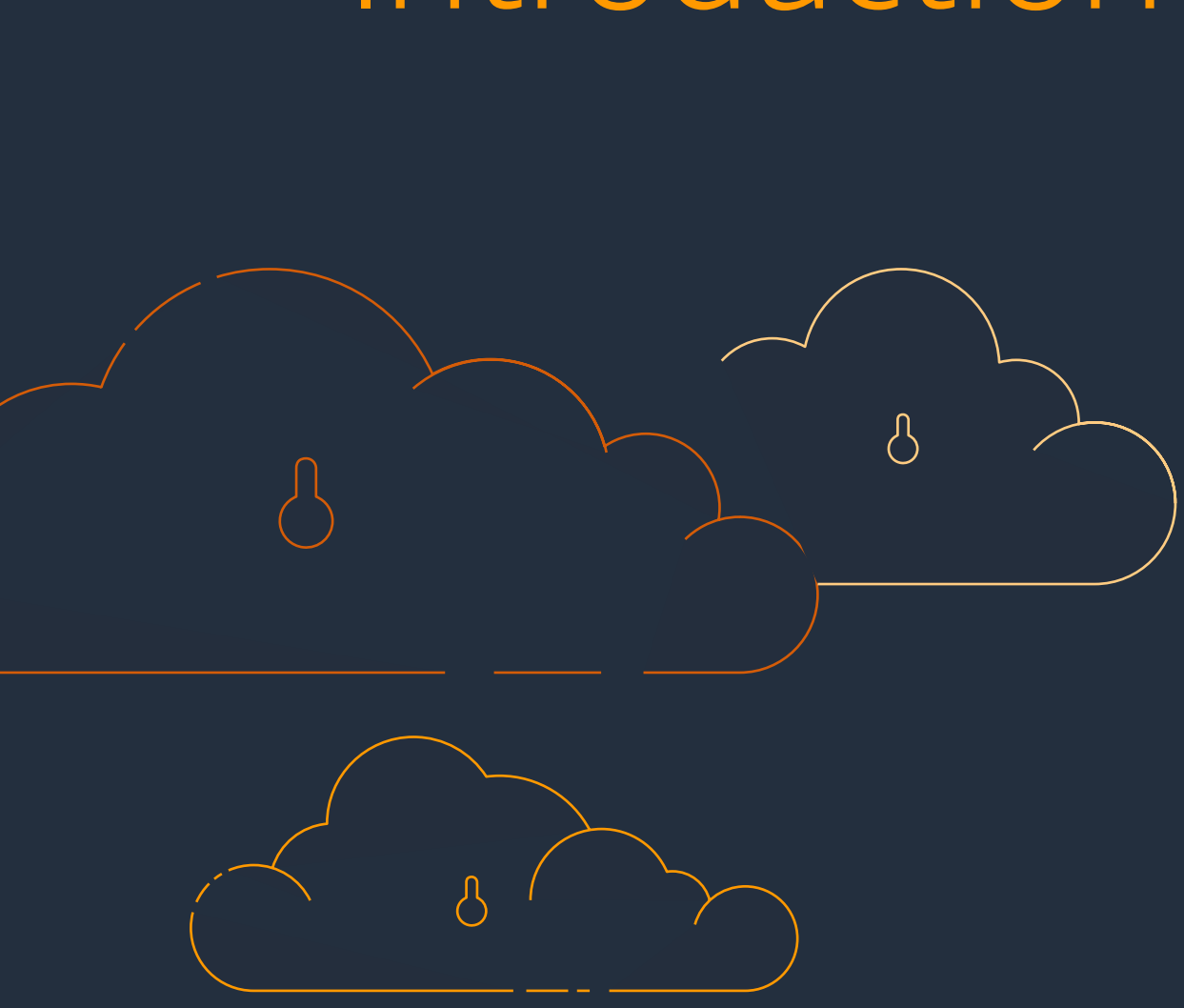
La sécurité dans le cloud d'AWS

Introduction



La sécurité dans le cloud AWS en **6 points clés**

1 PLEIN CONTRÔLE

Les clients d'AWS disposent du contrôle de la localisation de leurs contenus dans le cloud. En choisissant la Région AWS Europe (Paris), composée de trois zones de disponibilités (AZ), chacune comprenant au moins un centre de données, vous maîtrisez la localisation de vos données et vous pouvez construire des applications hautement disponibles sur le territoire français. Par ailleurs, vous disposez de nombreuses options de configuration, comme relier votre réseau à AWS avec des liens fibres dédiés, ou encore définir précisément quelles permissions vous donnez à vos administrateurs.

