Implémentation de l'infrastructure en tant que produit (iAP) sur AWS

AWS Directives prescriptives

AWS Directives prescriptives: Implémentation de l'infrastructure en tant que produit (iAP) sur AWS

Table of Contents

Implémentation d'iAP surAWS

Kirsten Kissmeyer, Amazon Web Services (AWS)

Janvier 2023 (historique du document)

Ce guide explore les approches permettant de gérer votreAWS infrastructure en tant que produit (iAP). L'iAP fournit un niveau d'abstraction et de contrôle supérieur à celui de l'infrastructure en tant que code (IAc), mais utilise des méthodes IaC pour atteindre ses objectifs. Le guide explore également lesServices AWS outils de gestion de l'iAP et explique comment chaque outil peut vous aider à atteindre vos objectifs en matière de gestion de votre infrastructure. Les informations contenues dans ce guide sont basées sur les enseignements tirés d'une initiativeAWS Service Catalog d'habilitation pour une très grande entreprise du secteur financier.

Ce guide est destiné aux utilisateurs qui souhaitent développer des servicesAWS Cloud d'infrastructure fonctionnels pouvant être facilement alloués et autorisés selon les besoins des différents utilisateurs de l'organisation, des unités commerciales et des tiers.

Pourquoi gérer l'infrastructure en tant que produits ?

L'avantage de gérer les ressources de votre infrastructure en tant que produits est que vous pouvez regrouper les fonctionnalités destinées aux consommateurs sous la forme d'un ensemble de ressources dotées de définitions et de configurations standardisées. Les produits constituent un moyen pratique pour une organisation de gérer et de contrôler la manière dont lesAWS capacités sont allouées et utilisées. Un produit peut être limité uniquement à des unités organisationnelles (UO) désignées ou à des personnes ayant besoin de ces fonctionnalités. Un produit peut également être limité àRégions AWS des produits spécifiques.

Un modèle de provisionnement de produit vous permet également d'encapsuler et de mettre à jour la définition d'un produit à partir d'un emplacement central. Vous pouvez ensuite distribuer les mises à jour du produit de manière ponctuelle ou planifiée, au fur et à mesure que sa mise en œuvre évolue au fil du temps.

Des résultats commerciaux ciblés

Organizations recherchent toujours de meilleurs moyens de gérer et de provisionner leurAWS infrastructure. Vos objectifs peuvent inclure :

- Atteindre un haut degré d'agilité, de fiabilité, de tolérance aux pannes et de contrôle centralisé, où des points de configuration uniques satisfont à l'évolution des normes internes et externes.
- Un mécanisme à touches ou à bouton-poussoir permettant de distribuer l'infrastructure de manière centralisée, tout en permettant un accès en libre-service en cas de besoin pour des équipes ou des individus spécifiques.
- La capacité de fournir uneAWS infrastructure et des services au personnel interne, aux comptes clients et aux comptes UO des partenaires. Vous souhaiterez peut-être également contrôler les unités d'organisation ou les organisations qui ont accès à des composants d'infrastructure spécifiques dans des régions spécifiques.
- Si vous utilisez des outils tiers (tels que ServiceNow) ou des outils personnalisés pour gérer les demandes d'accès et de mise en service des actifs et de l'infrastructure de votre entreprise, intégration facile entre votreAWS infrastructure et ces outils.
- La possibilité de fournir uneAWS infrastructure à des dizaines, voire des centaines de comptes cibles en même temps.
- Support du provisionnement de plusieursAWS ressources pour fournir une fonctionnalité unique.
- La possibilité de créer de nouveaux comptes avec l'infrastructure requise dans des délais serrés.
- Accès à un inventaire de l'infrastructure que vous avez mise en service et possibilité de mettre à jour ou de supprimer des composants d'infrastructure.
- Des approches et des technologies qui simplifient, accélèrent, sécurisent et fiabilisent le processus de provisionnement et de maintenance.

UtilisationAWS Service Catalog pour gérer iAP

AWSfournit un service appelé AWS Service Catalogqui prend en charge la gestion et le provisionnement deAWS l'infrastructure en tant que produit. Vous pouvez utiliser Service Catalog pour définir rapidement l'infrastructure que vous devez provisionner sous la forme d'un ensemble de produits, accorder l'autorisation d'utiliser ces produits aux parties souhaitées et mettre en œuvre les modèles de provisionnement et de mise à jour requis pour chaque produit.

Le Service Catalog est soutenu par AWS CloudFormation. Les portefeuilles, les produits et leurs modèles de provisionnement du Service Catalog sont gérés sous forme de CloudFormation piles. Vous pouvez définir ces piles de quatre manières :

- En utilisant des CloudFormation modèles standard.
- En utilisant la bibliothèque Service Catalog Construct AWS Cloud Development Kit (AWS CDK)et le Service Catalog avec le langage de programmation compatible que vous préférez.
- En utilisant un framework fourni par un outil tiers pour générer les définitions de CloudFormation pile à partir de métadonnées déclaratives qui décrivent les piles.
- En utilisant l'API Service Catalog. Cette API fournit des méthodes pour tout sauf pour la création du produit. Vous pouvez ajouter des produits à des portefeuilles, en supprimer, étiqueter des produits et des portefeuilles, définir des actions de service administratives et opérationnelles relatives aux produits, et parcourir et rechercher des définitions de portefeuilles et de produits.

À la base, un produit de Service Catalog est un ensemble d'une ou de plusieursAWS ressources configurées pour fournir une fonctionnalité collective personnalisable (par paramétrage). Par exemple, vous pouvez définir un Service Catalog Inventory ory ory ory ory ory ory Simple Storage Service (Amazon S3) privé dans un compte cible. Le compartiment S3 est un produit qui peut comporter des paramètres d'entrée tels que le nom du compartiment, une plage d'adresses Internet à partir de laquelle l'accès est autorisé, un ensemble d'utilisateurs pouvant accéder au compartiment, une politique de hiérarchisation du cycle de vie ou une spécification de gestion des versions du compartiment. Vous pouvez également définir un rôleAWS Identity and Access Management (IAM) pour fournir un accès au compartiment dans le cadre du produit.

