Création d'une fabrique de plans d'entreprise en utilisant AWS Service Catalog

AWS Conseils prescriptifs

AWS Conseils prescriptifs: Création d'une fabrique de plans d'entreprise en utilisant AWS Service Catalog

Table of Contents

Création d'une fabrique de plans d'entreprise en utilisant AWS Service Catalog

Amazon Web Services (contributeurs)

octobre 2024 (historique du document)

Présentation d'entreprise

De nombreuses entreprises sont confrontées à des défis lorsqu'elles font évoluer leurs charges de travail dans le cloud. Ces défis organisationnels sont notamment les suivants :

- Création de modèles d'infrastructure sous forme de code (IaC) réutilisables à grande échelle pour plusieurs Services AWS
- Vérifier que les modèles IaC respectent les meilleures pratiques en matière de sécurité
- Réduction des tâches indifférenciées ou répétitives susceptibles de réduire considérablement la productivité des développeurs et de prolonger les délais de commercialisation
- Établissement de la cohérence pour les modèles IaC
- Réduire l'utilisation des ressources, en particulier pour l'équipe de sécurité, afin d'éviter des révisions manuelles répétitives

La création d'un modèle IaC conforme aux meilleures pratiques de sécurité nécessite la mise en place de garde-fous et de contrôles de sécurité. Traditionnellement, l'équipe chargée de la plateforme cloud ou de la sécurité examinait manuellement le code de chaque modèle IaC. Les développeurs pourraient également déployer le modèle IaC dans un environnement hors production et s'appuyer sur des contrôles de détection pour détecter tout problème de sécurité. Ces deux approches nécessitent des cycles de feedback itératifs, ralentissent le processus de développement et augmentent les efforts d'ingénierie manuelle.

Par conséquent, de nombreuses entreprises souhaitent rationaliser la création, la validation et la publication de modèles IaC. Ils veulent également disposer d'un moyen de gérer et de gouverner ces modèles après leur publication. Des mécanismes de gestion et de gouvernance appropriés vous aident à mettre à jour les modèles et à garantir que les développeurs ont accès aux dernières versions. Ces mécanismes vous aident également à superviser et à auditer l'utilisation des modèles au sein de l'organisation.

Présentation de la solution

Ce guide explique la solution Enterprise Blueprint Factory, qui vous aide à rationaliser la création, la validation, la publication, la distribution et l'utilisation de modèles d'infrastructure sous forme de code (iAc) au sein de votre organisation. Ces modèles IaC sont également appelés plans. Cette solution prend en charge les fichiers de plan qui sont des AWS CloudFormation modèles ou des AWS Cloud Development Kit (AWS CDK) constructions.

L'Enterprise Blueprint Factory utilise une approche basée sur la configuration pour automatiser le partage, la publication et la distribution des plans. Un développeur ajoute un plan à un référentiel de produits, puis ajoute les informations du plan à un fichier de configuration. Cela lance automatiquement un pipeline de publication d'intégration continue et de livraison continue (CI/CD). Ce pipeline confirme que le plan respecte les meilleures pratiques en AWS matière de sécurité. Cela permet de s'assurer que les plans de votre organisation sont sécurisés dès leur conception. La sécurité dès la conception est une approche d'ingénierie système qui prend en compte la sécurité tout au long du processus de développement.

L'Enterprise Blueprint Factory publie des plans sous forme de produits dans. AWS Service Catalog En utilisant Service Catalog, les utilisateurs finaux peuvent rapidement déployer les plans approuvés que vous fournissez. Service Catalog est également conçu pour fournir des fonctionnalités de gestion et de gouvernance afin que les administrateurs puissent définir des contrôles d'accès précis et superviser l'utilisation des plans.

Public visé

La section Architecture d'Enterprise Blueprint Factory aide les architectes, les responsables et les responsables techniques à évaluer cette solution et à déterminer si elle convient à leur organisation. Cette section décrit ce que sont les plans, comment vous pouvez utiliser Service Catalog pour les gérer, ainsi que l'architecture de l'Enterprise Blueprint Factory.

La section Configuration de l'Enterprise Blueprint Factory aide les DevOps ingénieurs à déployer l'Enterprise Blueprint Factory dans votre AWS environnement. Il inclut des instructions détaillées pour configurer les référentiels requis et le pipeline de configuration.

La section Utilisation de l'Enterprise Blueprint Factory aide les développeurs de plans à créer, mettre à jour ou supprimer des plans dans votre environnement. Il fournit des instructions détaillées pour gérer un plan tout au long de son cycle de vie. Pour créer des plans, les développeurs doivent

comprendre comment créer des modèles IaC, tels que des CloudFormation modèles. Ce guide ne contient pas d'informations ni d'instructions sur la façon de définir ces plans.

Objectifs

L'Enterprise Blueprint Factory aide votre organisation à bénéficier des avantages suivants :

- Vérifiez que les plans respectent les meilleures pratiques en AWS matière de sécurité
- Automatisez et standardisez le processus de publication et de validation des plans
- Améliorez la productivité des développeurs en réduisant le nombre de tâches manuelles qu'ils doivent effectuer
- Utilisez des contrôles d'accès précis pour déterminer les plans auxquels les utilisateurs finaux peuvent accéder
- Utilisez le contrôle de version pour gérer les mises à jour des plans et les partager avec les utilisateurs finaux
- Aider les utilisateurs finaux à découvrir et à lancer des plans en libre-service
- Superviser et auditer l'utilisation des plans dans l'ensemble de l'organisation

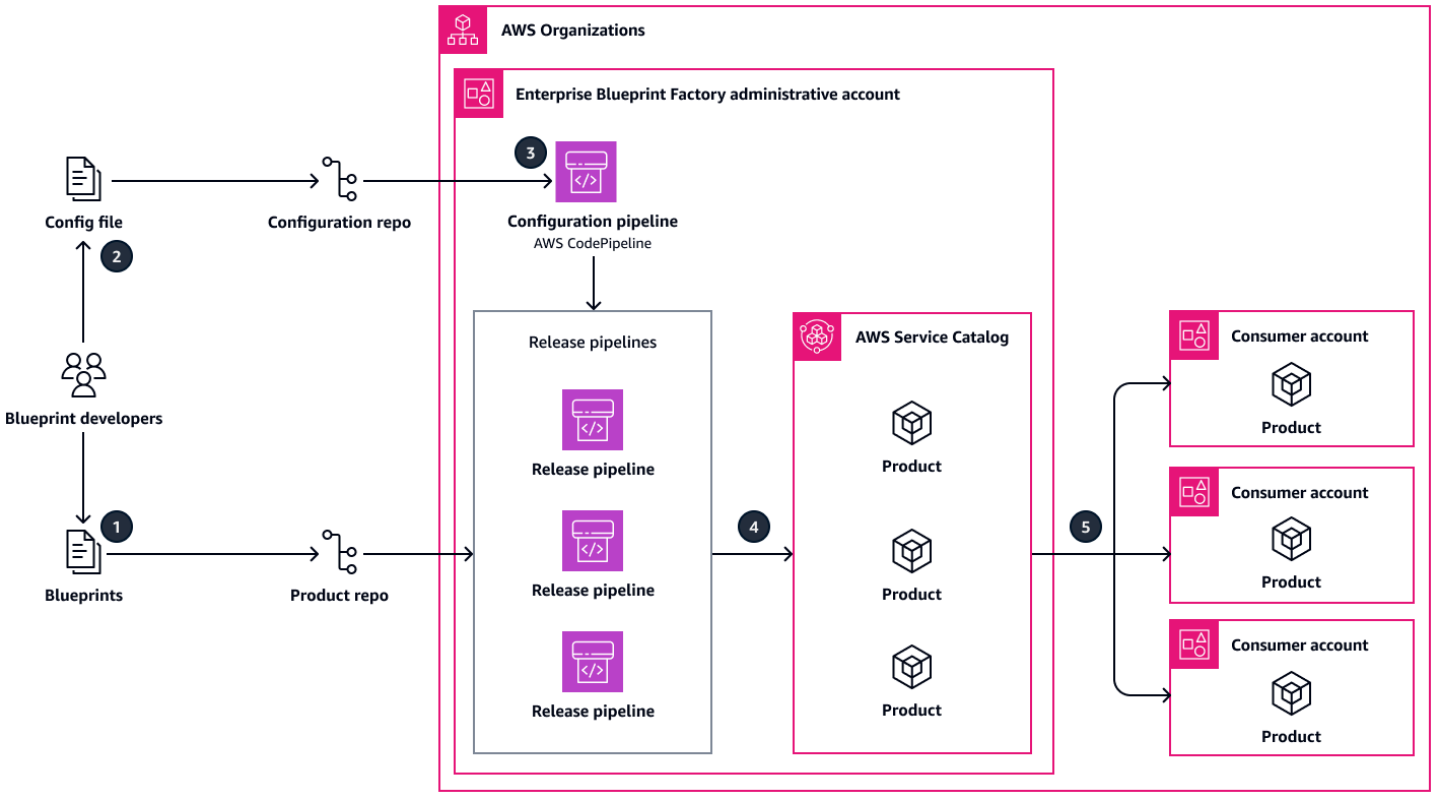
Architecture Enterprise Blueprint Factory

Un modèle d'infrastructure sous forme de code (IaC), également appelé plan, est un fichier de configuration qui vous aide à provisionner et à gérer les ressources du cloud. Un plan peut fournir une ressource unique ou l'architecture d'une application complexe à plusieurs niveaux. L'iAC est conçu pour vous aider à centraliser la gestion de l'infrastructure, à standardiser les ressources et à évoluer rapidement.

L'Enterprise Blueprint Factory vous aide à rationaliser la création, la validation, la publication, la distribution et la consommation de plans au sein de votre organisation. En plus de fournir un aperçu de l'architecture, cette section passe en revue les composants architecturaux de la solution et le cycle de vie du plan.

Lorsque vous publiez un plan par le biais de l'Enterprise Blueprint Factory, le plan devient un produit dans. AWS Service Catalog Vous collectez les produits dans un ou plusieurs portefeuilles, puis vous accordez des autorisations permettant aux utilisateurs finaux d'accéder aux produits de ce portefeuille. Vous pouvez utiliser un partage de portefeuille pour permettre à un administrateur de Service Catalog ou Compte AWS à un autre de distribuer vos produits aux utilisateurs finaux.

Le schéma suivant présente une présentation générale de l'architecture Enterprise Blueprint Factory. Ce flux de travail publie le plan en tant que produit dans Service Catalog. Il crée ou met également à jour les portefeuilles et les actions du portefeuille afin de mettre le plan à la disposition des utilisateurs finaux cibles.



