Mise en œuvre de politiques relatives aux autorisations de moindre privilège pour AWS CloudFormation

AWS Directives prescriptives

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Directives prescriptives: Mise en œuvre de politiques relatives aux autorisations de moindre privilège pour AWS CloudFormation

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques commerciales et la présentation commerciale d'Amazon ne peuvent pas être utilisées en relation avec un produit ou un service extérieur à Amazon, d'une manière susceptible d'entraîner une confusion chez les clients, ou d'une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d'Amazon sont la propriété de leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

Table of Contents

Mise en œuvre de politiques relatives aux autorisations de moindre privilège pour AWS CloudFormation

Nima Fotouhi et Moumita Saha, Amazon Web Services ()AWS

Mai 2023 (historique du document)

AWS CloudFormationest un service d'infrastructure sous forme de code (IaC) qui vous aide à adapter le développement de votre infrastructure cloud en provisionnant AWS des ressources. Il vous aide également à gérer ces ressources tout au long de leur cycle de vie, de bout Comptes AWS en bout Régions AWS. Dans CloudFormation, vous définissez des modèles qui servent de modèle pour un ensemble de ressources. Vous provisionnez ensuite ces ressources en créant et en déployant une pile, qui est un groupe de ressources connexes que vous gérez comme une seule unité. Vous pouvez également l'utiliser CloudFormation pour déployer des ensembles de piles, qui sont des groupes de piles que vous pouvez créer, mettre à jour et supprimer sur plusieurs comptes et Régions AWS en une seule opération. Ce guide fournit une vue d'ensemble de la manière dont vous pouvez implémenter les autorisations de moindre privilège AWS CloudFormation et les ressources mises en service par le biais de ce dernier. CloudFormation

Vous pouvez déployer des CloudFormation piles ou des ensembles de piles en effectuant l'une des opérations suivantes :

- Accédez directement à l' AWS environnement via un principal AWS Identity and Access Management (IAM) et déployez des CloudFormation piles.
- Transférez les CloudFormation piles dans un pipeline de déploiement et lancez le déploiement des piles via le pipeline. Le pipeline accède à l' AWS environnement via un principal IAM et déploie les piles. Cette approche est une bonne pratique recommandée.

Pour l'une ou l'autre de ces approches, des autorisations sont requises pour déployer des CloudFormation piles. Prenons l'exemple d'un utilisateur qui prévoit de l'utiliser CloudFormation pour créer une instance Amazon Elastic Compute Cloud (Amazon EC2). Cette instance nécessiterait un profil d'instance IAM pour accéder à un autre Services AWS. Le principal IAM utilisé pour déployer la CloudFormation pile aurait besoin des autorisations suivantes :

- Autorisations d'accès CloudFormation
- Autorisations pour créer des piles dans CloudFormation

- Autorisations pour créer des instances sur Amazon EC2
- Autorisations pour créer les profils d'instance IAM requis

Qu'est-ce que le moindre privilège ?

Le moindre privilège est la bonne pratique de sécurité qui consiste à accorder les autorisations minimales nécessaires à l'exécution d'une tâche. Le principe du moindre privilège fait partie du pilier de sécurité du AWS Well-Architected Framework. Lorsque vous mettez en œuvre cette bonne pratique, elle peut contribuer à protéger votre AWS environnement contre les risques d'augmentation des privilèges, à réduire la surface d'attaque, à améliorer la sécurité des données et à prévenir les erreurs des utilisateurs (telles que la mauvaise configuration ou la suppression d'une ressource par erreur).

Pour implémenter le moindre privilège pour vos AWS ressources, vous configurez des politiques, telles que les politiques basées sur l'identité dans AWS Identity and Access Management (IAM). Ces politiques définissent les autorisations et précisent les conditions d'accès. Organisations peuvent commencer par des politiques AWS gérées, mais elles créent ensuite généralement des politiques personnalisées qui limitent l'étendue des autorisations aux seules actions requises pour la charge de travail ou le cas d'utilisation.

Les autorisations de moindre privilège pour le CloudFormation service constituent une considération de sécurité importante. Étant donné que les utilisateurs et les développeurs qui interagissent avec eux CloudFormation peuvent créer, modifier ou supprimer rapidement des ressources à grande échelle, le moindre privilège est particulièrement essentiel. Cependant, CloudFormation nécessite les autorisations nécessaires pour créer, mettre à jour et modifier des ressources dans votre Comptes AWS. Vous devez trouver un équilibre entre le besoin d'autorisations pour fonctionner CloudFormation et le principe du moindre privilège.

Lorsque vous appliquez le principe du moindre privilège à CloudFormation, vous devez tenir compte des points suivants :

- Autorisations pour le CloudFormation service : à quels utilisateurs ont-ils besoin d'accéder CloudFormation, de quel niveau d'accès ont-ils besoin et quelles actions peuvent-ils entreprendre pour créer, mettre à jour ou supprimer des piles ?
- Autorisations de mise à disposition des ressources : par le biais de quelles ressources les utilisateurs peuvent-ils fournir CloudFormation ?

- Autorisations pour les ressources allouées — Comment configurez-vous les autorisations de moindre privilège pour les ressources que vous mettez à disposition ? CloudFormation

Résultats commerciaux ciblés

En suivant les meilleures pratiques et les recommandations de ce guide, vous pouvez :

- Déterminez les utilisateurs de votre organisation qui ont besoin d'un accès CloudFormation, puis configurez les autorisations du moindre privilège pour ces utilisateurs.
- Utilisez des politiques de pile pour protéger les CloudFormation piles contre les mises à jour involontaires.
- Configurez les autorisations de moindre privilège pour CloudFormation les utilisateurs et les ressources afin d'éviter l'augmentation des privilèges et le problème de confusion lié aux adjoints.
- AWS CloudFormation À utiliser pour provisionner AWS des ressources avec des autorisations de moindre privilège. Cela permet à votre entreprise de maintenir une posture de sécurité plus robuste.
- Réduisez de manière proactive le temps, l'énergie et l'argent nécessaires pour enquêter sur les incidents de sécurité et les atténuer.

Public visé

Ce guide est destiné aux architectes d'infrastructure cloud, aux DevOps ingénieurs et aux ingénieurs de fiabilité des sites (SREs) qui gèrent et fournissent des ressources en utilisant CloudFormation.

Utilisation de politiques d'accès pour accorder des autorisations dans AWS

Vous gérez l'accès en AWS créant des politiques basées sur l'identité et en les associant à des principes AWS Identity and Access Management (IAM), tels que des rôles ou des utilisateurs, et en créant des politiques basées sur les ressources et en les associant aux ressources. AWS AWS évalue ces politiques chaque fois qu'une demande est faite. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée.

Pour comprendre comment configurer l'accès au moindre privilège dans les politiques, vous devez comprendre les différents types de politiques, les éléments et la structure d'une politique, ainsi que la manière dont les politiques sont évaluées. Ce guide se concentre uniquement sur les politiques basées sur l'identité et les politiques basées sur les ressources. Cependant, AWS fournit d'autres types de politiques, telles que les politiques de contrôle des services (SCPs), les limites d'autorisations et les politiques de session. Chaque type de politique joue un rôle dans la mise en œuvre des autorisations du moindre privilège dans votre. Comptes AWS Pour plus d'informations, consultez les sections Politiques et autorisations et Appliquer les autorisations du moindre privilège dans la documentation IAM.

