Transition vers le multiple Comptes AWS

AWS Directives prescriptives

AWS Directives prescriptives: Transition vers le multiple Comptes AWS

Table of Contents

Transition vers le multiple Comptes AWS

Amazon Web Services (contributeurs)

Novembre 2024 (historique du document)

De nombreuses entreprises commencent leur parcours en utilisant un seul compte Amazon Web Services (AWS). Plusieurs rôles au sein d'une entreprise utilisent ce compte pour gérer l'activité. Les ingénieurs développent du code, le déploient dans des environnements de développement et de test et promeuvent les modifications apportées à la production. Les chefs de produit interrogent les sources de données pour recueillir des informations sur les performances métier. L'équipe commerciale organise des démonstrations depuis l'environnement de production pour attirer de nouveaux clients. L'équipe financière surveille les dépenses liées au cloud depuis la AWS Billing console.

Lorsque tous ces rôles distincts n'en utilisent qu'un Compte AWS, il peut s'avérer difficile d'appliquer les meilleures pratiques de sécurité qui consistent à appliquer les autorisations du moindre privilège, ce qui signifie que vous n'accordez que les autorisations minimales nécessaires pour effectuer le travail. À un certain stade du développement d'une start-up, quelqu'un se posera la question suivante : Tous nos ingénieurs doivent-ils avoir accès à la production ? La réponse est presque toujours non, mais de nombreuses entreprises ont du mal à transformer leur environnement à compte unique existant en un environnement à comptes multiples sans ralentir leur activité.

Ce guide présente les bonnes pratiques pour vous aider à passer d'un environnement à compte unique à un environnement à comptes multiples. Il décrit les décisions que vous devez prendre concernant la migration des comptes, la gestion des utilisateurs, la mise en réseau, la sécurité et l'architecture. Il vise à vous aider à réussir avec un minimum ou aucun temps d'arrêt pour votre activité et vos opérations quotidiennes. Ce guide met l'accent sur les fonctionnalités suivantes lorsque vous passez d'un environnement à compte unique Compte AWS à un environnement multicompte :

- Gestion des identités et contrôle d'accès
- Gestion des autorisations et des accès
- La connectivité réseau
- Réponse aux incidents de sécurité
- Sauvegardes
- Migration de compte

- Migration des ressources
- Considérations sur la facturation

Pour plus d'informations sur les capacités, consultez Cloud Foundation sur AWS.

Ce guide est aligné sur les ressources existantes liées à ce sujet, notamment le AWS Startup Security Baseline (AWS SSB), le livre blanc Organizing Your AWS Environment Using Multiple Accounts, l'architecture de référence de AWS sécurité (AWS SRA) et le livre blanc Establishing Your Cloud Foundation on. AWS Vous devez continuer à utiliser ces ressources pour obtenir des conseils plus spécifiques qui ne sont pas abordés dans ce guide.

Public visé

Ce guide est particulièrement adapté aux entreprises qui souhaitent ou doivent passer à plusieurs Comptes AWS. Pour les startups, ce besoin survient généralement lorsque vous avez trouvé un produit adapté au marché, que vous avez levé un cycle de financement et que vous commencez à recruter des disciplines d'ingénierie distinctes, telles que l'infrastructure, les opérations de développement (DevOps) ou la sécurité.

Même si votre entreprise n'est pas prête à effectuer cette transition, vous pouvez toujours utiliser ce guide pour comprendre les décisions qui doivent être prises pendant la transition et commencer votre préparation.

Objectifs de la transition vers une architecture multi-comptes

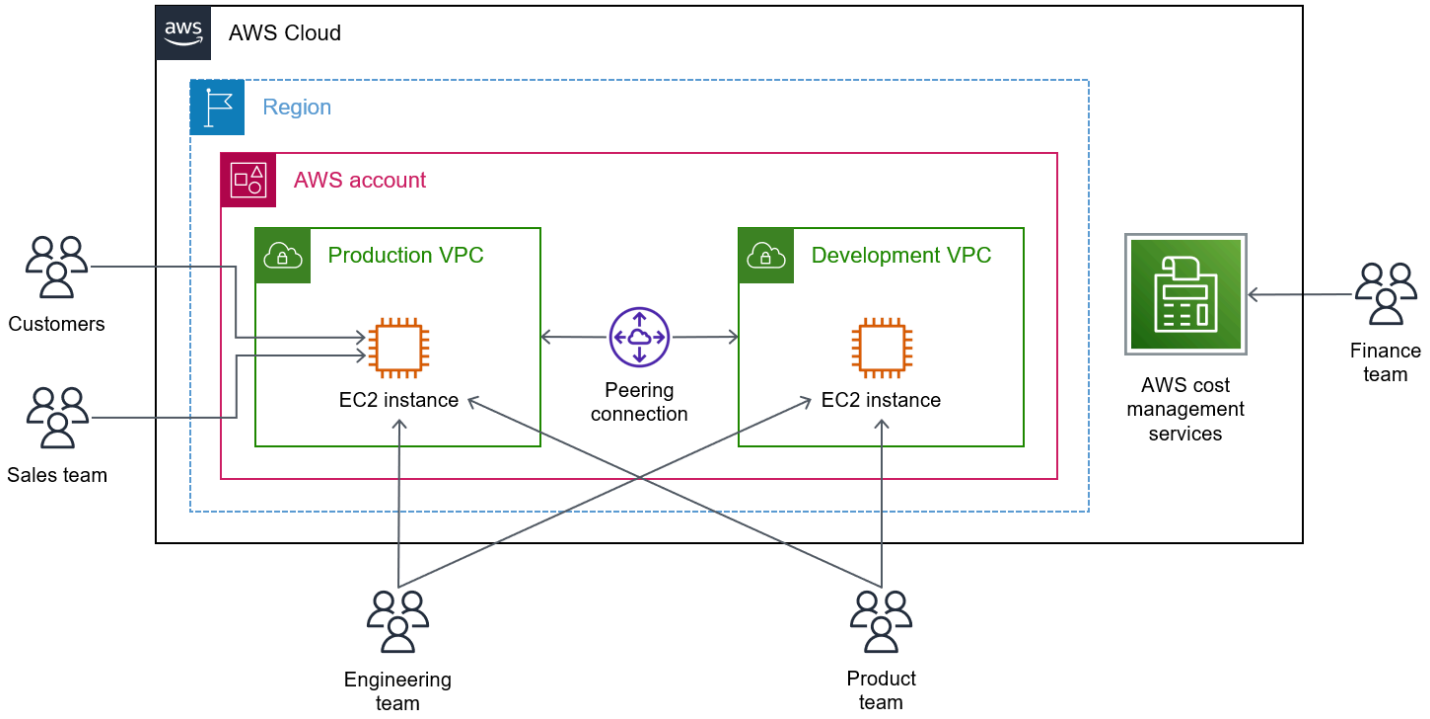
La transition vers une architecture à comptes multiples est généralement motivée par un besoin métier d'un ou de plusieurs des avantages suivants :

- Regroupement des charges de travail en fonction de l'objectif métier ou de la propriété
- Application de contrôles de sécurité distincts par environnement
- Limitation de l'accès aux données sensibles
- Promotion de l'innovation et de l'agilité
- Limitation de la portée de l'impact des effets indésirables
- Prise en charge de plusieurs modèles d'exploitation informatiques
- Gestion des coûts
- Distribution de Service AWS quotas et limites de taux de demandes d'API

Pour plus d'informations sur les nombreux avantages de l'utilisation d'une architecture multi-comptes, consultez Organiser votre AWS environnement à l'aide de plusieurs comptes (AWS livre blanc) et Directives pour configurer un environnement bien conçu (documentation).AWS Control Tower

Exemple d'architecture à compte unique

Comme point de départ, il est courant que les start-up ou les petites entreprises utilisent un seul cloud privé virtuel () Région AWS et disposent de deux clouds privés virtuels (VPCs) connectés par le biais d'un peering VPC. Chaque VPC contient des ressources de calcul, telles que des instances Amazon Elastic Compute Cloud EC2 (Amazon). L'équipe d'ingénierie développe le code directement dans le VPC de développement. L'équipe de produit examine les modifications, puis l'équipe d'ingénierie promeut manuellement les modifications apportées au VPC de production. L'équipe financière a accès au Compte AWS afin de pouvoir consulter la AWS Billing and Cost Management console.



Voici quelques exemples de difficultés qu'une entreprise peut rencontrer dans cet environnement :

- Un ingénieur a supprimé par erreur des données de production alors qu'il pensait accéder à une base de données de développement.
- Une démonstration commerciale a été affectée lorsqu'un déploiement de production a pris plus de temps que prévu.
- Lorsque le code de développement était testé en charge, le VPC de production est devenu lent et a généré des messages d'erreur concernant la limitation.
- L'équipe financière ne peut pas différencier les coûts des environnements de production et de développement.
- Le PDG craint que certains sous-traitants offshore récemment embauchés aient accès aux données des clients par le biais du VPC de production.
- L'équipe financière ne peut pas interdire l'accès à des informations spécifiques Services AWS susceptibles d'entraîner des coûts élevés.

L'adoption d'une stratégie multi-comptes permet de relever tous ces défis en utilisant le compartimentage Comptes AWS pour séparer les charges de travail et les accès.

Cadre de base et responsabilités en matière de sécurité pour la transition vers une architecture à comptes multiples

Les informations et les bonnes pratiques contenues dans ce guide sont conçues pour compléter les recommandations AWS existantes en matière d'infrastructure et de sécurité. Lorsque vous passez d'un compte unique Compte AWS à un compte multiple Comptes AWS, il est important de vous assurer que votre nouvelle architecture multi-comptes est conforme aux principes du AWS Well-Architected Framework et du Cloud Foundation. Cela vous permet de créer et d'exploiter un environnement conçu pour la sécurité, les performances et la résilience, tout en respectant les exigences de gouvernance et les AWS meilleures pratiques.

AWS Framework Well-Architected

AWS Well-Architected Framework vous aide à créer une infrastructure sécurisée, performante, résiliente et efficace pour les applications et les charges de travail. Ce guide s'aligne sur les piliers Excellence opérationnelle, Sécurité et Fiabilité de ce cadre. Cela vous permet de répondre à vos exigences commerciales et réglementaires en suivant les AWS recommandations actuelles.

Vous pouvez évaluer votre adhésion aux bonnes pratiques Well-Architected à l'aide de AWS Well-Architected Tool dans votre Compte AWS.

Cloud Foundation sur AWS

Establishing Your Cloud Foundation on AWS (AWS livre blanc) fournit des conseils qui vous aident à adapter votre AWS environnement aux besoins de votre entreprise. En utilisant une approche basée sur les capacités, vous pouvez créer un environnement pour déployer, exploiter et gérer vos charges de travail. Vous pouvez également améliorer les capacités pour étendre votre environnement à mesure que vos besoins évoluent et que vous déployez des charges de travail supplémentaires dans le cloud. Pour plus d'informations sur les 30 fonctionnalités définies par AWS, consultez la section Capacités. Ce guide inclut les bonnes pratiques pour mettre en œuvre les capacités initiales dans l'ordre prévu.

Vous pouvez adopter et mettre en œuvre des capacités en fonction de vos besoins opérationnels et de gouvernance. À mesure que vos exigences métier évoluent, l'approche basée sur les capacités peut être utilisée comme mécanisme pour vérifier que votre environnement cloud est prêt à prendre en charge vos charges de travail et à être mis à l'échelle selon les besoins. Cette approche vous

permet d'établir en toute confiance votre environnement cloud pour vos générateurs et votre entreprise.

Gestion des identités et contrôle d'accès pour la transition vers une architecture à comptes multiples

Cette première étape lors de la transition vers une architecture à comptes multiples consiste à configurer votre nouvelle structure de compte au sein d'une organisation. Vous pouvez ensuite ajouter des utilisateurs et configurer leur accès aux comptes. Cette section décrit les approches permettant de gérer l'accès humain à plusieurs Comptes AWS.

Cette section se compose des tâches suivantes :

- Configurer une organisation
- Création d'une zone de destination
- Ajouter des unités d'organisation
- Ajouter des utilisateurs d'origine
- Gérer les comptes membres

Configurer une organisation

Lorsque vous en avez plusieurs Comptes AWS, vous pouvez gérer ces comptes de manière logique par le biais d'une organisation dans AWS Organizations. Un compte dans AWS Organizations est une norme Compte AWS qui contient vos AWS ressources et les identités qui peuvent accéder à ces ressources. Une organisation est une entité qui consolide les vôtres Comptes AWS afin que vous puissiez les administrer en tant qu'unité unique.

Lorsque vous utilisez un compte pour créer une organisation, ce compte devient le compte de gestion (également appelé compte payeur ou compte root) pour l'organisation. Une organisation ne peut avoir qu'un seul compte de gestion. Lorsque vous ajoutez des informations supplémentaires Comptes AWS à l'organisation, elles deviennent des comptes membres.

> **Note**
>
> Chacun possède Compte AWS également une seule identité appelée utilisateur root. Vous pouvez vous connecter en tant qu'utilisateur root avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Toutefois, il est vivement recommandé de ne pas utiliser l'utilisateur root pour vos tâches quotidiennes, y compris pour les tâches administratives. Pour plus d'informations, veuillez consulter Utilisateur root Compte AWS.

Nous recommandons également de centraliser l'accès root pour les comptes membres et de supprimer les informations d'identification de l'utilisateur root des comptes membres de votre organisation.

Vous organisez les comptes dans une structure arborescente hiérarchique qui comprend la racine de l'organisation, les unités organisationnelles (OUs) et les comptes des membres. La racine est le conteneur parent pour tous les comptes de votre organisation. Une unité d'organisation (UO) est un conteneur pour comptes au sein de la racine. Une UO peut contenir d'autres comptes OUs ou des comptes de membres. Une unité d'organisation ne peut posséder qu'un seul parent et chaque compte peut être un membre d'une seule unité d'organisation. Pour plus d'informations, consultez Terminologie et concepts (AWS Organizations documentation).