Ce diagramme montre le flux de travail suivant :

1. Un développeur construit le plan. Ils créent une branche de fonctionnalités dans le référentiel de produits, transmettent le plan à la branche, puis créent une pull request. Une équipe administrative et une équipe de sécurité examinent la pull request pour s'assurer que le plan répond aux exigences organisationnelles et de sécurité. Ces équipes approuvent la pull request. Le développeur fusionne la branche des fonctionnalités dans la branche principale. Pour plus d'informations, consultez la section Référentiel de produits dans ce guide.
2. Le développeur ajoute ou met à jour les informations du plan dans le fichier de configuration situé dans le dépôt de configuration. Pour plus d'informations, consultez Référentiel de configuration et fichier de configuration dans ce guide.
3. La mise à jour du fichier de configuration appelle le pipeline de configuration. Ce pipeline utilise AWS CodePipelineet AWS CodeBuildprojette de créer ou de mettre à jour les portefeuilles et les parts de portefeuille du Service Catalog. Cela crée également un pipeline de publication pour le plan. Pour plus d'informations, consultez la section Pipeline de configuration dans ce guide.
4. Le pipeline de publication effectue divers contrôles de sécurité sur le plan. Si le plan est adopté, le pipeline de publication le déploie en tant que produit dans Service Catalog. Pour plus d'informations, consultez la section Liaison du pipeline dans ce guide.

5. En accédant au produit par le biais de portefeuilles et d'actions de portefeuille, les utilisateurs finaux déploient le plan dans leurs comptes de consommateurs cibles.

Composants d'Enterprise Blueprint Factory

L'Enterprise Blueprint Factory comprend les composants suivants :

- Référentiel de produits : référentiel dans lequel vous stockez les plans.
- Référentiel de configuration : référentiel dans lequel vous stockez le fichier de configuration qui définit vos AWS Service Catalog portefeuilles et vos produits.
- Fichier de configuration : fichier de configuration qui définit les plans disponibles, les personnes autorisées à les utiliser et la manière dont ils peuvent les utiliser.
- Pipeline de configuration : pipeline DevOps CI/CD qui définit le portefeuille Service Catalog et les parts de portefeuille et crée un pipeline de lancement pour chaque produit.
- Pipeline de publication : pipeline DevOps CI/CD qui publie des plans sous forme de produits Service Catalog.

L'équipe de l'infrastructure cloud gère généralement l'ensemble de l'usine de plans d'entreprise, car elle doit approuver chaque plan. Cependant, l'équipe chargée DevOps du code est généralement responsable du pipeline de configuration et du pipeline de publication. Pour publier de nouveaux plans, les développeurs interagissent uniquement avec le référentiel du produit, le référentiel de configuration et le fichier de configuration.

Référentiel de produits

Le référentiel de produits est un emplacement centralisé dans lequel vous stockez les plans approuvés par votre organisation. Une équipe administrative et une équipe de sécurité examinent les pull requests adressées à ce référentiel pour s'assurer que chaque plan répond aux exigences organisationnelles et de sécurité. Dans ce guide, nous utilisons GitHub pour le référentiel, mais vous pouvez utiliser une alternative.

Référentiel de configuration

Le référentiel de configuration (dépôt de configuration) est l'emplacement où votre organisation stocke le fichier de configuration pour vos portefeuilles et produits Service Catalog publiés via

Enterprise Blueprint Factory. Dans ce guide, nous utilisons GitHub pour le référentiel, mais vous pouvez utiliser une alternative.

Fichier de configuration

Le fichier de configuration Enterprise Blueprint Factory (fichier de configuration) est stocké dans le référentiel de configuration, qui appartient à l'équipe administrative du Blueprint. Le nom de ce fichier est bp_config.yml. Lorsqu'un développeur met à jour ce fichier, l'équipe administrative du plan examine les modifications. La fusion des modifications dans la branche principale lance le pipeline de configuration. Le fichier de configuration orchestre la publication, le partage et la distribution de tous les plans gérés via Enterprise Blueprint Factory.

Le fichier de configuration est un fichier YAML composé de deux objets principaux : `portfolios` et`products`. Voici un exemple de fichier de configuration :

```
portfolios:
  - portfolio_name: blueprint-portfolio
    owner: Blueprint-team
    provider_name: AWS
    description: "Blueprint portfolio"
    portfolio_access_role:
       - arn:aws:iam::123456789012:role/examplerole
       - arn:aws:iam::123456789012:user/exampleuser
    share_to_ou:
     - org_id: "o-exampleOrgID"
    stack_tags:
      DataClassification: Confidential
      Organization: AWS
products:
  - name: BP-S3-Product
    description: "Blueprint for BP-S3 product"
    product_config_file: 'BP-S3/product_config.json'
    owner: Blueprint-team
    stack_tags:
      DataClassification: Confidential
      Organization: AWS
    portfolio_associations:
      - blueprint-portfolio
    launch_constraint_role: arn:aws:iam::123456789012:role/examplelaunchrole
```

Dans l'`portfolios`objet, vous définissez vos portefeuilles Service Catalog cibles. Pour chaque portefeuille, vous fournissez les attributs suivants :

- `portfolio_name`est le nom du portefeuille. Cet attribut est obligatoire.
- `owner`est le nom de l'équipe propriétaire du portefeuille. Cet attribut est facultatif.
- `provider_name`est le nom de l'équipe ou de l'organisation qui gère le portefeuille. La valeur par défaut est `AWS`. Cet attribut est obligatoire.
- `description`est une brève description du portefeuille. Cet attribut est facultatif.
- `portfolio_access_roles`sont les identités AWS Identity and Access Management (IAM) (utilisateurs, rôles ou groupes) autorisées à accéder au portefeuille et aux produits associés. Cet attribut est facultatif.
- `share_to_ou`est l'unité organisationnelle (UO) avec AWS Organizations laquelle le portefeuille est partagé. Les utilisateurs finaux peuvent déployer les produits de ce portefeuille dans ceux Comptes AWS qui sont membres de l'unité d'organisation cible. Cet attribut est facultatif.
- `stack_tags`sont les tags appliqués au portefeuille. Cet attribut est facultatif.

Dans l'`products`objet, vous définissez chaque plan que vous souhaitez publier en tant que produit dans Service Catalog. Pour chaque produit, vous fournissez les attributs suivants :

- `name`est le nom du produit dans Service Catalog. Cet attribut est obligatoire.
- `description`est une brève description du produit. Cet attribut est obligatoire.
- `product_config_file`est le nom du fichier de configuration du produit Blueprint stocké dans le référentiel de produits. Cet attribut est obligatoire.
- `owner`est le nom de l'équipe propriétaire du produit. Cet attribut est obligatoire.
- `stack_tags`sont les étiquettes apposées sur le produit. Cet attribut est facultatif.
- `portfolio_associations`sont les portefeuilles cibles qui contiennent le produit. Cet attribut est facultatif.

> **Note**
>
> Nous vous recommandons d'ajouter des produits uniquement aux portefeuilles gérés par le biais de l'Enterprise Blueprint Factory. Si vous souhaitez ajouter des produits à des portefeuilles qui ne sont pas gérés via Enterprise Blueprint Factory, la politique IAM de l'utilisateur doit autoriser cette action. AssociateProductWithPortfolio Toutefois, pour des

raisons de sécurité, nous vous recommandons d'autoriser cette action uniquement pour le pipeline de configuration d'Enterprise Blueprint Factory.

- `launch_constraint_role`est le rôle de lancement assumé par Service Catalog lorsqu'un utilisateur final lance le produit. Cet attribut est obligatoire.

Pipeline de configuration

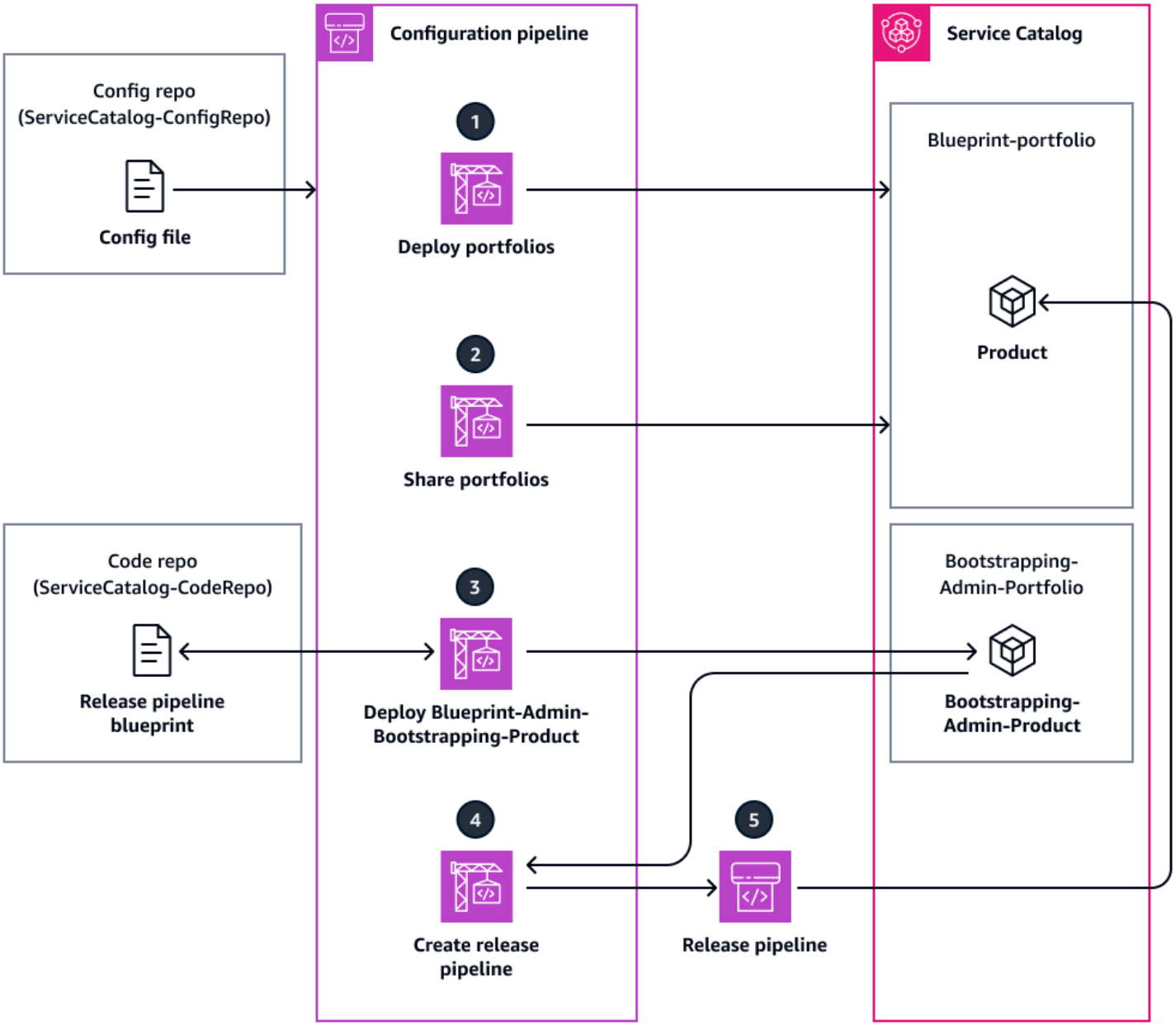
Le pipeline de configuration (pipeline de configuration) automatise la configuration du portefeuille Service Catalog et des parts de portefeuille. Il crée également le pipeline de lancement pour chaque produit. Ce pipeline est une AWS CodePipelineressource. Une mise à jour du fichier de configuration appelle le pipeline de configuration.