Configuration des autorisations de moindre privilège à utiliser CloudFormation

Ce chapitre passe en revue les options de configuration des autorisations d'accès et d'utilisation du AWS CloudFormation service.

Lorsqu'un utilisateur ou un service AWS fournit des ressources CloudFormation, la première étape consiste à appeler le CloudFormation service via un principal AWS Identity and Access Management (IAM). Ce principal IAM doit disposer des autorisations nécessaires pour créer les CloudFormation piles. Ensuite, le directeur IAM utilise l'une des approches suivantes pour fournir des ressources par le biais CloudFormation de :

- Si le principal IAM ne transmet pas les opérations de pile à un rôle de CloudFormation service, CloudFormation utilise les informations d'identification du principal IAM pour effectuer les opérations de pile. Il s'agit de l'option par défaut. Par conséquent, outre les autorisations nécessaires pour effectuer les opérations de CloudFormation stack, le principal IAM a également besoin d'autorisations pour fournir les ressources définies dans les CloudFormation modèles qu'il utilisera. Par exemple, si le responsable de l'IAM n'est pas autorisé à créer des instances Amazon Elastic Compute Cloud (Amazon EC2), il ne peut pas créer une CloudFormation pile qui fournirait une EC2 instance Amazon.
- Si le principal IAM transmet les opérations de pile à un rôle de CloudFormation service, il CloudFormation utilise ensuite le rôle de service pour effectuer les opérations de pile et provisionner les ressources dans le CloudFormation modèle. Ce rôle CloudFormation de service doit être défini avec les autorisations nécessaires pour Services AWS le fournir au nom du principal IAM. Cette approche évite d'accorder des autorisations directes au principal IAM pour fournir les AWS ressources définies dans les CloudFormation modèles. Le principal IAM a besoin d'autorisations de création de CloudFormation pile et CloudFormation utilise la politique du rôle de service pour passer des appels au lieu de la politique du principal IAM.

En utilisant l'approche des rôles de service et le principe du moindre privilège, vous pouvez standardiser le provisionnement des ressources dans votre AWS environnement et exiger que les utilisateurs fournissent les ressources sous forme d'IaC via iAc. CloudFormation Étant donné que les politiques associées aux principes IAM ne contiennent pas d'autorisations permettant de provisionner directement des AWS ressources, les utilisateurs doivent les utiliser CloudFormation pour les provisionner.

Ce chapitre passe en revue les mécanismes suivants pour configurer et gérer l'accès au CloudFormation service et aux CloudFormation piles :

- Stratégies basées sur l’identité pour CloudFormation— Utilisez ce type de politique pour configurer les adresses auxquelles les principaux IAM peuvent accéder CloudFormation et les actions qu'ils peuvent effectuer. CloudFormation
- Rôles de service pour CloudFormation— Créez un rôle de service qui permet de CloudFormation créer, de mettre à jour ou de supprimer des ressources de pile pour le compte du principal IAM qui déploie la pile. Le rôle de service est créé dans IAM et peut être associé à une ou plusieurs piles.
- CloudFormation politiques de pile— Utilisez ce type de politique pour déterminer quand une pile peut être mise à jour. Ce type de politique permet d'éviter que les ressources de pile ne soient mises à jour ou supprimées par inadvertance. Des politiques de stack sont créées et associées aux stacks in CloudFormation.

Stratégies basées sur l’identité pour CloudFormation

Tenez compte des types d'utilisateurs auxquels il est nécessaire d'accéder et des actions que ces utilisateurs doivent effectuer CloudFormation. AWS CloudFormation Vous configurez les autorisations des utilisateurs par le biais de politiques basées sur l'identité, que vous associez à un principal AWS Identity and Access Management (IAM), tel qu'un rôle ou un utilisateur.

Lorsque vous configurez une politique basée sur l'identité, les `Resource` éléments `EffectAction`, et sont obligatoires. Vous pouvez également définir un `Condition` élément en option. Pour plus d'informations sur ces éléments, consultez la référence des éléments de politique IAM JSON.

Cette section contient les rubriques suivantes :

- Meilleures pratiques pour configurer des politiques basées sur l'identité pour un accès avec le moindre privilège CloudFormation
- Exemples de politiques basées sur l'identité pour CloudFormation

Meilleures pratiques pour configurer des politiques basées sur l'identité pour un accès avec le moindre privilège CloudFormation

- Pour les responsables IAM qui ont besoin d'autorisations d'accès CloudFormation, vous devez trouver un équilibre entre le besoin d'autorisations pour fonctionner CloudFormation et le principe

du moindre privilège. Pour vous aider à respecter le principe du moindre privilège, nous vous recommandons de définir l'identité du principal IAM à l'aide d'actions spécifiques qui permettent au principal d'effectuer les opérations suivantes :

- Créez, mettez à jour et supprimez une CloudFormation pile.
- Transmettez un ou plusieurs rôles de service dotés des autorisations requises pour déployer les ressources définies dans les CloudFormation modèles. Cela permet d' CloudFormation assumer le rôle de service et de fournir les ressources de la pile pour le compte du principal IAM.

- L'augmentation des privilèges fait référence à la capacité d'un utilisateur disposant d'un accès à augmenter ses niveaux d'autorisation et à compromettre la sécurité. Le principe du moindre privilège est une bonne pratique importante qui peut aider à prévenir l'augmentation des privilèges. Dans la mesure où il CloudFormation prend en charge le provisionnement de types de ressources IAM, tels que les politiques et les rôles, un principal IAM peut augmenter ses privilèges en : CloudFormation
  - Utilisation d'une CloudFormation pile pour doter un principal IAM d'autorisations, de politiques ou d'informations d'identification hautement privilégiées — Pour éviter cela, nous recommandons d'utiliser des dispositifs de protection des autorisations afin de limiter le niveau d'accès pour les principaux IAM. Les barrières de protection des autorisations définissent le nombre maximum d'autorisations qu'une politique basée sur l'identité peut accorder à un principal IAM. Cela permet d'empêcher l'augmentation intentionnelle et involontaire des privilèges. Vous pouvez utiliser les types de politiques suivants pour protéger les autorisations :
    - Les limites d'autorisations définissent les autorisations maximales qu'une politique basée sur l'identité peut accorder à un principal IAM. Pour plus d'informations, consultez la section Limites des autorisations pour les entités IAM.
    - Dans AWS Organizations, vous pouvez utiliser les politiques de contrôle des services (SCPs) pour définir le maximum d'autorisations disponibles au niveau de l'organisation. SCPs concernent uniquement les rôles et les utilisateurs IAM gérés par des comptes au sein de l'organisation. Vous pouvez les joindre SCPs à des comptes, à des unités organisationnelles ou à la racine de l'organisation. Pour de plus amples informations, veuillez consulter Effets des SCP sur les autorisations.
  - Création d'un rôle de CloudFormation service offrant des autorisations étendues — Pour éviter cela, nous vous recommandons d'ajouter les autorisations détaillées suivantes aux politiques basées sur l'identité pour les principaux IAM qui utiliseront : CloudFormation
    - Utilisez la clé de `cloudformation:RoleARN` condition pour contrôler les rôles CloudFormation de service que le principal IAM peut utiliser.