Une politique de contrôle des services (SCP) spécifie les services et les actions que les utilisateurs et les rôles peuvent utiliser. SCPs sont similaires aux politiques d'autorisation AWS Identity and Access Management (IAM) sauf qu'elles n'accordent pas d'autorisations. SCPs Définissez plutôt les autorisations maximales. Lorsque vous attachez une politique à l'un des nœuds de la hiérarchie, elle s'applique à tous les comptes OUs et de ce nœud. Par exemple, si vous appliquez une politique à la racine, elle s'applique à tous les OUscomptes de l'organisation, et si vous appliquez une politique à une unité d'organisation, elle ne s'applique qu'aux comptes OUs et de l'unité d'organisation cible.

Une politique de contrôle des ressources (RCP) permet de contrôler de manière centralisée les autorisations maximales disponibles pour les ressources de votre organisation. RCPs vous aider à vous assurer que les ressources de votre compte respectent les directives de contrôle d'accès de votre organisation.

Vous pouvez utiliser la AWS Organizations console pour visualiser et gérer de manière centralisée tous vos comptes au sein d'une organisation. L'un des avantages de l'utilisation d'une organisation est que vous pouvez recevoir une facture consolidée indiquant tous les frais associés aux comptes de gestion et aux comptes membres. Pour plus d'informations, consultez la section Facturation consolidée (AWS Organizations documentation).

Bonnes pratiques

- N'utilisez pas une organisation existante Compte AWS pour créer une organisation. Commencez par un nouveau compte, qui devient votre compte de gestion pour l'organisation. Les opérations privilégiées peuvent être effectuées dans le compte de gestion d'une organisation SCPs et RCPs ne s'appliquent pas au compte de gestion. C’est pourquoi vous devez limiter les ressources et

données cloud contenues dans le compte de gestion à celles qui doivent être gérées dans le compte de gestion.

- Limitez l'accès au compte de gestion aux seules personnes qui ont besoin d'approvisionner de nouveaux comptes Comptes AWS et d'administrer l'organisation.
- SCPs À utiliser pour définir les autorisations maximales pour la racine, les unités organisationnelles et les comptes des membres. SCPs ne peut pas être directement appliqué au compte de gestion.
- RCPs À utiliser pour définir les autorisations maximales pour les ressources dans les comptes des membres. RCPsne peut pas être directement appliqué au compte de gestion.
- Respectez les meilleures pratiques pour AWS Organizations (AWS Organizations documentation).

Création d'une zone de destination

Une zone d'atterrissage est un AWS environnement multi-comptes bien conçu qui constitue un point de départ à partir duquel vous pouvez déployer des charges de travail et des applications. Elle sert de référence pour démarrer avec l'architecture à comptes multiples, la gestion des identités et des accès, la gouvernance, la sécurité des données, la conception de réseaux et la journalisation. AWS Control Tower est un service qui simplifie la maintenance et la gouvernance d'un environnement à comptes multiples en proposant des barrières de protection automatisées. En général, vous configurez une zone AWS Control Tower d'atterrissage unique qui gère l'ensemble de votre environnement Régions AWS. AWS Control Tower fonctionne en orchestrant les autres Services AWS au sein de votre compte. Pour plus d'informations, voir Que se passe-t-il lorsque vous configurez une zone d'atterrissage (AWS Control Tower documentation).

Lorsque vous configurez une zone d'atterrissage avec AWS Control Tower, vous identifiez trois comptes partagés : le compte de gestion, le compte d'archivage des journaux et le compte d'audit. Pour plus d'informations, voir Quels sont les comptes partagés (AWS Control Tower documentation). Pour le compte de gestion, vous devez utiliser un compte existant qui n'héberge aucune charge de travail pour configurer la zone de destination. Pour les comptes d'archivage des journaux et d'audit, vous pouvez choisir de réutiliser Comptes AWS les comptes existants ou AWS Control Tower de les créer pour vous.

Pour obtenir des instructions sur la configuration de votre zone AWS Control Tower d'atterrissage, consultez Getting started (AWS Control Tower documentation).

Bonnes pratiques

- Adhérez aux meilleures pratiques des principes de conception pour votre stratégie multi-comptes (AWS livre blanc).
- Respectez les meilleures pratiques pour AWS Control Tower les administrateurs (AWS Control Tower documentation).
- Créez votre zone de landing zone dans celle Région AWS qui héberge la majorité de vos charges de travail.

> **Important**
>
> Si vous décidez de modifier cette région après avoir déployé votre zone d'atterrissage, vous avez besoin de l'assistance de AWS Support la zone d'atterrissage et vous devez la mettre hors service. Cette pratique n'est pas recommandée.

- Lorsque vous déterminez quelles régions AWS Control Tower seront gouvernées, sélectionnez uniquement les régions dans lesquelles vous prévoyez de déployer immédiatement des charges de travail. Vous pouvez modifier ces régions ou en ajouter d'autres ultérieurement. S'il AWS Control Tower gouverne une région, il déploiera ses garde-fous détectives dans cette région en tant que. AWS Config Rules
- Après avoir déterminé quelles régions AWS Control Tower seront gouvernées, refusez l'accès à toutes les régions non gouvernées. Cela permet de garantir que vos charges de travail et vos développeurs ne peuvent utiliser que des Régions AWS approuvées. Ceci est mis en œuvre en tant que politique de contrôle des services (SCP) dans l'organisation. Pour plus d'informations, voir Configurer le contrôle de Région AWS refus (AWS Control Tower documentation).
- Lorsque vous configurez votre zone d'atterrissage dans AWS Control Tower, nous vous recommandons de renommer OUs les comptes suivants :
  - Nous vous recommandons de renommer l'UO Sécurité en Security_Prod pour indiquer que cette UO sera utilisée pour des Comptes AWS liés à la sécurité de la production.
  - Nous vous recommandons d'autoriser la création AWS Control Tower d'une unité d'organisation supplémentaire, puis de la renommer Sandbox en Workloads. Dans la section suivante, vous allez créer des éléments supplémentaires OUs au sein de l'unité d'organisation des charges de travail, que vous utiliserez pour organiser votre Comptes AWS.
  - Nous vous recommandons de renommer la journalisation centralisée Compte AWS de Log Archive en log-archive-prod.

  - Nous vous recommandons de renommer le compte d'audit d'Audit en security-tooling-prod.
- Pour aider à prévenir la fraude, il AWS faut Comptes AWS disposer d'un historique d'utilisation avant de pouvoir les ajouter à une zone d' AWS Control Tower atterrissage. Si vous utilisez une nouvelle instance Compte AWS sans historique d'utilisation, dans le nouveau compte, vous pouvez lancer une instance Amazon Elastic Compute Cloud (Amazon EC2) qui ne figure pas dans le niveau AWS gratuit. Laissez l'instance s'exécuter pendant quelques minutes, puis résiliez-la.

Ajouter des unités d'organisation

La mise en place d'une structure organisationnelle appropriée est essentielle à la configuration d'un environnement à comptes multiples. Dans la mesure où vous utilisez les politiques de contrôle des services (SCPs) pour définir les autorisations maximales pour une unité d'organisation et les comptes qu'elle contient, la structure de votre organisation doit être logique du point de vue de la gestion, des autorisations et des rapports financiers. Pour plus d'informations sur la structure d'une organisation, y compris les unités organisationnelles (OUs), voir Terminologie et concepts (AWS Organizations documentation).

Dans cette section, vous personnalisez la zone d'atterrissage en créant des environnements imbriqués OUs qui vous aident à segmenter et à structurer vos environnements, tels que ceux de production et de non-production. Ces bonnes pratiques recommandées sont conçues pour segmenter votre zone de destination afin de séparer les ressources de production des ressources autres que de production et de séparer l'infrastructure des charges de travail.

Pour plus d'informations sur la création OUs, voir Gestion des unités organisationnelles (AWS Organizations documentation).

Bonnes pratiques

- Dans l'unité d'organisation des charges de travail que vous avez crééeCréation d'une zone de destination, créez les éléments imbriqués OUs suivants :
  - Prod : utilisez cette UO pour les Comptes AWS qui stockent et accèdent aux données de production, y compris les données des clients.
  - NonProd— Utilisez cette UO pour Comptes AWS stocker des données non liées à la production, telles que des environnements de développement, de préparation ou de test

Sous la racine de l'organisation, créez une UO Infrastructure_Prod. Utilisez cette unité d'organisation pour héberger un compte de mise en réseau centralisé.

Ajouter des utilisateurs d'origine

Il existe deux manières de donner aux personnes l'accès aux Comptes AWS :

- Identités IAM, telles que les utilisateurs, les groupes et les rôles
- Fédération d'identité, par exemple en utilisant AWS IAM Identity Center

Dans les petites entreprises et les environnements à compte unique, il est courant que les administrateurs créent un utilisateur IAM lorsqu'une nouvelle personne rejoint l'entreprise. Les informations d'identification de la clé d'accès et de la clé secrète associées à un utilisateur IAM sont appelées informations d'identification à long terme, car elles n'expirent pas. Toutefois, il ne s'agit pas d'une bonne pratique de sécurité recommandée, car si un pirate informatique compromettait ces informations d'identification, vous devriez générer un autre ensemble d'informations d'identification pour l'utilisateur. Une autre méthode d'accès Comptes AWS consiste à utiliser les rôles IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour demander temporairement des informations d'identification à court terme, qui expirent au bout d'une période configurable.

Vous pouvez gérer l'accès des personnes à votre compte Comptes AWS via IAM Identity Center. Vous pouvez créer des comptes utilisateur individuels pour chacun de vos employés ou sous-traitants, où ils peuvent gérer leurs propres mots de passe et solutions d'authentification multifactorielle (MFA), et vous pouvez les regrouper pour gérer l'accès. Lorsque vous configurez le MFA, vous pouvez utiliser des jetons logiciels, tels que des applications d'authentification, ou des jetons matériels, tels que des appareils. YubiKey

IAM Identity Center prend également en charge la fédération à partir de fournisseurs d'identité externes (IdPs) tels qu'Okta et Ping Identity. JumpCloud Pour plus d'informations, veuillez consulter la rubrique Supported identity providers (documentation IAM Identity Center). En fédérant avec un IdP externe, vous pouvez gérer l'authentification des utilisateurs dans toutes les applications, puis utiliser IAM Identity Center pour autoriser l'accès à des applications spécifiques. Comptes AWS

Bonnes pratiques

- Adhérez aux bonnes pratiques de sécurité (documentation IAM) pour configurer l'accès des utilisateurs.

- Gérez l'accès aux comptes par groupes plutôt que par utilisateurs individuels. Dans IAM Identity Center, créez des groupes qui représentent chacune de vos fonctions métier. Par exemple, vous pouvez créer des groupes pour l'ingénierie, les finances, les ventes et la gestion de produits.
- Souvent, les groupes sont définis en séparant ceux qui ont besoin d'un accès à tous les Comptes AWS (accès souvent en lecture seule) et ceux qui ont besoin d'accéder à un seul Compte AWS. Nous vous recommandons d'utiliser la convention de dénomination suivante pour les groupes afin d'identifier facilement les autorisations Compte AWS et autorisations associées au groupe.

  `<prefix>-<account name>-<permission set>`
- Par exemple, pour le groupe `AWS-A-dev-nonprod-DeveloperAccess`, `AWS-A` est un préfixe qui indique l'accès à un seul compte, `dev-nonprod` est le nom du compte et `DeveloperAccess` est l'ensemble d'autorisations attribué au groupe. Pour le groupe `AWS-O-BillingAccess`, le préfixe `AWS-O` indique l'accès à l'ensemble de l'organisation, tandis que `BillingAccess` indique l'ensemble d'autorisations pour le groupe. Dans cet exemple, étant donné que le groupe a accès à l'ensemble de l'organisation, aucun nom de compte n'est représenté dans le nom du groupe.
- Si vous utilisez IAM Identity Center avec un IdP externe basé sur SAML et que vous souhaitez exiger la MFA, vous pouvez utiliser le contrôle d'accès par attributs (ABAC) pour transmettre la méthode d'authentification de l'IdP à IAM Identity Center. Les attributs sont envoyés via les assertions SAML. Pour plus d'informations, veuillez consulter la rubrique Enable and configure attributes for access control (documentation IAM Identity Center).

  De nombreuses entreprises IdPs, telles que Microsoft Azure Active Directory et Okta, peuvent utiliser la revendication Authentication Method Reference (`amr`) dans une assertion SAML pour transmettre le statut MFA de l'utilisateur à IAM Identity Center. La réclamation utilisée pour confirmer l'état de la MFA et son format varient selon l'IdP. Pour plus d'informations, consultez la documentation relative à votre IdP.

  Dans IAM Identity Center, vous pouvez ensuite créer des politiques d'ensemble d'autorisations qui déterminent qui peut accéder à vos AWS ressources. Lorsque vous activez ABAC et spécifiez des attributs, IAM Identity Center transmet la valeur d'attribut de l'utilisateur authentifié dans IAM pour une utilisation dans l'évaluation de politiques. Pour plus d'informations, veuillez consulter la rubrique Create permission policies for ABAC (documentation IAM Identity Center). Comme le montre l'exemple suivant, vous utilisez la clé de condition `aws:PrincipalTag` pour créer une règle de contrôle d'accès pour la MFA.

```
"Condition": {
```

```
  "StringLike": { "aws:PrincipalTag/amr": "mfa" }
}
```

Gérer les comptes membres

Dans cette section, vous invitez votre compte préexistant dans l'organisation et vous commencez à en créer d'autres au sein de votre organisation. Une partie importante de ce processus consiste à définir les critères que vous utilisez pour déterminer si vous devez allouer un nouveau compte.

Cette section se compose des tâches suivantes :

- Inviter votre compte préexistant
- Personnalisez les paramètres VPC dans AWS Control Tower
- Définir les critères de portée

Inviter votre compte préexistant

Au sein de cette section AWS Organizations, vous pouvez inviter le compte préexistant de votre entreprise à rejoindre votre nouvelle organisation. Seul le compte de gestion de l'organisation peut inviter d'autres comptes à la rejoindre. Lorsque l'administrateur du compte invité accepte, le compte rejoint immédiatement l'organisation, tandis que le compte de gestion de l'organisation devient responsable de tous les frais encourus par le nouveau compte membre. Pour plus d'informations, veuillez consulter les rubriques Invitation d'un Compte AWS à rejoindre votre organisation et Acceptation ou refus d'une invitation d'une organisation (documentation AWS Organizations).

> **Note**
>
> Vous pouvez inviter un compte à rejoindre une organisation uniquement s'il n'appartient pas actuellement à une autre organisation. Si le compte est membre d'une organisation existante, vous devez le supprimer de l'organisation. S'il s'agit du compte de gestion d'une autre organisation créée par erreur, vous devez supprimer l'organisation.