La première fois que vous appelez le pipeline de configuration, il crée deux portefeuilles supplémentaires qui ne sont pas définis dans votre fichier de configuration :

- `Blueprint-portfolio`— Chaque produit que vous déployez via l'Enterprise Blueprint Factory est ajouté à ce portefeuille. Ce portefeuille est accessible aux principaux IAM et aux unités organisationnelles que vous spécifiez dans le fichier de configuration.
- `Bootstrapping-Admin-Portfolio`— Le `Bootstrapping-Admin-Product` produit est associé à ce portefeuille. Ce produit est un CloudFormation modèle pour le pipeline de publication. Autorisez uniquement l'équipe administrative du Blueprint à accéder à ce portefeuille afin qu'elle puisse gérer les produits administratifs.

Étapes du pipeline de configuration

L'image suivante montre les étapes du pipeline de configuration et les ressources avec lesquelles le pipeline interagit. Chaque étape du pipeline est un AWS CodeBuildprojet.



Les étapes du pipeline de configuration sont les suivantes :

1. Déployer des portefeuilles : le pipeline de configuration déploie tous les portefeuilles ajoutés au fichier de configuration ou supprime tous les portefeuilles supprimés du fichier de configuration. Si aucune modification n'est apportée aux portefeuilles, le pipeline ignore cette étape.
2. Portefeuilles de partage : le pipeline de configuration partage les portefeuilles avec les unités organisationnelles cibles (OUs). Si aucune modification n'est apportée aux actions du portefeuille, le pipeline ignore cette étape.

3. Déployer Blueprint-Admin-Bootstrapping-Product — Le pipeline de configuration récupère le `bp-pipeline` plan depuis le `ServiceCatalog-CodeRepo` dépôt et le déploie dans Service Catalog en tant que. `Bootstrapping-Admin-Product` Ce produit est le CloudFormation modèle utilisé pour créer un pipeline de publication. Le déploiement de ce modèle en tant que produit Service Catalog permet de maintenir le contrôle des versions. Si aucune modification n'est apportée au `bp-pipeline` plan, le pipeline ignore cette étape.
4. Créer des pipelines de publication : en fonction des attributs du produit contenus dans le fichier de configuration, le pipeline de configuration prépare les paramètres de la pile et lance une CloudFormation pile qui crée un pipeline de publication pour le produit. Pour plus d'informations, consultez la section Liaison du pipeline dans ce guide.
5. Déployer des produits : le pipeline de publication déploie le plan en tant que produit Service Catalog et l'associe au portefeuille cible. Les utilisateurs finaux peuvent désormais déployer le produit dans ceux Comptes AWS qui sont membres de l'unité d'organisation cible.

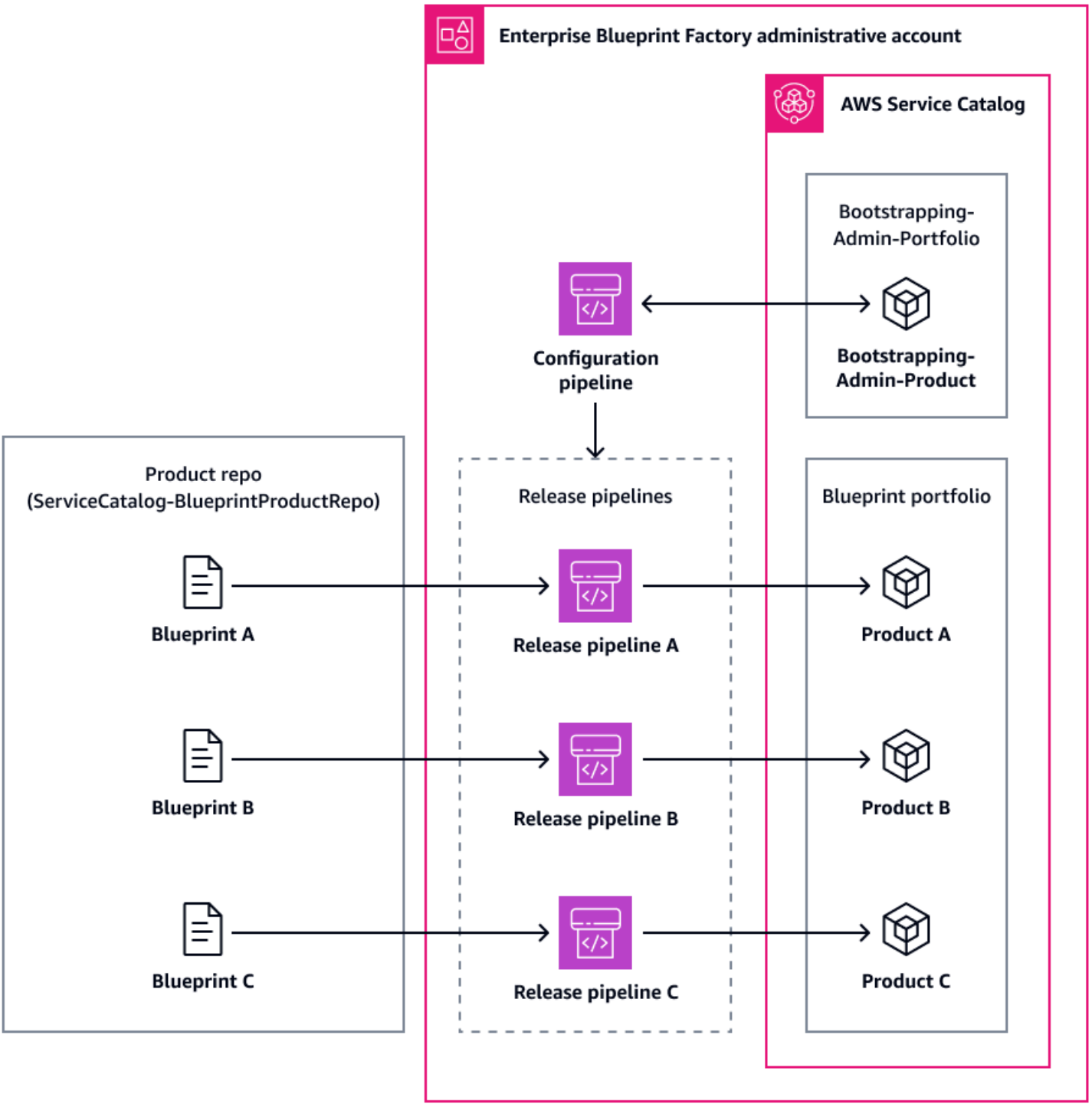
Pipeline de lancement

Le pipeline de publication automatise la publication des plans sous forme de produits Service Catalog. Ce pipeline est une AWS CodePipelineressource. Lorsque votre organisation souhaite publier un nouveau plan, un développeur télécharge le modèle iAC et son fichier de configuration du produit dans le référentiel du produit. L'ajout des détails du produit au fichier de configuration déclenche le pipeline de configuration. Le pipeline de configuration crée un pipeline de publication pour ce plan. Toute mise à jour ultérieure du plan déclenche ce pipeline de publication pour mettre à jour le produit dans Service Catalog avec une nouvelle version.

Le pipeline de publication inclut des contrôles proactifs qui automatisent les contrôles de sécurité et de conformité de vos plans. Les contrôles proactifs sont conçus pour empêcher la création de ressources non conformes. Ces contrôles peuvent réduire le nombre d'événements de sécurité gérés par d'autres types de contrôles de sécurité, tels que les contrôles réactifs et les contrôles de détection. Dans la mesure où les contrôles proactifs garantissent la conformité des ressources déployées avant leur déploiement, aucun événement de détection ne nécessite une réponse ou une correction.

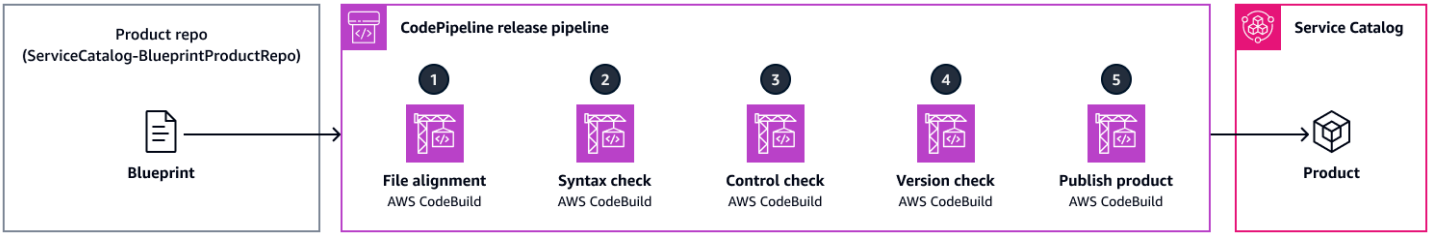
La première fois que vous appelez le pipeline de configuration, celui-ci crée un produit Service Catalog nomméBootstrapping-Admin-Product. Ce produit est le CloudFormation modèle du pipeline de publication. Comme le montre la figure suivante, le pipeline de configuration utilise le

`Bootstrapping-Admin-Product` produit pour créer un pipeline de publication dédié pour chaque nouveau plan. Il existe une one-to-one relation entre les plans et les pipelines de publication.



Étapes du pipeline de lancement

L'image suivante montre les étapes par défaut du pipeline de publication et les ressources avec lesquelles le pipeline interagit. Chaque étape du pipeline est un CodeBuild projet.



Les étapes du pipeline de publication sont les suivantes :

1. Alignement des fichiers — Cette étape vérifie que le plan est un CloudFormation modèle ou une AWS Cloud Development Kit (AWS CDK) construction. Si le plan est une AWS CDK construction, cette étape synthétise la AWS CDK construction dans un CloudFormation modèle. Ce processus automatise et normalise les déploiements via. CloudFormation Si des erreurs sont détectées, le pipeline échoue.
2. Vérification de syntaxe — Les erreurs de syntaxe sont une cause fréquente d'erreurs de CloudFormation déploiement. À ce stade, AWS CloudFormation Linter (cfn-lint) vérifie les erreurs de syntaxe en comparant le modèle à la spécification de la ressource.AWS CloudFormation Il effectue également d'autres contrôles, tels que la vérification de la validité des valeurs des propriétés des ressources et le respect des meilleures pratiques. Si des erreurs sont détectées, le pipeline échoue et cfn-lint renvoie des suggestions.
3. Contrôle : à ce stade, cfn_nag vérifie les éventuels problèmes de sécurité en recherchant des modèles. Par exemple, il vérifie la présence de groupes de sécurité et de politiques AWS Identity and Access Management (IAM) trop permissifs, de chiffrement manquant et de littéraux de mot de passe. Si des erreurs sont détectées, le pipeline échoue et cfn_nag renvoie des suggestions.
4. Vérification de version — Le pipeline de publication effectue le contrôle de version en fonction de la stratégie de version définie dans le fichier de configuration du produit. Si la version du produit est définie comme immuable, Service Catalog désactive la version précédente du produit.
5. Publier le produit : le pipeline de publication publie le produit dans Service Catalog.