- N'`iam:PassRole`autorisez l'action que pour les rôles CloudFormation de service spécifiques que le principal IAM doit transmettre.

Pour plus d'informations, consultez Octroi d'autorisations principales à un IAM pour utiliser un rôle CloudFormation de service dans ce guide.

- Limitez les autorisations en utilisant des barrières de sécurité, telles que des limites d'autorisations et SCPs accordez des autorisations en utilisant une politique basée sur l'identité ou les ressources.

Exemples de politiques basées sur l'identité pour CloudFormation

Cette section contient des exemples de politiques basées sur l'identité qui montrent comment accorder et refuser des autorisations pour. CloudFormation Vous pouvez utiliser ces exemples de politiques pour commencer à concevoir vos propres politiques conformes au principe du moindre privilège.

Pour obtenir la liste des actions et conditions CloudFormation spécifiques, consultez la section Actions, ressources et clés de condition pour AWS CloudFormation et AWS CloudFormation conditions. Pour une liste des types de ressources à utiliser avec les conditions, consultez la référence des types de AWS ressources et de propriétés.

Cette section contient les exemples de politiques suivants :

- Autoriser l'accès à la vue
- Autoriser la création de piles en fonction d'un modèle
- Refuser la mise à jour ou la suppression d'une pile

Autoriser l'accès à la vue

L'accès à la vue est le type d'accès le moins privilégié à. CloudFormation Ce type de politique peut être approprié pour les directeurs IAM qui souhaitent consulter toutes les CloudFormation piles du. Compte AWS L'exemple de politique suivant accorde des autorisations pour consulter les détails de n'importe quelle CloudFormation pile du compte.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```
      "Action": [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources"
      ],
      "Resource": "*"
    }
  ]
}
```

Autoriser la création de piles en fonction d'un modèle

L'exemple de politique suivant permet aux responsables IAM de créer des piles en utilisant uniquement les CloudFormation modèles stockés dans un compartiment Amazon Simple Storage Service (Amazon S3) spécifique. Le nom du bucket est`my-CFN-templates`.
Vous pouvez télécharger des modèles approuvés dans ce compartiment. La clé de `cloudformation:TemplateUrl` condition contenue dans la politique empêche le principal IAM d'utiliser d'autres modèles pour créer des piles.

> **Important**
>
> Autorisez le principal IAM à avoir un accès en lecture seule à ce compartiment S3. Cela permet d'empêcher le directeur IAM d'ajouter, de supprimer ou de modifier les modèles approuvés.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "cloudformation:TemplateUrl": "https:// my-CFN-templates.s3.amazonaws.com/*"
        }
```

```
      }
    }
  ]
}
```

Refuser la mise à jour ou la suppression d'une pile

Pour protéger les CloudFormation piles spécifiques qui fournissent des AWS ressources critiques pour l'entreprise, vous pouvez limiter les actions de mise à jour et de suppression pour cette pile spécifique. Vous pouvez autoriser ces actions uniquement pour quelques principes IAM spécifiés et les refuser pour tout autre principal IAM de l'environnement. La déclaration de politique suivante refuse les autorisations de mise à jour ou de suppression d'une CloudFormation pile spécifique dans un Région AWS et spécifique Compte AWS.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "cloudformation:DeleteStack",
        "cloudformation:UpdateStack"
      ],
      "Resource": "arn:aws:cloudformation:us-east-1:123456789012:stack/
MyProductionStack/<stack_ID>"
    }
  ]
}
```

Cette déclaration de politique refuse les autorisations de mise à jour ou de suppression de la `MyProductionStack` CloudFormation pile, qui se trouve dans le `us-east-1` Région AWS et dans le `123456789012` Compte AWS. Vous pouvez consulter l'ID de pile dans la CloudFormation console. Voici quelques exemples de la manière dont vous pourriez modifier l'`Resource`élément de cette déclaration en fonction de votre cas d'utilisation :

- Vous pouvez ajouter plusieurs CloudFormation piles IDs dans l'`Resource`élément de cette politique.
- Vous pouvez l'utiliser `arn:aws:cloudformation:us-east-1:123456789012:stack/*` pour empêcher les principaux IAM de mettre à jour ou de supprimer toute pile présente dans `us-east-1` Région AWS et dans le `123456789012` compte.

Une étape importante consiste à décider quelle politique doit contenir cette déclaration. Vous pouvez ajouter cette déclaration aux politiques suivantes :

- La politique basée sur l'identité attachée au principal IAM : le fait de placer la déclaration dans cette politique empêche le principal IAM spécifique de créer ou de supprimer une pile spécifique. CloudFormation
- Une limite d'autorisations attachée au principal IAM : le fait d'intégrer la déclaration dans cette politique crée un garde-fou en matière d'autorisations. Cela empêche plusieurs principaux IAM de créer ou de supprimer une CloudFormation pile spécifique, mais cela ne restreint pas tous les principaux de votre environnement.
- Un SCP attaché à un compte, à une unité organisationnelle ou à une organisation : l'inclusion de cette déclaration dans cette politique crée un garde-fou en matière d'autorisations. Il empêche tous les principaux IAM du compte, de l'unité organisationnelle ou de l'organisation cible de créer ou de supprimer une pile spécifique. CloudFormation

  Toutefois, si vous n'autorisez pas au moins un principal IAM, un principal privilégié, à mettre à jour ou à supprimer la CloudFormation pile, vous ne pourrez apporter aucune modification, si nécessaire, aux ressources fournies via cette pile. Un utilisateur ou un pipeline de développement (recommandé) peut assumer ce principe privilégié. Si vous souhaitez déployer la restriction en tant que SCP, nous vous recommandons plutôt la déclaration de politique suivante.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "cloudformation:DeleteStack",
        "cloudformation:UpdateStack"
      ],
      "Resource": "arn:aws:cloudformation:us-east-1:123456789012:stack/
MyProductionStack/<stack_ID>",
      "Condition": {
        "ArnNotLike": {
          "aws:PrincipalARN": [
            "<ARN of the allowed privilege IAM principal>"
          ]
        }
      }
```

```
    }
  ]
}
```

Dans cette déclaration, l'`Condition`élément définit le principal IAM qui est exclu du SCP. Cette déclaration refuse à tout principal IAM l'autorisation de mettre à jour ou de supprimer des CloudFormation piles, sauf si l'ARN du principal IAM correspond à l'ARN de l'élément. `Condition` La clé de `aws:PrincipalARN` condition accepte une liste, ce qui signifie que vous pouvez exclure plusieurs principaux IAM des restrictions, selon les besoins de votre environnement. Pour un SCP similaire qui empêche toute modification des CloudFormation ressources, consultez SCP-CLOUDFORMATION-1 (). GitHub

Rôles de service pour CloudFormation

Un rôle de service est un rôle AWS Identity and Access Management (IAM) qui permet de créer, de mettre AWS CloudFormation à jour ou de supprimer des ressources de pile. Si vous ne fournissez pas de rôle de service, CloudFormation utilise les informations d'identification du principal IAM pour effectuer les opérations de pile. Si vous créez un rôle de service CloudFormation et que vous le spécifiez lors de la création de la pile, CloudFormation utilisez les informations d'identification du rôle de service pour effectuer les opérations, au lieu des informations d'identification du principal IAM.

