AWS Guide de décision

Choix des services AWS de sécurité, d'identité et de gouvernance

Choix des services AWS de sécurité, d'identité et de gouvernance: AWS Guide de décision

Table of Contents

Choix des services AWS de sécurité, d'identité et de gouvernance

Faire le premier pas

C'est l'heure de lire	27 minutes	
Objectif	Vous aider à déterminer les services AWS de sécurité, d'identité et de gouvernance les mieux adaptés à votre entreprise.	
Dernière mise à jour	30 décembre 2024	
Services couverts	• AWS Artifact • AWS Audit Manager • AWS Certificate Manager • AWS CloudHSM • AWS CloudTrail • Amazon Cognito • AWS Config • AWS Control Tower • Amazon Detective • AWS Firewall Manager • Amazon GuardDuty • AWS IAM • AWS IAM Identity Center • Amazon Inspector	• AWS KMS • Amazon Macie • AWS Network Firewall • AWS Organizations • AWS Payment Cryptography • AWS CA privée • AWS RAM • AWS Secrets Manager • AWS Security Hub CSPM • Amazon Security Lake • AWS Réponse aux incidents de sécurité • AWS Shield • AWS WAF

Introduction

La sécurité, l'identité et la gouvernance dans le cloud sont des éléments importants qui vous permettent d'atteindre et de maintenir l'intégrité et la sécurité de vos données et services. Cela est

particulièrement pertinent alors que de plus en plus d'entreprises migrent vers des fournisseurs de cloud tels qu'Amazon Web Services (AWS).

Ce guide vous aide à sélectionner les services et outils de AWS sécurité, d'identité et de gouvernance les mieux adaptés à vos besoins et à ceux de votre organisation.

Voyons d'abord ce que nous entendons par sécurité, identité et gouvernance :

- La sécurité du cloud fait référence à l'utilisation de mesures et de pratiques pour protéger les actifs numériques contre les menaces. Cela inclut à la fois la sécurité physique des centres de données et les mesures de cybersécurité pour se prémunir contre les menaces en ligne. AWS donne la priorité à la sécurité grâce au stockage crypté des données, à la sécurité du réseau et à la surveillance continue des menaces potentielles.
- Les services d'identité vous aident à gérer en toute sécurité les identités, les ressources et les autorisations de manière évolutive. AWS fournit des services d'identité conçus pour les applications destinées au personnel et aux clients, ainsi que pour la gestion de l'accès à vos charges de travail et à vos applications.
- La gouvernance du cloud est un ensemble de règles, de processus et de rapports qui aident votre entreprise à suivre les meilleures pratiques. Vous pouvez établir une gouvernance du cloud pour l'ensemble de vos AWS ressources, utiliser les meilleures pratiques et normes intégrées et automatiser les processus de conformité et d'audit. La conformité dans le cloud fait référence au respect des lois et réglementations régissant la protection et la confidentialité des données. AWS Les programmes de conformité fournissent des informations sur les certifications, les réglementations et les cadres qui AWS s'alignent sur.

Cette vidéo d'une one-and-a-half minute résume comment AWS renforcer la sécurité au cœur de nos activités.

Comprendre les services AWS de sécurité, d'identité et de gouvernance

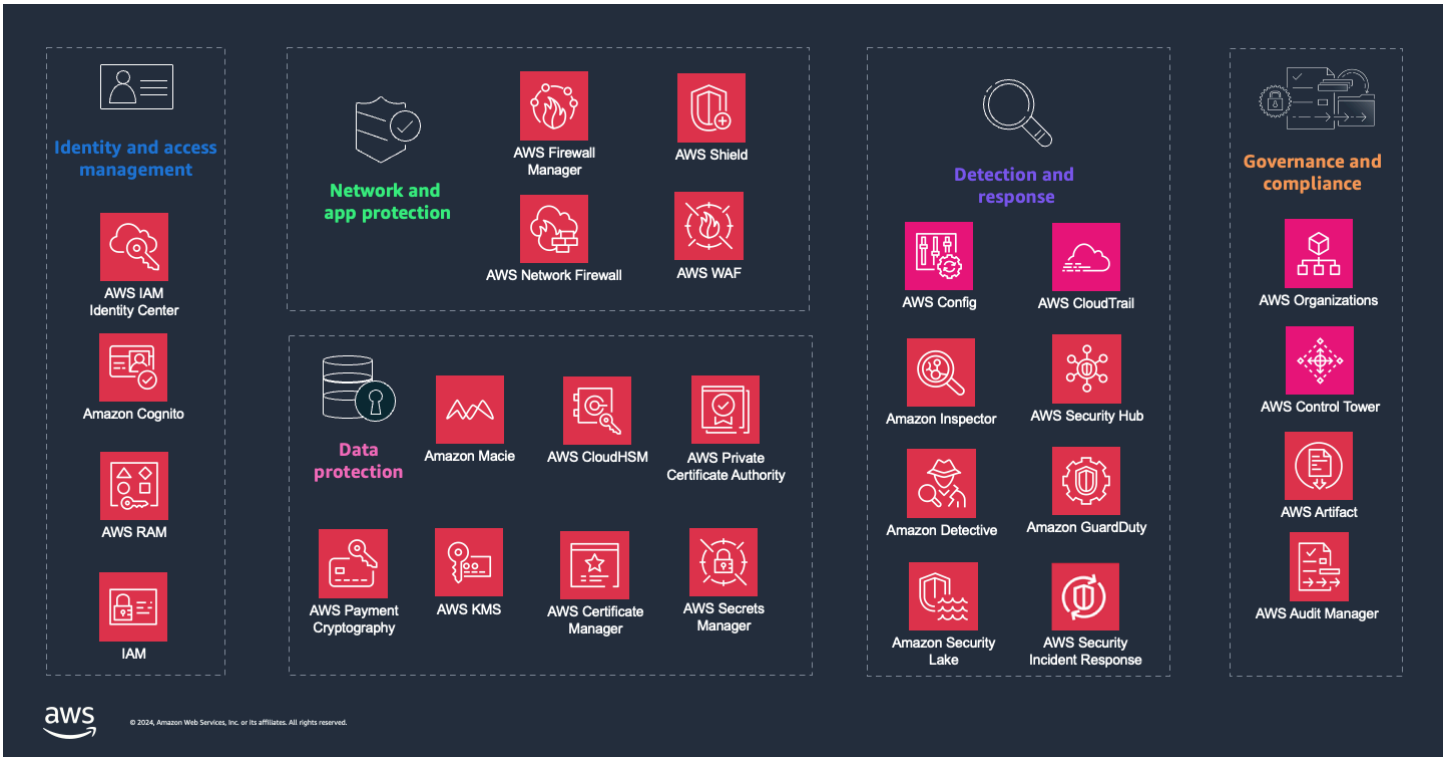
La sécurité et la conformité sont des responsabilités partagées

Avant de choisir vos services AWS de sécurité, d'identité et de gouvernance, il est important que vous compreniez que la sécurité et la conformité sont des responsabilités partagées entre vous et AWS.

