Livre blanc AWS

Présentation de la sécurité dans AWS

Présentation de la sécurité dans AWS: Livre blanc AWS

Table of Contents

Résumé 1
Résumé 1
Sécurité de l'infrastructure AWS 2
Produits et fonctions de sécurité 4
Sécurité de l'infrastructure 4
Inventaire et gestion de la configuration 5
Chiffrement des données 5
Contrôle des identités et des accès 6
Surveillance et journalisation 6
Produits de sécurité dans AWS Marketplace 7
Recommandations de sécurité 8
Conformité 10
Autres lectures 12
Révisions du document 13
Mentions légales 14

Présentation de la sécurité dans AWS

Date de publication : 11 novembre 2021 (Révisions du document)

Résumé

Amazon Web Services (AWS) propose une plateforme de cloud computing évolutive, conçue pour un niveau élevé de disponibilité et de fiabilité, et dotée des outils nécessaires pour exécuter une large gamme d'applications. Garantir la confidentialité, l'intégrité et la disponibilité de vos systèmes et données est une priorité pour AWS, et nous avons à cœur d'être à la hauteur de votre confiance. Ce document présente l'approche d'AWS en matière de sécurité, notamment les contrôles dans l'environnement AWS et certains des produits et fonctions qu'AWS met à la disposition de ses clients pour leur permettre d'atteindre leurs objectifs de sécurité.

Sécurité de l'infrastructure AWS

L'infrastructure AWS a été architecturée pour créer l'un des environnements de cloud computing les plus flexibles et sécurisés disponibles à ce jour. Elle est conçue pour fournir une plateforme extrêmement évolutive et fiable, qui permet aux clients de déployer des applications et des données rapidement et en toute sécurité.

Cette infrastructure est conçue et gérée non seulement conformément aux bonnes pratiques et aux standards de sécurité, mais également en conservant à l'esprit les besoins uniques du cloud. AWS utilise des contrôles redondants et multicouches, la validation et le test continus et une grande part d'automatisation pour garantir le suivi et la protection 24 heures sur 24 et 7 jours sur 7 de l'infrastructure sous-jacente. AWS garantit que ces contrôles sont répliqués dans chaque nouveau centre de données ou service.

Tous les clients AWS bénéficient d'une architecture de centre de données et de réseau conçue pour satisfaire aux exigences de nos clients les plus pointilleux en matière de sécurité. Cela vous permet de vous appuyer sur une infrastructure résiliente, conçue pour un niveau élevé de sécurité, sans les investissements ou les frais d'exploitation engendrés par un centre de données classique.

AWS fonctionne selon un modèle de sécurité partagé, dans lequel AWS est responsable de la sécurité de l'infrastructure de cloud sous-jacente et vous êtes responsable de la sécurisation des charges de travail que vous déployez sur AWS (Figure 1). Cela vous donne la flexibilité et l'agilité dont vous avez besoin pour mettre en œuvre les contrôles de sécurité les plus pertinents pour les fonctions liées à vos activités dans l'environnement AWS. Vous pouvez restreindre fortement l'accès aux environnements qui traitent les données sensibles, ou déployer des contrôles moins stricts pour les informations que vous souhaitez rendre publiques.