Lorsque vous utilisez un rôle de service, la politique basée sur l'identité attachée au principal IAM ne nécessite pas d'autorisations pour fournir toutes les AWS ressources définies dans le modèle. CloudFormation Si vous n'êtes pas prêt à fournir AWS des ressources pour les opérations commerciales critiques par le biais d'un pipeline de développement (une bonne pratique AWS recommandée), l'utilisation d'un rôle de service peut ajouter un niveau de protection supplémentaire pour la gestion des ressources dans AWS. Les avantages de cette approche sont les suivants :

- Les responsables IAM de votre organisation suivent un modèle de moindre privilège qui les empêche de créer ou de modifier manuellement des AWS ressources dans votre environnement.
- Pour créer, mettre à jour ou supprimer AWS des ressources, les responsables IAM doivent utiliser. CloudFormation Cela normalise le provisionnement des ressources via l'infrastructure en tant que code.

Par exemple, pour créer une pile contenant une instance Amazon Elastic Compute Cloud (Amazon EC2), le responsable IAM doit être autorisé à créer des EC2 instances par le biais de sa politique

basée sur l'identité. CloudFormation Vous pouvez plutôt assumer un rôle de service autorisé à créer des EC2 instances pour le compte du principal. Avec cette approche, le principal IAM peut créer la pile, et vous n'avez pas besoin de lui accorder des autorisations trop larges pour un service auquel il ne devrait pas avoir un accès régulier.

Pour utiliser un rôle de service pour créer des CloudFormation piles, les principaux IAM doivent être autorisés à transmettre le rôle de service CloudFormation, et la politique de confiance du rôle de service doit CloudFormation permettre d'assumer ce rôle.

Cette section contient les rubriques suivantes :

- Implémentation du moindre privilège pour les rôles CloudFormation de service
- Configuration des rôles de service
- Octroi d'autorisations principales à un IAM pour utiliser un rôle CloudFormation de service
- Configuration d'une politique de confiance pour le rôle CloudFormation de service
- Associer un rôle de service à une pile

Implémentation du moindre privilège pour les rôles CloudFormation de service

Dans un rôle de service, vous définissez une politique d'autorisation qui spécifie explicitement les actions que le service peut effectuer. Il se peut que ces actions ne soient pas les mêmes que celles qu'un directeur IAM peut effectuer. Nous vous recommandons de revenir en arrière à partir de vos CloudFormation modèles pour créer un rôle de service conforme au principe du moindre privilège.

Le fait de définir correctement la politique basée sur l'identité d'un principal IAM pour ne transmettre que des rôles de service spécifiques et de définir la politique de confiance d'un rôle de service pour permettre uniquement à des principaux spécifiques d'assumer le rôle permet d'éviter une éventuelle augmentation de privilèges liée aux rôles de service.

Configuration des rôles de service

> **Note**
>
> Les rôles de service sont configurés dans IAM. Pour créer un rôle de service, vous devez disposer des autorisations nécessaires. Un directeur IAM autorisé à créer un rôle et à associer n'importe quelle politique peut augmenter ses propres autorisations. AWS

recommande de créer un rôle de service Service AWS pour chaque cas d'utilisation. Une fois que vous avez créé des rôles de CloudFormation service pour vos cas d'utilisation, vous pouvez autoriser les utilisateurs à ne transmettre que le rôle de service approuvé à CloudFormation. Pour des exemples de politiques basées sur l'identité qui permettent aux utilisateurs de créer des rôles de service, consultez la section Autorisations relatives aux rôles de service dans la documentation IAM.

Pour obtenir des instructions sur la création de rôles de service, voir Création d'un rôle pour déléguer des autorisations à un Service AWS. Spécifiez CloudFormation (`cloudformation.amazonaws.com`) en tant que service habilité à assumer le rôle. Cela empêche un directeur IAM d'assumer lui-même le rôle ou de le transmettre à d'autres services. Lorsque vous configurez un rôle de service`Effect`, les `Resource` éléments`Action`, et sont obligatoires. Vous pouvez également définir un `Condition` élément en option.

Pour plus d'informations sur ces éléments, consultez la référence des éléments de politique IAM JSON. Pour une liste complète des actions, des ressources et des clés de condition, voir Actions, ressources et clés de condition pour la gestion des identités et des accès.

Octroi d'autorisations principales à un IAM pour utiliser un rôle CloudFormation de service

Pour provisionner des ressources à CloudFormation l'aide du rôle de CloudFormation service, le principal IAM doit être autorisé à transmettre le rôle de service. Vous pouvez limiter les autorisations du principal IAM afin de ne transmettre que certains rôles en spécifiant l'ARN du rôle dans les autorisations du principal. Pour plus d'informations, consultez la section Octroi à un utilisateur des autorisations lui permettant de transmettre un rôle à un Service AWS dans la documentation IAM.

La déclaration de politique basée sur l'identité IAM suivante permet au directeur de transmettre les rôles, y compris les rôles de service, qui se trouvent dans le chemin. `cfnroles` Le directeur ne peut pas transmettre des rôles qui suivent un chemin différent.

```
{
"Sid": "AllowPassingAppRoles",
"Effect": "Allow",
"Action": "iam:PassRole",
"Resource": "arn:aws:iam::<account ID>:role/cfnroles/*"
}
```

Une autre approche pour limiter les principaux à certains rôles consiste à utiliser un préfixe pour les noms des rôles CloudFormation de service. La déclaration de politique suivante autorise les responsables IAM à transmettre uniquement les rôles dotés d'un `CFN-` préfixe.

```
{
"Sid": "AllowPassingAppRoles",
"Effect": "Allow",
"Action": "iam:PassRole",
"Resource": "arn:aws:iam::<account ID>:role/CFN-*"
}
```

Outre les déclarations de politique précédentes, vous pouvez utiliser la clé de `cloudformation:RoleARN` condition pour fournir des contrôles plus précis dans la politique basée sur l'identité, pour l'accès au moindre privilège. La déclaration de politique suivante autorise le principal IAM à créer, mettre à jour et supprimer des piles uniquement si elles transmettent un rôle de CloudFormation service spécifique. En variante, vous pouvez définir plusieurs rôles ARNs de CloudFormation service dans la clé de condition.

```
{
  "Sid": "RestrictCloudFormationAccess",
  "Effect": "Allow",
  "Action": [
    "cloudformation:CreateStack",
    "cloudformation:DeleteStack",
    "cloudformation:UpdateStack"
  ],
  "Resource": "arn:aws:iam::<account ID>:role/CFN-*",
  "Condition": {
    "StringEquals": {
      "cloudformation:RoleArn": [
        "<ARN of the specific CloudFormation service role>"
      ]
    }
  }
}
```