> **Note**
>
> Le pipeline de publication est personnalisable. Par exemple, vous pouvez supprimer toutes les étapes qui ne sont pas applicables à votre cas d'utilisation. Vous pouvez également ajouter d'autres étapes si vous souhaitez ajouter d'autres contrôles, des

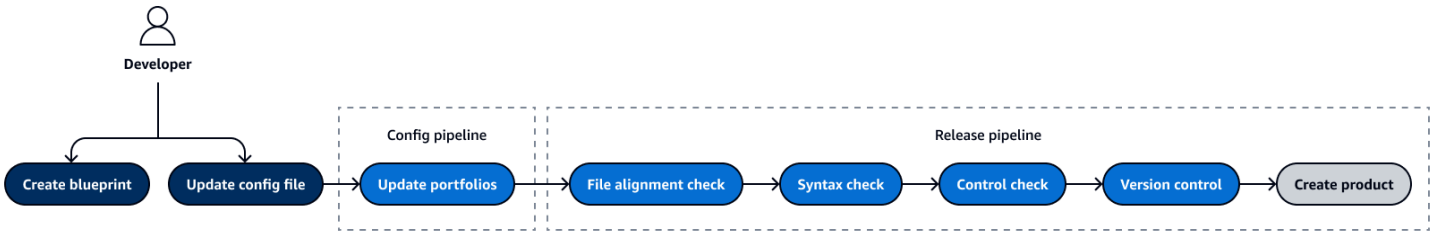
validations supplémentaires ou une étape d'approbation manuelle. Ce guide ne contient pas d'instructions pour modifier le pipeline de publication. Pour plus d'informations, consultez la CodeBuilddocumentation CodePipelineet.

Cycle de vie du Blueprint dans l'Enterprise Blueprint Factory

Le cycle de vie d'un plan Enterprise Blueprint Factory comprend trois étapes typiques : création, mise à jour et suppression. L'étape du cycle de vie affecte les actions effectuées par le pipeline de configuration et le pipeline de publication.

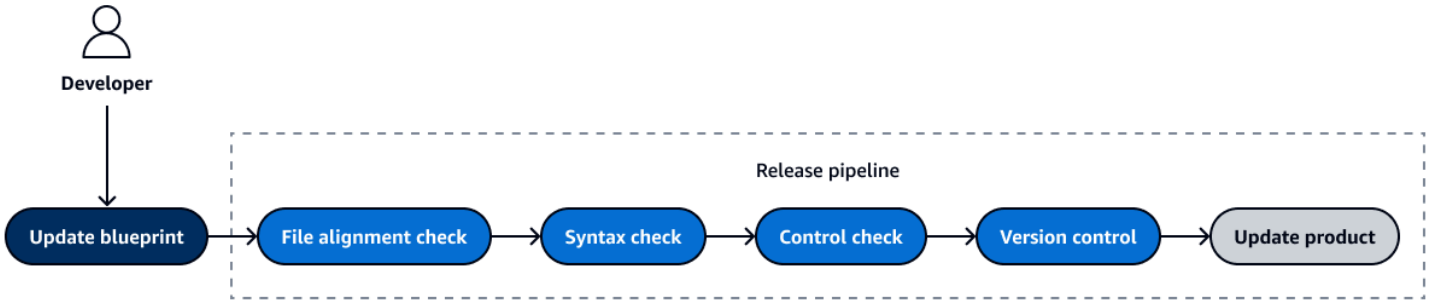
Création d'un plan

Pour publier un nouveau plan en tant que produit dans AWS Service Catalog, un développeur fusionne le plan dans le référentiel de produits, met à jour les portefeuilles dans le fichier de configuration et ajoute le nouveau produit au fichier de configuration. Cela appelle le pipeline de configuration. Le pipeline de configuration crée un pipeline de publication pour le produit. Dans le pipeline de publication, le plan est soumis à plusieurs contrôles de sécurité. Le pipeline de publication déploie ensuite le plan en tant que produit Service Catalog.

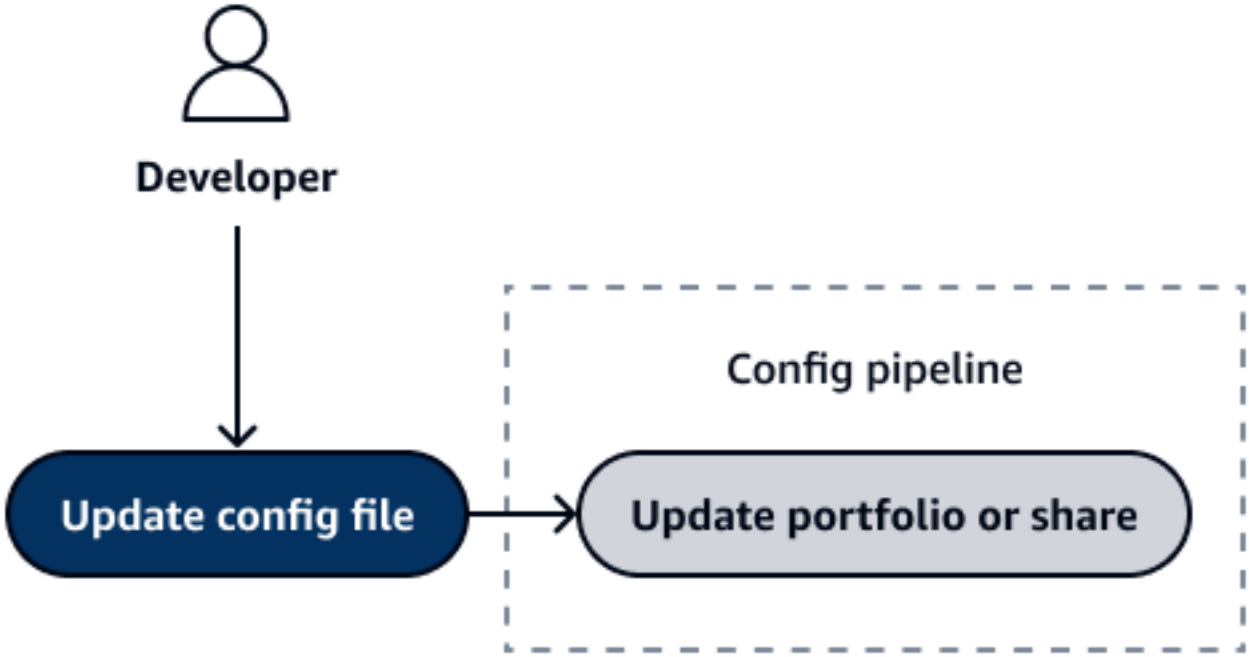


Mise à jour du plan

Un développeur peut mettre à jour le produit dans Service Catalog en fusionnant une version mise à jour du plan dans le référentiel de produits. Cette mise à jour appelle le pipeline de publication du produit. Le modèle mis à jour est soumis aux contrôles de sécurité dans le pipeline de publication. Le pipeline de publication déploie une nouvelle version du produit Service Catalog. Pour plus d'informations sur la façon dont Service Catalog met à jour la version du produit, consultez la section Gestion des versions dans la documentation Service Catalog.



Vous pouvez également mettre à jour le portefeuille Service Catalog auquel le plan est associé ou modifier les configurations de partage de ces portefeuilles. Dans ce cas, le développeur met à jour le fichier de configuration dans le dépôt de configuration. Le pipeline de configuration met à jour les portefeuilles ou les actions du portefeuille. Dans ce cas, le produit figurant dans Service Catalog est inchangé, bien qu'il puisse désormais être inclus dans différents portefeuilles.



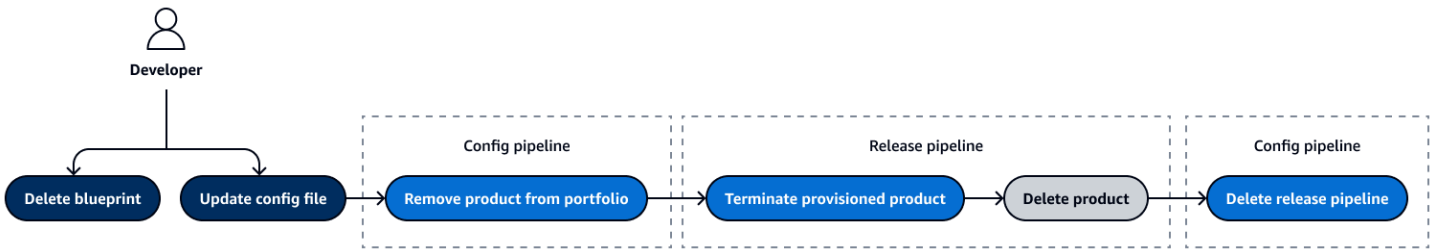
Suppression du plan

> **Important**
>
> Vous ne pouvez pas récupérer un produit Service Catalog une fois qu'il a été supprimé. Toutefois, vous pouvez redéployer le plan en tant que nouveau produit.

Lorsque vous supprimez un produit, Service Catalog supprime toutes les versions du produit de chaque portefeuille contenant le produit. Pour plus d'informations, consultez la section Suppression de produits dans la documentation du Service Catalog.

Pour supprimer un plan après son déploiement dans Service Catalog, un développeur supprime le plan dans le référentiel du produit. Ensuite, ils retirent le produit du fichier de configuration. Le pipeline de configuration dissocie le produit des portefeuilles qui le contiennent et supprime tous les produits associés. Le pipeline de publication met fin au produit Service Catalog et aux produits fournis. Ensuite, le pipeline de configuration supprime le pipeline de publication du produit.

Si le pipeline de configuration ne parvient pas à dissocier toutes les ressources du produit, le produit n'est pas supprimé et le pipeline échoue. Vous devez résoudre l'échec de dissociation des ressources, puis redémarrer le pipeline. Pour plus d'informations, voir Résolution des dissociations de ressources ayant échoué lors de la suppression d'un produit.



Configuration de l'Enterprise Blueprint Factory

Cette section vous aide à configurer l'Enterprise Blueprint Factory dans votre AWS environnement. Il inclut des instructions détaillées pour configurer les référentiels requis et les AWS ressources pour l'Enterprise Blueprint Factory.