Vous pouvez ajouter un produit du Service Catalog à un ou plusieurs portefeuilles. Un portefeuille de Service Catalog est un ensemble de produits regroupés, généralement parce qu'ils ont un objectif similaire (par exemple, analyse, développement, services d'accès client, services d'accès aux partenaires, etc.).

Vous autorisez un utilisateur, un groupe ou un rôle à accéder à la mise en service d'un produit au niveau du portefeuille. Pour le provisionnement, les produits sont associés soit à un rôle IAM de lancement (pour lancer le produit en libre-service à toute personne pouvant assumer ce rôle), soit à un ensemble de piles qui définit un ou plusieurs comptes sur lesquels le produit peut être approvisionné. Pour utiliser un ensemble de piles, vous devez définir un rôle d'administrateur de Service Catalog dans le compte hub de Service Catalog et un rôle d'exécution du provisionnement des produits Service Catalog dans chaque compte cible de l'ensemble de piles.

Les sections suivantes décrivent les fonctionnalités Service Catalog ory ory ory ory ory ory ory ory ory.

Rubriques

Support à la modularité et à la réutilisation du code

Vous pouvez assembler un produit à partir de nombreusesAWS ressources différentes ou même à partir d'autres produits. Idéalement, vous définissez les ressources de manière modulaire afin de pouvoir les réutiliser dans plusieurs produits. La réutilisation au niveau des ressources vous permet d'apporter les modifications future à un seul endroit plutôt que sur tous les produits utilisant ce type de ressource.

Le Service Catalog fournit une fonctionnalité appelée chaînage qui permet la réutilisation au niveau du produit. Vous pouvez associer un produit à un ou plusieurs autres produits. Par exemple, vous souhaiterez peut-être associer un produit de compartiment de journalisation S3 à un produit de surveillance de niveau supérieur. Bien que le chaînage favorise la modularité, il impose certaines complexités opérationnelles car vous devez gérer les dépendances. Service Catalog ne gère pas automatiquement la gestion des versions entre les produits enchaînés. Il ne peut donc pas

garantir que les modifications apportées à un produit n'endommagent pas les autres produits qui en dépendent. Utilisez le chaînage avec précaution et développez vos propres mécanismes pour garantir le contrôle des versions et la gestion des dépendances.

Service Catalog l'utilise de CloudFormation manière native pour déployer un modèle de provisionnement de produits sous forme de CloudFormation pile. Toutefois, Service Catalog impose certaines limites au CloudFormation déploiement de la gamme de produits. En particulier, le provisionnement du Service Catalog ne prend pas en charge la CloudFormation `include` macro permettant d'insérer des segments de script réutilisables ou de référencer CloudFormation des scripts imbriqués (ou des piles) à plusieurs niveaux. Ces restrictions du Service Catalog limitent la possibilité de définir des produits à partir de CloudFormation modèles ou de composants réutilisables, ce qui est une bonne pratique standard lorsque vous définissez des piles de manière native CloudFormation.

> **Note**
>
> Le Service Catalog vous permet de définir correctement des produits à l'aide de modèles de provisionnement qui CloudFormation utilisent ces structures. Toutefois, vous rencontrerez des erreurs de provisionnement si vous utilisez la`include` macro ou si vous imbriquez plusieurs niveaux de scripts dans un CloudFormation modèle de Service Catalog.

Ces restrictions peuvent compliquer la mise en œuvre de produits modulaires et réutilisables dans Service Catalog. Si la modularité est une exigence, vous pouvez envisager d'utiliser leAWS CDK pour implémenter vos produits et leurs modèles de provisionnement, ou utiliser les flux de travail et le moteur de provisionnement du projetAWS Labs Service Catalog Tools. Les deux solutions sont décrites plus loin dans ce guide.

Options de programmation pour définir les produits dans le Service Catalog

Les deux options de programmation permettant d'utiliser le Service Catalog pour provisionnerAWS l'infrastructure sont les CloudFormation modèles ou leAWS CDK. Il n'existe actuellement aucun mécanisme déclaratif ou sans code pour définir un produit du Service Catalog.

CloudFormation écriture de scripts

AWS CloudFormationest un langage de script natif IaC éprouvé pour le provisionnement deAWS l'infrastructure. Vous pouvez développer un CloudFormation script dansAWS Management Console ou à l'aide d'un outil de développement tel que Visual Studio Code (ou un simple éditeur de texte) et leAWS Command Line Interface (AWS CLI).

Pour en savoir plus, consultez la documentation CloudFormation. Pour plus d'informations sur l'utilisation d'un CloudFormation modèle pour spécifier un produit du Service Catalog, consultez la ressourceAWS::ServiceCatalog::CloudFormation Produit dans la CloudFormation documentation.

Approche programmatique avecAWS CDK

LeAWS CDK fournit un cadre de programmation orienté objet élégant et puissant pour définir et maintenir l'AWSinfrastructure en utilisant une sélection de langages de programmation. Vous pouvez utiliser leAWS CDK pour développer des personnalisations et des extensions précises et orientées objet pour le framework deAWS classes. AWS CDKIl s'adresse aux utilisateurs qui souhaitent personnaliserServices AWS pour répondre à des besoins d'infrastructure plus sophistiqués et qui possèdent les compétences et l'expérience de programmation requises.

Pour implémenter des solutions Service Catalog à l'aide deAWS CDK, vous utilisez les classes Service Catalog intégrées pour définir vos produits et portefeuilles. Ces classes sont fournies par le moduleAWS CDKaws-cdk-lib .aws_servicecatalog.