En outre, vous pouvez également utiliser la clé de `cloudformation:RoleARN` condition pour empêcher un principal IAM de transmettre un rôle de CloudFormation service hautement privilégié pour les opérations de stack. La seule modification requise concerne l'opérateur conditionnel, de `StringEquals` à`StringNotEquals`.

```
{
  "Sid": "RestrictCloudFormationAccess",
  "Effect": "Allow",
  "Action": [
    "cloudformation:CreateStack",
    "cloudformation:DeleteStack",
    "cloudformation:UpdateStack"
  ],
  "Resource": "arn:aws:iam::<account ID>:role/CFN-*",
  "Condition": {
    "StringNotEquals": {
      "cloudformation:RoleArn": [
        "<ARN of a privilege CloudFormation service role>"
      ]
    }
  }
}
```

Configuration d'une politique de confiance pour le rôle CloudFormation de service

Une politique de confiance des rôles est une politique obligatoire basée sur les ressources qui est attachée à un rôle IAM. Une politique de confiance définit les principaux IAM qui peuvent assumer ce rôle. Dans une politique de confiance, vous pouvez spécifier des utilisateurs, des rôles, des comptes ou des services en tant que principaux. Pour empêcher les principaux IAM de transmettre des rôles de service CloudFormation à d'autres services, vous pouvez définir CloudFormation comme principal la politique de confiance du rôle.

La politique de confiance suivante permet uniquement au CloudFormation service d'assumer le rôle de service.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": {
      "Service": "cloudformation.amazonaws.com"
    },
    "Action": "sts:AssumeRole"
  }
```

```
}
```

Associer un rôle de service à une pile

Une fois qu'un rôle de service est créé, vous pouvez l'associer à une pile lorsque vous créez la pile. Pour plus d'informations, consultez la section Configurer les options de pile. Avant de spécifier un rôle de service, assurez-vous que les principaux IAM sont autorisés à le transmettre. Pour de plus amples informations, veuillez consulter Octroi d'autorisations principales à un IAM pour utiliser un rôle CloudFormation de service.

CloudFormation politiques de pile

Les politiques de pile peuvent aider à empêcher les ressources de pile d'être mises à jour ou supprimées involontairement lors d'une mise à jour de pile. Une politique de pile est un document JSON qui définit les actions de mise à jour qui peuvent être effectuées sur des ressources désignées. Par défaut, tout principal IAM `cloudformation:UpdateStack` disposant d'autorisations peut mettre à jour toutes les ressources d'une AWS CloudFormation pile. Les mises à jour peuvent provoquer des interruptions ou supprimer et remplacer complètement des ressources. Vous pouvez utiliser une politique de pile pour configurer les autorisations du moindre privilège. Les politiques de pile peuvent fournir une couche de protection supplémentaire.

Par défaut, une politique de pile permet de protéger toutes les ressources de la pile. Cependant, le principal avantage des politiques de pile est qu'elles fournissent un contrôle granulaire pour chaque AWS ressource déployée dans une CloudFormation pile. Vous pouvez utiliser une politique de pile pour protéger uniquement des ressources spécifiques d'une pile et autoriser la mise à jour ou la suppression d'autres ressources de la même pile. Pour autoriser les mises à jour de ressources spécifiques, vous devez inclure une `Allow` déclaration explicite pour ces ressources dans votre politique de stack.

Les politiques relatives aux piles fournissent des contrôles préventifs pour les CloudFormation piles auxquelles elles sont associées. Chaque pile ne peut avoir qu'une seule politique de pile, mais vous pouvez utiliser cette politique de pile pour protéger toutes les ressources de cette pile. Vous pouvez appliquer une politique de pile à plusieurs piles.

Par exemple, imaginez que vous avez un pipeline qui produit des artefacts sensibles et les stocke temporairement dans un bucket Amazon Simple Storage Service (Amazon S3) pour un traitement ultérieur. Le compartiment S3 est approvisionné par CloudFormation, et tous les contrôles de sécurité

nécessaires sont en place. Sans politiques de stack, un développeur peut, intentionnellement ou non, modifier la destination des artefacts du pipeline vers un compartiment S3 moins sécurisé et exposer des données sensibles. Si une politique de pile est appliquée à la pile, elle empêche les utilisateurs autorisés d'effectuer des actions de mise à jour ou de suppression indésirables.

Cette section contient les rubriques suivantes :

- Configuration des politiques de stack
- Définition et remplacement des politiques de stack
- Politiques de limitation et d'exigence en matière de stack

Configuration des politiques de stack

Lorsque vous configurez une politique de pile`Effect`, les `Resource` éléments `ActionPrincipal`,, et sont obligatoires. Vous pouvez également définir un `Condition` élément en option.

Lorsque vous créez une politique de pile, par défaut, elle empêche les mises à jour pour toutes les ressources de la pile. Vous personnalisez la politique de pile pour définir les actions explicitement autorisées. Si vous souhaitez inverser la politique, vous pouvez définir une `Allow` instruction qui autorise toutes les actions, puis spécifier des `Deny` instructions explicites qui empêchent les actions sur des ressources spécifiques uniquement. Pour référence, consultez cet exemple de politique de pile dans la CloudFormation documentation.

Pour plus d'informations sur l'utilisation de ces éléments pour créer des politiques de pile personnalisées et d'autres exemples de politiques, consultez les sections Définition d'une politique de pile et Autres exemples de politiques de pile dans la CloudFormation documentation.

Définition et remplacement des politiques de stack

Après avoir créé une politique de pile, vous l'associez à une pile. Si vous attribuez la politique de pile à une pile existante, vous devez utiliser le AWS Command Line Interface (AWS CLI). Toutefois, si vous attribuez la politique au moment de la création de la pile, vous pouvez utiliser la CloudFormation console ou le AWS CLI. Pour obtenir des instructions, consultez la section Définition d'une politique de stack dans la CloudFormation documentation.

Lorsque vous souhaitez autoriser les utilisateurs à mettre à jour ou à supprimer les ressources de la pile, vous devez temporairement annuler la politique de la pile. Cette dérogation vous permet d'effectuer des actions autrement refusées sur les ressources protégées de cette pile. Pour obtenir

des instructions, consultez la section Mise à jour des ressources protégées dans la CloudFormation documentation.

Politiques de limitation et d'exigence en matière de stack

Comme meilleure pratique pour les autorisations de moindre privilège, pensez à obliger les principaux IAM à attribuer des politiques de pile et à limiter les politiques de pile que les principaux IAM peuvent attribuer. De nombreux responsables IAM ne devraient pas être autorisés à créer et à attribuer des politiques de pile personnalisées à leurs propres piles.

Après avoir créé vos politiques de stack, nous vous recommandons de les télécharger dans un compartiment S3. Vous pouvez ensuite référencer ces politiques de pile en utilisant la clé de `cloudformation:StackPolicyUrl` condition et en fournissant l'URL de la politique de pile dans le compartiment S3.

Octroi d'autorisations pour joindre des politiques de pile

La meilleure pratique en matière d'autorisations de moindre privilège consiste à envisager de limiter les politiques de pile que les responsables IAM peuvent associer aux piles. CloudFormation Dans la stratégie basée sur l'identité pour le principal IAM, vous pouvez spécifier les politiques de pile que le principal IAM est autorisé à attribuer. Cela empêche le principal IAM d'associer une politique de stack, ce qui peut réduire le risque de mauvaise configuration.

Par exemple, une organisation peut avoir différentes équipes ayant des exigences différentes. En conséquence, chaque équipe élabore des politiques de cumul pour ses propres équipes CloudFormation . Dans un environnement partagé, si toutes les équipes stockent leurs politiques de pile dans le même compartiment S3, un membre de l'équipe peut associer une politique de pile disponible mais non destinée aux CloudFormation piles de son équipe. Pour éviter ce scénario, vous pouvez définir une déclaration de politique qui permet aux principaux IAM d'associer uniquement des politiques de pile spécifiques.

L'exemple de politique suivant permet au directeur IAM d'associer des politiques de pile stockées dans un dossier spécifique à l'équipe dans un compartiment S3. Vous pouvez stocker les politiques de stack approuvées dans ce compartiment.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
      "Effect": "Allow",
      "Action": [
        "cloudformation:SetStackPolicy"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "cloudformation:StackPolicyUrl": "<Bucket URL>/<Team folder>/*"
        }
      }
    }
  ]
}
```

