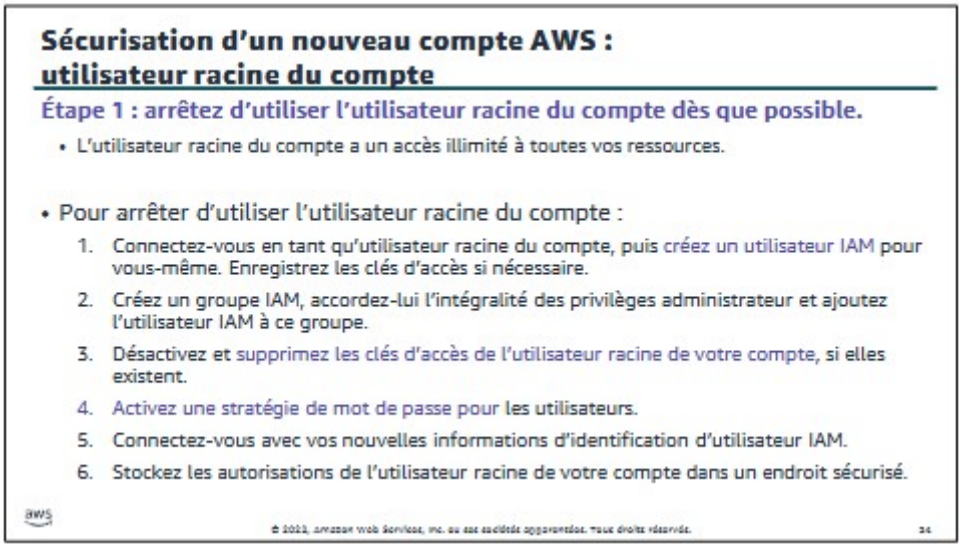
Sécurisation d'un nouveau compte AWS



Lorsque vous créez un compte AWS, vous commencez avec une seule identité de connexion disposant d'un accès complet à tous les services et ressources AWS du compte. Cette identité est appelée utilisateur racine du compte AWSet elle est accessible en se connectant à AWS Management Console à l'aide de l'adresse e-mail et du mot de passe utilisés pour la création du compte.

Les utilisateurs racines du compte AWS ont un accès complet à toutes les ressources du compte. Pour cette raison, AWS recommande fortement de ne pas utiliser les autorisations du compte racine pour vos interactions quotidiennes avec le compte.

À la place, utilisez IAM pour créer des utilisateurs supplémentaires auxquels vous attribuerez des autorisations sur la base du principe du moindre privilège. Par exemple, si vous avez besoin d'autorisations de niveau administrateur, vous pouvez créer un utilisateur IAM, lui accorder l'accès complet, puis utiliser ces informations d'identification pour interagir avec le compte.

Si plus tard vous avez besoin de modifier ou d'annuler vos autorisations, vous pouvez supprimer ou modifier les stratégies qui sont associées à cet utilisateur IAM.

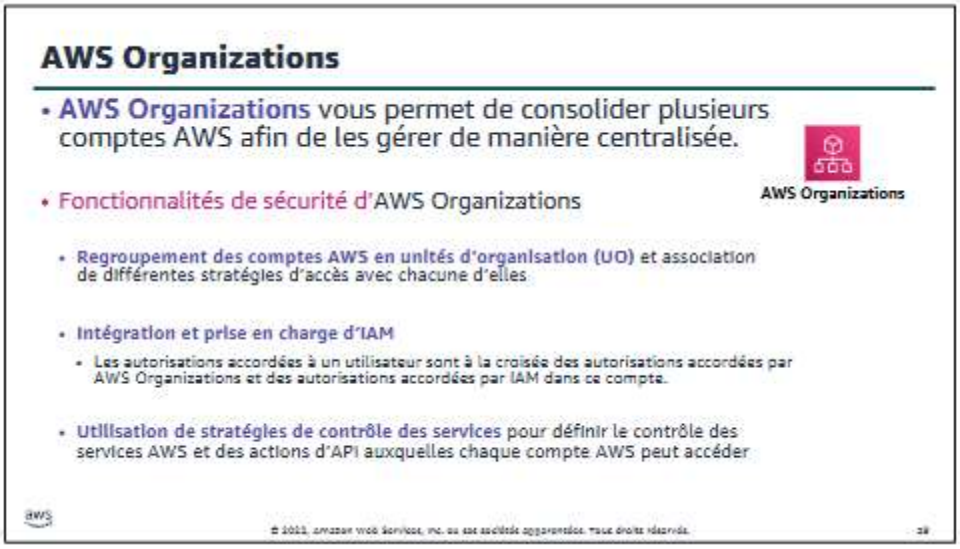
D'autre part, si plusieurs utilisateurs ont besoin d'accéder à ce compte, vous pouvez créer des autorisations uniques pour chaque utilisateur et définir qui a accès à quelles ressources. Par exemple, vous pouvez créer des utilisateurs IAM avec un accès en lecture seule aux ressources de votre compte AWS et distribuer ces informations d'identification à vos utilisateurs, selon les besoins.

