation des types d'instances Amazon EC2 pris en charge. Au niveau de la couche application, les clients ont le choix d'utiliser ou non le chiffrement à l'aide d'un protocole tel que Transport Layer Security (TLS). Tous les points de terminaison des services AWS prennent en charge TLS, afin de créer une connexion HTTPS sécurisée pour effectuer des demandes d'API.[1] Pour l'infrastructure gérée par le client dans AWS qui doit terminer TLS, AWS offre plusieurs options, notamment des services d'équilibrage de charge (par exemple, Elastic Load Balancing, dispositif d'équilibrage de charge réseau et Application Load Balancer), Amazon CloudFront (un réseau de distribution de contenu) et Amazon API Gateway. Pour mettre en œuvre une connexion TLS, chacun de ces services permet aux clients de télécharger leurs propres certificats numériques pour lier une identité cryptographique au point de terminaison. Les certificats numériques sont notoirement difficiles à gérer à grande échelle, car ils expirent et doivent être renouvelés. AWS simplifie le processus de génération, de distribution et de renouvellement des certificats numériques grâce au service AWS Certificate Manager (ACM). ACM offre gratuitement des certificats de confiance publics qui peuvent être utilisés dans les services AWS qui les requièrent pour terminer les connexions TLS vers Internet. ACM offre également la possibilité de créer une autorité de certification privée pour générer, distribuer et renouveler automatiquement les certificats, afin de sécuriser la communication interne entre les infrastructures gérées par le client.

Grâce à des services tels que AWS KMS, AWS CloudHSM et AWS ACM, les clients peuvent mettre en œuvre une stratégie complète de chiffrement des données au repos et en transit dans leur écosystème AWS, afin que toutes les données d'une classification partagent la même posture de sécurité.

Hôtes et instances

AWS fait constamment évoluer ses fonctionnalités de sécurité, tant au niveau de l'hôte que de l'instance des opérations. Ces fonctionnalités assurent l'isolement et le cloisonnement des opérations pour le matériel hôte et les instances qui s'exécutent sur ces hôtes. Avec l'introduction d'AWS Nitro System, AWS fournit des mécanismes de sécurité définis par le secteur pour les opérations du micrologiciel et de l'hyperviseur. AWS Nitro System est composé d'une gamme de cartes PCIe (Peripheral component Interconnect Express) dotées de circuits intégrés personnalisés (ASIC) qui contrôlent des fonctions distinctes telles que l'accès au stockage, les réseaux virtuels et une puce de sécurité Nitro qui contrôle et protège en permanence les ressources matérielles et vérifie indépendamment le micrologiciel à chaque démarrage du système. Ces éléments, associés à Nitro, un hyperviseur léger basé sur KVM (Kernel Virtual Machine), constituent l'épine dorsale de nombreuses familles d'instances AWS. Ainsi, AWS peut limiter les interactions opérateur-hôte à un petit ensemble de fonctions qui ne peuvent être appelées que par le biais d'une API. Il n'existe aucun accès à une console. Les instances virtuelles fonctionnant sur ces hôtes sont également soumises à de nombreux mécanismes de sécurité supplémentaires, tels que l'isolement de la mémoire et du processeur.

En plus de fournir des services de calcul à plusieurs locataires hautement sécurisés et isolés logiquement, AWS offre également des moyens de déployer le calcul sur du matériel dédié en utilisant des instances dédiées, des hôtes dédiés et du matériel nu. Ces options de déploiement peuvent être utilisées pour lancer des instances Amazon EC2 sur des serveurs physiques dédiés à l'usage des clients. Les instances dédiées sont des instances Amazon EC2 basées sur un hyperviseur qui fonctionnent dans un VPC sur du matériel dédié à un seul client. Les instances dédiées sont physiquement isolées au niveau du matériel hôte des instances appartenant à d'autres comptes AWS. Les instances dédiées peuvent partager du matériel avec d'autres instances du même compte AWS qui ne sont pas des instances dédiées. Un hôte dédié est également un serveur physique qui est dédié à l'usage du client. Avec un hôte dédié, les clients ont une visibilité et un contrôle sur la façon dont les instances basées sur un hypervisor sont placées sur le serveur. Les instances nues (« bare-metal ») sont des dispositifs matériels hôtes qui ne sont pas basés sur un hyperviseur. Grâce à la technologie AWS Nitro, qui permet de décharger le réseau et le stockage, ainsi qu'à la puce de sécurité Nitro, qui répond aux risques liés à la mise à disposition en série de matériel nu, les clients ont un accès direct au matériel