2 FACILITÉ DE MISE EN ŒUVRE

Les services de sécurité sont intégrés nativement dans les services AWS et vous permettent par exemple très facilement (en quelques clics) de chiffrer vos données avec vos clés, de vous protéger des attaques en déni de service, ou encore de répliquer vos données pour en assurer la haute disponibilité.

3 FAIBLE COÛT

Les services de sécurité AWS vous évitent d'investir dans des solutions coûteuses à l'achat, à l'intégration et à maintenir, en proposant un coût à l'usage très réduit, comme par exemple la fourniture gratuite de certificats SSL publics pour vos URLs, le niveau gratuit de protection anti-DDoS, le niveau gratuit de chiffrement de vos données au repos et en transit

4 PERFORMANCE

Les infrastructures AWS permettent de répondre aux attentes les plus exigeantes, avec par exemple trois zones de disponibilité dans les régions AWS, la durabilité de 99,999999999% des données dans S3 ou encore l'utilisation de composants cryptographiques matériels permettant le chiffrement des données sans impact sur les performances.

5 AUTOMATISATION ET GOUVERNANCE

AWS facilite le management de la sécurité grâce à une visibilité accrue sur leur SI et à de nombreux outils et mécanismes d'automatisation, par exemple vous disposez d'un inventaire complet et détaillé de vos ressources, vous pouvez centraliser et automatiser les mises à jour de vos logiciels, vous pouvez définir des alertes et actions de remédiation automatique sur détection d'incident, ou encore vérifier en permanence la conformité de vos configurations à vos propres règles.

6 CONFORMITÉ

Le cloud AWS est conçu pour le plus haut niveau d'exigence de sécurité, permettant à tous de bénéficier du même niveau de protection. Pour garantir ce meilleur niveau, AWS se soumet régulièrement à des auditeurs tiers pour vérifier la conformité de ses infrastructures et services à des milliers d'exigences, ce qui nous permet d'attester de notre conformité à de nombreux standards, lois, règlements et cadres dans le monde entier, tels que ISO 27001, 27017 et 27018, SOC 1,2,3, PCI-DSS et, par exemple en France, HDS.

Synthèse

Des enjeux forts de sécurité numérique dans le secteur public

Le secteur public a largement numérisé ses services, les a ouverts de plus en plus au public, exploite de nombreuses données issues de partenaires ou d'objets connectés. La sécurité des données est essentielle, qu'il s'agisse d'assurer la protection des données personnelles des citoyens et des agents et la continuité du service public. Lorsqu'on parle de sécurité numérique, on parle notamment d'assurer :

- **la disponibilité** des systèmes, c'est-à-dire s'assurer que les systèmes sont opérationnels quand on en a besoin. Il s'agit donc notamment de se prémunir des pannes, de limiter l'impact des maintenances, et se protéger des sabotages comme les attaques en déni de service.
- **l'intégrité** des données, c'est-à-dire s'assurer que les informations ne sont pas modifiées ou détruites lors de leur transmission ou leur traitement. Il s'agit donc notamment de se protéger contre les erreurs, les intrusions ou par exemple les attaques de type « ransomware ».
- **la confidentialité** des données, c'est-à-dire s'assurer que les informations ne sont accessibles qu'aux seuls systèmes et aux seules personnes autorisées. Il s'agit donc notamment de se protéger contre les accès non autorisés, contre l'écoute des réseaux ou par exemple les logiciels « espions ».

Le développement des usages des services publics numériques repose sur la **confiance** que les agents et les citoyens ont sur la disponibilité du service, la qualité de l'information, la confidentialité des échanges.

La sécurité informatique et le cloud AWS

Avec l'augmentation de la complexité des systèmes informatiques (de plus en plus de logiciels, de types d'appareils connectés, de partenaires…), il est de plus en plus difficile, pour une organisation, de maîtriser technologiquement l'ensemble des composants qui lui permettent d'assurer sa sécurité informatique, depuis la fiabilité des systèmes de refroidissement des salles informatiques jusqu'aux technologies de détection d'intrusion.

