Gérer la conformité au RGPD sur AWS

Décembre 2020

Mentions légales

Les clients sont responsables de leur propre évaluation indépendante des informations contenues dans ce document. Le présent document : (a) est fourni à titre informatif uniquement, (b) représente les offres et pratiques actuelles de produits AWS, qui sont susceptibles d’être modifiées sans préavis, et (c) ne crée aucun engagement ou assurance de la part d’AWS et de ses affiliés, fournisseurs ou concédants de licences. Les produits ou services AWS sont fournis « en l’état » sans garantie, représentation ou condition, de quelque nature que ce soit, explicite ou implicite. Les responsabilités et obligations d’AWS envers ses clients sont déterminées par les contrats AWS, et le présent document ne fait pas partie d’un contrat entre AWS et ses clients, ni ne le modifie.

Table des matières

Résumé

Le présent document fournit des informations à propos des services et ressources qu'Amazon Web Services (AWS) offre à ses clients pour les aider à s'aligner sur les exigences du Règlement général sur la protection des données (RGPD) qui pourraient s'appliquer à leurs activités. Ces services et ressources comprennent l'adhésion aux normes de sécurité informatique, l'attestation du catalogue de contrôle de conformité de l'informatique en nuage (Cloud Computing Compliance Controls Catalog, C5) d'AWS, l'adhésion au Code de conduite des fournisseurs européens de service d'infrastructure cloud (Cloud Infrastructure Services Providers, CISPE), les contrôles des accès aux données, les outils de surveillance et de journalisation, le chiffrement et la gestion de clé.

Règlement général sur la protection des données : aperçu

Le Règlement général sur la protection des données (RGPD) est une norme européenne de confidentialité[1] (Règlement (UE) 2016/679 du Parlement européen et du Conseil européen du 27 avril 2016[2]), entrée en vigueur le 25 mai 2018. Le RGPD remplace la directive européenne sur la protection des données (Directive 95/46/CE) et a pour but d'harmoniser la législation relative à la protection des données dans l'Union européenne (UE) en appliquant un même cadre juridique contraignant de protection des données dans tous les États membres.

Le RGPD s'applique à toutes les entreprises établies dans l'Union et aux entreprises, établies ou non dans l'Union, qui traitent les données à caractère personnel des personnes concernées qui se trouvent dans l'Union dans le cadre de l'offre de biens ou de services aux personnes concernées qui se trouvent dans l'Union ou du suivi du comportement de ces personnes au sein de l'Union. Les données à caractère personnel comprennent toute information liée à une personne physique identifiable ou identifiée.

Modifications apportées par le RGPD aux entités qui mènent leurs activités dans l'Union européenne

L'un des aspects clés du RGPD est l'harmonisation de la manière dont les États membres de l'Union européenne traitent, utilisent et échangent les données à caractère personnel en toute sécurité. Les organisations doivent démontrer en permanence la cybersécurité des données traitées ainsi que leur conformité au RGPD, en mettant en œuvre et en révisant régulièrement les mesures techniques et organisationnelles, ainsi que les politiques de conformité applicables au traitement des données à caractère personnel. Les autorités de contrôle de l'UE sont en mesure de sanctionner à hauteur de 20 millions d'euros (EUR) ou 4 % du chiffre d'affaire annuel mondial, en fonction de la valeur la plus élevée, en cas de violation du RGPD.

Préparation d'AWS pour le RGPD

Les experts de la conformité, de la protection des données et de la sécurité d'AWS travaillent avec leurs clients du monde entier pour répondre à leurs questions et pour les aider à préparer leur migration vers le cloud selon les exigences du RGPD. Ces équipes examinent également le niveau de préparation d'AWS par rapport aux critères du RGPD.

> *Nous confirmons que tous les services AWS peuvent être utilisés en conformité avec le RGPD.*

Addendum AWS en matière de traitement des données (Data Processing Addendum, DPA)

AWS propose un addendum en matière de traitement des données qui répond aux exigences du RGPD (GDPR DPA). L'AWS GDPR DPA est intégré aux Conditions de service AWS et s'applique automatiquement à tous les clients du monde entier qui en ont besoin pour se conformer au RGPD.

Le 16 juillet 2020, la Cour de justice de l'Union européenne (CJUE) a rendu un arrêt relatif au bouclier de protection des données UE-États-Unis et aux clauses contractuelles types (CCT), également appelées « clauses types ». La CJUE a statué que le bouclier de protection des données UE-États-Unis n'est plus valide pour le transfert de données à caractère personnel depuis l'Union vers les États-Unis. Toutefois, dans la même décision, la CJUE a confirmé que les entreprises peuvent continuer à utiliser les clauses types comme mécanisme de transfert de données en dehors de l'UE.

D'après cet arrêt, les clients et partenaires AWS peuvent continuer à utiliser AWS pour transférer leur contenu depuis l'Union européenne vers les États-Unis et autres pays tiers, dans le respect de la législation de l'UE en matière de protection des données à caractère personnel, y compris du Règlement général sur la protection des données (RGPD). Les clients AWS peuvent s'appuyer sur les clauses types incluses dans l'addendum AWS en matière de traitement des données s'ils choisissent de transférer leurs données en dehors de l'Union européenne en conformité avec le RGPD. Au fur et à mesure que le paysage réglementaire et législatif évolue, nous veillerons à ce que nos clients et partenaires puissent continuer à profiter des avantages d'AWS là où ils mènent leurs activités. Pour davantage d'informations, consultez les questions fréquentes (FAQ) sur le bouclier de protection des données UE-États-Unis.

Le rôle d'AWS dans le cadre du RGPD

AWS fait à la fois office de sous-traitant et de responsable du traitement des données dans le cadre du RGPD.

En vertu de l'article 32, les responsables du traitement et les sous-traitants sont tenus de « mettre en œuvre des 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 concernant les types d'actions de sécurité potentiellement nécessaires, notamment :

- 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.

AWS agissant en qualité de sous-traitant des données

Lorsque les clients et les membres du Réseau Partenaires AWS (APN) utilisent les services AWS pour traiter des données personnelles dans leur contenu, AWS agit en qualité de sous-traitant de ces données. Les clients et membres du Réseau Partenaires AWS (APN) peuvent utiliser les contrôles disponibles au sein des services AWS, notamment les contrôles de configuration de la sécurité, pour le traitement des données à caractère personnel. Dans ces circonstances, le client ou le membre du Réseau Partenaires AWS (APN) peut agir en qualité de responsable du traitement des données ou de sous-traitant, et AWS agit en qualité de sous-traitant. L'addendum AWS en matière de traitement des données respectant le RGPD (DPA) intègre les engagements d'AWS en qualité de sous-traitant des données.

AWS en qualité de responsable du traitement des données

Lorsqu'AWS collecte des données à caractère personnel et détermine les finalités et les moyens du traitement desdites données, AWS agit en qualité de responsable du traitement de ces données. Par exemple, lorsqu'AWS traite les informations relatives à l'enregistrement d'un compte, son administration, l'accès aux services ou les coordonnées liées au compte AWS afin de fournir une assistance par le biais du service clientèle, il agit en tant que responsable du traitement des données.

Modèle de responsabilité de sécurité partagée

La sécurité et la conformité sont des responsabilités partagées entre AWS et le client. Lorsque nos clients transfèrent leurs systèmes d'information et leurs données vers le cloud, les responsabilités en matière de sécurité sont partagées entre le client et le fournisseur de services cloud. Lorsque les clients migrent vers le Cloud AWS, AWS est responsable de la protection de l'infrastructure mondiale qui génère tous les services offerts dans le Cloud AWS. Pour les services abstraits, tels qu'Amazon S3 et Amazon DynamoDB, AWS est également responsable de la sécurité du système d'exploitation et de la plateforme. Les clients et les partenaires APN, agissant en tant que responsables du traitement des données ou en tant que sous-traitants, sont

responsables de tout ce qu'ils stockent dans le cloud ou connectent au cloud. La différentiation de la responsabilité est couramment résumée comme étant la sécurité *du* cloud, par rapport à la sécurité *dans* le cloud. Ce modèle partagé peut aider à réduire le poids opérationnel pesant sur les clients et leur apporter la flexibilité et les contrôles nécessaires pour déployer leur infrastructure dans le Cloud AWS. Pour plus d'informations, consultez le Modèle de responsabilité partagée AWS.

Le RGPD ne modifie pas le modèle de responsabilité partagée AWS, qui continue d'être pertinent pour les clients et les partenaires APN qui se concentrent sur l'utilisation des services d'informatique en nuage. Le modèle de responsabilité partagée est une approche utile pour illustrer les différentes responsabilités d'AWS (en tant que sous-traitant de données) et des clients ou partenaires APN (en tant que responsables du traitement des données ou sous-traitants de données) en vertu du RGPD.

Normes de sécurité et cadre de conformité stricte

En vertu du RGPD, les mesures techniques et organisationnelles appropriées sont susceptibles d'inclure « 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 procédures fiables de restauration, de test et de gestion globale des risques.

Programme de conformité AWS

AWS maintient en permanence un niveau élevé de sécurité et de conformité dans l'ensemble de ses opérations mondiales. La sécurité est depuis toujours notre priorité absolue et passe avant tout le reste. AWS se soumet régulièrement à des audits d'attestation indépendants conduits par des tiers afin de garantir le bon fonctionnement de ses activités de contrôle. Plus précisément, AWS est audité par rapport à différents cadres de sécurité mondiaux et régionaux, selon la région et le secteur. Actuellement, AWS participe à plus de 50 programmes d'audit différents.

