Assurer la conformité au RGPD sur AWS

Novembre 2017

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 et ne modifie aucun contrat entre AWS et ses clients.

Table des matières

Résumé

Le Règlement général sur la protection des données (le « RGPD ») entre en vigueur le 25 mai 2018. AWS vous offre des services et des ressources pour vous aider à vous conformer aux obligations du RGPD qui peuvent s'appliquer à vos activités. Cela comprend l'adhésion d'AWS au code de conduite CISPE, des contrôles précis des accès aux données, des outils de surveillance et de journalisation, le chiffrement, la gestion de clé, les capacités d'audit, l'adhésion aux normes de sécurité informatique et les attestations C5 d'AWS.

Le Règlement général sur la protection des données : présentation

Le RGPD est une nouvelle réglementation européenne relative à la protection de la vie privée, dont l'entrée en vigueur est prévue le 25 mai 2018. Le but du RGPD est d'harmoniser les lois de protection des données dans l'Union européenne (UE) en appliquant une seule loi pour la protection des données valable pour chacun des États membres.

Le RGPD s'applique à toutes les organisations disposant d'une installation au sein de l'UE ou qui proposent des biens ou des services aux individus vivant dans l'UE ou lors du traitement de « données à caractère personnel » de résidents de l'UE. Par « données à caractère personnel », on entend toute information liée à une personne physique identifiée ou identifiable.

Le RGPD remplacera l'actuelle Directive européenne sur la protection des données personnelles (Directive européenne 95/46/CE). À compter du 25 mai 2018, l'actuelle Directive sur la protection des données personnelles et toutes les lois s'y référant cesseront de s'appliquer.

Changements apportés par le RGPD pour les organisations menant des activités dans l'UE

L'un des aspects essentiels du RGPD est qu'il vise à unifier la manière dont les données à caractère personnel peuvent être traitées, utilisées et échangées de façon sécurisée dans les différents États membres de l'UE. Les organisations devront démontrer en permanence la sécurité des données traitées ainsi que leur conformité au RGPD, en mettant en œuvre et révisant régulièrement des mesures techniques et organisationnelles rigoureuses, ainsi que des politiques de conformité. Les autorités de contrôle pourront infliger des amendes d'un montant équivalent à 20 millions d'euros ou à 4 % du chiffre d'affaires annuel au niveau mondial, la valeur la plus élevée étant retenue.

Comment AWS se prépare-t-il au RGPD ?

Les experts en conformité, protection des données et sécurité d'AWS collaborent avec des clients du monde entier afin de répondre à leurs questions et de les aider à se préparer à exécuter leurs charges de travail dans le cloud

après l'entrée en vigueur du RGPD. Ces équipes ont également passé en revue toutes les actions déjà mises en œuvre par AWS, afin de s'assurer qu'elles respectent les exigences du RGPD.

> Nous pouvons vous assurer que tous les services AWS seront conformes au RGPD lorsque celui-ci entrera en vigueur, en mai 2018.

Conformément à l'article 32, les responsables du traitement et les sous-traitants « mettent en œuvre les mesures techniques et organisationnelles appropriées », en tenant compte de « l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques ». Le RGPD fournit des suggestions précises des types d'actions de sécurité pouvant être nécessaires, ce qui comprend :

- la pseudonymisation et le chiffrement des données à caractère personnel ;
- des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
- des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

Le code de conduite CISPE

Le RGPD prévoit la possibilité d'homologuer des codes de conduite pour aider les responsables du traitement et les sous-traitants à démontrer leur respect des exigences et leur application de la bonne pratique. Un de ces codes en attente d'homologation officielle est le code de conduite CISPE pour les fournisseurs d'infrastructure de cloud (le « Code »). Le Code donne aux clients l'assurance que leur fournisseur de cloud utilise des normes de protection des données appropriées cohérentes avec le RGPD.

Voici quelques-uns des atouts de ce code de conduite :

- **Clarification des responsabilités de chacun en matière de protection des données.** Le code de conduite explique le rôle du fournisseur et du client selon le RGPD, notamment dans le contexte des services d'infrastructure cloud.
- **Le code de conduite établit les principes auxquels les fournisseurs doivent adhérer.** Le code de conduite développe des principes clés dans le cadre du RGPD sur les actions et les engagements précis que les fournisseurs devraient adopter afin d'aider leurs clients à satisfaire aux exigences de ce règlement. Les clients peuvent s'appuyer sur ces avantages concrets dans leurs propres stratégies de conformité et de protection des données.
- **Le code de conduite donne aux clients les informations de sécurité dont ils ont besoin pour prendre des décisions relatives à la conformité**. Le code de conduite exige que les fournisseurs soient transparents concernant les procédures utilisées pour respecter leurs engagements en matière de sécurité. Pour n'en citer que quelques-unes, ces procédures concernent le signalement des violations de données, la suppression des données et la sous-traitance par des tiers, ainsi que le respect des lois et des exigences des entités gouvernementales. Les clients peuvent utiliser ces informations pour bien comprendre les hauts niveaux de sécurité fournis.