Prérequis

Les conditions préalables à la configuration de l'Enterprise Blueprint Factory dans votre AWS environnement sont les suivantes :

- Ce qui suit Comptes AWS :
  - Un compte utilisé pour administrer l'Enterprise Blueprint Factory et pour lancer des produits
  - Un ou plusieurs comptes consommant le produit publié
- Tous les comptes sont les suivants :
  - Géré en tant qu'organisation dans AWS Organizations
  - Situé dans la même unité organisationnelle (UO)
  - L'organisation suit le account-per-tenant modèle
- AWS Command Line Interface (AWS CLI), installé et configuré
- Autorisations permettant de déployer une AWS CloudFormation pile qui crée les AWS ressources suivantes :
  - Groupe de CloudWatch journaux Amazon Logs
  - AWS CodePipeline canalisations
  - AWS CodeBuild projets
  - Politique et règle d'Amazon EventBridge Event Bus
  - AWS Identity and Access Management rôle et politique (IAM)
  - AWS Key Management Service (AWS KMS) politique clé et clé
  - AWS Service Catalog portefeuilles, produits et produits approvisionnés
  - Rubrique, politique relative à Amazon Simple Notification Service (Amazon SNS) et abonnement
  - Compartiments Amazon Simple Storage Service (Amazon S3)
  - AWS Systems Manager Paramètres du magasin de paramètres

Pour plus d'informations sur la configuration de ces autorisations, consultez la CloudFormation documentation et la mise en œuvre de politiques pour les autorisations de moindre privilège pour. AWS CloudFormation

- Un GitHub compte

Bonnes pratiques

Nous vous recommandons de suivre les meilleures pratiques suivantes lors de la configuration de l'Enterprise Blueprint Factory dans votre AWS environnement :

- Lorsque vous configurez les autorisations nécessaires pour déployer l'Enterprise Blueprint Factory, suivez le principe du moindre privilège et accordez les autorisations minimales requises. Pour plus d'informations, consultez les sections Accorder le moindre privilège et Bonnes pratiques en matière de sécurité dans la documentation IAM.
- Lorsque vous configurez l'accès aux portefeuilles Service Catalog, suivez le principe du moindre privilège et accordez l'accès uniquement à des rôles, utilisateurs ou administrateurs spécifiques. Suivez les meilleures pratiques de sécurité pour Service Catalog.

Création des référentiels

Cette section vous aide à configurer le référentiel de configuration et le référentiel de produits pour Enterprise Blueprint Factory. Pour configurer vos référentiels, vous devez bifurquer les référentiels fournis. GitHub Ensuite, vous pouvez AWS CodeConnections créer une connexion à votre GitHub dépôt. Ensuite, vous clonez les GitHub référentiels sur votre machine locale.

Pour forger les GitHub référentiels

1. Connexion à GitHub.
2. Accédez au GitHub référentiel de configuration.
3. Choisissez Fork.
4. Sur la page Créer un nouveau fork, dans le champ Nom du référentiel, entrez`ServiceCatalog-ConfigRepo`.
5. (Facultatif) Entrez une description.
6. Sélectionnez Copier uniquement la branche principale.

7. Choisissez Create fork.
8. Répétez ces étapes pour forker le GitHub référentiel Code. Entrez le nom `ServiceCatalog-CodeRepo` de ce référentiel.
9. Répétez ces étapes pour créer un fork dans le GitHub référentiel Product Repo. Entrez le nom `ServiceCatalog-BlueprintProductRepo` de ce référentiel.

Pour créer la CodeConnections connexion

1. Dans la CLI AWS, entrez la commande suivante pour créer une CodeConnections connexion à GitHub :

```
aws codeconnections create-connection --provider-type GitHub --connection-name
 <MyConnection>
```

2. Utilisez la console AWS Developer Tools pour terminer la connexion. Pour plus d'informations, voir Mettre à jour une connexion en attente.

Pour cloner les référentiels bifurqués

- Entrez les commandes suivantes pour cloner les GitHub référentiels sur votre station de travail locale :

```
git clone git@github.com:<user>/aws-enterprise-blueprint-factory-config-repo
 ServiceCatalog-ConfigRepo
git clone git@github.com:<user>/aws-enterprise-blueprint-factory-blueprint-repo
 ServiceCatalog-BlueprintProductRepo
git clone git@github.com:<user>/aws-enterprise-blueprint-factory-code-repo
 ServiceCatalog-CodeRepo
```

Configuration de l'Enterprise Blueprint Factory

Les instructions de cette section décrivent comment configurer l'Enterprise Blueprint Factory sur votre compte cible. Le dépôt de produits à partir duquel vous avez cloné GitHub contient deux exemples de CloudFormation modèles, et`BP-S3`. `BP-SNS` En suivant ces instructions, vous déployez ces deux exemples de plans en tant que produits dans Service Catalog.

Pour configurer les rôles

1. Dans le compte Blueprint Developer, créez la politique de confiance suivante, puis enregistrez-la sous le nom : `sc-enduserrole-trust-policy.json`

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::123456789012:role/ServiceCatalogEndUserRole"
    },
    "Action": "sts:AssumeRole"
  }
}
```

2. Entrez la commande suivante pour créer le rôle `ServiceCatalogEndUserRole` IAM :

```
aws iam create-role \
--role-name ServiceCatalogEndUserRole \
--assume-role-policy-document file://sc-enduserrole-trust-policy.json
aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AWSServiceCatalogEndUserFullAccess \
-- role-name ServiceCatalogEndUserRole
```

> **Note**
>
> Les développeurs utilisent ce `ServiceCatalogEndUserRole` rôle pour fournir le produit Service Catalog. Ce rôle n'a pas besoin d'autorisations pour créer les ressources définies dans le plan. Cela suit les meilleures pratiques en matière d'autorisations les moins privilégiées et de séparation des tâches.

3. Créez la politique de confiance suivante, puis enregistrez-la sous le nom `sc-launchconstraintrole-trust-policy.json` :

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

```
      "Service": "servicecatalog.amazonaws.com"
    },
    "Action": "sts:AssumeRole"
  }
}
```

4. Entrez la commande suivante pour créer le rôle `ServiceCataloglogLaunchConstraintRole` IAM :

```
aws iam create-role \
--role-name ServiceCataloglogLaunchConstraintRole \
--assume-role-policy-document file://sc-launchconstraintrole-trust-policy.json
aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AmazonSNSFullAccess \
--role-name ServiceCataloglogLaunchConstraintRole
aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AWSCloudFormationFullAccess \
--role-name ServiceCataloglogLaunchConstraintRole
```

5. Ajoutez la politique suivante au rôle `ServiceCataloglogLaunchConstraintRole` IAM. Incluez toutes les autres autorisations requises pour les ressources du produit, comme décrit dans la section Configuration d'un rôle de lancement dans la documentation du Service Catalog :

```
{
          "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetObject"
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "s3:ExistingObjectTag/servicecatalog:provisioning":"true"
            }
         }
   ]
}
```

> **Note**
>
> Service Catalog utilise ce rôle pour déployer la CloudFormation pile en tant que produit dans Service Catalog. La politique de confiance associée à ce rôle garantit que seul Service Catalog peut l'assumer. Les autres utilisateurs ou services ne peuvent pas assumer ce rôle. Cela suit les meilleures pratiques en matière de séparation des tâches.

6. Créez la politique de confiance suivante, puis enregistrez-la sous le nom `sc-codebuild-trust-policy.json` :

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

7. Entrez la commande suivante pour créer le rôle `codebuild-servicecatalog-admin-role` IAM :

```
aws iam create-role \
--role-name codebuild-servicecatalog-admin-role \
--assume-role-policy-document file://sc-codebuild-trust-policy.json
aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AWSCodeBuildAdminAccess \
--role-name codebuild-servicecatalog-admin-role
```

> **Note**
>
> Les CodeBuild tâches du pipeline de configuration utilisent ce rôle.

Pour configurer le compartiment Amazon S3

- Pour créer un compartiment Amazon Simple Storage Service (Amazon S3) utilisé pour stocker les artefacts, suivez les instructions de CodePipeline la section Création d'un compartiment dans la documentation Amazon S3. Suivez les meilleures pratiques de sécurité pour Amazon S3.

Pour configurer les AWS Systems Manager paramètres

- Suivez les instructions de la section Création de paramètres de magasin de paramètres dans Systems Manager afin de créer les paramètres de Systems Manager dans le tableau suivant. Ces paramètres sont utilisés dans le CloudFormation modèle qui déploie le pipeline de configuration.

Nom du paramètre	Type	Description
`/blueprints/resources/vpc_id`	Chaîne	Paramètre qui stocke l'ID du cloud privé virtuel (VPC) cible.
`/blueprints/resources/subnets`	StringList	Paramètre qui stocke IDs les sous-réseaux cibles.
`/blueprints/resources/securitygroups`	StringList	Paramètre qui stocke les groupes IDs de sécurité cibles.
`/blueprints/resources/artifacts-bucket-name`	Chaîne	Paramètre qui stocke le nom du compartiment Amazon S3 utilisé pour les CodePipeline artefacts.

Nom du paramètre	Type	Description
`/blueprints/resources/BlueprintRepo`	Chaîne	Paramètre qui stocke le GitHub dépôt dans lequel sont stockés les plans d'Enterprise Blueprint Factory. La valeur par défaut est `<user>/aws-enterprise-blueprint-factory-blueprint-repo` .
`/blueprints/resources/CodeRepo`	Chaîne	Paramètre qui stocke le GitHub dépôt dans lequel le code du pipeline de configuration d'Enterprise Blueprint Factory et le `Bootstrapping-Admin-Product` code sont stockés. La valeur par défaut est `<user>/aws-enterprise-blueprint-factory-code-repo` .
`/blueprints/resources/ConfigRepo`	Chaîne	Paramètre qui stocke le GitHub dépôt dans lequel sont stockés les fichiers de configuration d'Enterprise Blueprint Factory. La valeur par défaut est `<user>/aws-enterprise-blueprint-factory-config-repo` .

Pour mettre à jour les CloudFormation modèles

1. Dans le référentiel de code (`ServiceCatalog-CodeRepo`), ouvrez le fichier ServiceCatalog-Pipeline.yml.
2. Modifiez les valeurs par défaut des paramètres suivants dans ce fichier :
   - `ConfigRepositoryName`est le paramètre Systems Manager qui stocke le GitHub dépôt dans lequel sont stockés les fichiers de configuration d'Enterprise Blueprint Factory. La valeur par défaut est `/blueprints/resources/ConfigRepo`.
   - `CodeRepositoryName`est le paramètre Systems Manager qui stocke le GitHub dépôt dans lequel le code du pipeline de configuration d'Enterprise Blueprint Factory et le `Bootstrapping-Admin-Product` code sont stockés. La valeur par défaut est `/blueprints/resources/CodeRepo`.
   - `BlueprintRepositoryName`est le paramètre Systems Manager qui stocke le GitHub dépôt dans lequel sont stockés les plans d'Enterprise Blueprint Factory. La valeur par défaut est `/blueprints/resources/BlueprintRepo`.
   - `BranchName`est la branche du référentiel de configuration dans laquelle le fichier de configuration est stocké. La valeur par défaut est `main`.
   - `VPCID`est le paramètre Systems Manager qui stocke l'ID du VPC cible. La valeur par défaut est `/blueprints/resources/vpc_id`.
   - `Subnets`est le paramètre Systems Manager qui stocke IDs les sous-réseaux cibles. La valeur par défaut est `/blueprints/resources/subnets`.
   - `SecurityGroupIds`est le paramètre Systems Manager qui stocke les groupes IDs de sécurité cibles. La valeur par défaut est `/blueprints/resources/securitygroups`.
   - `IamRoleName`est le nom du rôle IAM utilisé par les CodeBuild tâches. La valeur par défaut est`codebuild-servicecatalog-admin-role`.
   - `EnvironmentType`est l'environnement dans lequel vous déployez l'Enterprise Blueprint Factory. La valeur par défaut est `DEV`.
   - `ArtifactBucket`est le paramètre Systems Manager qui stocke le compartiment Amazon S3 dans lequel sont stockés CodePipeline les artefacts. La valeur par défaut est`/blueprints/resources/artifacts-bucket-name`.
   - `CodeConnectionArn`est le nom de ressource Amazon (ARN) de la CodeConnections connexion à GitHub.
3. Enregistrez et fermez le fichier ServiceCatalog-Pipeline.yml.

4. Entrez les commandes suivantes pour fusionner les modifications dans le référentiel de code :