Cette déclaration de politique n'oblige pas le principal IAM à attribuer une politique de pile à chaque pile. Même si le principal IAM est autorisé à créer des piles avec une politique de pile spécifique, il peut choisir de créer une pile qui n'a pas de politique de pile.

Exiger des politiques de stack

Pour garantir que tous les principaux IAM attribuent des politiques de pile à leurs piles, vous pouvez définir une politique de contrôle des services (SCP) ou une limite d'autorisations à titre de garde-fou préventif.

L'exemple de politique suivant montre comment configurer un SCP qui nécessite que les principaux IAM attribuent une politique de pile lors de la création d'une pile. Si le principal IAM n'attache pas de politique de pile, il ne peut pas créer la pile. En outre, cette politique empêche les principaux IAM disposant d'autorisations de mise à jour de pile de supprimer la politique de pile lors d'une mise à jour. La politique restreint l'`cloudformation:UpdateStack`action en utilisant la clé de condition. `cloudformation:StackPolicyUrl`

```
        {
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack"
      ],
```

```
      "Resource": "*",
      "Condition": {
        "Null": {
          "cloudformation:StackPolicyUrl": "true"
        }
      }
    }
  ]
}
```

En incluant cette déclaration de politique dans un SCP plutôt que dans une limite d'autorisations, vous pouvez appliquer votre garde-fou à tous les comptes de l'organisation. Cela peut avoir les effets suivants :

1. Réduisez les efforts nécessaires pour associer la politique individuellement à plusieurs principes IAM dans un. Compte AWS Les limites d'autorisations ne peuvent être directement attachées qu'à un principal IAM.
2. Réduisez les efforts liés à la création et à la gestion de plusieurs copies de la limite des autorisations pour différents Comptes AWS. Cela réduit le risque d'erreur de configuration dans plusieurs limites d'autorisations identiques.

> **Note**
>
> SCPs et les limites d'autorisations sont des barrières d'autorisations qui définissent le maximum d'autorisations disponibles pour les principaux IAM d'un compte ou d'une organisation. Ces politiques n'accordent pas d'autorisations aux principaux IAM. Si vous souhaitez standardiser l'obligation pour tous les principaux IAM de votre compte ou de votre organisation d'attribuer des politiques de stack, vous devez utiliser à la fois des barrières de protection des autorisations et des politiques basées sur l'identité.

Configuration des autorisations de moindre privilège pour les ressources fournies via CloudFormation

AWS CloudFormation vous permet de fournir de nombreux types de AWS ressources différents. Les ressources provisionnées nécessitent leur propre ensemble d'autorisations pour fonctionner comme prévu et pour configurer qui a accès à ces ressources. Le chapitre précédent a examiné les options de configuration des autorisations d'accès et d'utilisation du CloudFormation service. Ce chapitre explique comment appliquer le principe du moindre privilège aux ressources mises en service via CloudFormation.

Dans ce guide, il serait pratiquement impossible de passer en revue les recommandations de sécurité et les meilleures pratiques pour chaque type de AWS ressource pouvant être provisionnée. CloudFormation Si vous avez des questions concernant un service spécifique, nous vous recommandons de consulter la documentation relative à ce service. La plupart des Service AWS documents contiennent une section sur la sécurité et des informations sur les autorisations requises pour utiliser ce service. Pour une liste complète de la Service AWS documentation, consultez AWS la section Documentation.

Voici des étapes de haut niveau, indépendantes des services, que vous pouvez suivre pour créer des CloudFormation modèles conformes au principe du moindre privilège :

1. Préparez une liste des ressources que vous prévoyez de fournir en utilisant CloudFormation.
2. Consultez la AWS documentation des services correspondants et consultez les sections relatives à la sécurité et à la gestion des accès. Cela vous permet de comprendre les exigences et les recommandations spécifiques au service.
3. Utilisez les informations que vous avez recueillies au cours des étapes précédentes pour concevoir des CloudFormation modèles et des politiques associées qui n'autorisent que les autorisations requises et refusent toutes les autres.

Ce guide passe ensuite en revue un exemple de la manière dont vous pouvez appliquer le principe du moindre privilège dans les CloudFormation modèles, en utilisant un cas d'utilisation réel.

Exemple : compartiment Amazon S3 pour stocker les artefacts du pipeline

Cet exemple crée un bucket Amazon Simple Storage Service (Amazon S3) qui est utilisé pour AWS CodeBuildstocker les artefacts du projet. AWS CodePipelineutilise ces artefacts stockés. Vous pouvez autoriser CodeBuild et accéder CodePipeline à ce compartiment S3 via des rôles de service, et vous contrôlez cet accès en utilisant une politique de compartiment Amazon S3. Les noms de ressources utilisés dans cet exemple sont les suivants :

- `Deployfiles_build`est le nom du CodeBuild projet.
- `Deployment-Pipeline`est le nom du pipeline dans CodePipeline.