Vous pouvez utiliser leAWS CDK pour implémenter des produits de nombreuses manières. Pour éviter d'avoir à écrire le modèle de provisionnement pour un produit CloudFormation et pour préserver la réutilisabilité, nous vous recommandons d'utiliser laAWS CDK ProductStackclasse pour représenter le modèle de provisionnement. Une`ProductStack` instance est uneAWS CDK pile à laquelle vous ajoutez des ressources par programmation. Par exemple, vous pouvez ajouter un compartiment S3, des rôles IAM ou un CloudWatch journal Amazon. Lorsque vous ajoutez l'`ProductStack`instance à une`servicecatalog.CloudFormationProduct` instance définie en tant que modèle de provisionnement en appelant`servicecatalog.CloudFormationTemplate.fromProductStack (<ProductStack instance>)`, le modèle génèreAWS CDK automatiquement le CloudFormation modèle.

Voici un exemple d'`ProductStack`implémentation Java pour un produit Amazon S3.

```
import * as s3 from 'aws-cdk-lib/aws-s3';
import * as cdk from 'aws-cdk-lib';

class S3BucketProduct extends servicecatalog.ProductStack {
  constructor(scope: Construct, id: string) {
    super(scope, id);

    new s3.Bucket(this, 'BucketProduct');
  }
}

const product = new servicecatalog.CloudFormationProduct(this, 'Product', {
  productName: "My Product",
  owner: "Product Owner",
  productVersions: [
    {
      productVersionName: "v1",
      cloudFormationTemplate:
 servicecatalog.CloudFormationTemplate.fromProductStack(new S3BucketProduct(this,
 'S3BucketProduct')),
    },
  ],
});
```

AWS CDKfournit des pipelines intégrés d'intégration et de déploiement continus (CI/CD). Vous pouvez personnaliser ces pipelines intégrés et ces processus du cycle de vie du développement logiciel (SDLC) pour répondre à vos propres normes et objectifs de processus.

AWS CDKLes classes personnalisées peuvent hériter d'autres classes pour fournir des fonctions spécialisées, et une classe peut être composée d'instances d'autres classes. Si vous utilisez des structures deAWS CDK classes partagées pour implémenter plusieurs produits Service Catalog, prenez en compte les implications en matière de gestion des versions ou de compatibilité, en particulier au sein de plusieurs équipes de développement. Vous devrez vous assurer que les modifications sont rétrocompatibles ou que vous respectez un schéma de gestion des versions afin que les modifications de classe que vous apportez à un produit ne nuisent pas à un autre produit.

Pour en savoir plus, consultez la documentation AWS CDK.

Intégration aux processus de provisionnement et aux flux de travail externes

Vous pouvez interagir avec les composants du Service Catalog à l'aide des API duAWS SDK ou duAWS CLI. Vous pouvez utiliser l'APIAWS SDK Service Catalog pour gérer les produits Service Catalog à partir de n'importe quel outil capable d'intégrer les appels d'API Service Catalog. L'API couvre tous les aspects de la création et de la gestion du Service Catalog. Par exemple, Terraform prend en charge le lancement (approvisionnement) des produits Service Catalog en appelant l'APIAWS SDK Service Catalog dans son Launch Wizard. Pour plus d'informations, consultez la section Lancer desAWS Service Catalog produits avec Terraform dans laAWS documentation.

Vous pouvez également appeler les commandes duAWS CLI Service Catalog pour effectuer des actions sur le Service Catalog. Pour plus d'informations sur les commandes prises en charge, consultez le catalogue de services dans la référence desAWS CLI commandes.

Spécifications relatives à l'approvisionnement des produits

Service Catalog lance le processus de provisionnement en CloudFormation tant que déploiement d'un ensemble de ressources spécifiées dans le modèle de CloudFormation provisionnement. (Le modèle peut être créé directement dansAWS CloudFormation ou généré par laAWS CDK`ProductStack` construction.) Le provisionnement des produits du Service Catalog est un processus fermé. Vous ne pouvez pas le personnaliser pour ajouter des étapes préliminaires ou postérieures au processus, ni le régler. Vous pouvez toutefois modifier le modèle de provisionnement pour ajouter des étapes sous la forme de spécifications de CloudFormation ressources. Il peut s'agirAWS Lambda de ressources personnalisées basées sur Lambda qui effectuent des étapes préliminaires (telles que le démarrage personnalisé pour configurer un hôte bastion utilisé lors du provisionnement) et des étapes ultérieures (telles que le démontage de l'hôte Bastion).AWS Step Functions Cette méthode de mise en œuvre des étapes de pré-provisionnement et de post-provisionnement est soumise aux mêmes`include` restrictions de pile imbriquées que le modèle de provisionnement.

Vous pouvez spécifier des comptes cibles en tant que comptes individuels et non en tant qu'unités organisationnelles. Vous pouvez écrire une ressource ou une fonction personnalisée pour contourner cette limitation. La plupart des entreprises fournissent des portefeuilles de produits à des unités organisationnelles et non à des comptes individuels, car elles automatisent la génération de comptes et ne souhaitent pas gérer les listes de comptes manuellement.

DevSecOps support de cycle de vie

Actuellement, les produits fournis avec des CloudFormation scripts Service Catalog ne disposent pas d'un support intégré pour les processus CI/CD. Nous vous recommandons de créer un processus CI/CD dansAWS CodePipeline ou d'autres DevOps outils pour développer, tester et publier un produit dans des environnements de cycle de vie tels que le développement, les tests, les étapes et la production.

IlAWS CDK fournit un support CI/CD intégré pour les produits, comme indiqué précédemment dans ce guide.

Réutilisation personnalisée et provisionnement spécifique au compte

Les produits doivent être réutilisables à des fins personnalisées aussi nombreuses que possible. Le Service Catalog favorise la réutilisabilité grâce aux paramètres du produit. Vous pouvez fournir ces paramètres en entrée à un produit au moment de l'approvisionnement.

