Séparation logique

Évaluation des exigences du ministère de la Défense américain en matière de sécurité du cloud pour les charges de travail sensibles

Mai 2018

[Série de guides AWS destinés au gouvernement]

Mentions légales

Ce document est fourni à titre informatif uniquement. Il présente l'offre de produits et les pratiques actuelles d'AWS à la date de publication de ce document, des informations qui sont susceptibles d'être modifiées sans avis préalable. Il incombe aux clients de procéder à leur propre évaluation indépendante des informations contenues dans ce document et chaque client est responsable de son utilisation des produits ou services AWS, chacun étant fourni « en l'état », sans garantie d'aucune sorte, qu'elle soit explicite ou implicite. Ce document ne crée pas de garanties, représentations, engagements contractuels, conditions ou assurances à l'encontre d'AWS, de ses affiliés, fournisseurs ou donneurs de licence. 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.

Table des matières

Objectif

Ce document examine l'équivalent de la sécurité par séparation logique pour les clients qui utilisent l'infrastructure en tant que service (IaaS) d'Amazon Web Services (AWS) afin de répondre aux exigences de séparation définies dans le Guide des exigences de sécurité (SRG) en matière de cloud computing du ministère de la Défense américain. Ce document détaille l'approche en trois points (utilisation de la virtualisation, du chiffrement et du déploiement du calcul sur du matériel dédié) que les gouvernements du monde entier peuvent utiliser afin de migrer en toute confiance des charges de travail sensibles non classifiées (*par exemple*, celles qui ont un impact élevé) dans le cloud sans avoir besoin d'infrastructure physiquement dédiée.

Introduction

La technologie du cloud s'appuie sur des techniques informatiques transformatrices. Les clients qui utilisent le cloud peuvent bénéficier d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des organisations les plus pointilleuses en termes de sécurité dans le monde. De nouveaux modèles opérationnels et de nouvelles abstractions fournis par les technologies de cloud contribuent à la création d'un environnement informatique plus sécurisé. Les fournisseurs de services cloud (CSP) tels qu'AWS utilisent le cloud pour innover et offrir aux clients de nouvelles fonctionnalités de sécurité améliorées. AWS propose des services disponibles immédiatement et prend en charge les capacités de défense en profondeur et en ampleur avec des mécanismes de sécurité intrinsèques aux conceptions et fonctionnements des services de cloud.

La conception d'AWS permet aux clients de posséder et de contrôler leurs contenus grâce à des outils qui donnent aux clients la possibilité de déterminer où leurs contenus seront stockés. Les fonctionnalités d'AWS permettent aux clients de sécuriser leurs contenus en transit et au repos, et de gérer l'accès aux services et ressources AWS pour leurs utilisateurs. Les clients d'AWS conservent un contrôle total sur les accès aux contenus, ce qui empêche des utilisateurs et des clients non autorisés d'accéder à d'autres comptes clients. AWS fournit des services multilocataires avec la meilleure sécurité du secteur en matière de séparation des locataires. Cette séparation logique entre les environnements clients fournie par AWS offre une sécurité plus efficace et plus fiable que celle d'une infrastructure physique dédiée.

Contexte

En décembre 2011, le Directeur fédéral des informations américain a établi une politique s'appliquant à tout le gouvernement et rendant obligatoire l'utilisation du FedRAMP (Federal Risk and Authorization Management Program) par tous les organismes fédéraux. Ce programme national constitue une approche normalisée des autorisations de sécurité des services de cloud. L'approche « action unique/utilisations multiples » du programme FedRAMP a été conçue de façon à offrir des avantages importants, par exemple une cohérence et une fiabilité accrues de l'évaluation des contrôles de sécurité, des coûts réduits pour les prestataires de services et les clients des agences, ainsi que la rationalisation des évaluations d'autorisation faisant double emploi entre les agences qui acquièrent le même service. L'instance principale décisionnelle et de gouvernance du FedRAMP est le JAB (Joint Authorization Board), qui est composé des directeurs informatiques de l'Administration générale des services, du ministère de la Sécurité intérieure et du ministère de la Défense.

