Rampez, marchez, courez : accélérer la maturité en matière de sécurité dans AWS Cloud

AWS Conseils prescriptifs

AWS Conseils prescriptifs: Rampez, marchez, courez : accélérer la maturité en matière de sécurité dans AWS Cloud

Table of Contents

Rampez, marchez, courez : accélérer la maturité en matière de sécurité dans le AWS Cloud

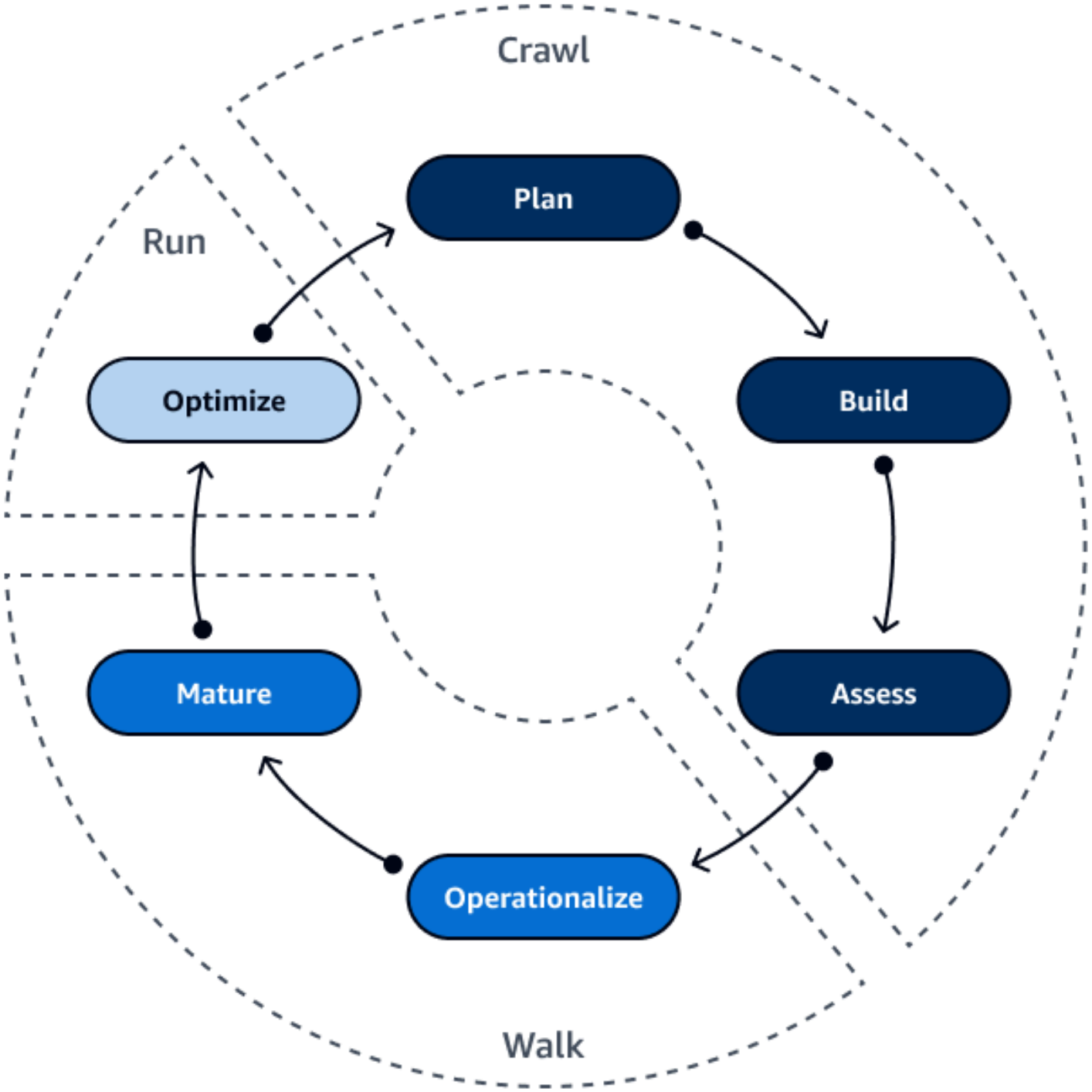
Amazon Web Services (contributeurs)

Décembre 2023 (historique du document)

Pour de nombreuses entreprises, la sécurité est la priorité numéro un et un élément à prendre en compte lors de la migration vers le cloud. La mise en œuvre de fonctionnalités et de contrôles de sécurité dans le cloud n'est pas une activité ponctuelle, c'est un modèle itératif. Vous augmentez progressivement votre niveau de sécurité et votre maturité à mesure que vous augmentez les opérations dans le cloud. Par exemple, vous pouvez commencer par des politiques AWS gérées, puis, lorsque votre organisation sera prête, vous pourrez mettre en œuvre des politiques personnalisées qui respectent le principe du moindre privilège.

Ce guide fournit une feuille de route pour l'utilisation d'une méthodologie « crawl, walk, run » afin d'accélérer la maturité de votre entreprise en matière de sécurité cloud. Il définit une step-by-step approche pour automatiser les fonctionnalités de sécurité. Il explique également de manière pragmatique comment tirer le meilleur parti des fonctionnalités Services AWS et des fonctionnalités. Ce guide vous aide à comprendre les défis et les opportunités du cloud et à savoir comment progresser rapidement et réussir avec AWS.

Une transition vers le cloud nécessite de créer des cadres, de gérer et de faire évoluer les opérations, ainsi que d'optimiser les processus. L'image suivante montre les phases de chaque étape de la méthodologie crawl, walk, run : planification, construction, évaluation, opérationnalisation, maturité et optimisation.



La phase d'exploration consiste à planifier, à jeter les bases et à évaluer votre posture de sécurité actuelle. Au cours de la phase de marche, vous opérationnalisez votre personnel, vos processus et votre technologie, puis vous faites évoluer vos opérations grâce à des ajustements et à des mesures. La phase d'exécution consiste à optimiser par le biais de l'évaluation et de l'automatisation.

Étape d'exploration : planification, construction et évaluation

La phase de crawl commence par la planification. La planification implique de déterminer le périmètre de sécurité et de choisir le modèle le mieux adapté à votre organisation. Après avoir établi le plan, vous pouvez commencer à construire une fondation. Ceci est suivi d'une évaluation de votre posture de sécurité actuelle et de la mise en place d'une discipline dès que vous construisez l'infrastructure de sécurité. La phase de crawl est itérative. L'itération dans le cloud est plus rapide que l'itération dans un environnement sur site. Au fur et à mesure que vous développez vos capacités cloud, le processus d'itération s'accélère.

Les phases de la phase de crawl sont les suivantes :

- Plan— Comment déterminez-vous votre champ d'application et choisissez-vous un modèle ?
- Génération— Comment allez-vous établir le cadre ?
- Évaluation— Quel est votre niveau de sécurité actuel ?

Plan : définition de votre périmètre et de votre modèle de sécurité

La planification est un processus itératif au fur et à mesure que vous faites évoluer votre modèle de sécurité. Les principales étapes du processus de planification sont les suivantes :

- Comprendre le périmètre de sécurité— L'étendue de la sécurité varie et dépend de la manière dont le cloud est utilisé.
- Choix d'un modèle de sécurité— Identifiez le modèle de sécurité le mieux adapté à votre cas d'utilisation de la sécurité.
- Création d'un modèle d'objectifs commerciaux— Définissez des objectifs et des mécanismes clairs pour mesurer le succès.

Lorsque vous élaborez votre plan, tenez compte des points suivants :

- Soyez prêt à répéter. L'itération est constante dans le cloud. L'itération vous aide à identifier les lacunes du plan.
- Ne commencez pas par les services. Commencez par votre plan au lieu de choisir les services dont vous avez besoin. Cela permet à votre organisation d'atteindre les résultats escomptés.

Comprendre le périmètre de sécurité

Le modèle de responsabilité AWS partagée définit la manière dont vous partagez les responsabilités en AWS matière de sécurité et de conformité dans le cloud. AWS sécurise l'infrastructure qui exécute tous les services proposés dans le AWS Cloud, et vous êtes responsable de la sécurisation de votre utilisation de ces services, tels que vos données et vos applications.

Ce modèle partagé peut vous aider à alléger votre charge opérationnelle et de conformité car il AWS exploite, gère et contrôle de nombreux composants, depuis le système d'exploitation hôte et la couche de virtualisation jusqu'à la sécurité physique des installations dans lesquelles le service fonctionne. Les services gérés vous aident à réduire vos obligations en matière de sécurité et de conformité en vous AWS permettant de gérer certaines tâches de sécurité, telles que les correctifs et la gestion des vulnérabilités. L'utilisation de services gérés est l'une des meilleures pratiques du AWS Well-Architected Framework. En général, à mesure que l'infrastructure est modernisée, de plus en plus de responsabilités sont transférées au fournisseur de services.

Voici trois exemples de services différents destinés à vous aider à comprendre comment votre périmètre de sécurité change en fonction des services que vous choisissez :

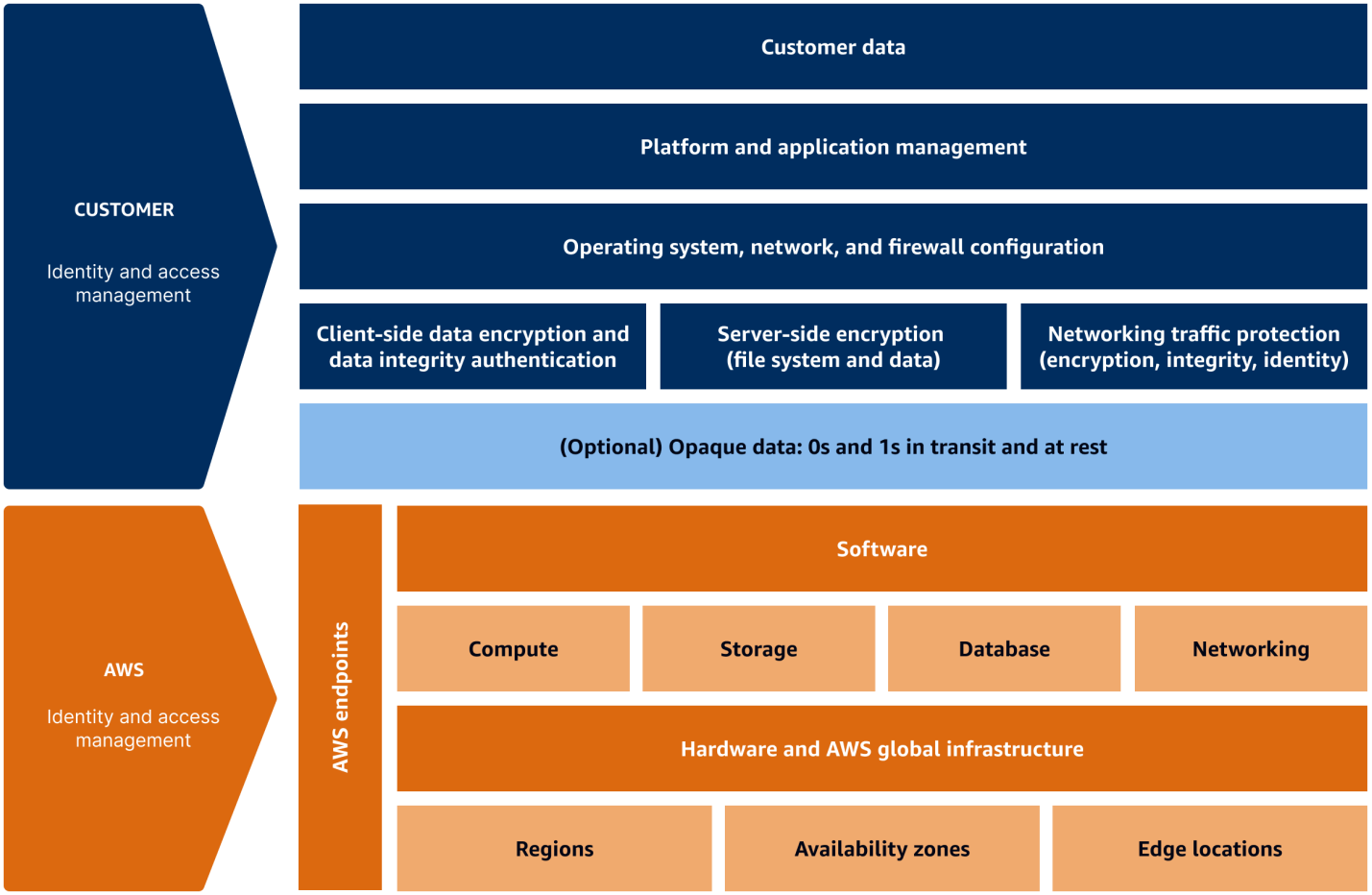
- Services d'infrastructure
- Services de conteneurs
- Services sans serveur

Votre responsabilité en matière de sécurité n'est pas statique et change en fonction du type d'architecture que vous sélectionnez. Votre temps, vos efforts et vos coûts dépendent de l'architecture cloud que vous choisissez.

Services d'infrastructure

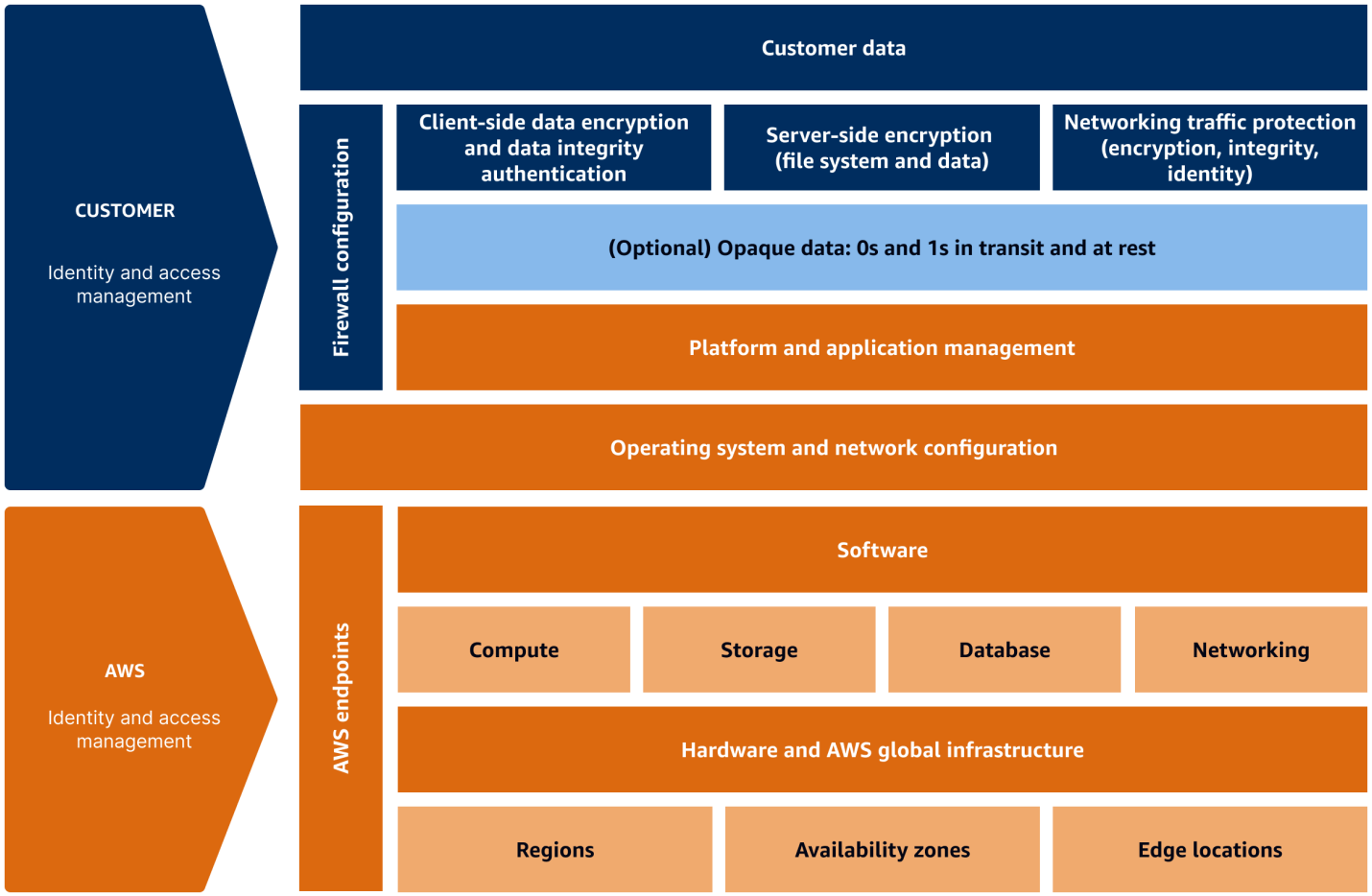
Pour les services d'infrastructure, AWS se concentre sur la sécurisation de l'infrastructure sous-jacente. En ce qui concerne les services d'infrastructure, le champ d'application est plus large pour le

client, car il doit s'occuper de la sécurité de la plate-forme, de l'application des correctifs du système d'exploitation et de la gestion des applications, par rapport aux autres modèles. Amazon Elastic Compute Cloud (Amazon EC2) est un exemple de service d'infrastructure courant.



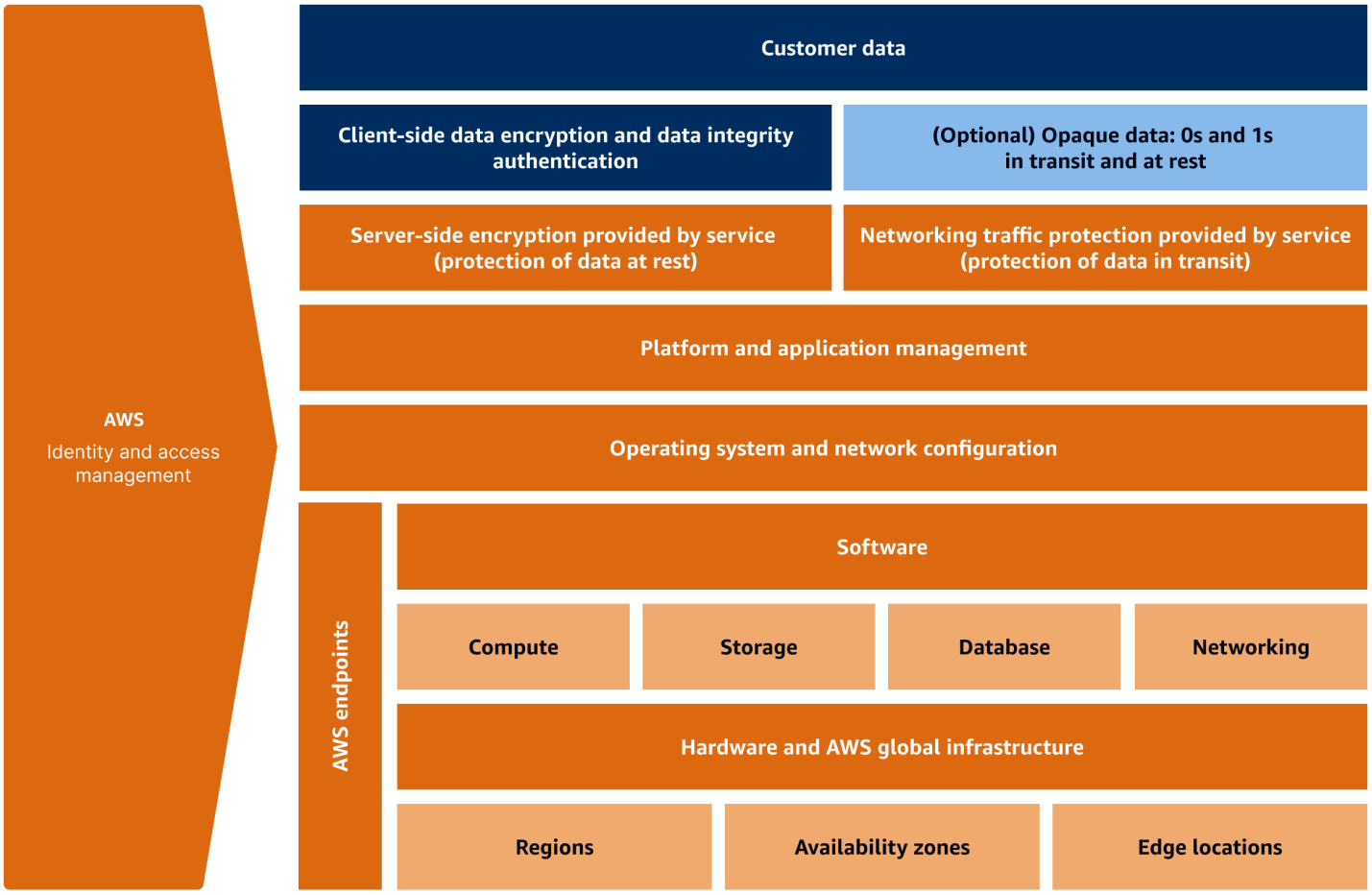
Services de conteneurs

À mesure que l'infrastructure devient plus abstraite et modernisée, l'encombrement diminue. Votre champ d'action se réduit car la responsabilité de certains éléments de sécurité passe à AWS. Les services de conteneurs sont un exemple sur lequel certaines des responsabilités du backend sont renvoyées AWS. Par exemple, AWS devient responsable de la configuration du système d'exploitation (OS), de la configuration du réseau, de la gestion de la plate-forme et de la gestion des applications. Les exemples de services de conteneurs courants incluent Amazon Elastic Kubernetes Service (Amazon EKS), Amazon Elastic Container Registry (Amazon ECR), Amazon Elastic Container Service (Amazon ECS) et. AWS Fargate



Services sans serveur

Lorsque vous utilisez des services sans serveur, la quasi-totalité de la responsabilité de la sécurité incombe à AWS. L'étendue de votre responsabilité est minimale. Par exemple, une base de données sans serveur (DB) gérée vous évite d'avoir à sécuriser le réseau, le matériel et le système d'exploitation. Tous les correctifs du système d'exploitation et de la base de données sont couverts par AWS. Votre seule préoccupation est de sécuriser l'accès aux données par le biais du cryptage et de l'authentification.