Vous pouvez également spécifier ces paramètres en tant que valeurs du magasin deAWS Systems Manager paramètres au niveau du CloudFormation modèle, afin d'appliquer des valeurs spécifiques au compte et à l'unité d'organisation. Il s'agit d'une bonne pratique pour la conception CloudFormation de modèles de mise en service. La valeur du paramètre nommé dans le compte cible est appliquée lors du provisionnement du produit. Par exemple, vous pouvez spécifier un paramètre de sous-réseau en tant que valeur du magasin de paramètres et appliquer ce sous-réseau au moment de la mise en service du produit pour un compte UO spécifique. Pour plus d'informations sur les valeurs du magasin de paramètres en tant que paramètres de CloudFormation modèle, consultez la section Utilisation de références dynamiques pour spécifier des valeurs de modèle dans laAWS CloudFormation documentation.

Définition et gestion des ressources des produits du Service Catalog en tant qu'applications

AWS Service Catalog AppRegistryfournit des fonctionnalités centralisées de recherche, de génération de rapports et de gestion des applications. Une AppRegistry application peut inclure une ou plusieurs piles de produits provisionnées ainsi que des CloudFormation piles indépendantes du Service Catalog. Vous pouvez regrouper et afficher toutes vos collections de ressources applicatives

parmi cellesComptes AWS que vous définissez comme cibles de déploiement. Ces comptes peuvent être vos comptes de développement, de test et de cycle de production.

Vous pouvez également l'utiliser AppRegistry pour associer des attributs de métadonnées à une application. Vous pouvez attribuer des groupes d'attributs réutilisables contenant des ensembles d'attributs. Vous pouvez ensuite effectuer des recherches et agir sur les ressources d'applications qui possèdent les attributs donnés à l'aide AppRegistry de services intégrés. Ces services intégrés incluent :

- ory ory ory ory ory ory ory ory ory oryAWS Systems Manager ory ory ory ory ory ory ory ory ory ory ory ory ory ory ory ory oryAWS ory ory ory ory ory ory ory ory ory ory ory ory ory ory ory ory ory ory ory
- AWS Resource Access Manager, pour partager des applications et des groupes d'attributs avec les responsables deAWS l'organisation
- Services AWS qui fonctionnent avec AWS Resource Groups
- AWS Resilience Hubpour la découverte de la structure du produit et l'évaluation de la résilience
- Connecteur AWS Service Managementpour déclarer et configurer des connexions à ServiceNow JIRA et à d'autres outils populaires

Pour de plus amples informations sur AppRegistry, veuillez consulter les ressources suivantes :

- AppRegistry Guide de l'administrateur.
- Améliorez la visibilité et la gouvernance des applications à l'aide d'AWS Service Catalog AppRegistryun article de blog. Cet article fournit une vue d'ensemble de l'utilisation AppRegistry dans la gouvernance de l'infrastructure, avec des exemples de ligne de commande permettant d'enregistrer votre infrastructure en tant qu'applications dans AppRegistry.
- Gérez vos applications de manière centralisée à l'aide AppRegistry d'un article de blog d'Application Manager. Cet article fournit une vue d'ensemble et un didacticiel expliquant comment AppRegistry enregistrer une application Web LAMP sur leAWS Management Console et la gérer à l'aide du Gestionnaire d'applications.

ory ory ory ory ory

Service Catalog possède sa propre fonctionnalité de gestion des stocks interne qui enregistre les produits lorsqu'ils sont approvisionnés via le partage de produits et le libre-service. Nous vous

recommandons toutefois d'utiliser AWS Configou AppRegistrydes services associés pour gérer les ressources fournies par vos produits. Ces outils offrent une approche plus complète et intégrée de la gestion de vos produits Service Catalog provisionnés avec le reste de votreAWS infrastructure. AWS Configvous permet d'inventorier et d'exécuter des actions sur les produits provisionnés sur la console ou à l'aide de l'APIAWS SDK. AppRegistry, intégré à Application Manager, permet également de gérer l'inventaire des produits fournis par Service Catalog.

Utilisation d'AWS Service Catalogoutils

Si vous souhaitez approvisionner vos produits iAC avec des flux de travail de provisionnement personnalisés de manière plus déclarative, vous souhaiterez peut-être augmenter certaines parties des fonctionnalités du Service Catalog. AWSfournit plusieurs outils pour répondre à ces exigences. Deux outils populaires sont fournis dans le projetAWS Labs : Service Catalog Puppet et Service Catalog Factory.

Rubriques

Service Catalog Catalog Catalog Catalog

Service Catalog Puppet est implémenté en Python à l'aide de l'APIAWS Boto3. Cet outil propose plusieurs fonctionnalités puissantes pour configurer et approvisionner les produits Service Catalog. Les développeurs peuvent configurer les informations de mise en service des produits et des portefeuilles du Service Catalog à l'aide de modèles YAML qui servent de manifestes. Les workflows de provisionnement de Service Catalog Puppet prennent en charge les produits qui nécessitent des processus de déploiement plus complexes que ceux de Service Catalog. Ils permettent également d'optimiser les performances afin de fournir des produits à grande échelle dans des délais serrés.

Service Catalog Puppet accède aux CloudFormation modèles du Service Catalog pour le provisionnement des produits au moment du déploiement. Il appelle CloudFormation directement pour déployer la pile de modèles de provisionnement pour un produit et contourne les restrictions imposées par le processus de provisionnement des ensembles de piles de Service Catalog. Si le modèle de provisionnement utilise des macros pour inclure d'autres CloudFormation scripts ou utilise des CloudFormation scripts imbriqués, vous devez fournir l'accès à ces scripts dans le compte cible dans la partie d'amorçage du flux de travail de provisionnement.

Pour plus d'informations, consultez:

- Consultez la documentation et le GitHubréférentiel Service Catalog Puppet.
- Si vous souhaitez utiliser le SDK Service Catalog Puppet pour interagir avec l'outil par programmation afin de lancer le provisionnement des produits et des portefeuilles, consultez la documentation du SDK.

- GitOpsest le mécanisme par défaut pour gérer l'environnement Service Catalog Puppet.