Pour répondre à ce besoin, le Cloud AWS vous met à la portée de quelques clics une infrastructure hautement disponible et des services de sécurité prêts à l'emploi. En effet, depuis 2006, en développant ses technologies et infrastructures aujourd'hui utilisées par des millions de clients dans le monde, AWS a érigé la sécurité en première priorité, à la fois dans la conception de son infrastructure hautement redondante, dans le développement de services couvrant la plupart des besoins (gestion des accès, détection, protection des infrastructures, protection des données, réponse aux incidents, conformité) et en employant les meilleurs experts pour opérer à l'échelle mondiale.

Dans ce livre blanc, nous vous proposons de découvrir **la manière dont le cloud AWS vous permet de satisfaire vos besoins de sécurité.** Nous accompagnons les clients du secteur public dans leur projet de transformation bien au-delà de l'aspect technique. Nous vous proposons des contenus de sensibilisation et de formation aux bonnes pratiques en matière de sécurité. A travers notre réseau de partenaires, nous assurons également une présence continue à vos côtés, tout au long de vos projets

Ce livre blanc met l'accent sur **nos bonnes pratiques de sécurité** adaptées au secteur public, avec un focus sur la conformité et les mécanismes de chiffrement qui **renforcent la confiance**, et donne un aperçu des dernières innovations dont vous disposez en utilisant AWS.

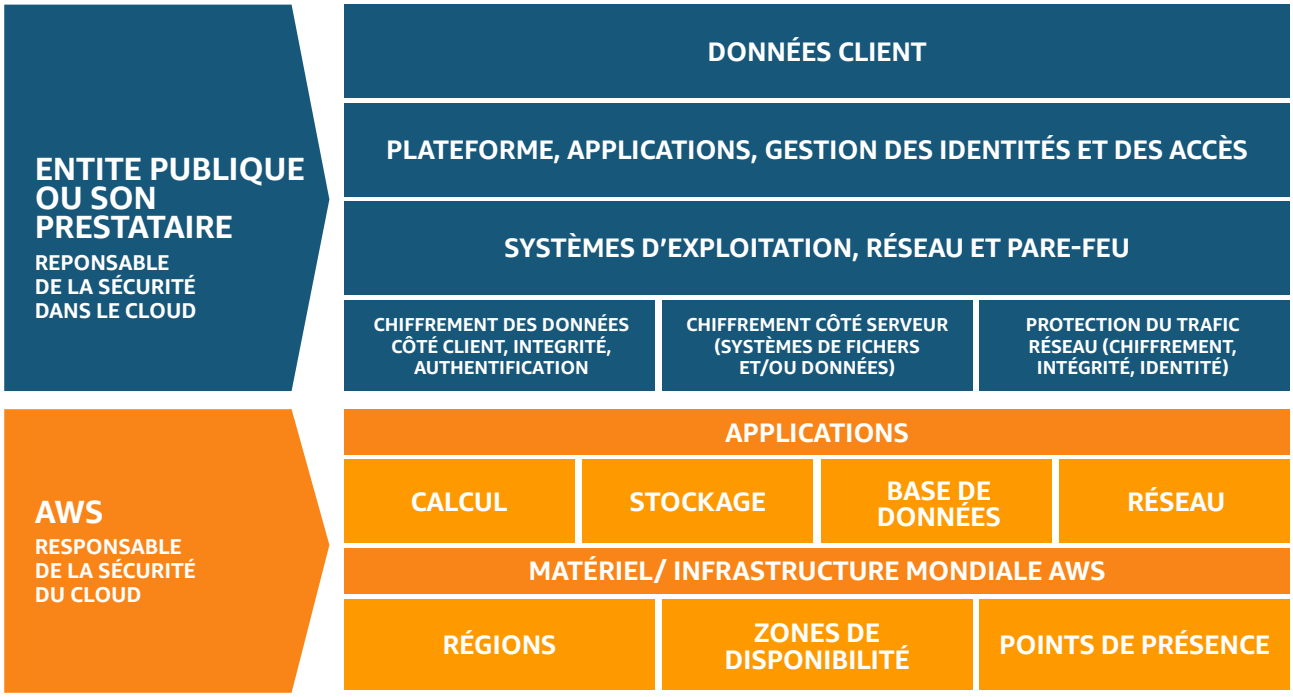
1

Comment déployer une solution cloud en toute sécurité ?