Le 13 février 2017, AWS a déclaré qu'Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (Amazon S3), Amazon Relational Database Service (Amazon RDS), AWS Identity and Access Management (IAM), AWS CloudTrail et Amazon Elastic Block Store (Amazon EBS) sont entièrement conformes au Code (voir).https://cispe.cloud/publicregister Cette déclaration fournit aux clients l'assurance supplémentaire que, lorsqu'ils utilisent AWS, ils contrôlent complètement leurs données, dans un environnement sûr, sécurisé et conforme. Notre respect des exigences du Code s'ajoute à la longue liste des certifications et accréditations internationalement reconnues déjà obtenues par AWS, sur laquelle on retrouve les certifications ISO 27001, ISO 27018, ISO 9001, SOC 1, SOC 2, SOC 3, PCI DSS de niveau 1, et bien d'autres encore.

Contrôles d'accès aux données

L'article 25 du RGPD dispose que le responsable du traitement doit « mettre en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées ». Les mécanismes de contrôle d'accès AWS suivants vous aident à vous conformer à cette exigence en n'autorisant que les administrateurs, utilisateurs et applications autorisés à accéder aux ressources AWS et aux données clients :

- **Accès précis et fin aux objets AWS situés dans les compartiments S3/SQS/SNS et autres** : vous pouvez accorder différentes permissions, à différentes personnes, pour différentes ressources. Par exemple, vous pouvez accorder à certains utilisateurs un accès total à Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (Amazon S3), Amazon DynamoDB, Amazon Redshift et à d'autres services AWS Pour d'autres utilisateurs, vous pouvez accorder un accès en lecture seule à certains compartiments S3 ou l'autorisation d'administrer certaines instances EC2 seulement, ou encore un accès à vos informations de facturation uniquement.
- **Authentification à plusieurs facteurs (MFA)** : vous pouvez ajouter une authentification à deux facteurs à votre compte et aux utilisateurs individuels pour une sécurité renforcée. Avec l'authentification MFA, vos utilisateurs ou vous-même fournissez non seulement un mot de passe ou une clé d'accès pour utiliser votre compte, mais aussi un code généré par un périphérique configuré spécialement.
- **Authentification par demande API :** vous pouvez utiliser les fonctions IAM pour fournir de manière sécurisée aux applications s'exécutant sur des instances EC2 les informations d'identification dont elles ont besoin pour accéder à d'autres ressources AWS, comme les compartiments S3 et les bases de données RDS ou DynamoDB.
- **Restrictions géographiques :** vous pouvez utiliser la restriction géographique, également appelée « blocage géographique », pour empêcher les utilisateurs d'emplacements géographiques spécifiques d'accéder au contenu que vous distribuez via une distribution Web CloudFront. Pour utiliser la restriction géographique, vous avez deux options :

  - **La fonction de restriction géographique de CloudFront.** Elle permet de limiter l'accès à tous les fichiers associés à une distribution et pour limiter l'accès au niveau du pays.
  - **Un service de géolocalisation tiers.** Il permet de limiter l'accès à un sous-ensemble des fichiers associés à une distribution ou pour le limiter à un niveau de détail plus fin que le niveau pays.

- **Jetons d'accès temporaires par STS :** vous pouvez utiliser AWS Security Token Service (AWS STS) pour créer des utilisateurs approuvés et leur fournir des informations d'identification de sécurité temporaires pouvant contrôler l'accès à vos ressources AWS. Les informations d'identification de sécurité temporaires ont un fonctionnement presque identique à celui des informations d'identification des clés d'accès à long terme que vos utilisateurs IAM peuvent utiliser, à quelques différences près :
  - **Les informations d'identification de sécurité temporaires sont à court terme, comme leur nom l'indique.** Elles peuvent être configurées pour être valides de quelques minutes à plusieurs heures. Une fois que les informations d'identification arrivent à expiration, AWS ne les reconnaît plus ou n'autorise plus aucun accès aux demandes d'API effectuées avec elles.
  - **Les informations d'identification de sécurité temporaires ne sont pas stockées avec l'utilisateur, mais sont générées automatiquement et fournies à l'utilisateur sur demande.** Lorsque les informations d'identification de sécurité temporaires arrivent à expiration (ou même avant), l'utilisateur peut en demander de nouvelles, tant qu'il y est autorisé.

  Ces différences offrent les avantages suivants à utiliser des informations d'identification temporaires :

  - Vous n'avez pas besoin de distribuer ou d'intégrer des informations d'identification de sécurité AWS à long terme avec une application.
  - Vous pouvez fournir l'accès à vos ressources AWS aux utilisateurs sans devoir définir une identité AWS pour eux. Les informations d'identification temporaires servent de base aux rôles et à la fédération d'identité.

  - Les informations d'identification de sécurité temporaires ont une durée de vie limitée. Vous n'avez donc pas besoin de les faire tourner ou de les révoquer de manière explicite une fois celles-ci devenues inutiles. Une fois que les informations d'identification de sécurité temporaires arrivent à expiration, elles ne peuvent pas être réutilisées. Vous pouvez spécifier le délai de validité des informations d'identification, jusqu'à une certaine limite.