Amazon EC2. Ces instances dites « bare-metal » font pleinement partie du service Amazon EC2 et ont accès à des services tels qu'Amazon VPC et Amazon Elastic Block Store (Amazon EBS).

Il existe peu ou pas de différences de performance, physiques ou de sécurité entre les instances dédiées et les instances déployées sur des hôtes dédiés. Cependant, les hôtes dédiés donnent aux clients un contrôle renforcé sur la façon dont les instances sont placées sur un serveur physique et la manière dont ce serveur est utilisé. Lorsque les clients utilisent des hôtes dédiés, ils contrôlent le placement des instances sur l'hôte en utilisant les paramètres d'affinité d'hôte et de placement automatique d'instance. Si les clients souhaitent utiliser AWS et disposent d'une licence logicielle existante qui exige que le logiciel soit exécuté sur un matériel particulier pendant une durée minimale, les hôtes dédiés offrent une visibilité sur le matériel de l'hôte, ce qui permet aux clients de satisfaire aux exigences de la licence.

Services sans serveur (« serverless ») et de conteneurs

En ayant la possibilité d'intégrer de manière transparente la technologie sans serveur (« serverless »), la technologie des conteneurs et les conceptions de microservices dans AWS, les clients peuvent créer plusieurs niveaux d'isolement pour les applications. Les services AWS utilisent plusieurs couches de sécurité pour réaliser des opérations isolées. De nombreuses fonctions de sécurité de services tels qu'AWS Lambda et AWS Fargate, opérant en arrière-plan, reposent sur les fonctionnalités fournies par les services AWS et les fonctions de sécurité abordées précédemment dans ce document. Par exemple, l'ensemble des services et fonctionnalités de sécurité inclus dans l'architecture EC2 Nitro, les réseaux VPC et IAM (par exemple, les ACL, les groupes de sécurité et les politiques IAM) s'appliquent également ici.

AWS aborde l'isolement logique avec son service serverless, AWS Lambda, et son service de conteneurs gérés, AWS Fargate, de manière multicouche. Ces couches commencent par des instances métal nu, les mêmes que les clients peuvent mettre en service, en utilisant la même architecture Nitro sous-jacente et en bénéficiant de ses avantages de sécurité qui ont été évoqués précédemment. Ensuite, à un niveau supérieur, se trouve le contrôleur de machine virtuelle léger spécialement conçu, appelé Firecracker, qui a été créé par AWS pour gérer en toute sécurité les conteneurs et les fonctions serverless. Firecracker fonctionne comme un environnement isolé qui fournit une exécution sécurisée pour les fonctions serverless et les conteneurs. Lambda fonctionne dans EC2 comme des micro-machines virtuelles (micro-VM) et offre des protections similaires à celles des autres instances EC2 en matière d'isolement logique. Chaque fonction s'exécute dans un environnement de test (sandbox) contenu dans la micro-VM. L'environnement de test offre un isolement sécurisé du noyau Linux à l'aide de cgroups, de namespaces, de seccomp et d'autres fonctions. En outre, des techniques telles que l'isolement de processus et l'établissement de liens statiques sont utilisées pour isoler de manière sûre l'environnement d'exécution. Firecracker présente de multiples fonctions de sécurité telles que « simple guest model » : il s'agit d'un modèle de virtualisation des interfaces qui présente une surface minimale exposant uniquement le nombre de fonctions nécessaires pour fonctionner. Ces niveaux de protection concentriques permettent d'exécuter des appels rapides, en une fraction de seconde, tout en isolant de manière sécurisée la micro-VM d'un compte client. Le code source de Firecracker a été fourni à l'ensemble de la communauté en open source, afin d'assurer la transparence totale avec sa configuration et ses fonctionnalités opérationnelles.