La nature de cette responsabilité partagée contribue à alléger votre charge opérationnelle et vous offre flexibilité et contrôle sur votre déploiement. Cette différenciation des responsabilités est communément appelée sécurité « du » cloud et sécurité « dans » le cloud.

En comprenant ce modèle, vous pouvez comprendre l'éventail des options qui s'offrent à vous et comment les options applicables Services AWS s'intègrent.

Vous pouvez combiner AWS des outils et des services pour protéger vos charges de travail



Comme le montre le schéma précédent, AWS propose des outils et des services dans cinq domaines pour vous aider à atteindre et à maintenir une sécurité, une gestion des identités et une gouvernance robustes dans le cloud. Vous pouvez utiliser Services AWS ces cinq domaines pour vous aider à effectuer les opérations suivantes :

- Adoptez une approche multicouche pour protéger vos données et vos environnements
- Renforcez votre infrastructure cloud contre les menaces en constante évolution
- Respectez des normes réglementaires strictes

Pour en savoir plus sur AWS la sécurité, y compris la documentation de sécurité pour Services AWS, consultez AWS la documentation de sécurité.

Dans les sections suivantes, nous examinons chaque domaine plus en détail.

Comprendre les services de gestion des AWS identités et des accès

Au cœur de la AWS sécurité se trouve le principe du moindre privilège : les individus et les services n'ont que l'accès dont ils ont besoin. AWS IAM Identity Centerest recommandé Service AWS pour gérer l'accès des utilisateurs aux AWS ressources. Vous pouvez utiliser ce service pour gérer l'accès à vos comptes et les autorisations associées à ces comptes, y compris les identités provenant de fournisseurs d'identité externes.

Le tableau suivant récapitule les offres de gestion des identités et des accès abordées dans ce guide :

AWS IAM Identity Center

> AWS IAM Identity Centervous aide à connecter votre source d'identités ou à créer des utilisateurs. Vous pouvez gérer de manière centralisée l'accès du personnel aux multiples applications Comptes AWS et applications.

Amazon Cognito

> Amazon Cognito fournit un outil d'identification pour les applications Web et mobiles afin d'authentifier et d'autoriser les utilisateurs à partir du répertoire des utilisateurs intégré, de votre annuaire d'entreprise et des fournisseurs d'identité des consommateurs.

AWS RAM

> AWS RAMvous permet de partager en toute sécurité vos ressources au sein de votre organisation et avec les rôles et utilisateurs IAM. Comptes AWS

IAM

> L'IAM permet un contrôle précis et sécurisé de l'accès aux ressources de charge de AWS travail.

Comprendre les services AWS de protection des données

La protection des données est vitale dans le cloud et AWS fournit des services qui vous aident à protéger vos données, vos comptes et vos charges de travail. Par exemple, le chiffrement de vos données en transit et au repos permet de les protéger contre toute exposition. Avec AWS Key Management Service(AWS KMS), AWS CloudHSMvous pouvez créer et contrôler les clés cryptographiques que vous utilisez pour protéger vos données.

Le tableau suivant récapitule les offres de protection des données présentées dans ce guide :

Amazon Macie

Amazon Macie découvre les données sensibles à l'aide de l'apprentissage automatique et de la correspondance de modèles, et permet une protection automatique contre les risques associés.

AWS KMS

AWS KMScrée et contrôle les clés cryptographiques que vous utilisez pour protéger vos données.

AWS CloudHSM

AWS CloudHSMfournit des modules de sécurité matériels basés sur le cloud à haute disponibilité (HSMs).

AWS Certificate Manager

AWS Certificate Managergère la complexité de la création, du stockage et du renouvellement des certificats et clés SSL/TLS X.509 publics et privés.

AWS CA privée

AWS CA privéevous permet de créer des hiérarchies d'autorités de certification privées, y compris des autorités de certification racine et subordonnées ()CAs.

AWS Secrets Manager

AWS Secrets Managervous permet de gérer, de récupérer et de faire pivoter les informations d'identification de base de données, les informations d'identification des applications, les OAuth jetons, les clés d'API et autres secrets.

AWS Payment Cryptography

AWS Payment Cryptographydonne accès aux fonctions cryptographiques et à la gestion des clés utilisées dans le traitement des paiements conformément aux normes de l'industrie des cartes de paiement (PCI).

Comprendre les services de protection des AWS réseaux et des applications

AWS propose plusieurs services pour protéger vos réseaux et vos applications. AWS Shieldvous protège contre les attaques par déni de service (DDoS) distribué et vous AWS WAFaide à protéger les applications Web contre les attaques d'exploitation Web courantes.

Le tableau suivant récapitule les offres de protection du réseau et des applications présentées dans ce guide :

AWS Firewall Manager

AWS Firewall Managersimplifie vos tâches d'administration et de maintenance sur plusieurs comptes et ressources à des fins de protection.

AWS Network Firewall

AWS Network Firewallfournit un pare-feu réseau géré et dynamique ainsi qu'un service de détection et de prévention des intrusions avec votre VPC.

AWS Shield

AWS Shieldfournit des protections contre les attaques DDo S pour les AWS ressources au niveau du réseau, du transport et des applications.

AWS WAF

AWS WAFfournit un pare-feu pour applications Web qui vous permet de surveiller les demandes HTTP (S) qui sont transmises aux ressources protégées de votre application Web.

Comprendre les services AWS de détection et de réponse

AWS fournit des outils pour vous aider à rationaliser les opérations de sécurité dans votre AWS environnement, y compris les environnements multi-comptes. Par exemple, vous pouvez utiliser Amazon GuardDuty pour la détection intelligente des menaces, et vous pouvez utiliser Amazon Detective pour identifier et analyser les résultats de sécurité en collectant des données de journal. AWS Security Hub CSPMprend en charge plusieurs normes de sécurité et fournit une vue d'ensemble des alertes de sécurité et de l'état de conformité de l'ensemble Comptes AWS. AWS CloudTrailsuit l'activité des utilisateurs et l'utilisation de l'interface de programmation d'applications (API), ce qui est essentiel pour comprendre les événements de sécurité et y répondre.

Le tableau suivant récapitule les offres de détection et de réponse abordées dans ce guide :

AWS Config

AWS Configfournit une vue détaillée de la configuration des AWS ressources de votre Compte AWS.

AWS CloudTrail

AWS CloudTrailenregistre les actions entreprises par un utilisateur, un rôle ou Service AWS.

AWS Security Hub CSPM

AWS Security Hub CSPMfournit une vue complète de votre état de sécurité dans AWS.

Amazon GuardDuty

Amazon surveille GuardDuty en permanence vos charges de travail Comptes AWS, votre activité d'exécution et vos données pour détecter toute activité malveillante.

