Atteindre la maturité d'Essential Eight le AWS

AWS Directives prescriptives

AWS Directives prescriptives: Atteindre la maturité d'Essential Eight le AWS

Table of Contents

Atteindre la maturité d'Essential Eight en matière de sécurité et de conformité pour les entreprises australiennes AWS

Amazon Web Services (contributeurs)

Novembre 2024 (historique du document)

L'Australian Signals Directorate (ASD) a créé et hiérarchisé des stratégies pour aider les entreprises à atténuer les risques liés aux menaces de cybersécurité. Huit de ces stratégies ont été choisies pour former le cadre Essential Eight. De nombreuses organisations des secteurs public et privé en Australie sont tenues d'atteindre la maturité dans le cadre Essential Eight.

Le Centre australien de cybersécurité (ACSC) a créé le cadre Essential Eight pour aider à protéger Microsoftbasés sur des réseaux connectés à Internet. Cependant, de nombreuses entreprises doivent atteindre la maturité Essential Eight pour tous leurs environnements, à la fois sur site et dans le cloud.

Le framework Essential Eight inclut également un modèle de maturité conçu pour aider les organisations à mettre en œuvre le framework par itération progressive. Le modèle décrit les niveaux de maturité de zéro à trois. Le niveau de maturité 3 représente la résilience face aux tactiques de cybersécurité avancées et aux attaques très ciblées. Ce guide fournit des conseils spécifiques et éclairés pour vous aider à atteindre le niveau 3 de maturité d'Essential Eight. AWS

Sécurité et conformité pour les entreprises australiennes

De nombreuses organisations en Australie AWS Cloud les utilisent pour stocker des données confidentielles, traiter des transactions sensibles et créer des services essentiels.

Bien que ce guide explique comment adapter le framework Essential Eight au cloud, il fournit AWS également les certifications et modèles suivants pour vous aider à répondre aux exigences de sécurité et de conformité de votre entreprise :

- Programme d'évaluateurs agréés en matière de sécurité de l'information
- Cadre de certification d'hébergement
- AWS modèle de responsabilité partagée
- AWS Framework Well-Architected

Programme d'évaluateurs agréés en matière de sécurité de l'information

Services AWS ont été évalués dans le cadre du programme d'évaluateurs enregistrés en matière de sécurité de l'information (IRAP) du Centre australien de cybersécurité (ACSC) au niveau PROTÉGÉ. Un évaluateur IRAP indépendant certifié par la Direction australienne des signaux (ASD) a effectué l'évaluation IRAP de. AWS Cette évaluation fournit l'assurance que, en ce qui concerne les AWS produits et services, les contrôles applicables sont mis en œuvre pour les charges de travail de niveau PROTÉGÉ.

Le package AWS IRAP PROTECTED est disponible via AWS Artifact. Le rapport IRAP a été développé à l'aide des directives de sécurité de l'ACSC Cloud (site Web de l'ACSC). Pour une liste complète de ceux Services AWS qui sont concernés, voir Services AWS dans le champ d'application : IRAP.

Cadre de certification d'hébergement

Le cadre australien de certification d'hébergement a été développé pour soutenir la gestion sécurisée des systèmes et des données gouvernementaux. Ce cadre vise à aider les organisations à atténuer les risques liés à la chaîne d'approvisionnement et à la propriété des centres de données. AWS a obtenu la certification au niveau stratégique certifié. Cela permet aux agences gouvernementales

de continuer à innover à un rythme rapide, en sachant que cela AWS répond aux exigences du gouvernement.

AWS modèle de responsabilité partagée

Le modèle de responsabilitéAWS 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. Vous êtes responsable de la gestion du système d'exploitation client (y compris les mises à jour et les correctifs de sécurité) et des autres logiciels d'application associés. Vous êtes également responsable de la configuration du pare-feu du groupe de sécurité AWS fourni.

Il est essentiel que vous compreniez le modèle de responsabilité AWS partagée lorsque vous abordez la maturité d'Essential Eight AWS. Vos responsabilités varient en fonction des services utilisés, de l'intégration de ces services dans votre environnement informatique et des lois et réglementations applicables.

AWS Framework Well-Architected

AWS Well-Architected aide les architectes du cloud à créer une infrastructure sécurisée, performante, résiliente et efficace pour une variété d'applications et de charges de travail. Le AWS Well-Architected Framework fournit les meilleures pratiques architecturales qui vous aident à concevoir, construire et exploiter des systèmes sur lesquels. AWS Ce cadre repose sur six piliers : excellence opérationnelle, sécurité, fiabilité, efficacité des performances, optimisation des coûts et durabilité.

AWS fournit également un service de révision de vos charges de travail. AWS Well-Architected ToolCela vous aide à revoir et à évaluer votre architecture à l'aide du AWS Well-Architected Framework. Il fournit des recommandations pour améliorer la fiabilité, la sécurité, l'efficacité et la rentabilité de vos charges de travail.

Réinterpréter les huit stratégies essentielles pour le cloud

Voici les stratégies d'atténuation originales d'Essential Eight conçues pour Microsoftréseaux connectés à Internet :

- Contrôle des applications
- Applications de correctifs
- Configuration Microsoft Office paramètres de macro
- Durcissement des applications utilisateur
- Restreindre les privilèges administratifs
- Corrigez les systèmes d'exploitation
- Authentification multifacteur
- Sauvegardes régulières

Il est important de rappeler que le framework Essential Eight n'est pas conçu pour les environnements cloud. Cependant, les principes sous-jacents sont applicables et il existe un chevauchement entre les stratégies Essential Eight et les meilleures pratiques du AWS Well-Architected Framework.

Diverses approches natives du cloud peuvent améliorer la sécurité et réduire considérablement votre charge de conformité. Dans les environnements sur site, vous êtes responsable de tous les aspects de la sécurité, et aucun contrôle n'est hérité. Lors de l'exécution de charges de travail dans le cloud, AWS est responsable de la protection de l'infrastructure qui gère nos services. Vous pouvez également réduire votre charge de conformité en utilisant l'automatisation et les services gérés. Les services gérés, également appelés services abstraits, concernent la couche Services AWS d'infrastructure AWS , 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. Pour plus d'informations, consultez la Thème 1 : Utiliser les services gérés section de ce guide.

Par conséquent, une certaine réinterprétation est nécessaire pour adapter les stratégies Essential Eight aux charges de travail. AWS Ce guide convertit les huit stratégies Essential Eight en AWS thèmes.

Utilisation des thèmes

Ce guide est divisé en huit thèmes. Chaque stratégie Essential Eight est associée à un ou plusieurs des thèmes suivants, et chaque thème est associé à une ou plusieurs meilleures pratiques du Well-Architected AWS Framework :

- Thème 1 : Utiliser les services gérés
- Thème 2 : Gérer une infrastructure immuable grâce à des pipelines sécurisés
- Thème 3 : Gérer une infrastructure mutable grâce à l'automatisation
- Thème 4 : Gérer les identités
- Thème 5 : Établir un périmètre de données
- Thème 6 : Automatiser les sauvegardes
- Thème 7 : Centralisation de la journalisation et de la surveillance
- Thème 8 : Mettre en œuvre des mécanismes pour les processus manuels

Chaque thème inclut une présentation du sujet, les meilleures pratiques associées au AWS Well-Architected Framework et des instructions sur la manière d'atteindre la maturité d'Essential Eight et de contrôler la conformité. Les instructions fournissent des étapes manuelles ou vous aident à configurer les automatisations à l'aide de AWS Config règles. Les étapes manuelles nécessitent des mécanismes pour s'assurer que les résultats sont pris en compte. Pour plus d'informations, consultezThème 8 : Mettre en œuvre des mécanismes pour les processus manuels. AWS Config les règles nécessitent une supervision ou une automatisation similaires afin de remédier aux ressources non conformes. En suivant les conseils correspondant à ces thèmes, vous pouvez atteindre la maturité d'Essential Eight grâce à une approche qui maximise également les avantages du cloud.

Réinterpréter les huit stratégies essentielles pour le cloud

Le framework Essential Eight n'étant pas conçu pour les environnements cloud, il est essentiel d'adopter une approche cloud native pour aborder les principes sous-jacents de chaque stratégie Essential Eight. L'approche varie en fonction de deux questions clés.

Quels sont les services que vous utilisez ?

Ils AWS modèle de responsabilité partagée peuvent vous aider à alléger vos charges opérationnelles et de conformité. Les services gérés transfèrent une plus grande AWS part de la responsabilité du

maintien de la disponibilité, des performances et de l'optimisation de la sécurité du service déployé. Les services gérés suppriment également le fardeau opérationnel et administratif lié à la maintenance d'un service, ce qui permet de consacrer plus de temps à l'innovation.

Les services gérés incluent les services sans serveur, tels qu'Amazon API Gateway et AWS LambdaDynamoDB. Une base de données sur Amazon Relational Database Service (Amazon RDS) nécessite moins de responsabilités opérationnelles qu'une base de données sur Amazon Elastic Compute Cloud (Amazon EC2).

Par exemple, si vous adaptez la stratégie Essential Eight des systèmes d'exploitation Patch au cloud, vous devez déterminer quels services vous utilisez et déterminer si vous êtes responsable de l'application des correctifs à ces ressources. AWS est responsable de l'application des correctifs aux services entièrement gérés, tels que Lambda et DynamoDB. Pour d'autres services, tels qu'Amazon RDS ou Amazon Redshift, vous devrez peut-être gérer les correctifs pendant les fenêtres de maintenance.

Quel modèle de déploiement utilisez-vous ?

Votre organisation utilise-t-elle une approche d'infrastructure mutable ou immuable ?

Le modèle d'infrastructure mutable met à jour et modifie l'infrastructure existante pour les charges de travail de production. Il s'agissait de la méthode de déploiement standard avant le cloud, lorsque le remplacement de l'infrastructure de serveurs était si coûteux et chronophage que l'approche la plus pratique consistait à appliquer des modifications aux serveurs déjà en production. Un exemple d'approche mutable dans le cloud consiste à déployer des modifications d'application directement sur les EC2 instances en cours d'exécution, soit manuellement, soit à l'aide d'un service de déploiement de logiciels, tel que AWS Systems Manager Run Command ou AWS CodeDeploy.

Le modèle d'infrastructure immuable 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. La définition d'une pile d'applications dans AWS CloudFormationou AWS Cloud Development Kit (AWS CDK)est un exemple d'approche immuable. Vous pouvez utiliser ces services pour déployer une pile d'applications par le biais de pipelines d'intégration continue et de livraison continue (CI/CD). Cette approche utilise des méthodes de déploiement telles que le roulement ou le bleu/vert. Pour plus d'informations sur cette approche, consultez les meilleures pratiques relatives au déploiement à l'aide d'une infrastructure immuable dans le AWS Well-Architected Framework.

Par exemple, si vous adaptez la stratégie Essential Eight des systèmes d'exploitation Patch au cloud, vous devez réfléchir à la manière dont les correctifs s'appliquent au modèle de déploiement. Dans

le cas d'une infrastructure mutable, vous pouvez appliquer des correctifs manuels aux ressources ou améliorer l'efficacité opérationnelle grâce à l'automatisation. Si vous utilisez une infrastructure immuable, vous devez utiliser un pipeline CI/CD pour déployer une nouvelle infrastructure avec la dernière version du système d'exploitation. En fait, le terme « patching » n'est pas approprié dans ce modèle, car l'infrastructure serait remplacée plutôt que corrigée.

Thème 1 : Utiliser les services gérés

Huit stratégies essentielles abordées

Corrigez les applications, limitez les privilèges administratifs, corrigez les systèmes d'exploitation

Les services gérés vous aident à réduire vos obligations de conformité en vous AWS permettant de gérer certaines tâches de sécurité, telles que les correctifs et la gestion des vulnérabilités.

Comme indiqué dans la AWS modèle de responsabilité partagée section, vous partagez la responsabilité de la sécurité et AWS de la conformité du cloud avec vous. Cela peut réduire votre charge opérationnelle, car il AWS exploite, gère et contrôle les composants, qu'il s'agisse du système d'exploitation hôte, de la couche de virtualisation ou de la sécurité physique des installations dans lesquelles le service fonctionne.

Vos responsabilités peuvent inclure la gestion des fenêtres de maintenance pour les services gérés, tels qu'Amazon Relational Database Service (Amazon RDS) ou Amazon Redshift, et l'analyse des vulnérabilités AWS Lambda dans le code ou les images de conteneur. Comme pour tous les thèmes de ce guide, vous êtes également responsable de la surveillance et des rapports de conformité. Vous pouvez utiliser Amazon Inspector pour signaler les vulnérabilités de tous vos sites Comptes AWS. Vous pouvez utiliser des règles pour vous AWS Config assurer que les services, tels qu'Amazon RDS et Amazon Redshift, disposent de mises à jour mineures et que les fenêtres de maintenance sont activées.