```
cd ServiceCatalog-CodeRepo
git add ServiceCatalog-Pipeline.yml
git commit -m "<description of change>"
git push origin main
```

5. Dans le référentiel de configuration (`ServiceCatalog-ConfigRepo`), ouvrez le fichier bp_config.yml.
6. Mettez à jour les valeurs de la section du portefeuille selon les besoins de votre organisation. Par exemple, mettez à jour les `share_to_ou` attributs `portfolio_access_roles` et. Pour plus d'informations, consultez la section Fichier de configuration de ce guide.
7. Enregistrez et fermez le fichier bp_config.yml.
8. Entrez les commandes suivantes pour fusionner les modifications dans le référentiel de code :

```
cd ServiceCatalog-ConfigRepo
git add bp_config.yml
git commit -m "<description of change>"
git push origin main
```

Pour déployer la CloudFormation pile

1. Connectez-vous au compte administratif d'Enterprise Blueprint Factory.
2. Passez à un rôle IAM doté d'autorisations administratives.
3. Ouvrez la CloudFormation console.
4. Dans la barre de navigation en haut de l'écran, choisissez la cible Région AWS.
5. Sur la page Stacks, choisissez Create stack en haut à droite, puis choisissez Avec de nouvelles ressources (standard).
6. Pour Préparer le modèle, choisissez Le modèle est prêt.
7. Sous Spécifier le modèle, choisissez Charger un fichier modèle.
8. Choisissez Choisir un fichier, naviguez jusqu'au `ServiceCatalog-CodeRepo` dossier, puis choisissez ServiceCatalog-Pipeline.yml.
9. Choisissez Next pour continuer et valider le modèle.
10. Dans Nom de la pile, entrez le nom de la pile.
11. Dans la section Paramètres, ne modifiez pas les valeurs par défaut.

12. Choisissez Suivant.
13. Sur la page Configurer les options de pile, ne modifiez pas les valeurs par défaut, puis choisissez Next.
14. Sur la page Réviser et créer, vérifiez les détails du modèle et de la pile, puis choisissez Soumettre.
15. Surveillez la progression du déploiement de la pile. Pour plus d'informations, consultez la documentation CloudFormation.
16. Attendez que le statut passe à`CREATE_COMPLETE`.

Pour valider le déploiement

1. Ouvrez la AWS Service Catalog console.
2. Dans le volet de navigation, sélectionnez Products.
3. Vérifiez que ServiceCatalog-Pipeline est disponible dans la liste des produits.
4. Ouvrez la AWS CodePipeline console.
5. Dans Nom, choisissez le pipeline de configuration. Par défaut, le nom du pipeline est`ServiceCatalog-Pipeline`.
6. Choisissez Afficher l'historique.
7. Consultez l'état du pipeline et de l'exécution de l'étape. Pour plus d'informations sur le statut, voir Afficher le statut d'exécution dans la CodePipeline documentation.
8. Attendez que l'état du pipeline de configuration soit atteint`Succeeded`.
9. Ouvrez la console Service Catalog.
10. Dans le volet de navigation, sélectionnez Products.
11. Vérifiez que les produits BP-S3 et BP-SNS sont disponibles. Cela indique que les pipelines de lancement du produit pour les exemples de plans ont été achevés avec succès.
12. Si vous souhaitez supprimer les exemples de plans que vous avez déployés lors de la configuration de l'Enterprise Blueprint Factory, suivez les instructions de la section Supprimer un plan.

Supprimer l'Enterprise Blueprint Factory

Si vous n'utilisez pas l'Enterprise Blueprint Factory, vous pouvez la supprimer pour ne plus avoir à supporter les coûts associés à ses ressources. AWS

Pour supprimer les ressources

1. Entrez les commandes suivantes pour supprimer les rôles IAM déployés dans le compte administratif d'Enterprise Blueprint Factory :

```
aws iam detach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AWSServiceCatalogEndUserFullAccess \
--role-name ServiceCatalogEndUserRole
aws iam delete-role --role-name ServiceCatalogEndUserRole
aws iam detach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AmazonSNSFullAccess \
--role-name ServiceCataloglogLaunchConstraintRole
aws iam delete-role --role-name ServiceCataloglogLaunchConstraintRole
```

2. Supprimez la CloudFormation pile de l'Enterprise Blueprint Factory. Pour obtenir des instructions, voir Supprimer une pile de la CloudFormation console ou Supprimer une pile de AWS CLI.
3. Supprimez le compartiment Amazon S3 utilisé pour stocker les CodePipeline artefacts. Pour obtenir des instructions, consultez Supprimer un compartiment dans la documentation Amazon S3.
4. Supprimez les paramètres Systems Manager suivants de Parameter Store :

   - `/blueprints/resources/vpc_id`
   - `/blueprints/resources/subnets`
   - `/blueprints/resources/securitygroups`
   - `/blueprints/resources/artifacts-bucket-name`
   - `/blueprints/resources/BlueprintRepo`
   - `/blueprints/resources/CodeRepo`
   - `/blueprints/resources/ConfigRepo`

   Pour obtenir des instructions, consultez Supprimer des paramètres du Parameter Store dans la documentation de Systems Manager.

Utilisation de l'Enterprise Blueprint Factory

Cette section vous aide à créer, mettre à jour ou supprimer des plans dans votre environnement. Il fournit des instructions détaillées pour gérer un plan tout au long de son cycle de vie.

Pour créer ou mettre à jour des plans personnalisés, vous devez savoir comment créer des modèles IaC, tels que des AWS CloudFormation modèles ou des AWS Cloud Development Kit (AWS CDK) constructions. Ce guide ne contient pas d'informations ni d'instructions sur la façon de définir les plans que vous publiez via Enterprise Blueprint Factory.

Prérequis

Les conditions préalables à l'utilisation de l'Enterprise Blueprint Factory dans votre AWS environnement sont les suivantes :

- AWS Command Line Interface (AWS CLI), installé et configuré
- Autorisations pour assumer le `ServiceCatalogEndUserRole` AWS Identity and Access Management rôle (IAM)
- Un CloudFormation modèle ou une AWS CDK construction

Création d'un plan

Les pipelines Enterprise Blueprint Factory déploient les plans que vous définissez dans le fichier de configuration. Le développeur lance le pipeline de configuration en fusionnant le fichier de configuration dans le référentiel de configuration. Ensuite, l'Enterprise Blueprint Factory utilise le `ServiceCatalogLaunchConstraintRole` pour déployer le plan en tant que produit dans Service Catalog. Pour plus d'informations sur les actions effectuées par le pipeline de configuration et le pipeline de publication lorsque vous créez un plan, consultez la section Création du plan dans ce guide.

Pour ajouter le plan au référentiel de produits

1. Assurez-vous d'avoir configuré votre Enterprise Blueprint Factory conformément aux instructions de la section Configuration de l'Enterprise Blueprint Factory de ce guide.
2. Vérifiez que la politique du `ServiceCataloglogLaunchConstraintRole` rôle vous permet de fournir les ressources définies dans le plan.

3. Dans le référentiel de produits (`ServiceCatalog-BlueprintProductRepo`), créez un dossier pour le nouveau plan.
4. Collez le modèle IaC (CloudFormation modèle ou AWS CDK construction) dans le dossier que vous avez créé.
5. Créez un fichier nommé product_config.json dans le dossier que vous avez créé.
6. Ouvrez le fichier product_config.json et collez-y le texte suivant :

```
{
    "SchemaVersion": "1.0",
    "ProductVersionName": "1.0.1",
    "Deprecated_Versions" : [],
    "ProductVersionDescription": "<description>",
    "ProductType": "CLOUD_FORMATION_TEMPLATE",
    "Properties": {
        "TemplateFilePath": "./<folder name>/<file name>"
    }
}
```

Où :

- `<description>`est une brève description de la version du plan
- `<folder name>`est le nom du dossier que vous avez créé dans le référentiel de produits
- `<file name>`est le nom du modèle IaC

> **Note**
>
> Vous pouvez mettre à jour la version du schéma ou les noms de version du produit en fonction des politiques de votre organisation.

7. Enregistrez et fermez le fichier product_config.json.
8. Entrez les commandes suivantes pour fusionner les modifications dans le référentiel de produits :

```
cd ServiceCatalog-BlueprintProductRepo
git add <folder name>/<file name> <folder name>\product_config.json
git commit -m "The first version of <file name> blueprint"
git push origin main
```

Pour mettre à jour le fichier de configuration

1. Dans le référentiel de configuration (`ServiceCatalog-ConfigRepo`), ouvrez le fichier config.yml.
2. Modifiez la `portfolios` section et `products` la section selon les besoins du nouveau plan. Pour plus d'informations, consultez la section Fichier de configuration de ce guide.
3. Enregistrez et fermez le fichier config.yml.
4. Entrez les commandes suivantes pour fusionner les modifications dans le référentiel de configuration :