Amazon Inspector

Amazon Inspector analyse vos AWS charges de travail pour détecter les vulnérabilités logicielles et toute exposition involontaire au réseau.

Amazon Security Lake

Amazon Security Lake centralise automatiquement les données de sécurité provenant des AWS environnements, des fournisseurs de SaaS, des environnements sur site, des sources cloud et des sources tierces dans un lac de données.

Amazon Detective

Amazon Detective vous permet d'analyser, d'enquêter et d'identifier rapidement la cause racine des résultats de sécurité ou des activités suspectes.

AWS Security Incident Response

AWS Réponse aux incidents de sécurité

Vous aide à vous préparer rapidement aux incidents de sécurité, à y répondre et à recevoir des conseils pour vous aider à vous remettre en état après un incident de sécurité.

Comprendre les services AWS de gouvernance et de conformité

AWS fournit des outils qui vous aident à respecter vos normes de sécurité, d'exploitation, de conformité et de coûts. Par exemple, vous pouvez l'utiliser AWS Control Towerpour configurer et gérer un environnement multi-comptes avec des contrôles prescriptifs. Vous pouvez AWS Organizationsainsi configurer une gestion basée sur des règles pour plusieurs comptes au sein de votre organisation.

AWS vous donne également une vue complète de votre état de conformité et surveille en permanence votre environnement à l'aide de contrôles de conformité automatisés basés sur les AWS meilleures pratiques et les normes du secteur suivies par votre organisation. Par exemple, AWS Artifactfournit un accès à la demande aux rapports de conformité et AWS Audit Managerautomatise

la collecte de preuves afin que vous puissiez évaluer plus facilement si vos contrôles fonctionnent efficacement.

Le tableau suivant récapitule les offres de gouvernance et de conformité abordées dans ce guide :

AWS Organizations

AWS Organizationsvous aide à Comptes AWS en consolider plusieurs au sein d'une organisation que vous créez et gérez de manière centralisée.

AWS Control Tower

AWS Control Towervous aide à configurer et à gérer un environnement AWS multi-comptes basé sur les meilleures pratiques.

AWS Artifact

AWS Artifactfournit des téléchargements à la demande de documents de AWS sécurité et de conformité.

AWS Audit Manager

AWS Audit Manager

Vous aide à auditer en permanence votre AWS utilisation afin de simplifier la façon dont vous évaluez les risques et la conformité.

Tenez compte des critères de AWS sécurité, d'identité et de gouvernance

Le choix des services de sécurité, d'identité et de gouvernance appropriés AWS dépend de vos besoins spécifiques et de vos cas d'utilisation. La décision d'adopter un service de AWS sécurité fournit un arbre décisionnel qui vous aide à décider si l'adoption Services AWS pour la sécurité, l'identité et la gouvernance convient à votre organisation. En outre, voici quelques critères à prendre en compte lors de la prise de décision concernant les services à utiliser.

Security requirements and threat landscape

Procédez à une évaluation complète des vulnérabilités et menaces spécifiques de votre entreprise. Cela implique d'identifier les types de données que vous gérez, telles que les informations personnelles des clients, les dossiers financiers ou les données commerciales exclusives. Comprenez les risques potentiels associés à chacun d'entre eux.

Évaluez l'architecture de votre application et de votre infrastructure. Déterminez si vos applications sont destinées au public et quel type de trafic Web elles gèrent. Cela tient compte de votre besoin de services tels que AWS WAF la protection contre l'exploitation du Web. Pour les applications internes, considérez l'importance de la détection interne des menaces et de la surveillance continue avec Amazon GuardDuty, qui peuvent identifier les modèles d'accès inhabituels ou les déploiements non autorisés.

Enfin, tenez compte de la sophistication de votre posture de sécurité actuelle et de l'expertise de votre équipe de sécurité. Si les ressources de votre équipe sont limitées, le choix de services offrant davantage d'automatisation et d'intégration peut vous apporter des améliorations de sécurité efficaces, sans surcharger votre équipe. Les exemples de services incluent AWS Shield la protection DDo S et AWS Security Hub CSPM la surveillance centralisée de la sécurité.

Compliance and regulatory requirements

Identifiez les lois et normes applicables à votre secteur d'activité ou à votre région géographique, telles que le règlement général sur la protection des données (RGPD), la loi américaine de 1996 sur la portabilité et la responsabilité de l'assurance maladie (HIPAA) ou la norme de sécurité des données du secteur des cartes de paiement (PCI DSS).

AWS propose des services tels que AWS Config AWS Artifact pour vous aider à gérer la conformité aux différentes normes. Vous pouvez ainsi évaluer, auditer et évaluer les configurations de vos AWS ressources, ce qui vous permet de garantir plus facilement la conformité aux politiques internes et aux exigences réglementaires. AWS Config AWS Artifact fournit un accès à la demande à la documentation de AWS conformité, qui vous aide à réaliser des audits et à établir des rapports de conformité.

Le choix de services adaptés à vos besoins spécifiques en matière de conformité peut aider votre entreprise à satisfaire aux exigences légales et à créer un environnement sécurisé et fiable pour vos données. Explorez les programmes de AWS conformité pour en savoir plus.

Scalability and flexibility

Réfléchissez à la manière dont votre organisation va se développer et à quelle vitesse. Choisissez Services AWS celle qui permettra à vos mesures de sécurité de s'adapter parfaitement à votre infrastructure et à l'évolution des menaces.

Pour vous aider à évoluer rapidement, AWS Control Tower orchestre les capacités de plusieurs autres entreprises Services AWS, notamment AWS Organizations AWS IAM Identity Center, afin de créer une zone de landing zone en moins d'une heure. Control Tower configure et gère les ressources en votre nom.

AWS conçoit également de nombreux services pour qu'ils s'adaptent automatiquement au trafic et aux modèles d'utilisation d'une application, tels qu'Amazon GuardDuty pour la détection des menaces et AWS WAF la protection des applications Web. Au fur et à mesure que votre entreprise grandit, ces services évoluent avec elle, sans nécessiter d'ajustements manuels ni créer de goulots d'étranglement.

En outre, il est essentiel que vous puissiez personnaliser vos contrôles de sécurité en fonction des exigences de votre entreprise et de l'environnement des menaces. Envisagez de gérer vos comptes avec AWS Organizations, afin de pouvoir gérer plus de 40 ressources de services sur plusieurs comptes. Cela donne aux équipes d'application individuelles la flexibilité et la visibilité nécessaires pour gérer les besoins de sécurité spécifiques à leur charge de travail, tout en leur offrant une gouvernance et une visibilité auprès des équipes de sécurité centralisées.

La prise en compte de l'évolutivité et de la flexibilité vous permet de garantir que votre posture de sécurité est robuste, réactive et capable de prendre en charge des environnements professionnels dynamiques.