Par exemple, si vous exécutez une EC2 instance Amazon, vos responsabilités sont les suivantes :

- Contrôle des applications
- Applications d'application de correctifs
- Restreindre les privilèges administratifs au plan EC2 de contrôle Amazon et au système d'exploitation (OS)
- Corriger le système d'exploitation
- Appliquer l'authentification multifactorielle (MFA) pour accéder au plan de AWS contrôle et au système d'exploitation
- Sauvegarde des données et de la configuration

Par contre, si vous exécutez une fonction Lambda, vos responsabilités sont réduites et incluent les éléments suivants :

- Contrôle des applications
- Confirmation du fait que les bibliothèques sont up-to-date
- Restreindre les privilèges administratifs au plan de contrôle Lambda
- Appliquer le MFA pour accéder au plan de contrôle AWS
- Sauvegarde du code et de la configuration de la fonction Lambda

Bonnes pratiques associées au AWS Well-Architected Framework

- SEC01-BP05 Réduire le périmètre de gestion de la sécurité

Implémentation de ce thème

Activer l'application de correctifs

- Appliquer les mises à jour d'Amazon RDS
- Activez les mises à jour gérées dans AWS Elastic Beanstalk
- Tenez compte des fenêtres de maintenance du cluster Amazon Redshift

Détecter les vulnérabilités

- Scannez des images de conteneurs Amazon Elastic Container Registry (Amazon ECR) avec Amazon Inspector
- Scannez les fonctions Lambda avec Amazon Inspector

Surveillance de ce thème

Mettre en œuvre des contrôles de gouvernance

- Activez les meilleures pratiques opérationnelles pour le pack de conformité ACSC Essential 8 dans AWS Config

Surveillez Amazon Inspector

- Évaluez la couverture au niveau du compte
- Gérez plusieurs comptes

Implémentez les AWS Config règles suivantes

- `RDS_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED`
- `ELASTIC_BEANSTALK_MANAGED_UPDATES_ENABLED`
- `REDSHIFT_CLUSTER_MAINTENANCESETTINGS_CHECK`
- `EC2_MANAGEDINSTANCE_PATCH_COMPLIANCE_STATUS_CHECK`
- `EKS_CLUSTER_SUPPORTED_VERSION`

Thème 2 : Gérer une infrastructure immuable grâce à des pipelines sécurisés

Huit stratégies essentielles abordées

Contrôle des applications, applications de correctifs, correctifs de systèmes d'exploitation

Pour une infrastructure immuable, vous devez sécuriser les pipelines de déploiement pour les modifications du système. AWS L'éminent ingénieur Colm MacCárthaigh a expliqué ce principe dans le livre Zero-Privilege Operations : Running Services Without Access to Data (YouTube vidéo) présentation lors de la conférence AWS re:Invent 2022.

En limitant l'accès direct pour configurer les AWS ressources, vous pouvez exiger que toutes les ressources soient déployées ou modifiées par le biais de pipelines approuvés, sécurisés et automatisés. En général, vous créez des politiques AWS Identity and Access Management (IAM) qui permettent aux utilisateurs d'accéder uniquement au compte hébergeant le pipeline de déploiement. Vous configurez également des politiques IAM qui autorisent un accès sans faille à un nombre limité d'utilisateurs. Pour empêcher les modifications manuelles, vous pouvez utiliser des groupes de sécurité pour bloquer SSH et Windows accès aux serveurs via le protocole RDP (Remote Desktop Protocol). Le gestionnaire de session, une fonctionnalité de AWS Systems Manager, peut fournir un accès aux instances sans qu'il soit nécessaire d'ouvrir des ports entrants ou de gérer des hôtes bastions.

Les images Amazon Machine (AMIs) et les images de conteneur doivent être créées de manière sécurisée et reproductible. Pour les EC2 instances Amazon, vous pouvez utiliser EC2 Image Builder pour créer des instances AMIs dotées de fonctionnalités de sécurité intégrées, telles que la découverte d'instances, le contrôle des applications et la journalisation. Pour plus d'informations sur le contrôle des applications, voir Implémentation du contrôle des applications sur le site Web de l'ACSC. Vous pouvez également utiliser Image Builder pour créer des images de conteneurs, et vous pouvez utiliser Amazon Elastic Container Registry (Amazon ECR) pour partager ces images entre comptes. Une équipe de sécurité centrale peut approuver le processus automatisé de création de ces images AMIs et des images de conteneur afin que toute image d'AMI ou de conteneur qui en résulte soit approuvée pour utilisation par les équipes d'application.

Les applications doivent être définies dans l'infrastructure en tant que code (IaC), en utilisant des services tels que AWS CloudFormationou AWS Cloud Development Kit (AWS CDK). Les

outils d'analyse de code AWS CloudFormation Guard, tels que cfn-nag ou cdk-nag, peuvent automatiquement tester le code par rapport aux meilleures pratiques de sécurité de votre pipeline approuvé.

Comme c'est Thème 1 : Utiliser les services gérés le cas, Amazon Inspector peut signaler des vulnérabilités sur votre site Comptes AWS. Les équipes centralisées chargées du cloud et de la sécurité peuvent utiliser ces informations pour vérifier que l'équipe chargée des applications répond aux exigences de sécurité et de conformité.

Pour surveiller la conformité et établir des rapports à ce sujet, effectuez des examens continus des ressources et des journaux IAM. Utilisez AWS Config des règles pour vous assurer que seules les ressources approuvées AMIs sont utilisées, et assurez-vous qu'Amazon Inspector est configuré pour analyser les ressources Amazon ECR à la recherche de vulnérabilités.

Bonnes pratiques associées au AWS Well-Architected Framework

- OPS05-BP04 Utiliser des systèmes de gestion du développement et du déploiement
- REL08-BP04 Effectuer le déploiement à l'aide d'une infrastructure immuable
- SEC06-BP03 Réduire la gestion manuelle et l'accès interactif

Implémentation de ce thème

Mettre en œuvre des API et des pipelines de création de conteneurs

- Utilisez EC2 Image Builder et intégrez les éléments suivants à votre AMIs :
  - AWS Systems Manager Agent (agent SSM), utilisé pour la découverte et la gestion des instances
  - Outils de sécurité pour le contrôle des applications, tels que Security Enhanced Linux (SELinux) (GitHub), File Access Policy Daemon (fapolicyd) (GitHub) ou OpenSCAP
  - Amazon CloudWatch Agent, qui est utilisé pour la journalisation
- Pour toutes les EC2 instances, incluez les `AmazonSSMManagedInstanceCore` politiques `CloudWatchAgentServerPolicy` et dans le profil d'instance ou le rôle IAM que Systems Manager utilise pour accéder à votre instance
- Partagez AMIs avec l'ensemble de l'organisation
- Partagez les ressources EC2 d'Image Builder

- Assurez-vous que les équipes chargées des applications font référence aux dernières AMIs
- Utilisez votre pipeline d'AMI pour la gestion des correctifs
- Implémenter des pipelines de construction de conteneurs :
  - Créez un pipeline d'images de conteneur à l'aide de l'assistant de console EC2 Image Builder
  - Créez un pipeline de livraison continue pour vos images de conteneurs en utilisant Amazon ECR comme source (article de AWS blog)
- Partagez des images de conteneurs ECR au sein de votre organisation via des architectures multicomptes et multirégionales

Implémenter des pipelines de création d'applications sécurisés

- Implémentez des pipelines de génération pour IaC, par exemple en utilisant EC2 Image Builder et AWS CodePipeline (article de AWS blog)
- Utilisez des outils d'analyse de code AWS CloudFormation Guard, tels que cfn-nag (GitHub) ou cdk-nag (GitHub), dans les pipelines CI/CD pour détecter les violations des meilleures pratiques, telles que :
  - Politiques IAM trop permissives, telles que celles qui utilisent des caractères génériques
  - Règles de groupe de sécurité trop permissives, telles que celles qui utilisent des caractères génériques ou autorisent l'accès SSH
  - Journaux d'accès non activés
  - Chiffrement non activé
  - Littéraux de mot de passe
- Implémenter des outils de numérisation dans les pipelines (article de AWS blog)
- Utilisation AWS Identity and Access Management Access Analyzer dans les pipelines (article de AWS blog) pour valider les politiques IAM définies dans CloudFormation les modèles
- Configurez les politiques IAM et les politiques de contrôle des services pour un accès au moindre privilège afin d'utiliser le pipeline ou d'y apporter des modifications

Mettre en œuvre l'analyse des vulnérabilités

- Activez Amazon Inspector dans tous les comptes de votre organisation
- Utilisez Amazon Inspector pour scanner AMIs le pipeline de génération de votre AMI :
  - Gérez le cycle de vie de AMIs dans EC2 Image Builder (GitHub)

- Configurez une analyse améliorée pour les référentiels Amazon ECR à l'aide d'Amazon Inspector
- Élaborez un programme de gestion des vulnérabilités pour trier et corriger les résultats de sécurité

Surveillance de ce thème

Surveillez l'IAM et les journaux en permanence

- Passez régulièrement en revue vos politiques IAM pour vous assurer que :
  - Seuls les pipelines de déploiement ont un accès direct aux ressources
  - Seuls les services approuvés ont un accès direct aux données
  - Les utilisateurs n'ont pas d'accès direct aux ressources ou aux données
- Surveillez AWS CloudTrail les journaux pour vérifier que les utilisateurs modifient les ressources par le biais de pipelines et qu'ils ne modifient pas directement les ressources ou n'accèdent pas aux données
- Passez régulièrement en revue les résultats d'IAM Access Analyzer
- Configurez une alerte pour vous avertir si les informations d'identification de l'utilisateur root Compte AWS sont utilisées

Implémentez les AWS Config règles suivantes

- `APPROVED_AMIS_BY_ID`
- `APPROVED_AMIS_BY_TAG`
- `ECR_PRIVATE_IMAGE_SCANNING_ENABLED`

Thème 3 : Gérer une infrastructure mutable grâce à l'automatisation

Huit stratégies essentielles abordées

Contrôle des applications, applications de correctifs, correctifs de systèmes d'exploitation

Comme dans le cas d'une infrastructure immuable, vous gérez une infrastructure mutable en tant qu'IaC, et vous modifiez ou mettez à jour cette infrastructure par le biais de processus automatisés. De nombreuses étapes de mise en œuvre d'une infrastructure immuable s'appliquent également à une infrastructure mutable. Toutefois, dans le cas d'une infrastructure mutable, vous devez également implémenter des contrôles manuels pour vous assurer que les charges de travail modifiées respectent toujours les meilleures pratiques.

Pour une infrastructure mutable, vous pouvez automatiser la gestion des correctifs à l'aide du Gestionnaire de correctifs, une fonctionnalité de AWS Systems Manager. Activez Patch Manager dans tous les comptes de votre AWS organisation.

Empêchez les accès SSH et RDP directs et obligez les utilisateurs à utiliser le Gestionnaire de session ou Run Command, qui sont également des fonctionnalités de Systems Manager. Contrairement à SSH et RDP, ces fonctionnalités peuvent enregistrer les accès au système et les modifications.

Pour surveiller la conformité et établir des rapports à ce sujet, vous devez effectuer des examens continus de la conformité des correctifs. Vous pouvez utiliser des AWS Config règles pour vous assurer que toutes les EC2 instances Amazon sont gérées par Systems Manager, qu'elles disposent des autorisations requises, que les applications sont installées et qu'elles sont conformes aux correctifs.

Bonnes pratiques associées au AWS Well-Architected Framework

- SEC06-BP03 Réduire la gestion manuelle et l’accès interactif
- SEC06-BP05 Automatiser la protection informatique

Implémentation de ce thème

Automatisez l'application de correctifs

- Mettez en œuvre les étapes décrites dans Activer le gestionnaire de correctifs dans tous les comptes de votre AWS organisation
- Pour toutes les EC2 instances, incluez le `CloudWatchAgentServerPolicy` et `AmazonSSMManagedInstanceCore` dans le profil d'instance ou le rôle IAM que Systems Manager utilise pour accéder à votre instance.

Utilisez l'automatisation plutôt que les processus manuels

- Mettez en œuvre les directives de la section Implémenter l'AMI et les pipelines de construction de conteneurs dans Thème 2 : Gérer une infrastructure immuable grâce à des pipelines sécurisés
- Utiliser le gestionnaire de session ou exécuter une commande au lieu d'un accès SSH ou RDP direct

Utilisez l'automatisation pour installer les éléments suivants sur les EC2 instances

- AWS Systems Manager Agent (agent SSM), utilisé pour la découverte et la gestion des instances
- Outils de sécurité pour le contrôle des applications, tels que Security Enhanced Linux (SELinux) (GitHub), File Access Policy Daemon (fapolicyd) (GitHub) ou OpenSCAP
- Amazon CloudWatch Agent, utilisé pour la journalisation

Utilisez l'évaluation par les pairs avant toute publication pour vous assurer que les modifications sont conformes aux meilleures pratiques

- Politiques IAM trop permissives, telles que celles qui utilisent des caractères génériques
- Règles de groupe de sécurité trop permissives, telles que celles qui utilisent des caractères génériques ou autorisent l'accès SSH
- Journaux d'accès non activés
- Chiffrement non activé

- Littéraux de mot de passe
- Politiques IAM sécurisées

Utiliser des contrôles au niveau de l'identité

- Pour obliger les utilisateurs à modifier les ressources par le biais de processus automatisés et empêcher toute configuration manuelle, autorisez les autorisations en lecture seule pour les rôles que les utilisateurs peuvent assumer
- Accordez des autorisations de modification des ressources uniquement aux rôles de service, tels que le rôle utilisé par Systems Manager

Mettre en œuvre l'analyse des vulnérabilités

- Appliquez les instructions de la section Implémenter l'analyse des vulnérabilités dans Thème 2 : Gérer une infrastructure immuable grâce à des pipelines sécurisés
- Scannez vos EC2 instances à l'aide d'Amazon Inspector

Surveillance de ce thème

Surveillez en permanence la conformité des correctifs

- Créez des rapports sur la conformité des correctifs à l'aide de l'automatisation et de tableaux de bord
- Mettre en œuvre un mécanisme pour examiner les tableaux de bord afin de vérifier la conformité des correctifs

Surveillez l'IAM et les journaux en permanence

- Passez régulièrement en revue vos politiques IAM pour vous assurer que :
  - Seuls les pipelines de déploiement ont un accès direct aux ressources
  - Seuls les services approuvés ont un accès direct aux données
  - Les utilisateurs n'ont pas d'accès direct aux ressources ou aux données

- Surveillez AWS CloudTrail les journaux pour vous assurer que les utilisateurs modifient les ressources par le biais de pipelines et qu'ils ne modifient pas directement les ressources ou n'accèdent pas aux données
- Examiner régulièrement AWS Identity and Access Management Access Analyzer les résultats
- Configurez une alerte pour vous avertir si les informations d'identification de l'utilisateur root pour un Compte AWS sont utilisées

Implémentez les AWS Config règles suivantes

- `EC2_MANAGEDINSTANCE_PATCH_COMPLIANCE_STATUS_CHECK`
- `EC2_INSTANCE_MANAGED_BY_SSM`
- `EC2_MANAGEDINSTANCE_APPLICATIONS_REQUIRED - SELinux/fapolicyd/OpenSCAP, CW Agent`
- `EC2_MANAGEDINSTANCE_APPLICATIONS_BLACKLISTED - any unsupported apps`
- `IAM_ROLE_MANAGED_POLICY_CHECK - CW Logs, SSM`
- `EC2_MANAGEDINSTANCE_ASSOCIATION_COMPLIANCE_STATUS_CHECK`
- `REQUIRED_TAGS`
- `RESTRICTED_INCOMING_TRAFFIC - 22, 3389`

Thème 4 : Gérer les identités

Huit stratégies essentielles abordées

Restreindre les privilèges administratifs, authentification multifactorielle

La gestion robuste de l'identité et des autorisations est un aspect essentiel de la gestion de la sécurité dans le cloud. De solides pratiques en matière d'identité équilibrent l'accès nécessaire et le moindre privilège. Cela permet aux équipes de développement d'agir rapidement sans compromettre la sécurité.