Les clients peuvent élaborer leurs propres pratiques d'isolement et de cloisonnement logiques adaptées à leur organisation en utilisant des fonctionnalités telles que les ressources serverless. Par exemple, les clients peuvent créer des architectures événementielles ayant plusieurs cas d'utilisation axés sur l'automatisation, de la réponse aux incidents à la gestion de la flotte. Lambda en combinaison avec d'autres services AWS, tels qu'Amazon CloudWatch Events ou Amazon EventBridge, AWS Step Functions, Amazon GuardDuty et d'autres services pour créer des fonctionnalités de sécurité. Grâce à ces services, les opérations peuvent être conçues de manière à remédier automatiquement aux problèmes de sécurité sans nécessiter d'intervention humaine. Par exemple, un résultat dans Amazon GuardDuty peut être envoyé à CloudWatch Events qui peut ensuite déclencher une fonction Lambda pour lancer une activité de résolution, comme la mise à jour des groupes de sécurité, du pare-feu d'application Web ou la modification des politiques IAM. AWS Step Functions et des fonctions Lambda supplémentaires peuvent être ajoutées au flux pour créer une logique plus complexe, comme l'appel à AWS

Systems Manager pour exécuter des commandes sur une instance EC2, afin de capturer ou de modifier des configurations. Ce concept peut être utilisé pour mettre en place des pratiques d'isolement similaires qui empêchent l'accès humain direct aux applications importantes, ce qui serait très difficile dans un environnement traditionnel sur site. Pour plus d'informations, consultez le guide de réponse aux incidents de sécurité AWS.

Le service d'orchestration de conteneur AWS, Amazon Elastic Container Service (Amazon ECS), fournit ses propres propriétés de cloisonnement et d'isolement de sécurité, que vous l'utilisiez pour gérer des services de conteneur tels qu'AWS Fargate ou dans un environnement autogéré sur EC2. Amazon ECS Task Definitions permet aux clients de définir la fonctionnalité de sécurité et les paramètres d'isolement en utilisant les fonctions de sécurité de leur propre VPC. Un ou plusieurs conteneurs peuvent fonctionner dans des contraintes prescrites en utilisant une définition Amazon ECS Task. Un client peut définir des règles détaillées de communication entre conteneurs, car chaque définition de tâche peut recevoir sa propre interface réseau Elastic dans un VPC client. Les conteneurs bénéficient ainsi des mêmes fonctions de sécurité réseau VPC que les instances EC2. Les clients peuvent appliquer des politiques IAM à chaque tâche, ce qui renforce les limites d'accès et opérationnelles de chaque conteneur ou ensemble de conteneurs. Les mécanismes de sécurité et d'isolation liés aux fonctions en amont, comme un registre de conteneur, sont traités avec Amazon Elastic Container Registry (Amazon ECR). Lorsqu'un conteneur est créé ou retiré, il est essentiel que des protections entourent ces images sources lors de leur hébergement et de leur transmission. Amazon ECR chiffre automatiquement les images des conteneurs au repos et en transit. Grâce aux politiques IAM, l'accès aux images Amazon ECR peut être limité aux seuls principaux qui ont besoin de cet accès. La suite de services de conteneurs AWS, utilisée conjointement, crée un environnement isolé et sécurisé de bout en bout pour des flottes de conteneurs ou de microservices.