Les résultats de ces audits sont répertoriés par l'organisme d'évaluation et mis à la disposition de tous les clients AWS via AWS Artefact. AWS Artefact est un portail libre-service gratuit qui permet d'accéder sur demande aux rapports de conformité AWS. Lorsque de nouveaux rapports sont publiés, ils sont accessibles de manière instantanée via AWS Artefact, ce qui permet aux clients de suivre en permanence la sécurité et la conformité d'AWS.

Les clients peuvent tirer parti des certifications et accréditations internationalement reconnues en démontrant leur conformité aux normes internationales strictes, telles que la norme ISO 27017 relative à la sécurité de l'information du cloud, ISO 27018 relative à la protection des données personnelles dans le cloud, SOC 1, SOC 2 et SOC 3, PCI DSS niveau 1, etc. AWS aide également les clients à respecter les normes de sécurité locales telles que le Catalogue de contrôles de conformité de l'informatique en nuage (Cloud Computing Compliance Controls Catalog, C5) de l'Office fédéral de la sécurité des technologies de l'information (BSI), une attestation soutenue par le gouvernement allemand.

Pour plus d'informations sur les programmes de certification AWS, les rapports et les attestations tierces, consultez les Programmes de conformité AWS. Pour plus d'informations relatives à un service précis, consultez les Services AWS concernés.

Catalogue des contrôles de conformité de l'informatique en nuage

Le catalogue des contrôles de conformité de l'informatique en nuage (Cloud Computing Compliance Controls Catalog, C5) est un programme de certification soutenu par le gouvernement allemand qui a été lancé en Allemagne par l'Office fédéral de la sécurité des technologies de l'information (BSI). Il a été créé pour aider les organisations à démontrer leur sécurité opérationnelle contre les cyber-attaques courantes dans le cadre des *Recommandations de sécurité pour les fournisseurs de service de cloud* du gouvernement allemand.

Les mesures techniques et organisationnelles de protection des données et les mesures de cybersécurité de l'information mettent l'accent sur la cybersécurité des données pour garantir la confidentialité, l'intégrité et la disponibilité de celles-ci. Le catalogue C5 définit des exigences de sécurité qui sont également pertinentes pour la protection des données. Les clients AWS et leurs consultants de conformité peuvent se servir du catalogue C5 pour comprendre l'offre de services d'assurance de sécurité informatique que propose AWS lors de la migration des charges de travail vers le cloud. Le catalogue C5 comprend un niveau de sécurité informatique équivalent au système de protection informatique IT-Grundschutz et intègre des contrôles spécifiques au cloud.

Le catalogue C5 inclut des contrôles supplémentaires qui informent sur la localisation des données, l'allocation de service, la juridiction compétente, les certifications existantes, les obligations de transparence et la description du service dans son ensemble. Grâce à ces informations, vous êtes en mesure d'évaluer les réglementations juridiques (relatives à la confidentialité des données, par exemple), vos propres politiques ou l'environnement de risque relatif à votre utilisation de services d'informatique en nuage.

Le code de conduite CISPE

Le RGPD envisage d'approuver des codes de conduite afin d'aider les responsables du traitement des données et les sous-traitants à démontrer leur respect de la règlementation. Le *code de conduite CISPE pour les fournisseurs d'infrastructure de cloud* (le « *Code* » ci-après)[3] fait partie des codes en attente d'homologation officielle par les autorités européennes de protection des données. Le Code de conduite CISPE aide les clients du cloud à s'assurer que leur fournisseur d'infrastructure cloud utilise des normes de protection des données appropriées afin de protéger leurs données en conformité avec le RGPD. Ci-après quelques atouts principaux du Code :

- **Il clarifie les responsabilités pour chaque point de la protection des données** : le Code explique le rôle du fournisseur de cloud et du client selon le RGPD, notamment dans le contexte des services d'infrastructure cloud.

- **Il définit les principes qui doivent être respectés par les fournisseurs** : le Code expose des principes clés dans le cadre du RGPD sur les actions et les engagements précis que les fournisseurs doivent adopter afin de démontrer leur conformité au RGPD et d'aider leurs clients à respecter ce règlement. Les clients peuvent s'appuyer sur ces points concrets dans leurs propres stratégies de conformité et de protection des données.
- **Il donne aux clients les informations concernant la sécurité et la confidentialité dont ils ont besoin pour atteindre leurs objectifs en matière de conformité** : le Code exige des fournisseurs qu'ils soient transparents au sujet des mesures qu'ils adoptent pour respecter leurs engagements de sécurité et de confidentialité. Par exemple, la mise en place de mesures de sauvegarde de sécurité et de confidentialité, de notifications de violation de données, d'effacement de données et de transparence en cas de sous-traitance par des tiers. Tous ces engagements sont vérifiés par des entités de contrôle tierces et indépendantes. Les clients peuvent utiliser ces informations pour pleinement comprendre les niveaux élevés de sécurité fournis.

Pour plus d'informations, consultez le Registre public CISPE (CISPE Public Register), qui fournit aux clients AWS une garantie supplémentaire selon laquelle ils contrôlent leurs données dans un environnement sûr, sécurisé et conforme lorsqu'ils utilisent AWS. La conformité d'AWS au Code s'ajoute à la liste des certifications et accréditations de renommée internationale obtenues par AWS. Celles-ci comprennent entre autres ISO 27001, ISO 27018, ISO 9001, SOC 1, SOC 2, SOC 3, PCI DSS niveau 1.

Contrôles d'accès aux données

L'article 25 du RGPD indique que le responsable du traitement est tenu de « [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 aident les clients à se conformer à cette exigence en n'autorisant que les administrateurs, utilisateurs et applications autorisés à accéder aux ressources AWS et aux données clients.

AWS Identity and Access Management (AWS IAM)

Lorsque vous créez un compte AWS, un compte utilisateur *root* (racine) est créé automatiquement pour votre compte AWS. Ce compte utilisateur possède un accès complet à tous vos services et ressources AWS dans votre compte AWS. Au lieu d'utiliser ce compte pour vos tâches quotidiennes, vous devez l'utiliser uniquement au début pour créer des rôles et comptes utilisateurs supplémentaires et pour les activités administratives qui le nécessitent. AWS vous recommande d'appliquer le principe du moindre privilège dès le début : définissez différents comptes utilisateurs et rôles pour

différentes tâches et indiquez l'ensemble minimal de permissions requises pour effectuer chaque tâche. Cette approche est un mécanisme affiné pour se conformer à un concept central du RGPD : la protection des données dès la conception (« by design »). AWS Identity and Access Management (IAM) est un service Web que vous pouvez utiliser pour contrôler de façon sécurisée l'accès à vos ressources AWS.

Les utilisateurs et les rôles définissent des identités IAM qui détiennent des permissions spécifiques. Un utilisateur autorisé peut endosser un rôle IAM pour effectuer des tâches spécifiques. Les informations d'identification temporaires sont créées lorsque le rôle est endossé. Par exemple, vous pouvez utiliser des rôles IAM pour fournir en toute sécurité des applications exécutées dans Amazon Elastic Compute Cloud (Amazon EC2) avec des informations d'identification temporaires requises pour accéder à d'autres ressources AWS, telles qu'Amazon S3 et les bases de données Amazon Relational Database Service (Amazon RDS) ou Amazon DynamoD. De même, les rôles d'exécution fournissent aux fonctions AWS Lambda les autorisations requises pour accéder à d'autres services et ressources AWS, tels que les journaux Amazon CloudWatch pour la diffusion en continu de journaux ou la lecture d'un message à partir d'une file d'attente Amazon Simple Queue Service (Amazon SQS). Lorsque vous créez un rôle, vous y ajoutez des stratégies pour définir des autorisations.

Pour aider les clients à surveiller les stratégies de ressources et à identifier les ressources qui disposent d'un accès public ou inter-comptes non désiré, IAM Access Analyzer peut être activé pour générer des résultats complets qui identifient les ressources accessibles depuis l'extérieur d'un compte AWS. IAM Access Analyzer évalue les stratégies de ressources à l'aide de la logique mathématique et de l'inférence pour déterminer les chemins d'accès possibles autorisés par ces stratégies. IAM Access Analyzer surveille en permanence les nouvelles stratégies ou mises à jour et analyse les autorisations accordées à l'aide de stratégies appliquées aux rôles IAM, mais aussi pour les ressources de services comme les compartiments Amazon S3, les clés AWS Key Management Service (AWS KMS), les files d'attente Amazon SQS et les fonctions Lambda.

Access Analyzer pour S3 vous avertit lorsque des compartiments S3 sont configurés pour permettre l'accès à toute personne à partir d'Internet ou d'autres comptes AWS, y compris les comptes AWS qui n'appartiennent pas à votre organisation. Lorsque vous examinez un compartiment à risque dans Access Analyzer pour S3, vous pouvez bloquer tout accès public au compartiment en un seul clic. AWS vous recommande de bloquer tout accès à vos compartiments, sauf si vous avez besoin d'un accès public pour prendre en charge un cas d'utilisation spécifique. Avant de bloquer tout accès public, assurez-vous que vos applications continueront à fonctionner correctement sans accès public. Pour plus d'informations, consultez L'option blocage d'accès public d'Amazon S3 (Amazon S3 Block Public Access).