Integration with existing systems

Envisagez des mesures de sécurité qui améliorent vos opérations actuelles au lieu de les perturber. Par exemple, considérez ce qui suit :

- Rationalisez vos flux de travail en agrégeant les données de sécurité et les alertes issues de celles-ci Services AWS et en les analysant avec les systèmes de gestion des informations et des événements de sécurité (SIEM) existants.
- Créez une vue unifiée des menaces de sécurité et des vulnérabilités dans les environnements locaux AWS et sur site.
- AWS CloudTrail Intégrez les solutions de gestion des journaux existantes pour une surveillance complète des activités des utilisateurs et de l'utilisation des API dans votre AWS infrastructure et dans les applications existantes.
- Examinez les moyens d'optimiser l'utilisation des ressources et d'appliquer de manière cohérente des politiques de sécurité dans tous les environnements. Cela vous permet de réduire le risque de lacunes dans la couverture de sécurité.

Cost and budget considerations

Passez en revue les modèles de tarification pour chaque service que vous envisagez. AWS les frais sont souvent basés sur l'utilisation, tels que le nombre d'appels d'API, le volume de données

traitées ou la quantité de données stockées. Par exemple, Amazon GuardDuty facture en fonction de la quantité de données de journal analysées pour détecter les menaces, tandis que les AWS WAF factures sont basées sur le nombre de règles déployées et le nombre de requêtes Web reçues.

Estimez votre consommation prévue pour prévoir les coûts avec précision. Tenez compte à la fois des besoins actuels et de la croissance potentielle ou des pics de demande. Par exemple, l'évolutivité est une caractéristique essentielle Services AWS, mais elle peut également entraîner une augmentation des coûts si elle n'est pas gérée avec soin. Utilisez-les Calculateur de tarification AWSpour modéliser différents scénarios et évaluer leur impact financier.

Évaluez le coût total de possession (TCO), qui inclut à la fois les coûts directs et les coûts indirects, tels que le temps et les ressources nécessaires à la gestion et à la maintenance. Opter pour des services gérés peut réduire les frais d'exploitation, mais leur prix peut être plus élevé.

Enfin, hiérarchisez vos investissements en matière de sécurité en fonction de l'évaluation des risques. Tous les services de sécurité n'auront pas la même importance pour votre infrastructure. Concentrez donc votre budget sur les domaines qui auront le plus d'impact sur la réduction des risques et la garantie de la conformité. L'équilibre entre rentabilité et niveau de sécurité dont vous avez besoin est essentiel pour une stratégie AWS de sécurité réussie.

Organizational structure and access needs

Évaluez la structure et le fonctionnement de votre organisation, ainsi que la façon dont vos besoins en matière d'accès peuvent varier en fonction de l'équipe, du projet ou du site. Cela influe sur la manière dont vous gérez et authentifiez les identités des utilisateurs, attribuez des rôles et appliquez les contrôles d'accès dans votre AWS environnement. Mettez en œuvre les meilleures pratiques, telles que l'application des autorisations du moindre privilège et l'exigence d'une authentification multifactorielle (MFA).

La plupart des entreprises ont besoin d'un environnement multi-comptes. Passez en revue les meilleures pratiques pour ce type d'environnement et envisagez de l'utiliser AWS Organizations AWS Control Tower pour vous aider à l'implémenter.

Un autre aspect à prendre en compte est la gestion des informations d'identification et des clés d'accès. Envisagez d'utiliser IAM Identity Center pour centraliser la gestion des accès entre de multiples Comptes AWS applications professionnelles, ce qui améliore à la fois la sécurité et le confort des utilisateurs. Pour vous aider à gérer facilement l'accès aux comptes de votre organisation, IAM Identity Center s'intègre à AWS Organizations.

En outre, évaluez comment ces services de gestion des identités et des accès s'intègrent à vos services d'annuaire existants. Si vous possédez déjà un fournisseur d'identité, vous pouvez l'intégrer à IAM Identity Center à l'aide de SAML 2.0 ou d'OpenID Connect (OIDC). IAM Identity Center prend également en charge le provisionnement du système de gestion des identités interdomaines (SCIM) afin de garantir la synchronisation de vos annuaires. Cela vous permet de garantir une expérience utilisateur fluide et sécurisée lors de l'accès aux AWS ressources.

Choisissez un service AWS de sécurité, d'identité et de gouvernance

Maintenant que vous connaissez les critères d'évaluation de vos options de sécurité, vous êtes prêt à choisir les services de AWS sécurité les mieux adaptés aux besoins de votre organisation.

Le tableau suivant indique quels services sont optimisés pour quelles circonstances. Utilisez le tableau pour déterminer le service le mieux adapté à votre organisation et à votre cas d'utilisation.

Note

[1] S'intègre à AWS Security Hub CSPM (liste complète)
[2] S'intègre à Amazon GuardDuty (liste complète)
[3] S'intègre à Amazon Security Lake (liste complète)

Choisissez les services de gestion des AWS identités et des accès

Accordez aux personnes concernées le niveau d'accès approprié aux systèmes, aux applications et aux données.

Quand devriez-vous l'utiliser ?	Pour quoi est-il optimisé ?	Services de sécurité, d'identité et de gouvernance
Utilisez ces services pour vous aider à gérer et à gouverner en toute sécurité l'accès de vos clients, de votre personnel et de vos charges de travail.	Vous aide à connecter votre source d'identités ou à créer des utilisateurs. Vous pouvez gérer de manière centralisée l'accès du personnel à	AWS IAM Identity Center

Quand devriez-vous l'utiliser ?	Pour quoi est-il optimisé ?	Services de sécurité, d'identité et de gouvernance
	plusieurs AWS comptes et applications.	
	Optimisé pour authentifier et autoriser les utilisateurs pour les applications Web et mobiles.	Amazon Cognito
	Optimisé pour partager des ressources en toute sécurité au sein de AWS.	AWS RAM
	Permet un contrôle précis et sécurisé de l'accès aux ressources de AWS charge de travail.	JE SUIS 1

Choisissez AWS les services de protection des données

Automatisez et simplifiez les tâches de protection et de sécurité des données allant de la gestion des clés à la découverte de données sensibles en passant par la gestion des informations d'identification.

Quand devriez-vous l'utiliser ?	Pour quoi est-il optimisé ?	Services de protection des données
Utilisez ces services pour garantir et maintenir la confidentialité, l'intégrité et la disponibilité des données sensibles stockées et traitées dans AWS des environne ments.	Optimisé pour la découverte de données sensibles.	Amazon Macie 1
	Optimisé pour les clés cryptographiques.	AWS KMS
	Optimisé pour HSMs.	AWS CloudHSM
	Optimisé pour les certificats et clés SSL/TLS X.509 privés.	AWS Certificate Manager

Quand devriez-vous l'utiliser ?	Pour quoi est-il optimisé ?	Services de protection des données
	Optimisé pour créer des hiérarchies d'autorités de certification privées.	AWS CA privée
	Optimisé pour les informations d'identification de base de données, les informations d'identification des applications, les OAuth jetons, les clés d'API et autres secrets.	AWS Secrets Manager
	Optimisé pour fournir un accès aux fonctions cryptographiques et à la gestion des clés utilisées dans le traitement des paiements conformément aux normes PCI.	AWS Payment Cryptography

Choisissez les services de protection du AWS réseau et des applications

Protégez de manière centralisée vos ressources Internet contre les attaques DDo informatiques et applicatives courantes.