Choix d'un modèle de sécurité

Vous pouvez choisir parmi différents modèles ou approches de sécurité pour AWS. Le choix de l'approche et du modèle le mieux adapté dépendent de votre public cible, des résultats commerciaux cibles et du processus commercial global. Il est possible d'utiliser un mélange de plusieurs modèles.

Voici quelques modèles courants :

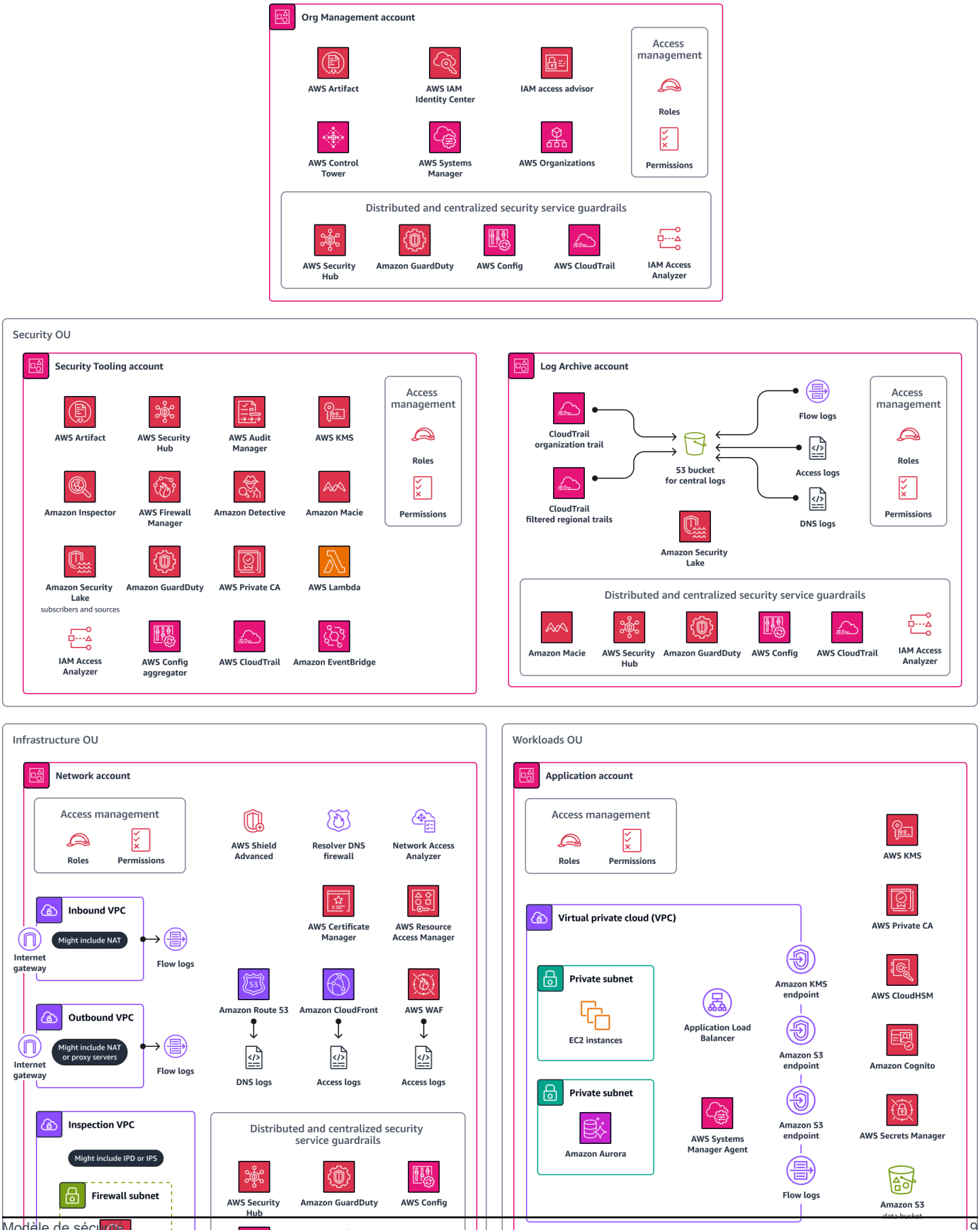
- Maquette architecturale
- Modèle de maturité
- Modèle de gouvernance

Chaque modèle a ses propres avantages et inconvénients. Il est important de déterminer quelle approche convient le mieux à votre organisation. Impliquez les professionnels de la sécurité dès le début du processus de modernisation de votre infrastructure et d'adoption de stratégies cloud. Le

modèle que vous choisissez a un impact significatif sur les rôles et les responsabilités au sein de votre organisation.

Maquette architecturale

L'image suivante montre l'architecture AWS de référence de sécurité. Cette approche architecturale fournit un modèle pour un modèle de sécurité. Cette approche est particulièrement adaptée lorsque vous interagissez avec des équipes techniques au sein de votre organisation. Cela aide à définir un objectif idéal pour l'avenir. Il s'aligne également sur de nombreux AWS cadres et normes de conformité.


Org Management account
AWS Artifact
AWS IAM Identity Center
IAM access advisor
Access management
Roles
Permissions
AWS Control Tower
AWS Systems Manager
AWS Organizations
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Security OU
Security Tooling account
AWS Artifact
AWS Security Hub
AWS Audit Manager
AWS KMS
Access management
Roles
Permissions
Amazon Inspector
AWS Firewall Manager
Amazon Detective
Amazon Macie
Amazon Security Lake
subscribers and sources
Amazon GuardDuty
AWS Private CA
AWS Lambda
IAM Access Analyzer
AWS Config aggregator
AWS CloudTrail
Amazon EventBridge
Log Archive account
CloudTrail organization trail
CloudTrail filtered regional trails
S3 bucket for central logs
Flow logs
Access logs
DNS logs
Amazon Security Lake
Access management
Roles
Permissions
Distributed and centralized security service guardrails
Amazon Macie
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Infrastructure OU
Network account
Access management
Roles
Permissions
AWS Shield Advanced
Resolver DNS firewall
Network Access Analyzer
AWS Certificate Manager
AWS Resource Access Manager
Inbound VPC
Might include NAT
Internet gateway
Flow logs
Outbound VPC
Might include NAT or proxy servers
Internet gateway
Flow logs
Amazon Route 53
Amazon CloudFront
AWS WAF
DNS logs
Access logs
Access logs
Inspection VPC
Might include IPD or IPS
Firewall subnet
AWS Network Firewall
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Workloads OU
Application account
Access management
Roles
Permissions
AWS KMS
AWS Private CA
AWS CloudHSM
Amazon Cognito
AWS Secrets Manager
Amazon S3
Virtual private cloud (VPC)
Private subnet
EC2 instances
Private subnet
Amazon Aurora
Application Load Balancer
AWS Systems Manager Agent
Amazon KMS endpoint
Amazon S3 endpoint
Amazon S3 endpoint
Flow logs
Distributed and centralized security service guardrails
Amazon Macie
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer

Avantages du modèle architectural :

- S'aligne sur les exigences de la Health Insurance Portability and Accountability Act (HIPAA) et du cadre de sécurité commun de la Health Information Trust Alliance (HITRUST CSF)
- Fournit une perspective architecturale
- S'aligne sur les stratégies cloud et les conseils destinés aux grandes entreprises
- S'aligne sur le cadre d'adoption du AWS cloud (AWS CAF)
- S'aligne sur le framework AWS Well-Architected

Inconvénient du modèle architectural :

- Est axé sur la technologie plutôt que sur les affaires

Modèle de maturité

L'approche du modèle AWS de maturité de la sécurité met l'accent sur la gestion et la réduction des risques en priorisant la mise en œuvre des mesures de sécurité. Cette approche convient parfaitement aux directeurs de la sécurité CISOs, mais elle n'est pas axée sur l'entreprise.

Avantages du modèle de maturité :

- Est axé sur la sécurité
- Est un modèle qui met l'accent sur l'utilisation d'une approche de mise en œuvre basée sur l'agilité
- Vous aide à réduire rapidement les risques
- S'aligne sur le cadre d'adoption du AWS cloud (AWS CAF)

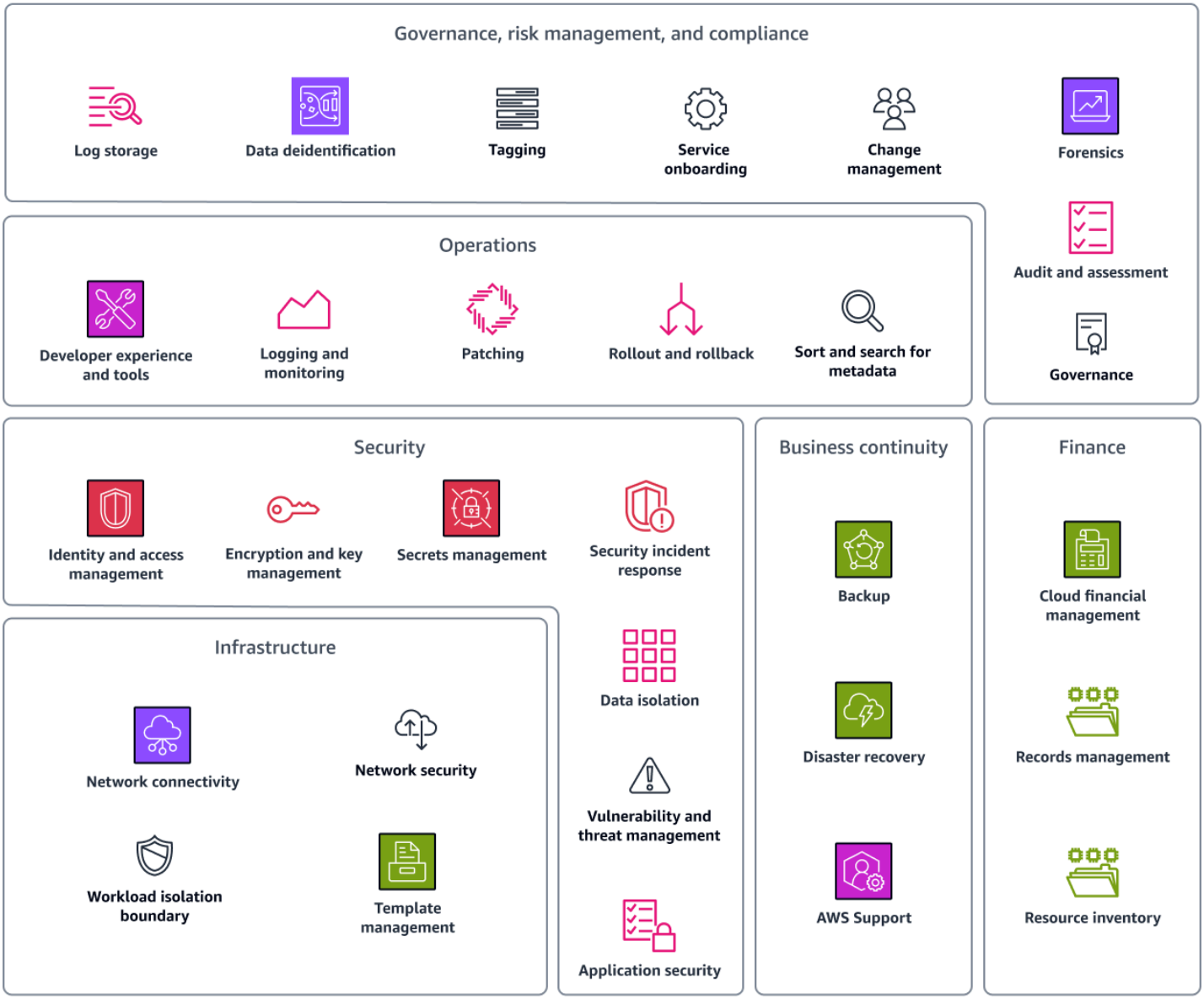
Inconvénients du modèle de maturité :

- Est axé sur la technologie plutôt que sur les affaires

Modèle de gouvernance

Le AWS modèle Cloud Foundation utilise une approche de gouvernance, de gestion des risques et de conformité (GRC) pour aider les entreprises à répondre aux exigences de sécurité et de conformité. Il définit les politiques générales que votre environnement cloud doit suivre. Les

fonctionnalités de ce modèle vous aident à définir les mesures à prendre, à définir votre propension au risque et à aligner les politiques internes.



Le modèle Cloud Foundation est un guide de capacité et de gouvernance qui vous aide à créer et à faire évoluer votre AWS Cloud environnement. Il est basé sur un ensemble de définitions, de scénarios, de conseils et d'automatisations. Le guide inclut les aspects liés aux personnes, aux processus et à la technologie liés à la création d'un AWS Cloud environnement. Il couvre six catégories de fonctionnalités essentielles pour une base cloud :

- Gouvernance, gestion des risques et conformité
- Opérations

- Sécurité
- Continuité des activités
- Finance
- Infrastructures

Le guide fournit également des exemples, des chronologies et des lectures supplémentaires pour chaque fonctionnalité.

Avantages du modèle de gouvernance :

- Possède une large orientation technologique
- Conçu pour la fiabilité
- Utilise une approche opérationnelle

Inconvénient du modèle de gouvernance :

- Est axé sur la technologie plutôt que sur les affaires

Création d'un modèle d'objectifs commerciaux

Le modèle d'objectifs commerciaux implique la définition des résultats commerciaux. Il est similaire au AWS Cloud Adoption Framework et au AWS Well-Architected Framework. Cette approche met l'accent sur ce qui intéresse l'entreprise en interprétant les résultats commerciaux cibles. L'avantage de cette approche réside dans le fait qu'il est facile de lier les objectifs commerciaux aux objectifs de sécurité. Voici un exemple d'objectif commercial : « Permettre des connexions externes sécurisées et accélérer le provisionnement de nouveaux utilisateurs et environnements, en automatisant la visibilité et en évaluant par rapport aux meilleures pratiques afin de réduire continuellement les risques ». Vous définissez des objectifs technologiques qui vous aident à atteindre les résultats commerciaux correspondants. Le modèle d'objectifs commerciaux est lié aux objectifs de sécurité, tels que le maintien de la visibilité. Vous mettez ensuite en œuvre un objectif technique, tel que les meilleures pratiques de sécurité Gestion des identités et des accès AWS (IAM), afin de réduire les risques de sécurité.

Avantages de l'approche axée sur les objectifs commerciaux :

- Comprend une justification des coûts

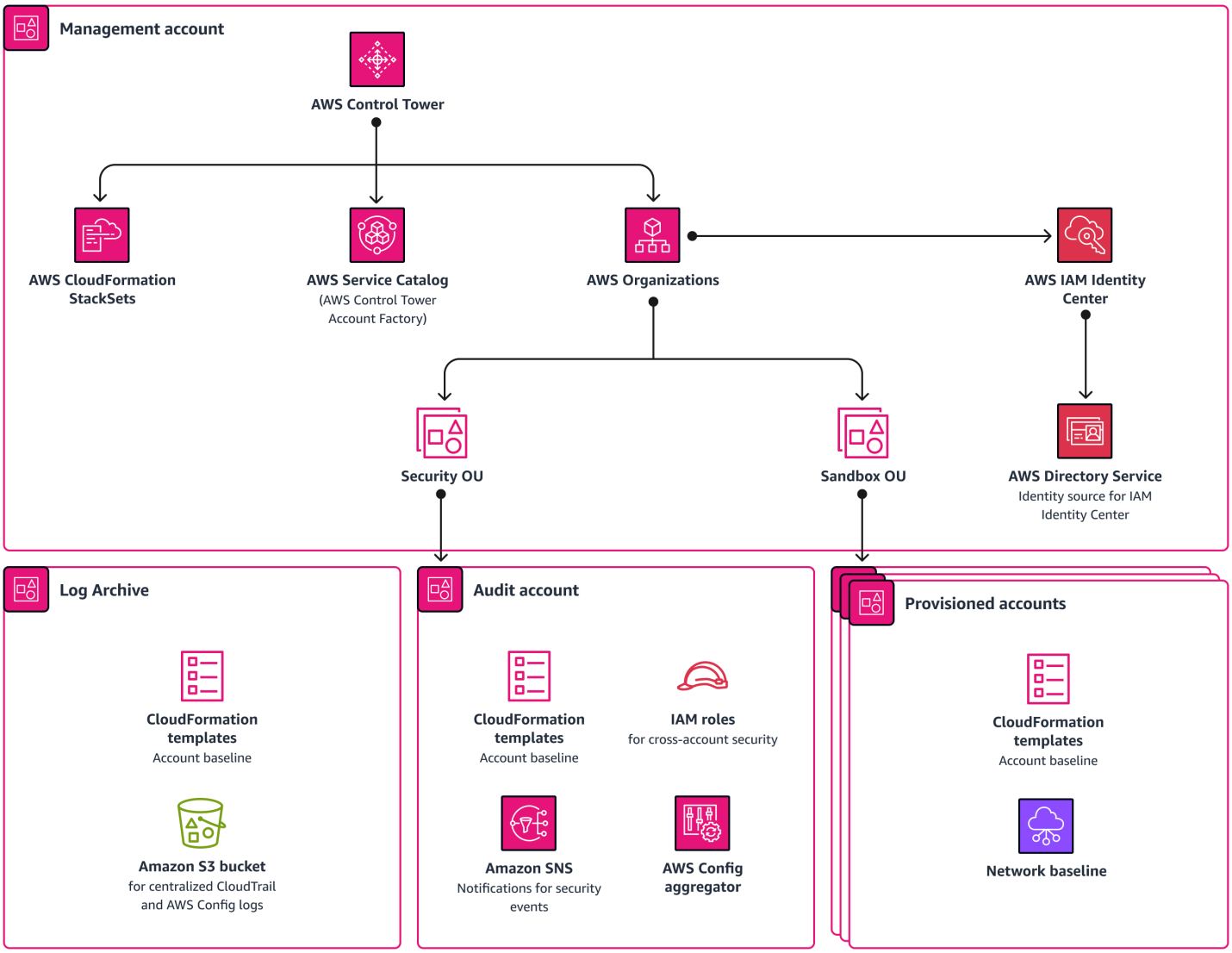
- Fournit une orientation de sécurité claire et adaptée à l'entreprise
- Définit les mesures du succès grâce à l'atteinte des résultats commerciaux cibles

Inconvénients de l'approche axée sur les objectifs commerciaux :

- Cela peut prendre beaucoup de temps car vous devez déterminer ce que veut l'entreprise
- Est axé sur les affaires plutôt que sur la technologie

Création : jeter les bases d'une base solide en matière de sécurité dans le cloud

Maintenant que vous avez un plan, l'étape suivante consiste à préparer le terrain. Cette étape montre comment créer une base AWS cloud initiale sécurisée, résiliente, évolutive et automatisée sur plusieurs comptes. La préparation du terrain peut être spécifiquement conçue et personnalisée en fonction des objectifs de votre entreprise. Vous pouvez adapter les commandes à une nouvelle zone d'atterrissage ou les inclure dans une zone d'atterrissage existante. Les automatisations intégrées AWS Control Towerpeuvent vous aider à jeter les bases de la sécurité dans le. AWS Cloud L'image suivante montre une zone d'atterrissage configurée via AWS Control Tower.



AWS Control Tower en orchestre plusieurs Services AWS en votre nom, tels que AWS Organizations AWS Service Catalog, et AWS IAM Identity Center. Vous pouvez configurer une nouvelle zone d'atterrissage en moins d'une heure, et cette zone d'atterrissage est conçue pour répondre à vos exigences de sécurité et de conformité. AWS Control Tower configure votre zone d'atterrissage conformément aux meilleures pratiques de sécurité prescriptives. AWS Control Tower vous aide à gérer le provisionnement dans le cloud en améliorant la visibilité et le contrôle des comptes et des utilisateurs finaux. Il aide les administrateurs à allouer et à superviser efficacement les ressources informatiques, à mettre en œuvre un contrôle d'accès basé sur les rôles, à surveiller les performances grâce à des outils de journalisation et de surveillance, à gérer efficacement les coûts, à automatiser les processus de déploiement, à appliquer les mesures de sécurité et à garantir la conformité aux normes du secteur.