Le programme FedRAMP comporte actuellement trois bases de référence en matière de sécurité (faible, modérée et à impact élevé), reposant sur les catégories de la Federal Information Processing Standards Publication (FIPS) 199 . Ces références ont été définies avec la collaboration des experts en cybersécurité du secteur privé et du gouvernement américain (dont le ministère de la Défense). Bien que le ministère de la Défense ait établi une réciprocité avec la référence modérée du FedRAMP, il n'a pas établi de réciprocité avec la référence élevée de ce programme. En revanche, il a élaboré et mis en œuvre ce qui est véritablement un ensemble de contrôles et d'exigences de sécurité « FedRAMP plus » via le Guide des exigences de sécurité (SRG) en matière de cloud computing du Ministère de la défense américain.

Dans ce cadre, le ministère de la Défense exige plus particulièrement une séparation entre les locataires/missions du ministère de la Défense et du gouvernement fédéral à l'aide de solutions physiques ou logiques. Le Guide SRG indique plus particulièrement que les « CSP doivent fournir des preuves des contrôles et de la surveillance solides de la séparation virtuelle, ainsi que la capacité de répondre aux demandes de perquisitions et de saisie sans diffusion d'informations et de données du ministère de la Défense ». Mais surtout, pour les systèmes de niveau d'impact 5 (IL5),[1] le ministère de la Défense exige « la séparation physique (par exemple, une infrastructure dédiée) des locataires autres que ceux liés au ministère de la Défense/au gouvernement fédéral ». Ces exigences du ministère de la Défense sont liées aux préoccupations relatives au mélange des données du ministère avec celles d'autres locataires en raison de fuites ou de débordements de données, et de l'accès non autorisé aux données du ministère de la Défense par un locataire autre ou de l'altération des données par ce dernier.

Pour mettre en œuvre une bonne pratique axée sur les résultats, le SRG a reconnu l'utilisation de la séparation logique comme une approche viable permettant de répondre aux exigences de séparation IL5 du ministère de la Défense américain :

> *« Un CSP peut offrir d'autres solutions de sécurité équivalente pour répondre aux exigences indiquées. L'approbation sera examinée au cas par cas lors de l'évaluation de l'autorisation provisoire. »*

---

1 5.2.2.2 Exigences d'emplacement et de séparation pour le 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, locale ou non, dans tout modèle de déploiement de cloud qui limite l'emplacement physique des informations tel que décrit à la section 5.2.1, « Exigences en matière de juridiction/emplacement ». Cela exclut les offres des services publics.

Les conditions suivantes s'appliquent :

- Seuls les clouds privés du ministère de la Défense américain, les clouds de la communauté du ministère de la Défense américain ou ceux de la communauté du gouvernement fédéral sont éligibles pour le niveau d'impact 5.
- Chaque modèle de déploiement peut prendre en charge plusieurs missions ou locataires/missions pour chaque organisation client.
- La séparation virtuelle/logique entre les locataires/missions du ministère de la Défense américain et du gouvernement fédéral est autorisée.
- La séparation virtuelle/logique entre les systèmes locataires/missions est exigée au minimum.
- La séparation physique (par exemple via une infrastructure dédiée) des locataires autres que ceux du ministère de la Défense américain/du gouvernement fédéral est obligatoire.

REMARQUE : Un CSP peut offrir d'autres solutions de sécurité équivalente pour répondre aux exigences indiquées. L'approbation sera examinée au cas par cas lors de l'évaluation de l'autorisation provisoire.

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

Quels sont les inconvénients des exigences de séparation physique ?

Les exigences des offres de cloud physiquement dédiées sont essentiellement liées aux risques d'accès non autorisés par des tiers ou autres à des applications, contenus ou données, ce qui inclut les accès contraints pour des raisons légales et les accès non autorisés par des tiers. Toutefois, pour les systèmes qui sont accessibles sur un réseau ou Internet, la séparation physique, par exemple via un placement dans une cage verrouillée ou dans un site de centre de données distinct, ne fournit pas de sécurité ou de contrôle supplémentaire des accès. En termes simples, tous les contrôles d'accès pour les systèmes connectés sont gérés via des contrôles d'accès logiques, la gestion des autorisations, le routage et le chiffrement du trafic réseau. AWS résout les problèmes liés à la séparation physique à l'aide des capacités de sécurité logique que nous fournissons à tous nos clients et des contrôles de sécurité que nous avons mis en place pour protéger les données clients, comme décrit plus loin dans l'approche de séparation logique en trois points.