Quand devriez-vous l'utiliser ?	Pour quoi est-il optimisé ?	Services de protection des réseaux et des applications
Utilisez ces services pour vous aider à appliquer des politiques de sécurité détaillées à chaque point de contrôle du réseau.	Optimisé pour la configuration et la gestion centralisées des règles de pare-feu.	AWS Firewall Manager[1]
	Optimisé pour fournir un pare-feu réseau géré et dynamique ainsi qu'un service	AWS Network Firewall

Quand devriez-vous l'utiliser ?	Pour quoi est-il optimisé ?	Services de protection des réseaux et des applications
	de détection et de prévention des intrusions.	
	Optimisé pour la protection contre les attaques DDo S visant les AWS ressources au niveau du réseau, du transport et des applications.	AWS Shield
	Optimisé pour fournir un pare-feu d'applications Web.	AWS WAF

Choisissez les services AWS de détection et de réponse

Identifiez et hiérarchisez en permanence les risques de sécurité, tout en intégrant les meilleures pratiques de sécurité à un stade précoce.

Quand devriez-vous l'utiliser ?	Pour quoi est-il optimisé ?	Services de détection et de réponse
Utilisez ces services pour vous aider à détecter les risques de sécurité liés à vos comptes et à y répondre, afin de protéger vos charges de travail à grande échelle.	Optimisé pour automatiser les contrôles de sécurité et centraliser les alertes de sécurité avec des AWS intégrations tierces.	AWS Security Hub CSPM[2, 3]
	Optimisé pour l'évaluation, l'audit et l'évaluation de la configuration de vos ressources.	AWS Config[1]
	Optimisé pour enregistrer des événements provenant	AWS CloudTrail

Quand devriez-vous l'utiliser ?	Pour quoi est-il optimisé ?	Services de détection et de réponse
	d'autres entités Services AWS sous forme de piste d'audit.	
	Optimisé pour la détection intelligente des menaces et la création de rapports détaillés.	Amazon GuardDuty [1]
	Optimisé pour la gestion des vulnérabilités.	Amazon Inspector [1]
	Optimisé pour centraliser les données de sécurité.	Amazon Security Lake [1]
	Optimisé pour agréger et résumer les problèmes de sécurité potentiels.	Amazon Detective [1, 2, 3]
	Optimisé pour vous aider à trier les résultats, à intensifier les événements de sécurité et à gérer les cas nécessita nt une attention immédiate de votre part.	AWS Réponse aux incidents de sécurité

Choisissez les services AWS de gouvernance et de conformité

Établissez une gouvernance du cloud pour l'ensemble de vos ressources et automatisez vos processus de conformité et d'audit.

Quand devriez-vous l'utiliser ?	Pour quoi est-il optimisé ?	Services de gouvernance et de conformité
Utilisez ces services pour vous aider à mettre en œuvre les meilleures pratiques et	Optimisé pour la gestion centralisée de plusieurs	AWS Organizations

Quand devriez-vous l'utiliser ?	Pour quoi est-il optimisé ?	Services de gouvernance et de conformité
à respecter les normes du secteur lors de l'utilisation AWS.	comptes et la facturation consolidée.	
	Optimisé pour fournir des téléchargements à la demande de documents de AWS sécurité et de conformité.	AWS Artifact
	Optimisé pour l'audit de AWS l'utilisation.	AWS Audit Manager[1]
	Optimisé pour configurer et gérer un environnement AWS multi-comptes.	AWS Control Tower

Utilisez des services AWS de sécurité, d'identité et de gouvernance

Vous devez maintenant avoir une idée claire de ce que fait chaque service de AWS sécurité, d'identité et de gouvernance (ainsi que AWS des outils et services de support), et de ceux qui pourraient vous convenir le mieux.

Pour découvrir comment utiliser et en savoir plus sur chacun des services de AWS sécurité, d'identité et de gouvernance disponibles, nous avons fourni un parcours permettant d'explorer le fonctionnement de chacun des services. Les sections suivantes fournissent des liens vers une documentation détaillée, des didacticiels pratiques et des ressources pour vous aider à démarrer.

Utiliser les services de gestion des AWS identités et des accès

Les tableaux suivants présentent des ressources utiles de gestion des identités et des accès, organisées par service, pour vous aider à démarrer.

AWS IAM Identity Center

- Activation AWS du centre d'identité IAM

Activez IAM Identity Center et commencez à l'utiliser avec votre AWS Organizations.

Explorez le guide

- Configuration de l'accès utilisateur avec le répertoire IAM Identity Center par défaut

  Utilisez le répertoire par défaut comme source d'identité, puis configurez et testez l'accès des utilisateurs.

  Commencez avec le didacticiel

- Utilisation d'Active Directory comme source d'identité

  Terminez la configuration de base pour utiliser Active Directory comme source d'identité IAM Identity Center.

  Commencez avec le didacticiel

- Configurer SAML et SCIM avec Okta et IAM Identity Center

  Configurez une connexion SAML avec Okta et IAM Identity Center.

  Commencez avec le didacticiel

Amazon Cognito

- Commencer à utiliser Amazon Cognito

  Découvrez les tâches Amazon Cognito les plus courantes.

  Explorez le guide

- Tutoriel : Création d'un groupe d'utilisateurs

  Créez un groupe d'utilisateurs, qui permet à vos utilisateurs de se connecter à votre application Web ou mobile.

  Commencez avec le didacticiel

- Tutoriel : Création d'un pool d'identités

  Créez un pool d'identités, qui permet à vos utilisateurs d'obtenir des informations d' AWS identification temporaires pour y accéder Services AWS.

Commencez avec le didacticiel

- Atelier Amazon Cognito

  Entraînez-vous à utiliser Amazon Cognito pour créer une solution d'authentification pour une animalerie hypothétique.

  Commencez avec le didacticiel

AWS RAM

- Commencer avec AWS RAM

  Apprenez-en davantage sur AWS RAM les termes et les concepts.

  Explorez le guide
- Travailler avec des AWS ressources partagées

  Partagez AWS les ressources que vous possédez et accédez aux AWS ressources partagées avec vous.

  Explorez le guide
- Gestion des autorisations dans la AWS RAM

  Découvrez les deux types d'autorisations gérées : les autorisations AWS gérées et les autorisations gérées par le client.