AWS Control Tower est le moyen le plus rapide de configurer et de gérer un AWS environnement multi-comptes sécurisé, conforme et basé sur les meilleures pratiques. Pour plus d'informations sur l'utilisation AWS Control Tower et les meilleures pratiques décrites dans la stratégie AWS multi-comptes, voir Stratégie AWS multi-comptes : guide des meilleures pratiques.

Bien que AWS Control Tower ce soit l'approche la plus rapide, ce n'est pas la seule. L'important est de configurer une zone d'atterrissage qui, au minimum, fournit les éléments suivants :

- Gestion multi-comptes
- Gestion des identités et des accès fédérés
- Une archive centralisée pour les journaux
- Accès aux audits entre comptes
- Approvisionnement du compte utilisateur final
- Surveillance et notifications centralisées

Évaluation : évaluation de votre posture actuelle en matière de sécurité du cloud

Avant de déployer quoi que ce soit dans la zone d'atterrissage, évaluez votre zone d'atterrissage pour vous assurer qu'elle répond à vos exigences et pour établir une base de référence. Cette pratique s'appelle une évaluation de la posture dans le cloud. Il vous aide à identifier et à corriger les risques au sein de votre infrastructure cloud. L'évaluation de votre niveau de sécurité dans le cloud fournit une visibilité sur les contrôles de sécurité pertinents dans l'environnement cloud.

Les avantages d'une évaluation de la posture dans le cloud sont les suivants :

- Il vous aide à comprendre votre posture de sécurité actuelle et à obtenir des recommandations pour réduire votre profil de risque, corriger les vulnérabilités existantes ou corriger les erreurs de configuration.
- Il vous aide à identifier les meilleures pratiques en matière de sécurité afin d'éviter les erreurs et de réduire les risques commerciaux.
- Il fournit des indicateurs qui vous aident à suivre les améliorations et à mesurer le succès.

Cette section passe en revue les services AWS Security Hub CSPM et Prowler les outils que vous pouvez utiliser pour évaluer la posture du cloud dans votre environnement.

Prowler

Prowlerest un outil de ligne de commande open source qui vous permet d'évaluer, d'auditer et de surveiller la conformité de vos comptes aux meilleures pratiques AWS de sécurité et aux autres cadres et normes de sécurité. Il inspecte votre configuration et identifie les problèmes de sécurité. Vous pouvez l'utiliser Prowler dans des environnements multi-comptes, et les fournisseurs tiers peuvent également l'utiliser pour évaluer la sécurité de votre AWS environnement.

Les avantages suivants sont les suivants Prowler :

- Il est gratuit et open source.
- Il propose des options de déploiement flexibles et est évolutif.
- Il effectue des contrôles de conformité, tels que ceux du Center for Internet Security (CIS) Benchmark for AWS, du règlement général sur la protection des données (RGPD) et de la loi HIPAA.
- Il vous permet de créer des instantanés et des lignes de base.

AWS Security Hub CSPM

AWS Security Hub CSPMfournit une vue complète de votre état de sécurité dans AWS. Il vous permet également de vérifier que votre environnement est conforme aux normes et aux meilleures pratiques du secteur de la sécurité. Il est intégré AWS Control Tower afin que vous puissiez configurer les contrôles de détection Security Hub CSPM via le AWS Control Tower service. L'objectif de l'accélération de la maturité de la sécurité est de faire passer le processus d'évaluation d'un instantané ponctuel à un processus continu de suivi des progrès.

Les avantages du Security Hub CSPM sont les suivants :

- Il fournit un tableau de bord unifié qui indique l'état actuel de l'environnement et vous aide à identifier et à résoudre les problèmes.
- Il effectue des évaluations continues à l'aide de contrôles automatisés.

Étape de marche : opérationnalisation et maturation

L'étape de marche est axée sur l'opérationnalisation. Au cours de cette étape, votre organisation doit évaluer son modèle d'exploitation actuel, déterminer comment il doit être adapté au cloud, mettre en œuvre ces changements, puis mesurer les progrès réalisés. Cela inclut la prise en compte des compétences, des processus opérationnels et de la technologie. Il est essentiel d'ajuster le déploiement du cloud et de mesurer les progrès tout au long de la phase de démarrage pour valider le succès.

Les phases de l'étape de marche sont les suivantes :

- Opérationnaliser— Comment préparez-vous votre personnel, votre technologie et vos processus au cloud ?
- Mûr— Comment mesurez-vous le progrès et le succès ?

Opérationnalisation : préparer votre entreprise à adopter une posture de sécurité cloud mature

Afin de poursuivre le processus de déploiement des charges opérationnelles dans le cloud, il est important de se concentrer sur l'alignement des personnes, des processus et de la technologie. Cela est particulièrement crucial dans l'environnement cloud, car les processus et les compétences sont susceptibles de différer des opérations sur site. Dans cette section, vous utilisez un cadre pour aligner votre personnel, vos processus et votre technologie, puis vous confirmez que le cadre vous a aidé à atteindre les résultats escomptés.

AWS Cadre d'adoption du cloud

Le cadre d'adoption du AWS cloud (AWS CAF) vous aide à accélérer les résultats de votre entreprise grâce à une utilisation Services AWS et à des fonctionnalités innovantes. AWS La CAF identifie six

perspectives organisationnelles spécifiques qui sous-tendent les transformations réussies du cloud : les entreprises, les personnes, la gouvernance, les plateformes, la sécurité et les opérations. Chaque point de vue contient des fonctionnalités qui peuvent améliorer votre préparation au cloud et vous aider à accélérer votre transition vers le cloud.

L'image suivante montre les six perspectives des AWS FAC et les capacités de chaque perspective. Pour plus d'informations, consultez la section Fonctionnalités de base dans la section Vue d'ensemble du cadre d'adoption du AWS cloud.

Résultats attendus

Lorsque vous utilisez la AWS CAF pour harmoniser votre personnel, vos processus et votre technologie, vous pouvez vous attendre à obtenir les résultats suivants :

- DevSecOps pipeline et processus — La mise en œuvre d'un DevOps pipeline avec des outils de sécurité intégrés peut vous aider à déployer de manière plus sécurisée l'infrastructure sous forme de code (IaC). Vous pouvez implémenter l'analyse de code et les contrôles de sécurité dans le processus de pipeline, comme cfn_nag (GitHub), qui est un analyseur de code statique open source.
- Balisage et gestion des actifs : les balises peuvent vous aider à gérer les ressources dans le cloud de manière plus efficace et plus cohérente. Pour plus d'informations, veuillez consulter la rubrique Balisage de vos AWS ressources. Il est important de développer une stratégie de gestion d'actifs dynamique capable de s'adapter à la nature en constante évolution du cloud. AWS Systems Manager L'inventaire vous permet d'attribuer des balises afin que vous puissiez rechercher, gérer et identifier rapidement vos ressources.
- Intégration de la surveillance et des détectives — Il est essentiel d'établir une méthode pour envoyer des alertes depuis le cloud aux centres d'opérations de sécurité sur site (SOCs) et aux systèmes de gestion des informations et des événements de sécurité (SIEM). Amazon GuardDuty est un service de surveillance continue de la sécurité qui analyse et traite les journaux afin d'identifier les activités inattendues et potentiellement non autorisées dans votre AWS environnement. Il s'intègre également à de nombreux outils tiers.
- Plan et programme de réponse aux incidents dans le cloud — Il est important de s'assurer que le personnel chargé de gérer les alertes cloud connaît le processus d'ingestion de ces alertes et sait comment réagir aux alertes cloud, par rapport aux alertes sur site. Pour améliorer les capacités de réponse aux incidents, formez le personnel à l'utilisation d'Amazon Detective pour l'analyse des journaux. Amazon Detective vous aide à analyser, à enquêter et à identifier la cause première des découvertes de sécurité ou des activités suspectes. Amazon Detective doit faire partie d'un plan de réponse aux incidents.
- Gestion des vulnérabilités dans le cloud — Le processus de gestion des vulnérabilités dans le cloud est différent de celui des environnements sur site. Outre la gestion traditionnelle des vulnérabilités, vous devez également évaluer la couche de code de l'infrastructure. Amazon Inspector est un service de gestion automatique des vulnérabilités qui évalue en permanence vos ressources pour détecter les vulnérabilités et les risques d'exposition involontaire au réseau.
- Gestion de la posture dans le cloud — La gestion de la posture dans le cloud, telle que décrite dans la section Évaluation, est un aspect important de la sécurité du cloud. Vous pouvez l'utiliser

AWS Security Hub CSPM pour automatiser les vérifications des meilleures pratiques de sécurité et évaluer votre position globale en matière de cloud dans l'ensemble de vos activités Comptes AWS.

- Formation à la sécurité du cloud — Il est essentiel de fournir une formation appropriée aux employés afin qu'ils maîtrisent la sécurité du cloud. Cela inclut l'accès aux ressources et l'allocation de temps aux employés pour qu'ils acquièrent les connaissances et les compétences nécessaires. AWS fournit de nombreuses ressources de formation pour améliorer les compétences et éduquer, telles que AWS Skill Builder.

Maturité : réglage et mesure des processus, des outils et des risques

Dans la phase de maturité du modèle de sécurité cloud, l'accent est mis sur l'alignement des équipes de sécurité sur les capacités de sécurité du AWS Cloud Adoption Framework (AWS CAF) et sur la mise en place de processus agiles. Cet alignement permet aux équipes spécialisées d'accélérer l'innovation lors de courts sprints tout en intégrant des feuilles de route et une planification à long terme. La phase de maturité met l'accent sur la collaboration avec les opérations informatiques et sur le renforcement des compétences approfondies et spécialisées dans le cloud. Chaque capacité de sécurité met en œuvre des outils et des processus clés pour améliorer l'efficacité et l'impact, tout en développant des indicateurs et des mécanismes de reporting pour mesurer les changements progressifs et l'impact global.

Au cours de cette phase, vous devez :

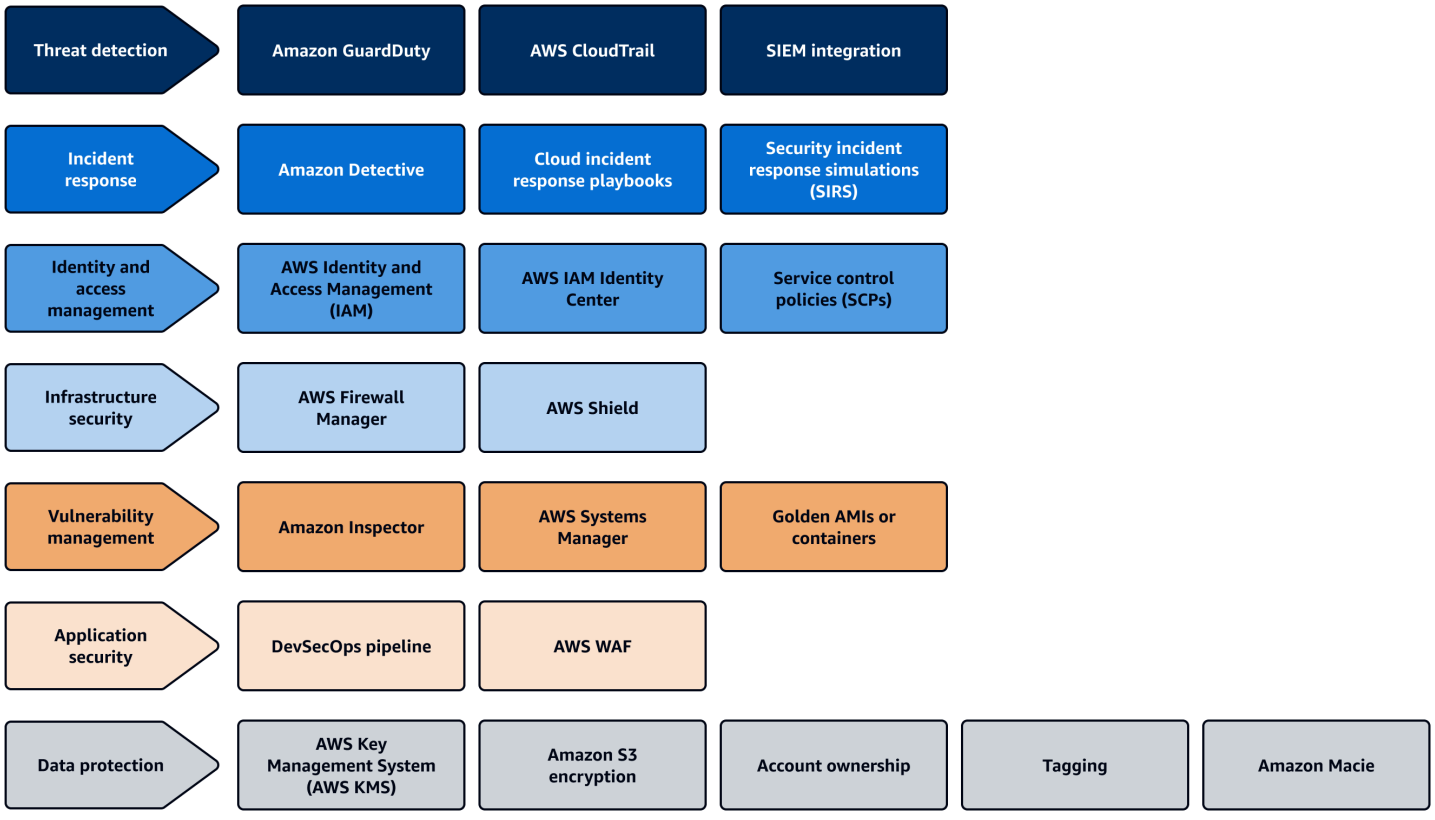
- Réglez et mesurez les processus
- Outils de réglage et de mesure
- Ajustez et mesurez les risques
- Passez en revue des exemples de cas d'utilisation en phase de maturité

Réglez et mesurez les processus

L'approche agile apporte plus de flexibilité et d'innovation, et elle peut vous aider à tester et à mettre en œuvre rapidement de nouvelles idées. Divisez vos équipes de sécurité en rôles spécialisés, tels que les intervenants en cas d'incident et les responsables des vulnérabilités. Les rôles doivent correspondre aux catégories de l'image suivante, qui correspondent aux fonctionnalités du AWS Cloud Adoption Framework (AWS CAF). L'approche agile encourage les équipes à voir les choses

en grand, à inventer, à simplifier et à identifier les failles potentielles en matière de sécurité. Cela se traduit par la création d'un arriéré de témoignages d'utilisateurs ou de feuilles de route pour les améliorations futures.

Un processus agile permet des solutions plus dynamiques et adaptatives, au lieu de s'appuyer uniquement sur les capacités d'un outil spécifique. La rapidité de l'échec est une philosophie qui utilise des tests fréquents et progressifs pour réduire le cycle de vie du développement, et c'est un élément essentiel d'une approche agile. Apportez une modification, testez-la, puis décidez de continuer avec l'approche actuelle ou de passer à une autre. Si les équipes travaillent dans ce cycle, cela permet à votre organisation de rester au fait de l'évolution rapide du cloud. Une formation ciblée est également cruciale, et vous devez proposer une formation spécifique à un domaine particulier de la sécurité du cloud.



> **Note**
>
> Cette image ne contient pas les fonctionnalités d'assurance de sécurité et de gouvernance de la sécurité de la AWS CAF. Ce guide se concentre sur les opérations de sécurité, et l'assurance de la sécurité et la gouvernance n'entrent pas dans le cadre de ce guide.

Pour plus d'informations sur l'assurance de sécurité, voir AWS Re:inForce 2023 - Scaling compliance with on. AWS Control Tower YouTube

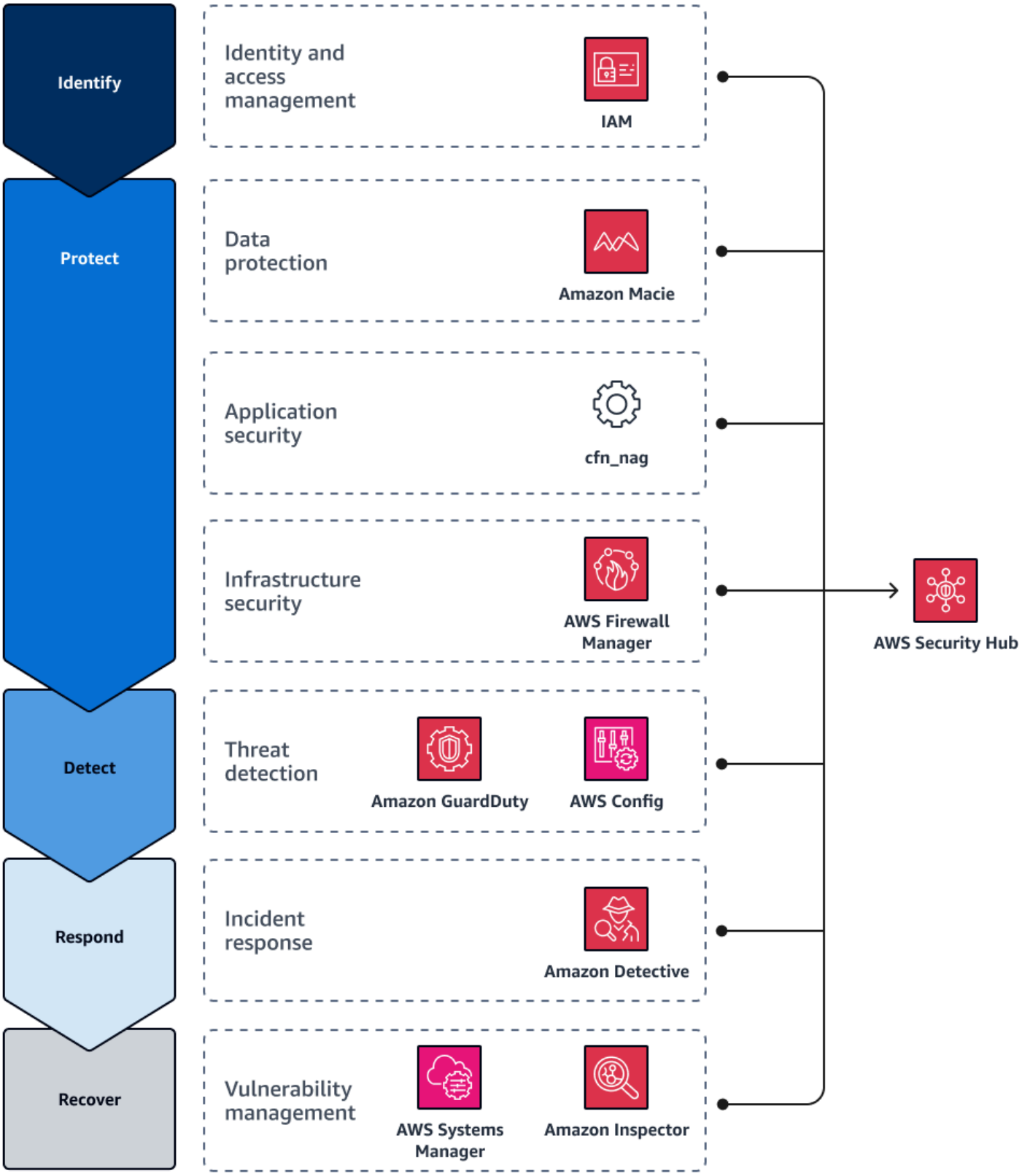
Dans votre organisation, adoptez une approche agile qui l'aide à suivre le rythme du développement et des changements rapides dans le cloud. Voici quelques méthodes pour commencer à expérimenter et à itérer dans votre environnement cloud :

- Spécialisez-vous sur les catégories définies dans la AWS CAF, comme indiqué dans l'image précédente.
- Pour être plus dynamique, concentrez-vous sur l'innovation plutôt que sur les opérations.
- Procédez rapidement aux sprints en permettant aux utilisateurs de tester, d'échouer rapidement et de mettre en œuvre rapidement, puis de poursuivre ce cycle pour suivre le rythme de l'entreprise.
- Pour assurer la continuité des opérations, dans la mesure du possible, alignez les processus pour les environnements basés sur le cloud et sur site.
- Pour aider les individus à approfondir et à se concentrer sur un domaine, offrez une formation ciblée plutôt qu'une formation générale.
- Encouragez les gens à voir les choses en grand, à étudier les hypothèses et à créer des arriérés (tels que des feuilles de route ou des lacunes).

Outils de réglage et de mesure

Après avoir mis en place des équipes spécialisées pour différents domaines de sécurité, alignez les équipes les unes avec les autres. AWS Security Hub CSPMpeut vous aider à y parvenir. Security Hub CSPM fournit un tableau de bord centralisé et unifié pour suivre les progrès par rapport aux frameworks. Il intègre également aux services AWS de sécurité de nombreux outils tiers.