Utilisez la fédération des identités pour centraliser la gestion des identités. Cela facilite la gestion de l'accès à plusieurs applications et services, car vous gérez l'accès à partir d'un seul emplacement. Cela vous permet également de mettre en œuvre des autorisations temporaires et une authentification multifactorielle (MFA).

Accordez aux utilisateurs uniquement les autorisations dont ils ont besoin pour effectuer leurs tâches. AWS Identity and Access Management Access Analyzer peut valider les politiques et vérifier l'accès public et entre comptes. Des fonctionnalités telles que les politiques de contrôle des AWS Organizations services (SCPs), les conditions de politique IAM, les limites des autorisations IAM et les ensembles d' AWS IAM Identity Center autorisations peuvent vous aider à configurer un contrôle d'accès détaillé (FGAC).

Quel que soit le type d'authentification, il est préférable d'utiliser des informations d'identification temporaires afin de réduire ou d'éliminer les risques, tels que la divulgation, le partage ou le vol d'informations d'identification par inadvertance. Utilisez des rôles IAM plutôt que des utilisateurs IAM.

Utilisez des mécanismes de connexion puissants, tels que le MFA, pour atténuer le risque que les informations de connexion soient divulguées par inadvertance ou soient facilement devinées. Exigez le MFA pour l'utilisateur root, et vous pouvez également l'exiger au niveau de la fédération. Si l'utilisation d'utilisateurs IAM est inévitable, appliquez le MFA.

Pour surveiller la conformité et établir des rapports à ce sujet, vous devez travailler en permanence à la réduction des autorisations, au suivi des résultats d'IAM Access Analyzer et à la suppression des ressources IAM inutilisées. Utilisez AWS Config des règles pour vous assurer que des mécanismes de connexion robustes sont appliqués, que les informations d'identification sont de courte durée et que les ressources IAM sont utilisées.

Bonnes pratiques associées au AWS Well-Architected Framework

- SEC02-BP01 Utiliser des mécanismes de connexion robustes
- SEC02-BP02 Utiliser des informations d’identification temporaires
- SEC02-BP03 Stocker et utiliser des secrets en toute sécurité
- SEC02-BP04 S’appuyer sur un fournisseur d’identité centralisé
- SEC02-BP05 Contrôler et effectuer régulièrement une rotation des informations d’identification
- SEC02-BP06 Utiliser des groupes d’utilisateurs et des attributs
- SEC03-BP01 Définir les conditions d’accès
- SEC03-BP02 Accorder un accès selon le principe du moindre privilège
- SEC03-BP03 Établir un processus d'accès d'urgence
- SEC03-BP04 Limiter les autorisations au minimum requis en permanence
- SEC03-BP05 Définir des garde-fous des autorisations pour votre organisation
- SEC03-BP06 Gérer l’accès en fonction du cycle de vie
- SEC03-BP07 Analyser l’accès public et intercompte
- SEC03-BP08 Partager des ressources en toute sécurité au sein de votre organisation

Implémentation de ce thème

Mettre en œuvre la fédération des identités

- Obliger les utilisateurs humains à se fédérer avec un fournisseur d'identité pour accéder à l'aide AWS d'informations d'identification temporaires
- Mettez en place un accès surélevé temporaire à vos AWS environnements

Appliquer les autorisations du moindre privilège

- Protégez vos informations d'identification d'utilisateur root et ne les utilisez pas pour les tâches quotidiennes
- Utilisez IAM Access Analyzer pour générer des politiques de moindre privilège en fonction de l'activité d'accès

- Vérifiez l'accès public et multicompte aux ressources avec IAM Access Analyzer
- Utilisez IAM Access Analyzer pour valider vos politiques IAM pour des autorisations sécurisées et fonctionnelles
- Établissez des barrières en matière d'autorisations sur plusieurs comptes
- Utilisez les limites d'autorisations pour définir le maximum d'autorisations qu'une politique basée sur l'identité peut accorder
- Utiliser les conditions des politiques IAM pour restreindre davantage l'accès
- Vérifiez et supprimez régulièrement les utilisateurs, rôles, autorisations, politiques et informations d'identification non utilisés
- Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège
- Utiliser la fonctionnalité des ensembles d'autorisations dans IAM Identity Center

Rotation des identifiants

- Exiger que les charges de travail utilisent des rôles IAM pour accéder AWS
- Suppression automatique des rôles IAM non utilisés
- Faites régulièrement pivoter les clés d'accès pour les cas d'utilisation nécessitant des informations d'identification à long terme

Appliquer la MFA

- Exiger le MFA pour l'utilisateur root
- Exiger le MFA via IAM Identity Center
- Envisagez d'exiger le MFA pour les actions d'API spécifiques au service

Surveillance de ce thème

Surveiller l'accès au moindre privilège

- Envoyez les résultats d'IAM Access Analyzer à AWS Security Hub
- Envisagez de configurer des notifications pour les conclusions critiques de l'IAM Identity Center
- Consultez régulièrement les rapports d'identification de votre Comptes AWS

Implémentez les AWS Config règles suivantes

- ACCESS_KEYS_ROTATED
- IAM_ROOT_ACCESS_KEY_CHECK
- IAM_USER_MFA_ENABLED
- IAM_USER_UNUSED_CREDENTIALS_CHECK
- IAM_PASSWORD_POLICY
- ROOT_ACCOUNT_HARDWARE_MFA_ENABLED

Thème 5 : Établir un périmètre de données

Huit stratégies essentielles abordées

Restreindre les privilèges administratifs

Un périmètre de données est un ensemble de barrières préventives dans votre AWS environnement qui permettent de garantir que seules les identités fiables accèdent aux ressources fiables des réseaux attendus. Ces barrières de sécurité constituent des limites permanentes qui aident à protéger vos données sur un large éventail de ressources. Comptes AWS Ces garde-corps à l'échelle de l'entreprise ne remplacent pas vos contrôles d'accès précis existants. Ils contribuent plutôt à améliorer votre stratégie de sécurité en s'assurant que tous les utilisateurs, rôles et ressources AWS Identity and Access Management (IAM) respectent un ensemble de normes de sécurité définies.

Vous pouvez établir un périmètre de données en utilisant des politiques qui empêchent l'accès depuis l'extérieur des limites de l'organisation, généralement créées dans AWS Organizations. Les trois principales conditions d'autorisation périmétrique utilisées pour établir un périmètre de données sont les suivantes :

- Identités fiables — Principaux (rôles ou utilisateurs IAM) qui vous Comptes AWS appartiennent ou qui Services AWS agissent en votre nom.
- Ressources fiables : ressources qui vous appartiennent Comptes AWS ou qui sont Services AWS gérées en votre nom.
- Réseaux attendus : vos centres de données sur site et vos clouds privés virtuels (VPCs), ou les réseaux qui Services AWS agissent en votre nom.

Envisagez de mettre en œuvre des périmètres de données entre des environnements présentant différentes classifications de données, telles que `OFFICIAL:SENSITIVE` ou`PROTECTED`, ou des niveaux de risque différents, tels que le développement, les tests ou la production. Pour plus d'informations, voir Création d'un périmètre de données sur AWS (AWS livre blanc) et Établissement d'un périmètre de données sur AWS : Vue d'ensemble (article de AWS blog).

Bonnes pratiques associées au AWS Well-Architected Framework

- SEC03-BP05 Définir des garde-fous des autorisations pour votre organisation

- SEC07-BP02 Appliquer des contrôles de protection des données en fonction de la sensibilité des données

Implémentation de ce thème

Mettre en œuvre des contrôles d'identité

- Autorisez uniquement les identités fiables à accéder à vos ressources : utilisez des politiques basées sur les ressources avec les clés `aws:PrincipalOrgID` de condition et. `aws:PrincipalIsAWSService` Cela permet uniquement aux directeurs de votre AWS organisation et d'accéder AWS à vos ressources.
- Autorisez les identités fiables uniquement à partir de votre réseau : utilisez les politiques de point de terminaison VPC avec les clés `aws:PrincipalOrgID` de condition et. `aws:PrincipalIsAWSService` Cela permet uniquement aux principaux de votre AWS organisation et à partir d'accéder AWS aux services via des points de terminaison VPC.

Mettre en œuvre des contrôles des ressources

- Autorisez vos identités à accéder uniquement aux ressources fiables : utilisez les politiques de contrôle des services (SCPs) avec la clé de condition`aws:ResourceOrgID`. Cela permet à vos identités d'accéder uniquement aux ressources de votre AWS organisation.
- Autorisez l'accès aux ressources fiables uniquement depuis votre réseau : utilisez les politiques de point de terminaison VPC avec la clé de condition. `aws:ResourceOrgID` Cela permet à vos identités d'accéder aux services uniquement via les points de terminaison VPC qui font partie de votre organisation. AWS

Mettre en œuvre des contrôles réseau

- Autoriser les identités à accéder aux ressources uniquement à partir des réseaux attendus : SCPs à utiliser avec les clés de condition `aws:SourceIp` `aws:SourceVpc`,`aws:SourceVpce`, et`aws:ViaAWSService`. Cela permet à vos identités d'accéder aux ressources uniquement à partir des adresses IP attendues VPCs, des points de terminaison VPC, et via. Services AWS
- Autorisez l'accès à vos ressources uniquement à partir des réseaux attendus : utilisez des politiques basées sur les ressources avec les clés de condition`aws:SourceIp`,`aws:SourceVpc`, `aws:SourceVpce`,`aws:ViaAWSService`, et. `aws:PrincipalIsAWSService` Cela permet

d'accéder à vos ressources uniquement à partir des points de terminaison VPC attendus VPCs, à partir des points de terminaison VPC attendus Services AWS, via ou lorsque l'identité de l'appelant est un. IPs Service AWS

Surveillance de ce thème

Politiques de surveillance

- Mettre en œuvre des mécanismes de révision SCPs, des politiques IAM et des politiques de point de terminaison VPC

Implémentez les AWS Config règles suivantes

- `SERVICE_VPC_ENDPOINT_ENABLED`

Thème 6 : Automatiser les sauvegardes

Huit stratégies essentielles abordées

Sauvegardes régulières

« Les défaillances vont de soi et tout finira par échouer au fil du temps : des routeurs aux disques durs, des systèmes d'exploitation aux unités de mémoire qui corrompent les paquets TCP, des erreurs transitoires aux défaillances permanentes. Cela va de soi, que vous utilisiez du matériel de la plus haute qualité ou des composants les moins coûteux. » —Werner Vogels, directeur technique, Amazon, All Things Distributed

La sauvegarde et la restauration des données sont essentielles à la fiabilité d'un système. AWS est conçu pour faciliter la création de sauvegardes, garantir la durabilité des données sauvegardées et garantir que les données sauvegardées restent récupérables.

AWS Backupest un service entièrement géré qui centralise et automatise la sauvegarde des données entre tous. Services AWS Il prend en charge plusieurs types de AWS ressources et vous aide à mettre en œuvre et à maintenir une stratégie de sauvegarde pour les charges de travail qui utilisent plusieurs AWS ressources qui doivent être sauvegardées collectivement. AWS Backup vous permet également de surveiller collectivement une opération de sauvegarde et de restauration de plusieurs AWS ressources.

AWS Backup Vault Lock est une fonctionnalité optionnelle d'un coffre-fort de sauvegarde, qui peut fournir une sécurité et un contrôle supplémentaires. Lorsqu'un verrou est actif en mode conformité et que le délai de grâce est expiré, la configuration du coffre-fort ne peut pas être modifiée ou supprimée par un utilisateur, un compte ou le propriétaire des données, ou AWS. Chaque coffre-fort peut avoir un verrouillage de coffre-fort en place. Cela permet la configuration WORM (écriture unique, lecture multiple) et l'application des périodes de rétention.