Service Catalog Puppet est assez facile à apprendre pour les développeurs. Il faut être familiarisé avec la mise CloudFormation en œuvre de modèles de provisionnement de produits et avec les modèles YAML pour implémenter des manifestes. De bons ateliers sont disponibles pour familiariser les nouveaux développeurs, tels que des ateliers à rythme libre.

Support des flux de travail de provisionnement

Service Catalog Puppet utilise le moteur d'orchestration de tâches Python Luigi pour implémenter des flux de travail de démarrage et de provisionnement. Toutes les étapes de ces flux de travail sont mises en œuvre en tant que tâches de flux de travail Luigi. Pour un aperçu de Luigi et de sa comparaison avec d'autres outils de flux de travail populaires, consultez Airflow contre Luigi contre Argo contre MLflow vs. KubeFlow sur le blog Data Revenue.

Luigi permet à Service Catalog Puppet de contrôler le nombre de collaborateurs associés aux tâches du flux de travail et de contrôler d'autres aspects des flux de travail, pour une meilleure évolutivité et de meilleures performances. Service Catalog Puppet fournit également un mécanisme dépendant permettant de gérer les dépendances entre les produits et les étapes, et d'orchestrer le provisionnement des produits. Cette fonctionnalité vous permet de mettre en œuvre et de gérer de manière opérationnelle des définitions de produits détaillées et des dépendances complexes.

Modes de provisionnement

Service Catalog Puppet prend en charge trois modes d'exécution : hub, spoke et async. Les trois modes fournissent des produits au sein de portefeuilles déjà définis dans le Service Catalog. Ils s'appuient sur le partage des produits Service Catalog avec les comptes cibles et utilisent les rôles d'administrateur et de lancement de Service Catalog pour réaliser le provisionnement auprès de ces cibles. Service Catalog Puppet exécute les étapes de démarrage au sein de la même organisation en fonction des configurations de rôles fournies dans les fichiers de configuration YAML. L'outil prend également en charge le provisionnement de plusieurs organisations à partir d'un seul compte hub. Dans ce scénario, le démarrage doit être effectué manuellement dans les organisations externes pour permettre à Service Catalog Puppet d'effectuer les actions de provisionnement requises sur les comptes de l'organisation externe.

Dans tous les modes de provisionnement, Service Catalog Puppet met en œuvre le provisionnement des produits directement sans appeler le processus de provisionnement de Service Catalog. Vous

pouvez configurer un manifeste de provisionnement pour utiliser les spécifications du rôle et du compte cible dans une contrainte d'ensemble de pile Service Catalog existante. Service Catalog Puppet utilise ces informations pour effectuer son propre provisionnement avec les flux de travail Luigi.

Vous pouvez définir des cibles pour le provisionnement du portefeuille de produits en fonction d'une approche de balisage des comptes, en plus de spécifier directement des unités d'organisation ou des comptes. Dans le cadre du provisionnement basé sur les balises de compte, un produit de portefeuille est approvisionné pour tous les comptes qui possèdent toutes les balises du jeu de balises de provisionnement du manifeste spécifié. Par exemple, si vous souhaitez proposer un produit de portefeuille à tous les comptes de production institutionnels des régions de l'est des États-Unis, vous pouvez spécifier les balises`type:prod partition:us-east`, et`scope:institutional-client`. Vous pouvez également déclarer des exclusions de comptes et d'unités d'organisation pour interdire le provisionnement vers des unités d'organisation ou des comptes dotés des balises que vous spécifiez, ou vers des comptes membres des cibles spécifiées par l'unité organisationnelle. Pour plus d'informations sur le balisage des comptes, consultez la documentation relative aux outils du Service Catalog.

Mode Hub

En mode de provisionnement du hub, tous les flux de travail Luigi pour les comptes Spoke sont gérés à partir du compte central désigné. Le compte hub assume un rôle IAM qui lui permet d'effectuer des actions dans un compte Spoke, mais la gestion des tâches s'effectue depuis le compte hub. Le compte hub attend de manière synchrone jusqu'à ce que toutes les tâches de provisionnement du compte Spoke soient terminées, avec ou sans succès. Il indique ensuite l'état final. Le mode compte hub est le mode de provisionnement le plus ancien et le plus évolué. Toutefois, de nombreux utilisateurs sont passés au mode de provisionnement en étoile afin d'améliorer la simultanéité et la rapidité du provisionnement.

Mode Spok

En mode Spoke, le compte hub Service Catalog initie les flux de travail Luigi pour qu'ils s'exécutent sur les comptes Spoke bootstrapés désignés. Le compte hub est averti lorsque les flux de travail Spoke sont terminés. Les échecs d'un compte Spoke se répercutent sur le compte hub. Le compte hub interroge le compte Spoke pour voir s'il est terminé et pour déterminer son statut.

Le mode Spoke est le moins susceptible de nécessiter des augmentations deService AWS quota, car presque tout fonctionne sur des comptes Spoke distincts. Le mode Spoke offre également une

simultanéité bien supérieure à celle du mode hub tout en conservant un contrôle centralisé. Il peut améliorer la vitesse de provisionnement de 800 % par rapport au mode hub. Le mode Spoke prend en charge le chaînage des produits par le biais de`DependsOn` relations entre les produits, ce qui garantit qu'un produit dont vous dépendez a déjà été approvisionné. Un produit qui comprend des produits enchaînés peut également fournir un produit chaîné à composants. Vous pouvez également utiliser des appels deAWS Lambda fonctions spécialisés pour effectuer les étapes requises. Les défauts d'un rayon sont isolés des autres rayons.

Le mode Spoke est utilisé par les entreprises qui possèdent plus de 980 comptes dans un maximum de 7 régions. Ces entreprises sont généralement en mesure de fournir un produit à toutes les régions et à tous les comptes de leur infrastructure en une heure.

> **Note**
>
> Ces résultats peuvent varier en fonction de facteurs tels que l'infrastructure réseau, la charge de travail et les quotas en place pour les comptes hub et Spoke deAWS l'organisation. Ils dépendent également des ressources du produit qui sont mises en service, de leurs délais de création inhérents et de leur dépendance à l'égard d'autres ressources.