IAM fournit également les dernières informations consultées pour vous aider à repérer les autorisations inutilisées et ainsi à les supprimer des entités associées. En utilisant les dernières informations consultées, il est possible d'affiner vos stratégies et

d'autoriser l'accès uniquement aux services et aux actions nécessaires. Cela aide à mieux respecter et appliquer les bonnes pratiques du moindre privilège. Vous pouvez afficher les dernières informations consultées pour les entités ou les stratégies qui existent dans IAM ou dans tout un environnement AWS Organisations.

Jetons d'accès temporaires via AWS STS

Vous pouvez utiliser le service AWS Security Token Service (AWS STS) pour créer et fournir à des utilisateurs de confiance des informations d'identification de sécurité temporaires qui leur donnent accès à vos ressources AWS. Les informations d'identification de sécurité temporaires fonctionnent sensiblement de la même manière que les informations d'identification de clé d'accès à long terme que vous fournissez à vos utilisateurs IAM, à ceci près :

- Les informations d'identification de sécurité temporaires sont conçues pour une utilisation à court terme. Vous pouvez configurer la durée pendant laquelle elles sont valides, de 15 minutes à une période maximale de 12 heures. Une fois que les informations d'identification temporaires 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 conservées avec le compte utilisateur. Elles sont générées de manière dynamique et fournies à l'utilisateur à sa requête. Lorsque (ou avant que) les informations d'identification de sécurité temporaires expirent, un utilisateur peut demander de nouvelles informations d'identification, s'il en a la permission.

Ces différences offrent les avantages suivants lorsque vous utilisez 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.
- Les informations d'identification temporaires servent de base aux rôles et à la fédération d'identité. Vous pouvez fournir à des utilisateurs l'accès à vos ressources AWS en définissant une identité AWS temporaire pour eux.
- Les informations d'identification de sécurité temporaires disposent d'une durée de vie limitée personnalisable. Cette caractéristique signifie que vous n'avez pas besoin d'effectuer une rotation ou de les révoquer explicitement lorsqu'elles ne sont plus nécessaires. Une fois que les informations d'identification de sécurité temporaires arrivent à expiration, elles ne peuvent pas être réutilisées. Vous pouvez indiquer la durée maximale de validité des informations d'identification temporaires.

Authentification multi-facteurs, MFA

Pour plus de sécurité, vous pouvez ajouter l'authentification à deux facteurs à votre compte AWS et à certains utilisateurs IAM. Avec l'activation de l'authentification multi-facteurs (MFA), lorsque vous vous connectez à AWS Management Console, il vous sera demandé votre identifiant et mot de passe (premier facteur), ainsi qu'une réponse d'authentification provenant de votre appareil MFA AWS (second facteur). Vous pouvez activer MFA pour votre compte AWS et pour les utilisateurs individuels IAM que vous avez créés dans votre compte. Vous pouvez également utiliser MFA pour contrôler l'accès aux API du service AWS.

Par exemple, vous pouvez définir une stratégie permettant un accès complet à toutes les opérations API AWS dans EC2, mais qui rejette explicitement l'accès à des opérations spécifiques d'API (comme `StopInstances` et `TerminateInstances`) si l'utilisateur n'est pas authentifié au moyen d'une MFA.

```
        {
          "Version": "2012-10-17",
          "Statement": [
              {
                 "Sid": "AllowAllActionsForEC2",
                 "Effect": "Allow",
                 "Action": "ec2:*",
                 "Resource": "*"
              },
             {
                 "Sid": "DenyStopAndTerminateWhenMFAIsNotPResent",
                 "Effect": "Deny",
                 "Action": [
                     "ec2:StopInstances",
                     "ec2:TerminateInstances"
                ],
                 "Resource": "*",
                 "Conditions": {
                    "BoolIfExists":
{"aws:MultiFactorAuthPresent":false}
                 }
             }
        }
}
```

Pour ajouter un degré de sécurité supplémentaire à vos compartiments S3, vous pouvez configurer la suppression MFA (MFA Delete), qui nécessite une authentification

supplémentaire pour modifier l'état de version d'un compartiment et supprimer définitivement une version d'objet. La fonction MFA Delete fournit une sécurité supplémentaire en cas de compromission de vos informations d'identification de sécurité.

Pour utiliser MFA Delete, vous pouvez utiliser un périphérique MFA virtuel ou matériel pour générer un code d'authentification. Consultez la page Authentification multi-facteurs pour obtenir la liste des périphériques MFA virtuels ou matériels pris en charge

Accès aux ressources AWS

Pour mettre en œuvre un accès précis et fin à vos ressources AWS, vous pouvez accorder différents niveaux de permission à différentes personnes pour différentes ressources. Par exemple, vous pouvez autoriser seulement certains utilisateurs à accéder à EC2, S3, DynamoDB, Amazon Redshiftet d'autres services AWS.

Vous pouvez accorder à d'autres utilisateurs l'accès en lecture seule à certains compartiments Amazon S3 ou l'autorisation d'administrer seulement certaines instances EC2, ou encore l'accès à vos informations de facturation uniquement.

La stratégie suivante est un exemple d'une méthode que vous pouvez utiliser pour permettre toutes les actions dans un compartiment Amazon S3 spécifique et refuser explicitement l'accès à tous les services AWS qui ne font pas partie d'Amazon S3.

```
{
         "Version": "2012-10-17",
         "Statement": [
             {
                "Effect": "Allow",
                "Action": "s3:*",
                "Resource": [
                     "arn:aws:s3:::bucket-name",
                     "arn:aws:s3:::bucket-name/*"
                 ],
              },
              {
                "Effect": "Deny",
                "NotAction": "s3:*",
                "NotResource": [
                     "arn:aws:s3:::bucket-name",
                     "arn:aws:s3:::bucket-name/*"
                 ]
               }
            ]
}
```

Vous pouvez associer une stratégie à un compte utilisateur ou à un rôle. Pour d'autres exemples de stratégies IAM, consultez les Stratégies basées sur une identité IAM d'exemple.

Définir les limites de l'accès aux services régionaux

En tant que client, vous conservez la propriété de votre contenu et vous sélectionnez quels services AWS peuvent traiter, stocker et héberger votre contenu. AWS n'accède pas à votre contenu ni ne l'utilise, à quelque fin que ce soit, sans votre consentement. Sur la base du modèle de responsabilité partagée, vous choisissez les régions AWS dans lesquelles votre contenu est stocké, ce qui vous permet de déployer des services AWS aux emplacements de votre choix, en fonction de vos besoins géographiques spécifiques. Par exemple, si vous souhaitez vous assurer que votre contenu se trouve uniquement en Europe, vous pouvez choisir de déployer des services AWS exclusivement dans l'une des régions AWS européennes.

Les stratégies IAM fournissent un mécanisme simple pour limiter l'accès aux services dans des régions particulières. Vous pouvez ajouter une condition globale (*aws:RequestedRegion* (région demandée)) aux stratégies IAM attachées à vos entités IAM afin de l'appliquer à tous les services AWS. Par exemple, la stratégie suivante utilise l'élément `NotAction (Pas d'action)` avec l'effet `Deny (Refuser)`, qui refuse explicitement l'accès, si la région demandée n'est pas européenne, à toutes les actions non répertoriées dans l'énoncé. Les actions dans les services CloudFront, IAM, Amazon Route 53 et AWS Support ne doivent pas être refusées car il s'agit de services AWS mondiaux et répandus.

```
{
          "Version": "2012-10-17",
          "Statement": [
              {
                 "Sid": "DenyAllOutsideRequestedRegions",
                 "Effect": "Deny",
                 "NotAction": [
                      "cloudfront:*",
                      "iam:*",
                      "route53:*",
                      "support:*"
                  ],
                  "Resource": "*",
                  "Condition": {
                     "StringNotLike": {
                         "aws:RequestedRegion": [
                               "eu-*"
                         ]
```

```
                        }
                    }
                }
            ]
}
```

Cet exemple de stratégie IAM peut également faire office de stratégie de contrôle des services (SCP) dans les organisations AWS, qui définit les limites d'autorisation appliquées à des comptes AWS spécifiques ou à des unités organisationnelles (OU) au sein d'une organisation. Cela vous permet de contrôler l'accès des utilisateurs aux services régionaux dans des environnements multi-comptes complexes.

Il existe des capacités de limitation géographique pour les régions nouvellement lancées. Les régions lancées après le 20 mars 2019 sont désactivées par défaut. Vous devez activer ces régions avant de pouvoir les utiliser. Si une région AWS est désactivée par défaut, vous pouvez utiliser votre AWS Management Console pour activer et désactiver la région. En activant et désactivant les régions AWS, vous pouvez contrôler quels utilisateurs peuvent accéder aux ressources de cette région dans votre compte AWS.[4]

Contrôle de l'accès aux applications Internet et mobiles

AWS fournit un service pour gérer le contrôle de l'accès aux données dans les applications client. Si vous avez besoin d'ajouter des fonctionnalités de contrôle d'identifiants et d'accès à vos applications Internet et mobiles, vous pouvez utiliser Amazon Cognito. Les groupes d'utilisateurs Amazon Cognito constituent un répertoire sécurisé de centaines de millions d'utilisateurs. Pour protéger l'identité des utilisateurs, vous pouvez ajouter l'authentification multi-facteurs (MFA) à vos groupes d'utilisateurs. Vous pouvez également utiliser une authentification adaptative qui utilise un modèle basé sur le risque pour prédire quand vous aurez probablement besoin d'un autre facteur d'authentification.