AWS Cloud Services offre aux clients une liste croissante de fonctionnalités permettant de rendre la sécurité « dans le cloud » robuste et facile à mettre en œuvre tout en maintenant un niveau de sécurité élevé. Des services et des fonctions de sécurité en constante évolution réduisent les processus lourds, améliorent la confidentialité et élargissent l'accessibilité, afin de démocratiser la sécurité et les avantages des techniques modernes et de l'innovation. L'application de pratiques de sécurité de base comme le chiffrement, avec une mise en œuvre appropriée par le client, peut efficacement remédier aux risques sécuritaires liés à la demande de cloisonnement physique.

Prévention de l'accès non autorisé aux données

Afin de prévenir tout accès non autorisé, il faut mettre en œuvre de bonnes pratiques de sécurité et implémenter de solides capacités de prévention et de détection. Par exemple, les systèmes doivent être conçus de manière à limiter la « portée des conséquences » des évènements de sécurité. De cette manière, un nœud non autorisé aura une incidence réduite sur un autre nœud de l'entreprise. Les fournisseurs de services cloud hyperscale, tels qu'AWS, fournissent un environnement d'outils de sécurité complet pour permettre aux clients de maintenir des communications chiffrées et de mettre en œuvre des protections contre la falsification afin d'atténuer le risque d'accès non autorisé. AWS n'a ni visibilité ni connaissance du contenu d'un compte client, ni même s'il comporte ou non des informations personnelles. Les clients AWS sont habilités à utiliser diverses techniques telles que le chiffrement, la création de jetons, la décomposition des données et les techniques d'obfuscation pour rendre le contenu inintelligible pour AWS ou d'autres parties souhaitant accéder à son contenu.

- **Chiffrement** : Le chiffrement approprié des données peut les rendre illisibles. Cela signifie que le stockage de données chiffrées dans le cloud, quel que soit leur emplacement, peut fournir une protection adéquate contre la grande majorité des menaces d'exfiltration. Il est essentiel que les clés de chiffrement des données soient soigneusement gérées afin de garantir une protection solide contre toute interception. AWS fournit des services qui peuvent offrir ces capacités de niveau entreprise grâce à AWS CloudHSM ou AWS KMS. [8] Le niveau de contrôle sur la méthode de chiffrement, le stockage et la gestion des clés cryptographiques utilisées avec les données est laissé à la volonté du client.
- **Création de jetons** : La création de jetons est un processus qui vous permet de définir une séquence de données pour la représentation d'une information normalement sensible (par exemple, un jeton représentant le numéro de carte de crédit d'un client). Seul, un jeton est dénué de sens et ne peut pas être associé aux données qu'il représente sans utiliser le système de création de jetons. Les coffres de jetons peuvent être construits dans des VPC pour stocker des informations sensibles sous forme cryptée tout en partageant des jetons vers des services approuvés pour la transmission de données masquées. En outre, AWS dispose d'un certain nombre de partenaires spécialisés dans la fourniture de services de création de jetons qui s'intègrent avec des bases de données populaires et d'autres services de stockage.

- **Décomposition des données** : Il s'agit d'un processus qui réduit les jeux de données en éléments non identifiables qui, seuls, sont dénués de sens.[10] Ces éléments ou des fragments de ceux-ci sont ensuite stockés de manière distribuée, de manière à ce que l'accès non autorisé à un nœud ne fournisse qu'un fragment de données insignifiant. Cette technique présente un avantage intrinsèque : un utilisateur non autorisé aurait besoin d'arriver à compromettre tous les nœuds, à obtenir tous les fragments et à connaître l'algorithme (ou le schéma de fragmentation) pour reconstituer les données de manière cohérente.
- **Défense par cyber-tromperie** : Les architectures et les solutions de cybercriminalité peuvent être un élément clé pour atténuer les évènements de sécurité avancés. Les solutions de tromperie peuvent utiliser des pièges et des leurres très sophistiqués pour donner à un attaquant l'impression qu'il s'est infiltré dans le système tout en le détournant en réalité vers un environnement hautement contrôlé. Des renseignements sur l'attaquant sont recueillis afin de limiter les menaces futures et l'attaque est neutralisée.