Mode Async

Le mode asynchrone lance les flux de travail de provisionnement dans les comptes spokes, mais il n'attend ni ne reçoit de réponses d'achèvement de la part des spokes.

Mise en cache

Un autre mécanisme utilisé par Service Catalog Puppet pour optimiser la vitesse des flux de travail consiste à mettre en cache les tâches courantes qui représentent les étapes du flux de travail. Lorsqu'une tâche mise en cache est terminée, elle écrit sa sortie sur Amazon Simple Storage Service (Amazon S3). La prochaine fois que la tâche est appelée dans la même session avec les mêmes paramètres, Service Catalog Puppet utilise les valeurs mises en cache au lieu de réexécuter la tâche. Pour plus d'informations, consultez Service Catalog Puppet.

DevSecOps support du cycle de vie

Service Catalog Puppet inclut un support pour la gestion du DevSecOps pipeline. Vous pouvez utiliser les actions des outils Service Catalog (comme illustré dans la présentation de Service Catalog

Puppet) pour automatiser les tests et promouvoir les produits sur l'ensemble de vos comptes deAWS cycle de vie, y compris le compte Canary recommandé. Pour plus d'informations, consultez la section Gestion de vos environnements dans la documentation de Service Catalog Puppet.

Pour s'assurer que tout problème lié à une modification du produit est détecté avant une utilisation généralisée en production, Service Catalog Puppet nécessite au moins un compte Canary pour le déploiement initial. Une fois que vous aurez testé la nouvelle version et que vous aurez acquis confiance en elle, vous pourrez la promouvoir sur des comptes de production autres que Canary. Si vous identifiez des problèmes, vous pouvez annuler la version et la réintroduire une fois les problèmes résolus. Lorsque vous utilisez cette approche, des problèmes de production peuvent survenir si vous publiez une version Canary qui présente un problème avec les comptes de production. Comme autre approche, vous pouvez exécuter des tests de régression complets pour chaque modification de produit avant de lancer la modification en production. Cela entraîne une surcharge supplémentaire dans le processus CI/CD, mais permet d'éviter les problèmes de production. Il est de la responsabilité de l' DevSecOps administrateur de déterminer les meilleurs scénarios et approches de sortie de fonctionnalités pour ses équipes de développement.

Service Catalog Puppet permet à plusieurs équipes de développer et de tester simultanément le provisionnement de solutions de produits Service Catalog. En tant que bonne pratique, un produit ne doit pas être modifié par plusieurs développeurs en même temps. Au lieu de cela, vous pouvez diviser les produits en composants plus fins pour des modifications distinctes et simultanées.

Service Catalog Puppet permet également d'automatiser les tests grâce à une déclaration d'assertion qui fournit des fonctionnalités de test statique et unitaire. Vous pouvez tester des stratégies de contrôle des services (SCP) et plusieurs. Il s'agit de end-to-end tests techniques, mais ils peuvent être utilisés dans des environnements de test d'intégration système (SIT). Pour plus d'informations, consultez les sections Utilisation de simulations de politiques et Application de politiques de contrôle des services dans la documentation Service Catalog Puppet.

Maturité, exhaustivité et support

Bien que Service Catalog Puppet ne soit pas officiellement pris en chargeService AWS, il a été largement adopté. Cet outil a été utilisé par de grandes entreprises au cours des dernières années pour approvisionner avec succès et de manière centralisée des produits à des centaines de comptes OU dans les délais de provisionnement souhaités. Elle s'est révélée capable de fournir des produits tolérants aux pannes à grande échelle. Les utilisateurs qui rencontrent des problèmes avec Service Catalog Puppet peuvent les enregistrer dans le GitHub référentiel afin que les contributeurs à cette solutionAWS Labs les résolvent.

Service Catalog Service Service Service Service

Service Catalog Factory est un autre outil fourni parAWS Labs. Il est similaire àAWS Control Tower : il génère des comptes et appelle Service Catalog (potentiellement via Puppet) pour provisionner iAP au sein de ces comptes. Il utilise bon nombre des mêmes mécanismes que Service Catalog Puppet pour implémenter ses fonctionnalités. Service Catalog Factory peut appeler Service Catalog ou Service Catalog Puppet pour configurer l'infrastructure des produits d'un compte. Cet outil prend également en charge la génération de comptes dans plusieursRégions AWS organisations. Pour plus d'informations, consultez la documentation et le GitHub référentiel de Service Catalog Factory.

Étapes suivantes :

Le Service Catalog vous permet de provisionner rapidement et de manière fiable votre infrastructure en tant que produit. Vous pouvez utiliser une infrastructure en libre-service à partir d'un catalogue de produits défini ou transférer des produits vers des comptes cibles désignés dans un hub-and-spoke modèle. Vous pouvez définir les produits Service Catalog et leurs modèles de provisionnement à l'aide de CloudFormation scripts ou duAWS CDK. Dans les deux approches, Service Catalog provisionne un produit en appelant CloudFormation pour déployer une pile qui représente le modèle de provisionnement du produit. La pile est déployée sur tous les comptes cibles désignés au sein d'un ensemble de CloudFormation piles.

L'AWS CDKapproche de développement du Service Catalog permet une modularisation et une réutilisation plus CloudFormation poussées que celle-ci, car vous pouvez définir les produits et leurs ressources en utilisant des classes de produits et de portefeuilles prédéfinies ainsi que des types de ressources prédéfinis. UneAWS CDK implémentation nécessite des compétences de programmation plus avancées. Cela peut se justifier si votre organisation souhaite établir sa propre structure de produits réutilisables avec des configurations de ressources et des comportements standardisés comme base pour le développement de votreAWS infrastructure.