Il est recommandé de ne pas partager les mêmes informations d'identification avec plusieurs utilisateurs.

Bien que l'utilisateur racine du compte ne doive pas être utilisé pour les tâches régulières, il est nécessaire pour certaines taches.
Une autre étape recommandée pour sécuriser un nouveau compte AWS consiste à exiger l'authentification multifacteur (MFA) pour la connexion de l'utilisateur racine du compte et pour toutes les autres connexions d'utilisateur IAM.

Une étape supplémentaire recommandée pour sécuriser un nouveau compte AWS consiste à activer les rapports de facturation, tel que le rapport d'utilisation et de coût AWS. Les rapports de facturation fournissent des informations relatives à votre utilisation des ressources AWS et aux coûts estimés pour cette utilisation. AWS transmet ces rapports à un compartiment AmazonS3 que vous spécifiez, puis les met à jour au moins une fois par jour.

AWS CloudTrailest un service qui journalise toutes les demandes d'API dans les ressources de votre compte. De cette manière, il permet un audit opérationnel de votre compte. AWS CloudTrail est activé par défaut lors de la création de tous les comptes AWS et conserve un enregistrement des 90 derniers jours d'activité des événements de gestion de compte. Vous pouvez afficher et télécharger les 90 derniers jours d'activité de votre compte pour les opérations de création, modification et suppression des services pris en charge par CloudTrail sans avoir à configurer manuellement un autre journal d'activité.

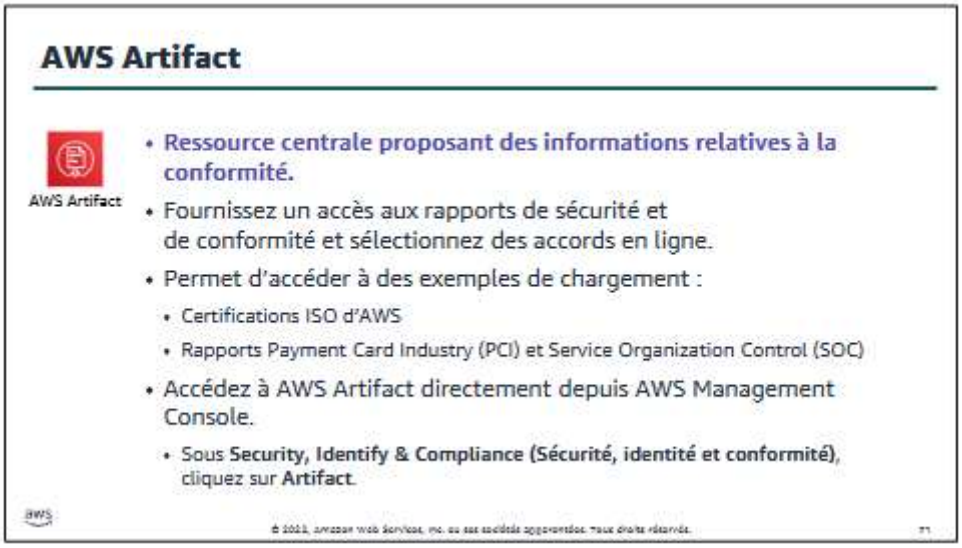


AWS Organizations est un service de gestion de comptes qui vous permet de consolider plusieurs comptes AWS dans une organisation que vous créez et gérez de façon centralisée. L'accent est mis sur les fonctionnalités de sécurité fournies par AWS Organizations.

AWS Key Management Service (AWS KMS) est un service qui vous permet de créer et de gérer des clés de chiffrement, et de contrôler l'utilisation du chiffrement dans un large éventail de services AWS et au sein de vos applications. AWS KMS est un service sécurisé et résilient qui utilise des modules de sécurité matériels (HSM) validés (ou en cours de validation) selon la norme FIPS140-2pour protéger vos clés. AWSKMS est également intégré à AWSCloudTrail pour vous fournir des journaux contenant des informations sur toutes les utilisations de vos clés, afin de vous aider à répondre à vos besoins en matière de réglementation et de conformité.

Amazon Cognito fournit des solutions pour contrôler l'accès aux ressources AWS à partir de votre application. Vous pouvez définir des rôles et mapper des utilisateurs à des rôles différents afin que votre application ne puisse accéder qu'aux ressources autorisées pour chaque utilisateur.