AWS surveille également la gestion à distance non autorisée et déconnecte ou désactive rapidement tout accès à distance non autorisé une fois qu'il est détecté. Toutes les tentatives d'accès administratif à distance sont consignées et les journaux sont examinés, non seulement par des humains pour la détection d'activités suspectes, mais également par des systèmes automatisés de machine learning conçus par l'équipe de sécurité AWS pour la détection des modes d'accès inhabituels qui peuvent indiquer des tentatives d'accès aux données non autorisées. Si une activité suspecte est détectée, les procédures d'intervention en cas d'incident sont lancées. En outre, AWS a instauré des stratégies et des procédures en bonne et due forme afin de définir les standards pour l'accès logique aux hôtes et à l'infrastructure AWS. Les politiques identifient également les responsabilités fonctionnelles pour l'administration de l'accès logique et de la sécurité. Sauf interdiction par la loi, AWS exige que tous les employés fassent l'objet d'une enquête sur leurs antécédents qui soit proportionnelle à leur poste et à leur niveau d'accès. Enfin, les instances virtuelles du client sont contrôlées uniquement par le client qui dispose d'un accès racine complet ou d'un contrôle administratif sur les comptes, les services et les applications. Le personnel d'AWS n'a pas la possibilité de se connecter aux instances EC2 ou les conteneurs ECS/EKS du client.

Les tâches et les domaines de responsabilité (demande d'accès et approbation, demande de gestion des modifications et approbation, etc.) sont répartis entre différentes personnes afin de réduire les possibilités de modification ou d'utilisation abusive non autorisée ou involontaire des

systèmes AWS. Le personnel AWS ayant besoin d'accéder aux outils de gestion doit d'abord utiliser l'authentification multifacteur, distincte de ses autorisations professionnelles Amazon normales, pour accéder à des hôtes d'administration spécialement conçus. Ces hôtes d'administration sont des systèmes spécialement conçus, développés, configurés et renforcés pour la protection des outils de gestion. Tous les accès sont consignés et vérifiés. Dès lors qu'un employé n'a plus de motif professionnel d'accéder aux outils de gestion, les autorisations et l'accès à ces hôtes et aux systèmes concernés sont révoqués. AWS a mis en œuvre une stratégie de verrouillage de session qui est systématiquement appliquée. Le verrou de session est retenu jusqu'à ce que les procédures d'identification et d'authentification soient exécutées.

AWS permet aux organisations de tenir des registres d'audit qui prennent en charge, après coup, les enquêtes des évènements de sécurité et la capacité de satisfaire aux exigences de rétention d'informations réglementaires et organisationnelles. Les clients peuvent récupérer les journaux d'audit sur le cloud et les rapports en exploitant CloudTrail et CloudWatch Logs, puis les fournir aux autorités compétentes. Ces solutions permettent aux clients d'AWS de se conformer directement aux demandes de renseignements émanant des autorités. Cela permet aux représentants du gouvernement d'obtenir les informations dont ils ont besoin sans devoir accéder au contenu sous-jacent des clients. Pour obtenir des informations supplémentaires sur la « communication forcée » ou l'application de la loi relative à l'accès aux données, consultez la section Livre blanc sur la résidence des données d'AWS.

Étude de cas

Le département de la Défense des États-Unis autorise le cloisonnement logique du stockage pour les applications sensibles non-classifiées.

En décembre 2011, le responsable fédéral de l'information (CIO) des États-Unis a mis en place une politique gouvernementale qui mandate les agences fédérales à se servir du programme fédéral de gestion des risques et des autorisations (FedRAMP), un programme standardisé, fédéral pour l'autorisation de sécurité des services cloud. FedRAMP garantit trois niveaux de sécurité standardisés, impact faible, modéré et élevé, en fonction des 199 catégorisations des Normes fédérales de traitement de l'information (FIPS). Ces niveaux ont été élaborés grâce à la collaboration d'experts de la cybersécurité du secteur privé et du gouvernement des États-Unis (notamment le département de la Défense (DoD)). Bien qu'ayant établi une réciprocité avec le niveau FedRAMP modéré, le DoD n'en a pas établi avec le niveau FedRAMP élevé. Il a plutôt

élaboré et mis en œuvre ce qui s'apparente effectivement à un ensemble de contrôles de sécurité et d'exigences « FedRAMP plus » au moyen du guide des exigences de sécurité (SRG) du cloud computing du DoD.

