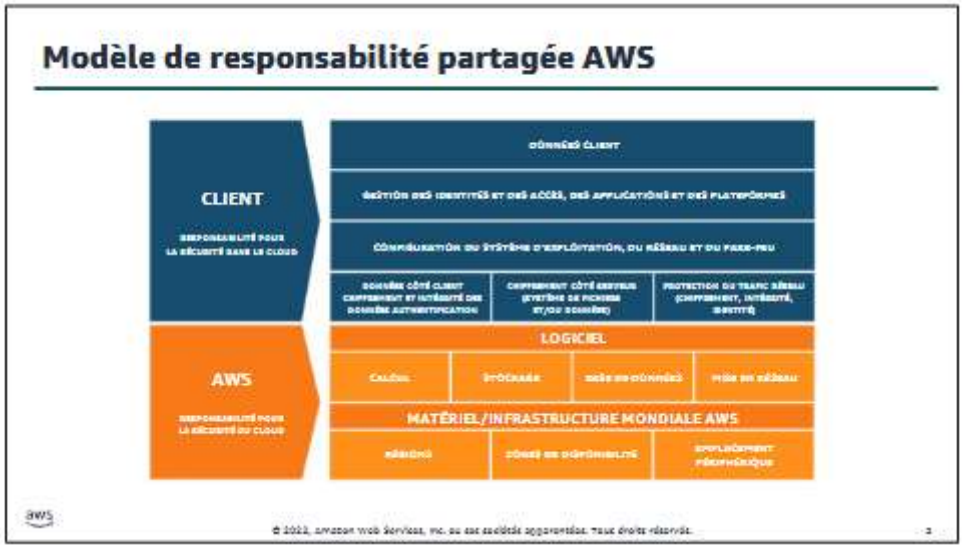
Responsabilités partagée du Cloud AWS

AWS et le client se partagent la responsabilité de la sécurité et de la conformité. Ce modèle de responsabilité partagée est conçu pour alléger la charge opérationnelle du client. Dans le même temps, pour assurer la flexibilité et le contrôle client qui permettent le déploiement de solutions client sur AWS, le client reste responsable de certains aspects de la sécurité globale. La répartition des responsabilités est souvent illustrée par le concept de sécurité du Cloud par opposition à la sécurité dans le Cloud.

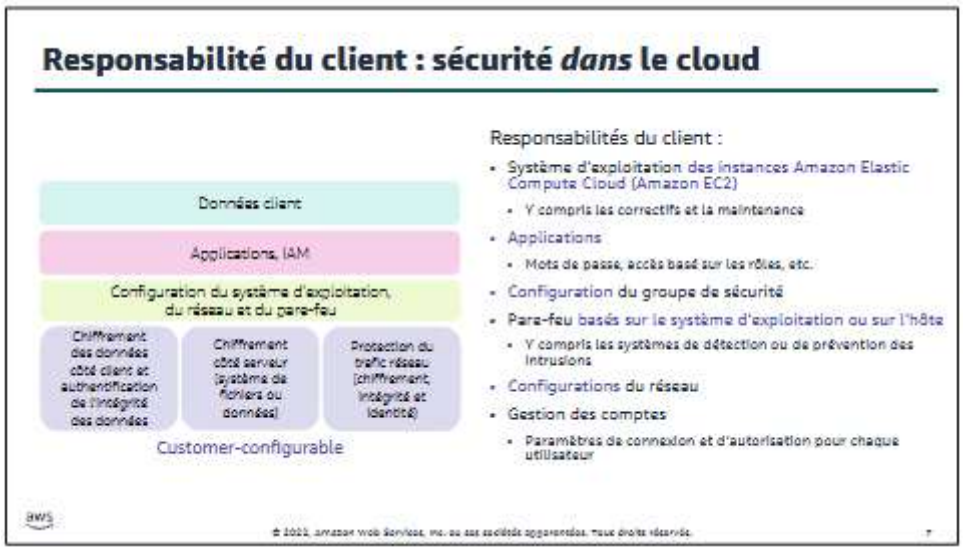


AWS exploite, gère et contrôle les composants depuis la couche de virtualisation logicielle jusqu'à la sécurité physique des installations dans lesquelles les services AWS opèrent. AWS se charge de protéger l'infrastructure sur laquelle s'exécutent tous les services proposés dans AWS Cloud. Cette infrastructure est composée du matériel, des logiciels, du réseau et des installations exécutant les services d'AWS Cloud.

Le client est responsable du chiffrement des données au repos et en transit. Il doit aussi s'assurer que le réseau est configuré de manière à garantir sa sécurité, et que les autorisations de sécurité et autres identifiants sont gérés de manière sûre. De plus, le client est responsable de la configuration des groupes de sécurité et de la configuration du système d'exploitation au niveau des instances de calcul qu'il lance (y compris les mises à jour et les correctifs de sécurité).

Tandis que l'infrastructure Cloud est sécurisée et maintenue par AWS, les clients sont responsables de la sécurité de tout ce qu'ils mettent dans le Cloud.

Le client est **responsable** de ce qui est mis en œuvre à l'aide des services AWS et des applications connectées à AWS. La procédure de sécurité que vous devez appliquer dépend des services que vous utilisez et de la complexité de votre système.



Les responsabilités du client incluent la sélection et la sécurisation de tous les systèmes d'exploitation d'instance, la sécurisation des applications lancées sur les ressources AWS, les configurations de groupe de sécurité, les configurations de pare-feu, les configurations réseau et la gestion sécurisée des comptes.