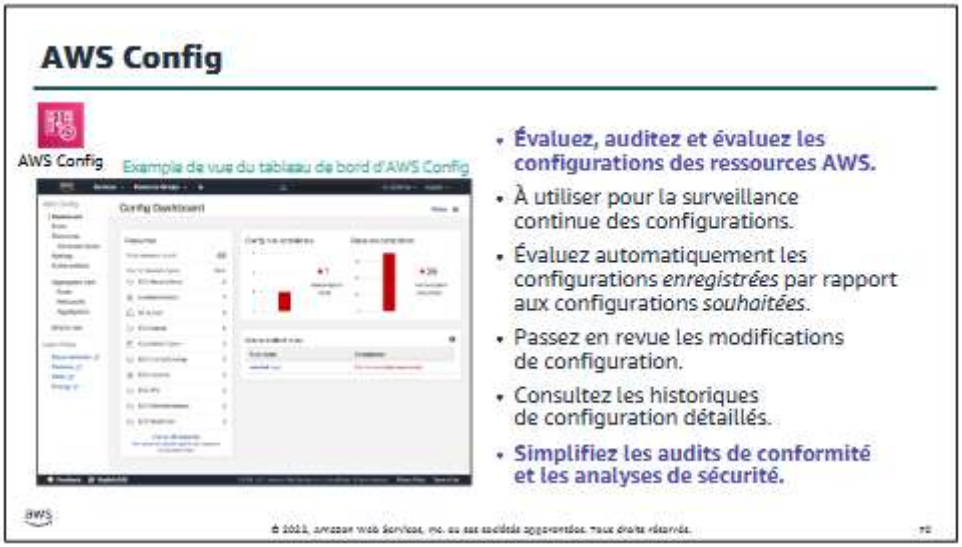
AWS Shield est un service de protection DDoS (Déni de service distribué) géré qui protège les applications exécutées sous AWS. Il assure une détection continue et intègre l'atténuation automatique des risques afin de minimiser les interruptions et la latence des applications. Il n'est donc pas nécessaire de faire appel à AWS Support pour bénéficier de la protection DDoS.



AWS Artifact fournit des téléchargements à la demande des documents de sécurité et de conformité AWS, tels que les certifications AWS ISO, les rapports PCI (Payment Card Industry) et les rapports SOC (Service Organization Control). Ces documents (également appelés «artefacts d'audit») peuvent ensuite être adressés à des auditeurs ou régulateurs afin d'attester du niveau de sécurité et de conformité de l'infrastructure et des services AWS dont vous faites usage.

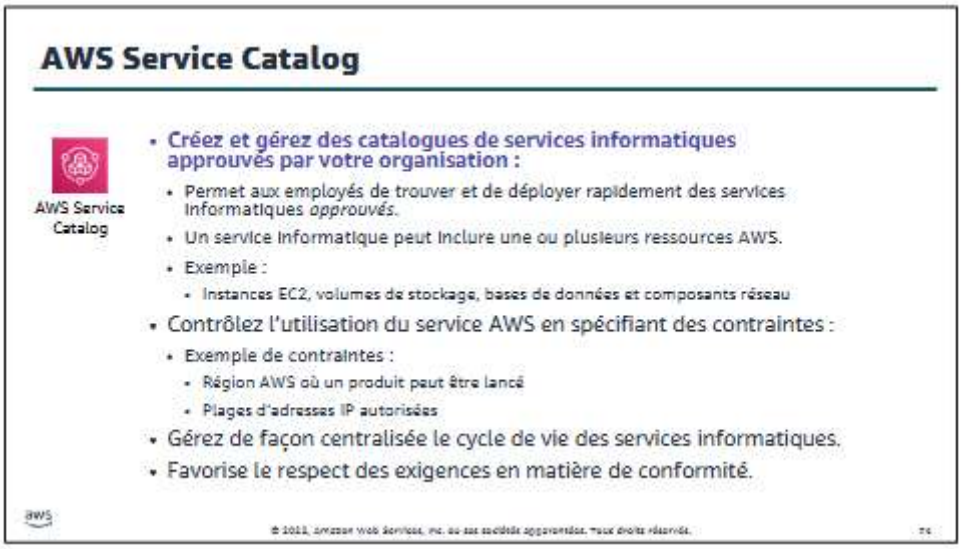
Vous pouvez également tirer parti de ces documents afin d'évaluer vous-même votre architecture cloud et l'efficacité des contrôles internes mis en place dans votre entreprise.

AWS Artifact ne fournit que des documents concernant AWS. Les clients AWS sont responsables de l'élaboration ou de l'obtention des documents qui prouvent la sécurité et la conformité de leurs applications.