Vous pouvez utiliser Service Catalog Puppet et Service Catalog Factory pour améliorer les fonctionnalités de Service Catalog, principalement pour le provisionnement. Service Catalog Puppet propose des spécifications de provisionnement de produits déclaratives et basées sur des balises, des flux de travail de provisionnement intégrés, personnalisables, performants et spécialisés, ainsi que des pipelines CI/CD et SDLC intégrés, personnalisables et basés sur l'action. En utilisant la gestion des dépendances du flux de travail et les fonctionnalités intégrées d'automatisation des tests, vous pouvez enchaîner les produits Service Catalog avec moins de risques opérationnels. Service Catalog Puppet vous permet de fournir des produits à des centaines de comptes dans des délais serrés de manière fiable. Service Catalog Factory est similaire àAWS Control Tower. Il génère des comptes et appelle Service Catalog pour approvisionner iAP au sein de ces comptes.

Les outils de Service Catalog et de Service Catalog fournissent des fonctionnalités étendues pour vous aider à gérer iAP onAWS. Le Service Catalog et ces outils font l'objet d'améliorations constantes. Pour les dernières fonctionnalités, consultez les AWS Service Catalogfonctionnalités et le référentielAWS Service Catalog des produits.

Ressources

Références

- Documentation du Service Catalog
- API du Service Catalog
- AppRegistry
- Documentation AWS CloudFormation
- AWS CloudFormationensembles empilables
- AWS::ServiceCatalog::CloudFormationRessource sur le produit
- LancezAWS Service Catalog des produits avec Terraform
- AWS Cloud Development Kit (AWS CDK)
- Bibliothèque de construction du Service Catalog
- AWS CDK ProductStackclasse
- Documentation AWS Organizations

Outils

- Documentation sur les marionnettes du Service Catalog
- GitHubRéférentiel Service Catalog Puppet
- Documentation d'usine du Service Catalog
- GitHubRéférentiel Service Catalog Factory

AWSModèles d'orientation prescriptive

- GérezAWS Service Catalog les produits de manière multipleComptes AWS etRégions AWS
- CopiezAWS Service Catalog des produits sur différentsComptes AWS etRégions AWS
- Automatisez le déploiement duAWS Service Catalog portefeuille et des produits en utilisantAWS CDK

Historique du document

Le tableau suivant décrit les modifications importantes apportées à ce guide. Si vous souhaitez être informé des future mises à jour, vous pouvez vous abonner à un fil RSS.

Modification	Description	Date
Publication initiale	—	30 janvier 2023

AWS Glossaire des directives prescriptives

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

Nombres

7 R

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

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

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

A

ABAC

Voir contrôle d'accès basé sur les attributs.

services abstraits

Consultez la section Services gérés.

ACIDE

Voir atomicité, consistance, isolation, durabilité.

migration active-active

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

migration active-passive

Méthode de migration de base de données dans laquelle 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 solution 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 la façon dont les AIOps sont utilisées dans la stratégie de migration AWS , veuillez consulter 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, connus sous le nom de mauvais robots, 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.

CCoE

Voir le Centre d'excellence du cloud.

CDC

Consultez la section 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 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 articles du CCoE sur le blog de 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 mettre à l'échelle l'adoption du cloud (par exemple, en créant une zone de destination, en définissant un CCoE ou en établissant 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 ou AWS CodeCommit. 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, AWS

Panorama propose des appareils qui ajoutent des CV aux réseaux de caméras locaux, et Amazon SageMaker 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 source, de génération, de test, intermédiaire et de production du processus de publication du logiciel. CI/CD est communément décrit comme un pipeline. CI/CD peut vous aider à automatiser les processus, à améliorer la productivité, à améliorer la qualité du code et à accélérer les livraisons. Pour plus d'informations, veuillez consulter Avantages de la livraison continue. CD peut également signifier déploiement continu. Pour plus d'informations, veuillez consulter Livraison continue et déploiement continu.

CV

Voir vision par ordinateur.

D

données au repos

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

classification des données

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

dérive des données

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

données en transit

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

maillage de données

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

minimisation des données

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

périmètre de données

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

prétraitement des données

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

provenance des données

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

sujet des données

Personne dont les données sont collectées et traitées.

entrepôt des données

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

langage de définition de base de données (DDL)

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

langage de manipulation de base de données (DML)

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

DDL

Voir langage de définition de base de données.

ensemble profond

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

deep learning

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

defense-in-depth

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

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

administrateur délégué

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

déploiement

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

environnement de développement

Voir environnement.

contrôle de détection

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

cartographie de la chaîne de valeur du développement (DVSM)

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

jumeau numérique

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

tableau des dimensions

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

catastrophe

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

reprise après sinistre (DR)

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

DML

Voir langage de manipulation de base de données.

conception axée sur le domaine

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

DR

Consultez la section Reprise après sinistre.

détection de dérive

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

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

DVSM

Voir la cartographie de la chaîne de valeur du développement.

E

EDA

Voir analyse exploratoire des données.

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.

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 principaux Comptes AWS ou à AWS Identity and Access Management (IAM) principaux. Ces comptes ou principaux peuvent se connecter à votre

service de point de terminaison de manière privée en créant des points de terminaison d'un VPC d'interface. Pour plus d'informations, veuillez consulter Création d'un service de point de terminaison dans la documentation Amazon Virtual Private Cloud (Amazon VPC).

planification des ressources d'entreprise (ERP)

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

chiffrement d'enveloppe

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

environment

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

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

épopée

Dans les méthodologies agiles, catégories fonctionnelles qui aident à organiser et à prioriser votre travail. Les épopées fournissent une description détaillée des exigences et des tâches d'implémentation. Par exemple, les points forts de la AWS CAF en matière de sécurité incluent la gestion des identités et des accès, les contrôles de détection, la sécurité des infrastructures,

la protection des données et la réponse aux incidents. Pour plus d'informations sur les épopées dans la stratégie de migration AWS , veuillez consulter le guide d'implémentation du programme.