Surveillance et journalisation

Le RGPD exige que « [c]haque responsable du traitement et, le cas échéant, le représentant du responsable du traitement tiennent un registre des activités de traitement effectuées sous leur responsabilité ». Ces articles comprennent également des détails sur les informations devant être enregistrées. En d'autres termes, le RGPD exige que le traitement des données personnelles soit surveillé. De plus, l'obligation de signaler immédiatement toute violation des données fait qu'il est nécessaire de détecter ces incidents presque en temps réel. Pour vous aider à répondre à ces exigences, AWS offre plusieurs services de journalisation et de surveillance :

- **Gestion et configuration des ressources avec AWS Config :** AWS Config fournit une vue détaillée de la configuration des ressources AWS dans votre compte AWS. Elle indique comment les ressources sont liées entre elles et comment elles ont été configurées dans le passé, pour que vous puissiez observer comment les configurations et les relations changent au fil du temps.

  Une ressource AWS est une ressource avec laquelle vous pouvez travailler dans AWS, comme une instance Amazon Elastic Compute Cloud (EC2), un volume Amazon Elastic Block Store (EBS), un groupe de sécurité ou un Amazon Virtual Private Cloud (VPC) Pour une liste complète des ressources AWS prises en charge par AWS Config, consultez la page Types de ressource AWS pris en charge

  AWS Config vous permet de faire ce qui suit :

  - Évaluer les configurations de vos ressources AWS pour les paramètres de votre choix.
  - Obtenir un instantané des configurations actuelles des ressources prises en charge qui sont associées à votre compte AWS.

  - Récupérer des configurations d'une ou plusieurs des ressources qui existent dans votre compte.
  - Récupérer les historiques de configuration d'une ou plusieurs ressources.
  - Recevoir une notification chaque fois qu'une ressource est créée, modifiée ou supprimée.
  - Afficher les relations entre les ressources. Par exemple, vous pouvez vouloir rechercher toutes les ressources qui utilisent un groupe de sécurité particulier.

- **Audit de la conformité et analyses de sécurité avec AWS CloudTrail :** avec AWS CloudTrail, vous pouvez surveiller vos déploiements AWS dans le cloud en obtenant un historique des appels d'API AWS pour votre compte, notamment les appels d'API effectués via AWS Management Console, les AWS SDK, les outils de ligne de commande, ainsi que les services AWS de niveau plus élevé. Vous pouvez aussi identifier les utilisateurs et les comptes qui ont appelé les API AWS pour des services prenant en charge CloudTrail, l'adresse IP source d'origine des appels, ainsi que le moment où les appels ont eu lieu. Vous pouvez intégrer CloudTrail dans des applications utilisant l'API, automatiser la création de journaux de suivi pour votre organisation, vérifier le statut de vos journaux de suivi et contrôler de quelle manière des administrateurs activent et désactivent la journalisation de CloudTrail.
- **Identifications des problèmes de configuration via TrustedAdvisor :** la journalisation permet de faire en sorte que des journaux d'accès détaillés soient livrés dans un compartiment S3. Un enregistrement du journal d'accès contient des détails sur la demande, tels que le type de demande, les ressources spécifiées dans la demande utilisée, ainsi que l'heure et la date du traitement de la demande. Pour davantage d'informations sur les contenus d'un fichier journal, voir Format des journaux[1] d'accès au serveur dans le guide développeur Amazon Simple Storage Service.
- Les journaux d'accès au serveur sont utiles pour de nombreuses applications, car ils fournissent aux propriétaires du compartiment des renseignements sur la nature des demandes effectuées par les clients qu'ils ne contrôlent pas. Par défaut, Amazon S3 ne collecte pas les

journaux d'accès au service. Toutefois, lorsque vous activez la journalisation, S3 transmet les journaux d'accès à votre compartiment, et ce toutes les heures.

- Enregistrement très précis des accès aux objets S3.
- Informations détaillées sur les flux du réseau via VPC-FlowLogs.
- Vérifications et actions de configuration reposant sur des règles avec AWS Config Rules.
- Filtrage et surveillance de l'accès HTTP aux applications avec les fonctions WAF dans CloudFront.

Protéger vos données sur AWS

Le RGPD dispose que les organisations doivent « mett[re] en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris (…) la pseudonymisation et le chiffrement des données à caractère personnel (…) ». De plus, les organisations doivent protéger les données à caractère personnel contre toute divulgation ou tout accès non autorisés. Enfin, dans le cas où une violation des données à caractère personnel a eu lieu et peut conduire à un risque accru pour les droits et libertés des personnes physiques, mais que le responsable du traitement a mis en place des « mesures techniques et organisationnelles appropriées (…) comme le chiffrement », ce dernier ne doit pas notifier les sujets des données affectés de la violation et peut donc éviter de devoir payer des frais administratifs et de voir sa réputation en pâtir. AWS offre plusieurs mécanismes de chiffrement des données sûrs et hautement dimensionnables pour aider à protéger les données clients stockées et traitées sur AWS :

- **Chiffrement de vos données au repos avec AES256 (EBS/S3/Glacier/RDS) :** chiffrer les données au repos[2] est crucial pour le respect des exigences pour assurer que les données sensibles stockées sur des disques ne sont pas lisibles par des utilisateurs ou des applications sans une clé valide. AWS offre des options pour les données au repos et une gestion des clés pour prendre en charge le processus de chiffrement. Par exemple, vous pouvez chiffrer des volumes Amazon EBS et configurer des compartiments Amazon S3 pour un chiffrement côté serveur (SSE) en utilisant un chiffrement AES-256. De plus, Amazon RDS prend en charge le chiffrement transparent des données (Transparent Data Encryption ou TDE).