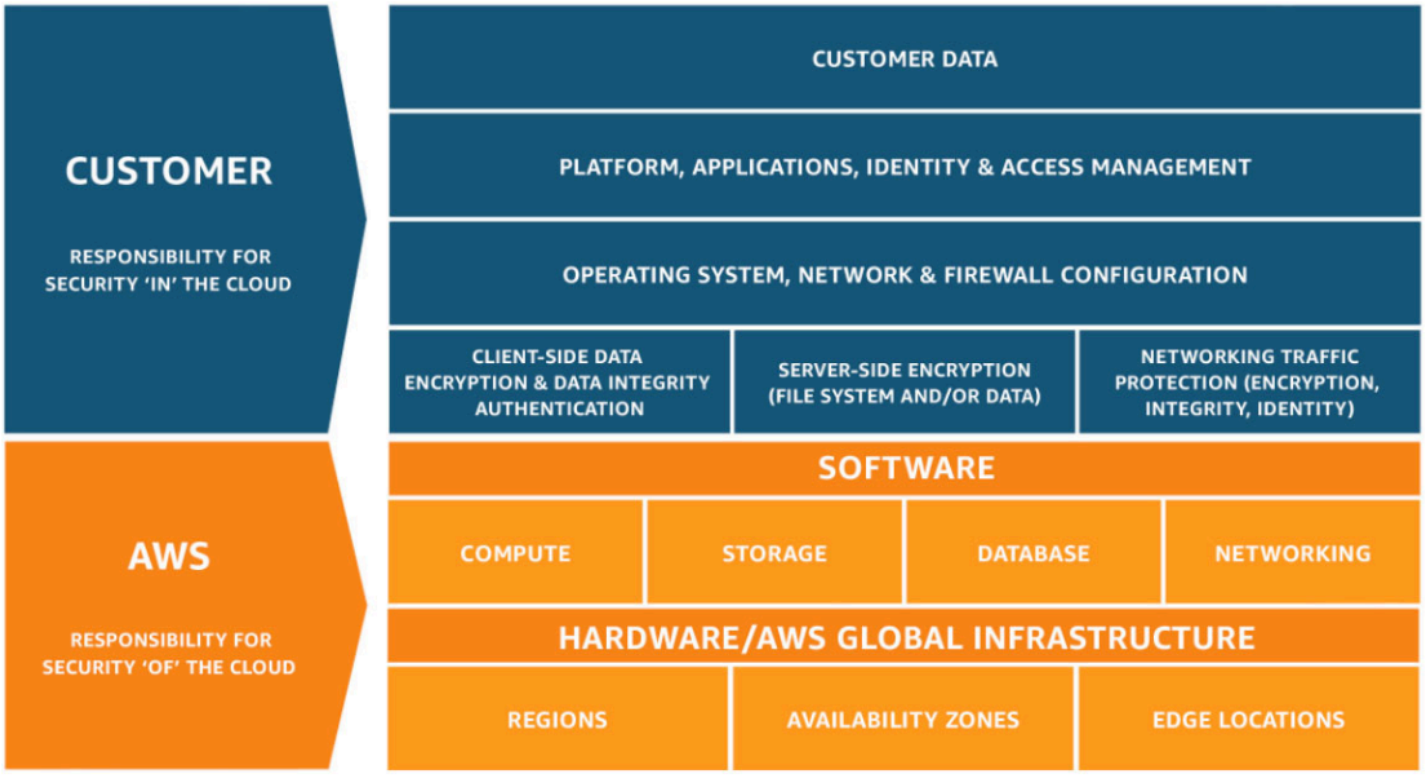

Figure 1 : modèle de responsabilité de sécurité partagée AWS

Produits et fonctions de sécurité

AWS et ses partenaires proposent une large gamme d'outils et de fonctions qui vous permettent d'atteindre vos objectifs de sécurité. Ces outils reproduisent les contrôles familiers que vous déployez dans vos environnements sur site. AWS propose des outils et des fonctions de sécurité spécifiques à la sécurité du réseau, à la gestion de la configuration, au contrôle d'accès et à la sécurité des données. De plus, AWS propose des outils de surveillance et de journalisation destinés à fournir une visibilité complète sur ce qui se passe dans votre environnement.

Rubriques

- Sécurité de l'infrastructure
- Inventaire et gestion de la configuration
- Chiffrement des données
- Contrôle des identités et des accès
- Surveillance et journalisation
- Produits de sécurité dans AWS Marketplace

Sécurité de l'infrastructure

AWS propose plusieurs fonctions et services de sécurité pour renforcer la confidentialité et contrôler l'accès au réseau. Par exemple :

- Des pare-feu intégrés dans Amazon VPC vous permettent de créer des réseaux privés et de contrôler l'accès à vos instances ou applications. Les clients peuvent contrôler le chiffrement en transit avec TLS entre les services AWS.
- Des options de connectivité autorisant les connexions privées ou dédiées depuis votre bureau ou un environnement sur site.
- Des technologies de limitation des attaques DDoS qui s'appliquent au niveau 3 ou 4, ainsi qu'au niveau 7. Elles peuvent être appliquées dans le cadre de stratégies de diffusion d'applications et de contenu.
- Chiffrement automatique de tout le trafic sur le réseau AWS mondial et les réseaux régionaux entre les installations sécurisées AWS.

Inventaire et gestion de la configuration

AWS propose une gamme d'outils destinés à vous aider à aller vite, tout en vous permettant de vous assurer que vos ressources cloud respectent les standards organisationnels et les bonnes pratiques en vigueur. Par exemple :

- Outils de déploiement pour gérer la création et la mise hors service des ressources AWS conformément aux standards de l'organisation.
- Outils d'inventaire et de gestion de la configuration destinés à identifier les ressources AWS, puis à suivre et gérer les modifications qui leur sont apportées au fil du temps.
- Outils de définition et de gestion de modèles servant à créer des machines virtuelles standard, préconfigurées et robustes pour les instances EC2.