Si vous choisissez AWS pour déployer votre système d'information, quelles sont les **bonnes pratiques pour atteindre vos objectifs de sécurité** ? Avec AWS, vous bénéficiez d'un socle technique sécurisé, ensuite, vous devez configurer de façon adéquate les services que vous souhaitez utiliser. Pour aller plus loin, nous vous recommandons de vous former, et éventuellement de faire appel à un partenaire de notre réseau.

Un modèle de responsabilité partagée

Le Cloud AWS repose sur **un modèle de responsabilité partagée.** AWS est responsable de **la sécurité du cloud**, sur un périmètre allant de la sécurité physique des installations jusqu'à la couche de virtualisation en passant par la gestion des systèmes d'exploitation des machines hôte, ce qui limite votre charge opérationnelle. Le client est, quant à lui, responsable de la sécurité dans le cloud, c'est notamment le client qui va décider s'il va chiffrer ses données, quels personnels il va habiliter pour gérer ses ressources dans le cloud, ou encore quels serveurs il va éventuellement exposer à Internet.



Aussi, pour atteindre ses objectifs de sécurité, le client bénéficie :

- d'une part, des protections et contrôles de sécurité qui s'appliquent à son périmètre de responsabilité. Ce niveau est le même pour tous les clients d'AWS, et est vérifié par de nombreux audits liés à notre programme de conformité à des standards internationaux (voir le paragraphe 2.1 lié à la conformité plus loin) ;
- d'autre part, des services de sécurité AWS que le client met en œuvre dans le cloud AWS. Ces services sont configurés par le client, qui peut bénéficier de nombreux retours d'expérience et bonnes pratiques décrites ci-après.

Les outils clé en main disponibles pour la sécurité dans le Cloud AWS

Vous disposez de nombreux outils, présentés dans le détail dans la documentation en ligne d'AWS, sur https://aws.amazon.com/fr/security listés dans le tableau suivant.

CATÉGORIE	SERVICE	DESCRIPTION
GESTION DES IDENTITÉS ET DES ACCÈS	**AWS IAM**	Contrôle des identités et des accès
	AWS SSO	Mutualisation des points d'authentification
	Amazon Cognito	Gestion des identités pour les applications
	AWS Directory Service	Service d'active directory managé
	AWS Ressource Access Manager	Partage de ressources AWS
DÉTECTION D'INTRUSION	**AWS Security Hub**	Gestion centrale des exigences de sécurité
	Amazon Guarduty	Système de détection de menaces
	Amazon Inspector	Analyse de la sécurité des machines virtuelle
	AWS Config	Analyse de configurations de ressources AWS
	AWS CloudTrail	Log des activités sur AWS
	AWS IoT Device Defender	Gestion de la sécurité IoT
PROTECTION DES INFRASTRUCTURES	**AWS WAF**	Filtrage du trafic web malicieux
	AWS Firewall Manager	Gestion centrale des règles de pare-feux
	AWS Shield	Protection DDoS
PROTECTION DES DONNÉES	**Amazon Macie**	Protection des données personnelles
	AWS KMS	Magasin de clef cryptographique
	AWS CloudHSM	Magasin physique de clef cryptographique
	AWS Certificate Manager	Gestion & déploiement de certificats TLS
	AWS Secret Manager	Création & gestion des secrets
RÉPONSE À INCIDENTS	**Amazon Detective**	Investigation des causes premières
	CloudEndure Disaster Recovery	Gestion automatisée de la réponse à un désastre
CONFORMITÉ RÉGLEMENTAIRE	**AWS Artifact**	Rapports de conformité réglementaire d'AWS
GOUVERNANCE	**Amazon CloudWatch**	Rapport d'utilisation des ressources AWS
	AWS CloudFormation	Service « d'infrastructure as code »
	AWS Service Catalog	Configuration d'un catalogue de ressources
	AWS Systems Manager	Gestion des ressources centralisée
	AWS Trusted Advisor	Implémentation des « best practices »
	AWS Control Tower	Gestion d'environnement multi-comptes
	AWS Organizations	Gestion d'environnement multi-comptes

TOP 10

des bonnes pratiques sécurité à mettre en place dans votre compte AWS

01

Assurez-vous que vos informations de compte AWS sont précises, à jour, non liées à une personne physique unique : en cas de problème, ce sont ces informations qu'AWS utilisera pour vous contacter