Le stockage d'instance fournit un stockage temporaire de niveau bloc aux instances Amazon EC2. Ce stockage se trouve sur des disques physiquement attachés à un ordinateur hôte. Le stockage d'instance est idéal pour stocker temporairement des données qui changent fréquemment, telles que des tampons, des caches ou des données temporaires. Par défaut, les fichiers stockés sur ces disques ne sont pas chiffrés.

- **Chiffrement de disque et de système de fichiers** : vous pouvez utiliser deux méthodes pour chiffrer des fichiers sur des stockages d'instance. La première méthode est le chiffrement de disque, qui consiste à chiffrer l'ensemble du disque ou du bloc dans le disque en utilisant une ou plusieurs clés de chiffrement. Le chiffrement de disque se fait sous le niveau du système de fichiers, ne dépend pas du système d'exploitation et cache les informations des répertoires et fichiers, comme leur nom et leur taille. Par exemple, l'Encrypting File System est une extension Microsoft pour le système New Technology File System (NTFS) du système d'exploitation Windows NT qui permet de chiffrer un disque.

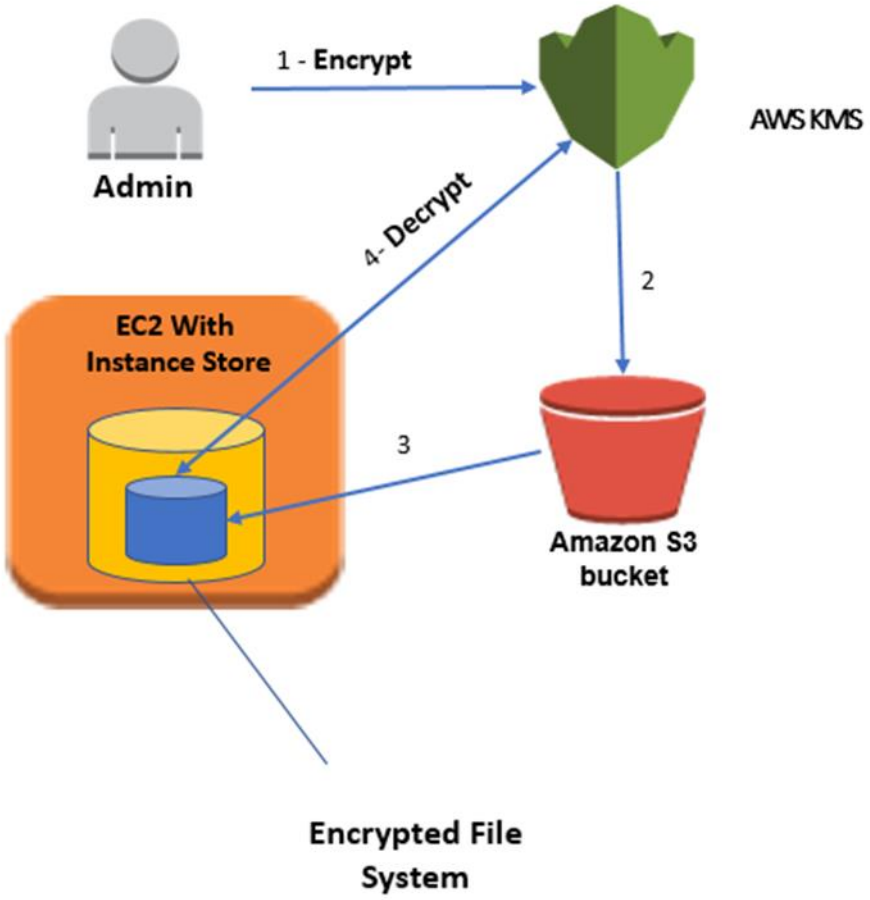
  La seconde méthode est le chiffrement au niveau du système de fichiers. Au lieu de chiffrer tout le disque ou toute la partition, on ne chiffre que les fichiers et les répertoires. Le chiffrement au niveau du système de fichiers fonctionne sur le système de fichiers et est portable sur différents systèmes d'exploitation.

- **L'infrastructure dm-crypt de Linux :** dm-crypt est un mécanisme de chiffrement du noyau Linux qui permet aux utilisateurs de monter un système de fichiers chiffré. Le montage d'un système de fichiers est le processus par lequel un système de fichiers est attaché à un répertoire (point de montage), ce qui le rend disponible pour le système d'exploitation. Après le montage, tous les fichiers dans le système de fichiers sont disponibles pour les applications sans interaction supplémentaire nécessaire. Cependant, ces fichiers sont chiffrés lorsqu'ils sont stockés sur un disque.