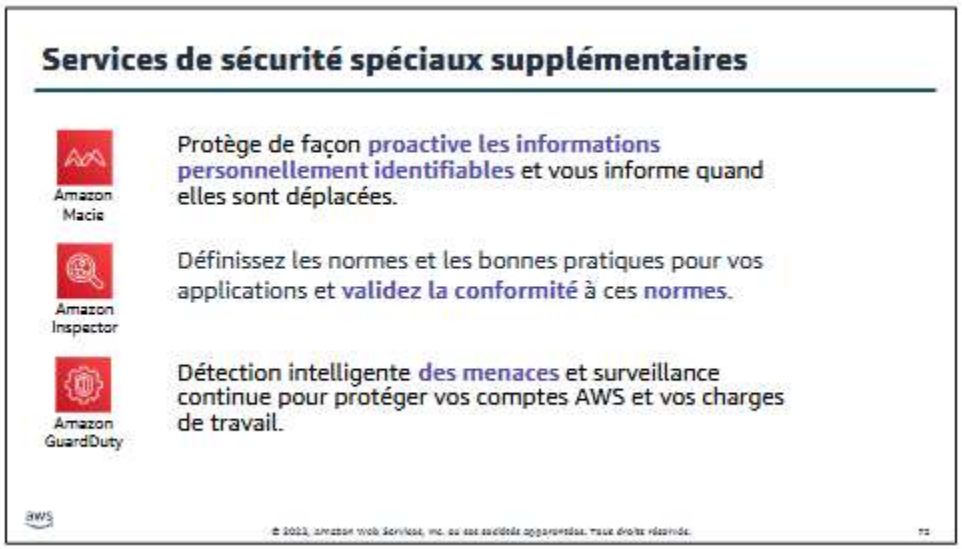


AWSConfig est un service qui vous permet d'analyser, de contrôler et d'évaluer les **configurations de vos ressources AWS**. Il surveille et enregistre en permanence les configurations de vos ressources AWS et vous permet d'automatiser l'évaluation des configurations enregistrées par rapport aux configurations souhaitées.

WS Config vous permet d'examiner l'évolution des configurations et des relations entre les ressources AWS, d'explorer des historiques de configuration de ressources détaillés et de déterminer votre niveau de conformité global par rapport aux configurations spécifiées dans vos directives internes. Cela vous permet de simplifier l'audit de la conformité, l'analyse de la sécurité, la gestion des modifications et le diagnostic des défaillances opérationnelles.



AWS Service Catalog permet aux organisations de créer et de gérer des catalogues de services informatiques dont l'utilisation est approuvée (par exemple, pour vos employés) sur AWS. Ces services informatiques peuvent comprendre toutes les solutions depuis les images de machine virtuelle, les serveurs, les logiciels et les bases de données, jusqu'aux architectures d'application à plusieurs niveaux complètes.



Amazon Macie est un service de sécurité qui utilise le machine learning pour découvrir, classer et protéger automatiquement les données sensibles dans AWS. Il reconnaît les données sensibles telles que les informations personnelles identifiables et la propriété intellectuelle. Ce service offre des tableaux de bord et génère des alertes pour vous aider à mieux comprendre comment l'accès à ces données est réalisé, ainsi que leurs déplacements. Ce service entièrement géré surveille en permanence l'activité liée à l'accès aux données pour détecter les anomalies et génère des alertes détaillées dès qu'il détecte un risque d'accès non autorisé ou de fuite accidentelle de données.

Amazon Inspector est un service d'évaluation automatique de la sécurité qui contribue à renforcer la sécurité et la conformité des applications déployées sur AWS. Il évalue automatiquement les applications afin de déterminer leur exposition et détecter les éventuelles vulnérabilités ou écarts par rapport aux meilleures pratiques. Après avoir effectué une évaluation, Amazon Inspector génère une liste détaillée de problèmes de sécurité potentiels, classés par niveau de sévérité. Ces problèmes peuvent être analysés directement ou dans le cadre de rapports d'évaluation détaillés, disponibles via la console d'Amazon Inspector ou l'API.

AmazonGuardDutyest un service de détection des menaces, qui surveille en continu les activités malveillantes et les comportements non autorisés pour protéger vos comptes AWS et vos charges de travail. Avec le cloud, la collecte et l'agrégation des activités de compte et de réseau sont simplifiées, mais analyser en continu les données de journaux d'événements reste souvent chronophage pour les équipes de sécurité. GuardDuty utilise le machine learning, la détection d'anomalie et des renseignements intégrés sur les menaces pour identifier et classer les menaces potentielles. Il analyse des dizaines de milliards d'événements issus de différentes sources de données AWS, telles que AWS CloudTrail, les journaux de flux Amazon VPC et les journaux DNS.