Définition du compartiment Amazon S3

Vous devez d'abord définir le compartiment S3 dans le CloudFormation modèle, qui est un fichier texte au format YAML.

```
amzn-s3-demo-bucket:
  Type: AWS::S3::Bucket
  Properties:
    PublicAccessBlockConfiguration:
        BlockPublicAcls: true
        BlockPublicPolicy: true
        IgnorePublicAcls: true
        RestrictPublicBuckets: true
```

Définition de la politique relative aux compartiments Amazon S3

Ensuite, dans le CloudFormation modèle, vous créez une politique de compartiment qui autorise uniquement le `Deployfiles_build` projet et le `Deployment-Pipeline` pipeline à accéder au compartiment.

```
MyBucketPolicy:
  Type: AWS::S3::BucketPolicy
  Properties:
    Bucket: !Ref amzn-s3-demo-bucket
    PolicyDocument:
      Version: "2012-10-17"
```

```
      Statement:
      - Sid: "S3ArtifactRepoAccess"
        Effect: Allow
        Action:
          - 's3:GetObject'
          - 's3:GetObjectVersion'
          - 's3:PutObject'
          - 's3:GetBucketVersioning'
        Resource:
          - !Sub 'arn:aws:s3:::${amzn-s3-demo-bucket}'
          - !Sub 'arn:aws:s3:::${amzn-s3-demo-bucket}/*'
        Principal:
          Service:
            - codebuild.amazonaws.com
            - codepipeline.amazonaws.com
        Condition:
          StringLike:
            'aws:SourceArn':
              - !Sub 'arn:aws:codebuild:${AWS::Region}:${AWS::AccountId}:project/
Deployfiles_build'
              - !Sub 'arn:aws:codepipeline:${AWS::Region}:${AWS::AccountId}:Deployment-
Pipeline'
              - !Sub 'arn:aws:codepipeline:${AWS::Region}:${AWS::AccountId}:Deployment-
Pipeline/*'
```

Notez ce qui suit à propos de cette politique de compartiment :

- L'`Resource`élément répertorie deux types de ressources différents qui utilisent les formats Amazon Resource Name (ARN) suivants :
  - Le format ARN d'un objet S3 est`arn:$`*`<Partition>`*`:s3:::$`*`<BucketName>`*`/$`*`<ObjectName>`*.
  - Le format ARN d'un compartiment S3 est`arn:$`*`<Partition>`*`:s3:::$`*`<BucketName>`*.

  `s3:GetObject`s`s3:GetObjectVersion`, et `s3:PutObject` nécessitent un type de ressource d'objet S3, ainsi `s3:GetBucketVersioning` qu'un type de ressource de compartiment S3. Pour plus d'informations sur les types de ressources requis pour chaque action, consultez Actions, ressources et clés de condition pour Amazon S3.
- L'`Principal`élément répertorie les entités autorisées à effectuer les actions Amazon S3 définies dans la déclaration. Dans ce cas, seuls CodeBuild et CodePipeline sont autorisés à effectuer ces actions.

- L'`Condition`élément restreint davantage l'accès au compartiment S3 afin que seuls le `Deployfiles_build` CodeBuild projet, le `Deployment-Pipeline` CodePipeline pipeline et les actions du pipeline puissent accéder au compartiment.

Création des rôles de service

Bien que la politique du compartiment contrôle l'accès au compartiment, elle n'accorde aucune autorisation CodePipeline pour CodeBuild y accéder. Pour accorder l'accès, vous devez créer un rôle de service pour chaque service et ajouter l'instruction suivante à chacun d'eux. Les rôles des services pour CodeBuild et CodePipeline permettent aux services d'accéder au compartiment S3 et à ses objets.

```
Sid: "ViewAccessToS3ArtifactRepo"
Effect: Allow
Action:
  - ‘s3:GetObject'
  - ‘s3:GetObjectVersion'
  - ‘s3:PutObject'
  - ‘s3:GetBucketVersioning'
Resource:
  - !Sub ‘arn:aws:s3:::${BuildArtifactsBucket}'
  - !Sub ‘arn:aws:s3:::${BuildArtifactsBucket}/*'
```

Bonnes pratiques en matière d'autorisations de moindre privilège pour AWS CloudFormation

Ce guide passe en revue les différentes approches et certains types de politiques que vous pouvez utiliser pour configurer l'accès au moindre privilège aux ressources mises en service par le biais AWS CloudFormation de ce dernier. CloudFormation Ce guide se concentre sur la configuration de l'accès CloudFormation via les principes IAM, les rôles de service et les politiques de stack. Les recommandations et les meilleures pratiques incluses sont conçues pour protéger vos comptes et vos ressources contre les actions involontaires des utilisateurs autorisés et contre les acteurs malveillants susceptibles d'exploiter des autorisations excessives.

Ce qui suit est un résumé des meilleures pratiques expliquées dans ce guide. Ces bonnes pratiques peuvent vous aider à respecter le principe du moindre privilège lors de la configuration des autorisations d'utilisation CloudFormation et des ressources fournies par le biais CloudFormation de :

- Déterminez le niveau d'accès dont les utilisateurs et les équipes ont besoin pour utiliser le CloudFormation service, et accordez uniquement l'accès minimum requis. Par exemple, accordez un accès de consultation aux stagiaires et aux auditeurs, et n'autorisez pas ces types d'utilisateurs à créer, mettre à jour ou supprimer des piles.
- Pour les responsables IAM qui doivent fournir plusieurs types de AWS ressources par le biais de CloudFormation piles, envisagez d'utiliser des rôles de service pour permettre CloudFormation de fournir des ressources au nom du principal, au lieu de configurer l'accès à celles définies Services AWS dans les politiques basées sur l'identité du principal.
- Dans les politiques basées sur l'identité pour les principaux IAM, utilisez la clé de `cloudformation:RoleARN` condition pour contrôler les rôles de CloudFormation service pouvant être transmis.
- Pour empêcher l'augmentation des privilèges, procédez comme suit :
  - Surveillez strictement tous les principaux IAM qui ont accès au CloudFormation service et les niveaux d'accès dont ils disposent.
  - Surveillez strictement quels utilisateurs peuvent accéder à ces principes IAM.
  - Surveillez l'activité des responsables IAM auxquels un rôle de service privilégié peut être transféré. CloudFormation Bien qu'ils ne soient pas autorisés à créer des ressources IAM par le biais de leur politique basée sur l'identité, le rôle de service qu'ils peuvent transmettre peut créer des ressources IAM.

- Spécifiez une politique de pile chaque fois que vous créez une pile qui contient des ressources critiques. Cela peut aider à protéger les ressources critiques contre les mises à jour involontaires susceptibles d'entraîner l'interruption ou le remplacement de ces ressources.
- Pour les ressources mises à disposition via CloudFormation ce service, reportez-vous aux recommandations de gestion des accès et aux meilleures pratiques de sécurité relatives à ce service.
- Pour compléter les recommandations de ce guide concernant les politiques basées sur l'identité et les politiques basées sur les ressources, envisagez de mettre en œuvre des contrôles de sécurité supplémentaires pour les autorisations relatives au moindre privilège, tels que des politiques de contrôle des services () et des limites d'autorisations. SCPs Pour de plus amples informations, veuillez consulter Étapes suivantes.

La CloudFormation documentation contient des bonnes pratiques supplémentaires et des meilleures pratiques de sécurité qui peuvent vous aider à les utiliser de manière CloudFormation plus efficace et plus sûre. Consultez également Meilleures pratiques pour configurer des politiques basées sur l'identité pour un accès avec le moindre privilège CloudFormation ce guide.