Le DoD, à travers le SRG, exige spécifiquement une séparation entre le DoD et les entités du gouvernement fédéral grâce à des moyens physiques ou logiques. Pour être plus précis, le SRG stipule que « Les fournisseurs de services cloud sont tenus de fournir des preuves de la solidité de leurs contrôles du cloisonnement virtuel et de leur surveillance. Ils doivent également prouver leur capacité à satisfaire aux demandes de « recherche et de saisie » sans divulgation d'informations et de données du DoD ». Pour aller plus loin, en ce qui concerne les systèmes de niveau d'impact 5 (IL5),[2] le DoD exige une « séparation physique (une infrastructure dédiée par exemple) avec les entités n'appartenant pas ni DoD ni au gouvernement fédéral. » De telles exigences visent à répondre aux préoccupations du DoD relatives au mélange de ses données avec les données d'autres entités suite à une divulgation involontaire des données et un accès non autorisé ou la falsification des données du DoD par une entité externe.

Le SRG a démontré que l'utilisation d'un cloisonnement logique en tant qu'approche viable répond aux exigences de séparation IL5 du DoD pour la mise en œuvre d'une bonne pratique axée sur le résultat :

« Un fournisseur de services cloud peut proposer des solutions alternatives qui offrent une sécurité équivalente aux exigences stipulées. Une approbation fera l'objet d'une évaluation au cas par cas au cours du processus d'évaluation de la PA (autorisation d'allocation). »

AWS a prouvé la suffisance, à travers le processus d'évaluation et d'autorisation (d'accréditation) du SRG sur le cloud computing du DoD, du cloisonnement logique *combiné à la dédicace des environnements logiques*[3] afin de satisfaire le besoin initialement exprimé sous la forme d'une exigence d'infrastructure dédiée et physiquement isolée pour les applications non confidentielles les plus sensibles du DoD. Notre approche autorisée confirme que les environnements multi-locataires logiquement cloisonnés qui satisfont aux contrôles de sécurité robustes peuvent offrir un niveau de sécurité supérieur aux déploiements de cloud privés dédiés, tout en offrant des avantages significatifs en matière de disponibilité, de capacité de mise à l'échelle et de coûts plus réduits. La technologie cloud moderne de fournisseurs bien établis peut offrir des solutions nouvelles pouvant permettre de réaliser l'objectif de sécurité des technologies traditionnelles, tant que les approches d'accréditation restent assez flexibles pour s'adapter à d'autres mises en œuvre.

Conclusion

L'approche d'AWS montre que des environnements logiquement séparés correctement configurés et aux locataires multiples peuvent offrir un niveau de sécurité supérieur aux déploiements de cloud privés, tout en fournissant des avantages significatifs en matière de disponibilité, de capacité de mise à l'échelle et de coût. La technologie cloud moderne de fournisseurs bien établis peut offrir des solutions nouvelles pouvant permettre d'atteindre l'objectif de sécurité des technologies traditionnelles sur la base du cloisonnement physique, tant que les approches d'accréditation restent assez flexibles pour s'adapter à d'autres mises en œuvre.