```
cd ServiceCatalog-ConfigRepo
git add config.yml
git commit -m "<description of change>"
git push origin main
```

   L'approbation de cette pull request lance le pipeline de configuration. Le pipeline de configuration crée un pipeline de lancement pour le produit.

Pour consulter les journaux de déploiement

1. Connectez-vous au compte administratif d'Enterprise Blueprint Factory.
2. Ouvrez la AWS CodePipeline console.
3. Dans Nom, choisissez le pipeline de publication du produit. Par défaut, le nom du pipeline est`BluePrint_<Product-Name>-<CloudFormation-Stack-Name>`.
4. Choisissez Afficher l'historique.
5. Consultez l'état du pipeline et de l'exécution de l'étape. Pour plus d'informations sur le statut, voir Afficher le statut d'exécution dans la CodePipeline documentation.
6. En cas de défaillance du pipeline, examinez la cause de la panne. Pour obtenir des instructions sur la façon de configurer la surveillance de vos pipelines, consultez la section Surveillance des pipelines dans la CodePipeline documentation. Si le pipeline de publication a échoué en raison d'une vérification cfn-lint ou cfn_nag, corrigez l'erreur dans le modèle. Soumettez une autre pull request au dépôt du produit. Cela redémarre le pipeline de publication. Pour plus d'informations sur la correction des erreurs de modèle, consultez la section Dépannage de ce guide.
7. Attendez que l'état du pipeline de publication soit atteint`Succeeded`.

Pour valider le déploiement

1. Connectez-vous à un compte client dans l'organisation.
2. Assumez le rôle `ServiceCatalogEndUserRole` IAM.
3. Ouvrez la console Service Catalog.
4. Dans le volet de navigation, sélectionnez Products.
5. Vérifiez que le nouveau produit est disponible dans la liste des produits.

Mise à jour d'un plan

Pour plus d'informations sur les actions effectuées par le pipeline de configuration et le pipeline de publication lorsque vous créez un plan, consultez la section Mise à jour du plan dans ce guide.

Pour mettre à jour un plan

1. Dans le référentiel du produit, accédez au dossier du produit.
2. Collez le modèle IaC mis à jour. Assurez-vous que le nom du fichier est identique à celui de la version précédente.
3. Ouvrez le fichier product_config.json.
4. Pour`ProductVersionName`, mettez à jour le numéro de version.
5. Si vous souhaitez empêcher le déploiement futur de la version précédente du produit`Deprecated_Versions`, entrez les numéros de version précédents dans une liste séparée par des virgules.
6. Entrez les commandes suivantes pour fusionner les modifications dans le référentiel de produits :

```
cd ServiceCatalog-BlueprintProductRepo
git add <folder name>/<file name> <folder name>\product_config.json
git commit -m "Version <number> of <file name> blueprint"
git push origin main
```

   L'approbation de cette pull request lance le pipeline de lancement du produit.

Pour consulter les journaux de déploiement

1. Connectez-vous au compte administratif d'Enterprise Blueprint Factory.

2. Ouvrez la AWS CodePipeline console.
3. Dans Nom, choisissez le pipeline de publication. Par défaut, le nom du pipeline est`BluePrint_<Product-Name>-<CloudFormation-Stack-Name>`.
4. Choisissez Afficher l'historique.
5. Consultez l'état du pipeline et de l'exécution de l'étape. Pour plus d'informations sur le statut, voir Afficher le statut d'exécution dans la CodePipeline documentation.
6. En cas de défaillance du pipeline, examinez la cause de la panne. Pour obtenir des instructions sur la façon de configurer la surveillance de vos pipelines, consultez la section Surveillance des pipelines dans la CodePipeline documentation. Si le pipeline de publication a échoué en raison d'une vérification cfn-lint ou cfn_nag, corrigez l'erreur dans le modèle. Soumettez une autre pull request au dépôt du produit. Cela redémarre le pipeline de publication. Pour plus d'informations sur la correction des erreurs de modèle, consultez la section Dépannage de ce guide.
7. Attendez que l'état du pipeline de publication soit atteint`Succeeded`.

Pour valider la mise à jour

1. Connectez-vous à un compte client dans l'organisation.
2. Assumez le rôle `ServiceCatalogEndUserRole` IAM.
3. Ouvrez la console Service Catalog.
4. Dans le volet de navigation, sélectionnez Products.
5. Vérifiez que la nouvelle version du produit est disponible dans la liste des produits.

Supprimer un plan

Lorsque vous supprimez un produit, Service Catalog supprime toutes les versions du produit de chaque portefeuille contenant le produit. Pour plus d'informations, consultez la section Suppression de produits dans la documentation du Service Catalog. Pour plus d'informations sur les actions effectuées par le pipeline de configuration et le pipeline de publication lorsque vous créez un plan, consultez la section Suppression du plan dans ce guide.

Pour supprimer un plan

1. Dans le référentiel de configuration, ouvrez le fichier config.yml.

2. Modifiez la section des produits, supprimez ou commentez le produit que vous souhaitez supprimer.
3. Enregistrez et fermez le fichier config.yml.
4. Entrez les commandes suivantes pour fusionner les modifications dans le référentiel de configuration :

```
cd ServiceCatalog-ConfigRepo
git add config.yml
git commit -m "<description of change>"
git push origin main
```

L'approbation de cette pull request lance le pipeline de configuration. Le pipeline de configuration supprime le produit et son pipeline de lancement.

5. Dans le référentiel du produit, supprimez le dossier du produit, y compris son contenu.
6. Entrez les commandes suivantes pour fusionner les modifications dans le référentiel de produits :

```
cd ServiceCatalog-BlueprintProductRepo
git add .
git commit -m "Delete <file name> blueprint"
git push origin main
```

Pour valider la suppression

1. Connectez-vous à un compte client dans l'organisation.
2. Assumez le rôle `ServiceCatalogEndUserRole` IAM.
3. Ouvrez la console Service Catalog.
4. Dans le volet de navigation, sélectionnez Products.
5. Vérifiez que le produit supprimé n'est plus disponible.

Résolution des problèmes

Lorsque vous créez ou mettez à jour un plan, les outils cfn-lint et cfn-nag valident le plan. Pour plus d'informations sur la validation dans le pipeline de publication, consultez la section Pipeline de publication de ce guide. Toute erreur de syntaxe ou de sécurité signalée entraîne l'échec du pipeline.

Pour déployer correctement le plan dans le pipeline de publication, vous devez corriger les erreurs contenues dans le plan.

Voici un exemple de sortie qui montre deux erreurs liées à la sécurité, une défaillance et un avertissement.

```
BP-SNS.yml
-------------------------------------------------
BP-SNS.yml
-------------------------------------------------
| WARN W47
|
| Resource: ["ExampleTopic"]
| Line numbers: [5]
|
| SNS Topic should specify KmsMasterKeyId property
-------------------------------------------------
| FAIL F18
|
| Resource: ["ExampleTopicPolicy"]
| Line numbers: [10]
|
| SNS topic policy should not allow * principal

Failures count: 1
Warnings count: 1
```

Pour corriger ces erreurs, dans le fichier de plan, vous devez remplacer le * principal dans la politique thématique d'Amazon Simple Notification Service (Amazon SNS) et associer une clé AWS Key Management Service (AWS KMS) au sujet. L'exemple de code suivant illustre ces mises à jour.

```
ExampleTopic:
    Type: AWS::SNS::Topic
    Properties:
      TopicName: ExampleTopic
  ExampleTopicPolicy:
    Type: AWS::SNS::TopicPolicy
    Properties:
      KmsMasterKeyId: alias/aws/sns  # Added KMS key
      PolicyDocument:
        Id: Id1
        Version: '2012-10-17'
```