02

Configurez une authentification multifacteur (MFA) pour protéger les accès d'administration

03

N'utilisez jamais de secrets (clés, mots de passe) dans vos développements

04

Assurez la rotation régulière des clés d'accès

05

Dans votre cloud privé virtuel, **filtrez strictement les flux réseau avec des groupes de sécurité** (Security Group) limités aux seuls échanges autorisés et documentés

06

Répertoriez et mettez en place une politique de classification de vos données

07

Centralisez les journaux CloudTrail, qui récapitulent les événements pour votre compte

08

Activez les outils de détection (GuardDuty, Security Hub, IAM Access Analyzer), apportez la réponse adaptée à chaque événement et automatisez progressivement

09

Privilégiez autant que possible les services managés AWS, qui limitent la charge de sécurité pour vous

10

Assurez-vous de la prise en compte de la sécurité en amont du cycle de développement logiciel ou du choix des progiciels

Lorsque vous démarrez sur AWS, et avant de vous lancer dans des déploiements complexes, quelques bonnes pratiques sont particulièrement importantes, décrites dans l'encadré.
D'une manière générale, AWS met à disposition de nombreux livres blancs et bonnes pratiques issues de son cadre « Well Architected Framework » avec un focus particulier sur la sécurité, disponibles sur https://aws.amazon.com/fr/security

Sécurité et formation : deux enjeux indissociables

Pour faciliter et accompagner le déploiement, AWS propose également **des contenus de formation gratuits.** Disponibles en autoformation, ces cours en ligne permettent aux responsables informatiques et à leurs équipes de découvrir les fondamentaux des concepts de sécurité du Cloud AWS, notamment le contrôle d'accès AWS, les méthodes de chiffrement des données et la manière dont l'accès réseau à votre infrastructure AWS peut être sécurisé.

Un réseau de partenaires spécialisés pour accompagner les administrations publiques

Le Réseau de partenaires AWS (APN) est l**e programme de partenariat mondial pour les entreprises de technologie et de conseil qui utilisent AWS** afin de créer des solutions et des services pour leurs clients.

Les partenaires membres de l'APN sont particulièrement bien placés pour vous aider à accélérer votre transition vers le cloud et à tirer pleinement parti des technologies de pointe qu'offre AWS. En ayant recours à leurs services, vous bénéficiez de conseils et de prestations d'experts de nos technologies, notamment pour l'utilisation de nos outils de sécurité et l'intégration des meilleures pratiques à chaque niveau de votre environnement. Vous trouverez l'ensemble de nos partenaires certifiés sur notre page : https://aws.amazon.com/fr/partners/

Les partenaires d'AWS pour vous accompagner pour la sécurité de votre SI

Les partenaires intégrateurs. Les partenaires intégrateurs sont notamment les intégrateurs de systèmes, les cabinets de conseil, les fournisseurs de services managés, qui peuvent vous aider à concevoir, auditer, opérer votre système d'information.

Les partenaires éditeurs de solutions sur AWS. Ce sont notamment des éditeurs de logiciels SaaS et des éditeurs indépendants, qui proposent sur notre marketplace par exemple des outils de test d'intrusion, des anti-virus, des systèmes d'exploitation durcis ou spécialisés, …
Vous trouverez l'ensemble de nos partenaires certifiés sur notre page :
https://aws.amazon.com/fr/partners/

2

Conformité et protection renforcée des données

En tant qu'entité du secteur public, vous devez vous assurer que votre système d'information sera conforme à la réglementation en vigueur et à votre politique de sécurité, il est donc important de comprendre comment AWS vous permet de répondre à vos exigences de sécurité.

AWS répond à vos besoins de conformité

Pour renforcer la confiance des clients dans les mesures de sécurité que nous mettons en œuvre, AWS se soumet régulièrement à des évaluations réalisées par des auditeurs tiers indépendants dans le cadre de nombreuses normes, standards, cadres et législations portant sur la sécurité. Ces évaluations donnent lieu à une certification, à un rapport d'audit ou une attestation de conformité.