Les environnements physiquement séparés de plus petite taille n'ont pas de parité avec les environnements de cloud généralement disponibles. C'est pourquoi toute obligation de séparation physique peut limiter ou retarder la capacité d'un client à tirer parti d'investissements novateurs (y compris des innovations en termes de fonctionnalités de sécurité) effectués au nom de tous les clients qui utilisent AWS Services. D'autres inconvénients sont à noter : une structure de coût plus élevé et une consommation moindre dues à une utilisation moins efficace de l'espace, ainsi qu'à des options et fonctionnalités de redondance limitées par rapport à la géodiversité des régions de centres de données commerciales.

En quoi la séparation logique est-elle plus efficace que la séparation physique ?

Les clients peuvent utiliser l'approche en trois points ci-dessous pour obtenir des résultats identiques à ceux de la séparation physique en termes de sécurité, comme requis pour le niveau IL5 du ministère de la Défense américain.

1. Cloud privé virtuel – Démonstration suffisante que VPC crée l'équivalent de domaines de réseau totalement distincts pour chaque locataire ;
2. Chiffrement des données au repos et en transit – Utilisation des capacités de chiffrement intrinsèques ou fournies par l'utilisateur des services de cloud AWS tels qu'EBS, S3 et DynamoDB, avec des clés de chiffrement générées et stockées par AWS Key Management Service (KMS) et/ou AWS Cloud Hardware Security Module (CloudHSM) ; et
3. Hôtes dédiés, instances dédiées et Bare Metal – Les chargés de mission du ministère de la Défense américain peuvent provisionner des hôtes physiques AWS complets afin de traiter les instances de machines hypervisées et non hypervisées qu'ils attribuent et les charges de travail associées.

1. Virtual Private Cloud (VPC)

AWS VPC permet la création d'une enclave réseau logiquement séparée au sein du réseau AWS Elastic Cloud Compute (Amazon EC2) afin d'héberger des ressources de calcul et de stockage. Cet environnement peut être connecté à l'infrastructure existante d'un client via une connexion réseau privé virtuel (VPN) sur Internet ou via AWS Direct Connect, un service qui fournit une connectivité privée au cloud AWS. L'utilisation d'un VPC offre aux chargés de mission de la flexibilité, de la sécurité et un contrôle complet sur leur présence réseau dans le cloud. Elle permet une transition contrôlée vers le cloud à l'aide d'un modèle de centre de données et d'un plan de gestion existants du client. Le client contrôle l'environnement privé, dont les adresses IP, les sous-réseaux, les listes de contrôle d'accès réseau, les groupes de sécurité, les pare-feu de système d'exploitation, les tables de routage, les VPN et/ou les passerelles Internet. Amazon VPC offre une isolation logique solide de toutes les ressources du client. Par exemple, chaque flux de paquets sur le réseau est autorisé individuellement à valider la source et la destination correctes avant la transmission et la livraison. Les informations ne peuvent pas être transmises entre plusieurs locataires sans être spécifiquement autorisées par les clients émetteurs et destinataires. Si un paquet est acheminé vers une destination sans règle qui lui correspond, il est abandonné. De plus, alors que les paquets ARP (Address Resolution Protocol, protocole de résolution d'adresses) déclenchent une recherche authentifiée dans la base de données, les paquets ARP n'atteignent jamais le réseau car ils ne sont pas nécessaires pour la découverte de la topologie de réseau virtuel, ce qui signifie que l'usurpation ARP est impossible. En outre, le mode de proximité ne révèle aucun trafic autre que celui se dirigeant vers le système d'exploitation du client ou provenant de celui-ci. Ces ensembles de règles précis et définis par le client qui régissent les entrées et sorties de trafic permettent non seulement une connectivité plus flexible, mais offrent également au client un meilleur contrôle sur la segmentation et le routage du trafic.