Si vous suivez les instructions de configuration actuelles, vous AWS Backup pouvez fournir une durabilité annuelle de 99,999999999 %, également connue sous le nom de 11 neuf. Il utilise l'infrastructure AWS globale pour répliquer vos sauvegardes sur plusieurs zones de disponibilité. Pour plus d’informations, consultez Résilience dans AWS Backup.

AWS Backup vous aide à automatiser la restauration et le test des données sauvegardées afin de vérifier l'intégrité et les processus de sauvegarde.

Bonnes pratiques associées au AWS Well-Architected Framework

- SEC09-BP01 Mettre en œuvre une gestion sécurisée des clés et des certificats
- SEC09-BP02 Application du chiffrement en transit
- SEC09-BP03 Authentifier les communications réseau

Implémentation de ce thème

Automatisez la sauvegarde et la restauration des données

- Implémenter la sauvegarde des données sur AWS
- Automatisez la sauvegarde des données à grande échelle (article de AWS blog)
- Automatisez la validation de la récupération des données avec AWS Backup (article de AWS blog)

Mettez en œuvre la gouvernance pour l'ensemble de vos AWS Backup résultats

- Les 10 meilleures pratiques de sécurité pour sécuriser les sauvegardes dans AWS (article de AWS blog)
- Utilisez AWS Backup Vault Lock pour améliorer la sécurité de vos coffres-forts de sauvegarde
- Utilisez AWS Backup Audit Manager pour vérifier la conformité de vos AWS Backup politiques

Surveillance de ce thème

Implémentez les AWS Config règles suivantes

- `RDS_IN_BACKUP_PLAN`
- `RDS_LAST_BACKUP_RECOVERY_POINT_CREATED`
- `RDS_RESOURCES_PROTECTED_BY_BACKUP_PLAN`
- `REDSHIFT_BACKUP_ENABLED`
- `AURORA_LAST_BACKUP_RECOVERY_POINT_CREATED`
- `AURORA_RESOURCES_PROTECTED_BY_BACKUP_PLAN`

- BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK
- BACKUP_RECOVERY_POINT_ENCRYPTED
- BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED
- BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK
- DB_INSTANCE_BACKUP_ENABLED
- DYNAMODB_IN_BACKUP_PLAN
- DYNAMODB_LAST_BACKUP_RECOVERY_POINT_CREATED
- DYNAMODB_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EBS_IN_BACKUP_PLAN
- EBS_LAST_BACKUP_RECOVERY_POINT_CREATED
- EBS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EC2_LAST_BACKUP_RECOVERY_POINT_CREATED
- S3_LAST_BACKUP_RECOVERY_POINT_CREATED
- S3_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- STORAGEGATEWAY_LAST_BACKUP_RECOVERY_POINT_CREATED
- STORAGEGATEWAY_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- VIRTUALMACHINE_LAST_BACKUP_RECOVERY_POINT_CREATED
- VIRTUALMACHINE_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Thème 7 : Centralisation de la journalisation et de la surveillance

Huit stratégies essentielles abordées

Contrôle des applications, application de correctifs, restriction des privilèges administratifs, authentification multifactorielle

AWS fournit des outils et des fonctionnalités qui vous permettent de voir ce qui se passe dans votre AWS environnement. Il s'agit des licences suivantes :

- AWS CloudTrailvous aide à surveiller vos AWS déploiements en créant un historique des appels d' AWS API pour votre compte, y compris les appels d'API effectués via les outils de ligne de commande et AWS Management Console AWS SDKs,. Pour les services compatibles CloudTrail, vous pouvez également identifier les utilisateurs et les comptes qui ont appelé l'API du service, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels.
- Amazon vous CloudWatch aide à surveiller les indicateurs de vos AWS ressources et des applications que vous utilisez AWS en temps réel.
- Amazon CloudWatch Logs vous aide à centraliser les journaux de tous vos systèmes et applications, Services AWS afin que vous puissiez les surveiller et les archiver en toute sécurité.
- 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. GuardDuty s'intègre EventBridge à Amazon afin de lancer une réponse automatique ou d'avertir un humain.
- AWS Security Hubfournit une vue complète de votre état de sécurité dans AWS. Il vous permet également de vérifier que votre AWS environnement est conforme aux normes et aux meilleures pratiques du secteur de la sécurité.

Ces outils et fonctionnalités sont conçus pour augmenter la visibilité et vous aider à résoudre les problèmes avant qu'ils n'affectent négativement votre environnement. Cela vous permet d'améliorer le niveau de sécurité de votre entreprise dans le cloud et de réduire le profil de risque de votre environnement.

Bonnes pratiques associées au AWS Well-Architected Framework

- SEC04-BP01 Configurer une journalisation de service et d'application
- SEC04-BP02 Capturez les journaux, les résultats et les mesures dans des emplacements standardisés

Implémentation de ce thème

Activer la journalisation

- Utiliser l' CloudWatch agent pour publier les journaux au niveau du système dans Logs CloudWatch
- Configurez des alertes pour les GuardDuty résultats
- Créez un parcours d'organisation dans CloudTrail

Mettre en œuvre les meilleures pratiques de sécurité de journalisation

- Mettre en œuvre les meilleures pratiques de CloudTrail sécurité
- Utilisation SCPs pour empêcher les utilisateurs de désactiver les services de sécurité (article de AWS blog)
- Chiffrez les données du journal dans CloudWatch Logs en utilisant AWS Key Management Service

Centralisez les journaux

- Recevoir CloudTrail les journaux de plusieurs comptes
- Envoyer des journaux vers un compte d'archivage de journaux
- Centraliser les CloudWatch journaux dans un compte à des fins d'audit et d'analyse (article de AWS blog)
- Centralisez la gestion d'Amazon Inspector
- Création d'un agrégateur à l'échelle de l'organisation dans AWS Config(article de blog)AWS
- Gestion centralisée de Security Hub
- Centralisez la gestion de GuardDuty
- Envisagez d'utiliser Amazon Security Lake

Surveillance de ce thème

Mettre en œuvre des mécanismes

- Mettre en place un mécanisme pour examiner les résultats du journal
- Mettre en place un mécanisme pour examiner les conclusions du Security Hub
- Mettre en place un mécanisme pour répondre aux GuardDuty conclusions

Implémentez les AWS Config règles suivantes

- `CLOUDTRAIL_SECURITY_TRAIL_ENABLED`
- `GUARDDUTY_ENABLED_CENTRALIZED`
- `SECURITYHUB_ENABLED`
- `ACCOUNT_PART_OF_ORGANIZATIONS`

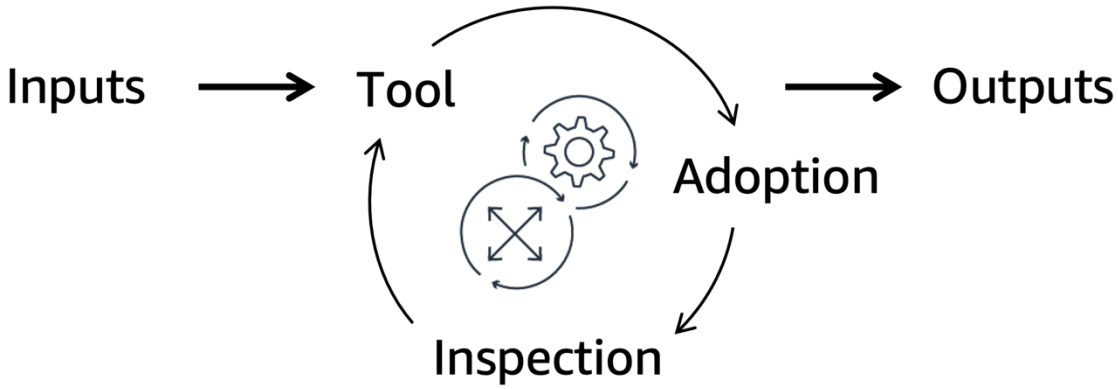
Thème 8 : Mettre en œuvre des mécanismes pour les processus manuels

Huit stratégies essentielles abordées

Contrôle des applications, applications de correctifs

Chez Amazon, nous avons un dicton : les bonnes intentions ne fonctionnent pas, les mécanismes, oui (article de AWS blog). Cela signifie que vous devez remplacer les meilleurs efforts par des processus et des outils automatisés, reproductibles et évolutifs afin d'obtenir les résultats souhaités.

Comme le montre le schéma suivant, un mécanisme est un processus complet dans lequel vous créez un outil, pilotez son adoption, puis inspectez les résultats afin de procéder aux ajustements. C'est un cycle qui se renforce et s'améliore au fur et à mesure qu'il fonctionne. Il prend des intrants contrôlables et les transforme en résultats permanents pour relever un défi commercial récurrent. Pour plus d'informations, voir Création de mécanismes dans le cadre AWS Well-Architected.



Bonnes pratiques associées au AWS Well-Architected Framework

- OPS02-BP01 Les ressources ont des propriétaires identifiés
- OPS02-BP02 Les processus et procédures ont des propriétaires identifiés
- OPS02-BP03 Les activités opérationnelles ont des propriétaires identifiés responsables de leurs performances

- OPS02-BP04 Des mécanismes sont en place pour gérer les responsabilités et qui est responsable de quoi
- OPS03-BP01 Assurer le parrainage de la direction
- OPS03-BP03 La remontée hiérarchique est encouragée

Implémentation de ce thème

- Mettre en place des mécanismes pour examiner et corriger les lacunes en matière de conformité
- Mettre en place des mécanismes pour mettre à jour les politiques de sécurité
- Supprimez les applications non prises en charge, puis ajoutez-les à la liste des AWS Config règles refusées
- Validez les politiques d'accès avec AWS Identity and Access Management Access Analyzer
- Activez Amazon Inspector, qui conserve automatiquement les registres des vulnérabilités up-to-date
- Passez en revue les ensembles de règles de contrôle des applications au moins une fois par an
- Envisagez de mettre en œuvre l'automatisation, par exemple des AWS Config règles, afin de réduire le fardeau des processus manuels
- Envisagez AWS Systems Manager d'utiliser l'inventaire pour avoir une meilleure visibilité sur les instances qui exécutent les logiciels requis par votre politique logicielle.

Surveillance de ce thème

- Établissez une supervision pour les sponsors exécutifs afin de suivre les progrès réalisés dans la réalisation des objectifs, notamment en matière de conformité, d'inspection des lacunes et d'évaluation des mécanismes.

Étude de cas indicative pour atteindre la maturité d'Essential Eight sur AWS

Ce chapitre présente une étude de cas indicative pour une agence gouvernementale ciblant la maturité d'Essential Eight sur AWS.

Sections de ce chapitre :

- Présentation du scénario et de l'architecture
- Exemple de charge de travail : lac de données sans serveur
- Exemple de charge de travail : service Web conteneurisé
- Exemple de charge de travail : logiciel COTS sur Amazon EC2

Présentation du scénario et de l'architecture

L'agence gouvernementale a trois charges de travail dans les AWS Cloud domaines suivants :

- Un lac de données sans serveur qui utilise Amazon Simple Storage Service (Amazon S3) pour le stockage AWS Lambda et pour les opérations d'extraction, de transformation et de chargement (ETL)
- Un service Web conteneurisé qui s'exécute sur Amazon Elastic Container Service (Amazon ECS) et utilise une base de données dans Amazon Relational Database Service (Amazon RDS)
- Un logiciel commercial off-the-shelf (COTS) exécuté sur Amazon EC2

Une équipe cloud fournit une plate-forme centralisée à l'organisation, exécutant les principaux services pour l' AWS environnement. Une équipe cloud fournit des services de base pour l' AWS environnement. Chaque charge de travail appartient à une équipe d'application distincte, également appelée équipe de développement ou équipe de livraison.

Architecture de base

L'équipe cloud a déjà mis en place les fonctionnalités suivantes dans AWS Cloud :

- Liens de la fédération d'identité AWS IAM Identity Center vers leur Microsoft Instance Entra ID (anciennement Azure Active Directory). La fédération applique le MFA, l'expiration automatique des

comptes utilisateurs et l'utilisation d'informations d'identification de courte durée par le AWS Identity and Access Management biais de rôles (IAM).

- Un pipeline d'AMI centralisé est utilisé pour appliquer des correctifs OSs et des applications de base avec EC2 Image Builder.
- Amazon Inspector est activé pour identifier les vulnérabilités, et tous les résultats de sécurité sont envoyés à Amazon GuardDuty pour une gestion centralisée.
- Les mécanismes établis sont utilisés pour mettre à jour les règles de contrôle des applications, répondre aux événements de cybersécurité et examiner les lacunes en matière de conformité.
- AWS CloudTrail est utilisé pour la journalisation et la surveillance.
- Les événements de sécurité, tels que la connexion de l'utilisateur root, déclenchent des alertes.
- SCPs et les politiques relatives aux points de terminaison VPC établissent les périmètres de données de vos environnements. AWS
- SCPs empêcher les équipes chargées des applications de désactiver les services de sécurité et de journalisation, tels que CloudTrail et AWS Config.
- AWS Config les résultats sont regroupés pour l'ensemble de AWS l'organisation en un seul Compte AWS pour la sécurité.
- Le pack de conformité AWS Config ACSC Essential 8 est activé dans l'ensemble de votre Comptes AWS organisation.

Exemple de charge de travail : lac de données sans serveur

Cette charge de travail en est un exempleThème 1 : Utiliser les services gérés.

Le lac de données utilise Amazon S3 pour le stockage et AWS Lambda pour l'ETL. Ces ressources sont définies dans une AWS Cloud Development Kit (AWS CDK) application. Les modifications apportées au système sont déployées via AWS CodePipeline. Ce pipeline est réservé à l'équipe chargée de l'application. Lorsque l'équipe chargée de l'application effectue une pull request pour le référentiel de code, la règle des deux personnes est utilisée.