  L'outil de mappage des périphériques est une infrastructure des noyaux Linux 2.6 et 3.x qui fournit un moyen générique pour créer des couches virtuelles de périphériques de traitement par blocs. La cible crypt de l'outil de mappage des périphériques fournit un chiffrement transparent des périphériques de traitement par bloc en

utilisant l'API de chiffrement du noyau. La solution présentée ici utilise dm-crypt en combinaison avec un système de fichiers sur disque mappé à un volume logique par le Logical Volume Manager (LVM, gestionnaire des volumes logiques). Le LVM fournit une gestion des volumes logiques pour le noyau Linux.

- **Présentation de l'architecture :** le diagramme d'architecture de haut niveau suivant illustre la solution proposée pour activer le chiffrement des stockages d'instance EC2.



1. L'administrateur chiffre un mot de passe secret en utilisant KMS. Le mot de passe chiffré est stocké sur un fichier.
2. L'administrateur place le fichier contenant le mot de passe chiffré dans un compartiment S3.
3. Au moment du démarrage de l'instance, cette dernière copie le fichier chiffré dans un disque interne.

4. L'instance EC2 déchiffre ensuite le fichier en utilisant KMS et récupère le mot de passe en un format intelligible. Le mot de passe est utilisé pour configurer le système de fichiers chiffré Linux avec LUKS. Toutes les données écrites dans le système de fichiers chiffré sont chiffrées en utilisant un algorithme de chiffrement AES-256 lorsqu'elles sont stockées sur un disque.

- **Gestion des clés centralisée (par région)** :
  AWS Key Management Service (KMS) est un service géré qui vous permet de créer et de contrôler facilement les clés de chiffrement utilisées pour chiffrer vos données. Il utilise des modules de sécurité matériels (HSM) pour assurer la sécurité de vos clés.
  AWS Key Management Service est intégré à plusieurs autres services AWS afin de vous aider à protéger les données stockées avec ces services. AWS Key Management Service est également intégré à AWS CloudTrail pour vous fournir des journaux contenant des informations sur toutes les utilisations de vos clés, dans le but de vous aider à répondre à vos besoins en matière de réglementation et de conformité.
  - **Gestion des clés centralisée** : AWS Key Management Service vous offre un contrôle centralisé de vos clés de chiffrement. Créer, importer et opérer une rotation des clés, définir des politiques d'utilisation et vérifier l'usage : autant d'opérations faciles à réaliser via AWS Management Console, le kit SDK ou l'interface de ligne de commande AWS. Les clés principales dans KMS, qu'elles soient importées par vos soins ou créées pour vous par KMS, sont conservées dans un stockage hautement durable et dans un format chiffré, ce qui permet de les extraire si besoin. Vous pouvez configurer KMS afin qu'il effectue une rotation automatique des clés principales créées dans KMS une fois par an, sans que vous ayez à chiffrer de nouveau les données déjà chiffrées à l'aide de votre clé principale. Vous n'avez pas besoin de garder une trace des anciennes versions de vos clés principales, étant donné que KMS les conserve pour le déchiffrement des données préalablement chiffrées. Vous pouvez créer de nouvelles clés principales et contrôler qui peut avoir accès à ces clés et quels services peuvent être utilisés avec celles-ci quand vous le voulez. Vous pouvez aussi importer des clés à partir de votre propre infrastructure de gestion de clés et les utiliser dans KMS.

- **Intégration de service AWS** : AWS Key Management Service est intégré de manière transparente à plusieurs autres services AWS. Cette intégration signifie que vous pouvez utiliser les clés principales AWS KMS pour chiffrer les données stockées avec ces services. Vous pouvez utiliser une clé principale par défaut, qui est créée automatiquement pour vous et ne peut être utilisée qu'au sein du service intégré. Vous pouvez également sélectionner une clé principale personnalisée que vous avez auparavant créée dans KMS (ou importée à partir de votre propre infrastructure de gestion de clés) et que vous êtes autorisé à utiliser.
- **Capacité d'audit** : si vous avez activé AWS CloudTrail[3] pour votre compte AWS, chaque utilisation d'une clé stockée dans KMS est enregistrée dans un fichier journal qui est envoyé dans le compartiment Amazon S3 que vous avez sélectionné lors de l'activation d'AWS CloudTrail. Les informations enregistrées comprennent des détails concernant l'utilisateur, l'heure, la date et la clé utilisée.
- **Dimensionnement, durabilité et haute disponibilité** : AWS Key Management Service est un service géré. Si votre utilisation des clés de chiffrement AWS KMS augmente, vous n'avez pas à acheter une infrastructure de gestion de clés supplémentaire. AWS KMS effectue une mise à l'échelle automatique afin de répondre à vos besoins relatifs aux clés de chiffrement.

  Il n'est pas possible d'exporter les clés principales importées par vos soins ou créées pour vous par AWS KMS. AWS KMS enregistre plusieurs copies des versions chiffrées de vos clés dans des systèmes conçus pour fournir une durabilité de 99,999999999 % afin de vous assurer de la disponibilité de vos clés lorsque vous en avez besoin. Si vous importez des clés dans KMS, vous devez conserver une copie de ces clés de manière sécurisée afin de pouvoir les réimporter à tout moment.