Grâce à Amazon Cognito Identity Pools (identités fédérées), vous pouvez voir qui a accédé à vos ressources et d'où provient l'accès (application mobile ou application Internet). Vous pouvez utiliser ces informations pour créer des rôles IAM qui autorisent ou refusent l'accès à une ressource selon le type d'origine de l'accès (application mobile ou Internet) et le fournisseur d'identité.

Surveillance et journalisation

L'article 30 du RGPD prévoit que « chaque responsable du traitement et, le cas échéant, le représentant du responsable du traitement tiennent un registre des activités de traitement effectuées sous leur responsabilité. » Cet article inclut également des précisions à propos des informations qui doivent être enregistrées lorsque vous surveillez le traitement de toutes les données à caractère personnel. Les responsables et les sous-traitants doivent également envoyer rapidement des notifications en cas de violation de données à caractère personnel, ce qui explique l'importance d'une détection rapide des incidents. Pour aider les clients à respecter ces exigences, AWS offre les services de surveillance et de journalisation suivants :

Gestion et configuration des ressources avec AWS Config

AWS Config fournit une vue détaillée de la configuration des nombreux types de ressources AWS sur votre compte AWS. Elle comprend la manière dont les ressources sont associées les unes aux autres et la façon dont elles étaient configurées par le passé pour que vous puissiez voir comment les configurations et relations évoluent.

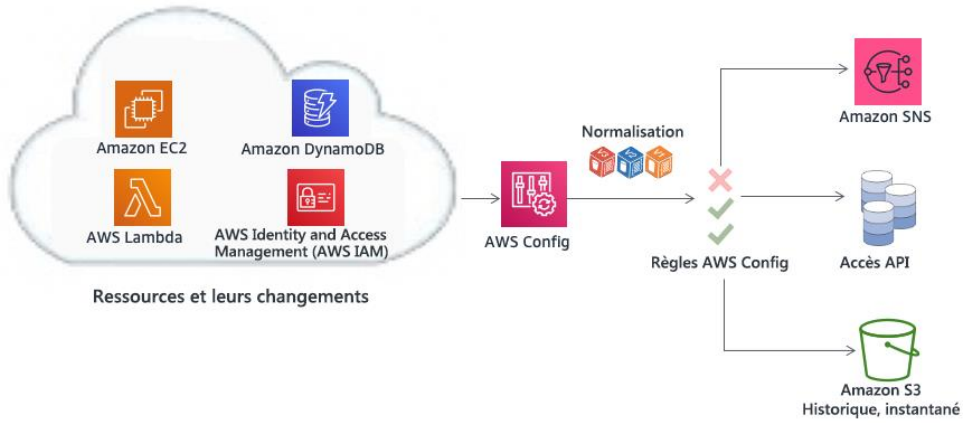

Figure 1 – Suivre les changements de configuration dans le temps avec AWS Config

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

Avec AWS Config, vous pouvez effectuer les actions suivantes :

- Évaluer les configurations de vos ressources AWS pour vérifier les paramètres
- 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 configurations passées 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, rechercher toutes les ressources qui utilisent un groupe de sécurité particulier.

Audit de conformité et analyses de sécurité

Avec AWS CloudTrail, vous pouvez surveiller continuellement l'activité de votre compte AWS. Un historique des appels d'API AWS pour votre compte est enregistré, notamment les appels d'API effectués via AWS Management Console, les kits de SDK AWS, les outils de ligne de commande et d'autres services AWS de haut niveau. Vous pouvez identifier les utilisateurs et comptes ayant appelé des API AWS en quête de services prenant en charge CloudTrail, l'adresse IP source à partir de laquelle les appels ont été effectués, et le moment où ils ont eu lieu. Vous pouvez intégrer CloudTrail à des applications à l'aide de l'API, automatiser la création de pistes pour votre organisation, vérifier le statut de vos pistes et contrôler la manière dont les administrateurs activent ou désactivent la journalisation de CloudTrail.

Les journaux CloudTrail peuvent être regroupés à partir de plusieurs régions et de plusieurs comptes AWS dans un seul compartiment S3. AWS vous recommande d'écrire des journaux, en particulier des journaux AWS CloudTrail, dans un compartiment S3 avec accès restreint à partir d'un compte AWS prévu à cet effet (archive des journaux). Les autorisations liées au compartiment doivent empêcher la suppression des journaux. Elles doivent être chiffrées au repos à l'aide du chiffrement côté serveur et des clés de chiffrement gérées par Amazon S3 (SSE-S3) ou les clés gérées par AWS KMS (SSE-KMS). La validation de l'intégrité du fichier journal CloudTrail peut être utilisée pour déterminer si un fichier journal a été modifié, supprimé ou s'il est resté inchangé après avoir été envoyé par CloudTrail. Cette fonctionnalité est construite à l'aide d'algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Cela rend difficile, sur le plan informatique, la modification, la suppression ou la falsification, sans qu'elle soit détectée, des fichiers journaux CloudTrail. Vous pouvez utiliser l'interface de ligne de commande (CLI) AWS pour valider les fichiers à l'emplacement où CloudTrail les a envoyés.

Les journaux CloudTrail agrégés dans un compartiment S3 peuvent être analysés en vue d'audit ou pour des activités de résolutions de problèmes. Une fois les journaux centralisés, vous pouvez intégrer les solutions SIEM (Security Information and Event Management) ou utiliser les services AWS, tels qu'Amazon Athena ou CloudTrail Insights, pour les analyser et les visualiser à l'aide des tableaux de bord Amazon QuickSight. Une fois les journaux CloudTrail centralisés, vous pouvez également utiliser le même compte d'archivage des journaux pour centraliser les journaux provenant d'autres sources, telles que CloudWatch Logs et les équilibreurs de charge AWS.

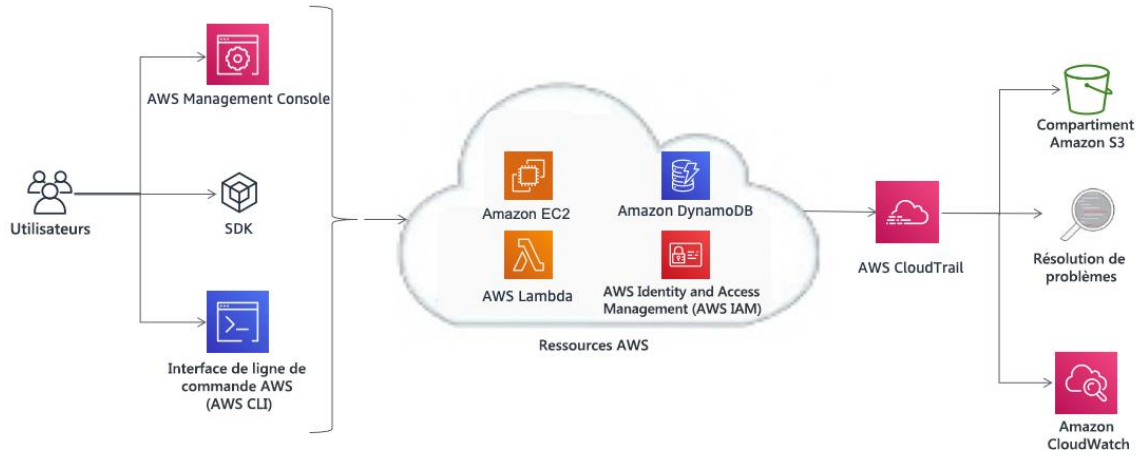

Figure 2 - Exemple d'architecture pour l'audit de conformité et l'analyse de sécurité avec AWS CloudTrail

Les journaux AWS CloudTrail peuvent aussi déclencher des événements Amazon Cloudwatch Events prédéfinis. Vous pouvez utiliser ces événements pour notifier les utilisateurs ou les systèmes de la survenue d'un événement ou pour prendre des actions de correction. Par exemple, si vous voulez surveiller des activités sur vos instances EC2, vous pouvez créer une règle CloudWatch Event. Lorsqu'une activité spécifique se produit sur l'instance Amazon EC2 et que l'événement est enregistré dans les journaux, la règle déclenche une fonction Lambda qui envoie à l'administrateur une notification par e-mail à propos de l'événement. (Voir la figure 3.) L'e-mail inclut des informations tels que le moment où l'événement s'est produit, l'utilisateur qui a effectué l'action, les détails EC2, etc. Le tableau suivant montre l'architecture de la notification par e-mail.