Pour cette charge de travail, l'équipe chargée des applications prend les mesures suivantes pour mettre en œuvre les stratégies Essential Eight.

Contrôle des applications

- L'équipe chargée de l'application active la protection Lambda et le scan GuardDuty Lambda dans Amazon Inspector.

- L'équipe chargée de l'application met en œuvre des mécanismes pour inspecter et gérer les résultats d'Amazon Inspector.

Applications de correctifs

- L'équipe chargée de l'application active le scan Lambda dans Amazon Inspector et configure les alertes pour les bibliothèques obsolètes ou vulnérables.
- L'équipe chargée de l'application permet AWS Config de suivre les AWS ressources pour la découverte des actifs.

Restreindre les privilèges administratifs

- Comme décrit dans la Architecture de base section, l'équipe chargée de l'application restreint déjà l'accès aux déploiements de production par le biais d'une règle d'approbation sur son pipeline de déploiement.
- L'équipe chargée de l'application s'appuie sur les solutions de fédération d'identité et de journalisation centralisées décrites dans la Architecture de base section.
- L'équipe chargée de l'application crée un AWS CloudTrail parcours et des CloudWatch filtres Amazon.
- L'équipe chargée de l'application configure les alertes Amazon Simple Notification Service (Amazon SNS) CodePipeline pour les déploiements AWS CloudFormation et les suppressions de piles.

Corrigez les systèmes d'exploitation

- L'équipe chargée de l'application active le scan Lambda dans Amazon Inspector et configure les alertes pour les bibliothèques obsolètes ou vulnérables.

Authentification multifacteur

- L'équipe chargée de l'application s'appuie sur la solution de fédération d'identité centralisée décrite dans la Architecture de base section. Cette solution applique l'authentification MFA, enregistre les authentifications et émet des alertes ou répond automatiquement aux événements MFA suspects.

Sauvegardes régulières

- L'équipe chargée des applications stocke le code, tel que AWS CDK les applications et les fonctions et configurations Lambda, dans un référentiel de code.
- L'équipe chargée de l'application active le versionnement et Amazon S3 Object Lock pour empêcher la suppression ou la modification d'objets.
- L'équipe chargée de l'application s'appuie sur la durabilité intégrée d'Amazon S3 plutôt que de répliquer l'intégralité de son ensemble de données sur un autre Région AWS.
- L'équipe chargée de l'application exécute une copie de la charge de travail dans un autre environnement Région AWS qui répond à ses exigences en matière de souveraineté des données. Ils utilisent les tables globales Amazon DynamoDB et Amazon S3 Cross-Replication pour répliquer automatiquement les données de la région principale vers la région secondaire.

Exemple de charge de travail : service Web conteneurisé

Cette charge de travail en est un exempleThème 2 : Gérer une infrastructure immuable grâce à des pipelines sécurisés.

Le service Web s'exécute sur Amazon ECS et utilise une base de données dans Amazon RDS. L'équipe chargée de l'application définit ces ressources dans un AWS CloudFormation modèle. Les conteneurs sont créés avec EC2 Image Builder et stockés dans Amazon ECR. L'équipe chargée de l'application déploie les modifications apportées au système par le biais AWS CodePipeline de. Ce pipeline est réservé à l'équipe chargée de l'application. Lorsque l'équipe chargée de l'application effectue une pull request pour le référentiel de code, la règle des deux personnes est utilisée.

Pour cette charge de travail, l'équipe chargée des applications prend les mesures suivantes pour mettre en œuvre les stratégies Essential Eight.

Contrôle des applications

- L'équipe chargée de l'application permet de numériser des images de conteneurs Amazon ECR dans Amazon Inspector.
- L'équipe chargée de l'application intègre l'outil de sécurité File Access Policy Daemon (fapolicyd) au pipeline Image Builder EC2 . Pour plus d'informations, voir Implémentation du contrôle des applications sur le site Web de l'ACSC.
- L'équipe chargée de l'application configure la définition de tâche Amazon ECS pour consigner les résultats dans Amazon CloudWatch Logs.
- L'équipe chargée de l'application met en œuvre des mécanismes pour inspecter et gérer les résultats d'Amazon Inspector.

Applications de correctifs

- L'équipe chargée de l'application permet de scanner les images des conteneurs Amazon ECR dans Amazon Inspector et de configurer les alertes pour les bibliothèques obsolètes ou vulnérables.
- L'équipe chargée de l'application automatise ses réponses aux résultats d'Amazon Inspector. Les nouvelles découvertes initient leur pipeline de déploiement via un EventBridge déclencheur Amazon, et CodePipeline constituent la cible.
- L'équipe d'application permet AWS Config de suivre les AWS ressources pour la découverte des actifs.

Restreindre les privilèges administratifs

- L'équipe chargée des applications restreint déjà l'accès aux déploiements de production par le biais d'une règle d'approbation sur son pipeline de déploiement.
- L'équipe chargée des applications s'appuie sur la fédération d'identité de l'équipe cloud centralisée pour la rotation des informations d'identification et la journalisation centralisée.
- L'équipe chargée de l'application crée une CloudTrail trace et des CloudWatch filtres.
- L'équipe chargée de l'application configure les alertes Amazon SNS pour les CodePipeline déploiements et CloudFormation les suppressions de piles.

Corrigez les systèmes d'exploitation

- L'équipe chargée de l'application permet de scanner les images des conteneurs Amazon ECR dans Amazon Inspector et de configurer les alertes pour les mises à jour des correctifs du système d'exploitation.
- L'équipe chargée de l'application automatise sa réponse aux résultats d'Amazon Inspector. Les nouvelles découvertes initient leur pipeline de déploiement par le biais d'un EventBridge déclencheur et CodePipeline constituent la cible.
- L'équipe chargée de l'application s'abonne aux notifications d'événements Amazon RDS afin d'être informée des mises à jour. Ils prennent une décision basée sur les risques avec le propriétaire de leur entreprise quant à savoir s'ils doivent appliquer ces mises à jour manuellement ou laisser Amazon RDS les appliquer automatiquement.
- L'équipe chargée de l'application configure l'instance Amazon RDS en tant que cluster de zones de disponibilité multiples afin de réduire l'impact des événements de maintenance.

Authentification multifacteur

- L'équipe chargée de l'application s'appuie sur la solution de fédération d'identité centralisée décrite dans la Architecture de base section. Cette solution applique l'authentification MFA, enregistre les authentifications et émet des alertes ou répond automatiquement aux événements MFA suspects.

Sauvegardes régulières

- L'équipe chargée de l'application configure AWS Backup pour automatiser la sauvegarde des données de son cluster Amazon RDS.
- L'équipe chargée de l'application stocke les CloudFormation modèles dans un référentiel de code.
- L'équipe chargée de l'application développe un pipeline automatisé pour créer une copie de sa charge de travail dans une autre région et exécuter des tests automatisés (article de AWS blog). Une fois les tests automatisés exécutés, le pipeline détruit la pile. Ce pipeline s'exécute automatiquement une fois par mois et valide l'efficacité des procédures de récupération.

Exemple de charge de travail : logiciel COTS sur Amazon EC2

Cette charge de travail en est un exempleThème 3 : Gérer une infrastructure mutable grâce à l'automatisation.

La charge de travail exécutée sur Amazon EC2 a été créée manuellement à l'aide du AWS Management Console. Les développeurs mettent à jour le système manuellement en se connectant aux EC2 instances et en mettant à jour le logiciel.

Pour cette charge de travail, les équipes du cloud et des applications prennent les mesures suivantes pour mettre en œuvre les stratégies Essential Eight.

Contrôle des applications

- L'équipe cloud configure son pipeline d'AMI centralisé pour installer et configurer l' AWS Systems Manager agent (agent SSM), CloudWatch l'agent et. SELinux Ils partagent l'AMI qui en résulte sur tous les comptes de l'organisation.
- L'équipe cloud utilise des AWS Config règles pour confirmer que toutes les EC2 instances en cours d'exécution sont gérées par Systems Manager et que l'agent SSM, l'agent et CloudWatch l'agent sont SELinux installés.

- L'équipe du cloud envoie CloudWatch les résultats d'Amazon Logs à une solution centralisée de gestion des informations et des événements de sécurité (SIEM) qui s'exécute sur Amazon OpenSearch Service.
- L'équipe chargée de l'application met en œuvre des mécanismes afin d'inspecter et de gérer les résultats provenant d' AWS Config Amazon Inspector et d'Amazon Inspector. GuardDuty L'équipe du cloud met en œuvre ses propres mécanismes pour détecter les résultats manqués par l'équipe chargée de l'application. Pour plus d'informations sur la création d'un programme de gestion des vulnérabilités adapté aux résultats, voir Création d'un programme de gestion des vulnérabilités évolutif sur AWS.

Applications de correctifs

- L'équipe chargée de l'application corrige les instances en fonction des résultats d'Amazon Inspector.
- L'équipe du cloud applique des correctifs à l'AMI de base et l'équipe chargée de l'application reçoit une alerte lorsque cette AMI change.
- L'équipe chargée de l'application restreint l'accès direct à ses EC2 instances en configurant des règles de groupe de sécurité pour autoriser le trafic uniquement sur les ports requis par la charge de travail.
- L'équipe chargée de l'application utilise le gestionnaire de correctifs pour appliquer des correctifs aux instances au lieu de se connecter à des instances individuelles.
- Pour exécuter des commandes arbitraires sur des groupes d' EC2 instances, l'équipe de l'application utilise Run Command.
- Dans les rares cas où l'équipe chargée de l'application a besoin d'un accès direct à une instance, elle utilise le gestionnaire de session. Cette approche d'accès utilise des identités fédérées et enregistre toute activité de session à des fins d'audit.

Restreindre les privilèges administratifs

- L'équipe chargée de l'application configure les règles du groupe de sécurité pour autoriser le trafic uniquement sur les ports requis par la charge de travail. Cela restreint l'accès direct aux EC2 instances Amazon et oblige les utilisateurs à accéder aux EC2 instances via le gestionnaire de session.
- L'équipe chargée des applications s'appuie sur la fédération d'identité de l'équipe cloud centralisée pour la rotation des informations d'identification et la journalisation centralisée.

- L'équipe chargée de l'application crée une CloudTrail trace et des CloudWatch filtres.
- L'équipe chargée de l'application configure les alertes Amazon SNS pour les CodePipeline déploiements et CloudFormation les suppressions de piles.

Corrigez les systèmes d'exploitation

- L'équipe du cloud applique des correctifs à l'AMI de base et l'équipe chargée de l'application reçoit une alerte lorsque cette AMI change. L'équipe chargée de l'application déploie de nouvelles instances à l'aide de cette AMI, puis utilise State Manager, une fonctionnalité de Systems Manager, pour installer le logiciel requis.
- L'équipe chargée de l'application utilise le gestionnaire de correctifs pour appliquer des correctifs aux instances, par exemple pour se connecter à des instances individuelles.
- Pour exécuter des commandes arbitraires sur des groupes d' EC2 instances, l'équipe de l'application utilise Run Command.
- Dans les rares cas où l'équipe chargée de l'application a besoin d'un accès direct, elle utilise le gestionnaire de session.

Authentification multifacteur

- L'équipe chargée de l'application s'appuie sur la solution de fédération d'identité centralisée décrite dans la Architecture de base section. Cette solution applique l'authentification MFA, enregistre les authentifications et émet des alertes ou répond automatiquement aux événements MFA suspects.

Sauvegardes régulières

- L'équipe chargée de l'application crée un AWS Backup plan pour ses EC2 instances et les volumes Amazon Elastic Block Store (Amazon EBS).
- L'équipe chargée de l'application met en œuvre un mécanisme permettant d'effectuer une restauration de sauvegarde manuellement chaque mois.

Ressources

AWS documentation

- AWS Architecture de référence de sécurité (AWS SRA)
- AWS documentation de sécurité
- Pilier de sécurité du AWS Well-Architected Framework

Autres AWS ressources

- AWS Sécurité du cloud
- AWS Cadre d'adoption du cloud (point de vue de la sécurité)

Ressources du Centre australien de cybersécurité

- Les huit éléments essentiels expliqués
- Modèle de maturité Essential Eight
- Guide du processus d'évaluation Essential Eight

Collaborateurs

Les personnes qui ont contribué à ce document incluent :

- James Kingsmill, architecte de solutions senior, architecture des solutions AWS
- Chris Harding, architecte de solutions senior, architecture de AWS solutions
- Jess Modini, architecte de solutions consultatives, AWS architecture de solutions
- Justin Bowden, responsable de l'assurance de la sécurité, assurance AWS de la sécurité
- Rob Powell, architecte de solutions senior, architecture de AWS solutions
- Tony Mihaljevic, architecte cloud senior, services professionnels AWS
- Volker Rath, conseiller principal en sécurité, AWS Global Services Security

Annexe : Huit matrices de contrôles essentielles

Les tableaux suivants relient les stratégies Essential Eight aux conseils de AWS mise en œuvre et aux meilleures pratiques pertinentes du AWS Well-Architected Framework. Pour les contrôles Essential Eight qui ne sont pas applicables dans le AWS Cloud, le tableau inclut un lien vers des directives supplémentaires du Centre australien de cybersécurité (ACSC).