Ainsi, par exemple, AWS dispose de certifications pour les normes ISO/IEC 27001, 27017 et 27018, de rapports SOC 1, 2 et 3 (System Organization Control) qui portent sur vérification dans la durée de la mise en œuvre par AWS de ses principaux contrôles et objectifs en termes de sécurité. AWS dispose également de la certification HDS (Hébergement de Données de Santé) définie par l'Agence du Numérique en Santé en France, pour les services présents dans les Région Europe (Paris), Irlande et Francfort. Les différents rapports, certifications, accréditations et attestations de tiers émis par les auditeurs d'AWS sont disponibles publiquement sur AWS Artifact (https://aws.amazon.com/fr/artifact/).

Ainsi, par rapport à votre propre cahier des charges d'exigences de sécurité, vous aurez connaissance des contrôles de sécurité mis en œuvre par AWS et dont vous héritez pour bâtir votre propre système d'information.

Zoom sur la conformité au RGPD

Le Règlement général sur la protection des données (RGPD) protège les droits fondamentaux des personnes concernées au sein de l'Union européenne en matière de respect de la confidentialité et de protection des données personnelles.

Outre notre propre conformité au RGPD, AWS s'engage à offrir des services et des ressources à nos clients pour leur permettre de respecter les exigences RGPD susceptibles de s'appliquer à leurs activités (chiffrement, surveillance et journalisation, contrôle d'accès, confidentialité des données, sécurité dans la conception…). Il est en effet important de comprendre que lorsque vous utilisez les services AWS pour traiter des données personnelles, AWS agit comme sous-traitant au sens du RGPD. Les engagements d'AWS en tant que sous-traitant sont portés par notre DPA (data privacy addendum), conforme au RGPD.

En tant que responsable du traitement, vous conservez alors la responsabilité de mettre en œuvre les mesures qui s'appliquent spécifiquement à votre système. Vous avez l'entier contrôle sur vos contenus dans AWS : vous déterminez la région géographique du stockage et du traitement des données, vous pouvez décider de positionner votre contenu dans une des régions AWS en Europe comme par exemple la région Paris, et AWS ne déplace pas le contenu des clients. Vous décidez du niveau de chiffrement, vous définissez les règles d'accès à vos contenus via des utilisateurs, des groupes, des autorisations et des informations d'identification que vous contrôlez vous-mêmes. AWS propose plus de 500 fonctions et services axés sur la sécurité et la conformité, et de nouvelles fonctions sont lancées régulièrement.

De nombreuses ressources en ligne sur https://aws.amazon.com/fr/gdpr-center/ sont également disponibles pour vous aider.

D'un point de vue **contractuel**, en tant que responsable du traitement, vous devez vous assurer que vos sous-traitants prennent des engagements contractuels sur la protection des données exigés par le RGPD. Les engagements d'AWS en la matière sont rassemblés dans notre DPA (*Data processing addendum* – Addendum sur le traitement des données).

Ce DPA est disponible ici : https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf

Le chiffrement : un niveau supplémentaire de protection des données

Le chiffrement des données est une mesure de sécurité généralement recommandée pour protéger vos données. Tout d'abord, dans son domaine de responsabilité, sur ses infrastructures, AWS met en œuvre massivement le chiffrement : par exemple, toutes les données circulant sur le réseau mondial AWS qui interconnectent nos centres de données et nos régions sont chiffrées automatiquement au niveau de la couche physique avant de quitter nos installations sécurisées. Des couches de chiffrement supplémentaires existent également : par exemple, pour les connexions TLS client ou de service à service.

Côté client, nous fournissons des outils qui vous permettent de chiffrer facilement vos données en transit et au repos afin de vous assurer que seuls vos utilisateurs autorisés peuvent y accéder, à l'aide de vos clés gérées par notre AWS Key Management System (KMS). **KMS s'appuie sur un module de sécurité matériel (Hardware Security Module, HSM).** Il s'agit d'un composant informatique spécialisé qui intègre plusieurs contrôles de sécurité visant à stocker hermétiquement les clés de chiffrement. KMS a été certifié par des auditeurs tiers indépendants (certification FIPS 140-2). Il est conçu de telle sorte que **les clés de chiffrement restent sous le contrôle exclusif du client.**

AWS KMS est intégré aux services AWS pour simplifier l'utilisation de clés afin de chiffrer les données dans votre système d'information. Vous définissez le niveau de contrôle d'accès dont vous avez besoin, notamment pour autoriser l'utilisation des clés. KMS consigne toutes les utilisations de clés dans AWS CloudTrail afin de vous donner une vue indépendante des personnes ayant accès à vos données chiffrées, y compris dans les services AWS qui les utilisent en votre nom. A noter que ces services de chiffrement sont **sans impact sur les performances.**

Pour répondre à des besoins spécifiques, AWS propose également **AWS CloudHSM**, qui donne aux clients un accès complet à une partition dédiée d'un HSM certifié FIPS 140-2 level 3, hébergé sur AWS.