Bien que le fait de passer en revue les contrôles de sécurité puisse être utile pour prouver la conformité, l'expérience a montré que les organisations qui se concentrent principalement (et pour certaines exclusivement) sur la mise en œuvre de contrôles traditionnels peuvent accidentellement limiter leur accès aux meilleures solutions de sécurité. Lorsque les organisations du secteur public et privé évaluent si les fournisseurs de services cloud répondent aux exigences sur la base de concepts hérités des architectures sur site, elles devraient prendre du recul et articuler clairement les attentes en matière de sécurité. Le mappage de tels résultats avec les capacités du fournisseur de services cloud et la compréhension de la façon correcte de satisfaire à ces besoins conduisent à une compréhension approfondie de la manière la plus efficace possible de concevoir une solution. Cela permet par ailleurs de clarifier le risque acceptable d'une exploitation dans le cloud.

Au fur et à mesure que les programmes d'assurance sécurité mûrissent et évoluent afin de s'aligner à l'évolution rapide de l'innovation des fonctions cloud et de la sécurité, les contrôles traditionnels deviendront de moins en moins pertinents par rapport aux capacités des fournisseurs de services cloud déjà existantes aujourd'hui et qui continueront probablement à s'améliorer très vite. L’état final souhaité, c’est à dire une sécurité cloud robuste basée sur un cadre défini par d’une part les objectifs de sécurité des clients et d’autre part les capacités de sécurités des fournisseurs de services cloud permettant de satisfaire à ces objectifs, peut uniquement survenir comme résultat d'un dialogue continu entre les différentes parties prenantes de l'assurance sécurité du cloud. AWS estime que cette approche continuera à apporter des améliorations significatives dans le maintien de l'assurance de la posture de sécurité d'un CSP.

Contributeurs

Ont participé à ce document :

- Tim Anderson, conseiller principal à la sécurité, aux stratégies de croissance et de la sécurité
- Ken Beer, Directeur général, crytographie
- Min Hyun, responsable mondial des stratégies de croissance et de la sécurité
- Mark Ryland, directeur, bureau du CISO, sécurité

Suggestions de lecture

Pour en savoir plus, reportez-vous à :

- Page des livres blancs AWS
- Livre blanc relatif à la résidence des données AWS
- Guide de réponse aux incidents de sécurité AWS

Révisions du document

Date	Description
Juillet 2020	Première publication

Notes

[1] AWS met à jour tous les points de terminaison FIPS vers une version de protocole TLS (Transport Layer Security) minimale 1.2 dans toutes les régions AWS, avec pour objectif de l'achever le 31 mars 2021. Après cela, ces mises à jour révoqueront toute possibilité d'utilisation des protocoles TLS 1.0 et TLS 1.1 sur tous les points de terminaison FIPS. Aucun autre point de terminaison AWS ne sera affecté par ce changement.

[2] Exigences d'emplacement et de séparation de niveau d'impact 5.

Les informations qui doivent être traitées et stockées au niveau d'impact 5 peuvent uniquement être traitées dans une infrastructure dédiée, sur site ou hors site dans tout modèle de déploiement cloud qui limite l'emplacement physique des informations comme stipulé dans la section 5.2.1 relative aux « Exigences de juridiction/d'emplacement. » Cela exclut les offres de service publiques.

Les conditions suivantes s'appliquent :

- Seuls les cloud DoD privés, de la communauté DoD ou de la communauté du gouvernement fédéral sont admissibles au niveau d'impact 5.
- Chaque modèle de déploiement peut prendre en charge plusieurs missions ou locataires/missions de chaque organisation cliente.
- Une séparation virtuelle/logique entre le DoD et les entités du gouvernement fédéral est autorisée.
- Une séparation virtuelle/logique entre les systèmes est au minimum exigée.
- Un cloisonnement physique (une infrastructure dédiée par exemple) avec les entités n'appartenant ni au DoD ni au gouvernement fédéral est requise.

REMARQUE : Un fournisseur de services cloud peut proposer d'autres solutions qui offrent une sécurité équivalente aux exigences stipulées. Une approbation fera l'objet d'une évaluation au cas par cas au cours du processus d'évaluation de la PA.

https://iasecontent.disa.mil/cloud/Downloads/Cloud_Computing_SRG_v1r3.pdf

[3] Reportez-vous à la section précédente sur les « Fonctions hôte et instance ».