Par exemple, les options de connectivité VPC[2] incluent la capacité d'effectuer les opérations suivantes pour le client :

- Se connecter à Internet à l'aide de la traduction d'adresses réseau NAT (sous-réseaux privés) : | Les sous-réseaux privés peuvent être utilisés pour des instances qui ne doivent 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 à son centre de données d'entreprise : | L'ensemble du trafic depuis et vers les instances de votre VPC peut être acheminé vers votre centre de données d'entreprise via une connexion VPN physique IPsec chiffrée, conforme à la norme du secteur.
- Se connecter de façon privée à d'autres VPC : | Appairez les VPC de façon à partager les ressources entre plusieurs réseaux virtuels détenus par vos comptes AWS.
- Se connecter de façon privée aux services internes sur différents comptes et VPC au sein de vos propres organisations, ce qui simplifie considérablement votre architecture réseau interne.

---

2 Remarque : l'utilisation d'un VPC avec une passerelle privée vers une solution approuvée de point d'accès au cloud (CAP) ou d'architecture de calcul de cloud sécurisée (SCCA) du ministère de la Défense américain est obligatoire pour tous les clients utilisant les charges de travail SRG IL5 dans la région AWS GovCloud (USA), sauf dispense accordée dans des circonstances spéciales par le directeur informatique du ministère de la Défense.

2. Chiffrement de données en transit et au repos

Pour les données stockées par les chargés de mission dans les services de stockage AWS ou transitant sur nos réseaux, nous recommandons fortement un chiffrement pour les données au repos et en transit. Afin de proposer un processus simple et sécurisé à nos clients, nous fournissons un certain nombre d'outils et de fonctionnalités qui leur permettent de chiffrer les données, ainsi que plusieurs options d'infrastructure de gestion des clés de chiffrement. Ces fonctionnalités de chiffrement et de contrôle d'accès aux données sont déjà intégrées aux offres de services de base telles qu'Amazon Simple Storage Service (Amazon S3), un service de stockage d'objets hautement évolutif, Amazon Elastic Block Store (Amazon EBS), qui fournit un stockage attaché au réseau aux instances EC2 et Amazon Relational Database Service (Amazon RDS), qui fournit des moteurs de bases de données gérées. Ces fonctionnalités sont prêtes à être utilisées et fournissent une documentation riche afin d'aider les clients à comprendre comment leurs données sont protégées et les options de configuration qu'ils peuvent contrôler pour personnaliser les accès aux systèmes. Les services natifs d'AWS disposent de capacités de sécurité en évolution qui, dans les environnements hérités, n'ont pu être atteintes qu'à l'aide d'un regroupement de fournisseurs tiers. Aujourd'hui, ces capacités sont de plus en plus disponibles, ce qui permet aux clients de se concentrer sur l'innovation des services.

L'association d'AWS KMS (AWS Key Management Service) et d'AWS CloudHSM se trouve au cœur d'une solution de chiffrement rigoureuse. AWS KMS est un service régional entièrement géré et extrêmement disponible qui utilise des modules de sécurité matériels (HSM) validés FIPS 140-2 niveau 3 (sécurité physique)[3] à la base, avec un logiciel de dimensionnement sophistiqué capable de gérer des centaines de milliers de demandes d'API par seconde. Il permet aux clients de réaliser des fonctions de gestion des clés de façon étroitement intégrée à d'autres services AWS. AWS CloudHSM fournit un HSM dédié, FIPS 140-2 niveau 3 (global) sous votre contrôle exclusif, directement dans votre Amazon Virtual Private Cloud (VPC).[4] Le service CloudHSM offre la disponibilité, la réplication et la sauvegarde automatisées des HSM dédiés à un seul client au sein des zones de disponibilité. Il s'intègre aux applications appartenant au client grâce à des API de chiffrement standard du secteur. Bien qu'applicables dans différents contextes, les deux services fonctionnent pour garantir que l'algorithme de chiffrement est assez solide pour rendre les données incompréhensibles et suffisamment protéger les clés afin que le texte chiffré soit illisible par des personnes non autorisées. En d'autres termes, le stockage de données bien chiffrées avec des clés correctement gérées et sécurisées peut vous offrir l'assurance de données totalement protégées. Cette approche est tout aussi pertinente, applicable et efficace qu'elle soit déployée dans un environnement cloud commercial physiquement ou logiquement isolé.