Le cadre de cybersécurité du National Institute of Standards and Technology (NIST) sur le site Web du NIST comprend cinq fonctions : identifier, protéger, détecter, répondre et récupérer. L'image suivante montre comment vous pouvez utiliser différents services Services AWS au cours de chaque fonction, puis configurer ces services pour envoyer leurs résultats à Security Hub CSPM pour des rapports consolidés. Si vous choisissez d'utiliser d'autres outils, vous pouvez utiliser l'API Security Hub CSPM AWS Command Line Interface (AWS CLI) et le AWS Security Finding Format (ASFF) pour créer des intégrations personnalisées. Pour plus d'informations sur les intégrations de Security Hub CSPM à d'autres services, consultez la section Intégrations de produits dans la documentation de AWS Security Hub CSPM Security Hub CSPM.



Security Hub CSPM s'intègre à tous ces services et outils et fournit les fonctionnalités suivantes :

- Fournit un tableau de bord unifié qui affiche les mises à jour et aide les équipes à itérer sur place
- S'intègre automatiquement aux services AWS de sécurité tels qu'Amazon Macie GuardDuty, Amazon et Amazon Detective
- Prend en charge l'intégration avec des outils tiers, tels que Prowleret cfn_nag
- Prend en charge les intégrations personnalisées avec des outils tels que l'API Security Hub CSPM et le format AWS CLI ASFF (AWS Security Finding Format)

Ajustez et mesurez les risques

Pendant la phase de maturité de l'étape de marche, vous pouvez l'utiliser AWS Security Hub CSPM pour ajuster et mesurer en permanence les risques de sécurité. Security Hub CSPM évalue en permanence le niveau de sécurité d'une organisation et prend des mesures pour remédier aux problèmes identifiés. Security Hub CSPM centralise et hiérarchise les résultats de sécurité provenant de l'ensemble des services et des partenaires tiers Comptes AWS pris en charge. Cela vous permet d'analyser les tendances en matière de sécurité et d'identifier les problèmes de sécurité prioritaires.

Security Hub CSPM effectue des centaines de contrôles de sécurité et les classe en fonction des risques pour votre environnement. AWS Vous pouvez consulter votre score par rapport aux contrôles de sécurité dans un tableau de bord unifié de la console Security Hub CSPM. Pour plus d'informations, consultez la section Détermination des scores de sécurité dans la documentation Security Hub CSPM. Grâce à ce tableau de bord, la DevSecOps fonction peut rapidement identifier les vérifications qui ont échoué, la gravité du problème de sécurité Région AWS et les ressources affectées. Une fois le problème identifié, l' DevSecOps équipe peut prioriser le problème et y remédier. Au fur et à mesure que les problèmes sont résolus, Security Hub CSPM met automatiquement à jour l'état.

Passez en revue des exemples de cas d'utilisation en phase de maturité

Voici des exemples de la phase de maturité. Ces exemples approfondissent les modèles, les outils et les processus relatifs aux différents objectifs commerciaux, d'un point de vue pratique.

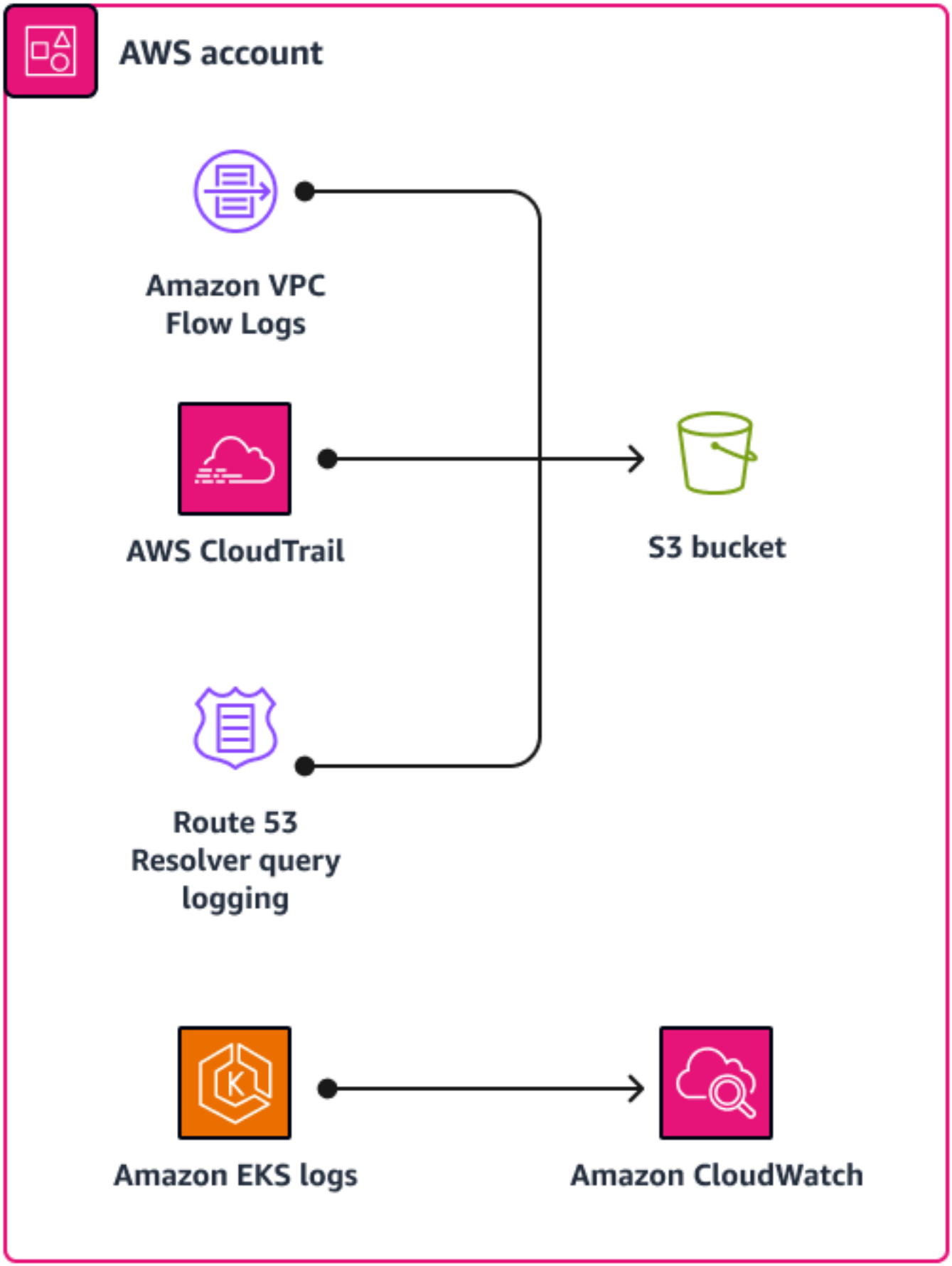
Mature : exemple de détection de menaces

Résultat commercial en matière de contrôles de détection : augmenter la visibilité et la rapidité de détection des incidents liés au cloud afin de réduire les risques et de permettre une utilisation et un développement accélérés des ressources du cloud.

Tool : Assisted Log Enabler for AWS(GitHub) est un outil open source qui vous aide à activer la journalisation en cas d'incident de sécurité. Cela peut rapidement augmenter votre visibilité sur un incident.

Exemple de cas d'utilisation : considérez le cas d'utilisation d'un compte unique illustré dans le schéma suivant. Certains événements nécessitent une enquête plus approfondie. Vous ne savez pas si la journalisation est activée. Dans ce cas, la meilleure solution consiste à effectuer un essai à sec avec le Assisted Log Enabler pour voir quels services sont activés ou désactivés. Assisted Log Enablervérifie la présence de AWS CloudTrail traces, de journaux de requêtes DNS, de journaux de flux VPC et d'autres journaux. S'ils ne sont pas activés, les Assisted Log Enabler active. Assisted Log Enablerpeut vérifier et activer la journalisation dans tous les domaines Régions AWS.

Vous pouvez également Assisted Log Enabler augmenter ou diminuer l'accélération. Une fois que vous avez terminé votre essai à sec, clôturé l'événement et résolu le problème, vous vous rendez compte que vous n'avez plus besoin de ce niveau de journalisation. Vous pouvez rapidement nettoyer le déploiement pour arrêter la journalisation. Cette fonctionnalité vous permet de l'utiliser Assisted Log Enabler comme outil de triage.


AWS account
Amazon VPC Flow Logs
AWS CloudTrail
S3 bucket
Route 53 Resolver query logging
Amazon EKS logs
Amazon CloudWatch

Voici les principales caractéristiques de Assisted Log Enabler for AWS :

- Vous pouvez l'exécuter dans un environnement à compte unique ou multicompte.
- Vous pouvez l'utiliser pour établir une base de référence pour la connexion à votre environnement.
- Vous pouvez utiliser la fonction de fonctionnement à sec pour vérifier l'état actuel et déterminer quels services ont activé la journalisation.
- Vous pouvez sélectionner les services pour lesquels vous souhaitez activer la journalisation.
- Vous pouvez Assisted Log Enabler augmenter ou diminuer l'accélération, selon votre cas d'utilisation.

Mature : exemple IAM

Résultat commercial IAM : automatisez la visibilité et mesurez par rapport aux meilleures pratiques afin de réduire continuellement les risques, de garantir des connexions externes sécurisées et de fournir rapidement de nouveaux utilisateurs et environnements

Outil :AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) vous aide à identifier les ressources partagées avec une entité externe, à valider les politiques IAM par rapport à la grammaire des politiques et aux meilleures pratiques, et à générer des politiques IAM basées sur l'historique des activités d'accès. Nous vous recommandons vivement d'activer IAM Access Analyzer au niveau du compte et de l'organisation.

Avantages du service : IAM Access Analyzer fournit une multitude de résultats pertinents. Il peut identifier les ressources et les comptes de votre organisation qui sont partagés avec une entité externe. Il peut détecter des ressources telles qu'un compartiment S3 public, un compartiment AWS KMS key partagé avec un autre compte ou un rôle partagé avec un compte externe, vous offrant ainsi une excellente visibilité pour identifier les ressources qui ne sont pas sous le contrôle de votre organisation. Il valide non seulement les politiques IAM, mais peut également les générer pour vous.

Étape d'exécution : optimisation de vos opérations de sécurité dans le cloud

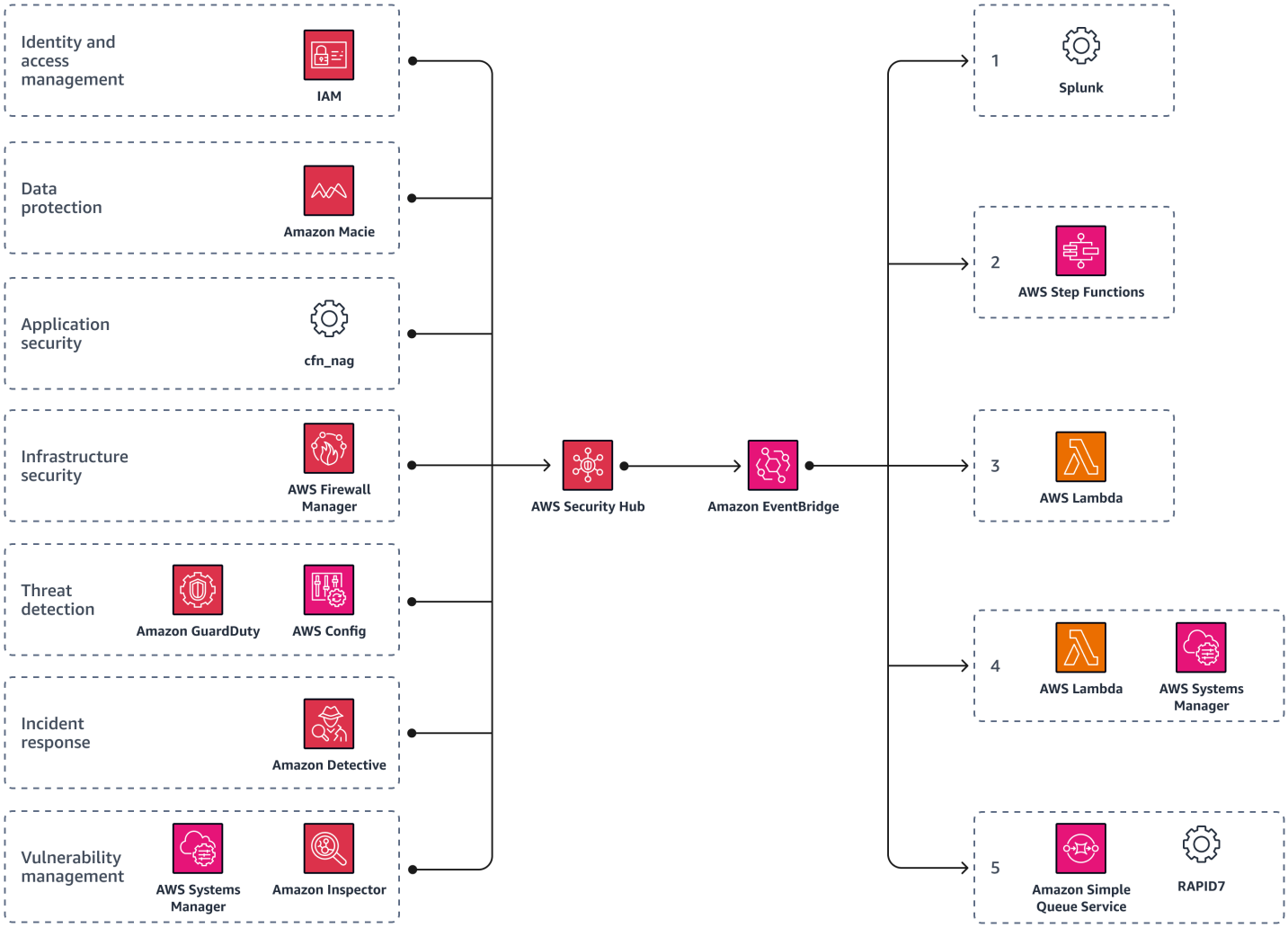
Une fois que vous avez mis en place une base de référence pendant la phase de marche, votre organisation passe à la phase de mise en œuvre. Cette étape vise à démontrer les capacités de cybersécurité disponibles dans le cloud, dont beaucoup ne sont pas possibles ou sont très difficiles à mettre en œuvre avec des solutions sur site. Cette étape réunit différents composants de sécurité et automatise les processus. Les automatisations libèrent vos ressources afin qu'elles puissent se concentrer sur des tâches à forte valeur ajoutée.

La seule phase de la phase d'exécution est la suivante :

- Optimisez— Comment améliorer ce processus et ajouter de l'automatisation ?

Optimisation : automatisez et renouvelez vos opérations de sécurité dans le cloud

Dans la phase d'optimisation, vous automatisez vos opérations de sécurité. Tout comme les étapes de crawl et de marche, vous pouvez les utiliser AWS Security Hub CSPM pendant la phase de course pour obtenir une automatisation et une itération. L'image suivante montre comment Security Hub CSPM peut déclencher une EventBridge règle Amazon personnalisée qui définit les actions automatiques à entreprendre en fonction de résultats et d'informations spécifiques. Pour plus d'informations, consultez la section Automations dans la documentation Security Hub CSPM.



En utilisant Security Hub CSPM comme hub d'automatisation central, vous pouvez également transférer des activités vers. Splunk Splunkpeut ensuite détecter celles qui sont anormales et déclencher les actions correspondantes dans EventBridge. Cela vous permet d'automatiser les tâches répétitives et donne plus de temps aux membres qualifiés de l'équipe pour qu'ils puissent se concentrer sur des activités à plus forte valeur ajoutée. Vous pouvez également l'utiliser AWS Step Functionspour collecter des journaux, prendre des instantanés médico-légaux, mettre en quarantaine les serveurs compromis et les remplacer par une image dorée. En outre, vous pouvez utiliser une AWS Lambdafonction qui corrige les vulnérabilités de l'environnement et qui utilise une fonction Amazon Simple Queue Service (Amazon SQS) pour valider la sécurité des systèmes. AWS Systems Manager En adoptant cette approche, il est possible de contenir et de corriger rapidement les incidents de sécurité avec un impact minimal sur les opérations commerciales normales.

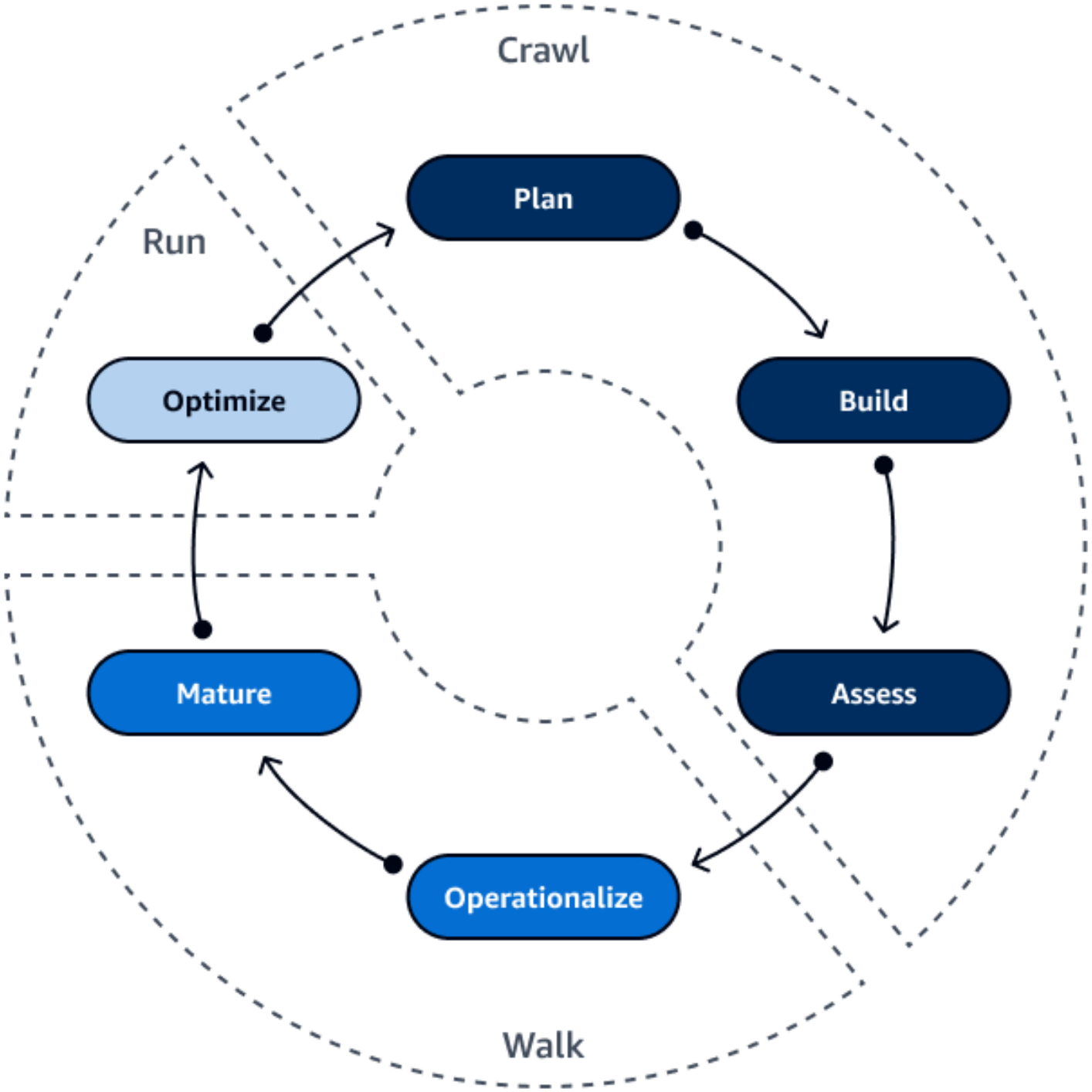
Voici un exemple d'actions automatisées répétées, comme indiqué dans l'image précédente :

1. SplunkÀ utiliser pour détecter les activités douteuses.
2. Utilisez Step Functions pour collecter des journaux, révoquer l'accès, mettre en quarantaine et prendre des instantanés médico-légaux.
3. Utilisez une EventBridge règle pour démarrer une fonction Lambda qui met en quarantaine, prend des instantanés médico-légaux et remplace les serveurs compromis par une image dorée.
4. Démarrez une fonction Lambda qui utilise Systems Manager pour corriger et appliquer des correctifs dans le reste de l'environnement.
5. Lancez un message Amazon SQS qui utilise le scanner Rapid7 pour scanner et valider si la AWS ressource est sécurisée.

Pour plus d'informations, consultez la section Comment automatiser la réponse aux incidents dans AWS Cloud les instances EC2 du blog sur la AWS sécurité.

Conclusion : rampez, marchez, courez, puis volez !