```
        Statement:
        - Sid: Sid2
          Effect: Allow
          Principal:
            "Service" : "s3.amazonaws.com"  # Replaced "AWS": '*'
          Action: 'sns:Publish'
          Resource: !Ref ExampleTopic
      Topics:
        - !Ref ExampleTopic
```

Ressources connexes

AWS documentation

- Tutoriel : Création d'un pipeline qui se déploie sur Service Catalog (AWS CodePipeline documentation)
- AWS CodePipeline documentation
- AWS CodeBuild documentation
- Guide de l'administrateur AWS Service Catalog
- AWS Service Catalog Guide de l'utilisateur

AWS articles de blog

- Déclarez et visualisez votre AWS Service Catalog succession (article de AWS blog)
- Implémentation d'une alarme pour détecter automatiquement la dérive dans les AWS CloudFormation piles (article de AWS blog)

Collaborateurs

Les personnes suivantes ont contribué à ce guide.

Conception

- Haofei Feng, architecte cloud senior, AWS
- Cam Maxwell, conseiller principal en matière de sécurité, AWS
- Joe Guo, ingénieur de support cloud, AWS
- Shreejesh MV, architecte cloud senior, AWS

Révision

- Joseph Dominic, architecte du cloud, AWS

- Naresh Rajaram, architecte de solutions pour partenaires consultants, AWS

Rédaction technique

- Lilly AbouHarb, rédactrice technique senior, AWS

Historique du document

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

Modification	Description	Date
Publication initiale	—	10 octobre 2024

AWS Glossaire des directives prescriptives

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

Nombres

7 R

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

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

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

A

ABAC

Voir contrôle d'accès basé sur les attributs.

services abstraits

Consultez la section Services gérés.

ACIDE

Voir atomicité, consistance, isolation, durabilité.

migration active-active

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

migration active-passive

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

fonction d'agrégation

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

AI

Voir intelligence artificielle.

AIOps

Voir les opérations d'intelligence artificielle.

anonymisation

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

anti-motif

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

contrôle des applications

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

portefeuille d'applications

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

intelligence artificielle (IA)

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

opérations d'intelligence artificielle (AIOps)

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

chiffrement asymétrique

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

atomicité, cohérence, isolement, durabilité (ACID)

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

contrôle d'accès par attributs (ABAC)

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

source de données faisant autorité

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

Zone de disponibilité

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

AWS Cadre d'adoption du cloud (AWS CAF)

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

l'organisation à une adoption réussie du cloud. Pour plus d'informations, veuillez consulter le site Web AWS CAF et le livre blanc AWS CAF.

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

Outil qui évalue les charges de travail liées à la migration des bases de données, recommande des stratégies de migration et fournit des estimations de travail. AWS Le WQF est inclus avec AWS Schema Conversion Tool (AWS SCT). Il analyse les schémas de base de données et les objets de code, le code d'application, les dépendances et les caractéristiques de performance, et fournit des rapports d'évaluation.

B

mauvais bot

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

BCP

Consultez la section Planification de la continuité des activités.

graphique de comportement

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

système de poids fort

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

classification binaire

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

filtre de Bloom

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

déploiement bleu/vert

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

bot

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

botnet

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

branche

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

accès par brise-vitre

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

stratégie existante (brownfield)

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

cache de tampon

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

capacité métier

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

planification de la continuité des activités (BCP)

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

C

CAF

Voir le cadre d'adoption du AWS cloud.

déploiement de Canary

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

CCo E

Voir le Centre d'excellence du cloud.

CDC

Voir capture des données de modification.

capture des données de modification (CDC)

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

ingénierie du chaos

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

CI/CD

Découvrez l'intégration continue et la livraison continue.

classification

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

chiffrement côté client

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

Centre d'excellence du cloud (CCoE)

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

cloud computing

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

modèle d'exploitation du cloud

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

étapes d'adoption du cloud

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

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

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

CMDB

Voir base de données de gestion de configuration.

référentiel de code

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

cache passif

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

données gelées

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

vision par ordinateur (CV)

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

dérive de configuration

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

base de données de gestion des configurations (CMDB)

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

pack de conformité

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

intégration continue et livraison continue (CI/CD)

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

CV

Voir vision par ordinateur.

D

données au repos

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

classification des données

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

dérive des données

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

données en transit

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

maillage de données

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

minimisation des données

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

périmètre de données

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

prétraitement des données

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

provenance des données

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

sujet des données

Personne dont les données sont collectées et traitées.

entrepôt des données

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

langage de définition de base de données (DDL)

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

langage de manipulation de base de données (DML)

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

DDL

Voir langage de définition de base de données.

ensemble profond

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

deep learning

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

defense-in-depth

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

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

administrateur délégué

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

déploiement

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

environnement de développement

Voir environnement.

contrôle de détection

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

cartographie de la chaîne de valeur du développement (DVSM)

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

jumeau numérique

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

tableau des dimensions

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

catastrophe

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

reprise après sinistre (DR)

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

DML

Voir langage de manipulation de base de données.

conception axée sur le domaine

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

DR

Voir reprise après sinistre.

détection de dérive

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

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

DVSM

Voir la cartographie de la chaîne de valeur du développement.

E

EDA

Voir analyse exploratoire des données.

EDI

Voir échange de données informatisé.

informatique de périphérie

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

échange de données informatisé (EDI)

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

chiffrement

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

clé de chiffrement

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

endianisme

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

point de terminaison

Voir point de terminaison de service.

service de point de terminaison

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

planification des ressources d'entreprise (ERP)

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

chiffrement d'enveloppe

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

environment

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

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

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

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

métadonnées de migration

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

modèle de migration

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

Évaluation du portefeuille de migration (MPA)

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

Évaluation de la préparation à la migration (MRA)

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

stratégie de migration

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

ML

Voir apprentissage automatique.

modernisation

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

évaluation de la préparation à la modernisation

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

applications monolithiques (monolithes)

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

MPA

Voir Évaluation du portefeuille de migration.

MQTT

Voir Message Queuing Telemetry Transport.

classification multi-classes

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

infrastructure mutable

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

O

OAC

Voir Contrôle d'accès à l'origine.

OAI

Voir l'identité d'accès à l'origine.

OCM

Voir gestion du changement organisationnel.

migration hors ligne

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

OI

Voir Intégration des opérations.

OLA

Voir l'accord au niveau opérationnel.

migration en ligne

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

OPC-UA

Voir Open Process Communications - Architecture unifiée.

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

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

accord au niveau opérationnel (OLA)

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

examen de l'état de préparation opérationnelle (ORR)

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

technologie opérationnelle (OT)

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

intégration des opérations (OI)

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

journal de suivi d'organisation

Un parcours créé par AWS CloudTrail qui enregistre tous les événements pour tous les membres Comptes AWS d'une organisation dans AWS Organizations. Ce journal de suivi est créé dans

chaque Compte AWS qui fait partie de l'organisation et suit l'activité de chaque compte. Pour plus d'informations, consultez la section Création d'un suivi pour une organisation dans la CloudTrail documentation.

gestion du changement organisationnel (OCM)

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

contrôle d'accès d'origine (OAC)

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

identité d'accès d'origine (OAI)

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

ORR

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

DE

Voir technologie opérationnelle.

VPC sortant (de sortie)

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

P

limite des autorisations

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

informations personnelles identifiables (PII)

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

PII

Voir les informations personnelles identifiables.

manuel stratégique

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

PLC

Voir contrôleur logique programmable.

PLM

Consultez la section Gestion du cycle de vie des produits.

politique

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

persistance polyglotte

Choix indépendant de la technologie de stockage de données d'un microservice en fonction des modèles d'accès aux données et d'autres exigences. Si vos microservices utilisent la même

technologie de stockage de données, ils peuvent rencontrer des difficultés d'implémentation ou présenter des performances médiocres. Les microservices sont plus faciles à mettre en œuvre, atteignent de meilleures performances, ainsi qu'une meilleure capacité de mise à l'échelle s'ils utilisent l'entrepôt de données le mieux adapté à leurs besoins. Pour plus d'informations, veuillez consulter Enabling data persistence in microservices.

évaluation du portefeuille

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

predicate

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

prédicat pushdown

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

contrôle préventif

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

principal

Entité capable d'effectuer AWS des actions et d'accéder à des ressources. Cette entité est généralement un utilisateur root pour un Compte AWS rôle IAM ou un utilisateur. Pour plus d'informations, veuillez consulter la rubrique Principal dans Termes et concepts relatifs aux rôles, dans la documentation IAM.

confidentialité dès la conception

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

zones hébergées privées

Conteneur contenant des informations sur la manière dont vous souhaitez qu'Amazon Route 53 réponde aux requêtes DNS pour un domaine et ses sous-domaines au sein d'un ou de plusieurs

VPCs domaines. Pour plus d'informations, veuillez consulter Working with private hosted zones dans la documentation Route 53.

contrôle proactif

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

gestion du cycle de vie des produits (PLM)

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

environnement de production

Voir environnement.

contrôleur logique programmable (PLC)

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

chaînage rapide

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

pseudonymisation

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

publish/subscribe (pub/sub)

Modèle qui permet des communications asynchrones entre les microservices afin d'améliorer l'évolutivité et la réactivité. Par exemple, dans un MES basé sur des microservices, un microservice peut publier des messages d'événements sur un canal auquel d'autres microservices

peuvent s'abonner. Le système peut ajouter de nouveaux microservices sans modifier le service de publication.

Q

plan de requête

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

régression du plan de requêtes

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

R

Matrice RACI

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

CHIFFON

Voir Retrieval Augmented Generation.

rançongiciel

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

Matrice RASCI

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

RCAC

Voir contrôle d'accès aux lignes et aux colonnes.

réplica en lecture

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

réarchitecte

Voir 7 Rs.

objectif de point de récupération (RPO)

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

objectif de temps de récupération (RTO)

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

refactoriser

Voir 7 Rs.

Région

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

régression

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

réhéberger

Voir 7 Rs.

version

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

déplacer

Voir 7 Rs.

replateforme

Voir 7 Rs.

rachat

Voir 7 Rs.

résilience

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

politique basée sur les ressources

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

matrice responsable, redevable, consulté et informé (RACI)

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

contrôle réactif

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

retain

Voir 7 Rs.

se retirer

Voir 7 Rs.

Génération augmentée de récupération (RAG)

Technologie d'IA générative dans laquelle un LLM fait référence à une source de données faisant autorité qui se trouve en dehors de ses sources de données de formation avant de générer une

réponse. Par exemple, un modèle RAG peut effectuer une recherche sémantique dans la base de connaissances ou dans les données personnalisées d'une organisation. Pour plus d'informations, voir Qu'est-ce que RAG ?

rotation

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

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

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

RPO

Voir l'objectif du point de récupération.

RTO

Voir l'objectif relatif au temps de rétablissement.

runbook

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

S

SAML 2.0

Un standard ouvert utilisé par de nombreux fournisseurs d'identité (IdPs). Cette fonctionnalité permet l'authentification unique fédérée (SSO), afin que les utilisateurs puissent se connecter AWS Management Console ou appeler les opérations de l' AWS API sans que vous ayez à créer un utilisateur dans IAM pour tous les membres de votre organisation. Pour plus d'informations sur la fédération SAML 2.0, veuillez consulter À propos de la fédération SAML 2.0 dans la documentation IAM.

SCADA

Voir Contrôle de supervision et acquisition de données.

SCP

Voir la politique de contrôle des services.

secret

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

sécurité dès la conception

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

contrôle de sécurité

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

renforcement de la sécurité

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

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

Outils et services qui associent les systèmes de gestion des informations de sécurité (SIM) et de gestion des événements de sécurité (SEM). Un système SIEM collecte, surveille et analyse les données provenant de serveurs, de réseaux, d'appareils et d'autres sources afin de détecter les menaces et les failles de sécurité, mais aussi de générer des alertes.

automatisation des réponses de sécurité

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

chiffrement côté serveur

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

Politique de contrôle des services (SCP)

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

point de terminaison du service

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

contrat de niveau de service (SLA)

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

indicateur de niveau de service (SLI)

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

objectif de niveau de service (SLO)

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

modèle de responsabilité partagée

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

SIEM

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

point de défaillance unique (SPOF)

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

SLA

Voir le contrat de niveau de service.

SLI

Voir l'indicateur de niveau de service.

SLO

Voir l'objectif de niveau de service.

split-and-seed modèle

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

SPOF

Voir point de défaillance unique.

schéma en étoile

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

modèle de figuier étrangleur

Approche de modernisation des systèmes monolithiques en réécrivant et en remplaçant progressivement les fonctionnalités du système jusqu'à ce que le système hérité puisse être mis hors service. Ce modèle utilise l'analogie d'un figuier de vigne qui se développe dans un arbre existant et qui finit par supplanter son hôte. Le schéma a été présenté par Martin Fowler comme un moyen de gérer les risques lors de la réécriture de systèmes monolithiques. Pour obtenir un

exemple d'application de ce modèle, veuillez consulter Modernizing legacy Microsoft ASP.NET (ASMX) web services incrementally by using containers and Amazon API Gateway.

sous-réseau

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

contrôle de supervision et acquisition de données (SCADA)

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

chiffrement symétrique

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

tests synthétiques

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

invite du système

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

T

balises

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

variable cible

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

liste de tâches

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

environnement de test

Voir environnement.

entraînement

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

passerelle de transit

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

flux de travail basé sur jonction

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

accès sécurisé

Accorder des autorisations à un service que vous spécifiez pour effectuer des tâches au sein de votre organisation AWS Organizations et dans ses comptes en votre nom. Le service de confiance crée un rôle lié au service dans chaque compte, lorsque ce rôle est nécessaire, pour effectuer des tâches de gestion à votre place. Pour plus d'informations, consultez la section Utilisation AWS Organizations avec d'autres AWS services dans la AWS Organizations documentation.

réglage

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

équipe de deux pizzas

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

U

incertitude

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

tâches indifférenciées

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

environnements supérieurs

Voir environnement.

V

mise à vide

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

contrôle de version

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

Appairage de VPC

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

vulnérabilités

Défaut logiciel ou matériel qui compromet la sécurité du système.

W

cache actif

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

données chaudes

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

fonction de fenêtre

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

charge de travail

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

flux de travail

Groupes fonctionnels d'un projet de migration chargés d'un ensemble de tâches spécifique. Chaque flux de travail est indépendant, mais prend en charge les autres flux de travail du projet.

Par exemple, le flux de travail du portefeuille est chargé de prioriser les applications, de planifier les vagues et de collecter les métadonnées de migration. Le flux de travail du portefeuille fournit ces actifs au flux de travail de migration, qui migre ensuite les serveurs et les applications.

VER

Voir écrire une fois, lire plusieurs.

WQF

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

écrire une fois, lire plusieurs (WORM)

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

Z

exploit Zero-Day

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

vulnérabilité « jour zéro »

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

invite Zero-Shot

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

application zombie

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

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