Chiffrement des données

AWS vous donne la possibilité d'ajouter une couche de sécurité supplémentaire à vos données au repos dans le cloud, en vous fournissant des fonctions de chiffrement évolutives et efficaces. Par exemple :

- Des fonctions de chiffrement des données au repos disponibles avec la plupart des services AWS, notamment Amazon EBS, Amazon S3, Amazon RDS, Amazon Redshift, Amazon ElastiCache, AWS Lambda et Amazon SageMaker
- Des possibilités flexibles de gestion des clés, notamment AWS Key Management Service, qui permettent de choisir entre confier la gestion des clés de chiffrement à AWS et garder le contrôle complet de ses propres clés
- Un stockage matériel dédié de clés cryptographiques utilisant AWS CloudHSM, ce qui vous aide à répondre à vos exigences en matière de conformité
- Des files d'attente de messages chiffrées pour la transmission des données sensibles à l'aide du chiffrement côté serveur (SSE) pour Amazon SQS

En outre, AWS fournit des API pour vous permettre d'intégrer le chiffrement et la protection des données à tous les services que vous développez ou déployez dans un environnement AWS.

Contrôle des identités et des accès

AWS vous propose des fonctions servant à définir, appliquer et gérer les stratégies d'accès utilisateur pour tous les services AWS. Par exemple :

- AWS Identity and Access Management (IAM) vous permet de définir des comptes utilisateurs avec des autorisations d'accès aux différentes ressources AWS et AWS Multi-Factor Authentication pour les comptes privilégiés, y compris des options pour les authentificateurs logiciels et matériels. IAM peut être utilisé pour accorder à vos employés et vos applications un accès fédéré à AWS Management Console et aux API de service AWS, à l'aide de vos systèmes d'identités existants, tels que Microsoft Active Directory (AD) ou l'offre d'un autre partenaire.
- AWS Directory Service permet l'intégration et la fédération avec les annuaires d'entreprise pour réduire les coûts administratifs et améliorer l'expérience de l'utilisateur final.
- AWS Single Sign-On (AWS SSO) vous permet de gérer facilement l'accès SSO et les autorisations utilisateur de l'ensemble de vos comptes dans AWS Organizations et ce, de façon centralisée.

AWS propose une intégration d'Identity and Access Management pour beaucoup de ses services, ainsi que l'intégration d'API dans vos propres applications ou services.

Surveillance et journalisation

AWS fournit des outils et des fonctions qui vous permettent de voir ce qui se passe au sein de votre environnement AWS. Par exemple :

- Avec AWS CloudTrail, vous pouvez surveiller vos déploiements AWS dans le cloud en obtenant un historique des appels d'API AWS pour votre compte, notamment les appels d'API effectués via AWS Management Console, les kits de développement AWS, les outils de ligne de commande, ainsi que les services AWS de niveau plus élevé. Vous pouvez également identifier les utilisateurs et les comptes ayant appelé des API AWS pour les services prenant en charge CloudTrail, l'adresse IP source à partir de laquelle les appels ont été effectués, ainsi que le moment où ils ont eu lieu.
- Amazon CloudWatch fournit une solution de surveillance fiable, évolutive et flexible que vous pouvez commencer à utiliser en seulement quelques minutes. Vous n'avez plus besoin de configurer, gérer et mettre à l'échelle vos propres systèmes et infrastructures de surveillance.
- Amazon GuardDuty est un service de détection des menaces qui surveille en permanence les activités malveillantes et les comportements non autorisés afin de protéger vos comptes AWS et

vos charges de travail. Amazon GuardDuty affiche des notifications via Amazon CloudWatch afin de vous permettre de déclencher une réponse automatisée ou de notifier un intervenant humain.

Ces outils et fonctions vous donnent la visibilité dont vous avez besoin pour détecter les problèmes avant qu'ils n'affectent vos activités, ainsi que pour améliorer la sécurité et réduire le profil de risque de votre environnement.

Produits de sécurité dans AWS Marketplace

Le fait de déplacer des charges de travail de production vers AWS peut permettre aux organisations d'améliorer leur agilité, leur capacité de mise à l’échelle, leur innovation et de réaliser des économies de coûts, tout en maintenant un environnement sécurisé. AWS Marketplace propose des produits de sécurité de pointe qui sont équivalents, identiques ou qui s'intègrent aux contrôles existants dans vos environnements sur site. Ces produits complètent les services AWS existants pour vous permettre de déployer une architecture de sécurité exhaustive et une expérience plus homogène dans vos environnements cloud et sur site.