  Explorez le guide
- Configurez un accès détaillé à vos ressources partagées à l'aide de la AWS RAM

  Utilisez les autorisations gérées par le client pour personnaliser l'accès à vos ressources et appliquer la meilleure pratique du moindre privilège.

  Lisez le blogue

IAM

- Commencer à utiliser IAM

  Créez des rôles, des utilisateurs et des politiques IAM à l'aide du AWS Management Console.

Commencez avec le didacticiel

- Déléguer l'accès entre Comptes AWS les différents rôles

  Utilisez un rôle pour déléguer l'accès aux ressources dans un autre Comptes AWS domaine que vous possédez, appelé Production et développement.

  Commencez avec le didacticiel

- Création d'une politique gérée par le client

  Utilisez le AWS Management Console pour créer une politique gérée par le client, puis attachez cette politique à un utilisateur IAM de votre Compte AWS.

  Commencez avec le didacticiel

- Définissez les autorisations d'accès aux AWS ressources en fonction des balises

  Créez et testez une politique qui permet aux rôles IAM dotés de balises principales d'accéder aux ressources dotées de balises correspondantes.

  Commencez avec le didacticiel

- Bonnes pratiques de sécurité dans IAM

  Sécurisez vos AWS ressources en utilisant les meilleures pratiques en matière d'IAM.

  Explorez le guide

Utiliser les services AWS de protection des données

La section suivante contient des liens vers des ressources détaillées qui décrivent la protection AWS des données.

Macie

- Commencer à utiliser Amazon Macie

  Activez Macie pour vous Compte AWS, évaluez votre niveau de sécurité sur Amazon S3 et configurez les principaux paramètres et ressources pour découvrir et signaler les données sensibles dans vos compartiments S3.

  Explorez le guide

- Surveillance de la sécurité et de la confidentialité des données avec Amazon Macie

  Utilisez Amazon Macie pour surveiller la sécurité des données Amazon S3 et évaluer votre niveau de sécurité.

  Explorez le guide
- Analyse des résultats d'Amazon Macie

  Passez en revue, analysez et gérez les résultats d'Amazon Macie.

  Explorez le guide
- Extraction d'échantillons de données sensibles à l'aide des résultats d'Amazon Macie

  Utilisez Amazon Macie pour récupérer et révéler des échantillons de données sensibles signalées par des résultats individuels.

  Explorez le guide
- Découvrir des données sensibles avec Amazon Macie

  Automatisez la découverte, la journalisation et le reporting des données sensibles dans votre parc de données Amazon S3.

  Explorez le guide

AWS KMS

- Commencer avec AWS KMS

  Gérez les clés KMS de chiffrement symétriques, de leur création à leur suppression.

  Explorez le guide
- Clés spéciales

  Découvrez les différents types de clés compatibles, AWS KMS en plus des clés KMS de chiffrement symétriques.

  Explorez le guide
- Élargir vos capacités de chiffrement au repos avec AWS KMS

  Découvrez les options de chiffrement au repos disponibles dans ce document AWS.

Découvrez l'atelier

AWS CloudHSM

- Commencer avec AWS CloudHSM

  Créez, initialisez et activez un AWS CloudHSM cluster.

  Explorez le guide
- Gestion des AWS CloudHSM clusters

  Connectez-vous à votre AWS CloudHSM cluster et aux différentes tâches administratives liées à la gestion de votre cluster.

  Explorez le guide
- Gestion des utilisateurs et des clés HSM dans AWS CloudHSM

  Créez des utilisateurs et des clés sur le HSMs dans votre cluster.

  Explorez le guide
- Automatisez le déploiement d'un service Web NGINX à l'aide d'Amazon ECS avec le déchargement TLS dans CloudHSM

  AWS CloudHSM Utilisez-le pour stocker vos clés privées pour vos sites Web hébergés dans le cloud.

  Lisez le blogue

AWS Certificate Manager

- Demande de certificat public

  Utilisez la console AWS Certificate Manager (ACM) ou AWS CLI pour demander un certificat ACM public.

  Explorez le guide
- Les meilleures pratiques pour AWS Certificate Manager

  Découvrez les meilleures pratiques basées sur l'expérience réelle des clients actuels d'ACM.

Explorez le guide

- Comment utiliser pour appliquer AWS Certificate Manager les contrôles d'émission de certificats

  Utilisez les clés de condition IAM pour vous assurer que vos utilisateurs émettent ou demandent des certificats TLS conformément aux directives de votre organisation.

  Lisez le blogue

AWS CA privée

- Planification de votre AWS CA privée déploiement

  AWS CA privée Préparez-vous à l'utiliser avant de créer une autorité de certification privée.

  Explorez le guide

- AWS CA privée administration

  Créez une hiérarchie entièrement AWS hébergée d'autorités de certification racines et subordonnées pour une utilisation interne par votre organisation.

  Explorez le guide

- Administration des certificats

  Effectuez des tâches d'administration de certificats de base AWS CA privée, telles que l'émission, la récupération et la liste de certificats privés.

  Explorez le guide

- AWS CA privée atelier

  Développez une expérience pratique des différents cas d'utilisation des autorités de certification privées.

  Découvrez l'atelier

- Comment simplifier le provisionnement des certificats dans Active Directory avec AWS CA privée

  AWS CA privée Utilisez-le pour fournir plus facilement des certificats aux utilisateurs et aux machines de votre environnement Microsoft Active Directory.

Lisez le blogue

- Comment appliquer les contraintes de nom DNS dans AWS CA privée

  Appliquez des contraintes de nom DNS à une autorité de certification subordonnée à l'aide du AWS CA privée service.

  Lisez le blogue

AWS Secrets Manager

- AWS Secrets Manager concepts

  Effectuez des tâches d'administration de certificats de base AWS CA privée, telles que l'émission, la récupération et la liste de certificats privés.

  Explorez le guide
- Configurez la rotation alternée des utilisateurs pour AWS Secrets Manager

  Configurez une rotation alternée entre les utilisateurs pour un secret contenant les informations d'identification de la base de données.

  Explorez le guide
- Utiliser des AWS Secrets Manager secrets avec Kubernetes

  Affichez les secrets de Secrets Manager sous forme de fichiers montés dans des pods Amazon EKS à l'aide du fournisseur de AWS secrets et de configuration (ASCP).

  Explorez le guide

AWS Payment Cryptography

- Commencer avec AWS Payment Cryptography

  Créez des clés et utilisez-les dans diverses opérations cryptographiques.

  Explorez le guide
- AWS Payment Cryptography FAQs

  Comprenez les bases de AWS Payment Cryptography.

Découvrez le FAQs

Utiliser les services de protection du AWS réseau et des applications

Les tableaux suivants fournissent des liens vers des ressources détaillées décrivant la protection AWS du réseau et des applications.

AWS Firewall Manager

- Commencer à utiliser les AWS Firewall Manager politiques

  AWS Firewall Manager À utiliser pour activer différents types de politiques de sécurité.