En résumé, le modèle crawl, walk, run est un framework qui vous aide à améliorer progressivement votre posture de sécurité et à adopter les meilleures pratiques pour sécuriser AWS l'infrastructure. Ce processus continue d'évoluer à mesure que de nouvelles technologies et de nouveaux besoins commerciaux apparaissent. En suivant ce cadre et en utilisant les ressources fournies AWS, vous pouvez établir une base solide pour la sécurité du cloud, gérer efficacement les risques de sécurité, accélérer la maturité de la sécurité et stimuler l'innovation.

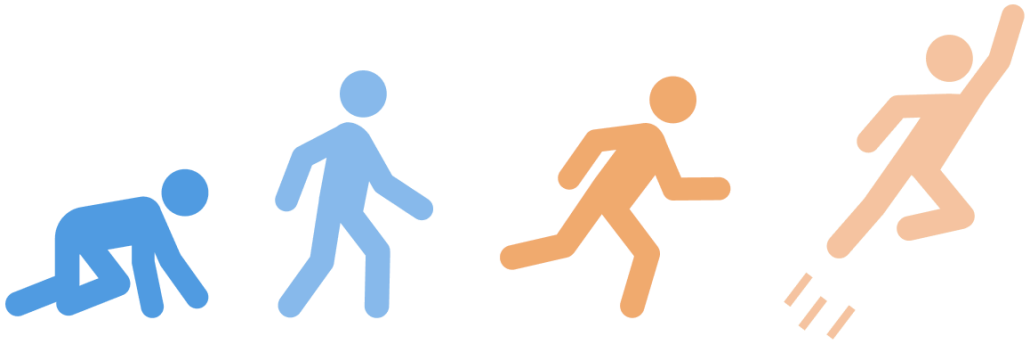


Au stade du crawl, vous posez les bases. Vous définissez votre plan de sécurité, utilisez une architecture de meilleures pratiques de sécurité définie et menez une évaluation continue des objectifs commerciaux de votre entreprise.

Au cours de l'étape de marche, vous faites les premiers pas. Vous examinez les politiques, élaborez des manuels, formez le personnel et alignez les stratégies. Cette étape vous aide à comprendre comment tirer parti de l'innovation pour suivre le rythme des technologies du cloud.

Au stade de la course, tu vois les choses en grand. Vous utilisez l'automatisation et vous placez stratégiquement votre personnel qualifié au bon endroit. Vous mettez en œuvre l'automatisation pour favoriser l'évaluation continue en vue d'atteindre les objectifs commerciaux de votre organisation.

Maintenant, c'est l'heure de prendre l'avion. Suivez les recommandations de ce guide pour accélérer la maturité de votre sécurité dans le AWS Cloud.



Ressources

Cadres et modèles

- AWS Cadre d'adoption du cloud (AWS CAF)
- AWS Framework Well-Architected
- AWS Architecture de référence de sécurité (AWS SRA)
- AWS Modèle de maturité de sécurité
- Architecture de référence HIPAA
- Architecture de référence HITRUST

Services AWS

- AWS Control Tower
- AWS Identity and Access Management Access Analyzer
- AWS Security Hub CSPM

Autres AWS ressources

- Réponse de sécurité automatisée activée AWS dans la bibliothèque de AWS solutions
- Automatisez vos opérations informatiques à l'aide AWS Step Functions d'Amazon CloudWatch Events in the AWS Compute Blog
- Comment automatiser la réponse aux incidents dans AWS Cloud les EC2 exemples du blog sur la AWS sécurité
- Comment effectuer une réponse automatique aux incidents dans un environnement multi-comptes dans le blog sur la AWS sécurité
- AWS Vidéo Re:inForce 2022 - Crawl, walk, run : Accélérer la maturité de la sécurité YouTube
- AWS RE:inForce 2022 - Crawl, walk, run : présentation sur l'accélération de la maturité PowerPoint de la sécurité (pièce jointe)

Collaborateurs

Les personnes suivantes ont contribué à ce guide.

Conception

- Tchad Lorenc, responsable des pratiques de sécurité, AWS
- Ivy Gin, consultante en assurance de sécurité, AWS
- Sayali Paseband, consultante en sécurité, AWS

Révision

- Deeps Baisya, architecte de sécurité senior, AWS
- Mike LaRue, consultant principal en sécurité, AWS
- Raul Radu, ingénieur de sécurité senior, AWS

Rédaction technique

- Lilly AbouHarb, rédactrice technique senior, AWS

Historique du document

Le tableau suivant décrit les modifications importantes apportées à ce guide. Pour être averti des mises à jour à venir, abonnez-vous à un fil RSS.

Modification	Description	Date
Publication initiale	—	20 décembre 2023

AWS Glossaire des directives prescriptives

Les termes suivants sont couramment utilisés dans les stratégies, les guides et les modèles fournis par les directives AWS prescriptives. Pour suggérer des entrées, veuillez utiliser le lien Faire un commentaire à la fin du glossaire.

Nombres

7 R

Sept politiques de migration courantes pour transférer des applications vers le cloud. Ces politiques s'appuient sur les 5 R identifiés par Gartner en 2011 et sont les suivantes :

- Refactorisation/réarchitecture : transférez une application et modifiez son architecture en tirant pleinement parti des fonctionnalités natives cloud pour améliorer l'agilité, les performances et la capacité de mise à l'échelle. Cela implique généralement le transfert du système d'exploitation et de la base de données. Exemple : migrez votre base de données Oracle sur site vers l'édition compatible avec Amazon Aurora PostgreSQL.
- Replateformer (déplacer et remodeler) : transférez une application vers le cloud et introduisez un certain niveau d'optimisation pour tirer parti des fonctionnalités du cloud. Exemple : migrez votre base de données Oracle sur site vers Amazon Relational Database Service (Amazon RDS) pour Oracle dans le. AWS Cloud
- Racheter (rachat) : optez pour un autre produit, généralement en passant d'une licence traditionnelle à un modèle SaaS. Exemple : migrez votre système de gestion de la relation client (CRM) vers Salesforce.com.
- Réhéberger (lift and shift) : transférez une application vers le cloud sans apporter de modifications pour tirer parti des fonctionnalités du cloud. Exemple : migrez votre base de données Oracle sur site vers Oracle sur une instance EC2 dans le. AWS Cloud
- Relocaliser (lift and shift au niveau de l'hyperviseur) : transférez l'infrastructure vers le cloud sans acheter de nouveau matériel, réécrire des applications ou modifier vos opérations existantes. Vous migrez des serveurs d'une plateforme sur site vers un service cloud pour la même plateforme. Exemple : migrer une Microsoft Hyper-V application vers AWS.
- Retenir : conservez les applications dans votre environnement source. Il peut s'agir d'applications nécessitant une refactorisation majeure, que vous souhaitez retarder, et d'applications existantes que vous souhaitez retenir, car rien ne justifie leur migration sur le plan commercial.

- Retirer : mettez hors service ou supprimez les applications dont vous n'avez plus besoin dans votre environnement source.

A

ABAC

Voir contrôle d'accès basé sur les attributs.

services abstraits

Consultez la section Services gérés.

ACIDE

Voir atomicité, consistance, isolation, durabilité.

migration active-active

Méthode de migration de base de données dans laquelle la synchronisation des bases de données source et cible est maintenue (à l'aide d'un outil de réplication bidirectionnelle ou d'opérations d'écriture double), tandis que les deux bases de données gèrent les transactions provenant de la connexion d'applications pendant la migration. Cette méthode prend en charge la migration par petits lots contrôlés au lieu d'exiger un basculement ponctuel. Elle est plus flexible mais demande plus de travail qu'une migration active-passive.

migration active-passive

Méthode de migration de base de données dans laquelle les bases de données source et cible sont synchronisées, mais seule la base de données source gère les transactions liées à la connexion des applications pendant que les données sont répliquées vers la base de données cible. La base de données cible n'accepte aucune transaction pendant la migration.

fonction d'agrégation

Fonction SQL qui agit sur un groupe de lignes et calcule une valeur de retour unique pour le groupe. Des exemples de fonctions d'agrégation incluent `SUM` et`MAX`.

AI

Voir intelligence artificielle.

AIOps

Voir les opérations d'intelligence artificielle.

anonymisation

Processus de suppression définitive d'informations personnelles dans un ensemble de données. L'anonymisation peut contribuer à protéger la vie privée. Les données anonymisées ne sont plus considérées comme des données personnelles.

anti-motif

Solution fréquemment utilisée pour un problème récurrent lorsque la solution est contre-productive, inefficace ou moins efficace qu'une alternative.

contrôle des applications

Une approche de sécurité qui permet d'utiliser uniquement des applications approuvées afin de protéger un système contre les logiciels malveillants.

portefeuille d'applications

Ensemble d'informations détaillées sur chaque application utilisée par une organisation, y compris le coût de génération et de maintenance de l'application, ainsi que sa valeur métier. Ces informations sont essentielles pour le processus de découverte et d'analyse du portefeuille et permettent d'identifier et de prioriser les applications à migrer, à moderniser et à optimiser.

intelligence artificielle (IA)

Domaine de l'informatique consacré à l'utilisation des technologies de calcul pour exécuter des fonctions cognitives généralement associées aux humains, telles que l'apprentissage, la résolution de problèmes et la reconnaissance de modèles. Pour plus d'informations, veuillez consulter Qu'est-ce que l'intelligence artificielle ?

opérations d'intelligence artificielle (AIOps)

Processus consistant à utiliser des techniques de machine learning pour résoudre les problèmes opérationnels, réduire les incidents opérationnels et les interventions humaines, mais aussi améliorer la qualité du service. Pour plus d'informations sur son AIOps utilisation dans la stratégie de AWS migration, consultez le guide d'intégration des opérations.

chiffrement asymétrique

Algorithme de chiffrement qui utilise une paire de clés, une clé publique pour le chiffrement et une clé privée pour le déchiffrement. Vous pouvez partager la clé publique, car elle n'est pas utilisée pour le déchiffrement, mais l'accès à la clé privée doit être très restreint.

atomicité, cohérence, isolement, durabilité (ACID)

Ensemble de propriétés logicielles garantissant la validité des données et la fiabilité opérationnelle d'une base de données, même en cas d'erreur, de panne de courant ou d'autres problèmes.

contrôle d'accès par attributs (ABAC)

Pratique qui consiste à créer des autorisations détaillées en fonction des attributs de l'utilisateur, tels que le service, le poste et le nom de l'équipe. Pour plus d'informations, consultez ABAC pour AWS dans la documentation Gestion des identités et des accès AWS (IAM).

source de données faisant autorité

Emplacement où vous stockez la version principale des données, considérée comme la source d'information la plus fiable. Vous pouvez copier les données de la source de données officielle vers d'autres emplacements à des fins de traitement ou de modification des données, par exemple en les anonymisant, en les expurgant ou en les pseudonymisant.

Zone de disponibilité

Un emplacement distinct au sein d'un Région AWS réseau isolé des défaillances dans d'autres zones de disponibilité et fournissant une connectivité réseau peu coûteuse et à faible latence aux autres zones de disponibilité de la même région.

AWS Cadre d'adoption du cloud (AWS CAF)

Un cadre de directives et de meilleures pratiques visant AWS à aider les entreprises à élaborer un plan efficace pour réussir leur migration vers le cloud. AWS La CAF organise ses conseils en six domaines prioritaires appelés perspectives : les affaires, les personnes, la gouvernance, les plateformes, la sécurité et les opérations. Les perspectives d'entreprise, de personnes et de gouvernance mettent l'accent sur les compétences et les processus métier, tandis que les perspectives relatives à la plateforme, à la sécurité et aux opérations se concentrent sur les compétences et les processus techniques. Par exemple, la perspective liée aux personnes cible les parties prenantes qui s'occupent des ressources humaines (RH), des fonctions de dotation en personnel et de la gestion des personnes. Dans cette perspective, la AWS CAF fournit des conseils pour le développement du personnel, la formation et les communications afin de préparer l'organisation à une adoption réussie du cloud. Pour plus d'informations, veuillez consulter le site Web AWS CAF et le livre blanc AWS CAF.

AWS Cadre de qualification de la charge de travail (AWS WQF)

Outil qui évalue les charges de travail liées à la migration des bases de données, recommande des stratégies de migration et fournit des estimations de travail. AWS Le WQF est inclus avec

AWS Schema Conversion Tool (AWS SCT). Il analyse les schémas de base de données et les objets de code, le code d'application, les dépendances et les caractéristiques de performance, et fournit des rapports d'évaluation.

B

mauvais bot

Un bot destiné à perturber ou à nuire à des individus ou à des organisations.

BCP

Consultez la section Planification de la continuité des activités.

graphique de comportement

Vue unifiée et interactive des comportements des ressources et des interactions au fil du temps. Vous pouvez utiliser un graphique de comportement avec Amazon Detective pour examiner les tentatives de connexion infructueuses, les appels d'API suspects et les actions similaires. Pour plus d'informations, veuillez consulter Data in a behavior graph dans la documentation Detective.

système de poids fort

Système qui stocke d'abord l'octet le plus significatif. Voir aussi endianité.

classification binaire

Processus qui prédit un résultat binaire (l'une des deux classes possibles). Par exemple, votre modèle de machine learning peut avoir besoin de prévoir des problèmes tels que « Cet e-mail est-il du spam ou non ? » ou « Ce produit est-il un livre ou une voiture ? ».

filtre de Bloom

Structure de données probabiliste et efficace en termes de mémoire qui est utilisée pour tester si un élément fait partie d'un ensemble.

déploiement bleu/vert

Stratégie de déploiement dans laquelle vous créez deux environnements distincts mais identiques. Vous exécutez la version actuelle de l'application dans un environnement (bleu) et la nouvelle version de l'application dans l'autre environnement (vert). Cette stratégie vous permet de revenir rapidement en arrière avec un impact minimal.

bot

Application logicielle qui exécute des tâches automatisées sur Internet et simule l'activité ou l'interaction humaine. Certains robots sont utiles ou bénéfiques, comme les robots d'exploration Web qui indexent des informations sur Internet. D'autres robots, appelés « bots malveillants », sont destinés à perturber ou à nuire à des individus ou à des organisations.

botnet

Réseaux de robots infectés par des logiciels malveillants et contrôlés par une seule entité, connue sous le nom d'herder ou d'opérateur de bots. Les botnets sont le mécanisme le plus connu pour faire évoluer les bots et leur impact.

branche

Zone contenue d'un référentiel de code. La première branche créée dans un référentiel est la branche principale. Vous pouvez créer une branche à partir d'une branche existante, puis développer des fonctionnalités ou corriger des bogues dans la nouvelle branche. Une branche que vous créez pour générer une fonctionnalité est communément appelée branche de fonctionnalités. Lorsque la fonctionnalité est prête à être publiée, vous fusionnez à nouveau la branche de fonctionnalités dans la branche principale. Pour plus d'informations, consultez À propos des branches (GitHub documentation).

accès par brise-vitre

Dans des circonstances exceptionnelles et par le biais d'un processus approuvé, c'est un moyen rapide pour un utilisateur d'accéder à un accès auquel Compte AWS il n'est généralement pas autorisé. Pour plus d'informations, consultez l'indicateur Implementation break-glass procedures dans le guide Well-Architected AWS .

stratégie existante (brownfield)

L'infrastructure existante de votre environnement. Lorsque vous adoptez une stratégie existante pour une architecture système, vous concevez l'architecture en fonction des contraintes des systèmes et de l'infrastructure actuels. Si vous étendez l'infrastructure existante, vous pouvez combiner des politiques brownfield (existantes) et greenfield (inédites).

cache de tampon

Zone de mémoire dans laquelle sont stockées les données les plus fréquemment consultées.

capacité métier

Ce que fait une entreprise pour générer de la valeur (par exemple, les ventes, le service client ou le marketing). Les architectures de microservices et les décisions de développement peuvent être dictées par les capacités métier. Pour plus d'informations, veuillez consulter la section Organisation en fonction des capacités métier du livre blanc Exécution de microservices conteneurisés sur AWS.

planification de la continuité des activités (BCP)

Plan qui tient compte de l'impact potentiel d'un événement perturbateur, tel qu'une migration à grande échelle, sur les opérations, et qui permet à une entreprise de reprendre ses activités rapidement.

C

CAF

Voir le cadre d'adoption du AWS cloud.

déploiement de Canary

Diffusion lente et progressive d'une version pour les utilisateurs finaux. Lorsque vous êtes sûr, vous déployez la nouvelle version et remplacez la version actuelle dans son intégralité.

CCo E

Voir le Centre d'excellence du cloud.

CDC

Voir capture des données de modification.

capture des données de modification (CDC)

Processus de suivi des modifications apportées à une source de données, telle qu'une table de base de données, et d'enregistrement des métadonnées relatives à ces modifications. Vous pouvez utiliser la CDC à diverses fins, telles que l'audit ou la réplication des modifications dans un système cible afin de maintenir la synchronisation.

ingénierie du chaos

Introduire intentionnellement des défaillances ou des événements perturbateurs pour tester la résilience d'un système. Vous pouvez utiliser AWS Fault Injection Service (AWS FIS) pour effectuer des expériences qui stressent vos AWS charges de travail et évaluer leur réponse.

CI/CD

Découvrez l'intégration continue et la livraison continue.

classification

Processus de catégorisation qui permet de générer des prédictions. Les modèles de ML pour les problèmes de classification prédisent une valeur discrète. Les valeurs discrètes se distinguent toujours les unes des autres. Par exemple, un modèle peut avoir besoin d'évaluer la présence ou non d'une voiture sur une image.

chiffrement côté client

Chiffrement des données localement, avant que la cible ne les Service AWS reçoive.

Centre d'excellence du cloud (CCoE)

Une équipe multidisciplinaire qui dirige les efforts d'adoption du cloud au sein d'une organisation, notamment en développant les bonnes pratiques en matière de cloud, en mobilisant des ressources, en établissant des délais de migration et en guidant l'organisation dans le cadre de transformations à grande échelle. Pour plus d'informations, consultez les CCoarticles électroniques du blog sur la stratégie AWS Cloud d'entreprise.

cloud computing

Technologie cloud généralement utilisée pour le stockage de données à distance et la gestion des appareils IoT. Le cloud computing est généralement associé à la technologie informatique de pointe.

modèle d'exploitation du cloud

Dans une organisation informatique, modèle d'exploitation utilisé pour créer, faire évoluer et optimiser un ou plusieurs environnements cloud. Pour plus d'informations, consultez la section Création de votre modèle d'exploitation cloud.

étapes d'adoption du cloud

Les quatre phases que les entreprises traversent généralement lorsqu'elles migrent vers AWS Cloud :

- Projet : exécution de quelques projets liés au cloud à des fins de preuve de concept et d'apprentissage
- Base : réaliser des investissements fondamentaux pour accélérer votre adoption du cloud (par exemple, créer une zone de landing zone, définir un CCo E, établir un modèle opérationnel)
- Migration : migration d'applications individuelles
- Réinvention : optimisation des produits et services et innovation dans le cloud

Ces étapes ont été définies par Stephen Orban dans le billet de blog The Journey Toward Cloud-First & the Stages of Adoption publié sur le blog AWS Cloud Enterprise Strategy. Pour plus d'informations sur leur lien avec la stratégie de AWS migration, consultez le guide de préparation à la migration.

CMDB

Consultez la base de données de gestion des configurations.

référentiel de code

Emplacement où le code source et d'autres ressources, comme la documentation, les exemples et les scripts, sont stockés et mis à jour par le biais de processus de contrôle de version. Les référentiels cloud courants incluent GitHub ouBitbucket Cloud. Chaque version du code est appelée branche. Dans une structure de microservice, chaque référentiel est consacré à une seule fonctionnalité. Un seul pipeline CI/CD peut utiliser plusieurs référentiels.

cache passif

Cache tampon vide, mal rempli ou contenant des données obsolètes ou non pertinentes. Cela affecte les performances, car l'instance de base de données doit lire à partir de la mémoire principale ou du disque, ce qui est plus lent que la lecture à partir du cache tampon.

données gelées

Données rarement consultées et généralement historiques. Lorsque vous interrogez ce type de données, les requêtes lentes sont généralement acceptables. Le transfert de ces données vers des niveaux ou classes de stockage moins performants et moins coûteux peut réduire les coûts.

vision par ordinateur (CV)

Domaine de l'IA qui utilise l'apprentissage automatique pour analyser et extraire des informations à partir de formats visuels tels que des images numériques et des vidéos. Par exemple, Amazon SageMaker AI fournit des algorithmes de traitement d'image pour les CV.

dérive de configuration

Pour une charge de travail, une modification de configuration par rapport à l'état attendu. Cela peut entraîner une non-conformité de la charge de travail, et cela est généralement progressif et involontaire.

base de données de gestion des configurations (CMDB)

Référentiel qui stocke et gère les informations relatives à une base de données et à son environnement informatique, y compris les composants matériels et logiciels ainsi que leurs configurations. Vous utilisez généralement les données d'une CMDB lors de la phase de découverte et d'analyse du portefeuille de la migration.

pack de conformité

Ensemble de AWS Config règles et d'actions correctives que vous pouvez assembler pour personnaliser vos contrôles de conformité et de sécurité. Vous pouvez déployer un pack de conformité en tant qu'entité unique dans une région Compte AWS et, ou au sein d'une organisation, à l'aide d'un modèle YAML. Pour plus d'informations, consultez la section Packs de conformité dans la AWS Config documentation.

intégration continue et livraison continue (CI/CD)

Processus d'automatisation des étapes de source, de construction, de test, de préparation et de production du processus de publication du logiciel. CI/CD est communément décrit comme un pipeline. CI/CD peut vous aider à automatiser les processus, à améliorer la productivité, à améliorer la qualité du code et à accélérer les livraisons. Pour plus d'informations, veuillez consulter Avantages de la livraison continue. CD peut également signifier déploiement continu. Pour plus d'informations, veuillez consulter Livraison continue et déploiement continu.