3 https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3139

4 https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/3108

Avec le chiffrement, la confidentialité des clés de chiffrement du chargé de mission est cruciale. La sécurité dépend du lieu de chiffrement des données et des personnes qui ont accès aux clés et les protègent.
Si les données sont chiffrées par le chargé de mission avant d'être insérées dans le cloud, le CSP n'a aucune raison d'avoir accès aux clés : le chargé de mission est pleinement maître et responsable. D'un autre côté, si les données sont chiffrées à l'aide de services inhérents au CSP, alors le CSP et le propriétaire des données font tous deux partie de la chaîne de traçabilité des clés. AWS KMS est conçu de telle façon que personne, y compris les employés AWS, ne puisse récupérer vos clés en texte brut dans le service. Le service utilise des HSM validés FIPS 140-2 pour protéger la confidentialité et l'intégrité de vos clés, que vous demandiez à KMS de créer des clés pour vous ou que vous les importiez dans le service. Vos clés en texte brut ne sont jamais écrites sur un disque et sont uniquement utilisées dans la mémoire volatile des HSM pendant la durée nécessaire permettant de réaliser l'opération de chiffrement que vous avez demandée. Les clés KMS ne sont jamais transmises en dehors des régions AWS dans lesquelles elles ont été créées. Les mises à jour du microprogramme HSM KMS sont contrôlées par un contrôle d'accès basé sur le quorum audité et vérifié par un groupe indépendant au sein d'Amazon. Ces stratégies, ces processus et ces procédures ont été audités et accrédités de façon indépendante dans le cadre du programme FedRAMP et par le département de la Défense américain. La section ci-dessous récapitule les capacités d'AWS KMS et d'AWS CloudHSM. Les clients peuvent consulter les liens intégrés pour des ressources supplémentaires sur AWS KMS et AWS CloudHSM.

AWS Key Management Service (KMS)

AWS Key Management Service (KMS) offre aux clients un contrôle centralisé des clés de chiffrement utilisées pour protéger leurs données. Avec AWS KMS, les clients peuvent créer, changer, désactiver, supprimer et définir des stratégies d'utilisation et auditer l'utilisation des clés de chiffrement utilisées pour chiffrer les données des clients. AWS KMS est intégré aux services AWS pour simplifier le chiffrement des données stockées dans ces services avec des clés de chiffrement gérées par un client (ou via des clés de chiffrement par défaut qu'un service AWS gère au nom du client). Ce service est inclus avec cinq services de base accrédités pour répondre aux exigences IL5 du département de la Défense américain afin de permettre le chiffrement des données au repos et en transit et offrir une séparation logique suffisante des données du département de la Défense américain en transition dans l'infrastructure AWS et co-implantées sur du matériel avec des données de clients n'appartenant pas au département de la Défense américain. Par exemple, dans le cas de données au repos, l'utilisation d'algorithmes de chiffrement solides pour une séparation logique des données client constitue la base pour établir une équivalence à la séparation physique de données au repos, ce qui est une exigence pour IL5.

La limite de sécurité interne d'AWS KMS est le module de sécurité matériel (HSM). Le HSM possède une API web interne limitée et aucune autre interface physique active en état de fonctionnement. Un HSM opérationnel est configuré et chargé avec les clés de chiffrement appropriées lors de l'initialisation. Les matériaux de chiffrement sensibles du HSM sont uniquement stockés dans une mémoire volatile et supprimés lorsque le HSM n'est plus en fonctionnement, y compris en cas d'arrêts prévus ou non, ou de réinitialisations. En état de fonctionnement, aucun opérateur humain ne peut accéder au HSM. Seuls les hôtes de service gérant les demandes des clients peuvent établir des connexions via l'API limitée. Les API HSM sont disponibles via une session confidentielle authentifiée mutuelle établie par des opérateurs humains (hors état de fonctionnement) ou des hôtes de service (en état de fonctionnement).

Le système est conçu de telle façon que plusieurs opérateurs humains utilisant une authentification à deux facteurs sont requis via un processus basé sur le quorum pour mettre à jour la configuration du microprogramme ou du logiciel sur tout HSM KMS ; encore une fois, cela est uniquement possible s'il n'est plus en état de fonctionnement et s'il ne contient aucune clé.

> **Remarque :** AWS Key Management Service (KMS) utilise maintenant des modules de sécurité matériels (HSM) validés FIPS 140-2 et prend en charge les points de terminaison validés FIPS 140-2, pour une garantie indépendante de la confidentialité et l'intégrité de vos clés.