Recommandations de sécurité

AWS fournit aux clients des recommandations et une expertise par le biais des outils en ligne, des ressources, du support et des services professionnels proposés par AWS et ses partenaires.

AWS Trusted Advisor est un outil en ligne faisant office d'expert en cloud personnalisé, qui vous permet de configurer vos ressources de manière à respecter les bonnes pratiques. Trusted Advisor inspecte votre environnement AWS pour combler les lacunes de sécurité, et détecte les opportunités d'économies, d'amélioration des performances du système et d'augmentation de la fiabilité.

Les équipes de compte AWS constituent un premier point de contact. Elles vous guident dans le déploiement et la mise en œuvre et vous orientent vers les ressources adéquates pour résoudre les problèmes de sécurité que vous pouvez rencontrer.

AWS Enterprise Support offre un temps de réponse de 15 minutes et est disponible 24 heures sur 24 et 7 jours sur 7 par téléphone, messagerie instantanée ou e-mail, avec un responsable technique de compte dédié. Ce service de conciergerie garantit que les problèmes des clients sont traités le plus rapidement possible.

Le réseau de partenaires AWS propose des centaines de produits de pointe du secteur qui sont équivalents, identiques ou intégrables aux contrôles en place dans vos environnements sur site. Ces produits complètent les services AWS existants pour vous permettre de déployer une architecture de sécurité exhaustive et une expérience plus homogène dans vos environnements cloud et sur site, et vous pouvez aussi mobiliser des centaines de partenaires consultants AWS certifiés dans le monde entier pour vous aider à répondre à vos besoins en matière de sécurité et de conformité.

AWS Professional Services comprend une pratique spécialisée de sécurité, de risque et de conformité destinée à vous aider à gagner en confiance et en capacité technique lors de la migration de vos charges de travail les plus sensibles vers le cloud AWS. AWS Professional Services aide les clients à élaborer des politiques et des pratiques de sécurité fondées sur des modèles éprouvés, et à garantir que la conception de la sécurité des clients répond aux exigences internes et externes en matière de conformité.

AWS Marketplace est un catalogue numérique contenant une liste des milliers de logiciels provenant de fournisseurs indépendants de logiciels qui vous permettent de facilement trouver, tester, acheter et déployer des logiciels qui s'exécutent sur AWS. Les produits AWS Marketplace Security complètent les services AWS existants pour vous permettre de déployer une architecture de sécurité exhaustive et une expérience plus homogène dans vos environnements cloud et sur site.

Les bulletins de sécurité AWS fournissent des bulletins de sécurité concernant les vulnérabilités et menaces actuelles. Ils permettent aux clients de travailler avec les experts en sécurité d'AWS pour répondre aux préoccupations liées, par exemple, au signalement des abus et des vulnérabilités, et à la réalisation de tests d'intrusion. Nous disposons aussi de ressources en ligne pour le signalement des vulnérabilités.

La documentation de sécurité AWS montre comment configurer les services AWS pour atteindre vos objectifs en matière de sécurité et de conformité. Les clients AWS bénéficient d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des organisations les plus pointilleuses en termes de sécurité.

L'AWS Well-Architected Framework aide les architectes cloud à créer une infrastructure sécurisée, hautement performante, résiliente et efficace pour leurs applications. L'AWS Well-Architected Framework comprend un pilier de sécurité qui se concentre sur la protection des informations et des systèmes. Parmi les thèmes clés figurent la confidentialité et l'intégrité des données, l'identification et la gestion des identités autorisées à gérer les privilèges, la protection des systèmes et l'établissement de contrôles pour détecter les événements de sécurité. Les clients peuvent utiliser AWS Well-Architected Tool depuis AWS Management Console ou faire appel aux services de l'un des partenaires AWS pour les aider.

AWS Well-Architected Tool vous aide à passer en revue l'état de vos charges de travail et à les comparer aux bonnes pratiques les plus récentes en matière d'architecture AWS. Cet outil gratuit est disponible dans AWS Management Console, après avoir répondu à une série de questions au sujet de l'excellence opérationnelle, de la sécurité, de la fiabilité, de l'efficacité des performances, et de l'optimisation des coûts. AWS Well-Architected Tool fournit alors un plan sur la façon de concevoir une architecture pour le cloud en appliquant les bonnes pratiques établies.