Lorsque les clients utilisent les services AWS, ils conservent un contrôle total de leur contenu. Les clients sont responsables de la gestion des exigences critiques en matière de sécurité des contenus, notamment :

·Le contenu qu'ils ont choisi de stocker sur AWS

·Quels services AWS sont utilisés avec le contenu

· Dans quel pays le contenu est stocké

·Le format et la structure de ce contenu et sa dissimulation, son anonymisation ou son chiffrement.

·Les personnes qui ont accès à ce contenu et la façon dont ces droits d'accès sont accordées, gérés et révoqués.

Les clients conservent le contrôle sur la sécurité qu'ils ont choisi de mettre en place pour protéger leurs propres donnés, leur environnement, les applications, les configurations IAM, ainsi que les systèmes d'exploitation.

L'infrastructure en tant que service (IaaS) fait référence aux services qui fournissent des composants de base pour l'Informatique dans le cloud. Cela comprend généralement l'accès requis pour configurer le réseau, les ordinateurs (virtuels ou sur du matériel dédié) et l'espace de stockage de données. Les services cloud qui entrent dans la catégorie IaaS offrent au client le niveau de flexibilité et de contrôle de gestion le plus élevé de leurs ressources informatiques. Les services IaaS s'apparentent aux ressources informatiques sur site que de nombreux services informatiques connaissent bien.

Les services AWS, comme Amazon EC2, peut être classé comme des services IaaS. Dès lors, le client doit effectuer toutes les tâches de configuration et de gestion de la sécurité nécessaires. Les clients qui déploient les instances EC2 sont **responsables de la gestion du système d'exploitation invité (y compris les mises à jour et les correctifs de sécurité), de tout logiciel d'application installé sur les instances et de la configuration des groupes de sécurité fournis par AWS.**

La plateforme en tant que service (PaaS) désigne services qui **évitent au client de devoir gérer l'infrastructure sous-jacente (matériel, systèmes d'exploitation, etc.)**. Les services PaaS permettent au client de se concentrer entièrement sur le déploiement et la gestion des applications. Les clients n'ont pas à se soucier de l'approvisionnement des ressources, de la planification de la capacité, de la maintenance logicielle ou de l'application des correctifs

Les services AWS tels qu'**AWS Lambda** et **Amazon RDS** peuvent être classés dans la catégorie **PaaS**, car AWS gère la couche d'infrastructure, le système d'exploitation et les plateformes. Les clients ont uniquement besoin d'accéder aux points de terminaison pour stocker et récupérer leurs données. Avec les services PaaS, les clients sont responsables de la gestion de leurs données, de la classification de leurs ressources et de l'application des autorisations appropriées. Toutefois, ces services ressemblent davantage à des services gérés, AWS gérant une plus grande partie des exigences en matière de sécurité.

Pour ces services, AWS gère les tâches de sécurité de base, telles que l'application de correctifs au système d'exploitation et aux bases de données, la configuration des pare-feu et la reprise après sinistre.

Le logiciel en tant que service (SaaS) désigne les services qui fournissent des logiciels hébergés de manière centralisée qui sont généralement accessibles via un navigateur Web, une application mobile ou une interface de programmation d'applications (API).

Le modèle de licence des offres SaaS est généralement un abonnement ou un paiement à l'utilisation. Avec les offres SaaS, les clients n'ont pas besoin de gérer l'infrastructure qui prend en charge le service.

Certains services AWS, comme **AWS Trusted Advisor**, **AWS Shield** et **Amazon Chime**, peuvent être classés dans la catégorie des offres SaaS, compte tenu de leurs caractéristiques.

AWS Trusted Advisor est un outil en ligne qui analyse votre environnement AWS et offre des conseils et des recommandations en temps réel pour vous aider à allouer vos ressources en suivant les bonnes pratiques AWS. Le service Trusted Advisor est proposé dans le cadre de votre programme de support AWS. Certaines fonctionnalités de Trusted Advisor sont gratuites pour tous les comptes, mais les clients Business Support et Enterprise Support ont accès à l'ensemble complet des vérifications et des recommandations de Trusted Advisor.

AWS Shield est un service de protection contre le déni de service distribué (DDoS) géré. Il protège les applications s'exécutant sous AWS. Il assure une détection continue et intègre l'atténuation automatique des risques afin de minimiser les interruptions et la latence des applications. Il n'est donc pas nécessaire de faire appel à AWS Support pour bénéficier de la protection DDoS. AWS Shield Advanced est disponible pour tous les clients. Toutefois, pour contacter l'équipe d'intervention DDoS, les clients doivent bénéficier d'un contrat de support Enterprise ou Business auprès d'AWS Support.

Amazon Chime est un service de communication qui vous permet de vous réunir et de discuter avec vos collaborateurs, mais également de passer des appels professionnels au sein de votre organisation comme en dehors, le tout à partir d'une simple application.
Il s'agit d'un service de communication facturé à l'utilisation sans frais initiaux, sans engagement et sans contrat de longue durée.

Voici les points clés à retenir :

- Les responsabilités quant à la sécurité sont réparties entre AWS et le client :
    - AWS est responsable de la sécurité **du** cloud.
    - Le client est responsable de la sécurité **dans** le cloud.

- **AWS est responsable de la protection de l'infrastructure** (y compris le matériel, les logiciels, la mise en réseau et les installations) qui exécutent les services AWS Cloud.

- Pour les services classés dans la catégorie Infrastructure en tant que service (IaaS), **le client est responsable de l'exécution des tâches de configuration et de gestion de la sécurité nécessaires.**
    - Par exemple, les mises à jour du système d'exploitation invité et les correctifs de sécurité, les pare-feu, les configurations des groupes de sécurité.