3

Les innovations d'AWS dans le domaine de la sécurité

AWS investit massivement dans le domaine de la sécurité pour que vous puissiez bénéficier des services les plus avancés. A travers trois exemples, les architectures NITRO, l'utilisation de l'intelligence artificielle et les techniques de sécurité vérifiables, nous souhaitons vous donner un aperçu des mécanismes techniques spécifiques dont vous bénéficiez lorsque vous utilisez le Cloud AWS.

L'architecture de nos hyperviseurs NITRO

Le système AWS NITRO est la plateforme sous-jacente à nos instances virtuelles EC2, dont vous bénéficiez dès que vous utilisez une instance EC2 récente. AWS a complètement reconçu son infrastructure de virtualisation. Classiquement, cette virtualisation repose sur un logiciel d'hypervision, qui s'appuie sur le matériel physique et son BIOS, et virtualise le processeur, le stockage, le réseau, et fournit les capacités de management. Avec NITRO, nous avons découplé ces fonctions et les avons déléguées à des composants matériels dédiés (cartes NITRO pour le stockage, pour le réseau, pour les fonctions de gestion, pour le contrôle de sécurité du BIOS, …). Ainsi, la plupart des fonctions classiques de l'hyperviseur sont ainsi exécutées sur des cartes matérielles.

En termes de sécurité, ceci présente de nombreux avantages. Par exemple, en redéveloppant un hyperviseur réduit aux fonctions strictement nécessaires, **nous avons supprimé la possibilité de se connecter à l'hôte.** Cela signifie qu'aucun employé d'AWS n'a d'accès administrateur ni au serveur hôte, ni aux instances EC2 du client ou à leur contenu. De même, AWS n'a aucune possibilité (cette possibilité n'existe pas dans le code) d'accéder à la mémoire vive utilisée par un client, ou d'en faire un « dump ». Nitro vous permet également de créer des enclaves particulières dans lesquelles vous pouvez exécuter du code sensible que vous pouvez isoler de vos autres processus.

Vous pouvez trouver une description plus complète de ces avantages sur :
https://aws.amazon.fr/ec2/nitro

L'intelligence artificielle au service de la sécurité

L'intelligence artificielle (IA) est présente dans de nombreuses innovations aujourd'hui. AWS propose à ses clients de nombreux services d'apprentissage automatisé, des services IA pré-entraînés prêts à l'emploi et des infrastructures spécialement adaptées à l'IA.

Dans le domaine de la sécurité, AWS utilise des algorithmes basés sur de l'apprentissage machine pour enrichir ses services. Par exemple :

- Amazon Macie est un service que vous pouvez utiliser pour identifier et répertorier vos données sensibles et vérifier qu'elles sont stockées avec le niveau de protection adéquat.
- Predictive Scaling for EC2 est une fonction que vous pouvez utiliser pour anticiper les besoins de performance lors de pics de charge et ainsi réduire les risques d'indisponibilité de services.
- Amazon Fraud Detector est un service entièrement géré qui facilite l'identification de pratiques douteuses comme la fraude au paiement en ligne et la création de faux comptes. Amazon Fraud Detector utilise le machine learning (ML), et au travers de ce service, vous bénéficiez de plus de 20 ans d'expertise en détection de fraude d'AWS et d'Amazon.com.

Amazon GuardDuty et la détection des menaces

Amazon GuardDuty est le service de détection des menaces. Vous pouvez l'activer et l'utiliser pour surveiller en permanence les activités malveillantes et les comportements non autorisés afin de protéger vos comptes AWS, vos charges de travail et vos données stockées dans Amazon Simple Storage Service (Amazon S3).