  AWS KMS est déployé dans plusieurs zones de disponibilité à l'intérieur d'une région afin d'assurer une haute disponibilité de vos clés de chiffrement.
- **Sûr** : AWS KMS est conçu de telle sorte que personne n'ait accès à vos clés principales. Le service repose sur des systèmes conçus pour protéger vos clés principales à l'aide de techniques de renforcement

extensives. Il s'agit notamment d'éviter le stockage de clés principales intelligibles sur un disque dur ou leur conservation en mémoire, et de limiter le nombre de systèmes pouvant accéder aux hôtes qui utilisent les clés. Tout accès destiné à mettre à jour le logiciel sur le service fait l'objet d'un contrôle d'accès impliquant plusieurs parties, qui est vérifié et examiné par un groupe indépendant au sein d'Amazon.

Pour en savoir plus sur le fonctionnement du service AWS KMS, vous pouvez consulter le livre blanc AWS Key Management Service[4].

- **Tunnels IPsec vers AWS avec les passerelles VPN :** Amazon VPC vous permet d'allouer une section du cloud Amazon Web Services (AWS) isolée de manière logique, au sein de laquelle vous pouvez lancer des ressources AWS dans un réseau virtuel que vous définissez. Vous conservez ainsi la totale maîtrise de votre environnement de mise en réseau virtuel, y compris pour la sélection de votre propre plage d'adresses IP, la création de sous-réseaux et la configuration de tables de routage et de passerelles réseau. De plus, vous pouvez créer une connexion VPN (Virtual Private Network) matérielle entre le centre de données de votre entreprise et votre VPC, et exploiter le cloud AWS comme une extension de votre centre de données d'entreprise.

  Vous pouvez facilement adapter la configuration du réseau à votre instance Amazon VPC. Par exemple, vous pouvez créer un sous-réseau destiné au public pour vos serveurs Web : un sous-réseau qui a accès à Internet et place vos systèmes backend, comme les bases de données ou les serveurs d'application, dans un sous-réseau non destiné au public sans accès Internet. Vous pouvez exploiter plusieurs couches de sécurité, y compris les groupes de sécurité et les listes de contrôles d'accès au réseau, afin de renforcer le contrôle des accès aux instances Amazon EC2 dans chaque sous-réseau.

- **Modules HSM dédiés dans le cloud avec CloudHSM :** le service AWS CloudHSM vous permet de respecter les exigences professionnelles, contractuelles et réglementaires relatives à la sécurité des données en mettant à votre disposition des modules de sécurité matériels (HSM, Hardware Security Module) dédiés dans le cloud AWS. Grâce à CloudHSM, vous pouvez contrôler les clés et les opérations de chiffrement réalisées via HSM.

AWS et les partenaires AWS Marketplace proposent différentes solutions de protection des données sensibles sur la plate-forme AWS, mais dans le cas d'applications et de données soumises à des exigences contractuelles ou réglementaires très strictes en termes de gestion des clés cryptographiques, une protection supplémentaire peut s'avérer nécessaire. Jusqu'à maintenant, la seule option qui s'offrait à vous consistait à stocker les données sensibles (ou les clés de chiffrement protégeant ces données) dans vos centres de données sur site. Cependant, cette solution vous empêchait de procéder à la migration de ces applications vers le cloud, ou ralentissait fortement leurs performances. Le service AWS CloudHSM permet de protéger vos clés de chiffrement dans des HSM conformes aux normes gouvernementales relatives à la gestion sécurisée des clés. Vous pouvez générer, stocker et gérer de manière sécurisée les clés cryptographiques utilisées pour le chiffrement des données, afin d'être le seul à pouvoir y accéder. Avec AWS CloudHSM, vous êtes en mesure de respecter des exigences strictes en termes de gestion des clés sans que les performances de vos applications en pâtissent.

Le service AWS CloudHSM fonctionne avec Amazon Virtual Private Cloud (VPC). Les instances CloudHSM sont allouées dans votre VPC avec l'adresse IP que vous indiquez. Vous disposez ainsi d'une connexion réseau simple et privée pour vos instances
Amazon Elastic Compute Cloud (EC2). En plaçant les instances CloudHSM à proximité de vos instances EC2, vous réduisez la latence du réseau, ce qui permet d'améliorer les performances de vos applications. AWS fournit un accès dédié et exclusif (locataire unique) aux instances CloudHSM, isolé des autres clients AWS. Disponible dans différentes régions et zones de disponibilité (AZ), AWS CloudHSM vous permet de bénéficier d'un stockage durable et sécurisé de vos clés pour vos applications.

- **Intégré** : vous pouvez utiliser CloudHSM avec Amazon Redshift, Amazon Relational Database Service (RDS) Oracle ou des applications tierces telles que SafeNet Virtual KeySecure pour servir de racine de confiance, pour Apache (terminaison SSL) ou pour Microsoft SQL Server (chiffrement transparent des données). Vous pouvez également utiliser CloudHSM pour développer vos propres applications, tout en continuant à utiliser vos bibliothèques

cryptographiques standard habituelles, telles que PKCS#11, Java JCA/JCE, Microsoft CAPI et CNG.