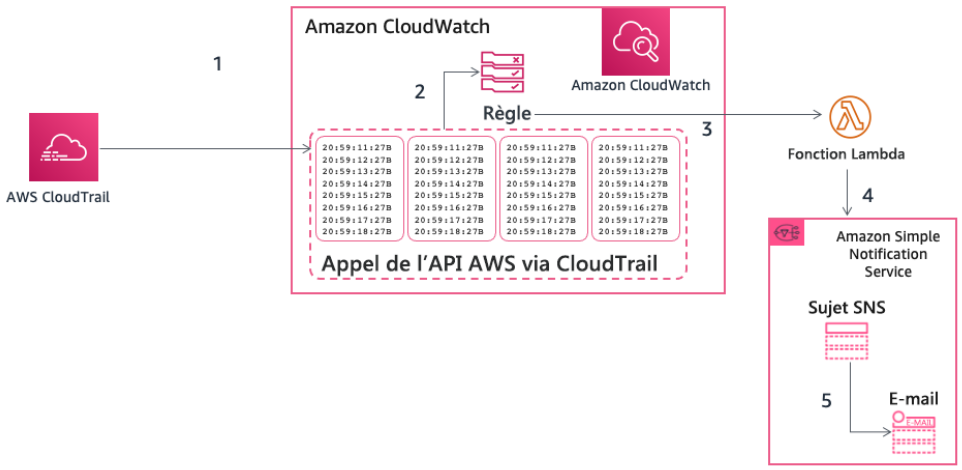

Figure 3 – Exemple de notification d'événement AWS CloudTrail

Collecte et traitement des journaux

CloudWatch Logs peut être utilisé pour surveiller, stocker et accéder à vos fichiers journaux à partir d'instances EC2, AWS CloudTrail, Route 53 et d'autres sources. Consultez la page de documentation des services AWS qui publient des journaux dans CloudWatch Logs.

Les informations des journaux comprennent, par exemple :

- Enregistrement précis des accès aux objets S3
- Informations détaillées sur les flux du réseau via VPC-Flow Logs
- Vérifications et actions de configuration reposant sur des règles selon les règles AWS Config
- Filtrage et surveillance de l'accès HTTP aux applications avec les fonctions WAF (Pare-feu pour applications Internet, Web Application Firewall) dans CloudFront

Les métriques des applications et les journaux personnalisés peuvent également être publiés dans CloudWatch Logs après installation de l'agent CloudWatch sur des instances EC2 ou des serveurs locaux.

Les journaux peuvent être analysés de manière interactive à l'aide de CloudWatch Logs Insights, qui effectue des requêtes pour vous aider à répondre de manière plus efficiente et efficace aux problèmes opérationnels.

Les journaux CloudWatch peuvent être traités en temps quasi réel grâce à la configuration des filtres d'abonnement et peuvent être envoyés à d'autres services tels

qu'un cluster Amazon Elasticsearch Service (Amazon ES), un flux Amazon Kinesis, un flux Amazon Kinesis Data Firehose ou Lambda pour le traitement, l'analyse ou le chargement personnalisé vers d'autres systèmes.

Les filtres de métriques CloudWatch peuvent être utilisés pour définir des modèles qui effectuent des recherches dans les données de journal, les transforment en métriques CloudWatch numériques et configurent des alarmes en fonction des besoins de votre entreprise. Par exemple, dans la continuité de la recommandation AWS selon laquelle il ne faut pas utiliser l'utilisateur racine (root) pour les tâches quotidiennes, il est possible de configurer un filtre de métriques CloudWatch spécifique sur un journal CloudTrail (envoyé à CloudWatch Logs) pour créer une métrique personnalisée et configurer une alarme qui avertit les parties prenantes concernées lorsque des informations d'identification racine sont utilisées pour accéder à votre compte AWS.

Les journaux tels que les journaux d'accès au serveur S3, les journaux d'accès Elastic Load Balancing, les journaux de flux VPC et les journaux de flux AWS Global Accelerator peuvent être envoyés directement à un compartiment S3. Par exemple, lorsque vous activez les journaux d'accès au serveur Amazon S3, vous pouvez obtenir des informations détaillées sur les demandes envoyées à votre compartiment S3. Une archive de journal d'accès contient des informations concernant la requête, comme le type de requête, les ressources spécifiées dans la requête, ainsi que l'heure et la date de traitement de la requête. Pour davantage d'informations sur les contenus d'un message de journal, consultez le Format des journaux d'accès au serveur Amazon S3 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, S3 ne collecte pas les journaux d'accès au service. Toutefois, lorsque vous activez la journalisation, S3 transmet généralement les journaux d'accès à votre compartiment en quelques heures. Si vous avez besoin d'un envoi plus rapide ou si vous avez besoin d'envoyer des journaux vers plusieurs destinations, envisagez d'utiliser les journaux CloudTrail ou une combinaison de journaux CloudTrail et S3. Vous pouvez chiffrer vos journaux au repos en configurant le chiffrement des objets par défaut dans le compartiment de destination. Les objets sont chiffrés à l'aide du chiffrement côté serveur et à l'aide de clés gérées par S3 (SSE-S3) ou bien des clés principales client (CMK) stockées dans AWS Key Management Service (AWS KMS).

Les journaux stockés dans un compartiment S3 peuvent être interrogés et analysés à l'aide d'Amazon Athena. Amazon Athena est un service de requête interactif qui vous permet d'analyser des données dans S3 en utilisant le langage structuré d'interrogation (SQL) standard. Vous pouvez utiliser Athena pour exécuter des requêtes ad hoc à l'aide d'ANSI SQL sans avoir besoin d'agréger ou de charger les données dans Athena. Athena peut traiter des ensembles de données non structurés, semi-structurés et structurés et intègre ces ensembles à Amazon QuickSight pour une visualisation facile.

Les journaux sont également une source d'informations utiles pour la détection automatisée de menaces. Amazon GuardDuty est un service de surveillance continue de la sécurité qui analyse et traite les événements provenant de plusieurs sources, telles que les journaux de flux VPC, les journaux des événements de gestion CloudTrail, les journaux d'événements CloudTrail S3 et les journaux du système de noms de domaine (DNS). Ce service utilise des flux d'intelligence de menaces, tels que des listes d'adresses IP et de domaines malveillants, ainsi que le Machine Learning (apprentissage machine) pour détecter les activités inattendues, potentiellement non autorisées et malveillantes au sein de votre environnement AWS. Lorsque vous activez GuardDuty dans une région, il commence immédiatement à analyser vos journaux d'événements CloudTrail. Il analyse les événements de gestion CloudTrail et de données S3 directement à partir de CloudTrail via un flux d'événements indépendant et dupliqué.

Découvrir et protéger les données à grande échelle avec Amazon Macie

L'article 32 du RGDP dispose que « ... le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins : [...]

b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;

[…]

d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement. »

Il est essentiel de disposer d'une procédure continue de classification des données pour adapter le traitement des données de sécurité à la nature des données. Si votre organisation gère des données sensibles, surveillez leur lieu de résidence, protégez-les correctement et fournissez la preuve que vous appliquez la sécurité et la confidentialité des données conformément aux exigences réglementaires. Pour aider le client à identifier et à protéger ses données sensibles à grande échelle, AWS propose Amazon Macie, un service de cybersécurité des données et de confidentialité des données entièrement géré qui utilise des modèles de correspondance et de Machine Learning (apprentissage machine) pour la détection des informations personnelles identifiables (Personally Identifiable Information, PII) afin de découvrir et de protéger les données sensibles stockées dans des compartiments S3. Amazon Macie analyse ces compartiments et fournit une catégorisation des données à l'aide d'identifiants de données gérés qui sont conçus pour détecter plusieurs catégories de données sensibles. Macie peut détecter des informations personnelles identifiables telles que le nom complet, l'adresse électronique, la date de naissance, le numéro de carte

d'identité, l'identité ou le numéro de référence du contribuable, etc.[5] Le client peut définir des identifiants de données personnalisés qui reflètent les scénarios particuliers de son organisation (par exemple, numéros de compte client ou classification interne des données).

Amazon Macie évalue continuellement l'objet à l'intérieur des compartiments et fournit automatiquement un résumé des résultats (Figure 4) pour toutes les données non chiffrées ou accessibles au public qui correspondent à la catégorie de données définie. Ces données peuvent inclure des alertes pour tous les objets ou compartiments non chiffrés et accessibles au public partagés avec des comptes AWS en dehors de ceux que vous avez définis dans AWS Organizations. Amazon Macie est intégré à d'autres services AWS, tels qu'AWS Security Hub, afin de générer des résultats de sécurité exploitables et de réagir de manière automatique et réactive à ces résultats (Figure 5).

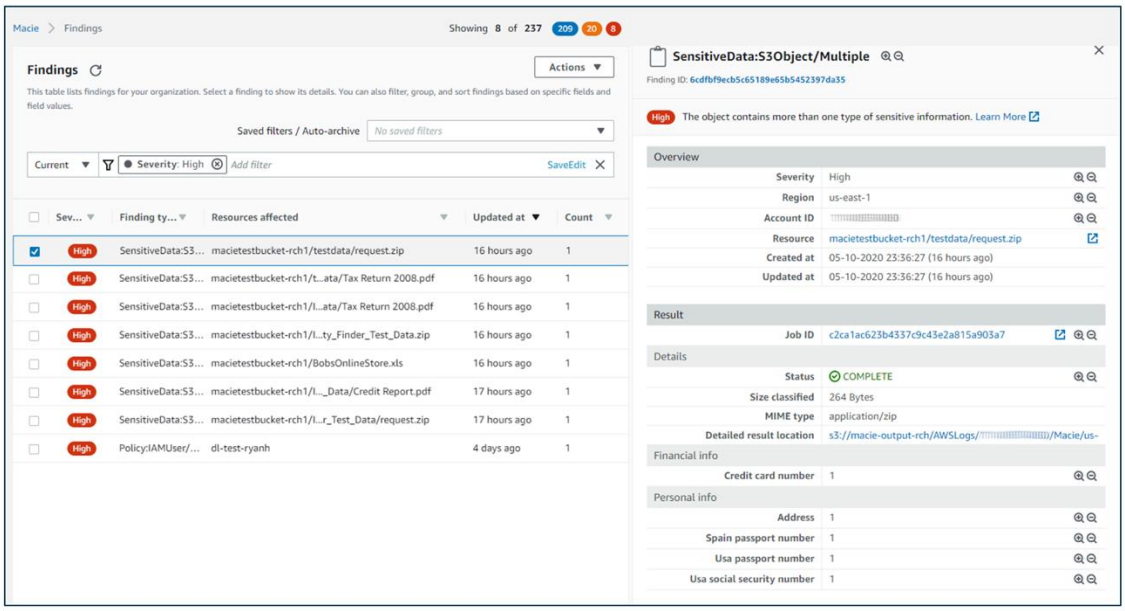

Figure 4 – Inspections des données et exemple de résultats

Gestion centralisée de la sécurité

De nombreuses organisations ont des problèmes de visibilité et de gestion centralisée de leurs environnements. Ces problèmes peuvent s'aggraver à mesure que l'empreinte organisationnelle grandit, sauf si vous attachez beaucoup d'importance à vos systèmes de sécurité. Le manque de connaissances, ajouté à une gestion décentralisée et incohérente de la gouvernance et des procédés de sécurité peuvent rendre votre environnement vulnérable.