> **Important**
>
> Si vous avez besoin d'accéder à des informations historiques sur les coûts ou l'utilisation depuis votre compte préexistant, vous pouvez les utiliser AWS Cost and Usage Report pour

exporter ces informations vers un bucket Amazon Simple Storage Service (Amazon S3). Faites-le avant d'accepter l'invitation à rejoindre l'organisation. Lorsqu'un compte rejoint une organisation, vous perdez l'accès à ses données historiques. Pour plus d'informations, veuillez consulter la rubrique Setting up an Amazon S3 bucket for Cost and Usage Reports (documentation AWS Cost and Usage Report).

Bonnes pratiques

- Nous vous recommandons d'ajouter votre compte préexistant, qui contient probablement des charges de travail de production, à l'unité d'organisation Charges de travail > Prod que vous avez créée dans Ajouter des unités d'organisation .
- Par défaut, le compte de gestion de l'organisation ne dispose pas d'un accès administratif sur les comptes membres invités à rejoindre l'organisation. Si vous souhaitez que le compte de gestion dispose d'un contrôle administratif, vous devez créer le rôle OrganizationAccountAccessRoleIAM dans le compte de membre et autoriser le compte de gestion à assumer ce rôle. Pour plus d'informations, voir Création du OrganizationAccountAccessRole dans un compte de membre invité (AWS Organizations documentation).
- Pour le compte préexistant que vous avez invité à rejoindre l'organisation, consultez les meilleures pratiques pour les comptes de membres (AWS Organizations documentation) et vérifiez que le compte est conforme à ces recommandations.

Personnalisez les paramètres VPC dans AWS Control Tower

Nous vous recommandons d'en approvisionner de nouvelles Comptes AWS par le biais de l'Account Factory dans AWS Control Tower. En utilisant Account Factory, vous pouvez utiliser l' AWS Control Tower intégration avec Amazon EventBridge pour provisionner de nouvelles ressources Comptes AWS dès la création du compte.

Lorsque vous en configurez un nouveau Compte AWS, un cloud privé virtuel (VPC) par défaut est automatiquement provisionné. Toutefois, lorsque vous créez un compte via Account Factory, AWS Control Tower alloue automatiquement un VPC supplémentaire. Pour plus d'informations, consultez la section Présentation de AWS Control Tower et VPCs (AWS Control Tower documentation). Cela signifie que, par défaut, deux AWS Control Tower provisions sont par défaut VPCs sur chaque nouveau compte.

Il est courant que les entreprises souhaitent avoir plus de contrôle VPCs sur leurs comptes. Beaucoup préfèrent utiliser d'autres services AWS CloudFormation, tels que Hashicorp Terraform ou Pulumi, pour configurer et gérer leur. VPCs Vous devez personnaliser les paramètres d'Account Factory pour empêcher la création du VPC supplémentaire alloué par AWS Control Tower. Pour obtenir des instructions, consultez Configurer les paramètres Amazon VPC (AWS Control Tower documentation) et appliquez les paramètres suivants :

1. Désactivez l'option Sous-réseau accessible par Internet.
2. Dans Nombre maximum de sous-réseaux privés, choisissez 0.
3. Dans Régions pour la création de VPC, supprimez toutes les régions.
4. Dans Zones de disponibilité, choisissez 3.

Bonnes pratiques

- Supprimez le VPC par défaut qui est automatiquement alloué dans chaque nouveau compte. Cela empêche les utilisateurs de lancer EC2 des instances publiques dans le compte sans créer explicitement un VPC dédié. Pour plus d'informations, veuillez consulter la rubrique Supprimer vos sous-réseaux par défaut et votre VPC par défaut (documentation Amazon Virtual Private Cloud). Vous pouvez également configurer AWS Control Tower Account Factory pour Terraform (AFT) pour supprimer automatiquement le VPC par défaut dans les comptes qui viennent d'être créés.
- Fournissez un nouveau Compte AWS nom appelé dev-nonprod dans l'unité organisationnelle Workloads >. NonProd Utilisez ce compte pour votre environnement de développement. Pour obtenir des instructions, consultez la section Comptes Provision Account Factory avec AWS Service Catalog (AWS Control Tower documentation).

Définir les critères de portée

Vous devez sélectionner les critères que votre entreprise utilisera pour décider d'en fournir un nouveau Compte AWS. Vous pouvez décider d'allouer des comptes pour chaque unité commerciale, ou vous pouvez décider d'allouer des comptes en fonction de l'environnement, tel que l'environnement de production, de test ou d'assurance qualité. Chaque entreprise a ses propres exigences quant à sa Comptes AWS taille. En règle générale, vous évaluez les trois facteurs suivants lorsque vous décidez de la taille de vos comptes :

- Équilibrage des quotas de service — Les quotas de service sont les valeurs maximales du nombre de ressources, d'actions et d'éléments pour chacun Service AWS au sein d'un Compte AWS. Si de

nombreuses charges de travail partagent le même compte et qu'une charge de travail consomme la majeure partie ou la totalité d'un quota de service, cela peut avoir un impact négatif sur une autre charge de travail du même compte. Dans ce cas, vous devrez peut-être répartir ces charges de travail dans différents comptes. Pour plus d'informations, veuillez consulter Quotas Service AWS (Références générales AWS).

- Rapport sur les coûts : isolez des charges de travail dans des comptes distincts pour visualiser les coûts au niveau du compte dans les rapports sur les coûts et l'utilisation. Lorsque vous utilisez le même compte pour plusieurs charges de travail, vous pouvez utiliser des balises pour vous aider à gérer et à identifier les ressources. Pour plus d'informations sur le balisage, consultez AWS Ressources de balisage ()Références générales AWS.
- Contrôle d'accès : lorsque des charges de travail partagent un compte, vous devez réfléchir à la manière dont vous allez configurer les politiques IAM afin de limiter l'accès aux ressources du compte pour que les utilisateurs n'aient pas accès aux charges de travail auxquelles ils n'ont pas besoin. Au lieu de cela, vous pouvez utiliser plusieurs comptes et ensembles d'autorisations dans IAM Identity Center pour gérer l'accès aux comptes individuels.

Bonnes pratiques

- Respectez les meilleures pratiques en matière de stratégie AWS multi-comptes pour votre zone de AWS Control Tower landing zone (AWS Control Tower documentation).
- Établissez une stratégie de balisage efficace qui vous aide à identifier et à gérer les ressources AWS . Vous pouvez utiliser des balises pour classer vos ressources par objectif, unité commerciale, environnement ou selon d'autres critères. Pour plus d'informations, consultez la section Meilleures pratiques en matière de balisage (Références générales AWS documentation).
- Ne surchargez pas un compte avec trop de charges de travail. Si la demande de la charge de travail dépasse un quota de service, cela peut entraîner des problèmes de performances. Vous pouvez séparer les charges de travail concurrentes en différentes Comptes AWS ou demander une augmentation du quota de service. Pour plus d'informations, veuillez consulter la rubrique Requesting a quota increase (Documentation Service Quotas).

Gestion des autorisations et des accès pour une architecture à comptes multiples

Cette section se compose des rubriques suivantes :

- Considérations culturelles en matière d'ingénierie
- Création d'ensembles d'autorisations
- Création d'une limite des autorisations
- Gestion des autorisations pour les personnes

Considérations culturelles en matière d'ingénierie

L'un des piliers du AWS Well-Architected Framework est l'excellence opérationnelle. Les équipes doivent comprendre le modèle d'exploitation et le rôle qu'elles jouent pour atteindre vos résultats métier. Les équipes peuvent se concentrer sur la réalisation d'objectifs communs lorsqu'elles comprennent leurs responsabilités, les assument et qu'elles savent comment les décisions sont prises.

Dans les entreprises débutantes qui se développent rapidement, chaque membre de l'équipe joue plusieurs rôles. Il n'est pas rare que ces utilisateurs disposent d'un accès hautement privilégié à l'ensemble de l' Compte AWS. Au fur et à mesure que les entreprises se développent, elles souhaitent souvent suivre le principe de moindre privilège et n'accordent que les autorisations nécessaires pour que l'utilisateur puisse effectuer son travail. Pour vous aider à limiter la portée, vous pouvez utiliser AWS Identity and Access Management Access Analyzer afin de voir quelles autorisations un utilisateur ou un rôle IAM utilise réellement, ce qui vous permet de supprimer les autorisations excédentaires.

Il peut être difficile de déterminer qui, au sein de votre entreprise, est autorisé à créer des rôles IAM. Il s'agit généralement d'un vecteur d'escalade des privilèges. L'escalade des privilèges se produit lorsqu'un utilisateur peut étendre ses propres autorisations ou la portée de son accès. Par exemple, si un utilisateur dispose d'autorisations limitées, mais peut créer des rôles IAM, il peut escalader ses privilèges en créant et en endossant un nouveau rôle IAM, auquel la politique gérée par `AdministratorAccess` est appliquée.

Certaines entreprises limitent l'attribution des rôles IAM à une équipe centralisée de personnes de confiance. L'inconvénient de cette approche est que cette équipe peut rapidement devenir un

goulot d'étranglement, car presque toutes Services AWS ont besoin d'un rôle IAM pour fonctionner. Comme alternative, vous pouvez recourir aux limites des autorisations pour déléguer l'accès IAM uniquement aux utilisateurs qui développent, testent, lancent et gèrent votre infrastructure cloud. Pour des exemples de politiques, voir Example Permission Boundaries (GitHub).

Les équipes chargées des opérations de développement (DevOps), également appelées équipes de plateforme, doivent souvent trouver un équilibre entre les capacités de libre-service de plusieurs équipes de développement internes et la stabilité opérationnelle des applications. Favoriser une culture d'ingénierie qui prône l'autonomie, la maîtrise et la détermination au travail peut contribuer à motiver les équipes. Les ingénieurs veulent faire leur travail de manière autonome, sans compter sur les autres pour faire les choses à leur place. Si DevOps les équipes peuvent mettre en œuvre des solutions en libre-service, cela réduit également le temps que les autres personnes comptent sur elles pour accomplir leurs tâches.

Création d'ensembles d'autorisations

Vous pouvez gérer Compte AWS l'accès à l'aide des ensembles d'autorisations intégrés AWS IAM Identity Center. Un ensemble d'autorisations est un modèle qui vous permet de déployer une ou plusieurs politiques IAM sur plusieurs Comptes AWS. Lorsque vous attribuez un ensemble d'autorisations à un Compte AWS, IAM Identity Center crée un rôle IAM et lui associe vos politiques IAM. Pour plus d'informations, veuillez consulter la rubrique Create and manage permission sets (documentation IAM Identity Center).

AWS recommande de créer des ensembles d'autorisations correspondant aux différentes personnes de votre entreprise.

Par exemple, vous pouvez créer les ensembles d'autorisations suivants :

- Ensemble d'autorisations de facturation
- Ensemble d'autorisations pour les développeurs
- Ensemble d'autorisations de production

Les ensembles d'autorisations suivants sont des extraits d'un AWS CloudFormation modèle. Vous devez utiliser ce code comme point de départ et le personnaliser pour votre entreprise. Pour plus d'informations sur les CloudFormation modèles, voir Apprendre les bases des modèles (CloudFormation documentation).

Ensemble d'autorisations de facturation

L'équipe financière a l'habitude BillingAccessPermissionSetde consulter le tableau de bord de la AWS Billing console et AWS Cost Explorer de chaque compte.

```
BillingAccessPermissionSet:
  Type: "AWS::SSO::PermissionSet"
  Properties:
    Description: Access to Billing and Cost Explorer
    InstanceArn: !Sub "arn:${AWS::Partition}:sso:::instance/ssoins-instanceId"
    ManagedPolicies:
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/job-function/Billing"
    Name: BillingAccess
    SessionDuration: PT8H
    RelayStateType: https://console.aws.amazon.com/billing/home
```

Ensemble d'autorisations pour les développeurs

L'équipe d'ingénierie a l'habitude d'accéder DeveloperAccessPermissionSetà des comptes non liés à la production.

```
DeveloperAccessPermissionSet:
  Type: "AWS::SSO::PermissionSet"
  Properties:
    Description: Access to provision resources through CloudFormation
    InlinePolicy: !Sub |-
      {
        "Version": "2012-10-17",
        "Statement": [
          {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:${AWS::Partition}:iam::*:role/CloudFormationRole",
            "Condition": {
              "StringEquals": {
                "aws:ResourceAccount": "${!aws:PrincipalAccount}",
                "iam:PassedToService": "cloudformation.${AWS::URLSuffix}"
              }
            }
          },
          {
            "Effect": "Allow",
```

```
            "Action": [
              "cloudformation:ContinueUpdateRollback",
              "cloudformation:CreateChangeSet",
              "cloudformation:CreateStack",
              "cloudformation:DeleteStack",
              "cloudformation:RollbackStack",
              "cloudformation:UpdateStack"
            ],
            "Resource": "arn:${AWS::Partition}:cloudformation:*:*:stack/app-*",
            "Condition": {
              "ArnLike": {
                "cloudformation:RoleArn": "arn:${AWS::Partition}:iam::${!
aws:PrincipalAccount}:role/CloudFormationRole"
              },
              "Null": {
                "cloudformation:ImportResourceTypes": true
              }
            }
          },
          {
            "Effect": "Allow",
            "Action": [
              "cloudformation:CancelUpdateStack",
              "cloudformation:DeleteChangeSet",
              "cloudformation:DetectStackDrift",
              "cloudformation:DetectStackResourceDrift",
              "cloudformation:ExecuteChangeSet",
              "cloudformation:TagResource",
              "cloudformation:UntagResource",
              "cloudformation:UpdateTerminationProtection"
            ],
            "Resource": "arn:${AWS::Partition}:cloudformation:*:*:stack/app-*"
          },
          {
           "Effect": "Allow",
            "Action": [
              "cloudformation:CreateUploadBucket",
              "cloudformation:ValidateTemplate",
              "cloudformation:EstimateTemplateCost"
            ],
            "Resource": "*"
          }
        ]
      }
```

```
    InstanceArn: !Sub "arn:${AWS::Partition}:sso:::instance/ssoins-instanceId"
    ManagedPolicies:
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSServiceCatalogEndUserFullAccess"
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSProtonDeveloperAccess"
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSBillingReadOnlyAccess"
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSSupportAccess"
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/ReadOnlyAccess"
    Name: DeveloperAccess
    SessionDuration: PT8H
```