CV

Voir vision par ordinateur.

D

données au repos

Données stationnaires dans votre réseau, telles que les données stockées.

classification des données

Processus permettant d'identifier et de catégoriser les données de votre réseau en fonction de leur sévérité et de leur sensibilité. Il s'agit d'un élément essentiel de toute stratégie de gestion des risques de cybersécurité, car il vous aide à déterminer les contrôles de protection et de conservation appropriés pour les données. La classification des données est une composante du pilier de sécurité du AWS Well-Architected Framework. Pour plus d'informations, veuillez consulter Classification des données.

dérive des données

Une variation significative entre les données de production et les données utilisées pour entraîner un modèle ML, ou une modification significative des données d'entrée au fil du temps. La dérive des données peut réduire la qualité, la précision et l'équité globales des prédictions des modèles ML.

données en transit

Données qui circulent activement sur votre réseau, par exemple entre les ressources du réseau.

maillage de données

Un cadre architectural qui fournit une propriété des données distribuée et décentralisée avec une gestion et une gouvernance centralisées.

minimisation des données

Le principe de collecte et de traitement des seules données strictement nécessaires. La pratique de la minimisation des données AWS Cloud peut réduire les risques liés à la confidentialité, les coûts et l'empreinte carbone de vos analyses.

périmètre de données

Ensemble de garde-fous préventifs dans votre AWS environnement qui permettent de garantir que seules les identités fiables accèdent aux ressources fiables des réseaux attendus. Pour plus d'informations, voir Création d'un périmètre de données sur AWS.

prétraitement des données

Pour transformer les données brutes en un format facile à analyser par votre modèle de ML. Le prétraitement des données peut impliquer la suppression de certaines colonnes ou lignes et le traitement des valeurs manquantes, incohérentes ou en double.

provenance des données

Le processus de suivi de l'origine et de l'historique des données tout au long de leur cycle de vie, par exemple la manière dont les données ont été générées, transmises et stockées.

sujet des données

Personne dont les données sont collectées et traitées.

entrepôt des données

Un système de gestion des données qui prend en charge les informations commerciales, telles que les analyses. Les entrepôts de données contiennent généralement de grandes quantités de données historiques et sont généralement utilisés pour les requêtes et les analyses.

langage de définition de base de données (DDL)

Instructions ou commandes permettant de créer ou de modifier la structure des tables et des objets dans une base de données.

langage de manipulation de base de données (DML)

Instructions ou commandes permettant de modifier (insérer, mettre à jour et supprimer) des informations dans une base de données.

DDL

Voir langage de définition de base de données.

ensemble profond

Sert à combiner plusieurs modèles de deep learning à des fins de prédiction. Vous pouvez utiliser des ensembles profonds pour obtenir une prévision plus précise ou pour estimer l'incertitude des prédictions.

deep learning

Un sous-champ de ML qui utilise plusieurs couches de réseaux neuronaux artificiels pour identifier le mappage entre les données d'entrée et les variables cibles d'intérêt.

defense-in-depth

Approche de la sécurité de l'information dans laquelle une série de mécanismes et de contrôles de sécurité sont judicieusement répartis sur l'ensemble d'un réseau informatique afin de protéger la confidentialité, l'intégrité et la disponibilité du réseau et des données qu'il contient. Lorsque vous adoptez cette stratégie AWS, vous ajoutez plusieurs contrôles à différentes couches de

la AWS Organizations structure afin de sécuriser les ressources. Par exemple, une defense-in-depth approche peut combiner l'authentification multifactorielle, la segmentation du réseau et le chiffrement.

administrateur délégué

Dans AWS Organizations, un service compatible peut enregistrer un compte AWS membre pour administrer les comptes de l'organisation et gérer les autorisations pour ce service. Ce compte est appelé administrateur délégué pour ce service. Pour plus d'informations et une liste des services compatibles, veuillez consulter la rubrique Services qui fonctionnent avec AWS Organizations dans la documentation AWS Organizations .

déploiement

Processus de mise à disposition d'une application, de nouvelles fonctionnalités ou de corrections de code dans l'environnement cible. Le déploiement implique la mise en œuvre de modifications dans une base de code, puis la génération et l'exécution de cette base de code dans les environnements de l'application.

environnement de développement

Voir environnement.

contrôle de détection

Contrôle de sécurité conçu pour détecter, journaliser et alerter après la survenue d'un événement. Ces contrôles constituent une deuxième ligne de défense et vous alertent en cas d'événements de sécurité qui ont contourné les contrôles préventifs en place. Pour plus d'informations, veuillez consulter la rubrique Contrôles de détection dans Implementing security controls on AWS.

cartographie de la chaîne de valeur du développement (DVSM)

Processus utilisé pour identifier et hiérarchiser les contraintes qui nuisent à la rapidité et à la qualité du cycle de vie du développement logiciel. DVSM étend le processus de cartographie de la chaîne de valeur initialement conçu pour les pratiques de production allégée. Il met l'accent sur les étapes et les équipes nécessaires pour créer et transférer de la valeur tout au long du processus de développement logiciel.

jumeau numérique

Représentation virtuelle d'un système réel, tel qu'un bâtiment, une usine, un équipement industriel ou une ligne de production. Les jumeaux numériques prennent en charge la maintenance prédictive, la surveillance à distance et l'optimisation de la production.

tableau des dimensions

Dans un schéma en étoile, table plus petite contenant les attributs de données relatifs aux données quantitatives d'une table de faits. Les attributs des tables de dimensions sont généralement des champs de texte ou des nombres discrets qui se comportent comme du texte. Ces attributs sont couramment utilisés pour la contrainte des requêtes, le filtrage et l'étiquetage des ensembles de résultats.

catastrophe

Un événement qui empêche une charge de travail ou un système d'atteindre ses objectifs commerciaux sur son site de déploiement principal. Ces événements peuvent être des catastrophes naturelles, des défaillances techniques ou le résultat d'actions humaines, telles qu'une mauvaise configuration involontaire ou une attaque de logiciel malveillant.

reprise après sinistre (DR)

La stratégie et le processus que vous utilisez pour minimiser les temps d'arrêt et les pertes de données causés par un sinistre. Pour plus d'informations, consultez Disaster Recovery of Workloads on AWS : Recovery in the Cloud in the AWS Well-Architected Framework.

DML

Voir langage de manipulation de base de données.

conception axée sur le domaine

Approche visant à développer un système logiciel complexe en connectant ses composants à des domaines évolutifs, ou objectifs métier essentiels, que sert chaque composant. Ce concept a été introduit par Eric Evans dans son ouvrage Domain-Driven Design: Tackling Complexity in the Heart of Software (Boston : Addison-Wesley Professional, 2003). Pour plus d'informations sur l'utilisation du design piloté par domaine avec le modèle de figuier étrangleur, veuillez consulter Modernizing legacy Microsoft ASP.NET (ASMX) web services incrementally by using containers and Amazon API Gateway.

DR

Voir reprise après sinistre.

détection de dérive

Suivi des écarts par rapport à une configuration de référence. Par exemple, vous pouvez l'utiliser AWS CloudFormation pour détecter la dérive des ressources du système ou AWS Control Tower

pour détecter les modifications de votre zone d'atterrissage susceptibles d'affecter le respect des exigences de gouvernance.

DVSM

Voir la cartographie de la chaîne de valeur du développement.

E

EDA

Voir analyse exploratoire des données.

EDI

Voir échange de données informatisé.

informatique de périphérie

Technologie qui augmente la puissance de calcul des appareils intelligents en périphérie d'un réseau IoT. Comparé au cloud computing, l'informatique de pointe peut réduire la latence des communications et améliorer le temps de réponse.

échange de données informatisé (EDI)

L'échange automatique de documents commerciaux entre les organisations. Pour plus d'informations, voir Qu'est-ce que l'échange de données informatisé ?

chiffrement

Processus informatique qui transforme des données en texte clair, lisibles par l'homme, en texte chiffré.

clé de chiffrement

Chaîne cryptographique de bits aléatoires générée par un algorithme cryptographique. La longueur des clés peut varier, et chaque clé est conçue pour être imprévisible et unique.

endianisme

Ordre selon lequel les octets sont stockés dans la mémoire de l'ordinateur. Les systèmes de poids fort stockent d'abord l'octet le plus significatif. Les systèmes de poids faible stockent d'abord l'octet le moins significatif.

point de terminaison

Voir point de terminaison de service.

service de point de terminaison

Service que vous pouvez héberger sur un cloud privé virtuel (VPC) pour le partager avec d'autres utilisateurs. Vous pouvez créer un service de point de terminaison avec AWS PrivateLink et accorder des autorisations à d'autres Comptes AWS ou à Gestion des identités et des accès AWS (IAM) principaux. Ces comptes ou principaux peuvent se connecter à votre service de point de terminaison de manière privée en créant des points de terminaison d'un VPC d'interface. Pour plus d'informations, veuillez consulter Création d'un service de point de terminaison dans la documentation Amazon Virtual Private Cloud (Amazon VPC).

planification des ressources d'entreprise (ERP)

Système qui automatise et gère les principaux processus métier (tels que la comptabilité, le MES et la gestion de projet) pour une entreprise.

chiffrement d'enveloppe

Processus de chiffrement d'une clé de chiffrement à l'aide d'une autre clé de chiffrement. Pour plus d'informations, consultez la section Chiffrement des enveloppes dans la documentation AWS Key Management Service (AWS KMS).

environment

Instance d'une application en cours d'exécution. Les types d'environnement les plus courants dans le cloud computing sont les suivants :

- Environnement de développement : instance d'une application en cours d'exécution à laquelle seule l'équipe principale chargée de la maintenance de l'application peut accéder. Les environnements de développement sont utilisés pour tester les modifications avant de les promouvoir dans les environnements supérieurs. Ce type d'environnement est parfois appelé environnement de test.
- Environnements inférieurs : tous les environnements de développement d'une application, tels que ceux utilisés pour les générations et les tests initiaux.
- Environnement de production : instance d'une application en cours d'exécution à laquelle les utilisateurs finaux peuvent accéder. Dans un CI/CD pipeline, l'environnement de production est le dernier environnement de déploiement.
- Environnements supérieurs : tous les environnements accessibles aux utilisateurs autres que l'équipe de développement principale. Ils peuvent inclure un environnement de production, des

environnements de préproduction et des environnements pour les tests d'acceptation par les utilisateurs.

époppée

Dans les méthodologies agiles, catégories fonctionnelles qui aident à organiser et à prioriser votre travail. Les épopées fournissent une description détaillée des exigences et des tâches d'implémentation. Par exemple, les points forts de la AWS CAF en matière de sécurité incluent la gestion des identités et des accès, les contrôles de détection, la sécurité des infrastructures, la protection des données et la réponse aux incidents. Pour plus d'informations sur les épopées dans la stratégie de migration AWS , veuillez consulter le guide d'implémentation du programme.

ERP

Voir Planification des ressources d'entreprise.

analyse exploratoire des données (EDA)

Processus d'analyse d'un jeu de données pour comprendre ses principales caractéristiques. Vous collectez ou agrégez des données, puis vous effectuez des enquêtes initiales pour trouver des modèles, détecter des anomalies et vérifier les hypothèses. L'EDA est réalisée en calculant des statistiques récapitulatives et en créant des visualisations de données.

F

tableau des faits

La table centrale dans un schéma en étoile. Il stocke des données quantitatives sur les opérations commerciales. Généralement, une table de faits contient deux types de colonnes : celles qui contiennent des mesures et celles qui contiennent une clé étrangère pour une table de dimensions.

échouer rapidement

Une philosophie qui utilise des tests fréquents et progressifs pour réduire le cycle de vie du développement. C'est un élément essentiel d'une approche agile.

limite d'isolation des défauts

Dans le AWS Cloud, une limite telle qu'une zone de disponibilité Région AWS, un plan de contrôle ou un plan de données qui limite l'effet d'une panne et contribue à améliorer la résilience des

charges de travail. Pour plus d'informations, consultez la section Limites d'isolation des AWS pannes.

branche de fonctionnalités

Voir succursale.

fonctionnalités

Les données d'entrée que vous utilisez pour faire une prédiction. Par exemple, dans un contexte de fabrication, les fonctionnalités peuvent être des images capturées périodiquement à partir de la ligne de fabrication.

importance des fonctionnalités

Le niveau d'importance d'une fonctionnalité pour les prédictions d'un modèle. Il s'exprime généralement sous la forme d'un score numérique qui peut être calculé à l'aide de différentes techniques, telles que la méthode Shapley Additive Explanations (SHAP) et les gradients intégrés. Pour plus d'informations, voir Interprétabilité du modèle d'apprentissage automatique avec AWS.

transformation de fonctionnalité

Optimiser les données pour le processus de ML, notamment en enrichissant les données avec des sources supplémentaires, en mettant à l'échelle les valeurs ou en extrayant plusieurs ensembles d'informations à partir d'un seul champ de données. Cela permet au modèle de ML de tirer parti des données. Par exemple, si vous décomposez la date « 2021-05-27 00:15:37 » en « 2021 », « mai », « jeudi » et « 15 », vous pouvez aider l'algorithme d'apprentissage à apprendre des modèles nuancés associés à différents composants de données.

invitation en quelques coups

Fournir à un LLM un petit nombre d'exemples illustrant la tâche et le résultat souhaité avant de lui demander d'effectuer une tâche similaire. Cette technique est une application de l'apprentissage contextuel, dans le cadre de laquelle les modèles apprennent à partir d'exemples (prises de vue) intégrés dans des instructions. Les instructions en quelques étapes peuvent être efficaces pour les tâches qui nécessitent un formatage, un raisonnement ou des connaissances de domaine spécifiques. Voir également l'invite Zero-Shot.

FGAC

Découvrez le contrôle d'accès détaillé.

contrôle d'accès détaillé (FGAC)

Utilisation de plusieurs conditions pour autoriser ou refuser une demande d'accès.

migration instantanée (flash-cut)

Méthode de migration de base de données qui utilise la réplication continue des données par le biais de la capture des données de modification afin de migrer les données dans les plus brefs délais, au lieu d'utiliser une approche progressive. L'objectif est de réduire au maximum les temps d'arrêt.

FM

Voir le modèle de fondation.

modèle de fondation (FM)

Un vaste réseau neuronal d'apprentissage profond qui s'est entraîné sur d'énormes ensembles de données généralisées et non étiquetées. FMs sont capables d'effectuer une grande variété de tâches générales, telles que comprendre le langage, générer du texte et des images et converser en langage naturel. Pour plus d'informations, voir Que sont les modèles de base ?

G

IA générative

Sous-ensemble de modèles d'IA qui ont été entraînés sur de grandes quantités de données et qui peuvent utiliser une simple invite textuelle pour créer de nouveaux contenus et artefacts, tels que des images, des vidéos, du texte et du son. Pour plus d'informations, consultez Qu'est-ce que l'IA générative.

blocage géographique

Voir les restrictions géographiques.

restrictions géographiques (blocage géographique)

Sur Amazon CloudFront, option permettant d'empêcher les utilisateurs de certains pays d'accéder aux distributions de contenu. Vous pouvez utiliser une liste d'autorisation ou une liste de blocage pour spécifier les pays approuvés et interdits. Pour plus d'informations, consultez la section Restreindre la distribution géographique de votre contenu dans la CloudFront documentation.

Flux de travail Gitflow

Approche dans laquelle les environnements inférieurs et supérieurs utilisent différentes branches dans un référentiel de code source. Le flux de travail Gitflow est considéré comme existant, et le flux de travail basé sur les troncs est l'approche moderne préférée.

image dorée

Un instantané d'un système ou d'un logiciel utilisé comme modèle pour déployer de nouvelles instances de ce système ou logiciel. Par exemple, dans le secteur de la fabrication, une image dorée peut être utilisée pour fournir des logiciels sur plusieurs appareils et contribue à améliorer la vitesse, l'évolutivité et la productivité des opérations de fabrication des appareils.

stratégie inédite

L'absence d'infrastructures existantes dans un nouvel environnement. Lorsque vous adoptez une stratégie inédite pour une architecture système, vous pouvez sélectionner toutes les nouvelles technologies sans restriction de compatibilité avec l'infrastructure existante, également appelée brownfield. Si vous étendez l'infrastructure existante, vous pouvez combiner des politiques brownfield (existantes) et greenfield (inédites).

barrière de protection

Règle de haut niveau qui permet de régir les ressources, les politiques et la conformité au sein des unités organisationnelles (OUs). Les barrières de protection préventives appliquent des politiques pour garantir l'alignement sur les normes de conformité. Elles sont mises en œuvre à l'aide de politiques de contrôle des services et de limites des autorisations IAM. Les barrières de protection de détection détectent les violations des politiques et les problèmes de conformité, et génèrent des alertes pour y remédier. Ils sont implémentés à l'aide d'Amazon AWS Config AWS Security Hub CSPM GuardDuty AWS Trusted Advisor, d'Amazon Inspector et de AWS Lambda contrôles personnalisés.

H

HA

Découvrez la haute disponibilité.

migration de base de données hétérogène

Migration de votre base de données source vers une base de données cible qui utilise un moteur de base de données différent (par exemple, Oracle vers Amazon Aurora). La migration hétérogène fait généralement partie d'un effort de réarchitecture, et la conversion du schéma peut s'avérer une tâche complexe. AWS propose AWS SCT qui facilite les conversions de schémas.

haute disponibilité (HA)

Capacité d'une charge de travail à fonctionner en continu, sans intervention, en cas de difficultés ou de catastrophes. Les systèmes HA sont conçus pour basculer automatiquement, fournir constamment des performances de haute qualité et gérer différentes charges et défaillances avec un impact minimal sur les performances.

modernisation des historiens

Approche utilisée pour moderniser et mettre à niveau les systèmes de technologie opérationnelle (OT) afin de mieux répondre aux besoins de l'industrie manufacturière. Un historien est un type de base de données utilisé pour collecter et stocker des données provenant de diverses sources dans une usine.

données de rétention

Partie de données historiques étiquetées qui n'est pas divulguée dans un ensemble de données utilisé pour entraîner un modèle d'apprentissage automatique. Vous pouvez utiliser les données de blocage pour évaluer les performances du modèle en comparant les prévisions du modèle aux données de blocage.

migration de base de données homogène

Migration de votre base de données source vers une base de données cible qui partage le même moteur de base de données (par exemple, Microsoft SQL Server vers Amazon RDS for SQL Server). La migration homogène s'inscrit généralement dans le cadre d'un effort de réhébergement ou de replateforme. Vous pouvez utiliser les utilitaires de base de données natifs pour migrer le schéma.

données chaudes

Données fréquemment consultées, telles que les données en temps réel ou les données translationnelles récentes. Ces données nécessitent généralement un niveau ou une classe de stockage à hautes performances pour fournir des réponses rapides aux requêtes.

correctif

Solution d'urgence à un problème critique dans un environnement de production. En raison de son urgence, un correctif est généralement créé en dehors du flux de travail de DevOps publication habituel.

période de soins intensifs

Immédiatement après le basculement, période pendant laquelle une équipe de migration gère et surveille les applications migrées dans le cloud afin de résoudre les problèmes éventuels. En règle générale, cette période dure de 1 à 4 jours. À la fin de la période de soins intensifs, l'équipe de migration transfère généralement la responsabilité des applications à l'équipe des opérations cloud.

I

IaC

Considérez l'infrastructure comme un code.

politique basée sur l’identité

Politique attachée à un ou plusieurs principaux IAM qui définit leurs autorisations au sein de l' AWS Cloud environnement.

application inactive

Application dont l'utilisation moyenne du processeur et de la mémoire se situe entre 5 et 20 % sur une période de 90 jours. Dans un projet de migration, il est courant de retirer ces applications ou de les retenir sur site.

IIo T

Voir Internet industriel des objets.

infrastructure immuable

Modèle qui déploie une nouvelle infrastructure pour les charges de travail de production au lieu de mettre à jour, d'appliquer des correctifs ou de modifier l'infrastructure existante. Les infrastructures immuables sont intrinsèquement plus cohérentes, fiables et prévisibles que les infrastructures mutables. Pour plus d'informations, consultez les meilleures pratiques de déploiement à l'aide d'une infrastructure immuable dans le AWS Well-Architected Framework.