  Explorez le guide
- Comment auditer et limiter en permanence les groupes de sécurité avec AWS Firewall Manager

  AWS Firewall Manager À utiliser pour limiter les groupes de sécurité, en veillant à ce que seuls les ports requis soient ouverts.

  Lisez le blogue
- AWS Firewall Manager À utiliser pour déployer une protection à grande échelle dans AWS Organizations

  AWS Firewall Manager À utiliser pour déployer et gérer les politiques de sécurité dans l'ensemble de votre AWS Organizations.

  Lisez le blogue

AWS Network Firewall

- Commencer avec AWS Network Firewall

  Configurez et implémentez un AWS Network Firewall pare-feu pour un VPC doté d'une architecture de passerelle Internet de base.

  Explorez le guide
- AWS Network Firewall Atelier

  Déployez et AWS Network Firewall en utilisant l'infrastructure sous forme de code.

Découvrez l'atelier

- Présentation pratique du moteur de règles AWS Network Firewall flexibles — Partie 1

  Déployez une démonstration de AWS Network Firewall Within your Compte AWS pour interagir avec son moteur de règles.

  Lisez le blogue

- Présentation pratique du moteur de règles AWS Network Firewall flexibles — Partie 2

  Créez une politique de pare-feu avec un ordre de règles strict et définissez une ou plusieurs actions par défaut.

  Lisez le blogue

- Modèles de déploiement pour AWS Network Firewall

  Découvrez les modèles de déploiement pour les cas d'utilisation courants dans lesquels vous pouvez ajouter AWS Network Firewall des éléments au trajet du trafic.

  Lisez le blogue

- Modèles de déploiement AWS Network Firewall avec améliorations du routage VPC

  Utilisez des primitives de routage VPC améliorées pour les insérer AWS Network Firewall entre les charges de travail des différents sous-réseaux d'un même VPC.

  Lisez le blogue

AWS Shield

- Comment AWS Shield fonctionne

  Découvrez comment AWS Shield Standard protéger AWS Shield Advanced les AWS ressources des couches réseau et transport (couches 3 et 4) et de la couche application (couche 7) contre les attaques DDo S.

  Explorez le guide

- Commencer avec AWS Shield Advanced

  Commencez AWS Shield Advanced par utiliser la console Shield Advanced.

Explorez le guide

- AWS Shield Advanced atelier

  Protégez les ressources exposées à Internet contre les attaques DDo S, surveillez les attaques DDo S contre votre infrastructure et informez les équipes appropriées.

  Découvrez l'atelier

AWS WAF

- Commencer avec AWS WAF

  Configurez AWS WAF, créez une ACL Web et protégez Amazon CloudFront en ajoutant des règles et des groupes de règles pour filtrer les requêtes Web.

  Commencez avec le didacticiel
- Analyse AWS WAF des journaux dans Amazon CloudWatch Logs

  Configurez la AWS WAF journalisation native dans CloudWatch les journaux Amazon et visualisez et analysez les données contenues dans les journaux.

  Lisez le blogue
- Visualisez AWS WAF les journaux avec un tableau de CloudWatch bord Amazon

  Utilisez Amazon CloudWatch pour surveiller et analyser AWS WAF l'activité à l'aide de CloudWatch métriques, de Contributor Insights et de Logs Insights.

  Lisez le blogue

Utiliser les services AWS de détection et de réponse

Les tableaux suivants fournissent des liens vers des ressources détaillées décrivant les services AWS de détection et de réponse.

AWS Config

- Commencer avec AWS Config

  Configurez AWS Config et travaillez avec AWS SDKs.

Explorez le guide

- Atelier sur les risques et la conformité

  Automatisez les contrôles à AWS Config l'aide de règles de configuration AWS gérées.

  Découvrez l'atelier

- AWS Config Bibliothèque de kits de développement de règles : créez et gérez des règles à grande échelle

  Utilisez le kit de développement de règles (RDK) pour créer une AWS Config règle personnalisée et la déployer avec le RDKLib.

  Lisez le blogue

AWS CloudTrail

- Afficher l'historique des événements

  Passez en revue l'activité de votre AWS API Compte AWS pour les services qui le prennent en charge CloudTrail.

  Commencez avec le didacticiel

- Créez une trace pour consigner les événements de gestion

  Créez un journal pour enregistrer les événements de gestion dans toutes les régions.

  Commencez avec le didacticiel

AWS Security Hub CSPM

- Activant AWS Security Hub CSPM

  Activez AWS Security Hub CSPM avec AWS Organizations ou dans un compte autonome.

  Explorez le guide

- Agrégation entre régions

  Regroupez AWS Security Hub CSPM les résultats d'une région d'agrégation multiple Régions AWS vers une seule région d'agrégation.

Explorez le guide

- AWS Security Hub CSPM atelier

  Découvrez comment utiliser, gérer AWS Security Hub CSPM et améliorer le niveau de sécurité de vos AWS environnements.

  Découvrez l'atelier

- Trois modèles d'utilisation récurrents du Security Hub CSPM et comment les déployer

  Découvrez les trois modèles AWS Security Hub CSPM d'utilisation les plus courants et comment améliorer votre stratégie d'identification et de gestion des résultats.

  Lisez le blogue

Amazon GuardDuty

- Commencer à utiliser Amazon GuardDuty

  Activez Amazon GuardDuty, générez des échantillons de résultats et configurez des alertes.

  Explorez le didacticiel

- Protection EKS sur Amazon GuardDuty

  Utilisez Amazon GuardDuty pour surveiller vos journaux d'audit Amazon Elastic Kubernetes Service (Amazon EKS).

  Explorez le guide

- Protection Lambda sur Amazon GuardDuty

  Identifiez les menaces de sécurité potentielles lorsque vous invoquez une AWS Lambda fonction.

  Explorez le guide

- GuardDuty Protection Amazon RDS

  Utilisez Amazon GuardDuty pour analyser et profiler l'activité de connexion à Amazon Relational Database Service (Amazon RDS) afin de détecter les menaces d'accès potentielles à vos bases de données Amazon Aurora.

Explorez le guide

- Protection d'Amazon S3 sur Amazon GuardDuty

  Utilisez-le GuardDuty pour surveiller CloudTrail les événements liés aux données et pour identifier les risques de sécurité potentiels dans vos compartiments S3.

  Explorez le guide

- Détection des menaces et réponse avec Amazon GuardDuty et Amazon Detective

  Découvrez les bases d'Amazon GuardDuty et d'Amazon Detective.

  Découvrez l'atelier

Amazon Inspector

- Commencer à utiliser Amazon Inspector

  Activez les scans Amazon Inspector pour comprendre les résultats dans la console.

  Commencez avec le didacticiel

- Gestion des vulnérabilités avec Amazon Inspector

  Utilisez Amazon Inspector pour scanner les instances Amazon EC2 et les images de conteneur dans Amazon Elastic Container Registry (Amazon ECR) afin de détecter des vulnérabilités logicielles.