Ensemble d'autorisations de production

L'équipe d'ingénierie a l'habitude ProductionPermissionSetd'accéder aux comptes de production. Cet ensemble d'autorisations dispose d'un accès limité en lecture seule.

```
ProductionPermissionSet:
  Type: "AWS::SSO::PermissionSet"
  Properties:
    Description: Access to production accounts
    InlinePolicy: !Sub |-
      {
        "Version": "2012-10-17",
        "Statement": [
          {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:${AWS::Partition}:iam::*:role/CloudFormationRole",
            "Condition": {
              "StringEquals": {
                "aws:ResourceAccount": "${!aws:PrincipalAccount}",
                "iam:PassedToService": "cloudformation.${AWS::URLSuffix}"
              }
            }
          },
          {
            "Effect": "Allow",
            "Action": "cloudformation:ContinueUpdateRollback",
            "Resource": "arn:${AWS::Partition}:cloudformation:*:*:stack/app-*",
            "Condition": {
              "ArnLike": {
                "cloudformation:RoleArn": "arn:${AWS::Partition}:iam::${!
aws:PrincipalAccount}:role/CloudFormationRole"
              }
```

```
            }
          },
          {
            "Effect": "Allow",
            "Action": "cloudformation:CancelUpdateStack",
            "Resource": "arn:${AWS::Partition}:cloudformation:*:*:stack/app-*"
          }
        ]
      }
    InstanceArn: !Sub "arn:${AWS::Partition}:sso:::instance/ssoins-instanceId"
    ManagedPolicies:
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSBillingReadOnlyAccess"
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSSupportAccess"
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/job-function/ViewOnlyAccess"
    Name: ProductionAccess
    SessionDuration: PT2H
```

Création d'une limite des autorisations

Après avoir déployé les ensembles d'autorisations, vous définissez une limite des autorisations. Cette limite des autorisations est un mécanisme permettant de déléguer l'accès IAM uniquement aux utilisateurs qui développent, testent, lancent et gèrent votre infrastructure cloud. Ces utilisateurs ne peuvent effectuer que les actions autorisées par la politique et les limites des autorisations.

Vous pouvez définir la limite des autorisations dans un AWS CloudFormation modèle, puis l'utiliser CloudFormation StackSets pour déployer le modèle sur plusieurs comptes. Cela vous permet d'établir et de maintenir des politiques normalisées au sein de votre organisation en une seule opération. Pour plus d'informations et d'instructions, consultez la section Travailler avec AWS CloudFormation StackSets (CloudFormation documentation).

Le CloudFormation modèle suivant fournit un rôle IAM et crée une politique IAM qui sert de limite d'autorisation. À l'aide d'un ensemble de piles, vous pouvez déployer ce modèle sur tous les comptes membres de votre organisation.

```
CloudFormationRole:
  Type: "AWS::IAM::Role"
  Properties:
    AssumeRolePolicyDocument:
      Version: "2012-10-17"
      Statement:
        Effect: Allow
```

```
        Principal:
          Service: !Sub "cloudformation.${AWS::URLSuffix}"
        Action: "sts:AssumeRole"
        Condition:
          StringEquals:
            "aws:SourceAccount": !Ref "AWS::AccountId"
    Description: !Sub "DO NOT DELETE - Used by CloudFormation. Created by
 CloudFormation ${AWS::StackId}"
    ManagedPolicyArns:
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AdministratorAccess"
    PermissionsBoundary: !Ref DeveloperBoundary
    RoleName: CloudFormationRole

DeveloperBoundary:
  Type: "AWS::IAM::ManagedPolicy"
  Properties:
    Description: Permission boundary for developers
    ManagedPolicyName: PermissionsBoundary
    PolicyDocument:
      Version: "2012-10-17"
      Statement:
        - Sid: AllowModifyIamRolesWithBoundary
          Effect: Allow
          Action:
            - "iam:AttachRolePolicy"
            - "iam:CreateRole"
            - "iam:DeleteRolePolicy"
            - "iam:DetachRolePolicy"
            - "iam:PutRolePermissionsBoundary"
            - "iam:PutRolePolicy"
          Resource: !Sub "arn:${AWS::Partition}:iam::${AWS::AccountId}:role/app/*"
          Condition:
            ArnEquals:
              "iam:PermissionsBoundary": !Sub "arn:${AWS::Partition}:iam::
${AWS::AccountId}:policy/PermissionsBoundary"
        - Sid: AllowModifyIamRoles
          Effect: Allow
          Action:
            - "iam:DeleteRole"
            - "iam:TagRole"
            - "iam:UntagRole"
            - "iam:UpdateAssumeRolePolicy"
            - "iam:UpdateRole"
            - "iam:UpdateRoleDescription"
```

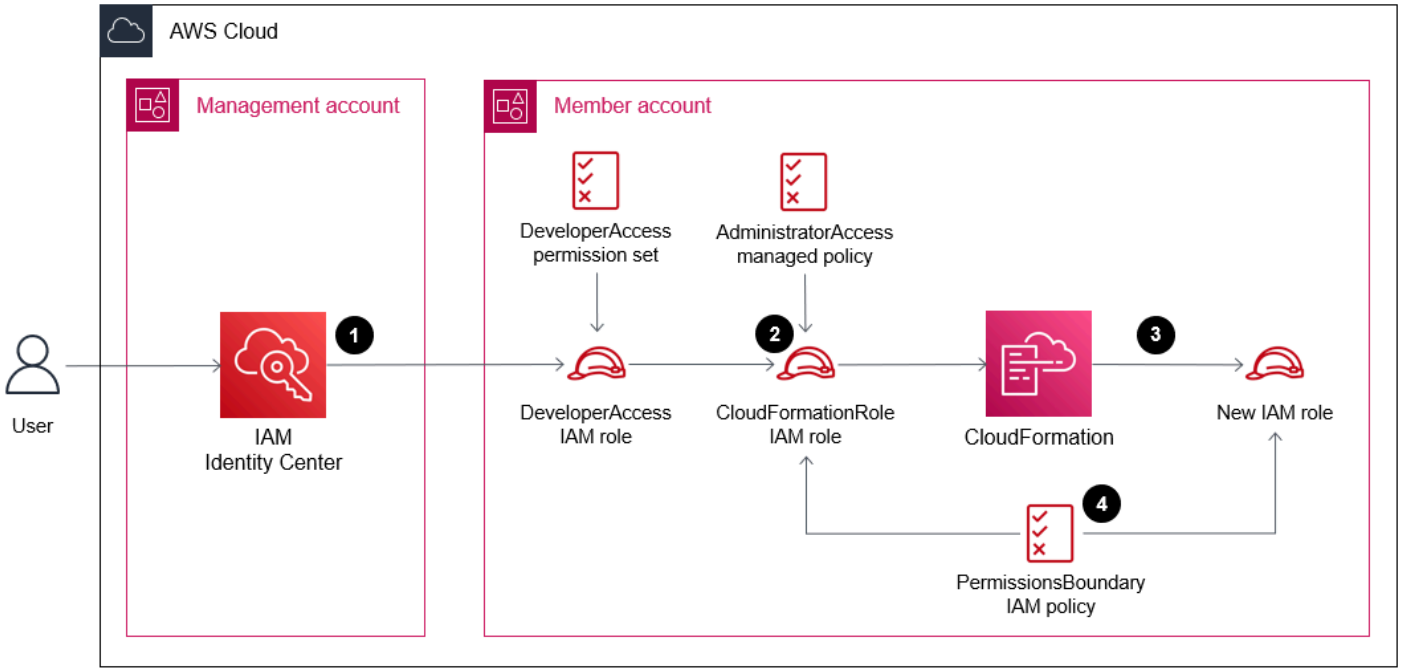
```
      Resource: !Sub "arn:${AWS::Partition}:iam::${AWS::AccountId}:role/app/*"
    - Sid: OverlyPermissiveAllowedServices
      Effect: Allow
      Action:
        - "lambda:*"
        - "apigateway:*"
        - "events:*"
        - "s3:*"
        - "logs:*"
      Resource: "*"
```

Le CloudFormationRolerôle, la PermissionsBoundarypolitique et l'ensemble DeveloperAccessd'autorisations fonctionnent ensemble pour accorder les autorisations suivantes :

- Les utilisateurs ont un accès en lecture seule à la plupart Services AWS, via la politique ReadOnlyAccess AWS gérée.
- Les utilisateurs ont accès aux dossiers de support ouverts, par le biais de la politique de AWS gestion des AWSSupportaccès.
- Les utilisateurs ont un accès en lecture seule au tableau de bord de la AWS Billing console, via la politique AWSBillingReadOnlyAccess AWS gérée.
- Les utilisateurs peuvent approvisionner de nouveaux environnements à partir de AWS Proton la politique AWSProtonDeveloperAccess AWS gérée.
- Les utilisateurs peuvent approvisionner des produits à partir de Service Catalog, via la politique AWSServiceCatalogEndUserFullAccess AWS gérée.
- Les utilisateurs peuvent valider et estimer le coût de n'importe quel CloudFormation modèle, grâce à la politique en ligne.
- En utilisant le rôle CloudFormationRoleIAM, les utilisateurs peuvent créer, mettre à jour ou supprimer toute CloudFormation pile commençant par app/.
- Les utilisateurs peuvent l'utiliser CloudFormation pour créer, mettre à jour ou supprimer des rôles IAM commençant par app/. La politique PermissionsBoundaryIAM empêche les utilisateurs d'augmenter leurs privilèges.
- Les utilisateurs peuvent AWS Lambda approvisionner les ressources Amazon EventBridge CloudWatch, Amazon, Amazon Simple Storage Service (Amazon S3) et Amazon API Gateway uniquement en utilisant. CloudFormation

L'image suivante montre comment un utilisateur autorisé, tel qu'un développeur, peut créer un rôle IAM dans un compte membre en utilisant les ensembles d'autorisations, les rôles IAM et les limites des autorisations décrits dans ce guide :

1. L'utilisateur s'authentifie dans le centre d'identité IAM et assume le rôle DeveloperAccessIAM.
2. L'utilisateur lance l'`cloudformation:CreateStack`action et assume le rôle CloudFormationRoleIAM.
3. L'utilisateur lance l'`iam:CreateRole`action et l'utilise CloudFormation pour créer un nouveau rôle IAM.
4. La politique PermissionsBoundaryIAM est appliquée au nouveau rôle IAM.



La politique AdministratorAccessgérée est attachée au CloudFormationRolerôle, mais en raison de la stratégie PermissionsBoundaryIAM, les autorisations effectives du CloudFormationRolerôle deviennent égales à la PermissionsBoundarypolitique. La PermissionsBoundarypolitique se référence elle-même lorsqu'elle autorise l'`iam:CreateRole`action, ce qui garantit que les rôles ne peuvent être créés que si la limite des autorisations est appliquée.

Gestion des autorisations pour les personnes

En utilisant les ensembles d'autorisations, la limite des autorisations et le rôle CloudFormationRoleIAM, vous pouvez limiter le nombre d'autorisations que vous devez attribuer directement aux principaux individuels. Cela vous permet de gérer l'accès au fur et à mesure que votre entreprise se développe et d'appliquer les bonnes pratiques de sécurité qui consistent à accorder le moindre privilège.

Vous pouvez également utiliser des rôles liés à un service, qui accordent des autorisations à un service AWS afin d'allouer des ressources en votre nom. Au lieu d'accorder des autorisations au principal IAM (utilisateur, groupe d'utilisateurs ou rôle), vous pouvez accorder les autorisations au service. Par exemple, les rôles liés à un service pour AWS Proton et AWS Service Catalog vous permettent d'allouer vos propres modèles, ressources et environnements, sans attribuer d'autorisations au principal IAM. Pour plus d'informations, veuillez consulter les rubriques Services AWS qui fonctionnent avec IAM et Utilisation des rôles liés à un service (documentation IAM).

Une autre bonne pratique consiste à limiter le niveau d'accès dont disposent les personnes à la AWS Management Console. En limitant l'accès à la console, vous pouvez obliger les utilisateurs à provisionner des ressources en utilisant des technologies d'infrastructure sous forme de code (IaC) AWS CloudFormation, telles que HashiCorp Terraform ou Pulumi. La gestion de l'infrastructure via iAC vous permet de suivre l'évolution des ressources au fil du temps et d'introduire des mécanismes d'approbation des modifications, tels que les GitHub pull requests.

Connectivité réseau pour une architecture à comptes multiples

Connecter VPCs

De nombreuses entreprises utilisent le peering VPC dans Amazon Virtual Private Cloud (Amazon VPC) pour connecter le développement et la production. VPCs À l'aide d'une connexion d'appairage VPC, vous pouvez acheminer le trafic entre deux VPCs en utilisant un adressage IP privé.
Le connecté VPCs peut être différent Comptes AWS ou différent Régions AWS. Pour plus d'informations, veuillez consulter la rubrique Qu'est-ce que l'appairage de VPC (documentation Amazon VPC). À mesure que les entreprises se développent et que VPCs leur nombre augmente, le maintien de connexions de peering entre toutes VPCs peut devenir un fardeau de maintenance. Vous pouvez également être limité par le nombre maximal de connexions d'appairage de VPC par VPC. Pour plus d'informations, veuillez consulter la rubrique Quotas d'une connexion d'appairage de VPC (documentation Amazon VPC).

Si vous disposez de plusieurs environnements de développement, de test et de préparation hébergeant des données non liées à la production sur plusieurs d'entre eux Comptes AWS, vous souhaiterez peut-être fournir une connectivité réseau entre tous ces environnements VPCs , mais interdire tout accès aux environnements de production. Vous pouvez l'AWS Transit Gatewayutiliser pour connecter VPCs plusieurs comptes. Vous pouvez séparer les tables de routage pour VPCs empêcher le développement de communiquer avec la production VPCs via la passerelle de transit, qui fait office de routeur centralisé. Pour plus d'informations, veuillez consulter la rubrique Routeur centralisé (documentation Transit Gateway).

Transit Gateway prend également en charge l'appairage avec d'autres passerelles de transit, y compris celles situées dans différents Comptes AWS ou différentes Régions AWS. Transit Gateway étant un service hautement disponible et entièrement géré, vous ne devez allouer qu'une seule passerelle de transit pour chaque région.