HSM Cloud AWS

AWS CloudHSM offre une solution matérielle efficace de gestion des clés à l'échelle du cloud pour les charges de travail sensibles et réglementées. CloudHSM permet aux chargés de mission d'allouer et de tirer profit de clés de chiffrement pour chiffrer leurs données dans les services AWS et leurs applications résidentes. Avec CloudHSM, les clients gèrent leurs propres clés de chiffrement grâce à un HSM validé FIPS 140-2 de niveau 3 et il offre la flexibilité de s'intégrer à leurs applications en utilisant des API standard comme les bibliothèques PKCS#11, Java Cryptography Extensions (JCE) et Microsoft CryptoNG (CNG). Il est également conforme aux normes et permet aux chargés de mission d'exporter toutes les clés vers la plupart des autres HSM disponibles sur le marché. CloudHSM est un service géré qui automatise les tâches administratives fastidieuses, comme la mise en service de matériel, l'application de correctifs logiciels, la haute disponibilité et les sauvegardes. Pour assurer la protection et l'isolation de votre CloudHSM par rapport aux autres clients Amazon, CloudHSM doit être déployé dans un VPC.

La séparation des fonctions et du contrôle d'accès basé sur les rôles est inhérente à la conception du CloudHSM. AWS bénéficie d'un accès limité au HSM qui nous permet de surveiller et maintenir l'état de santé ainsi que la disponibilité du HSM, d'effectuer des sauvegardes chiffrées, mais aussi d'extraire et de publier des journaux d'audit sur votre CloudWatch Logs. AWS ne peut pas voir, accéder à ou utiliser vos clés, ni forcer votre HSM à effectuer des opérations cryptographiques grâce aux clés.

3. Hôtes dédiés, instances dédiées et matériel nu

En plus de fournir des services de calcul à locataires multiples logiquement isolés et hautement sécurisés, AWS offre également trois moyens de déployer le calcul vers 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 votre utilisation. Les instances dédiées sont des instances Amazon EC2 hypervisées exécutées dans un VPC (Virtual Private Cloud) sur du matériel dédié à un seul client. Les instances dédiées sont physiquement isolées au niveau matériel hôte des instances qui appartiennent 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 dédié à votre utilisation. Un hôte dédié vous procure de la visibilité et du contrôle sur la façon dont les instances hypervisées sont placées sur le serveur. Les instances de matériel nu sont des appareils de matériel hôte non hypervisés. Avec l'aide de la technologie Nitro d'AWS pour décharger le stockage et le réseau ainsi que la puce de sécurité Nitro pour éliminer les risques associés à une location de série unique de matériel nu, les clients ont un accès direct au matériel Amazon EC2. Ces instances de matériel nu sont de véritables membres du service Amazon EC2 et ont accès à des services tels qu'Amazon VPC et Amazon Elastic Block Store (EBS).[5]

---

5 Actuellement, les instances Amazon EC2 de matériel nu peuvent être expérimentées sur la famille d'instance I3 sous la forme du type d'instance i3.metal.

Il n'existe pas de différence physique, de sécurité ou de performance entre les instances dédiées et les instances déployées sur des hôtes dédiés. Toutefois, les hôtes dédiés offrent aux chargés de mission un contrôle supplémentaire sur la façon dont les instances sont placées sur un serveur physique et dont ce serveur est utilisé. Lorsque vous utilisez les hôtes dédiés, vous pouvez contrôler le placement des instances sur l'hôte à l'aide des paramètres d'affinité de l'hôte et de placement automatique des instances. Si votre organisation souhaite utiliser AWS et dispose d'une licence logicielle existante qui implique que le logiciel soit exécuté sur du matériel spécifique pendant une durée minimale. Les hôtes dédiés offrent de la visibilité sur le matériel de l'hôte, ce qui vous permet de satisfaire aux exigences concernant ces licences.

Comment le cloud à locataires multiples prend-il en charge les exigences réglementaires pour les données sans libérer de données du département de la Défense américain ?