ERP

Voir Planification des ressources d'entreprise.

analyse exploratoire des données (EDA)

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

F

tableau des faits

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

échouer rapidement

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

limite d'isolation des défauts

Dans le AWS Cloud, une limite telle qu'une zone de disponibilité Région AWS, un plan de contrôle ou un plan de données qui limite l'effet d'une panne et contribue à améliorer la résilience des charges de travail. Pour plus d'informations, consultez la section Limites d'isolation des AWS pannes.

branche de fonctionnalités

Voir la 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.

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 via 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.

G

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.

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 d'organisation (UO). 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 de l'historien

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.

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.

IIoT

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 de référence de sécuritéAWS recommande de configurer votre compte réseau avec des VPC entrants, sortants et d'inspection afin de protéger l'interface bidirectionnelle entre votre application et 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, veuillez consulter Building an industrial Internet of Things (IIoT) digital transformation strategy.

VPC d'inspection

Dans une architecture AWS multi-comptes, un VPC centralisé qui gère les inspections du trafic réseau entre les VPC (identiques ou Régions AWS différents), Internet et les réseaux sur site. L'architecture de référence de sécuritéAWS recommande de configurer votre compte réseau avec des VPC entrants, sortants et d'inspection afin de protéger l'interface bidirectionnelle entre votre application et 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, veuillez consulter Machine learning model interpretability with 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

Consultez la section 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.

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.

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

système d'exécution de la fabrication (MES)

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

MAP

Voir Migration Acceleration Program.

mécanisme

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

compte membre

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

MAILLES

Voir le système d'exécution de la fabrication.

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

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

microservice

Petit service indépendant qui communique via des API bien définies 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 à l'aide d'API légères. Chaque microservice de cette architecture peut être mis à jour, déployé et mis à l'échelle pour répondre à la demande de fonctions spécifiques d'une application. Pour plus d'informations, consultez la section Implémentation de microservices sur AWS.

Programme d'accélération des migrations (MAP)

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

migration à grande échelle

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

usine de migration

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

métadonnées de migration

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

modèle de migration

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

Évaluation du portefeuille de migration (MPA)

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

Évaluation de la préparation à la migration (MRA)

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

stratégie de migration

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

ML

Voir apprentissage automatique.

modernisation

Transformation d'une application obsolète (héritée ou monolithique) et de son infrastructure en un système agile, élastique et hautement disponible dans le cloud afin de réduire les coûts, de

gagner en efficacité et de tirer parti des innovations. Pour plus d'informations, consultez la section Stratégie de modernisation des applications dans le AWS Cloud.

évaluation de la préparation à la modernisation

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

applications monolithiques (monolithes)

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

MPA

Voir Évaluation du portefeuille de migration.

MQTT

Voir Message Queuing Telemetry Transport.

classification multi-classes

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

infrastructure mutable

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

O

OAC

Voir Contrôle d'accès à l'origine.

OAI

Voir l'identité d'accès à l'origine.

OCM

Voir gestion du changement organisationnel.

migration hors ligne

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

OI

Consultez la section Intégration des opérations.

OLA

Voir l'accord au niveau opérationnel.

migration en ligne

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

OPC-UA

Voir Open Process Communications - Architecture unifiée.

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

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

accord au niveau opérationnel (OLA)

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

examen de l'état de préparation opérationnelle (ORR)

Une liste de questions et de bonnes pratiques associées qui vous aident à comprendre, 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.

OU

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 de référence de sécuritéAWS recommande de configurer votre compte réseau avec des VPC entrants, sortants et d'inspection afin de protéger l'interface bidirectionnelle entre votre application et 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 AWS capable d'effectuer des actions et d'accéder aux ressources. Cette entité est généralement un utilisateur root pour un Compte AWS rôle IAM ou un utilisateur. Pour plus d'informations, veuillez consulter la rubrique Principal dans Termes et concepts relatifs aux rôles, dans la documentation IAM.

Confidentialité dès la conception

Une approche de l'ingénierie des systèmes qui prend en compte la confidentialité tout au long du processus d'ingénierie.

zones hébergées privées

Conteneur qui contient des informations concernant la façon dont vous souhaitez qu'Amazon Route 53 réponde aux requêtes DNS pour un domaine et ses sous-domaines dans un ou plusieurs VPC. 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.

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.

publier/souscrire (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).

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. Cela permet de déterminer ce qui est considéré comme une perte de données acceptable entre le dernier point de restauration 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. Chacune Région AWS est isolée et indépendante des autres pour garantir tolérance aux pannes, stabilité et résilience. Pour plus d'informations, voir Spécifier ce que Régions AWS votre compte peut utiliser.

régression

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

réhéberger

Voir 7 Rs.

version

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

déplacer

Voir 7 Rs.

replateforme

Voir 7 Rs.

rachat

Voir 7 Rs.

résilience

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

politique basée sur les ressources

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

matrice responsable, redevable, consulté et informé (RACI)

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

contrôle réactif

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

retain

Voir 7 Rs.

se retirer

Voir 7 Rs.

rotation

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

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

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

RPO

Voir l'objectif du point de récupération.

RTO

Voir l'objectif en matière de temps de rétablissement.

runbook

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

S

SAML 2.0

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

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 instance Amazon EC2 ou la rotation des informations d'identification.

chiffrement côté serveur

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

Politique de contrôle des services (SCP)

Politique qui propose un contrôle centralisé des autorisations pour tous les comptes d'une organisation dans AWS Organizations. Les SCP définissent des barrières de protection ou des limites aux actions qu'un administrateur peut déléguer à des utilisateurs ou à des rôles. Vous pouvez utiliser les SCP comme listes d'autorisation ou de refus, pour indiquer 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.

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

Hub de transit de réseau que vous pouvez utiliser pour relier vos VPC et vos réseaux 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

Connexion entre deux VPC qui vous permet d'acheminer le trafic à l'aide d'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

Consultez le cadre de qualification des charges de travail AWS.

écrire une fois, lire plusieurs (WORM)

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

Z

exploit Zero-Day

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

vulnérabilité de type « jour zéro »

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

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.