AWS fournit des outils qui vous aident à régler certains problèmes informatiques parmi les plus complexes en matière de gestion et de gouvernance informatiques, ainsi que des outils d'aide à une approche de protection des données dès la conception.

AWS Control Tower fournit une méthode d'installation et de gouvernance pour un nouvel environnement AWS multi-comptes sécurisé. Il automatise la configuration d'une zone d'atterrissage,[6] qui est un environnement multi-comptes basé sur des règles de bonnes pratiques et qui permet la gouvernance à l'aide de barrières que vous pouvez choisir parmi une liste préétablie. Les barrières mettent en place des règles de gouvernance pour la sécurité, la conformité et les opérations. AWS Control Tower fournit une gestion de l'identité à l'aide d'un répertoire par défaut AWS Single Single-On (SSO) et permet un audit sur plusieurs comptes à l'aide d'AWS SSO et d'AWS IAM. Il centralise également des journaux provenant de CloudTrail et des journaux AWS Config qui sont conservés dans S3.

AWS Security Hub est un autre service qui soutient la centralisation et peut améliorer la visibilité dans une organisation. Security Hub centralise et hiérarchise les résultats de sécurité et de conformité des comptes et des services AWS, tels qu'Amazon GuardDuty et Amazon Inspector, et peut être combiné à des logiciels de sécurité de partenaires tiers pour vous aider à analyser les tendances de sécurité et à hiérarchiser les problèmes de sécurité.

Amazon GuardDuty est un service intelligent de détection des menaces qui permet aux clients de surveiller et de protéger plus précisément et facilement leurs comptes AWS, leurs charges de travail et leurs données stockés dans S3. GuardDuty analyse des milliards d'événements sur vos comptes AWS à partir de plusieurs sources, notamment AWS CloudTrail Management Events, AWS CloudTrail S3 Data Events, les journaux de flux Amazon VPC et les journaux du système de noms de domaine (DNS). Par exemple, il détecte les appels d'API inhabituels, les communications sortantes suspectes vers des adresses IP malveillantes connues ou le vol de données possible à l'aide de requêtes DNS comme mécanisme de transport. GuardDuty est en mesure de fournir des résultats plus précis en tirant parti des informations sur les menaces alimentées par le Machine Learning (l'appretissage machine) et des partenaires de sécurité tiers.

Amazon Inspector est un service automatisé d'évaluation de la sécurité qui aide à améliorer la sécurité et la conformité des applications déployées sur des instances EC2. Amazon Inspector évalue automatiquement les applications afin de déterminer leur exposition et de détecter les possibles vulnérabilités et écarts par rapport aux bonnes pratiques. Après avoir effectué une évaluation, Amazon Inspector produit une liste détaillée des résultats de sécurité classés par degré de gravité.

Amazon CloudWatch Events vous permet de configurer votre compte AWS afin d'envoyer des événements vers d'autres comptes AWS ou de devenir un destinataire pour les événements provenant d'autres comptes et organisations. Ce mécanisme peut être très utile afin de mettre en œuvre des scénarios de réponse aux incidents à travers

plusieurs comptes en adoptant des actions correctives rapides (par exemple, en appelant une fonction Lambda ou en effectuant une commande sur une instance EC2) selon les besoins à chaque fois qu'un événement d'incident de sécurité se produit.

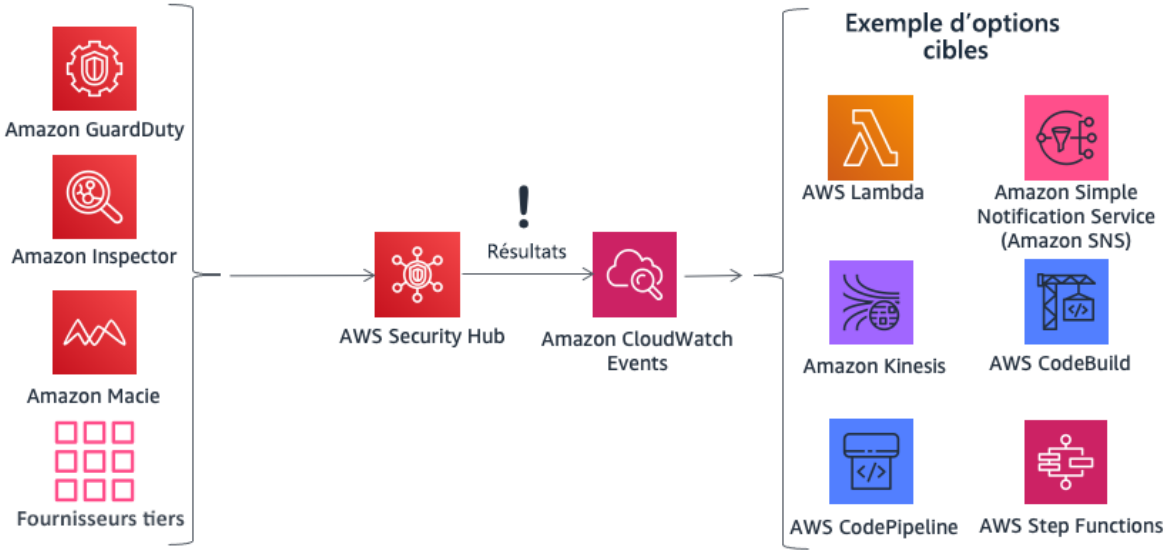

Figure 5 – Adopter une action avec AWS Security Hub et Amazon CloudWatch Events

AWS Organizations vous aide à centraliser la gestion et la gouvernance des environnements complexes. Il vous permet de contrôler les accès, la conformité et la sécurité dans un environnement multi-comptes. AWS Organizations prend en charge les politiques de contrôle des services (SCP), qui définissent les actions de service AWS qui peuvent être utilisées pour des comptes spécifiques ou des unités organisationnelles au sein d'une organisation.

AWS Systems Manager vous offre la visibilité et le contrôle de votre infrastructure sur AWS. Vous pouvez afficher les données opérationnelles provenant de plusieurs services AWS à partir d'une seule et même console et automatiser les tâches opérationnelles de ces services. Vous pouvez afficher des informations sur les activités récentes de l'API, les modifications de la configuration des ressources, les alertes opérationnelles, l'inventaire logiciel et l'état de conformité des correctifs. En utilisant l'intégration avec d'autres services AWS, vous pouvez également agir sur les ressources en fonction de vos besoins opérationnels, et ainsi rendre votre environnement conforme.

Par exemple, en intégrant Amazon Inspector à AWS Systems Manager, les évaluations de sécurité sont simplifiées et automatisées, car vous pouvez installer l'agent Amazon Inspector automatiquement à l'aide d'Amazon EC2 Systems Manager lorsqu'une instance EC2 est lancée. Vous pouvez également effectuer des remédiations automatiques pour les résultats d'Amazon Inspector à l'aide des fonctions EC2 System Manager et Lambda.

Protection de vos données sur AWS

L'article 32 du RGPD exige que les organisations « ...mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins : la pseudonymisation et le chiffrement des données à caractère personnel [...] » En outre, les organisations doivent se prémunir contre la divulgation non autorisée de données à caractère personnel ou de l'accès non autorisé à de telles données.

Le chiffrement réduit les risques associés au stockage des données à caractère personnel car les données ne sont pas lisibles sans la clé adéquate. Une stratégie complète de chiffrement peut aider à réduire l'impact de plusieurs événements de sécurité, y compris certains cas de violation de données à caractère personnel.

Chiffrement des données au repos

Le chiffrement des données au repos est vital pour la conformité règlementaire et la protection des données. Il aide à garantir que les données sensibles stockées sur des disques ne sont pas lisibles par des utilisateurs ou des applications sans une clé valide. AWS fournit de multiples options de chiffrement au repos et de gestion de la clé de chiffrement. Par exemple, vous pouvez utiliser le kit de développement logiciel de chiffrement AWS (AWS Encryption SDK) avec une clé principale client (CMK) créée et gérée dans AWS KMS pour chiffrer des données arbitraires.