VPC entrant (d'entrée)

Dans une architecture AWS multi-comptes, un VPC qui accepte, inspecte et achemine les connexions réseau depuis l'extérieur d'une application. L'architecture AWS de référence de sécurité recommande de configurer votre compte réseau avec les fonctions entrantes, sortantes

et d'inspection VPCs afin de protéger l'interface bidirectionnelle entre votre application et l'Internet en général.

migration incrémentielle

Stratégie de basculement dans le cadre de laquelle vous migrez votre application par petites parties au lieu d'effectuer un basculement complet unique. Par exemple, il se peut que vous ne transfériez que quelques microservices ou utilisateurs vers le nouveau système dans un premier temps. Après avoir vérifié que tout fonctionne correctement, vous pouvez transférer progressivement des microservices ou des utilisateurs supplémentaires jusqu'à ce que vous puissiez mettre hors service votre système hérité. Cette stratégie réduit les risques associés aux migrations de grande ampleur.

Industry 4.0

Terme introduit par Klaus Schwab en 2016 pour désigner la modernisation des processus de fabrication grâce aux avancées en matière de connectivité, de données en temps réel, d'automatisation, d'analyse et d'IA/ML.

infrastructure

Ensemble des ressources et des actifs contenus dans l'environnement d'une application.

infrastructure en tant que code (IaC)

Processus de mise en service et de gestion de l'infrastructure d'une application via un ensemble de fichiers de configuration. IaC est conçue pour vous aider à centraliser la gestion de l'infrastructure, à normaliser les ressources et à mettre à l'échelle rapidement afin que les nouveaux environnements soient reproductibles, fiables et cohérents.

Internet industriel des objets (IIoT)

L'utilisation de capteurs et d'appareils connectés à Internet dans les secteurs industriels tels que la fabrication, l'énergie, l'automobile, les soins de santé, les sciences de la vie et l'agriculture. Pour plus d'informations, voir Élaboration d'une stratégie de transformation numérique de l'Internet des objets (IIoT) industriel.

VPC d'inspection

Dans une architecture AWS multi-comptes, un VPC centralisé qui gère les inspections du trafic réseau VPCs entre (identique ou Régions AWS différent), Internet et les réseaux locaux. L'architecture AWS de référence de sécurité recommande de configurer votre compte réseau

avec les fonctions entrantes, sortantes et d'inspection VPCs afin de protéger l'interface bidirectionnelle entre votre application et l'Internet en général.

Internet des objets (IoT)

Réseau d'objets physiques connectés dotés de capteurs ou de processeurs intégrés qui communiquent avec d'autres appareils et systèmes via Internet ou via un réseau de communication local. Pour plus d'informations, veuillez consulter la section Qu'est-ce que l'IoT ?.

interprétabilité

Caractéristique d'un modèle de machine learning qui décrit dans quelle mesure un être humain peut comprendre comment les prédictions du modèle dépendent de ses entrées. Pour plus d'informations, voir Interprétabilité du modèle d'apprentissage automatique avec AWS.

IoT

Voir Internet des objets.

Bibliothèque d'informations informatiques (ITIL)

Ensemble de bonnes pratiques pour proposer des services informatiques et les aligner sur les exigences métier. L'ITIL constitue la base de l'ITSM.

gestion des services informatiques (ITSM)

Activités associées à la conception, à la mise en œuvre, à la gestion et à la prise en charge de services informatiques d'une organisation. Pour plus d'informations sur l'intégration des opérations cloud aux outils ITSM, veuillez consulter le guide d'intégration des opérations.

ITIL

Consultez la bibliothèque d'informations informatiques.

ITSM

Voir Gestion des services informatiques.

L

contrôle d'accès basé sur des étiquettes (LBAC)

Une implémentation du contrôle d'accès obligatoire (MAC) dans laquelle une valeur d'étiquette de sécurité est explicitement attribuée aux utilisateurs et aux données elles-mêmes. L'intersection

entre l'étiquette de sécurité utilisateur et l'étiquette de sécurité des données détermine les lignes et les colonnes visibles par l'utilisateur.

zone de destination

Une zone d'atterrissage est un AWS environnement multi-comptes bien conçu, évolutif et sécurisé. Il s'agit d'un point de départ à partir duquel vos entreprises peuvent rapidement lancer et déployer des charges de travail et des applications en toute confiance dans leur environnement de sécurité et d'infrastructure. Pour plus d'informations sur les zones de destination, veuillez consulter Setting up a secure and scalable multi-account AWS environment.

grand modèle de langage (LLM)

Un modèle d'intelligence artificielle basé sur le deep learning qui est préentraîné sur une grande quantité de données. Un LLM peut effectuer plusieurs tâches, telles que répondre à des questions, résumer des documents, traduire du texte dans d'autres langues et compléter des phrases. Pour plus d'informations, voir Que sont LLMs.

migration de grande envergure

Migration de 300 serveurs ou plus.

LBAC

Voir contrôle d'accès basé sur des étiquettes.

principe de moindre privilège

Bonne pratique de sécurité qui consiste à accorder les autorisations minimales nécessaires à l'exécution d'une tâche. Pour plus d'informations, veuillez consulter la rubrique Accorder les autorisations de moindre privilège dans la documentation IAM.

lift and shift

Voir 7 Rs.

système de poids faible

Système qui stocke d'abord l'octet le moins significatif. Voir aussi endianité.

LLM

Voir le grand modèle de langage.

environnements inférieurs

Voir environnement.

M

machine learning (ML)

Type d'intelligence artificielle qui utilise des algorithmes et des techniques pour la reconnaissance et l'apprentissage de modèles. Le ML analyse et apprend à partir de données enregistrées, telles que les données de l'Internet des objets (IoT), pour générer un modèle statistique basé sur des modèles. Pour plus d'informations, veuillez consulter Machine Learning.

branche principale

Voir succursale.

malware

Logiciel conçu pour compromettre la sécurité ou la confidentialité de l'ordinateur. Les logiciels malveillants peuvent perturber les systèmes informatiques, divulguer des informations sensibles ou obtenir un accès non autorisé. Parmi les malwares, on peut citer les virus, les vers, les rançongiciels, les chevaux de Troie, les logiciels espions et les enregistreurs de frappe.

services gérés

Services AWS pour lequel AWS fonctionnent la couche d'infrastructure, le système d'exploitation et les plateformes, et vous accédez aux points de terminaison pour stocker et récupérer des données. Amazon Simple Storage Service (Amazon S3) et Amazon DynamoDB sont des exemples de services gérés. Ils sont également connus sous le nom de services abstraits.

système d'exécution de la fabrication (MES)

Un système logiciel pour le suivi, la surveillance, la documentation et le contrôle des processus de production qui convertissent les matières premières en produits finis dans l'atelier.

MAP

Voir Migration Acceleration Program.

mécanisme

Processus complet au cours duquel vous créez un outil, favorisez son adoption, puis inspectez les résultats afin de procéder aux ajustements nécessaires. Un mécanisme est un cycle qui se renforce et s'améliore lorsqu'il fonctionne. Pour plus d'informations, voir Création de mécanismes dans le cadre AWS Well-Architected.

compte membre

Tous, à l' Comptes AWS exception du compte de gestion, qui font partie d'une organisation dans AWS Organizations. Un compte ne peut être membre que d'une seule organisation à la fois.

MAILLES

Voir le système d'exécution de la fabrication.

Transport télémétrique en file d'attente de messages (MQTT)

Protocole de communication léger machine-to-machine (M2M), basé sur le modèle de publication/d'abonnement, pour les appareils IoT aux ressources limitées.

microservice

Un petit service indépendant qui communique via un réseau bien défini APIs et qui est généralement détenu par de petites équipes autonomes. Par exemple, un système d'assurance peut inclure des microservices qui mappent à des capacités métier, telles que les ventes ou le marketing, ou à des sous-domaines, tels que les achats, les réclamations ou l'analytique. Les avantages des microservices incluent l'agilité, la flexibilité de la mise à l'échelle, la facilité de déploiement, la réutilisation du code et la résilience. Pour plus d'informations, consultez la section Intégration de microservices à l'aide de services AWS sans serveur.

architecture de microservices

Approche de création d'une application avec des composants indépendants qui exécutent chaque processus d'application en tant que microservice. Ces microservices communiquent via une interface bien définie en utilisant Lightweight. APIs Chaque microservice de cette architecture peut être mis à jour, déployé et mis à l'échelle pour répondre à la demande de fonctions spécifiques d'une application. Pour plus d'informations, consultez la section Implémentation de microservices sur AWS.

Programme d'accélération des migrations (MAP)

Un AWS programme qui fournit un support de conseil, des formations et des services pour aider les entreprises à établir une base opérationnelle solide pour passer au cloud, et pour aider à compenser le coût initial des migrations. MAP inclut une méthodologie de migration pour exécuter les migrations héritées de manière méthodique, ainsi qu'un ensemble d'outils pour automatiser et accélérer les scénarios de migration courants.

migration à grande échelle

Processus consistant à transférer la majeure partie du portefeuille d'applications vers le cloud par vagues, un plus grand nombre d'applications étant déplacées plus rapidement à chaque vague. Cette phase utilise les bonnes pratiques et les enseignements tirés des phases précédentes pour implémenter une usine de migration d'équipes, d'outils et de processus en vue de rationaliser la migration des charges de travail grâce à l'automatisation et à la livraison agile. Il s'agit de la troisième phase de la stratégie de migration AWS.

usine de migration

Équipes interfonctionnelles qui rationalisent la migration des charges de travail grâce à des approches automatisées et agiles. Les équipes de Migration Factory comprennent généralement des responsables des opérations, des analystes commerciaux et des propriétaires, des ingénieurs de migration, des développeurs et DevOps des professionnels travaillant dans le cadre de sprints. Entre 20 et 50 % du portefeuille d'applications d'entreprise est constitué de modèles répétés qui peuvent être optimisés par une approche d'usine. Pour plus d'informations, veuillez consulter la rubrique discussion of migration factories et le guide Cloud Migration Factory dans cet ensemble de contenus.

métadonnées de migration

Informations relatives à l'application et au serveur nécessaires pour finaliser la migration. Chaque modèle de migration nécessite un ensemble de métadonnées de migration différent. Les exemples de métadonnées de migration incluent le sous-réseau cible, le groupe de sécurité et le AWS compte.

modèle de migration

Tâche de migration reproductible qui détaille la stratégie de migration, la destination de la migration et l'application ou le service de migration utilisé. Exemple : réorganisez la migration vers Amazon EC2 AWS avec le service de migration d'applications.

Évaluation du portefeuille de migration (MPA)

Outil en ligne qui fournit des informations pour valider l'analyse de rentabilisation en faveur de la migration vers le. AWS Cloud La MPA propose une évaluation détaillée du portefeuille (dimensionnement approprié des serveurs, tarification, comparaison du coût total de possession, analyse des coûts de migration), ainsi que la planification de la migration (analyse et collecte des données d'applications, regroupement des applications, priorisation des migrations et planification des vagues). L'outil MPA (connexion requise) est disponible gratuitement pour tous les AWS consultants et consultants APN Partner.

Évaluation de la préparation à la migration (MRA)

Processus qui consiste à obtenir des informations sur l'état de préparation d'une organisation au cloud, à identifier les forces et les faiblesses et à élaborer un plan d'action pour combler les lacunes identifiées, à l'aide du AWS CAF. Pour plus d'informations, veuillez consulter le guide de préparation à la migration. La MRA est la première phase de la stratégie de migration AWS.

stratégie de migration

L'approche utilisée pour migrer une charge de travail vers le AWS Cloud. Pour plus d'informations, reportez-vous aux 7 R de ce glossaire et à Mobiliser votre organisation pour accélérer les migrations à grande échelle.

ML

Voir apprentissage automatique.

modernisation

Transformation d'une application obsolète (héritée ou monolithique) et de son infrastructure en un système agile, élastique et hautement disponible dans le cloud afin de réduire les coûts, de gagner en efficacité et de tirer parti des innovations. Pour plus d'informations, consultez la section Stratégie de modernisation des applications dans le AWS Cloud.

évaluation de la préparation à la modernisation

Évaluation qui permet de déterminer si les applications d'une organisation sont prêtes à être modernisées, d'identifier les avantages, les risques et les dépendances, et qui détermine dans quelle mesure l'organisation peut prendre en charge l'état futur de ces applications. Le résultat de l'évaluation est un plan de l'architecture cible, une feuille de route détaillant les phases de développement et les étapes du processus de modernisation, ainsi qu'un plan d'action pour combler les lacunes identifiées. Pour plus d'informations, consultez la section Évaluation de l'état de préparation à la modernisation des applications dans le AWS Cloud.

applications monolithiques (monolithes)

Applications qui s'exécutent en tant que service unique avec des processus étroitement couplés. Les applications monolithiques ont plusieurs inconvénients. Si une fonctionnalité de l'application connaît un pic de demande, l'architecture entière doit être mise à l'échelle. L'ajout ou l'amélioration des fonctionnalités d'une application monolithique devient également plus complexe lorsque la base de code s'élargit. Pour résoudre ces problèmes, vous pouvez utiliser une architecture de microservices. Pour plus d'informations, veuillez consulter Decomposing monoliths into microservices.

MPA

Voir Évaluation du portefeuille de migration.

MQTT

Voir Message Queuing Telemetry Transport.

classification multi-classes

Processus qui permet de générer des prédictions pour plusieurs classes (prédiction d'un résultat parmi plus de deux). Par exemple, un modèle de ML peut demander « Ce produit est-il un livre, une voiture ou un téléphone ? » ou « Quelle catégorie de produits intéresse le plus ce client ? ».

infrastructure mutable

Modèle qui met à jour et modifie l'infrastructure existante pour les charges de travail de production. Pour améliorer la cohérence, la fiabilité et la prévisibilité, le AWS Well-Architected Framework recommande l'utilisation d'une infrastructure immuable comme meilleure pratique.

O

OAC

Voir Contrôle d'accès à l'origine.

OAI

Voir l'identité d'accès à l'origine.

OCM

Voir gestion du changement organisationnel.

migration hors ligne

Méthode de migration dans laquelle la charge de travail source est supprimée au cours du processus de migration. Cette méthode implique un temps d'arrêt prolongé et est généralement utilisée pour de petites charges de travail non critiques.

OI

Consultez la section Intégration des opérations.

OLA

Voir l'accord au niveau opérationnel.

migration en ligne

Méthode de migration dans laquelle la charge de travail source est copiée sur le système cible sans être mise hors ligne. Les applications connectées à la charge de travail peuvent continuer à fonctionner pendant la migration. Cette méthode implique un temps d'arrêt nul ou minimal et est généralement utilisée pour les charges de travail de production critiques.

OPC-UA

Voir Open Process Communications - Architecture unifiée.

Communications par processus ouvert - Architecture unifiée (OPC-UA)

Un protocole de communication machine-to-machine (M2M) pour l'automatisation industrielle. L'OPC-UA fournit une norme d'interopérabilité avec des schémas de cryptage, d'authentification et d'autorisation des données.

accord au niveau opérationnel (OLA)

Accord qui précise ce que les groupes informatiques fonctionnels s'engagent à fournir les uns aux autres, afin de prendre en charge un contrat de niveau de service (SLA).

examen de l'état de préparation opérationnelle (ORR)

Une liste de questions et de bonnes pratiques associées qui vous aident à comprendre, à évaluer, à prévenir ou à réduire l'ampleur des incidents et des défaillances possibles. Pour plus d'informations, voir Operational Readiness Reviews (ORR) dans le AWS Well-Architected Framework.

technologie opérationnelle (OT)

Systèmes matériels et logiciels qui fonctionnent avec l'environnement physique pour contrôler les opérations, les équipements et les infrastructures industriels. Dans le secteur manufacturier, l'intégration des systèmes OT et des technologies de l'information (IT) est au cœur des transformations de l'industrie 4.0.

intégration des opérations (OI)

Processus de modernisation des opérations dans le cloud, qui implique la planification de la préparation, l'automatisation et l'intégration. Pour en savoir plus, veuillez consulter le guide d'intégration des opérations.

journal de suivi d'organisation

Un parcours créé par AWS CloudTrail qui enregistre tous les événements pour tous les membres Comptes AWS d'une organisation dans AWS Organizations. Ce journal de suivi est créé dans chaque Compte AWS qui fait partie de l'organisation et suit l'activité de chaque compte. Pour plus d'informations, consultez la section Création d'un suivi pour une organisation dans la CloudTrail documentation.

gestion du changement organisationnel (OCM)

Cadre pour gérer les transformations métier majeures et perturbatrices du point de vue des personnes, de la culture et du leadership. L'OCM aide les organisations à se préparer et à effectuer la transition vers de nouveaux systèmes et de nouvelles politiques en accélérant l'adoption des changements, en abordant les problèmes de transition et en favorisant des changements culturels et organisationnels. Dans la stratégie de AWS migration, ce cadre est appelé accélération du personnel, en raison de la rapidité du changement requise dans les projets d'adoption du cloud. Pour plus d'informations, veuillez consulter le guide OCM.

contrôle d'accès d'origine (OAC)

Dans CloudFront, une option améliorée pour restreindre l'accès afin de sécuriser votre contenu Amazon Simple Storage Service (Amazon S3). L'OAC prend en charge tous les compartiments S3 dans leur ensemble Régions AWS, le chiffrement côté serveur avec AWS KMS (SSE-KMS) et les requêtes dynamiques `PUT` adressées au compartiment S3. `DELETE`

identité d'accès d'origine (OAI)

Dans CloudFront, une option permettant de restreindre l'accès afin de sécuriser votre contenu Amazon S3. Lorsque vous utilisez OAI, il CloudFront crée un principal auprès duquel Amazon S3 peut s'authentifier. Les principaux authentifiés peuvent accéder au contenu d'un compartiment S3 uniquement via une distribution spécifique CloudFront . Voir également OAC, qui fournit un contrôle d'accès plus précis et amélioré.

ORR

Voir l'examen de l'état de préparation opérationnelle.

DE

Voir technologie opérationnelle.

VPC sortant (de sortie)

Dans une architecture AWS multi-comptes, un VPC qui gère les connexions réseau initiées depuis une application. L'architecture AWS de référence de sécurité recommande de configurer votre compte réseau avec les fonctions entrantes, sortantes et d'inspection VPCs afin de protéger l'interface bidirectionnelle entre votre application et l'Internet en général.

P

limite des autorisations

Politique de gestion IAM attachée aux principaux IAM pour définir les autorisations maximales que peut avoir l'utilisateur ou le rôle. Pour plus d'informations, veuillez consulter la rubrique Limites des autorisations dans la documentation IAM.

informations personnelles identifiables (PII)

Informations qui, lorsqu'elles sont consultées directement ou associées à d'autres données connexes, peuvent être utilisées pour déduire raisonnablement l'identité d'une personne. Les exemples d'informations personnelles incluent les noms, les adresses et les informations de contact.

PII

Voir les informations personnelles identifiables.

manuel stratégique

Ensemble d'étapes prédéfinies qui capturent le travail associé aux migrations, comme la fourniture de fonctions d'opérations de base dans le cloud. Un manuel stratégique peut revêtir la forme de scripts, de runbooks automatisés ou d'un résumé des processus ou des étapes nécessaires au fonctionnement de votre environnement modernisé.

PLC

Voir contrôleur logique programmable.

PLM

Consultez la section Gestion du cycle de vie des produits.

policy

Objet capable de définir les autorisations (voir la politique basée sur l'identité), de spécifier les conditions d'accès (voir la politique basée sur les ressources) ou de définir les autorisations maximales pour tous les comptes d'une organisation dans AWS Organizations (voir la politique de contrôle des services).

persistance polyglotte

Choix indépendant de la technologie de stockage de données d'un microservice en fonction des modèles d'accès aux données et d'autres exigences. Si vos microservices utilisent la même technologie de stockage de données, ils peuvent rencontrer des difficultés d'implémentation ou présenter des performances médiocres. Les microservices sont plus faciles à mettre en œuvre, atteignent de meilleures performances, ainsi qu'une meilleure capacité de mise à l'échelle s'ils utilisent l'entrepôt de données le mieux adapté à leurs besoins.