Matrices de contrôle :

- Contrôle des applications
- Applications de correctifs
- Configuration Microsoft Office paramètres de macro
- Renforcement des applications utilisateur
- Restreindre les privilèges administratifs
- Corrigez les systèmes d'exploitation
- Authentification multifacteur
- Sauvegardes régulières

Contrôle des applications

Contrôle Essential Eight	Directives d'impléme ntation	AWS ressources	AWS Conseils Well-Architected
Le contrôle des applications est mis en œuvre sur les postes de travail et les serveurs afin de limiter l'exécution des exécutables, des bibliothèques logiciell es, des scripts, des programmes d'install ation, du HTML compilé, des applicati	Thème 2 : Gérer une infrastructure immuable grâce à des pipelines sécurisés : Mettre en œuvre des API et des pipelines de création de conteneurs	Utilisez EC2 Image Builder et intégrez : • AWS Systems Manager Agent (agent SSM) • Outils de sécurité pour le contrôle des applications, tels que Security Enhanced Linux (SELinux) (GitHub),	SEC06-BP02 Provisionner des calculs à partir d'images renforcées

Contrôle Essential Eight	Directives d'impléme ntation	AWS ressources	AWS Conseils Well-Architected
ons HTML, des applets du panneau de configuration et des pilotes à un ensemble approuvé par l'organisation.		File Access Policy Daemon (fapolicy d) (GitHub) ou OpenSCAP CloudWatch Agent Amazon Partagez AMIs avec l'ensemble de l'organisation Assurez-vous que les équipes chargées des applications font référence aux dernières AMIs Utilisez votre pipeline d'AMI pour la gestion des correctifs	
Microsoftles « règles de blocage recommandées » sont mises en œuvre.	Voir Implémentation du contrôle des applications (site Web de l'ACSC)	Ne s'applique pas	Ne s'applique pas
Microsoftles « règles de blocage des pilotes recommandées » sont mises en œuvre.			

Contrôle Essential Eight	Directives d'impléme ntation	AWS ressources	AWS Conseils Well-Architected
Les ensembles de règles de contrôle des applications sont validés sur une base annuelle ou plus fréquemment.	Thème 8 : Mettre en œuvre des mécanismes pour les processus manuels: Mettre en œuvre un mécanisme pour mettre à jour les politiques de sécurité	Non disponible	SEC01-BP08 Évaluer et implémenter régulièrement de nouveaux services et fonctionnalités de sécurité
Les exécution s autorisées et bloquées sur les postes de travail et les serveurs sont enregistrées de manière centralisée et protégées contre les modifications et suppressions non autorisées, surveillé es pour détecter tout signe de compromis sion et prises en compte lorsque des événements de cybersécurité sont détectés.	Thème 7 : Centralis ation de la journalis ation et de la surveilla nce: Activer la journalisation	Utiliser l' CloudWatch agent pour publier les journaux au niveau du système dans Logs CloudWatch Configurez des alertes pour les GuardDuty résultats Créez un parcours d'organisation dans CloudTrail Protégez les données stockées dans Amazon S3 à l'aide de la gestion des versions et du verrouillage des objets S3	SEC04-BP01 Configurer une journalisation de service et d'applica tion SEC04-BP02 Capturez les journaux, les résultats et les mesures dans des emplacements standardisés

Contrôle Essential Eight	Directives d'implémentation	AWS ressources	AWS Conseils Well-Architected
	Thème 7 : Centralisation de la journalisation et de la surveillance: Mettre en œuvre les meilleures pratiques de sécurité de journalisation	Mettre en œuvre les meilleures pratiques de CloudTrail sécurité Utilisation SCPs pour empêcher les utilisateurs de désactiver les services de sécurité (article de AWS blog) Chiffrez les données du journal dans CloudWatch Logs en utilisant AWS Key Management Service	SEC04-BP01 Configurer une journalisation de service et d'application SEC04-BP02 Capturez les journaux, les résultats et les mesures dans des emplacements standardisés

Contrôle Essential Eight	Directives d'implémentation	AWS ressources	AWS Conseils Well-Architected
	Thème 7 : Centralisation de la journalisation et de la surveillance: Centralisez les journaux	Recevoir CloudTrail les journaux de plusieurs comptes Envoyer des journaux vers un compte d'archivage de journaux Centraliser les CloudWatch journaux dans un compte à des fins d'audit et d'analyse (article de AWS blog) Centralisez la gestion d'Amazon Inspector Création d'un agrégateur à l'échelle de l'organisation dans AWS Config(article de blog)AWS Gestion centralisée de Security Hub Centralisez la gestion de GuardDuty Envisagez d'utiliser Amazon Security Lake	SEC04-BP02 Capturez les journaux, les résultats et les mesures dans des emplacements standardisés

Contrôle Essential Eight	Directives d'implémentation	AWS ressources	AWS Conseils Well-Architected
	Thème 8 : Mettre en œuvre des mécanismes pour les processus manuels: Mettre en œuvre des mécanismes pour examiner et corriger les lacunes en matière de conformité	Envisagez de mettre en œuvre l'automatisation, par exemple des AWS Config règles, afin de réduire le fardeau des processus manuels	OPS02-BP02 Les processus et procédures ont des propriétaires identifiés OPS02-BP03 Les activités opérationnelles ont des propriétaires identifiés responsables de leurs performances OPS02-BP04 Des mécanismes sont en place pour gérer les responsabilités et qui est responsable de quoi

Applications de correctifs

Contrôle Essential Eight	Directives d'implémentation	AWS ressources	AWS Conseils Well-Architected
Une méthode automatisée de découverte des actifs est utilisée au moins tous les quinze jours pour faciliter la détection des actifs en vue des activités d'analyse	Thème 1 : Utiliser les services gérés: Détecter les vulnérabilités Thème 2 : Gérer une infrastructure immuable grâce à des pipelines sécurisés:	Activez Amazon Inspector dans tous les comptes de votre organisation Configurez une analyse améliorée pour les référentiels	SEC06-BP01 Effectuer la gestion des vulnérabilités SEC06-BP05 Automatiser la protection informatique

Contrôle Essential Eight	Directives d’implémentation	AWS ressources	AWS Conseils Well-Architected
des vulnérabilités ultérieures.	Mettre en œuvre une analyse des vulnérabilités Thème 3 : Gérer une infrastructure mutable grâce à l'automatisation: Mettre en œuvre une analyse des vulnérabilités	Amazon ECR à l'aide d'Amazon Inspector Élaborez un programme de gestion des vulnérabilités pour trier et corriger les résultats de sécurité	

Contrôle Essential Eight	Directives d’implémentation	AWS ressources	AWS Conseils Well-Architected
	Thème 7 : Centralisation de la journalisation et de la surveillance: Centralisez les journaux	Recevoir CloudTrail les journaux de plusieurs comptes Envoyer des journaux vers un compte d'archivage de journaux Centraliser les CloudWatch journaux dans un compte à des fins d'audit et d'analyse (article de AWS blog) Centralisez la gestion d'Amazon Inspector Création d'un agrégateur à l'échelle de l'organisation dans AWS Config(article de blog)AWS Gestion centralisée de Security Hub Centralisez la gestion de GuardDuty Envisagez d'utiliser Security Lake	SEC04-BP02 Capturez les journaux, les résultats et les mesures dans des emplacements standardisés

Contrôle Essential Eight	Directives d'impléme ntation	AWS ressources	AWS Conseils Well-Architected
Un scanner de vulnérabilités doté d'une base de données de up-to-date vulnérabilités est utilisé pour les activités d'analyse des vulnérabilités. Un scanner de vulnérabilités est utilisé au moins une fois par jour pour identifier les correctif s ou les mises à jour manquants afin de corriger les failles de sécurité dans les services connectés à Internet.	Thème 1 : Utiliser les services gérés: Détecter les vulnérabi lités Thème 2 : Gérer une infrastructure immuable grâce à des pipelines sécurisés: Mettre en œuvre une analyse des vulnérabi lités Thème 3 : Gérer une infrastructure mutable grâce à l'automat isation: Mettre en œuvre une analyse des vulnérabilités	Activez Amazon Inspector dans tous les comptes de votre organisation Configurez une analyse améliorée pour les référentiels Amazon ECR à l'aide d'Amazon Inspector Élaborez un programme de gestion des vulnérabi lités pour trier et corriger les résultats de sécurité	SEC06-BP01 Effectuer la gestion des vulnérabilités SEC06-BP05 Automatiser la protection informati que

Contrôle Essential Eight	Directives d’implémentation	AWS ressources	AWS Conseils Well-Architected
Un scanner de vulnérabilités est utilisé au moins une fois par semaine pour identifier les correctifs ou les mises à jour manquants pour corriger les failles de sécurité dans les suites de productivité bureautiques, les navigateurs Web et leurs extensions, les clients de messagerie, les logiciels PDF et les produits de sécurité.	Voir Exemple technique : applications de correctifs (site Web de l'ACSC)	Ne s’applique pas	Ne s’applique pas

Contrôle Essential Eight	Directives d'implémentation	AWS ressources	AWS Conseils Well-Architected
Un scanner de vulnérabilités est utilisé au moins tous les quinze jours pour identifier les correctifs ou les mises à jour manquants afin de détecter les failles de sécurité dans d'autres applications.	Thème 1 : Utiliser les services gérés: Détecter les vulnérabilités Thème 2 : Gérer une infrastructure immuable grâce à des pipelines sécurisés: Mettre en œuvre une analyse des vulnérabilités Thème 3 : Gérer une infrastructure mutable grâce à l'automatisation: Mettre en œuvre une analyse des vulnérabilités	Activez Amazon Inspector dans tous les comptes de votre organisation Configurez une analyse améliorée pour les référentiels Amazon ECR à l'aide d'Amazon Inspector Élaborez un programme de gestion des vulnérabilités pour trier et corriger les résultats de sécurité	SEC06-BP01 Effectuer la gestion des vulnérabilités SEC06-BP05 Automatiser la protection informatique

Contrôle Essential Eight	Directives d'implémentation	AWS ressources	AWS Conseils Well-Architected
Les correctifs, les mises à jour ou les mesures d'atténuation prises par les fournisseurs pour corriger les failles de sécurité des services connectés à Internet sont appliqués dans les deux semaines suivant leur publication, ou dans les 48 heures en cas d'exploit.	Thème 1 : Utiliser les services gérés: Détecter les vulnérabilités Thème 2 : Gérer une infrastructure immuable grâce à des pipelines sécurisés: Mettre en œuvre une analyse des vulnérabilités Thème 3 : Gérer une infrastructure mutable grâce à l'automatisation: Mettre en œuvre une analyse des vulnérabilités	Activez Amazon Inspector dans tous les comptes de votre organisation Configurez une analyse améliorée pour les référentiels Amazon ECR à l'aide d'Amazon Inspector Élaborez un programme de gestion des vulnérabilités pour trier et corriger les résultats de sécurité	SEC06-BP01 Effectuer la gestion des vulnérabilités
	Thème 3 : Gérer une infrastructure mutable grâce à l'automatisation: Automatiser l'application des correctifs	Activez le gestionnaire de correctifs dans tous les comptes de votre AWS organisation	SEC06-BP01 Effectuer la gestion des vulnérabilités SEC06-BP05 Automatiser la protection informatique

Contrôle Essential Eight	Directives d’implémentation	AWS ressources	AWS Conseils Well-Architected
Les correctifs, les mises à jour ou les mesures d'atténuation prises par les fournisseurs pour corriger les failles de sécurité des suites de productivité bureautiques, des navigateurs Web et de leurs extensions, des clients de messagerie, des logiciels PDF et des produits de sécurité sont appliqués dans les deux semaines suivant leur publication, ou dans les 48 heures en cas d'exploit.	Voir Exemple technique : applications de correctifs (site Web de l'ACSC)	Ne s’applique pas	Ne s’applique pas

Contrôle Essential Eight	Directives d'implémentation	AWS ressources	AWS Conseils Well-Architected
Les correctifs, les mises à jour ou les mesures d'atténuation prises par les fournisseurs pour corriger les failles de sécurité d'autres applications sont appliqués dans le mois suivant leur publication.	Thème 1 : Utiliser les services gérés: Détecter les vulnérabilités Thème 2 : Gérer une infrastructure immuable grâce à des pipelines sécurisés: Mettre en œuvre une analyse des vulnérabilités Thème 3 : Gérer une infrastructure mutable grâce à l'automatisation: Mettre en œuvre une analyse des vulnérabilités	Activez Amazon Inspector dans tous les comptes de votre organisation Configurez une analyse améliorée pour les référentiels Amazon ECR à l'aide d'Amazon Inspector Élaborez un programme de gestion des vulnérabilités pour trier et corriger les résultats de sécurité	SEC06-BP01 Effectuer la gestion des vulnérabilités
	Thème 3 : Gérer une infrastructure mutable grâce à l'automatisation: Automatiser l'application des correctifs	Activez le gestionnaire de correctifs dans tous les comptes de votre AWS organisation	SEC06-BP01 Effectuer la gestion des vulnérabilités SEC06-BP05 Automatiser la protection informatique

Contrôle Essential Eight	Directives d'implémentation	AWS ressources	AWS Conseils Well-Architected
Les applications qui ne sont plus prises en charge par les fournisseurs sont supprimées.	Thème 8 : Mettre en œuvre des mécanismes pour les processus manuels: Mettre en œuvre des mécanismes pour examiner et corriger les lacunes en matière de conformité	Envisagez AWS Systems Manager d'utiliser l'inventaire pour avoir une meilleure visibilité sur les instances qui exécutent les logiciels requis par votre politique logicielle	SEC06-BP02 Provisionner des calculs à partir d'images renforcées

Configuration Microsoft Office paramètres de macro

Contrôle Essential Eight	Directives d'implémentation	AWS ressources	AWS Conseils Well-Architected
Microsoft Office les macros sont désactivés pour les utilisateurs dont les besoins commerciaux ne sont pas démontrés.	Voir Exemple technique : configurer les paramètres des macros (site Web de l'ACSC)	Ne s'applique pas	Ne s'applique pas
Uniquement Microsoft Office les macros exécutées depuis un environnement sandbox, un emplacement sécurisé ou signées numériquement par un éditeur approuvé			

Contrôle Essential Eight	Directives d’impléme ntation	AWS ressources	AWS Conseils Well-Architected
sont autorisées à s'exécuter.			
Seuls les utilisate urs privilégiés sont chargés de le valider Microsoft Office les macros sont exemptes de code malveillant et peuvent écrire et modifier du contenu dans Trusted Locations.			
Microsoft Office les macros signées numériquement par un éditeur non fiable ne peuvent pas être activées via la barre des messages ou le mode Backstage.			
Microsoft OfficeLa liste des éditeurs de confiance est validée sur une base annuelle ou plus fréquemment.			
Microsoft Office les macros contenues dans les fichiers provenant d'Internet sont bloquées.			