Étapes suivantes

Vous pouvez utiliser les informations et les exemples contenus dans ce guide pour commencer à appliquer le principe du moindre privilège dans votre organisation. Nous vous recommandons de consulter les ressources supplémentaires de la Ressources section, qui contient des références documentaires et des outils qui peuvent vous aider à affiner vos politiques.

Ce guide est destiné à vous aider à commencer à mettre en œuvre l'accès au moindre privilège pour. AWS CloudFormation Cependant, il existe d'autres types de politiques qui peuvent vous aider à renforcer le principe du moindre privilège au sein de votre organisation. En fonction de votre environnement et des exigences de votre entreprise, vous souhaiterez peut-être mettre en œuvre des contrôles supplémentaires qui ne sont pas abordés dans ce guide. À l'étape suivante et pour plus d'informations, nous vous recommandons de consulter les rubriques suivantes relatives au moindre privilège et à la configuration de l'accès et des autorisations :

- Limites d'autorisations pour les entités IAM
- Politiques de contrôle des services (SCP)
- Rôles pour l'accès entre comptes
- Fédération d'identité
- Afficher les dernières informations consultées pour IAM

Les outils suivants peuvent vous aider à contrôler l'accès et les autorisations selon le principe du moindre privilège pour : CloudFormation

- AWS Identity and Access Management Access Analyzer
- Vous pouvez utiliser l'onglet Access Advisor de la console AWS Identity and Access Management (IAM) pour identifier les autorisations excessives pour les identités IAM. Par exemple, consultez Renforcer les autorisations S3 pour vos utilisateurs et rôles IAM à l'aide de l'historique des accès aux actions S3 (article de AWS blog).
- Vous pouvez utiliser un outil de linting, tel que cfn-policy-validator(GitHub), pour identifier les autorisations excessives.

Lorsque vous êtes à l'aise avec la création et la gestion CloudFormation des autorisations, il est recommandé d'utiliser des pipelines d'intégration continue et de livraison continue (CI/CD) pour

déployer vos CloudFormation modèles. Cela réduit le risque d'erreurs humaines et accélère votre processus de déploiement.

Ressources

AWS CloudFormation documentation

- Contrôler l'accès avec AWS Identity and Access Management
- AWS référence aux types de ressources et de propriétés
- Configuration des options de AWS CloudFormation pile
- AWS CloudFormation rôle de service

AWS Identity and Access Management documentation (IAM)

- Stratégies et autorisations dans IAM
- Références des éléments de stratégie JSON IAM
- Logique d’évaluation de stratégies
- Services AWS qui fonctionnent avec IAM
- Création d'un rôle pour déléguer des autorisations à un Service AWS
- Le problème de l'adjoint confus
- Bonnes pratiques de sécurité dans IAM

Autres AWS références

- Actions, ressources et clés de condition pour Services AWS (référence d'autorisation de service)
- Accorder l'accès avec le moindre privilège (AWS Well-Architected Framework)
- Techniques de rédaction des politiques IAM du moindre privilège (article de AWS blog)

Historique du document

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

Modification	Description	Date
Mises à jour importantes	Nous avons révisé et affiné de manière significative les directives et les exemples de déclarations de politique afin de répondre aux cas d'utilisation organisationnels courants.	5 mai 2023
Publication initiale	—	9 mars 2023

AWS Glossaire des directives prescriptives

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

Nombres

7 R

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

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

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

A

ABAC

Voir contrôle d'accès basé sur les attributs.

services abstraits

Consultez la section Services gérés.

ACIDE

Voir atomicité, consistance, isolation, durabilité.

migration active-active

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

migration active-passive

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

fonction d'agrégation

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

AI

Voir intelligence artificielle.

AIOps

Voir les opérations d'intelligence artificielle.

anonymisation

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

anti-motif

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

contrôle des applications

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

portefeuille d'applications

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

intelligence artificielle (IA)

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

opérations d'intelligence artificielle (AIOps)

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

chiffrement asymétrique

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

atomicité, cohérence, isolement, durabilité (ACID)

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

contrôle d'accès par attributs (ABAC)

Pratique qui consiste à créer des autorisations détaillées en fonction des attributs de l'utilisateur, tels que le service, le poste et le nom de l'équipe. Pour plus d'informations, consultez ABAC pour AWS dans la documentation 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 est communément décrit comme un pipeline. CI/CD peut vous aider à automatiser les processus, à améliorer la productivité, à améliorer la qualité du code et à accélérer les livraisons. Pour plus d'informations, veuillez consulter Avantages de la livraison continue. CD peut également signifier déploiement continu. Pour plus d'informations, veuillez consulter Livraison continue et déploiement continu.

CV

Voir vision par ordinateur.

D

données au repos

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

classification des données

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

dérive des données

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

données en transit

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

maillage de données

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

minimisation des données

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

périmètre de données

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

prétraitement des données

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

provenance des données

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

sujet des données

Personne dont les données sont collectées et traitées.

entrepôt des données

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

langage de définition de base de données (DDL)

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

langage de manipulation de base de données (DML)

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

DDL

Voir langage de définition de base de données.

ensemble profond

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

deep learning

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

defense-in-depth

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

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

administrateur délégué

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

deployment

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

Consultez la section 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 CI/CD pipeline, l'environnement de production est le dernier environnement de déploiement.
- Environnements supérieurs : tous les environnements accessibles aux utilisateurs autres que l'équipe de développement principale. Ils peuvent inclure un environnement de production, des

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

époppée

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

ERP

Voir Planification des ressources d'entreprise.

analyse exploratoire des données (EDA)

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

F

tableau des faits

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

échouer rapidement

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

limite d'isolation des défauts

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

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

branche de fonctionnalités

Voir succursale.

fonctionnalités

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

importance des fonctionnalités

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

transformation de fonctionnalité

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

invitation en quelques coups

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

FGAC

Découvrez le contrôle d'accès détaillé.

contrôle d'accès détaillé (FGAC)

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

migration instantanée (flash-cut)

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

FM

Voir le modèle de fondation.

modèle de fondation (FM)

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

G

IA générative

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

blocage géographique

Voir les restrictions géographiques.

restrictions géographiques (blocage géographique)

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

Flux de travail Gitflow

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

image dorée

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

stratégie inédite

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

barrière de protection

Règle de haut niveau qui permet de régir les ressources, les politiques et la conformité au sein des unités organisationnelles (OUs). Les barrières de protection préventives appliquent des politiques pour garantir l'alignement sur les normes de conformité. Elles sont mises en œuvre à l'aide de politiques de contrôle des services et de limites des autorisations IAM. Les barrières de protection de détection détectent les violations des politiques et les problèmes de conformité, et génèrent des alertes pour y remédier. Ils sont implémentés à l'aide d'Amazon AWS Config AWS Security Hub 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 les opérations, les analystes commerciaux et les propriétaires, les ingénieurs de migration, les développeurs et les DevOps 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.

Region (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 de type « 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.