Les données chiffrées peuvent être stockées en toute sécurité au repos et peuvent être déchiffrées seulement par un acteur autorisé à accéder à la clé principale client (CMK). Le résultat : des données confidentielles avec chiffrement d'enveloppe, des mécanismes de stratégie pour le chiffrement de l'authentification et de l'autorisation, et une journalisation de l'audit par AWS CloudTrail. Certains services de fondation AWS possèdent des fonctionnalités intégrées de chiffrement au repos, qui offrent la possibilité de chiffrer des données avant qu'elles ne soient inscrites dans un stockage non volatile. Par exemple, vous pouvez chiffrer des volumes Amazon EBS et configurer des compartiments S3 pour un chiffrement côté serveur (SSE) à l'aide d'un chiffrement AES-256. S3 prend également en charge le *chiffrement côté client*, ce qui vous permet de chiffrer les données avant de les envoyer à S3. Les kits SDK AWS prennent en charge le chiffrement côté client pour faciliter les opérations de chiffrement et de déchiffrement des objets. Amazon Relational Database Service (Amazon RDS) est également compatible avec le chiffrement transparent des données (Transparent Data Encryption, TDE).

Il est possible de chiffrer des données sur les stockages d'instance Linux EC2 à l'aide de bibliothèques Linux intégrées. Cette méthode permet de chiffrer les fichiers de façon transparente, ce qui protège les données confidentielles. Les applications qui traitent les données ne remarquent pas le chiffrement au niveau du disque.

Vous pouvez employer deux méthodes pour chiffrer des fichiers sur des stockages d'instance.

- **Chiffrement au niveau du disque** — Avec cette méthode, le disque entier, ou un bloc à l'intérieur du disque, est chiffré à l'aide d'une ou de 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.
- **Chiffrement au niveau du système de fichiers** — Dans ce cas, 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.

Pour la mémoire non volatile expresse (NVMe)*, le chiffrement au niveau du disque* de volumes de stockage d'instance SSD est l'option par défaut. Les données sur un stockage d'instance NVMe sont chiffrées à l'aide d'un chiffrement par bloc XTS-AES-256 appliqué dans un module matériel de l'instance. Les clés de chiffrement sont générées à l'aide du module matériel et sont uniques à chaque périphérique de stockage d'instance NVMe. Toutes les clés de chiffrement sont détruites une fois l'instance arrêtée ou mise hors service, sans possibilité de les récupérer. Vous ne pouvez pas utiliser vos propres clés de chiffrement.

Chiffrement des données en transit

AWS recommande fortement de chiffrer les données en transit d'un système à un autre, notamment dans le cas de ressources à l'intérieur et en dehors d'AWS.

Lorsque vous créez un compte AWS, une section isolée logique du Cloud AWS est réservée pour celui-ci : l'Amazon Virtual Private Cloud (Amazon VPC). Il s'agit du point de départ des ressources AWS dans un réseau virtuel que vous définissez. Vous disposez d'un contrôle total sur votre environnement de mise en réseau virtuel, notamment la sélection de votre propre gamme 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, réseau privé virtuel) matérielle entre le centre de données de votre entreprise et votre VPC Amazon, de manière à exploiter le Cloud AWS comme une extension de votre centre de données d'entreprise.

Afin de protéger les communications entre votre VPC Amazon et le centre de données de votre entreprise, vous pouvez choisir parmi plusieurs options de connectivité VPN et sélectionner celle qui répond le mieux à vos besoins. Vous pouvez utiliser le VPN Client AWS pour activer l'accès sécurisé à vos ressources AWS à l'aide des services VPN

orientés client. Vous pouvez également utiliser une application de logiciel VPN tiers disponible sur AWS Marketplace, que vous pouvez installer sur une instance EC2 dans votre Amazon VPC. Ou alors, vous pouvez créer une connexion VPN IPsec pour protéger les communications entre votre VPC et votre réseau distant. Pour créer une connexion privée dédiée à partir d'un réseau distant vers votre VPC Amazon, vous pouvez utiliser AWS Direct Connect. Vous pouvez combiner cette connexion avec un VPN AWS site à site pour créer une connexion privée chiffrée par IPsec.

AWS fournit des points de terminaison HTTPS à l'aide du protocole TLS (Transport Layer Security, sécurité de couche de transport) pour les communications, ce qui permet un chiffrement en transit lorsque vous utilisez les API AWS. Vous pouvez utiliser le service AWS Certificate Manager (ACM, gestionnaire de certificat AWS) pour générer, gérer et déployer les certificats privés et publics utilisés pour établir un transport chiffré entre les systèmes de vos charges de travail. Amazon Elastic Load Balancing est intégré avec ACM et sert à soutenir les protocoles HTTPS. Si votre contenu est distribué par Amazon CloudFront, ce service prend en charge les points de terminaison chiffrés.

Outils de chiffrement

AWS propose divers services, outils et mécanismes évolutifs de chiffrement des données pour vous aider à protéger les données des clients stockées et traitées sur AWS. Pour plus d'informations à propos de la fonctionnalité et de la confidentialité du service AWS, consultez les Remarques de capacités du service AWS en matière de confidentialité.[7]

Les services de chiffrement d'AWS utilisent une large gamme de technologies de chiffrement et stockage conçues pour maintenir l'intégrité et la confidentialité de vos données au repos ou en transit. AWS offre quatre outils et services principaux pour les opérations de cryptographie :

- **AWS Key Management Service** (AWS KMS, service de gestion de clé) est un service géré par AWS qui génère et gère à la fois les clés principales et les clés de données. AWS KMS est intégré avec de nombreux services AWS pour fournir un chiffrement des données côté serveur à l'aide des clés KMS provenant des comptes client. Les modules physiques de sécurité KMS (HSM) sont validés au niveau 2 de la norme FIPS 140-2.
- **AWS CloudHSM** fournit des HSM qui sont validés au niveau 3 de la norme FIPS 140-2. Ils stockent de manière sécurisée une variété de clés cryptographiques auto-gérées, notamment les clés principales et les clés de données.
- **Services et outils cryptographiques AWS**

- **Le SDK de chiffrement AWS** fournit une bibliothèque de chiffrement côté client pour mettre en œuvre des opérations de chiffrement et déchiffrement sur *tous* les types de données.
- **L'Amazon DynamoDB Encryption Client** fournit une bibliothèque de chiffrement côté client pour chiffrer les tables de données avant de les envoyer à un service de base de données, tel qu'Amazon DynamoDB.

AWS Key Management Service

AWS Key Management Service (AWS KMS) est un service géré qui simplifie la création et le contrôle des clés de chiffrement utilisées pour chiffrer vos données. Ce service utilise des Hardware Security Modules (HSM, modules physiques de sécurité) pour protéger la sécurité de vos clés. AWS KMS s'intègre à plusieurs autres services AWS pour vous aider à protéger les données que vous stockez à l'aide de ces services. AWS KMS s'intègre également à AWS CloudTrail pour vous fournir des journaux relatifs à l'utilisation de toutes vos clés afin de répondre à vos besoins en matière de réglementation et de conformité.

Vous pouvez en toute simplicité créer, importer et renouveler des clés, mais aussi définir des stratégies d'utilisation et procéder à des audits d'utilisation à partir d'AWS Management Console, ou encore à l'aide du kit SDK AWS ou de l'interface de ligne de commande AWS (AWS Command Line Interface, CLI).

Les clés principales (CMK) dans AWS KMS, qu'elles soient importées par vos soins ou créées pour vous par AWS KMS, sont conservées dans un stockage hautement durable et dans un format chiffré, ce qui permet de les extraire si besoin. Vous pouvez configurer AWS KMS afin qu'il effectue une rotation automatique des clés principales créées dans AWS 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 automatique des données préalablement chiffrées.

Pour toute clé principale dans KMS, vous pouvez contrôler les personnes y ayant accès et quels services peuvent être utilisés grâce à de nombreux contrôles d'accès, notamment des autorisations et des conditions de stratégie de clé dans le cadre des stratégies de clé ou des stratégies IAM. Vous pouvez également importer des clés depuis votre propre infrastructure de gestion de clé et les utiliser dans KMS.

Par exemple, la stratégie suivante utilise la condition `kms:ViaService` pour autoriser l'utilisation d'une clé principale gérée par le client pour des actions précises uniquement lorsque la requête provient d'Amazon EC2 ou d'Amazon RDS dans une région spécifique (*us-west-2*) depuis un utilisateur spécifique (`ExampleUser`).

```
{
          "Version": "2012-10-17",
          "Statement": [
              {
                 "Effect": "Allow",
                 "Principal": {
                     "AWS":
"arn:aws:iam::111122223333:user/ExampleUser"
                  }
                 "Action": [
                      "kms:Encrypt*",
                      "kms:Decrypt",
                      "kms:ReEncrypt*",
                      "kms:GenerateDataKey*",
                      "kms:CreateGrant",
                      "kms:ListGrants",
                      "kms:DescribeKey"
                  ],
                  "Resource": "*",
                  "Condition": {
                     "ForAnyValue:StringEquals": {
                         "kms:ViaService": [
                               "ec2.us-west-2.amazonaws.com",
                               "rds.us-west-2.amazonaws.com"
                         ]
                      }
                }
}
```

Intégration du service AWS

AWS KMS s'est intégré à un certain nombre de services AWS. Consultez le site Internet KMS pour obtenir la liste complète des services intégrés. Ces intégrations signifient que vous pouvez utiliser en toute simplicité les clés principales client (CMK) d'AWS KMS pour chiffrer les données que vous stockez avec ces services. En plus d'utiliser une clé principale gérée par le client, de nombreux services intégrés vous permettent d'utiliser une clé principale gérée par AWS qui est créée et gérée automatiquement pour vous, mais qui n'est utilisable que dans le cadre du service spécifique qui l'a créée.