Contrôle Essential Eight	Directives d’implémentation	AWS ressources	AWS Conseils Well-Architected
Microsoft Office l'analyse antivirus des macros est activée.			
Microsoft Office la création de macros est bloquée Win32 Appels d'API.			
Microsoft Office les paramètres de sécurité des macros ne peuvent pas être modifiés par les utilisateurs.			
Autorisé et bloqué Microsoft Office les exécutions de macros sont enregistrées de manière centralisée et protégées contre toute modification ou suppression non autorisées, surveillées pour détecter tout signe de compromission et prises en compte lorsque des événements de cybersécurité sont détectés.			

Renforcement des applications utilisateur

Contrôle Essential Eight	Directives d'implémentation	AWS ressources	AWS Conseils Well-Architected
Les navigateurs Web ne traitent pas Java depuis Internet.	Voir Exemple technique : renforcement des applications utilisateur (site Web de l'ACSC)	Ne s'applique pas	Ne s'applique pas
Les navigateurs Web ne traitent pas les publicités Web provenant d'Internet.			
Internet Explorer 11 est désactivé ou supprimé.			
Microsoft Office est empêché de créer des processus enfants.			
Microsoft Office est empêché de créer du contenu exécutable.			
Microsoft Office est empêché d'injecter du code dans d'autres processus.			
Microsoft Office est configuré pour empêcher l'activation des packages OLE.			

Contrôle Essential Eight	Directives d’implémentation	AWS ressources	AWS Conseils Well-Architected
Les logiciels PDF ne peuvent pas créer de processus enfants.			
conseils de renforcement de l'ACSC ou du fournisseur pour les navigateurs Web, Microsoft Office et le logiciel PDF est implémenté.			
navigateur Web, Microsoft Office et les paramètres de sécurité du logiciel PDF ne peuvent pas être modifiés par les utilisateurs.			
.NET Framework 3,5 (inclut .NET 2.0 et 3.0) est désactivé ou supprimé.			
Windows PowerShell La version 2.0 est désactivée ou supprimée.			
PowerShell est configuré pour utiliser le mode langue contrainte.			

Contrôle Essential Eight	Directives d'impléme ntation	AWS ressources	AWS Conseils Well-Architected
Bloqué PowerShel l les exécution s de scripts sont enregistrées de manière centralis ée et protégées contre les modificat ions et suppressi ons non autorisée s, surveillées pour détecter tout signe de compromission et exécutées lorsque des événements de cybersécurité sont détectés.			

Restreindre les privilèges administratifs

Contrôle Essential Eight	Directives d'impléme ntation	AWS ressources	AWS Conseils Well-Architected
Les demandes d'accès privilégié aux systèmes et aux applications sont validées dès leur première demande.	Thème 4 : Gérer les identités: Implémenter la fédération d'identit és	Obliger les utilisateurs humains à se fédérer avec un fournisse ur d'identité pour accéder à l'aide AWS d'informations d'identif ication temporaires	SEC02-BP04 S'appuyer sur un fournisseur d'identité centralisé SEC03-BP01 Définir les conditions d'accès
L'accès privilégié aux systèmes et aux applications est	Thème 4 : Gérer les identités: Implémenter	Obliger les utilisateurs humains à se fédérer avec un fournisse	SEC02-BP04 S'appuyer sur un

Contrôle Essential Eight	Directives d’implémentation	AWS ressources	AWS Conseils Well-Architected
automatiquement désactivé au bout de 12 mois, sauf revalidation.	la fédération d'identités	ur d'identité pour accéder à l'aide AWS d'informations d'identification temporaires	fournisseur d’identité centralisé
	Thème 4 : Gérer les identités: Rotation des informations d'identification	Exiger que les charges de travail utilisent des rôles IAM pour accéder AWS Suppression automatique des rôles IAM non utilisés Faites régulièrement pivoter les clés d'accès pour les cas d'utilisation nécessitant des informations d'identification à long terme AWS Summit ANZ 2023 : Votre parcours vers des identifiants temporaires dans le cloud (YouTube vidéo)	SEC02-BP05 Contrôler et effectuer régulièrement une rotation des informations d’identification

Contrôle Essential Eight	Directives d’implémentation	AWS ressources	AWS Conseils Well-Architected
L'accès privilégié aux systèmes et aux applications est automatiquement désactivé après 45 jours d'inactivité.	Thème 4 : Gérer les identités: Implémenter la fédération d'identités Thème 4 : Gérer les identités: Rotation des informations d'identification	Obliger les utilisateurs humains à se fédérer avec un fournisseur d'identité pour accéder à l'aide AWS d'informations d'identification temporaires Exiger que les charges de travail utilisent des rôles IAM pour accéder AWS Suppression automatique des rôles IAM non utilisés Faites régulièrement pivoter les clés d'accès pour les cas d'utilisation nécessitant des informations d'identification à long terme AWS Summit ANZ 2023 : Votre parcours vers des identifiants temporaires dans le cloud (YouTube vidéo)	SEC02-BP04 S’appuyer sur un fournisseur d’identité centralisé SEC02-BP05 Contrôler et effectuer régulièrement une rotation des informations d’identification

Contrôle Essential Eight	Directives d'impléme ntation	AWS ressources	AWS Conseils Well-Architected
L'accès privilégié aux systèmes et aux applications est limité à ce qui est nécessaire pour que les utilisateurs et les services puissent accomplir leurs tâches.	Thème 4 : Gérer les identités: appliquer les autorisations du moindre privilège	Protégez vos informati ons d'identification d'utilisateur root et ne les utilisez pas pour les tâches quotidien nes Utilisez IAM Access Analyzer pour générer des politiques de moindre privilège en fonction de l'activité d'accès Vérifiez l'accès public et multicompte aux ressources avec IAM Access Analyzer Utilisez IAM Access Analyzer pour valider vos politiques IAM pour des autorisat ions sécurisées et fonctionnelles Établissez des barrières en matière d'autorisations sur plusieurs comptes Utilisez les limites d'autorisations pour définir le maximum d'autorisations qu'une	SEC01-BP02 Utilisate ur root et propriétés du compte sécurisé SEC03-BP02 Accorder un accès selon le principe du moindre privilège

Contrôle Essential Eight	Directives d'impléme ntation	AWS ressources	AWS Conseils Well-Architected
		politique basée sur l'identité peut accorder Utiliser les condition s des politiques IAM pour restreindre davantage l'accès Vérifiez et supprimez régulièrement les utilisateurs, les rôles, les autorisations, les politiques et les informations d'identif ication non utilisés Commencez avec les politiques AWS gérées et passez aux autorisations du moindre privilège Utiliser la fonctionn alité des ensembles d'autorisations dans IAM Identity Center	
Les comptes privilégi és ne peuvent pas accéder à Internet, au courrier électronique et aux services Web.	Voir Exemple technique : Restreind re les privilèges administratifs (site Web de l'ACSC)	Envisagez de mettre en œuvre un SCP qui empêche tout VPC qui n'a pas encore accès à Internet de l'obtenir	Ne s'applique pas

Contrôle Essential Eight	Directives d’implémentation	AWS ressources	AWS Conseils Well-Architected
Les utilisateurs privilégiés utilisent des environnements d'exploitation privilégiés et non privilégiés distincts.	Thème 5 : Établir un périmètre de données	Mise en place d’un périmètre de données. Envisagez de mettre en œuvre des périmètres de données entre des environnements présentant différentes classifications de données, telles que `OFFICIAL: SENSITIVE` ou`PROTECTED` , ou des niveaux de risque différents, tels que le développement, les tests ou la production.	SEC06-BP03 Réduire la gestion manuelle et l’accès interactif
Les environnements d'exploitation privilégiés ne sont pas virtualisés dans les environnements d'exploitation non privilégiés.			
Les comptes non privilégiés ne peuvent pas se connecter à des environnements d'exploitation privilégiés.			
Les comptes privilégiés (à l'exception des comptes d'administrateur local) ne peuvent pas se connecter à des environnements d'exploitation non privilégiés.			

Contrôle Essential Eight	Directives d’impléme ntation	AWS ressources	AWS Conseils Well-Architected
Just-in-time l'adminis tration est utilisée pour administrer les systèmes et les applications.	Thème 4 : Gérer les identités: Implémenter la fédération d'identit és	Obliger les utilisateurs humains à se fédérer avec un fournisse ur d'identité pour accéder à l'aide AWS d'informations d'identif ication temporaires Implémentez un accès élevé temporair e à vos AWS envir onnements (article de AWS blog)	SEC02-BP04 S’appuyer sur un fournisseur d’identité centralisé
Les activités administratives sont menées par le biais de serveurs de démarrage.	Thème 1 : Utiliser les services gérés Thème 3 : Gérer une infrastructure mutable grâce à l'automatisation: Utiliser l'automat isation plutôt que les processus manuels	Utiliser le gestionna ire de session ou exécuter une commande au lieu d'un accès SSH ou RDP direct	SEC01-BP05 Réduire le périmètre de gestion de la sécurité SEC06-BP03 Réduire la gestion manuelle et l’accès interactif
Les informations d'identification des comptes d'adminis trateurs locaux et des comptes de service sont uniques, imprévisibles et gérées.	Voir Exemple technique : Restreind re les privilèges administratifs (site Web de l'ACSC)	Ne s’applique pas	Ne s’applique pas

Contrôle Essential Eight	Directives d’implémentation	AWS ressources	AWS Conseils Well-Architected
Windows Defender Credential Guard and Windows Defender Remote Credential Guard sont activés.			

Contrôle Essential Eight	Directives d'impléme ntation	AWS ressources	AWS Conseils Well-Architected
L'utilisation de l'accès privilégié est enregistrée de manière centralisée et protégée contre les modifications et suppressions non autorisées, surveillé e pour détecter tout signe de compromis sion et prise en compte lorsque des événements de cybersécurité sont détectés.	Thème 7 : Centralis ation de la journalis ation et de la surveilla nce: Activer la journalisation Thème 7 : Centralis ation de la journalis ation et de la surveilla nce: Centralisez les journaux	Utiliser l' CloudWatch agent pour publier les journaux au niveau du système d'exploitation dans Logs CloudWatc h Activez CloudTrail pour votre organisat ion Centraliser les CloudWatch journaux dans un compte à des fins d'audit et d'analyse (article de AWS blog) Centralisez la gestion d'Amazon Inspector Gestion centralisée de Security Hub Création d'un agrégateur à l'échelle de l'organisation dans AWS Config(article de blog)AWS Centralisez la gestion de GuardDuty Envisagez d'utilise r Amazon Security Lake	SEC04-BP01 Configurer une journalisation de service et d'applica tion SEC04-BP02 Capturez les journaux, les résultats et les mesures dans des emplacements standardisés
Les modifications apportées aux comptes et aux groupes privilégiés sont enregistrées de manière centralisée et protégées contre toute modification ou suppression non autorisées, surveillé es pour détecter tout signe de compromis sion et prises en compte lorsque des événements de cybersécurité sont détectés.			