Pour plus d'informations et des architectures réseau détaillées, voir Création d'une infrastructure AWS réseau multi-VPC évolutive et sécurisée (AWS livre blanc).

Connexion d'applications

Si vous devez établir une communication entre des applications différentes Comptes AWS dans le même environnement (tel que la production), vous pouvez utiliser l'une des options suivantes :

- L'appairage de VPC ou AWS Transit Gateway peut fournir une connectivité au niveau du réseau si vous souhaitez ouvrir un accès étendu à plusieurs adresses IP et ports.
- AWS PrivateLink crée des points de terminaison dans un sous-réseau privé du VPC, et ces points de terminaison sont enregistrés en tant qu'entrées DNS dans Amazon Route 53 Resolver. Avec DNS, les applications peuvent résoudre les points de terminaison et se connecter aux services enregistrés, sans avoir besoin de passerelles NAT ou de passerelles Internet dans le VPC.
- Amazon VPC Lattice associe des services, tels que des applications, entre plusieurs comptes VPCs et les collecte dans un réseau de services. Les clients VPCs associés au réseau de service peuvent envoyer des demandes à tous les autres services associés au réseau de service, qu'ils soient ou non dans le même compte. VPC Lattice s'intègre à AWS Resource Access Manager (AWS RAM) afin que vous puissiez partager des ressources avec d'autres comptes ou via. AWS Organizations Vous ne pouvez associer un VPC qu'à un seul réseau de services. Cette solution ne nécessite pas l'utilisation de l'appairage de VPC ou de AWS Transit Gateway pour communiquer entre les comptes.

Bonnes pratiques pour la connectivité réseau

- Créez un réseau Compte AWS que vous utiliserez pour le réseau centralisé. Nommez ce compte network-prod et utilisez-le pour AWS Transit Gateway Amazon VPC IP Address Manager (IPAM). Ajoutez ce compte à l'unité d'organisation Infrastructure_Prod.
- Utilisez AWS Resource Access Manager (AWS RAM) pour partager la passerelle de transit, les réseaux de services VPC Lattice et les groupes IPAM avec le reste de l'organisation. Cela permet à tous Compte AWS les membres de votre organisation d'interagir avec ces services.
- En utilisant des pools IPAM pour gérer IPv4 et IPv6 gérer les allocations de manière centralisée, vous pouvez permettre à vos utilisateurs finaux de s'approvisionner eux-mêmes VPCs en utilisant. AWS Service Catalog Cela vous permet de dimensionner correctement les espaces d'adresses IP VPCs et d'éviter les chevauchements.
- Utilisez une approche de sortie centralisée pour le trafic lié à Internet, et utilisez une approche d'entrée décentralisée pour le trafic entrant dans votre environnement depuis Internet. Pour plus d’informations, consultez Sortie centralisée et Entrée décentralisée.

Sortie centralisée

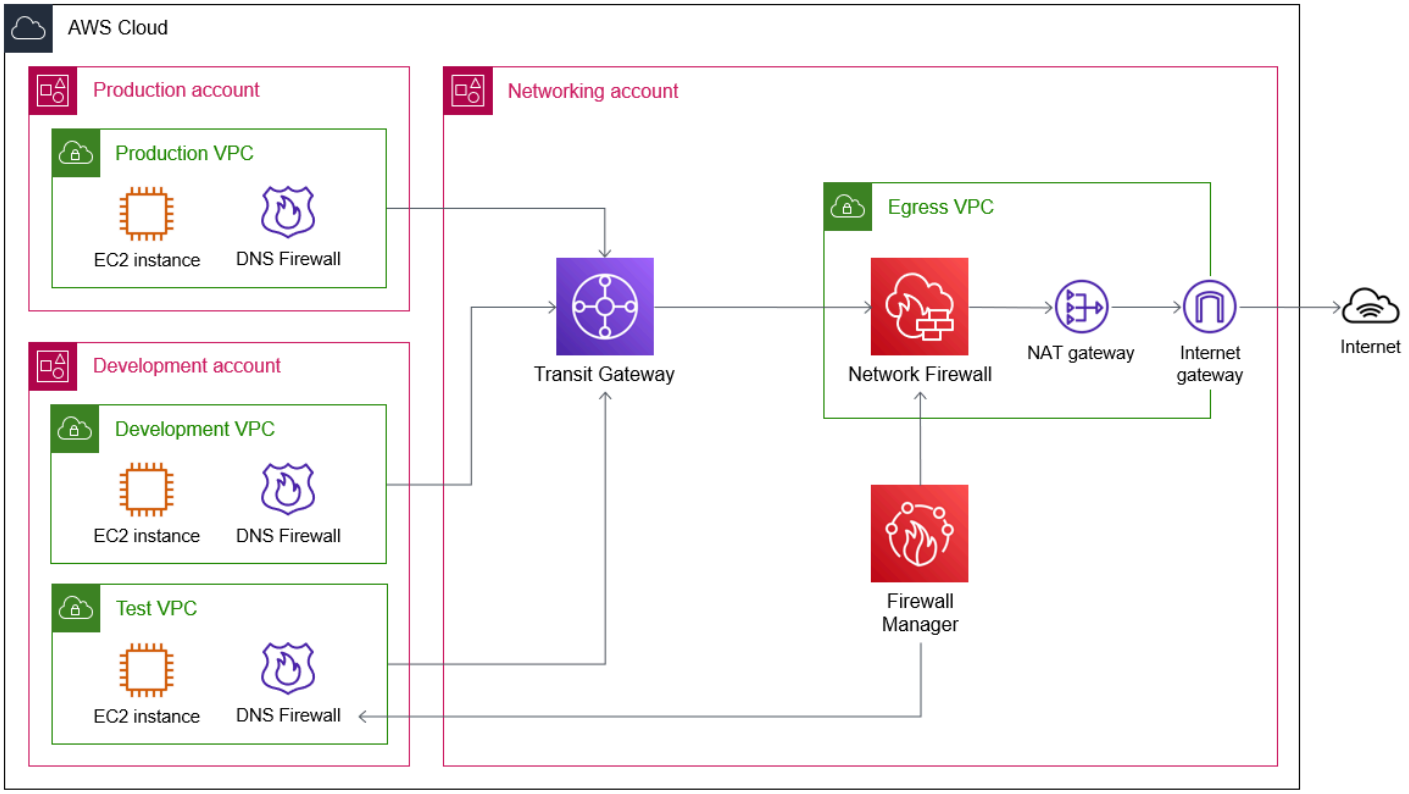
La sortie centralisée est le principe qui consiste à utiliser un point d'inspection unique et commun pour tout le trafic réseau destiné à Internet. À ce stade de l'inspection, vous pouvez autoriser le trafic uniquement vers des domaines spécifiques ou uniquement via des ports ou des protocoles spécifiés. La centralisation des sorties peut également vous aider à réduire les coûts en éliminant le besoin de déployer des passerelles NAT dans chacun d'entre vous VPCs pour accéder à Internet. Cela s'avère avantageux du point de vue de la sécurité, en raison de la limitation de l'exposition aux ressources malveillantes accessibles de l'extérieur, telles que l'infrastructure de commande et de contrôle (C&C) des logiciels malveillants. Pour plus d'informations et pour connaître les options d'architecture relatives à la sortie centralisée, consultez la section Sortie centralisée vers Internet (AWS livre blanc).

Vous pouvez utiliser AWS Network Firewall, qui est un pare-feu réseau dynamique et un service de détection et de prévention des intrusions, en tant que point d'inspection central pour le trafic sortant. Vous configurez ce pare-feu dans un VPC dédié pour le trafic sortant. Network Firewall prend en charge les règles dynamiques que vous pouvez utiliser pour limiter l'accès à Internet à des domaines spécifiques. Pour plus d'informations, veuillez consulter la rubrique Domain List (documentation Network Firewall).

Vous pouvez également utiliser Amazon Route 53 Resolver DNS Firewall pour limiter le trafic sortant vers des noms de domaine spécifiques, essentiellement pour empêcher l'exfiltration non autorisée de vos données. Dans les règles DNS Firewall, vous pouvez appliquer des listes de domaines (documentation Route 53), qui autorisent ou refusent l'accès à des domaines spécifiés. Vous pouvez utiliser des listes de domaines AWS gérées, qui contiennent des noms de domaine associés à des activités malveillantes ou à d'autres menaces potentielles, ou vous pouvez créer des listes de domaines personnalisées. Vous créez des groupes de règles de pare-feu DNS, puis vous les appliquez à votre VPCs. Les demandes DNS sortantes sont acheminées via un résolveur dans le VPC pour la résolution des noms de domaine, tandis que DNS Firewall filtre les demandes en fonction des groupes de règles appliqués au VPC. Les demandes DNS récursives qui accèdent au résolveur ne passent pas par la passerelle de transit et le chemin Network Firewall. Route 53 Resolver et DNS Firewall doivent être considérés comme un chemin de sortie distinct du VPC.

L'image suivante montre un exemple d'architecture pour une sortie centralisée. Avant le début de la communication réseau, les demandes DNS sont envoyées à Route 53 Resolver, où DNS Firewall autorise ou refuse la résolution de l'adresse IP utilisée pour la communication. Le trafic destiné à Internet est acheminé vers une passerelle de transit dans un compte de mise en réseau centralisée. La passerelle de transit transfère le trafic à Network Firewall pour inspection. Si la

politique de pare-feu autorise le trafic sortant, le trafic est acheminé via une passerelle NAT, via une passerelle Internet et vers Internet. Vous pouvez l'utiliser AWS Firewall Manager pour gérer de manière centralisée les groupes de règles du pare-feu DNS et les politiques de pare-feu réseau au sein de votre infrastructure multi-comptes.



Bonnes pratiques pour sécuriser le trafic sortant

- Commencez dans mode de journalisation uniquement (documentation Route 53). Passez en mode blocage après avoir vérifié que le trafic légitime n'est pas affecté.
- Bloquez le trafic DNS vers Internet en utilisant des AWS Firewall Manager politiques pour les listes de contrôle d'accès au réseau ou en utilisant AWS Network Firewall. Toutes les requêtes DNS doivent être acheminées via un résolveur Route 53, où vous pouvez les surveiller avec Amazon GuardDuty (si activé) et les filtrer avec le pare-feu DNS Route 53 Resolver (si activé). Pour plus d'informations, consultez Résolution des requêtes DNS entre VPCs et votre réseau (documentation Route 53).
- Utilisez les listes de domaines gérées AWS (documentation Route 53) dans DNS Firewall et Network Firewall.
- Envisagez de bloquer les domaines de premier niveau inutilisés à haut risque, tels que .info, .top, .xyz ou certains domaines de code de pays.

- Envisagez de bloquer les ports non utilisés à haut risque, tels que les ports 1389, 4444, 3333, 445, 135, 139 ou 53.
- Comme point de départ, vous pouvez utiliser une liste de refus qui inclut les règles AWS gérées. Vous pouvez ensuite travailler au fil du temps à la mise en œuvre d'un modèle de liste d'autorisation. Par exemple, au lieu de n'inclure qu'une liste stricte de noms de domaine complets dans la liste d'autorisation, commencez par utiliser des caractères génériques, tels que *.exemple.com. Vous pouvez même autoriser uniquement les domaines de premier niveau auxquels vous vous attendez et bloquer tous les autres. Puis, au fil du temps, réduisez-les également.
- Utilisez les profils Route 53 (documentation Route 53) pour appliquer des configurations Route 53 liées au DNS dans de nombreuses VPCs configurations différentes. Comptes AWS
- Définissez un processus pour gérer les exceptions à ces meilleures pratiques.

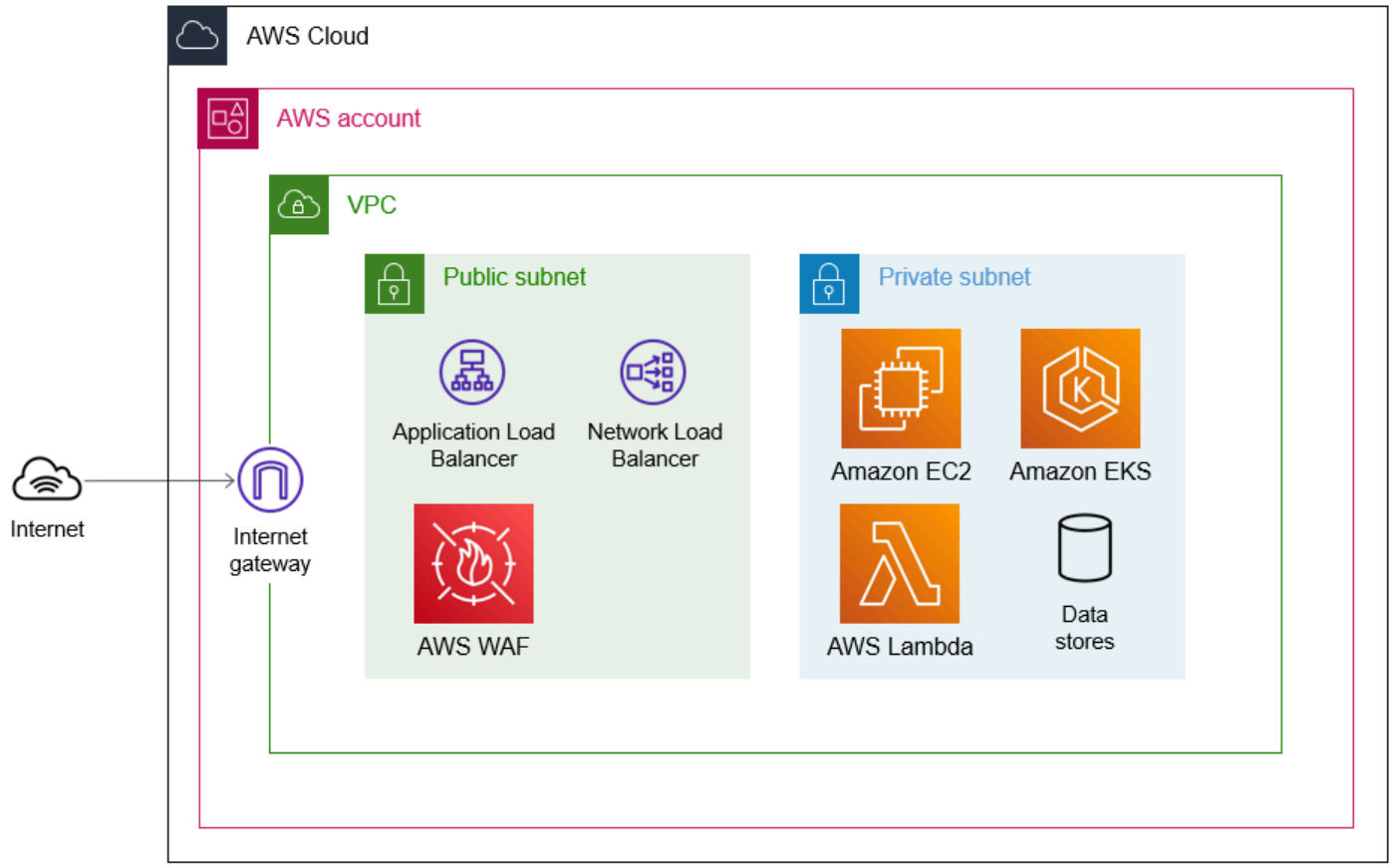
Entrée décentralisée

L'entrée décentralisée est le principe qui permet de définir, au niveau d'un compte individuel, la manière dont le trafic provenant d'Internet atteint les charges de travail de ce compte. Dans les architectures à comptes multiples, l'un des avantages de l'entrée décentralisée est que chaque compte peut utiliser le service ou la ressource d'entrée les plus appropriés pour ses charges de travail, comme un Application Load Balancer, Amazon API Gateway ou Network Load Balancer.