Capacités d'audit

AWS CloudTrail enregistre chaque utilisation d'une clé que vous stockez dans KMS dans un fichier journal envoyé au compartiment S3 que vous avez spécifié dans votre configuration de CloudTrail. Les informations enregistrées incluent les informations relatives à l'utilisateur, l'heure, la date, l'opération exécutée et la clé utilisée.

Sécurité

AWS KMS est conçu de manière à ce que personne ne puisse accéder à vos clés principales. Le service repose sur des systèmes conçus pour protéger vos clés principales à l'aide de techniques de renforcement approfondies. 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 est vérifié par un contrôle d'accès à plusieurs parties qui est audité et examiné par un groupe indépendant au sein d'AWS.

Pour plus d'informations à propos d'AWS KMS, consultez le livre blanc *AWS Key Management Service*.

AWS CloudHSM

AWS CloudHSM est un module physique de sécurité (HSM) basé sur le cloud qui vous aide à répondre aux exigences de conformité d'entreprise, aux exigences contractuelles et réglementaires en matière de cybersécurité des données. Il vous permet en effet de générer et d'utiliser vos clés de chiffrement sur un matériel validé au niveau 3 de la norme FIPS 140 -2.

Avec CloudHSM, vous contrôlez les clés de chiffrement et les opérations de cryptographie effectuées par le HSM.

AWS et les partenaires AWS Marketplace proposent différentes solutions de protection des données sensibles sur la plateforme AWS, mais dans le cas d'applications et de données soumises à des exigences contractuelles ou réglementaires très strictes en matière de gestion des clés cryptographiques, une protection supplémentaire peut s'avérer nécessaire. Par le passé, 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. Cette solution pouvait vous empêcher de procéder à la migration de ces applications vers le Cloud, ou ralentissait fortement leurs performances. Avec le service AWS CloudHSM vous pouvez 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 matière de gestion des clés sans que les performances de vos applications en pâtissent.

Le service AWS CloudHSM fonctionne avec Amazon VPC. Les instances CloudHSM sont allouées dans votre VPC Amazon avec l'adresse IP que vous indiquez. Vous disposez ainsi d'une connexion réseau simple et privée pour vos instances 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, lesquelles sont isolées des autres clients AWS. Disponible dans plusieurs régions et zones de disponibilité (AZ), AWS CloudHSM vous permet d'ajouter un stockage de clé durable et sécurisé à vos applications.

Intégration avec les services AWS et les applications tierces

Vous pouvez utiliser CloudHSM avec Amazon Redshift, Amazon Relational Database Service (Amazon RDS) pour 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, telles que PKCS#11, Java JCA/JCE, Microsoft CAPI et CNG.

Activités d'audit

Si vous devez suivre des modifications de ressources ou auditer des activités à des fins de sécurité et de conformité, vous pouvez vérifier tous les appels d'API de gestion du CloudHSM qui sont effectués à partir de votre compte via AWS CloudTrail. De plus, vous pouvez auditer des opérations sur l'application HSM à l'aide de syslog ou envoyer des messages de journal syslog à votre propre collecteur.

Services et outils cryptographiques AWS

AWS offre des mécanismes en conformité avec une large gamme de normes de sécurité cryptographique que vous pouvez utiliser pour mettre en œuvre de bonnes pratiques en matière de chiffrement. Le SDK de chiffrement AWS[8] est une bibliothèque de chiffrement côté client, disponible en Java, Python, C, JavaScript, et une interface de ligne de commande qui est compatible avec Linux, macOS et Windows. Il offre des fonctionnalités avancées de protection des données, notamment des suites d'algorithmes de clés symétriques, sécurisées et authentifiées, telles que 256-bit AES-GCM avec dérivation de clé et signature. En raison d'une conception spécifiquement axée sur les applications qui utilisent Amazon DynamoDB, le DynamoDB Encryption Client[9] permet aux utilisateurs de protéger leurs tableaux de données avant qu'ils ne soient envoyées vers la base de données. Il vérifie et déchiffre aussi les données lorsqu'elles sont récupérées. Le client est disponible en Java et Python.

Infrastructure Linux DM-Crypt

Dm-crypt est un mécanisme de chiffrement au niveau du noyau Linux qui permet aux utilisateurs de monter un système de fichiers chiffré. Le montage d'un système de fichiers consiste à joindre un système de fichiers à un répertoire (point de montage) pour le rendre 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 stockage en mode bloc. 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 gestionnaire LVM permet une gestion de volume logique pour le noyau Linux.

Protection des données dès la conception et par défaut

À chaque fois qu'un utilisateur ou une application tente d'utiliser la console AWS Management Console, l'API AWS ou la CLI AWS, une requête est envoyée à AWS. Le service AWS reçoit la requête et exécute plusieurs étapes pour déterminer s'il doit autoriser ou rejeter la requête, selon une logique d'évaluation de stratégie spécifique. À l'exception des demandes d'informations d'identification racine, toutes les demandes sur AWS sont refusées par défaut (la stratégie de *refus* par défaut est appliquée). Cela signifie que tout ce qui n'est pas explicitement autorisé par la stratégie est rejeté. Dans la définition des stratégies et bonnes pratiques, AWS vous conseille d'appliquer le principe du moindre privilège, ce qui signifie que chaque composant (comme les utilisateurs, les modules ou les services) doit être autorisé à accéder uniquement aux ressources nécessaires à la réalisation de ses tâches.

Cette approche s'aligne sur l'article 25 du RGPD qui 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. »

AWS fournit également des outils pour mettre en œuvre *l'infrastructure sous forme de code* qui est un mécanisme puissant pour inclure la sécurité dès le début de la conception d'une architecture. AWS CloudFormation fournit un langage commun pour décrire et allouer toutes les ressources d'infrastructure, notamment les politiques et protocoles de sécurité. Avec ces outils et pratiques, la sécurité devient une part entière de votre code et peut être déclinée en plusieurs versions, surveillée et modifiée (avec

un système de versions) selon les exigences de votre organisation. Cela permet de mettre en pratique la *protection de données dès la conception*, car les protocoles et politiques de sécurité peuvent être inclus dans la définition de votre architecture et peuvent également être surveillés en continu par les mesures de sécurité de votre organisation.

Aide d'AWS

Tableau 1 — Comment AWS peut vous aider à gérer la conformité au RGPD

Domaine	Description	Outils et services AWS
Cadre de conformité stricte	Les mesures techniques et organisationnelles appropriées peuvent devoir inclure « des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ».	SOC 1 / SSAE 16 / ISAE 3402 (anciennement SAS 70) / SOC 2 / SOC 3 PCI DSS, niveau 1 ISO 9001 / ISO 27001 / ISO 27017 / ISO 27018 NIST FIPS 140-2 Catalogue de contrôles de conformité de Cloud computing (C5)
Contrôle d'accès aux données	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. »	AWS Identity and Access Management (IAM) Amazon Cognito AWS Shield et WAF AWS Resource Access Manager AWS Organizations AWS CloudFormation AWS CloudTrail AWS Config

Domaine	Description	Outils et services AWS
Surveillance et journalisation	« Chaque responsable du traitement et, le cas échéant, le représentant du responsable du traitement tiennent un registre des activités de traitement effectuées sous leur responsabilité. » « ... le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque [...] »	 Amazon CloudWatch  AWS Control Tower  Amazon GuardDuty  Amazon Inspector  Amazon Macie  AWS Systems Manager  AWS Security Hub
		 AWS Tools et SDK
Protection de vos données sur AWS	Les organisations doivent « mettre 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 ».	 AWS Certificate Manager  AWS CloudHSM  AWS Key Management Service

Participants

Ont participé à l'élaboration de ce document :

- Tim Anderson, Technical Industry Specialist, Amazon Web Services
- Carmela Gambardella, Public Sector Senior Solutions Architect, Amazon Web Services
- Giuseppe Russo, Security Assurance Manager, Amazon Web Services
- Marta Taggart, Senior Program Manager, Amazon Web Services
- Luca Iannario, Public Sector Solutions Architect, Amazon Web Services

Révisions du document

Date	Description
Novembre 2017	Première publication
Décembre 2020	Mise à jour pour inclure l'ajout de nouveaux services et fonctionnalités AWS.

Notes

[1] https://ec.europa.eu/info/law/law-topic/data-protection_fr

[2] https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679

[3] https://cispe.cloud/

[4] https://docs.aws.amazon.com/general/latest/gr/rande-manage.html

[5] https://docs.aws.amazon.com/macie/latest/user/managed-data-identifiers.html#managed-data-identifiers-pii

[6] https://aws.amazon.com/solutions/aws-landing-zone/

[7] https://aws.amazon.com/compliance/data-privacy/service-capabilities/

[8] https://docs.aws.amazon.com/crypto/latest/userguide/awscryp-service-encrypt.html

[9] https://docs.aws.amazon.com/crypto/latest/userguide/awscryp-service-ddb-client.html