- **Contrôlable** : si vous avez besoin de suivre l'évolution de vos ressources ou de vos activités d'audit à des fins de sécurité et de conformité, vous pouvez consulter tous les appels d'API CloudHSM effectués depuis votre compte via CloudTrail. De plus, vous pouvez contrôler les opérations effectuées sur l'appliance HSM via syslog, ou envoyer des messages de consignation syslog vers votre propre module de collecte.

Normes de sécurité et cadre de conformité solides

Conformément au RGPD, les mesures techniques et organisationnelles appropriées peuvent devoir comprendre « des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement » ainsi que des processus fiables de restauration, de test et de gestion des risques généraux. AWS vous offre un cadre de conformité fort et des normes de sécurité avancées.

Modèle de sécurité à responsabilité partagée

Avant d'entrer dans les détails de la sécurisation de vos données avec AWS, voyons en quoi la sécurité dans le cloud diffère légèrement de la sécurité des centres de données sur site. Lorsque vous transférez des systèmes informatiques et des données vers le cloud, les responsabilités en matière de sécurité sont partagées entre vous et le fournisseur de services de cloud. Dans le cas présent, les services AWS sont responsables de la sécurisation de l'infrastructure sous-jacente du cloud et vous êtes responsable de tout ce que vous placez dans le cloud ou que vous connectez au cloud. Ce modèle de responsabilité partagée en matière de sécurité peut réduire votre charge opérationnelle de nombreuses façons et, dans certains cas, peut même améliorer votre niveau de sécurité par défaut sans nécessiter d'action de votre part.

Responsabilités d'AWS en matière de sécurité

Amazon Web Services est responsable de la protection de l'infrastructure globale qui exécute tous les services offerts dans le cloud AWS. Cette

infrastructure est composée du matériel, des logiciels, des réseaux et des installations qui permettent l'exécution des services AWS. Protéger cette infrastructure est la priorité d'AWS et, bien que vous ne puissiez pas visiter nos centres de données ou bureaux pour voir cette protection de vos yeux, nous fournissons plusieurs rapports d'auditeurs tiers qui ont contrôlé notre respect des exigences de plusieurs normes et régulations en matière de sécurité informatique. Pour en savoir plus, consultez la page suivante : https://aws.amazon.com/compliance/.

Sachez que, outre la protection de cette infrastructure globale, AWS est responsable de la configuration de la sécurité de ses produits considérés comme des services gérés. Parmi les exemples de ces types de services, citons, entre autres, Amazon DynamoDB, Amazon RDS, Amazon Redshift, Amazon Elastic MapReduce, Amazon WorkSpaces. Ces services offrent l'évolutivité et la flexibilité de ressources basées sur le cloud, tout en présentant l'avantage d'être gérés. En ce qui concerne ces services, AWS gère les tâches de sécurité de base, telles que le système d'exploitation invité et l'application de correctifs de bases de données, la configuration du pare-feu et la reprise après sinistre. Pour la plupart de ces services gérés, il vous suffit de configurer les contrôles d'accès logiques pour les ressources et protéger les informations d'identification de votre compte. Un certain nombre d'entre eux peuvent nécessiter des tâches supplémentaires, comme la mise en place de comptes utilisateur pour la base de données, mais dans l'ensemble le travail de configuration de la sécurité est effectué par le service.

Responsabilités des clients en matière de sécurité

Grâce au cloud AWS, l'allocation des serveurs virtuels, du stockage, des bases de données et des ordinateurs de bureau ne vous prendra que quelques minutes, et non plus plusieurs semaines. Vous pouvez également utiliser des outils d'analyse et de flux de travail basés sur le cloud pour traiter vos données selon vos besoins, puis les stocker dans vos propres centres de données ou dans le cloud. Les services AWS que vous utilisez déterminent le niveau de travail de configuration que vous devez assumer dans le cadre de vos responsabilités de sécurité.

Les produits AWS entrant dans la catégorie bien connue de l'infrastructure en tant que service (IaaS)—tels qu'Amazon EC2, Amazon VPC et Amazon S3—sont entièrement sous votre contrôle et nécessitent que vous réalisiez toutes les

tâches de configuration et de gestion de la sécurité nécessaires. Par exemple, pour les instances EC2, vous êtes responsable de la gestion du système d'exploitation invité (notamment les mises à jour et les correctifs de sécurité), de tous logiciels ou utilitaires que vous installez sur les instances, ainsi que de la configuration du pare-feu fourni par AWS (appelé groupe de sécurité) sur chaque instance. Ces tâches sont fondamentalement les mêmes tâches de sécurité que celles que vous avez l'habitude de faire, peu importe où vos serveurs se situent.