Contrôle Essential Eight	Directives d'impléme ntation	AWS ressources	AWS Conseils Well-Architected
		Recevoir CloudTrai l les journaux de plusieurs comptes Envoyer des journaux vers un compte d'archivage de journaux	

Corrigez les systèmes d'exploitation

Contrôle Essential Eight	Directives d'impléme ntation	AWS ressources	AWS Conseils Well-Architected
Les correctifs, les mises à jour ou les mesures d'atténua tion prises par les fournisseurs pour corriger les failles de sécurité des systèmes d'exploit ation des services connectés à Internet sont appliqués dans les deux semaines suivant leur publicati on, ou dans les 48 heures en cas d'exploit.	Thème 2 : Gérer une infrastructure immuable grâce à des pipelines sécurisés : Mettre en œuvre des API et des pipelines de création de conteneurs	Utilisez EC2 Image Builder et intégrez : • AWS Systems Manager Agent (agent SSM) • Outils de sécurité pour le contrôle des applications, tels que Security Enhanced Linux (SELinux) (GitHub), File Access Policy Daemon (fapolicy d) (GitHub) ou OpenSCAP • CloudWatch Agent Amazon	SEC01-BP05 Réduire le périmètre de gestion de la sécurité SEC06-BP01 Effectuer la gestion des vulnérabilités SEC06-BP03 Réduire la gestion manuelle et l'accès interactif

Contrôle Essential Eight	Directives d'impléme ntation	AWS ressources	AWS Conseils Well-Architected
		Partagez AMIs avec l'ensemble de l'organisation Assurez-vous que les équipes chargées des applications font référence aux dernières AMIs Utilisez votre pipeline d'AMI pour la gestion des correctifs	
	Thème 1 : Utiliser les services gérés: Activer l'application de correctifs Thème 3 : Gérer une infrastructure mutable grâce à l'automat isation: Automatis er l'application des correctifs	Activez le gestionna ire de correctifs dans tous les comptes de votre AWS organ isation	SEC06-BP01 Effectuer la gestion des vulnérabilités SEC06-BP05 Automatiser la protection informati que

Contrôle Essential Eight	Directives d'impléme ntation	AWS ressources	AWS Conseils Well-Architected
Les correctifs, les mises à jour ou les mesures d'atténua tion prises par les fournisseurs pour remédier aux failles de sécurité des systèmes d'exploit ation des postes de travail, des serveurs et des appareils réseau sont appliqués dans les deux semaines suivant leur publication, ou dans les 48 heures en cas d'exploit.	Thème 2 : Gérer une infrastructure immuable grâce à des pipelines sécurisés : Mettre en œuvre des API et des pipelines de création de conteneurs	Utilisez EC2 Image Builder et intégrez : • AWS Systems Manager Agent (agent SSM) • Outils de sécurité pour le contrôle des applications, tels que Security Enhanced Linux (SELinux) (GitHub), File Access Policy Daemon (fapolicy d) (GitHub) ou OpenSCAP • CloudWatch Agent Amazon Partagez AMIs avec l'ensemble de l'organisation Assurez-vous que les équipes chargées des applications font référence aux dernières AMIs Utilisez votre pipeline d'AMI pour la gestion des correctifs	SEC01-BP05 Réduire le périmètre de gestion de la sécurité SEC06-BP01 Effectuer la gestion des vulnérabilités SEC06-BP02 Provisionner des calculs à partir d'images renforcées

Contrôle Essential Eight	Directives d’implémentation	AWS ressources	AWS Conseils Well-Architected
	Thème 1 : Utiliser les services gérés: Activer l'application de correctifs Thème 3 : Gérer une infrastructure mutable grâce à l'automatisation: Automatiser l'application des correctifs	Activez le gestionnaire de correctifs dans tous les comptes de votre AWS organisation	SEC06-BP01 Effectuer la gestion des vulnérabilités SEC06-BP05 Automatiser la protection informatique

Contrôle Essential Eight	Directives d'impléme ntation	AWS ressources	AWS Conseils Well-Architected
Un scanner de vulnérabilités est utilisé au moins une fois par jour pour identifier les correctif s ou les mises à jour manquants afin de remédier aux failles de sécurité des systèmes d'exploit ation des services connectés à Internet.	Thème 1 : Utiliser les services gérés: Détecter les vulnérabi lités Thème 2 : Gérer une infrastructure immuable grâce à des pipelines sécurisés: Mettre en œuvre une analyse des vulnérabi lités Thème 3 : Gérer une infrastructure mutable grâce à l'automat isation: Mettre en œuvre une analyse des vulnérabilités	Activez Amazon Inspector dans tous les comptes de votre organisation Configurez une analyse améliorée pour les référentiels Amazon ECR à l'aide d'Amazon Inspector Élaborez un programme de gestion des vulnérabi lités pour trier et corriger les résultats de sécurité	SEC01-BP05 Réduire le périmètre de gestion de la sécurité SEC06-BP01 Effectuer la gestion des vulnérabilités SEC06-BP02 Provisionner des calculs à partir d'images renforcées
Un scanner de vulnérabilités est utilisé au moins une fois par semaine pour identifier les correctifs ou les mises à jour manquants afin de remédier aux failles de sécurité des systèmes d'exploit ation des postes de travail, des serveurs et des périphériques réseau.			

Contrôle Essential Eight	Directives d'implémentation	AWS ressources	AWS Conseils Well-Architected
La dernière version, ou la version précédente, des systèmes d'exploitation est utilisée pour les postes de travail, les serveurs et les périphériques réseau. Les systèmes d'exploitation qui ne sont plus pris en charge par les fournisseurs sont remplacés.	Thème 2 : Gérer une infrastructure immuable grâce à des pipelines sécurisés: Mettre en œuvre une analyse des vulnérabilités	Utilisez EC2 Image Builder et intégrez : • AWS Systems Manager Agent (agent SSM) • Outils de sécurité pour le contrôle des applications, tels que Security Enhanced Linux (SELinux) (GitHub), File Access Policy Daemon (fapolicyd) (GitHub) ou OpenSCAP • CloudWatch Agent Amazon Partagez AMIs avec l'ensemble de l'organisation Assurez-vous que les équipes chargées des applications font référence aux dernières AMIs Utilisez votre pipeline d'AMI pour la gestion des correctifs	SEC01-BP05 Réduire le périmètre de gestion de la sécurité SEC06-BP01 Effectuer la gestion des vulnérabilités SEC06-BP02 Provisionner des calculs à partir d'images renforcées

Authentification multifacteur

Contrôle Essential Eight	Directives d'implémentation	AWS ressources	AWS Conseils Well-Architected
L'authentification multifactorielle est utilisée par les utilisateurs d'une organisation s'ils s'authentifient auprès des services Internet de leur organisation.	Thème 4 : Gérer les identités: Implémenter la fédération d'identités	Obliger les utilisateurs humains à se fédérer avec un fournisseur d'identité pour accéder à l'aide AWS d'informations d'identification temporaires Mettez en place un accès surélevé temporaire à vos AWS environnements	SEC02-BP04 S'appuyer sur un fournisseur d'identité centralisé
	Thème 4 : Gérer les identités: Appliquer la MFA	Exiger le MFA pour l'utilisateur root Exiger le MFA via AWS IAM Identity Center Envisagez d'exiger le MFA pour les actions d'API spécifiques au service	SEC02-BP01 Utiliser des mécanismes de connexion robustes
L'authentification multifactorielle est utilisée par les utilisateurs d'une entreprise s'ils s'authentifient auprès de services Internet tiers qui	Voir Implémentation de l'authentification multifactorielle (site Web de l'ACSC)	Ne s'applique pas	Ne s'applique pas

Contrôle Essential Eight	Directives d’impléme ntation	AWS ressources	AWS Conseils Well-Architected
traitent, stockent ou communiquent les données sensibles de leur organisation.			
L'authentification multifactorielle (lorsqu'elle est disponible) est utilisée par les utilisateurs d'une entreprise s'ils s'authentifient auprès de services Internet tiers qui traitent, stockent ou communiquent les données non sensibles de leur organisation.			
L'authentification multifactorielle est activée par défaut pour les utilisateurs n'appartenant pas à une organisation (mais les utilisateurs peuvent choisir de se désinscrire) s'ils s'authentifient auprès des services Internet d'une organisation.			

Contrôle Essential Eight	Directives d'impléme ntation	AWS ressources	AWS Conseils Well-Architected
L'authentification multifactorielle est utilisée pour authentif ier les utilisate urs privilégiés des systèmes.	Thème 4 : Gérer les identités: Implémenter la fédération d'identit és	Obliger les utilisateurs humains à se fédérer avec un fournisse ur d'identité pour accéder à l'aide AWS d'informations d'identif ication temporaires Mettez en place un accès surélevé temporaire à vos AWS environnements	SEC02-BP04 S'appuyer sur un fournisseur d'identité centralisé
	Thème 4 : Gérer les identités: Appliquer la MFA	Exiger le MFA pour l'utilisateur root Exiger le MFA via IAM Identity Center Envisagez d'exiger le MFA pour les actions d'API spécifiques au service	SEC02-BP01 Utiliser des mécanismes de connexion robustes
L'authentification multifactorielle est utilisée pour authentif ier les utilisateurs accédant à des référentiels de données importants.	Thème 4 : Gérer les identités: Appliquer la MFA	Envisagez d'exiger le MFA pour les actions d'API spécifiques au service	SEC02-BP01 Utiliser des mécanismes de connexion robustes

Contrôle Essential Eight	Directives d’implémentation	AWS ressources	AWS Conseils Well-Architected
L'authentification multifactorielle résiste à l'usurpation d'identité par un vérificateur et utilise soit quelque chose que les utilisateurs possèdent et connaissent, soit quelque chose que les utilisateurs possèdent qui est déverrouillé par quelque chose qu'ils connaissent ou sont.	Voir Implémentation de l'authentification multifactorielle (site Web de l'ACSC)	Ne s’applique pas	Ne s’applique pas

Contrôle Essential Eight	Directives d'impléme ntation	AWS ressources	AWS Conseils Well-Architected
Les authentifications multifactorielles réussies ou non sont enregistrées de manière centralisée et protégées contre les modifications et suppressions non autorisées, surveillé es pour détecter les signes de compromis sion et prises en compte lorsque des événements de cybersécurité sont détectés.	Thème 7 : Centralis ation de la journalis ation et de la surveilla nce: Activer la journalisation Thème 7 : Centralis ation de la journalis ation et de la surveilla nce: Centralisez les journaux	Centraliser les CloudWatch journaux dans un compte à des fins d'audit et d'analyse (article de AWS blog) Centralisez la gestion d'Amazon Inspector Gestion centralisée de Security Hub Création d'un agrégateur à l'échelle de l'organisation dans AWS Config(article de blog)AWS Centralisez la gestion de GuardDuty Envisagez d'utiliser Security Lake Recevoir CloudTrai l les journaux de plusieurs comptes Envoyer des journaux vers un compte d'archivage de journaux	SEC04-BP01 Configurer une journalisation de service et d'applica tion SEC04-BP02 Capturez les journaux, les résultats et les mesures dans des emplacements standardisés

Sauvegardes régulières

Contrôle Essential Eight	Directives d'implémentation	AWS ressources	AWS Conseils Well-Architected
Les sauvegardes des données, des logiciels et des paramètres de configuration importants sont effectuées et conservées de manière coordonnée et résiliente conformément aux exigences de continuité des activités.	Thème 6 : Automatiser les sauvegardes: Automatisez la sauvegarde et la restauration des données	Implémenter la sauvegarde des données sur AWS Automatisez la sauvegarde des données à grande échelle (article de AWS blog)	REL09-BP01 Identifier et sauvegarder toutes les données qui doivent être sauvegardées, ou reproduire les données à partir de sources REL09-BP02 Sécuriser et chiffrer les sauvegardes REL09-BP03 Effectuer automatiquement la sauvegarde des données
La restauration des systèmes, des logiciels et des données importantes à partir de sauvegardes est testée de manière coordonnée dans le cadre d'exercices de reprise après sinistre.	Thème 6 : Automatiser les sauvegardes: Automatisez la sauvegarde et la restauration des données Thème 6 : Automatiser les sauvegardes: Mettez en œuvre la gouvernance pour l'ensemble de vos AWS Backup résultats	Automatisez la validation de la récupération des données avec AWS Backup (article de AWS blog) Utilisez AWS Backup Audit Manager pour vérifier la conformité de vos AWS Backup politiques	REL09-BP04 Effectuer une récupération périodique des données pour vérifier l'intégrité et les processus de sauvegarde

Contrôle Essential Eight	Directives d’implémentation	AWS ressources	AWS Conseils Well-Architected
Les comptes non privilégiés et les comptes privilégiés (à l'exception des administrateurs de sauvegarde) ne peuvent pas accéder aux sauvegardes.	Thème 6 : Automatiser les sauvegardes: Mettez en œuvre la gouvernance pour l'ensemble de vos AWS Backup résultats	Les 10 meilleures pratiques de sécurité pour sécuriser les sauvegardes dans AWS (article de AWS blog) Utilisez AWS Backup Vault Lock pour améliorer la sécurité de vos coffres-forts de sauvegarde Utilisez AWS Backup Audit Manager pour vérifier la conformité de vos AWS Backup politiques	SEC08-BP04 Appliquer le contrôle d’accès
Les comptes non privilégiés et les comptes privilégiés (à l'exception des comptes Backup Break Glass) ne peuvent pas modifier ou supprimer des sauvegardes.			

Avis

Il incombe aux clients de procéder à une évaluation indépendante des informations contenues dans le présent document. Ce document : (a) est fourni à titre informatif uniquement, (b) représente les offres de AWS produits et les pratiques actuelles, qui sont susceptibles d'être modifiées sans préavis, et (c) ne crée aucun engagement ni aucune assurance de la part de AWS ses filiales, fournisseurs ou concédants de licence. AWS les produits ou services sont fournis « tels quels » sans garanties, déclarations ou conditions d'aucune sorte, qu'elles soient explicites ou implicites. Les responsabilités et obligations AWS de ses clients sont régies par AWS des accords, et ce document ne fait partie d'aucun accord conclu entre AWS et ses clients et ne les modifie pas.

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
Mises à jour des meilleures pratiques	Nous avons mis à jour ce guide afin de refléter les meilleures pratiques les plus récentes en matière de sécurité du AWS Well-Arch itected Framework.	6 novembre 2024
Publication initiale	—	20 octobre 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 locale vers Oracle sur une EC2 instance du 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 la synchronisation des bases de données source et cible est maintenue, mais seule la base de données source gère les transactions provenant de la connexion d'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 AWS Identity and Access Management (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

Voir base de données de gestion de configuration.

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 is commonly described as a pipeline. CI/CDpeut 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 AWS Identity and Access Management (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 pipeline CI/CD, 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.

épopée

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 clics 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 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 au fur et à mesure de son fonctionnement. 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 avec le service de migration AWS 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

Voir 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, évaluer, prévenir ou 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 ne peuvent accéder au contenu d'un compartiment S3 que par le biais d'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.

politique

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. Pour plus d'informations, veuillez consulter Enabling data persistence in microservices.

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 capable d'effectuer AWS des actions et d'accéder à des 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 des 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).

CHIFFON

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 la section 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 relatif au 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 AWS de sécurité. Parmi les actions de réponse automatique, citons la modification d'un groupe de sécurité VPC, l'application de correctifs à une EC2 instance Amazon 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, consultez la section 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

balises

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.