évaluation du portefeuille

Processus de découverte, d'analyse et de priorisation du portefeuille d'applications afin de planifier la migration. Pour plus d'informations, veuillez consulter Evaluating migration readiness.

predicate

Une condition de requête qui renvoie `true` ou`false`, généralement située dans une `WHERE` clause.

prédicat pushdown

Technique d'optimisation des requêtes de base de données qui filtre les données de la requête avant le transfert. Cela réduit la quantité de données qui doivent être extraites et traitées à partir de la base de données relationnelle et améliore les performances des requêtes.

contrôle préventif

Contrôle de sécurité conçu pour empêcher qu'un événement ne se produise. Ces contrôles constituent une première ligne de défense pour empêcher tout accès non autorisé ou toute modification indésirable de votre réseau. Pour plus d'informations, veuillez consulter Preventative controls dans Implementing security controls on AWS.

principal

Entité AWS capable d'effectuer des actions et d'accéder aux ressources. Cette entité est généralement un utilisateur root pour un Compte AWS rôle IAM ou un utilisateur. Pour plus

d'informations, veuillez consulter la rubrique Principal dans Termes et concepts relatifs aux rôles, dans la documentation IAM.

confidentialité dès la conception

Une approche d'ingénierie système qui prend en compte la confidentialité tout au long du processus de développement.

zones hébergées privées

Conteneur contenant des informations sur la manière dont vous souhaitez qu'Amazon Route 53 réponde aux requêtes DNS pour un domaine et ses sous-domaines au sein d'un ou de plusieurs VPCs domaines. Pour plus d'informations, veuillez consulter Working with private hosted zones dans la documentation Route 53.

contrôle proactif

Contrôle de sécurité conçu pour empêcher le déploiement de ressources non conformes. Ces contrôles analysent les ressources avant qu'elles ne soient provisionnées. Si la ressource n'est pas conforme au contrôle, elle n'est pas provisionnée. Pour plus d'informations, consultez le guide de référence sur les contrôles dans la AWS Control Tower documentation et consultez la section Contrôles proactifs dans Implémentation des contrôles de sécurité sur AWS.

gestion du cycle de vie des produits (PLM)

Gestion des données et des processus d'un produit tout au long de son cycle de vie, depuis la conception, le développement et le lancement, en passant par la croissance et la maturité, jusqu'au déclin et au retrait.

environnement de production

Voir environnement.

contrôleur logique programmable (PLC)

Dans le secteur manufacturier, un ordinateur hautement fiable et adaptable qui surveille les machines et automatise les processus de fabrication.

chaînage rapide

Utiliser le résultat d'une invite LLM comme entrée pour l'invite suivante afin de générer de meilleures réponses. Cette technique est utilisée pour décomposer une tâche complexe en sous-tâches ou pour affiner ou développer de manière itérative une réponse préliminaire. Cela permet d'améliorer la précision et la pertinence des réponses d'un modèle et permet d'obtenir des résultats plus précis et personnalisés.

pseudonymisation

Processus de remplacement des identifiants personnels dans un ensemble de données par des valeurs fictives. La pseudonymisation peut contribuer à protéger la vie privée. Les données pseudonymisées sont toujours considérées comme des données personnelles.

publish/subscribe (pub/sub)

Modèle qui permet les communications asynchrones entre les microservices afin d'améliorer l'évolutivité et la réactivité. Par exemple, dans un MES basé sur des microservices, un microservice peut publier des messages d'événements sur un canal auquel d'autres microservices peuvent s'abonner. Le système peut ajouter de nouveaux microservices sans modifier le service de publication.

Q

plan de requête

Série d'étapes, telles que des instructions, utilisées pour accéder aux données d'un système de base de données relationnelle SQL.

régression du plan de requêtes

Le cas où un optimiseur de service de base de données choisit un plan moins optimal qu'avant une modification donnée de l'environnement de base de données. Cela peut être dû à des changements en termes de statistiques, de contraintes, de paramètres d'environnement, de liaisons de paramètres de requêtes et de mises à jour du moteur de base de données.

R

Matrice RACI

Voir responsable, responsable, consulté, informé (RACI).

RAG

Voir Retrieval Augmented Generation.

rançongiciel

Logiciel malveillant conçu pour bloquer l'accès à un système informatique ou à des données jusqu'à ce qu'un paiement soit effectué.

Matrice RASCI

Voir responsable, responsable, consulté, informé (RACI).

RCAC

Voir contrôle d'accès aux lignes et aux colonnes.

réplica en lecture

Copie d'une base de données utilisée en lecture seule. Vous pouvez acheminer les requêtes vers le réplica de lecture pour réduire la charge sur votre base de données principale.

réarchitecte

Voir 7 Rs.

objectif de point de récupération (RPO)

Durée maximale acceptable depuis le dernier point de récupération des données. Il détermine ce qui est considéré comme étant une perte de données acceptable entre le dernier point de reprise et l'interruption du service.

objectif de temps de récupération (RTO)

Le délai maximum acceptable entre l'interruption du service et le rétablissement du service.

refactoriser

Voir 7 Rs.

Région

Un ensemble de AWS ressources dans une zone géographique. Chacun Région AWS est isolé et indépendant des autres pour garantir tolérance aux pannes, stabilité et résilience. Pour plus d'informations, voir Spécifier ce que Régions AWS votre compte peut utiliser.

régression

Technique de ML qui prédit une valeur numérique. Par exemple, pour résoudre le problème « Quel sera le prix de vente de cette maison ? », un modèle de ML pourrait utiliser un modèle de régression linéaire pour prédire le prix de vente d'une maison sur la base de faits connus à son sujet (par exemple, la superficie en mètres carrés).

réhéberger

Voir 7 Rs.

version

Dans un processus de déploiement, action visant à promouvoir les modifications apportées à un environnement de production.

déplacer

Voir 7 Rs.

replateforme

Voir 7 Rs.

rachat

Voir 7 Rs.

résilience

La capacité d'une application à résister aux perturbations ou à s'en remettre. La haute disponibilité et la reprise après sinistre sont des considérations courantes lors de la planification de la résilience dans le AWS Cloud. Pour plus d'informations, consultez AWS Cloud Résilience.

politique basée sur les ressources

Politique attachée à une ressource, comme un compartiment Amazon S3, un point de terminaison ou une clé de chiffrement. Ce type de politique précise les principaux auxquels l'accès est autorisé, les actions prises en charge et toutes les autres conditions qui doivent être remplies.

matrice responsable, redevable, consulté et informé (RACI)

Une matrice qui définit les rôles et les responsabilités de toutes les parties impliquées dans les activités de migration et les opérations cloud. Le nom de la matrice est dérivé des types de responsabilité définis dans la matrice : responsable (R), responsable (A), consulté (C) et informé (I). Le type de support (S) est facultatif. Si vous incluez le support, la matrice est appelée matrice RASCI, et si vous l'excluez, elle est appelée matrice RACI.

contrôle réactif

Contrôle de sécurité conçu pour permettre de remédier aux événements indésirables ou aux écarts par rapport à votre référence de sécurité. Pour plus d'informations, veuillez consulter la rubrique Responsive controls dans Implementing security controls on AWS.

retain

Voir 7 Rs.

se retirer

Voir 7 Rs.

Génération augmentée de récupération (RAG)

Technologie d'IA générative dans laquelle un LLM fait référence à une source de données faisant autorité qui se trouve en dehors de ses sources de données de formation avant de générer une réponse. Par exemple, un modèle RAG peut effectuer une recherche sémantique dans la base de connaissances ou dans les données personnalisées d'une organisation. Pour plus d'informations, voir Qu'est-ce que RAG ?

rotation

Processus de mise à jour périodique d'un secret pour empêcher un attaquant d'accéder aux informations d'identification.

contrôle d'accès aux lignes et aux colonnes (RCAC)

Utilisation d'expressions SQL simples et flexibles dotées de règles d'accès définies. Le RCAC comprend des autorisations de ligne et des masques de colonnes.

RPO

Voir l'objectif du point de récupération.

RTO

Voir l'objectif en matière de temps de rétablissement.

runbook

Ensemble de procédures manuelles ou automatisées nécessaires à l'exécution d'une tâche spécifique. Elles visent généralement à rationaliser les opérations ou les procédures répétitives présentant des taux d'erreur élevés.

S

SAML 2.0

Un standard ouvert utilisé par de nombreux fournisseurs d'identité (IdPs). Cette fonctionnalité permet l'authentification unique fédérée (SSO), afin que les utilisateurs puissent se connecter

AWS Management Console ou appeler les opérations de l' AWS API sans que vous ayez à créer un utilisateur dans IAM pour tous les membres de votre organisation. Pour plus d'informations sur la fédération SAML 2.0, veuillez consulter À propos de la fédération SAML 2.0 dans la documentation IAM.

SCADA

Voir Contrôle de supervision et acquisition de données.

SCP

Voir la politique de contrôle des services.

secret

Dans AWS Secrets Manager des informations confidentielles ou restreintes, telles qu'un mot de passe ou des informations d'identification utilisateur, que vous stockez sous forme cryptée. Il comprend la valeur secrète et ses métadonnées. La valeur secrète peut être binaire, une chaîne unique ou plusieurs chaînes. Pour plus d'informations, voir Que contient le secret d'un Secrets Manager ? dans la documentation de Secrets Manager.

sécurité dès la conception

Une approche d'ingénierie système qui prend en compte la sécurité tout au long du processus de développement.

contrôle de sécurité

Barrière de protection technique ou administrative qui empêche, détecte ou réduit la capacité d'un assaillant d'exploiter une vulnérabilité de sécurité. Il existe quatre principaux types de contrôles de sécurité : préventifs, détectifs, réactifs et proactifs.

renforcement de la sécurité

Processus qui consiste à réduire la surface d'attaque pour la rendre plus résistante aux attaques. Cela peut inclure des actions telles que la suppression de ressources qui ne sont plus requises, la mise en œuvre des bonnes pratiques de sécurité consistant à accorder le moindre privilège ou la désactivation de fonctionnalités inutiles dans les fichiers de configuration.

système de gestion des informations et des événements de sécurité (SIEM)

Outils et services qui associent les systèmes de gestion des informations de sécurité (SIM) et de gestion des événements de sécurité (SEM). Un système SIEM collecte, surveille et analyse les

données provenant de serveurs, de réseaux, d'appareils et d'autres sources afin de détecter les menaces et les failles de sécurité, mais aussi de générer des alertes.

automatisation des réponses de sécurité

Action prédéfinie et programmée conçue pour répondre automatiquement à un événement de sécurité ou y remédier. Ces automatisations servent de contrôles de sécurité détectifs ou réactifs qui vous aident à mettre en œuvre les meilleures pratiques en matière AWS de sécurité. Parmi les actions de réponse automatique, citons la modification d'un groupe de sécurité VPC, l'application de correctifs à une instance Amazon EC2 ou la rotation des informations d'identification.

chiffrement côté serveur

Chiffrement des données à destination, par celui Service AWS qui les reçoit.

Politique de contrôle des services (SCP)

Politique qui fournit un contrôle centralisé des autorisations pour tous les comptes d'une organisation dans AWS Organizations. SCPs définissez des garde-fous ou des limites aux actions qu'un administrateur peut déléguer à des utilisateurs ou à des rôles. Vous pouvez les utiliser SCPs comme listes d'autorisation ou de refus pour spécifier les services ou les actions autorisés ou interdits. Pour plus d'informations, consultez la section Politiques de contrôle des services dans la AWS Organizations documentation.

point de terminaison du service

URL du point d'entrée pour un Service AWS. Pour vous connecter par programmation au service cible, vous pouvez utiliser un point de terminaison. Pour plus d'informations, veuillez consulter la rubrique Service AWS endpoints dans Références générales AWS.

contrat de niveau de service (SLA)

Accord qui précise ce qu'une équipe informatique promet de fournir à ses clients, comme le temps de disponibilité et les performances des services.

indicateur de niveau de service (SLI)

Mesure d'un aspect des performances d'un service, tel que son taux d'erreur, sa disponibilité ou son débit.

objectif de niveau de service (SLO)

Mesure cible qui représente l'état d'un service, tel que mesuré par un indicateur de niveau de service.

modèle de responsabilité partagée

Un modèle décrivant la responsabilité que vous partagez en matière AWS de sécurité et de conformité dans le cloud. AWS est responsable de la sécurité du cloud, alors que vous êtes responsable de la sécurité dans le cloud. Pour de plus amples informations, veuillez consulter Modèle de responsabilité partagée.

SIEM

Consultez les informations de sécurité et le système de gestion des événements.

point de défaillance unique (SPOF)

Défaillance d'un seul composant critique d'une application susceptible de perturber le système.

SLA

Voir le contrat de niveau de service.

SLI

Voir l'indicateur de niveau de service.

SLO

Voir l'objectif de niveau de service.

split-and-seed modèle

Modèle permettant de mettre à l'échelle et d'accélérer les projets de modernisation. Au fur et à mesure que les nouvelles fonctionnalités et les nouvelles versions de produits sont définies, l'équipe principale se divise pour créer des équipes de produit. Cela permet de mettre à l'échelle les capacités et les services de votre organisation, d'améliorer la productivité des développeurs et de favoriser une innovation rapide. Pour plus d'informations, voir Approche progressive de la modernisation des applications dans le. AWS Cloud

SPOF

Voir point de défaillance unique.

schéma en étoile

Structure organisationnelle de base de données qui utilise une grande table de faits pour stocker les données transactionnelles ou mesurées et utilise une ou plusieurs tables dimensionnelles plus petites pour stocker les attributs des données. Cette structure est conçue pour être utilisée dans un entrepôt de données ou à des fins de business intelligence.

modèle de figuier étrangleur

Approche de modernisation des systèmes monolithiques en réécrivant et en remplaçant progressivement les fonctionnalités du système jusqu'à ce que le système hérité puisse être mis hors service. Ce modèle utilise l'analogie d'un figuier de vigne qui se développe dans un arbre existant et qui finit par supplanter son hôte. Le schéma a été présenté par Martin Fowler comme un moyen de gérer les risques lors de la réécriture de systèmes monolithiques. Pour obtenir un exemple d'application de ce modèle, veuillez consulter Modernizing legacy Microsoft ASP.NET (ASMX) web services incrementally by using containers and Amazon API Gateway.

sous-réseau

Plage d'adresses IP dans votre VPC. Un sous-réseau doit se trouver dans une seule zone de disponibilité.

contrôle de supervision et acquisition de données (SCADA)

Dans le secteur manufacturier, un système qui utilise du matériel et des logiciels pour surveiller les actifs physiques et les opérations de production.

chiffrement symétrique

Algorithme de chiffrement qui utilise la même clé pour chiffrer et déchiffrer les données.

tests synthétiques

Tester un système de manière à simuler les interactions des utilisateurs afin de détecter les problèmes potentiels ou de surveiller les performances. Vous pouvez utiliser Amazon CloudWatch Synthetics pour créer ces tests.

invite du système

Technique permettant de fournir un contexte, des instructions ou des directives à un LLM afin d'orienter son comportement. Les instructions du système aident à définir le contexte et à établir des règles pour les interactions avec les utilisateurs.

T

tags

Des paires clé-valeur qui agissent comme des métadonnées pour organiser vos AWS ressources. Les balises peuvent vous aider à gérer, identifier, organiser, rechercher et filtrer des ressources. Pour plus d'informations, veuillez consulter la rubrique Balisage de vos AWS ressources.

variable cible

La valeur que vous essayez de prédire dans le cadre du ML supervisé. Elle est également qualifiée de variable de résultat. Par exemple, dans un environnement de fabrication, la variable cible peut être un défaut du produit.

liste de tâches

Outil utilisé pour suivre les progrès dans un runbook. Liste de tâches qui contient une vue d'ensemble du runbook et une liste des tâches générales à effectuer. Pour chaque tâche générale, elle inclut le temps estimé nécessaire, le propriétaire et l'avancement.

environnement de test

Voir environnement.

entraînement

Pour fournir des données à partir desquelles votre modèle de ML peut apprendre. Les données d'entraînement doivent contenir la bonne réponse. L'algorithme d'apprentissage identifie des modèles dans les données d'entraînement, qui mettent en correspondance les attributs des données d'entrée avec la cible (la réponse que vous souhaitez prédire). Il fournit un modèle de ML qui capture ces modèles. Vous pouvez alors utiliser le modèle de ML pour obtenir des prédictions sur de nouvelles données pour lesquelles vous ne connaissez pas la cible.

passerelle de transit

Un hub de transit réseau que vous pouvez utiliser pour interconnecter vos réseaux VPCs et ceux sur site. Pour plus d'informations, voir Qu'est-ce qu'une passerelle de transit dans la AWS Transit Gateway documentation.

flux de travail basé sur jonction

Approche selon laquelle les développeurs génèrent et testent des fonctionnalités localement dans une branche de fonctionnalités, puis fusionnent ces modifications dans la branche principale. La branche principale est ensuite intégrée aux environnements de développement, de préproduction et de production, de manière séquentielle.

accès sécurisé

Accorder des autorisations à un service que vous spécifiez pour effectuer des tâches au sein de votre organisation AWS Organizations et dans ses comptes en votre nom. Le service de

confiance crée un rôle lié au service dans chaque compte, lorsque ce rôle est nécessaire, pour effectuer des tâches de gestion à votre place. Pour plus d'informations, consultez la section Utilisation AWS Organizations avec d'autres AWS services dans la AWS Organizations documentation.

réglage

Pour modifier certains aspects de votre processus d'entraînement afin d'améliorer la précision du modèle de ML. Par exemple, vous pouvez entraîner le modèle de ML en générant un ensemble d'étiquetage, en ajoutant des étiquettes, puis en répétant ces étapes plusieurs fois avec différents paramètres pour optimiser le modèle.

équipe de deux pizzas

Une petite DevOps équipe que vous pouvez nourrir avec deux pizzas. Une équipe de deux pizzas garantit les meilleures opportunités de collaboration possible dans le développement de logiciels.

U

incertitude

Un concept qui fait référence à des informations imprécises, incomplètes ou inconnues susceptibles de compromettre la fiabilité des modèles de ML prédictifs. Il existe deux types d'incertitude : l'incertitude épistémique est causée par des données limitées et incomplètes, alors que l'incertitude aléatoire est causée par le bruit et le caractère aléatoire inhérents aux données. Pour plus d'informations, veuillez consulter le guide Quantifying uncertainty in deep learning systems.

tâches indifférenciées

Également connu sous le nom de « levage de charges lourdes », ce travail est nécessaire pour créer et exploiter une application, mais qui n'apporte pas de valeur directe à l'utilisateur final ni d'avantage concurrentiel. Les exemples de tâches indifférenciées incluent l'approvisionnement, la maintenance et la planification des capacités.

environnements supérieurs

Voir environnement.

V

mise à vide

Opération de maintenance de base de données qui implique un nettoyage après des mises à jour incrémentielles afin de récupérer de l'espace de stockage et d'améliorer les performances.

contrôle de version

Processus et outils permettant de suivre les modifications, telles que les modifications apportées au code source dans un référentiel.

Appairage de VPC

Une connexion entre deux VPCs qui vous permet d'acheminer le trafic en utilisant des adresses IP privées. Pour plus d'informations, veuillez consulter la rubrique Qu'est-ce que l'appairage de VPC ? dans la documentation Amazon VPC.

vulnérabilités

Défaut logiciel ou matériel qui compromet la sécurité du système.

W

cache actif

Cache tampon qui contient les données actuelles et pertinentes fréquemment consultées. L'instance de base de données peut lire à partir du cache tampon, ce qui est plus rapide que la lecture à partir de la mémoire principale ou du disque.

données chaudes

Données rarement consultées. Lorsque vous interrogez ce type de données, des requêtes modérément lentes sont généralement acceptables.

fonction de fenêtre

Fonction SQL qui effectue un calcul sur un groupe de lignes liées d'une manière ou d'une autre à l'enregistrement en cours. Les fonctions de fenêtre sont utiles pour traiter des tâches, telles que le calcul d'une moyenne mobile ou l'accès à la valeur des lignes en fonction de la position relative de la ligne en cours.

charge de travail

Ensemble de ressources et de code qui fournit une valeur métier, par exemple une application destinée au client ou un processus de backend.

flux de travail

Groupes fonctionnels d'un projet de migration chargés d'un ensemble de tâches spécifique. Chaque flux de travail est indépendant, mais prend en charge les autres flux de travail du projet. Par exemple, le flux de travail du portefeuille est chargé de prioriser les applications, de planifier les vagues et de collecter les métadonnées de migration. Le flux de travail du portefeuille fournit ces actifs au flux de travail de migration, qui migre ensuite les serveurs et les applications.

VER

Voir écrire une fois, lire plusieurs.

WQF

Voir le cadre AWS de qualification de la charge de travail.

écrire une fois, lire plusieurs (WORM)

Modèle de stockage qui écrit les données une seule fois et empêche leur suppression ou leur modification. Les utilisateurs autorisés peuvent lire les données autant de fois que nécessaire, mais ils ne peuvent pas les modifier. Cette infrastructure de stockage de données est considérée comme immuable.

Z

exploit Zero-Day

Une attaque, généralement un logiciel malveillant, qui tire parti d'une vulnérabilité de type « jour zéro ».

vulnérabilité « jour zéro »

Une faille ou une vulnérabilité non atténuée dans un système de production. Les acteurs malveillants peuvent utiliser ce type de vulnérabilité pour attaquer le système. Les développeurs prennent souvent conscience de la vulnérabilité à la suite de l'attaque.

invite Zero-Shot

Fournir à un LLM des instructions pour effectuer une tâche, mais aucun exemple (plans) pouvant aider à la guider. Le LLM doit utiliser ses connaissances pré-entraînées pour gérer la tâche. L'efficacité de l'invite zéro dépend de la complexité de la tâche et de la qualité de l'invite. Voir également les instructions en quelques clics.

application zombie

Application dont l'utilisation moyenne du processeur et de la mémoire est inférieure à 5 %. Dans un projet de migration, il est courant de retirer ces applications.

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.