Les services gérés AWS (AWS Managed Services) tels qu'Amazon RDS ou Amazon Redshift fournissent toutes les ressources dont vous avez besoin pour effectuer une tâche donnée, mais sans le travail de configuration généralement associé. Grâce aux services gérés, vous n'avez pas à vous soucier du lancement et de la maintenance des instances, de l'application de correctifs sur le système d'exploitation invité ou la base de données, ou de la réplication des bases de données ; AWS gère tout cela à votre place. Cependant, comme avec tous les services, vous devez protéger les informations d'identification de votre compte AWS et configurer des comptes d'utilisateurs individuels avec Amazon Identity and Access Management (IAM), de sorte que chacun de vos utilisateurs dispose de ses propres informations d'identification et que vous puissiez mettre en place une séparation des fonctions. Nous recommandons également d'utiliser la Multi-Factor Authentication (MFA) avec chaque compte, qui implique d'utiliser SSL/TLS pour communiquer avec vos ressources AWS et de configurer la consignation de l'activité de l'API/des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur les mesures supplémentaires que vous pouvez prendre, consultez le livre blanc Bonnes pratiques relatives à la sécurité AWS et la littérature recommandée sur la page Web sur les ressources de sécurité AWS

Programme de conformité AWS

Le programme de conformité Amazon Web Services vous permet de comprendre les contrôles de sécurité renforcés dans AWS destinés à assurer la sécurité et la protection des données dans le cloud. Lorsque des systèmes sont créés sur l'infrastructure cloud AWS, les responsabilités en termes de conformité sont partagées. En reliant les fonctions de service axées sur la gouvernance, propices aux audits, aux normes de conformité ou d'audit en vigueur, les aides à la conformité d'AWS s'appuient sur des programmes classiques pour vous aider à construire et à opérer dans un environnement de contrôle de sécurité AWS. L'infrastructure informatique qu'AWS vous fournit

est conçue et gérée conformément aux bonnes pratiques de sécurité et à une grande variété de normes de sécurité informatique, ce qui comprend :

- SOC 1/SSAE 16/ISAE 3402 (anciennement SAS 70)
- SOC 2
- SOC 3
- FISMA, DIACAP et FedRAMP
- DOD CSM, niveaux 1-5
- PCI DSS, niveau 1
- ISO 9001/ISO 27001
- ITAR
- FIPS 140-2
- MTCS, niveau 3

En outre, la flexibilité et le contrôle fournis par la plate-forme AWS vous permettent de déployer des solutions qui correspondent à plusieurs normes propres au secteur, notamment :

- Les services Criminal Justice Information Services (CJIS)
- Cloud Security Alliance (CSA)
- Loi américaine Family Educational Rights and Privacy Act (FERPA)
- La loi américaine Health Insurance Portability and Accountability Act (HIPAA)
- Motion Picture Association of America (MPAA)

AWS fournit à ses clients une grande variété d'informations concernant son environnement de contrôle informatique par le biais de livres blancs, rapports, certifications, accréditations, ainsi que d'attestations délivrées par des organismes tiers. Le livre blanc Risque et sécurité, disponible à l'adresse http://aws.amazon.com/compliance/, fournit davantage d'informations à ce sujet.

Cloud Computing Compliance Controls Catalog (C5 – programme d'attestation de conformité approuvé par le gouvernement allemand)

Cloud Computing Compliance Controls Catalog (C5)[5] est un programme d'attestation du gouvernement allemand. Implémenté en Allemagne par l'Office fédéral de la sécurité des technologies de l'information (BSI), son objectif est d'aider les organisations à démontrer leur sécurité opérationnelle contre les cyber-attaques courantes dans le cadre des « recommandations de sécurité pour les fournisseurs de cloud[6] » du gouvernement allemand.

L'attestation C5 peut être utilisée par les clients d'AWS et par leurs consultants de conformité pour mieux comprendre la gamme de services d'assurance de sécurité informatique proposés par AWS pour la migration de leurs charges de travail dans le cloud. La norme C5 comprend un niveau de sécurité informatique équivalent à IT-Grundschutz et intègre des contrôles spécifiques au cloud.

La norme C5 inclut des contrôles supplémentaires qui informent sur la localisation des données, l'allocation de service, la juridiction, les certifications existantes, les obligations de transparence et la description du service dans son ensemble. Grâce à ces informations, les clients sont en mesure d'évaluer les réglementations juridiques (relatives à la confidentialité des données, par exemple), leurs propres politiques et les risques d'attaques dans le cadre de leur utilisation des services de cloud computing.

Révisions du document

Date	Description
Novembre 2017	Première publication

Notes

[1] http://docs.aws.amazon.com/AmazonS3/latest/dev/LogFormat.html

[2] https://do.awsstatic.com/whitepapers/AWS_Securing_Data_at_Rest_with_Encryption.pdf

[3] https://aws.amazon.com/cloudtrail/

[4] https://do.awsstatic.com/whitepapers/KMS-Cryptographic-Details.pdf

[5] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/ComplianceControlsCatalogue.pdf;jsessionid=E5F009E49EB2689FAC3705578821BCB6.2_cid286?__blob=publicationFile&v=3

[6] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CloudComputing/SecurityRecommendationsCloudComputingProviders.pdf?__blob=publicationFile&v=2