AWS respecte les exigences réglementaires légales concernant les données. Bien que les systèmes sur site permettent généralement aux autorités de directement saisir du matériel physique du propriétaire des données ou d'y accéder, le cloud computing présente un nouveau modèle puisque les données sont hébergées dans un environnement à locataires multiples. Saisir physiquement le matériel physique ou y accéder n'est pas possible dans AWS puisque les données d'un client sont réparties sur différents appareils physiques, ce qui force toutes les demandes de données à passer via un processus de récupération logique approuvé et autorisé. Grâce à notre accréditation FedRAMP, AWS respecte les contrôles NIST 800-53 constituant les bases de niveau modéré FedRAMP, dont les contrôles de sécurité « Rétention et gestion des informations » et « Intégrité des informations et du système ». Entre autres, cela signifie que les services AWS délimitent les différents comptes clients, empêchent tout emmêlement des comptes clients et permettent aux clients d'avoir un contrôle total sur les contenus et les opérations de leurs comptes AWS spécifiques. Les clients du département de la Défense américain, comme tous les clients, peuvent être assurés que toute exigence réglementaire légale ne s'appliquera qu'aux données contenues dans le compte du client en question. Nous respectons également les contrôles « Intégrité des informations et du système » qui nécessitent que les CSP conformes permettent aux clients d'accéder à leurs données et demandent que les données des agences conformes respectent les législations applicables. De plus, les contrôles « Audit et responsabilité » nécessitent que les organisations conservent les enregistrements d'audit afin d'aider les investigations a posteriori des incidents de sécurité et de respecter les exigences relatives à la conservation des informations organisationnelles et réglementaires. Les clients peuvent récupérer les rapports et les journaux d'audit du cloud en tirant parti des journaux de CloudTrail et de CloudWatch Logs qu'ils peuvent ensuite fournir aux autorités appropriées. Ces solutions permettent au département de la Défense américain de répondre directement aux exigences réglementaires ou générales de l'inspecteur, afin que les autorités gouvernementales aient un accès direct aux informations dont elles peuvent avoir besoin sans saisir de matériel.

AWS applique également des stratégies et des contrôles stricts en termes de nettoyage et de destruction. Par exemple, AWS suit, documente et vérifie les mesures de nettoyage et de destruction des supports. Un client n'a à aucun moment physiquement accès au support mappé à son volume logique ou son objet. Toute suppression ou élimination des supports est réalisée par le personnel AWS désigné. Les contenus sur les lecteurs sont traités au plus haut niveau de classification conformément à la stratégie de classification des données d'AWS. Tous les supports sont rendus illisibles ou détruits à la fin du cycle de vie du support avant de quitter la salle du centre de données d'AWS, conformément aux normes de sécurité d'AWS dans le cadre de la mise hors service.

Comment le cloud à locataires multiples protège-t-il les données du département de la Défense américain de l'accès non autorisé de tiers, dont l'accès des employés du CSP ?

Le risque d'accès non autorisé de tiers au contenu du client et l'adéquation des mesures de contrôle destinées à empêcher les accès non autorisés par le personnel du CSP représentent une autre inquiétude associée à l'étendue de la capacité des organismes d'application de la loi à légalement demander des données de clients. L'accès au contenu des clients, ainsi que son utilisation, se font toujours uniquement dans le cas d'une obligation légale ou de la nécessité de procéder à la maintenance des services AWS dans le but de pouvoir les proposer à nos clients et à leurs utilisateurs finaux.

L'accès des employés aux systèmes AWS est alloué sur la base du moindre privilège, approuvé par une personne agréée avant la mise à disposition de l'accès et supervisé par un employé d'AWS. Les obligations et zones de responsabilité (demande et approbation d'accès, demande et approbation de gestion des modifications, etc.) doivent être réparties entre différentes personnes afin de réduire le risque de modification non autorisée ou non intentionnelle, ou de mauvais usage des systèmes AWS. Le personnel AWS ayant besoin, pour des raisons professionnelles, d'accéder au niveau de gestion doit commencer par utiliser l'authentification MFA (Multi-Factor Authentication), distincte des informations d'identification Amazon standard, pour accéder aux hôtes d'administration conçus dans ce but. Ces hôtes d'administration sont des systèmes spécifiquement conçus, développés, configurés et renforcés pour protéger le niveau de gestion. Un tel accès est consigné et vérifié. Dès lors qu'un employé n'a plus de motif professionnel d'accéder au plan de gestion, les autorisations et l'accès à ces hôtes et aux systèmes concernés sont révoqués. AWS a implémenté une stratégie de verrouillage de gestion qui est systématiquement mise en œuvre. Le verrouillage de la session est maintenu jusqu'à l'exécution de procédures d'identification et d'authentification établies.