Amazon GuardDuty identifie les menaces en surveillant en permanence l'activité du réseau, les modèles d'accès aux données et le comportement des comptes dans l'environnement AWS. Amazon GuardDuty, en préintégrant des flux d'information externes sur les menaces, associé au machine learning et aux modèles de comportement, vous aide à détecter des activités telles que le minage de crypto-monnaie, le comportement de compromission des informations d'identification, l'accès non autorisé et inhabituel aux données, la communication avec des serveurs de commande et de contrôle connus ou les appels d'API provenant d'IP malveillantes connues.

Amazon GuardDuty permet par ailleurs d'automatiser facilement la manière dont vous répondez aux menaces afin d'accélérer les corrections et la récupération.

La sécurité vérifiable : une preuve de sécurité additionnelle

Avec la technologie de raisonnement automatisé et l'application de la logique mathématique pour aider à répondre aux questions critiques sur votre infrastructure, AWS est capable de vérifier l'absence d'erreurs de codes et de mauvaises configurations qui pourraient constituer des vulnérabilités et exposer des données sensibles. Nous appelons cela la sécurité vérifiable. Celle-ci fournit une assurance plus élevée en matière de sécurité du cloud et dans le cloud.

Ces principes sont appliqués par AWS dans de nombreux domaines, notamment les plus sensibles du point de vue de la sécurité. Par exemple :

- **Vérification du code de boot :** nous avons formellement démontré que le code de boot utilisé sur nos serveurs AWS sont exempts de faille de sécurité mémoire, un point essentiel pour assurer la sécurité de nos centres de données.
- **Vérification formelle en continu de s2n, notre implémentation open source de TLS :** TLS est un protocole de sécurisation des échanges très répandu et largement utilisé par AWS, l'absence de vulnérabilité dans notre implémentation est donc critique. Aussi, nous en faisons une vérification formelle, et à chaque évolution du code, les preuves sont automatiquement revérifiées avec peu ou pas d'interaction avec les développeurs.
- **Analyse de l'accessibilité réseau :** Avec l'ensemble des mécanismes réseau disponibles (VPC, sous-réseaux, security groups, NACL), il peut être difficile de vérifier si une machine est potentiellement exposée à une connexion extérieure. AWS a développé un outil basé sur une analyse formelle, pour d'une part répondre à ses propres besoins de sécurité, et d'autre part, pour le mettre à disposition des clients (network reachability assessments dans Amazon Inspector)

Vous trouverez d'autres exemples et plus d'informations sur :
https://aws.amazon.com/fr/security/provable-security/

IAM Access Analyzer, le raisonnement automatisé pour vérifier vos configurations

La gestion des droits et des accès sur AWS repose sur un ensemble de stratégies IAM, stratégies liées aux ressources, stratégie de contrôles de services, qui permettent aux clients de définir qui peut accéder, sous quelles conditions, à une ressource. Certaines configurations peuvent parfois être complexes, et il est important, pour nos clients, d'être certains que la configuration mise en place correspond à la règle souhaitée, et surtout éviter de découvrir une erreur de configuration à l'occasion d'une intrusion.

IAM Access Analyzer s'appuie sur Zelkova, un moteur d'analyse formelle qui vérifie automatiquement et mathématiquement les politiques d'accès et les conséquences potentielles de ses modifications. Vous pouvez vous appuyer sur IAM Access Analyzer pour vous représenter précisément les politiques et vérifier qu'elles correspondent à la configuration que vous souhaitez, pour améliorer la confiance dans vos configurations de sécurité, éviter des erreurs, et appliquer le **principe de moindre privilège** dans vos politiques de sécurité IAM.

LE SAVIEZ-VOUS ?

Vous souhaitez vous lancer ? AWS est disponible à l'UGAP.

Le marché de Services d'informatique en nuage (Cloud Externe) de l'UGAP a été attribué à Capgemini, partenaire d'AWS, en avril 2020. Capgemini agit en tant que revendeur de technologies de cloud public, incluant le catalogue d'AWS. Ce marché soutient la stratégie cloud de l'Etat et sa doctrine d'utilisation des services cloud en permettant à l'ensemble des entités publiques bénéficiaires de l'UGAP d'accéder facilement et rapidement (sans procédure d'appel d'offres) aux services cloud leur permettant d'implémenter leurs projets.

Grâce à ce marché, vous pouvez accélérer vos projets sur AWS en bénéficiant de toute la souplesse du catalogue ainsi que de tarifs préférentiels.