Bien que l'entrée décentralisée signifie que vous devez gérer chaque compte individuellement, vous pouvez administrer et maintenir vos configurations de manière centralisée via AWS Firewall Manager. Firewall Manager prend en charge des protections telles que AWS WAF et Groupes de sécurité Amazon VPC. Vous pouvez AWS WAF l'associer à un Application Load Balancer CloudFront, Amazon, API Gateway ou. AWS AppSync Si vous utilisez un VPC sortant et une passerelle de transit, comme décrit dans Sortie centralisée, chaque VPC en étoile contient des sous-réseaux publics et privés. Cependant, il n'est pas nécessaire de déployer des passerelles NAT, car le trafic passe par le VPC sortant du compte de mise en réseau.

L'image suivante montre un exemple de personne Compte AWS possédant un seul VPC contenant une charge de travail accessible par Internet. Le trafic provenant d'Internet accède au VPC via une passerelle Internet et atteint les services d'équilibrage de charge et de sécurité hébergés dans un sous-réseau public. (Un sous-réseau public contient une route par défaut vers une passerelle Internet). Déployez des équilibreurs de charge dans des sous-réseaux publics et associez des listes de contrôle d' AWS WAF accès (ACLs) pour vous protéger contre le trafic malveillant, tel que les

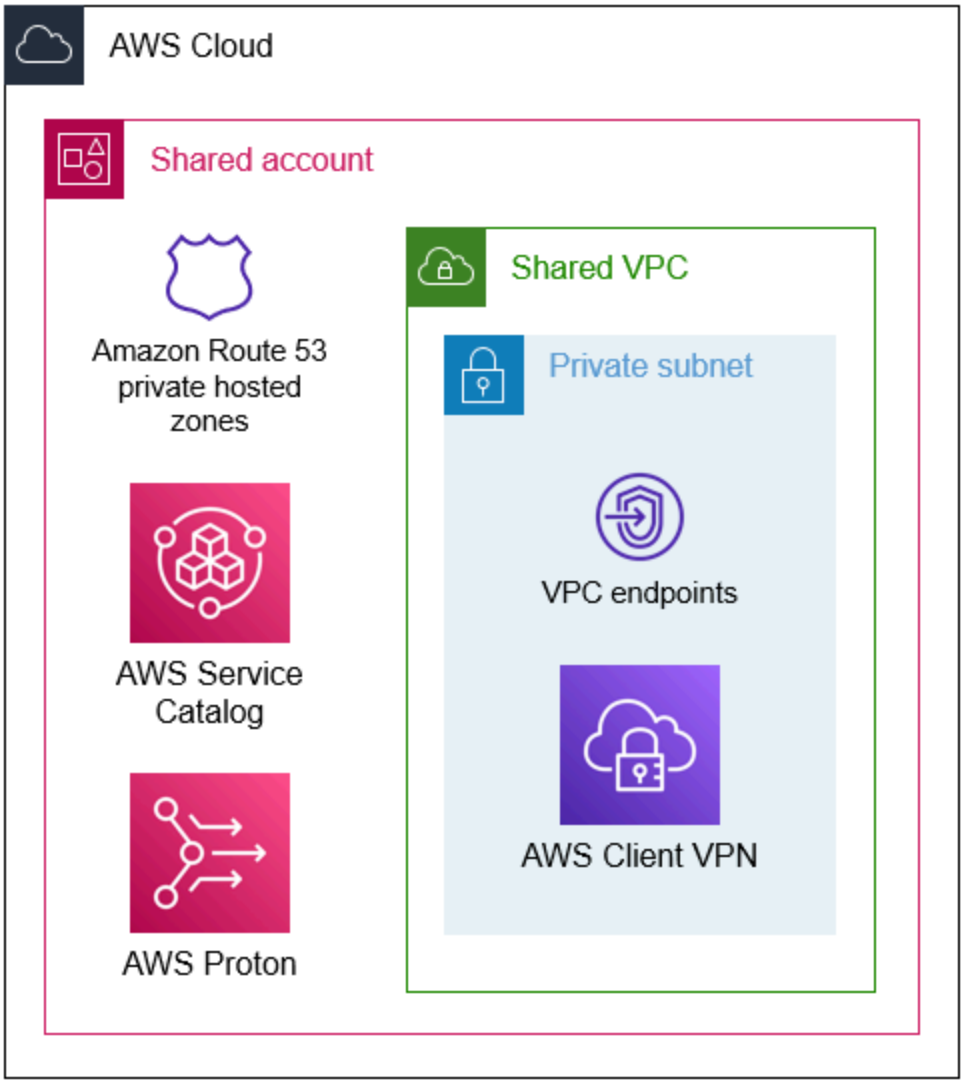
scripts intersites. Déployez des charges de travail hébergeant des applications dans des sous-réseaux privés, qui n'ont pas d'accès direct à Internet.



Si vous en avez beaucoup VPCs dans votre organisation, vous souhaiterez peut-être partager des points communs en Services AWS créant des points de terminaison VPC d'interface ou des zones hébergées privées dans un environnement dédié et partagé. Compte AWS Pour plus d'informations, consultez Accès et Service AWS utilisation d'un point de terminaison VPC d'interface (AWS PrivateLink documentation) et Utilisation de zones hébergées privées (documentation Route 53).

L'image suivante montre un exemple de site hébergeant des ressources pouvant être partagées au sein de l'organisation. Compte AWS Les points de terminaison d'un VPC peuvent être partagés entre plusieurs comptes en les créant dans un VPC dédié. Lorsque vous créez un point de terminaison d'un VPC, vous pouvez éventuellement faire en sorte qu' AWS gère les entrées DNS pour le point de terminaison. Pour partager un point de terminaison, désactivez cette option et créez les entrées DNS dans une zone hébergée privée (PHZ) Route 53 distincte. Vous pouvez ensuite associer le PHZ à tous les éléments de votre organisation pour une résolution DNS centralisée des points de terminaison VPC. VPCs Vous devez également vous assurer que les tables de routage de

la passerelle de transit incluent les itinéraires entre le VPC partagé et l'autre. VPCs Pour plus d'informations, consultez la section Accès centralisé aux points de terminaison VPC de l'interface (AWS livre blanc).



Un espace partagé Compte AWS est également un bon endroit pour héberger AWS Service Catalog des portefeuilles. Un portefeuille est un ensemble de services informatiques sur lesquels vous souhaitez mettre à disposition pour le déploiement AWS, et le portefeuille contient des informations de configuration pour ces services. Vous pouvez créer les portefeuilles dans le compte partagé, les partager avec l'organisation, puis chaque compte membre importe le portefeuille dans sa propre instance régionale de Service Catalog. Pour plus d'informations, veuillez consulter Partage avec AWS Organizations (documentation Service Catalog).

De même AWS Proton, vous pouvez utiliser le compte partagé pour gérer de manière centralisée votre environnement et vos modèles de services, puis configurer des connexions de compte avec les comptes des membres de l'organisation. Pour plus d'informations, consultez Connexions aux comptes d'environnement (AWS Proton documentation).

Réponse aux incidents de sécurité pour une architecture à comptes multiples

Lorsque vous passez à plusieurs Comptes AWS, il est important que vous conserviez une visibilité sur les événements de sécurité susceptibles de se produire au sein de votre organisation. Dans Gestion des identités et contrôle d'accès, vous avez utilisé AWS Control Tower pour configurer votre zone de destination. Au cours de ce processus de configuration, AWS Control Tower j'ai désigné un Compte AWS pour la sécurité. Vous devez déléguer l'administration des services de sécurité au security-tooling-prodcompte et utiliser ce compte pour gérer ces services de manière centralisée.

Ce guide passe en revue l'utilisation des éléments suivants Services AWS pour vous aider à protéger votre entreprise Comptes AWS et vous-même :

- Amazon GuardDuty
- Amazon Macie
- AWS Security Hub

Amazon GuardDuty

Amazon GuardDuty est un service de surveillance continue de la sécurité qui analyse les sources de données, telles que les journaux AWS CloudTrail d'événements. Pour obtenir la liste complète des sources de données prises en charge, consultez Comment Amazon GuardDuty utilise ses sources de données (GuardDuty documentation). Il utilise des flux d'intelligence de menaces, comme les listes d'adresses IP et de domaines malveillants, ainsi que le machine learning pour identifier toute activité inattendue et potentiellement non autorisée et malveillante au sein de votre environnement AWS .

Lorsque vous utilisez GuardDuty avec AWS Organizations, le compte de gestion de l'organisation peut désigner n'importe quel compte de l'organisation comme administrateur GuardDuty délégué. L'administrateur délégué devient le compte GuardDuty administrateur de la région. GuardDuty est automatiquement activé en ce sens que :Région AWS, et le compte administrateur délégué est autorisé à activer et à gérer tous GuardDuty les comptes de l'organisation au sein de cette région. Pour plus d'informations, consultez la section Gestion GuardDuty des comptes avec AWS Organizations (GuardDuty documentation).

GuardDuty est un service régional. Cela signifie que vous devez l'activer GuardDuty dans chaque région que vous souhaitez surveiller.

Bonnes pratiques

- Activer GuardDuty dans tous les appareils pris en charge Régions AWS. GuardDuty peut générer des informations concernant des activités non autorisées ou inhabituelles, même dans les régions que vous n'utilisez pas activement. La tarification GuardDuty est basée sur le nombre d'événements analysés. Même dans les régions où vous n'utilisez pas de charges de travail, l'activation GuardDuty constitue un outil de détection efficace et rentable qui vous alerte en cas d'activité potentiellement malveillante. Pour plus d'informations sur les régions où cette GuardDuty option est disponible, consultez Amazon GuardDuty Service Endpoints (Références générales AWS).
- Dans chaque région, déléguez le security-tooling-prodcompte à administrer GuardDuty pour votre organisation. Pour plus d'informations, consultez la section Désignation d'un administrateur GuardDuty délégué (GuardDuty documentation).
- Configurez GuardDuty pour inscrire automatiquement les nouveaux membres au Comptes AWS fur et à mesure qu'ils sont ajoutés à l'organisation. Pour plus d'informations, voir Étape 3 - Automatiser l'ajout de nouveaux comptes d'organisation en tant que membres dans Gestion des comptes avec AWS Organizations (GuardDuty documentation).

Amazon Macie

Amazon Macie est un service totalement géré de sécurité et de confidentialité des données qui utilise le machine learning et la correspondance de modèles pour identifier, surveiller et protéger vos données sensibles dans Amazon Simple Storage Service (Amazon S3). Vous pouvez exporter des données depuis Amazon Relational Database Service (Amazon RDS) et Amazon DynamoDB dans un compartiment S3, puis utiliser Macie pour analyser les données.

Lorsque vous utilisez Macie avec AWS Organizations, le compte de gestion de l'organisation peut désigner n'importe quel compte de l'organisation comme compte administrateur Macie. Le compte administrateur peut activer et gérer Macie pour les comptes membres de l'organisation, accéder aux données d'inventaire Amazon S3 et exécuter des tâches de découverte de données sensibles pour les comptes. Pour plus d'informations, veuillez consulter la rubrique Managing accounts with AWS Organizations (documentation Macie).

Macie est un service régional. Cela signifie que vous devez activer Macie dans chaque région que vous souhaitez surveiller et que le compte administrateur Macie ne peut gérer les comptes membres que dans la même région.

Bonnes pratiques

- Adhérez aux Considerations and recommendations for using Macie with AWS Organizations (documentation Macie).
- Dans chaque région, déléguez le security-tooling-prodcompte pour administrer Macie pour votre organisation. Pour gérer de manière centralisée plusieurs comptes Macie Régions AWS, le compte de gestion doit se connecter à chaque région dans laquelle l'organisation utilise actuellement ou utilisera Macie, puis désigner le compte administrateur Macie dans chacune de ces régions. Le compte administrateur Macie peut ensuite configurer l'organisation dans chacune de ces régions. Pour plus d'informations, veuillez consulter la rubrique Integrating and configuring an organization (documentation Macie).
- Macie propose une offre gratuite mensuelle pour les tâches de découverte de données sensibles. Si des données sensibles sont stockées dans Amazon S3, utilisez Macie pour analyser vos compartiments S3 dans le cadre de l'offre gratuite mensuelle. Si vous dépassez l'offre gratuite, des frais de découverte de données sensibles commencent à être facturés sur votre compte.

AWS Security Hub

AWS Security Hubvous fournit une vue complète de votre état de sécurité dans AWS. Vous pouvez l'utiliser pour vérifier votre environnement par rapport aux normes et aux bonnes pratiques de l'industrie de la sécurité. Security Hub collecte des données de sécurité provenant de tous vos Comptes AWS services (y compris Macie) GuardDuty et des produits partenaires tiers pris en charge. Security Hub vous aide à analyser les tendances en matière de sécurité et à identifier les problèmes de sécurité hautement prioritaires. Security Hub propose différentes normes de sécurité que vous pouvez activer pour effectuer des contrôles de conformité dans chaque Compte AWS.