Les clients peuvent gérer l'accès au contenu de leurs clients, ainsi qu'aux services et aux ressources AWS. Nous proposons un ensemble élaboré de fonctionnalités d'accès, de chiffrement et de journalisation afin de vous permettre de réaliser toutes ces tâches de la façon la plus efficace possible (grâce à AWS CloudTrail, CloudWatch, CloudHSM et AWS KMS tel que décrit précédemment).

Quelles sont les recommandations d'AWS aux gouvernements concernant les exigences de séparation physique ?

Via le processus d'autorisation du guide des exigences de sécurité (SRG) en matière de cloud computing du département de la Défense américain, AWS a démontré qu'une séparation logique suffisait à répondre à l'objectif qui se trouve derrière une demande d'infrastructure dédiée physiquement isolée pour les charges de travail non classifiées les plus sensibles du département de la Défense américain. Notre approche confirme que les environnements à locataires multiples logiquement séparés qui répondent à des contrôles de sécurité efficaces peuvent fournir un niveau de sécurité supérieur aux déploiements dans le cloud privé dédié tout en offrant des avantages considérables en termes de disponibilité, de scalabilité et de coût moindre. Les technologies de cloud modernes de fournisseurs établis offrent des solutions innovantes qui peuvent atteindre l'objectif de sécurité des technologies traditionnelles tant que les approches d'accréditation sont assez flexibles pour accueillir d'autres implémentations.

Bien que la révision des contrôles de sécurité puisse être utile pour prouver une certaine conformité, notre expérience nous a montré que les organisations qui se concentrent principalement (et dans certains cas exclusivement) sur l'implémentation de contrôles traditionnels peuvent accidentellement limiter leur accès aux meilleures solutions de sécurité. Puisque les gouvernements évaluent si les CSP répondent aux exigences basées sur des concepts existants, ils devraient clairement exprimer les résultats souhaités en termes de sécurité et permettre aux CSP de développer des techniques optimales pour atteindre (et même excéder) ces résultats. La mise en évidence des objectifs de sécurité souhaités derrière une exigence spécifique peut aider les agences fédérales à se concentrer à juste titre sur les résultats qu'elles veulent atteindre plutôt que sur les informations d'implémentation.

Puisque les programmes d'assurance de sécurité évoluent et s'agrandissent pour suivre le rythme rapide des innovations du cloud en matière de sécurité et de fonctionnalités, les informations d'implémentation de contrôle deviendront de moins en moins importantes par rapport aux capacités offertes par le CSP. L'aboutissement souhaité, une sécurité robuste du cloud basée sur un cadre défini par les résultats en termes de sécurité du client et des techniques de sécurité déterminées par le CSP pour atteindre ces résultats, peut uniquement se produire à la suite d'un dialogue continu au sein de la communauté de parties prenantes d'assurance du cloud. Nous pensons que cette approche permettrait d'améliorer de manière significative la préservation de la sécurité des CSP.

En plus de fournir une autre solution logiquement équivalente, AWS a utilisé une approche de bout en bout et des séances d'analyse pour résoudre les principaux problèmes de sécurité du ministère de la Défense. Après avoir étudié les besoins du client exprimés dans le guide des exigences de sécurité (SRG) en matière de cloud computing du ministère de la Défense, AWS a organisé plusieurs sessions d'informations pour expliquer au ministère de la Défense en quoi notre triple approche répond aux exigences de séparation physique. L'organisme d'évaluation tiers qui a validé nos services a également participé à ces sessions pour attester de l'exactitude de nos propos et proposer une évaluation basée sur les risques. Ces sessions collaboratives sont un moyen utile et efficace de garantir la sécurité, d'accélérer l'accréditation et à terme de faire progresser les objectifs de modernisation informatique du ministère de la Défense.

L'évolution du ministère de la Défense vers des solutions novatrices adaptables au cloud nous encourage à atteindre l'objectif que visent les exigences de séparation physique dans le cloud. Nous nous engageons à poursuivre notre collaboration avec les gouvernements du monde entier qui évaluent les avantages et les bonnes pratiques de l'approche d'équivalence de la séparation logique du ministère de la Défense.