  Découvrez l'atelier

- Comment scanner EC2 à l'aide AMIs d'Amazon Inspector

  Créez une solution en utilisant plusieurs Services AWS AMIs pour rechercher des vulnérabilités connues.

  Lisez le blogue

Amazon Security Lake

- Commencer à utiliser Amazon Security Lake

  Activez et commencez à utiliser Amazon Security Lake.

Explorez le guide

- Gérer plusieurs comptes avec AWS Organizations

  Collectez des journaux et des événements de sécurité à partir de plusieurs Comptes AWS.

  Explorez le guide

- Ingérez, transformez et diffusez des événements publiés par Amazon Security Lake sur Amazon Service OpenSearch

  Ingérez, transformez et transmettez les données Amazon Security Lake à Amazon OpenSearch Service pour qu'elles soient utilisées par vos SecOps équipes.

  Lisez le blogue

- Comment visualiser les résultats d’Amazon Security Lake avec Quick

  Interrogez et visualisez les données d'Amazon Security Lake à l'aide d'Amazon Athena et de Quick.

  Lisez le blogue

Amazon Detective

- Termes et concepts d'Amazon Detective

  Découvrez les termes et concepts clés qui sont importants pour comprendre Amazon Detective et son fonctionnement.

  Explorez le guide

- Configuration d'Amazon Detective

  Activez Amazon Detective depuis la console Amazon Detective, l'API Amazon Detective ou AWS CLI.

  Explorez le guide

- Détection des menaces et réponse avec Amazon GuardDuty et Amazon Detective

  Découvrez les bases d'Amazon GuardDuty et d'Amazon Detective.

  Découvrez l'atelier

Utilisez les services AWS de gouvernance et de conformité

Les tableaux suivants fournissent des liens vers des ressources détaillées qui décrivent la gouvernance et la conformité.

AWS Organizations

- Création et configuration d'une organisation

  Créez votre organisation et configurez-la avec deux comptes AWS membres.

  Commencez avec le didacticiel
- Des services qui fonctionnent avec AWS Organizations

  Découvrez quels services Services AWS vous pouvez utiliser AWS Organizations et quels sont les avantages de l'utilisation de chaque service à l'échelle de l'organisation.

  Explorez le guide
- Organisation de votre AWS environnement à l'aide de plusieurs comptes

  Mettez en œuvre les meilleures pratiques et les recommandations actuelles pour organiser votre AWS environnement global.

  Lire le livre blanc

AWS Artifact

- Commencer avec AWS Artifact

  Téléchargez les rapports de sécurité et de conformité, gérez les accords juridiques et gérez les notifications.

  Explorez le guide
- Gestion des accords dans AWS Artifact

  Utilisez le AWS Management Console pour consulter, accepter et gérer les accords relatifs à votre compte ou à votre organisation.

  Explorez le guide

- Préparez-vous à un audit dans AWS la partie 1 — AWS Audit Manager et AWS Artifact AWS Config

  Services AWS À utiliser pour vous aider à automatiser la collecte des preuves utilisées dans les audits.

  Lisez le blogue

AWS Audit Manager

- Activation AWS d'Audit Manager

  Activez Audit Manager à l' AWS Management Console aide de l'API Audit Manager ou du AWS CLI.

  Explorez le guide
- Tutoriel pour les responsables d'audit : Création d'une évaluation

  Créez une évaluation à l'aide de l'exemple de framework Audit Manager.

  Explorez le guide
- Tutoriel pour les délégués : Révision d'un ensemble de contrôles

  Passez en revue un ensemble de contrôles qui a été partagé avec vous par un propriétaire d'audit dans Audit Manager.

  Explorez le guide

AWS Control Tower

- Commencer avec AWS Control Tower

  Configurez et lancez un environnement multi-comptes, appelé zone d'atterrissage, qui suit les meilleures pratiques prescriptives.

  Explorez le guide
- Modernisation de la gestion des comptes avec Amazon Bedrock et AWS Control Tower

  Fournissez un compte d'outils de sécurité et tirez parti de l'IA générative pour accélérer le processus de Compte AWS configuration et de gestion.

Lisez le blogue

- Création d'un environnement bien conçu AWS GovCloud (aux États-Unis) avec AWS Control Tower

  Configurez votre gouvernance dans les régions AWS GovCloud (États-Unis), notamment en gérant vos AWS charges de travail à l'aide des unités organisationnelles (OUs) et Comptes AWS.

  Lisez le blogue

Explorez les services AWS de sécurité, d'identité et de gouvernance

Editable architecture diagrams

Schémas d'architecture de référence

Explorez les diagrammes d'architecture de référence pour vous aider à développer votre stratégie de sécurité, d'identité et de gouvernance.

Explorez les architectures de référence en matière de sécurité, d'identité et de gouvernance

Ready-to-use code

Solution en vedette

Informations sur la sécurité sur AWS

Déployez du code AWS intégré pour vous aider à visualiser les données dans Amazon Security Lake afin d'étudier et de réagir plus rapidement aux événements de sécurité.

Découvrez cette solution

AWS Des solutions

Explorez les solutions déployables préconfig urées et leurs guides de mise en œuvre, conçus par. AWS

Découvrez toutes les solutions AWS de sécurité, d'identité et de gouvernance

Documentation

Livres blancs sur la sécurité, l'identité et la gouvernance

Consultez les livres blancs pour obtenir des informations supplémentaires et des meilleure s pratiques sur le choix, la mise en œuvre et l'utilisation des services de sécurité, d'identité et de gouvernance les mieux adaptés à votre organisation.

Explorez les livres blancs sur la sécurité, l'identité et la gouvernance

AWS Blog sur la sécurité

Consultez les articles de blog qui traitent de cas d'utilisation spécifiques de la sécurité.

Explorez le blog sur AWS la sécurité

Historique du document

Le tableau suivant décrit les modifications importantes apportées à ce guide de décision. Pour recevoir des notifications concernant les mises à jour de ce guide, vous pouvez vous abonner à un flux RSS.

Modification	Description	Date
Mise à jour de re:Invent	Ajout d'informations sur AWS la réponse aux incidents de sécurité et AWS Payment Cryptography. Informations de service mises à jour pour Gestion des identités et des accès AWS et AWS IAM Identity Center.	30 décembre 2024
Mise à jour vidéo	Vidéo d'introduction mise à jour avec une récente conférence éclair de Re:inForce 2024.	25 juin 2024
Services de gouvernance supplémentaires	Élargissement de la portée du document pour inclure la gouvernance, notamment en ajoutant AWS CloudTrail AWS Control Tower, et AWS Organizations. Graphismes mis à jour pour refléter la nouvelle portée. Meilleures pratiques clarifiées en matière d'identité. Modifications rédactionnelles dans tout le document.	7 juin 2024
Publication initiale	Guide publié pour la première fois.	21 mars 2024

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.