Lorsque vous utilisez Security Hub avec AWS Organizations, le compte de gestion de l'organisation peut désigner n'importe quel compte de l'organisation comme compte administrateur du Security Hub. Le compte administrateur de Security Hub peut ensuite activer et gérer les autres comptes membres de l'organisation. Pour plus d'informations, consultez la section Utilisation AWS Organizations pour gérer les comptes (documentation Security Hub).

Security Hub est un service régional. Cela signifie que vous devez activer Security Hub dans chaque région que vous souhaitez analyser et dans AWS Organizations laquelle vous devez définir l'administrateur délégué pour chaque région.

Bonnes pratiques

- Adhérez aux Prerequisites and recommendations (documentation Security Hub).
- Dans chaque région, déléguez le security-tooling-prodcompte pour administrer Security Hub pour votre organisation. Pour plus d'informations, veuillez consulter la rubrique Designating a Security Hub administrator account (documentation Security Hub).
- Configurez Security Hub pour qu'il en inscrive automatiquement de nouveaux Comptes AWS lorsqu'ils sont ajoutés à l'organisation.
- Suivez la norme Pratiques exemplaires en matière de sécurité de base AWS (documentation Security Hub) pour détecter les cas où les ressources s'écartent des bonnes pratiques en matière de sécurité.
- Activez l'agrégation interrégionale (documentation Security Hub) afin que vous puissiez consulter et gérer tous vos résultats Security Hub d'une seule région.

Configuration des sauvegardes pour une architecture à comptes multiples

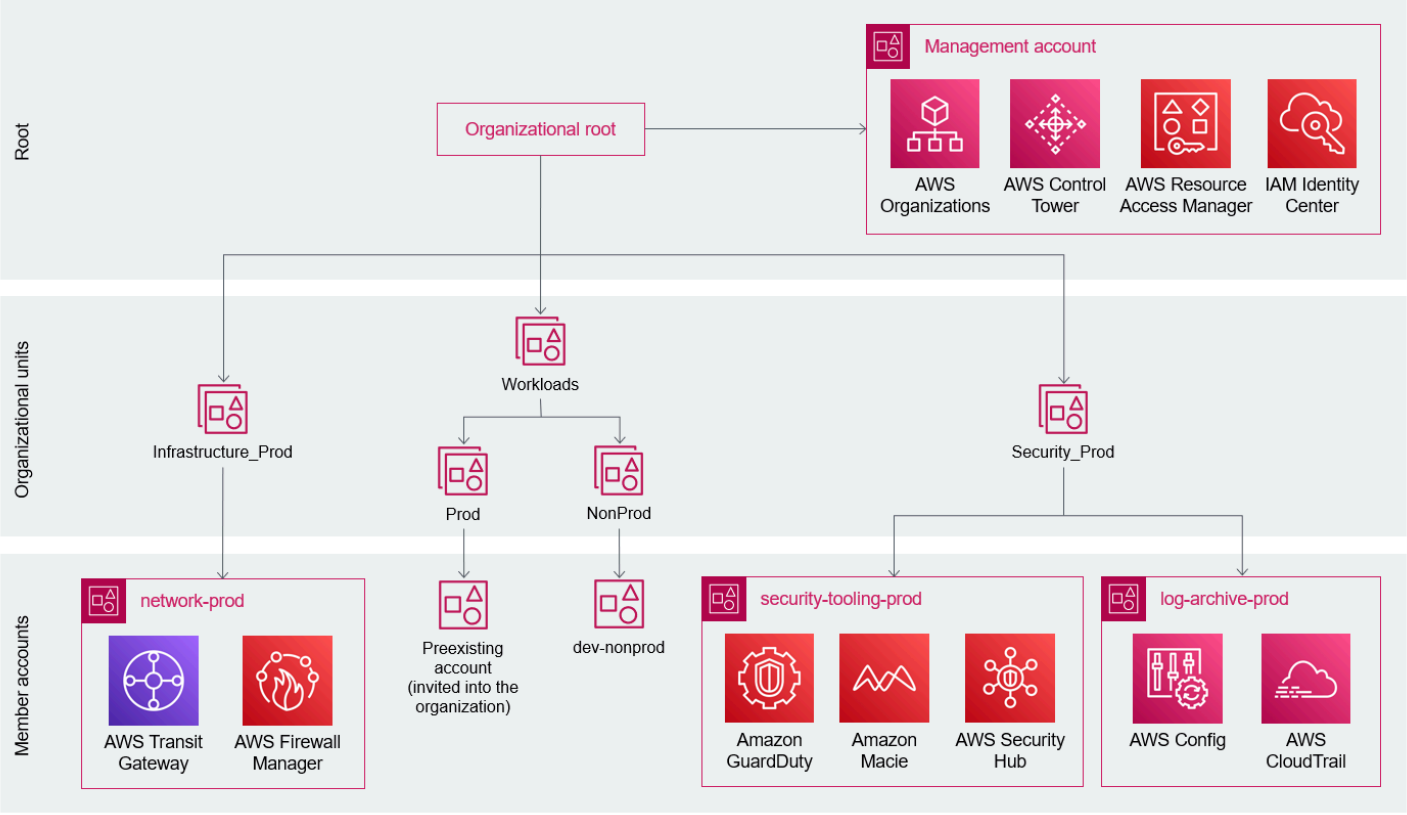
Une stratégie de sauvegarde complète est un élément essentiel du plan de protection des données d'une entreprise afin de résister à un événement de sécurité, de s'en remettre et d'en réduire l'impact. Type de stratégie qui vous aide à normaliser et à mettre en œuvre une stratégie de sauvegarde pour les ressources de tous les comptes de votre organisation. Dans une politique de sauvegarde, vous pouvez configurer et déployer des plans de sauvegarde pour vos ressources. Pour plus d'informations, consultez la section Politiques de sauvegarde (AWS Organizations documentation). Pour plus d'informations, consultez les 10 meilleures pratiques de sécurité pour sécuriser les sauvegardes dans AWS (directives AWS prescriptives).

Migration de compte lors de la transition vers une architecture à comptes multiples

Dans Inviter votre compte préexistant, vous avez invité votre compte préexistant à rejoindre l'unité d'organisation Charges de travail > Prod. Ce compte est désormais géré dans votre organisation.

Vous avez également configuré un nouveau compte dev-nonprod dans l'unité organisationnelle Workloads >. NonProd Les membres de l'équipe devraient désormais être en mesure d'accéder aux comptes appropriés via AWS IAM Identity Center. Supprimez tous les comptes utilisateur individuels dans AWS Identity and Access Management (IAM).

Si vous avez suivi les recommandations de ce guide, votre organisation a désormais la structure suivante.



Si des charges de travail sont exécutées dans le compte préexistant, vous pouvez désormais les migrer vers des comptes indépendants, conformément aux critères que vous avez définis dans Définir les critères de portée. Migrez toutes les charges de travail non liées à la production vers la nouvelle unité d'organisation dev-nonprod, puis migrez les charges de travail de production vers le

compte network-prod. Pour plus d'informations sur la migration AWS des ressources communes, consultez la section suivante de ce guide,Migration des ressources.

Réplication ou migration de ressources entre Comptes AWS

Après la migration d'une architecture mono-compte Compte AWS vers une architecture multi-comptes, il est courant que des charges de travail de production et non liées à la production soient exécutées dans le compte préexistant. La migration de ces ressources vers des comptes de production et autres que de production ou des unités d'organisation dédiés vous permet de gérer l'accès et la mise en réseau pour ces charges de travail. Voici quelques options pour migrer des AWS ressources communes vers une autre Compte AWS.

Cette section porte sur les politiques de réplication des données entre Comptes AWS. Vous devez faire en sorte que vos charges de travail soient aussi sans état que possible afin d'éviter de devoir répliquer les ressources de calcul entre les comptes. Il est également avantageux de gérer vos ressources par le biais de l'infrastructure en tant que code (IaC) afin de pouvoir réallouer un environnement dans un Compte AWS distinct.

Cette section examine les options de migration des ressources de données suivantes :

- AWS AppConfig configurations et environnements
- AWS Certificate Manager certificats
- CloudFront Distributions Amazon
- AWS CodeArtifact domaines et référentiels
- Tables Amazon DynamoDB
- Volumes Amazon EBS
- EC2 Instances Amazon ou AMIs
- Registres Amazon ECR
- Système de fichiers Amazon EFS
- Clusters Amazon ElastiCache (Redis OSS)
- AWS Elastic Beanstalk environnements
- Adresses IP Elastic
- AWS Lambda couches
- Instances Amazon Lightsail
- Clusters Amazon Neptune
- Domaines Amazon OpenSearch Service
- Instantanés Amazon RDS

- Cluster Amazon Redshift
- Domaines et zones hébergées Amazon Route 53
- Compartiments Amazon S3
- Modèles Amazon SageMaker AI
- AWS WAF web ACLs

AWS AppConfig configurations et environnements

AWS AppConfig ne prend pas en charge la copie directe de sa configuration vers une autre Compte AWS. Cependant, il est recommandé de gérer les AWS AppConfig configurations et les environnements séparément de ceux Comptes AWS qui les hébergent. Pour plus d'informations, voir Configuration entre comptes avec AWS AppConfig (article de AWS blog).

AWS Certificate Manager certificats

Vous ne pouvez pas exporter directement un certificat AWS Certificate Manager (ACM) d'un compte à un autre car la clé AWS Key Management Service (AWS KMS) utilisée pour chiffrer la clé privée du certificat est unique pour chaque Région AWS compte. Cependant, vous pouvez allouer simultanément plusieurs certificats avec le même nom de domaine sur plusieurs comptes et régions. ACM prend en charge la validation de la propriété du domaine à l'aide de DNS (recommandé) ou du courrier électronique. Lorsque vous utilisez la validation DNS et que vous créez un certificat, ACM génère un enregistrement CNAME unique pour chaque domaine du certificat. L'enregistrement CNAME est unique pour chaque compte, et il doit être ajouté à la zone hébergée Amazon Route 53 ou au fournisseur DNS dans les 72 heures pour que le certificat soit correctement validé.

CloudFront Distributions Amazon

Amazon CloudFront ne prend pas en charge la migration des distributions de l'une Compte AWS à l'autre Compte AWS. Cependant, CloudFront prend en charge la migration d'un nom de domaine alternatif, également appelé CNAME, d'une distribution à une autre. Pour plus d'informations, consultez Comment résoudre l'erreur CNAMEAlready Exists lorsque je configure un alias CNAME pour ma CloudFront distribution (AWS Knowledge Center).

AWS CodeArtifact domaines et référentiels

Bien qu'une organisation puisse avoir plusieurs domaines, il est recommandé de disposer d'un seul domaine de production contenant tous les artefacts publiés. Cela permet aux équipes de développement de rechercher et de partager des packages au sein d'une organisation. Le Compte AWS propriétaire du domaine peut être différent du compte propriétaire des référentiels associés au domaine. Vous pouvez copier des packages entre des référentiels, mais ils doivent appartenir au même domaine. Pour plus d'informations, voir Copier des packages entre des référentiels (CodeArtifact documentation).

Tables Amazon DynamoDB

Vous pouvez utiliser l'un des services suivants pour migrer une table Amazon DynamoDB vers un autre Compte AWS :

- AWS Backup
- Importation et exportation de DynamoDB vers Amazon S3
- Amazon S3 et AWS Glue
- AWS Data Pipeline
- Amazon EMR

Pour plus d'informations, consultez Comment puis-je migrer mes tables Amazon DynamoDB de l' Compte AWS une à l'autre AWS (Knowledge Center).

Volumes Amazon EBS

Vous pouvez prendre un instantané d'un volume Amazon Elastic Block Store (Amazon EBS) existant, partager cet instantané avec le compte de destination, puis créer une copie du volume dans ce compte. Cela permet de migrer le volume d'un compte à un autre. Pour plus d'informations, consultez Comment partager un instantané ou un volume Amazon EBS chiffré avec un autre Compte AWS (AWS Knowledge Center).

EC2 Instances Amazon ou AMIs

Il n'est pas possible de transférer directement des instances Amazon Elastic Compute Cloud (Amazon EC2) ou Amazon Machine Images (AMIs) existantes vers une autre instance Compte AWS.

Vous pouvez plutôt créer une AMI personnalisée dans le compte source, partager l'AMI avec le compte cible, lancer une nouvelle EC2 instance à partir de l'AMI partagée dans le compte cible, puis annuler l'enregistrement de l'AMI partagée.

Registres Amazon ECR

Amazon Elastic Container Registry (Amazon ECR) prend en charge la réplication entre comptes et entre régions. Vous configurez la réplication sur le registre source et une politique d'autorisations de registre sur le registre cible. Pour plus d'informations, veuillez consulter les rubriques Configuration de la réplication inter-comptes (documentation Amazon ECR) et Autoriser l'utilisateur racine d'un compte source à répliquer tous les référentiels (documentation Amazon ECR).

Système de fichiers Amazon EFS

Amazon Elastic File System (Amazon EFS) prend en charge la réplication entre comptes et entre régions. Vous pouvez configurer la réplication sur le système de fichiers source. Pour plus d'informations, consultez la section Réplication de systèmes de fichiers (documentation Amazon EFS).

Clusters Amazon ElastiCache (Redis OSS)

Vous pouvez utiliser une sauvegarde d'un cluster de base de données Amazon ElastiCache (Redis OSS) pour le migrer vers un autre compte. Pour plus d'informations, consultez Quelles sont les meilleures pratiques pour migrer mon cluster ElastiCache (Redis OSS) (AWS Knowledge Center).

AWS Elastic Beanstalk environnements

En effet AWS Elastic Beanstalk, vous pouvez utiliser des configurations enregistrées (documentation Elastic Beanstalk) pour migrer un environnement vers un autre. Compte AWS Pour plus d'informations, consultez Comment migrer mon environnement Elastic Beanstalk de l'un Compte AWSàAWS l'autre (Compte AWS Knowledge Center).