Conformité

La conformité AWS permet aux clients de comprendre les contrôles rigoureux mis en place chez AWS pour garantir la sécurité et la protection des données dans le cloud AWS. Lorsque les systèmes sont intégrés au cloud AWS, AWS et ses clients partagent les responsabilités en matière de conformité. Les environnements informatiques AWS font l'objet d'audits continus et bénéficient de certifications de la part d'organismes d'accréditation de plusieurs régions et secteurs d'activité, notamment SOC 1/SSAE 16/ISAE 3402 (anciennement SAS 70), SOC 2, SOC 3, ISO 9001/ ISO 27001, FedRAMP, DoD SRG et PCI DSS niveau 1.i. En outre, AWS dispose également de programmes d'assurance qui fournissent des modèles et des mappages de contrôle pour aider les clients à établir la conformité de leurs environnements exécutés sur AWS. Pour obtenir la liste complète des programmes, veuillez consulter Programmes de conformité AWS.

Nous pouvons confirmer que tous les services AWS peuvent être utilisés en conformité avec le RGPD. Cela signifie qu'en plus de tirer parti de toutes les mesures qu'AWS prend déjà pour maintenir la sécurité des services, les clients peuvent déployer les services AWS dans le cadre de leurs plans de conformité au RGPD. AWS propose un addendum sur le traitement des données respectant le RGPD (GDPR DPA) qui vous permet de respecter les obligations contractuelles du RGPD. Le RGPD DPA d'AWS est intégré aux Conditions de service AWS et s'applique automatiquement à tous les clients dans le monde entier qui en ont besoin pour respecter le RGPD. Amazon.com, Inc. est certifié conforme au bouclier de protection des données UE-États-Unis et AWS est couvert par cette certification. Cela aide les clients qui choisissent de transférer leurs données personnelles vers les États-Unis à respecter leurs obligations de protection des données. La certification d'Amazon.com Inc. est disponible sur le site Web du bouclier de protection des données UE-États-Unis : https://www.privacyshield.gov/list

En travaillant dans un environnement accrédité, les clients réduisent la portée et le coût des audits qu'ils doivent effectuer. AWS fait continuellement l'objet d'évaluations de son infrastructure sous-jacente, y compris l'environnement physique et la sécurité de son matériel et des centres de données, ce qui permet aux clients d'exploiter ces certifications et tout simplement d'hériter de ces contrôles.

Dans un centre de données classique, les activités de conformité courantes sont souvent manuelles et périodiques. Ces activités comprennent la vérification des configurations de ressources et la génération de rapports sur les activités administratives. En outre, les rapports qui en résultent sont obsolètes avant même d'être publiés. L'exploitation dans un environnement AWS permet aux clients de tirer parti d'outils intégrés et automatisés comme AWS Security Hub, AWS Config et AWS

CloudTrail pour la validation de la conformité. Ces outils permettent de réduire les efforts nécessaires aux audits, car ces tâches deviennent routinières, continues et automatisées. En passant moins de temps sur les opérations manuelles, vous faites évoluer le rôle de la conformité dans votre entreprise, transformant une charge administrative nécessaire en un processus de gestion des risques et d'amélioration de votre niveau de sécurité.

Autres lectures

Pour plus d'informations, consultez les ressources suivantes :

Pour plus d'informations sur...	Consultez
Rubriques clés, zones de recherche et opportunités de formation à la sécurité du cloud sur AWS	Apprentissage de la sécurité du cloud AWS
Le framework d'adoption du Cloud AWS qui organise les recommandations en six zones d'intérêt : entreprise, collaborateurs, gouvernance, plateforme, sécurité et opérations.	Cadre d'adoption du cloud AWS
Contrôles spécifiques mis en place chez AWS ; comment intégrer AWS dans votre framework existant	Amazon Web Services : risques et conformité
Bonnes pratiques en matière de sécurité, d'identité et de conformité	Bonnes pratiques en matière de sécurité, d'identité et de conformité
Pilier Sécurité - AWS Well-Architected Framework	Pilier Sécurité - AWS Well-Architected Framework

Révisions du document

Pour être informé des mises à jour de ce livre blanc, abonnez-vous au flux RSS.

update-history-change	update-history-description	update-history-date
Livre blanc mis à jour	Mise à jour pour les liens relatifs aux lectures supplémentaires.	11 novembre 2021
Livre blanc mis à jour	Mis à jour pour les derniers services, ressources et technologies.	22 janvier 2020
Publication initiale	Publication de Présentation de la sécurité dans AWS.	1 juillet 2015

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 le modifie.