Adresses IP Elastic

Vous pouvez transférer des adresses IP élastiques entre deux Comptes AWS adresses situées dans le même emplacement Région AWS. Pour plus d'informations, veuillez consulter la rubrique Transfert d'adresses IP Elastic (documentation Amazon VPC).

AWS Lambda couches

Par défaut, une AWS Lambda couche que vous créez est privée pour votre Compte AWS. Toutefois, vous pouvez éventuellement partager la couche avec d'autres Comptes AWS personnes ou la rendre publique. Pour copier une couche, vous devez la reprovisionner dans une autre Compte AWS. Pour plus d'informations, consultez Configuration des autorisations de couche (documentation Lambda).

Instances Amazon Lightsail

Vous pouvez créer un instantané d'une instance Amazon Lightsail et l'exporter vers une Amazon Machine Image (AMI) et un instantané chiffré d'un volume Amazon EBS. Pour plus d'informations, consultez Exporter des instantanés Amazon Lightsail vers Amazon EC2 (documentation Lightsail). Par défaut, le snapshot est chiffré à l'aide d'une clé gérée par AWS créée dans AWS Key Management Service (AWS KMS). Toutefois, ce type de clé KMS ne peut pas être partagé entre eux Comptes AWS. Au lieu de cela, vous chiffrez manuellement une copie de l'AMI à l'aide d'une clé gérée par le client qui peut être utilisée depuis le compte de destination. Pour plus d'informations, consultez Autoriser les utilisateurs d'autres comptes à utiliser une clé KMS (AWS KMS documentation). Vous pouvez ensuite partager l'AMI copiée avec la cible Compte AWS et lancer une nouvelle EC2 instance pour Lightsail à partir de l'AMI copiée. Pour plus d'informations, consultez Lancer une instance à l'aide du nouvel assistant de lancement d'instance (EC2documentation Amazon).

Clusters Amazon Neptune

Vous pouvez copier un instantané automatique du cluster de base de données Amazon Neptune vers un autre Compte AWS. Pour plus d'informations, veuillez consulter la rubrique Copying a database (DB) cluster snapshot (documentation Neptune).

Vous pouvez également partager un instantané manuel avec un maximum de 20 Comptes AWS qui peuvent restaurer directement un cluster de base de données à partir de l'instantané. Pour plus d'informations, veuillez consulter la rubrique Sharing a DB Cluster Snapshot (documentation Neptune).

Domaines Amazon OpenSearch Service

Pour copier des données entre des domaines Amazon OpenSearch Service, vous pouvez utiliser Amazon S3 pour créer un instantané du domaine source, puis restaurer l'instantané dans un domaine

cible d'un autre domaine Compte AWS. Pour plus d'informations, consultez Comment restaurer les données d'un domaine Amazon OpenSearch Service dans un autre Compte AWS (AWS Knowledge Center).

Si vous disposez d'une connectivité réseau entre eux Comptes AWS, vous pouvez également utiliser la fonctionnalité de réplication entre clusters (documentation du OpenSearch service) dans OpenSearch Service.

Instantanés Amazon RDS

Pour Amazon Relational Database Service (Amazon RDS), vous pouvez partager des instantanés manuels d'instances ou de clusters de bases de données avec un maximum de 20 Comptes AWS. Vous pouvez ensuite restaurer l'instance ou le cluster de base de données à partir de l'instantané partagé. Pour plus d'informations, consultez Comment partager des instantanés de base de données Amazon RDS manuels ou des instantanés de cluster de bases de données Aurora avec un autre utilisateur Compte AWS (AWS Knowledge Center).

Vous pouvez également utiliser AWS Database Migration Service (AWS DMS) pour configurer la réplication continue entre les instances de base de données de différents comptes. Cependant, cela nécessite une connectivité réseau entre les comptes, telle que l'appairage de VPC ou une passerelle de transit.

Cluster Amazon Redshift

Pour migrer un cluster Amazon Redshift vers un autre Compte AWS, vous devez créer un instantané manuel du cluster dans le compte source, partager l'instantané avec la cible Compte AWS, puis restaurer le cluster à partir de l'instantané. Pour plus d'informations, consultez Comment copier un cluster provisionné Amazon Redshift vers un autre Compte AWS (AWS Knowledge Center).

Domaines et zones hébergées Amazon Route 53

Vous pouvez transférer des domaines Amazon Route 53 entre Comptes AWS. Pour plus d'informations, veuillez consulter la rubrique Transfer a domain to a different Compte AWS (documentation Route 53).

Vous pouvez également migrer une zone hébergée Route 53 vers une autre Compte AWS. Pour plus d'informations sur les cas où cette opération est recommandée ou requise, veuillez consulter

la rubrique Migration d'une zone hébergée vers un autre Compte AWS (documentation Route 53). Lorsque vous migrez une zone hébergée, vous la recréez dans le Compte AWS cible. Pour plus d'instructions, veuillez consulter la rubrique Migration d'une zone hébergée vers un autre Compte AWS(documentation Route 53).

Compartiments Amazon S3

Vous pouvez utiliser la réplication dans une même région Amazon Simple Storage Service (Amazon S3) pour copier des objets entre compartiments S3 d'une même Région AWS. Pour plus d'informations, veuillez consulter la rubrique Réplication d'objets (documentation Amazon S3). Remarques :

- Remplacez le propriétaire de la réplique par Compte AWS celui qui possède le compartiment de destination. Pour plus d'instructions, veuillez consulter la rubrique Modification du propriétaire d'un réplica (documentation Amazon S3).
- Mettez à jour les conditions du propriétaire du compartiment pour refléter l' Compte AWS ID du compartiment cible. Pour plus d'informations, veuillez consulter la rubrique Vérification de la propriété du compartiment avec la condition de propriétaire du compartiment (documentation Amazon S3).
- Depuis avril 2023, le paramètre obligatoire pour le propriétaire du bucket est activé pour les buckets nouvellement créés, ce qui rend les listes de contrôle d'accès aux compartiments (ACLs) et les objets ACLs inefficaces. Pour plus d'informations, consultez les modifications de sécurité d'Amazon S3 à venir (article de AWS blog).
- Vous pouvez utiliser Réplication d'objets existants via la réplication par lot S3 (documentation Amazon S3) pour répliquer des objets qui existaient avant la configuration de la réplication.

Modèles Amazon SageMaker AI

SageMaker Les modèles d'IA sont stockés dans un compartiment Amazon S3 pendant l'entraînement. En accordant l'accès au compartiment S3 depuis le compte de destination, vous pouvez déployer un modèle stocké dans le compte source vers le compte de destination. Pour plus d'informations, consultez Comment déployer un modèle Amazon SageMaker AI sur un autre Compte AWS (AWS Knowledge Center).

AWS WAF web ACLs

AWS WAF les listes de contrôle d'accès Web (Web ACLs) doivent résider dans le même compte que les ressources auxquelles elles sont associées, telles que les CloudFront distributions Amazon, les équilibreurs de charge d'application, Amazon API Gateway REST et APIs AWS AppSync GraphQL APIs. Vous pouvez l'utiliser AWS Firewall Manager pour gérer le AWS WAF Web de manière centralisée ACLs dans l'ensemble de votre organisation, dans AWS Organizations et entre les régions. Pour plus d'informations, veuillez consulter la rubrique Getting started with AWS Firewall Manager AWS WAF policies (documentation Firewall Manager).

Considérations relatives à la facturation lors de la transition vers une architecture multi-comptes

Si vous optez AWS Organizations pour la transition vers la facturation multiple Comptes AWS, vous pouvez utiliser la fonctionnalité de facturation consolidée (AWS Organizations documentation). Cette fonctionnalité fournit une facture unique et combinée qui indique les frais sur plusieurs comptes.

Vous trouverez ci-dessous les meilleures pratiques de facturation et les recommandations relatives à la transition vers plusieurs comptes :

- Si vous avez besoin d'accéder à vos données de facturation historiques, avant d'accepter l'invitation à rejoindre une organisation, créez un rapport sur les coûts et l'utilisation (AWS Cost and Usage Report documentation) pour exporter les données de facturation historiques du compte vers un bucket Amazon Simple Storage Service (Amazon S3). Une fois que vous avez accepté l'invitation à rejoindre l'organisation, les données de facturation historiques du compte ne sont plus accessibles.
- Si vous devez combiner deux organisations, par exemple pour une fusion ou une acquisition, vous pouvez utiliser l'évaluation des comptes pour AWS Organizations (bibliothèque de AWS solutions) pour évaluer les politiques basées sur les ressources de chaque organisation et identifier les problèmes potentiels avant de les combiner.

Conclusion

La transition d'un compte unique Compte AWS à plusieurs comptes peut sembler difficile au début sans stratégie d'adoption. En mettant en œuvre une stratégie à comptes multiples, vous pouvez relever de nombreux défis auxquels les entreprises sont confrontées lorsqu'elles utilisent un Compte AWS unique :

- Confondre les données de production AWS IAM Identity Center avec les données de développement — Vous pouvez accorder des autorisations et des accès différents en utilisant des ensembles d'autorisations distincts pour les unités organisationnelles de production et de non-production. Seuls les utilisateurs disposant de privilèges élevés doivent avoir accès à la base de données de production, et cet accès doit être limité dans le temps et audité.
- Déploiement de la production affectant d'autres opérations métier : vous pouvez séparer les parties prenantes en utilisant plusieurs comptes et environnements. Par exemple, vous pouvez créer un environnement de démonstration commerciale dédié, au sein d'un compte autre que de production, afin de pouvoir planifier des déploiements et des publications en l'absence de démonstrations.
- Faible performance des charges de production lors du test des charges de travail de développement : chaque service Compte AWS dispose de quotas de service indépendants qui régissent chaque service. En utilisant plusieurs comptes, vous pouvez limiter l'impact d'un environnement sur un autre environnement.
- Distinction entre les coûts de production et les coûts de développement : la facturation consolidée de l'organisation regroupe tous les coûts au niveau du Compte AWS , ce qui permet à l'équipe financière de voir le montant des coûts de production par rapport aux environnements autres que de production, tels que les environnements de développement, de test et de démonstration. Vous pouvez également utiliser des balises et des politiques de balisage pour séparer les coûts au sein d'un compte.
- Limitation de l'accès aux données sensibles : IAM Identity Center vous permet de définir des politiques d'accès distinctes pour un groupe de personnes associées à un compte spécifique.
- Contrôle des coûts : en utilisant des politiques de contrôle des services (SCPs) dans une architecture multi-comptes, vous pouvez interdire l'accès à des informations spécifiques Services AWS susceptibles d'entraîner des coûts élevés pour votre organisation. SCPs peut refuser tout accès à des services spécifiques ou peut limiter l'utilisation d'un service à un type spécifique, par exemple en limitant les types d'instances Amazon Elastic Compute Cloud (Amazon EC2) qui peuvent être créées.

Collaborateurs

Les personnes qui ont contribué à ce document incluent :

- Justin Plock, architecte principal des solutions, AWS (auteur principal)
- Emily Arnautovic, architecte principale, AWS
- Jason DiDomenico, architecte de solutions senior, AWS
- Michael Leighty, architecte de solutions spécialisé en sécurité senior, AWS
- Jesse Lepich, architecte de solutions spécialisé en sécurité senior, AWS
- Rodney Lester, architecte principal des solutions, AWS
- Israël Lopez Moriano, architecte de solutions, AWS
- George Rolston, architecte de solutions senior, AWS
- Alex Torres, architecte de solutions senior, AWS
- Dave Walker, architecte principal des solutions, AWS

Ressources

AWS Conseils prescriptifs

- AWS Base de référence de sécurité au démarrage (AWS SSB)
- AWS Architecture de référence de sécurité (AWS SRA)
- Les 10 meilleures pratiques de sécurité pour sécuriser les sauvegardes dans AWS

AWS articles de blog

- How Setting Up IAM Users and IAM Roles Can Help Keep Your Startup Secure
- How to let builders create IAM resources while improving security and agility for your organization

AWS Livres blancs

- Organisation de votre AWS environnement à l'aide de plusieurs comptes
- Établissement de la base de votre cloud sur AWS
- Création d'une infrastructure réseau multi-VPC AWS évolutive et sécurisée

AWS exemples de code

- Automatisez la configuration des services de sécurité avec AWS Control Tower (GitHub)

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
Politiques de contrôle des ressources	Nous avons ajouté des informations sur les politique s de contrôle des ressources dans la section Configurer une organisation.	20 novembre 2024
Meilleures pratiques en matière de sortie centralisée	Nous avons mis à jour les meilleures pratiques pour sécuriser le trafic sortant.	6 mai 2024
Bonnes pratiques organisat ionnelles	Nous avons mis à jour les bonnes pratiques pour créer une organisation dans AWS Organizations.	4 décembre 2023
Considérations sur la facturati on	Nous avons ajouté la section Considérations sur la facturati on.	20 septembre 2023
Migration des ressources, connectivité des applications et Amazon VPC Lattice	Nous avons ajouté les sections Migration de ressources et Connecter des applications. Nous avons également ajouté des informati ons sur un nouveau Service AWS, Amazon Virtual Private Cloud (Amazon VPC) Lattice.	27 avril 2023
Historique du compte et ABAC	Nous avons révisé la section Créer une zone d'atterrissage pour ajouter des informations	6 janvier 2023

	sur la façon de vérifier que vos nouveaux Comptes AWS utilisateurs disposent d'un historique d'utilisation afin que vous puissiez les ajouter à votre zone AWS Control Tower d'atterrissage. Nous avons également révisé la section Ajouter des utilisateurs initiaux pour ajouter des informations sur la manière dont vous pouvez utiliser le contrôle d'accès par attributs (ABAC) afin de transmettre la méthode d'authentification d'un IdP basé sur SAML à AWS IAM Identity Center.	
Réseau de trafic sortant	Nous avons révisé la section Sortie centralisée pour ajouter des informations sur l'utilisation du pare-feu Amazon Route 53 Resolver DNS afin de limiter le trafic de sortie à des noms de domaine spécifiques.	13 octobre 2022
Sécurité du trafic sortant	Nous avons ajouté Bonnes pratiques pour sécuriser le trafic sortant.	6 octobre 2022

Limites d'autorisations	Nous avons amélioré la définition d'une limite des autorisations, et dans la section Ressources, nous avons ajouté un nouveau lien pour obtenir davantage d'informations sur ce sujet.	22 septembre 2022
Publication initiale	—	6 septembre 2022

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.