Guide de sécurité et d'exploitation d'Autonomous Driving Data Framework (ADDF)

AWS Directives prescriptives

AWS Directives prescriptives: Guide de sécurité et d'exploitation d'Autonomous Driving Data Framework (ADDF)

Table of Contents

Guide de sécurité et d'exploitation d'Autonomous Driving Data Framework (ADDF)

Andreas Falkenberg, Junjie Tang, Torsten Reitemeyer et Srinivas Reddy Cheruku, Amazon Web Services (AWS)

Novembre 2022 (historique du document)

Autonomous Driving Data Framework (ADDF) est un projet open source conçu pour fournir des artefacts de code réutilisables et modulaires aux équipes automobiles qui souhaitent implémenter des tâches courantes pour les systèmes avancés d'assistance au conducteur (ADAS), telles que la configuration du stockage de données centralisé, des pipelines de traitement des données, des mécanismes de visualisation, des interfaces de recherche, des charges de travail de simulation, des interfaces d'analytique et des tableaux de bord prédéfinis. Avec ADDF, vous pouvez partager, modifier ou créer des modules entièrement personnalisables qui réduisent les efforts nécessaires à la création et au déploiement de ces solutions.

Ce guide a pour but de vous aider à comprendre les bonnes pratiques en matière de déploiement et d'exploitation sécurisés d'ADDF dans le AWS Cloud. Il aborde les sujets suivants :

- Architecture et terminologie : examinez l'architecture générale, les flux de travail et les termes importants.
- Modèle de responsabilité partagée : comprenez votre rôle et celui d'AWS pour sécuriser votre déploiement ADDF et vos ressources cloud.
- Processus de révision de la sécurité : le projet ADDF étant un projet open source disponible, découvrez comment AWS et les contributeurs effectuent des examens de sécurité.
- Fonctionnalités de sécurité intégrées : découvrez comment les bonnes pratiques et fonctionnalités de sécurité sont intégrées au projet open source ADDF et à son cadre de déploiement.
- Configuration et fonctionnement sécurisés : apprenez à déployer et à utiliser ADDF dans le AWS Cloud.

Public visé

Ce guide est destiné aux équipes des opérations de développement (DevOps), aux ingénieurs d'infrastructure, aux administrateurs, au personnel de sécurité informatique et aux équipes de

réponse aux incidents chargés d'évaluer, de déployer, de personnaliser et d'exploiter ADDF. Vous pouvez appliquer les recommandations de ce guide pour les environnements de preuve de concept ou de production.

Ce guide suppose que vous n'avez aucune connaissance préalable d'ADDF. Nous vous recommandons toutefois de lire le fichier readme ADDF (GitHub) avant de continuer.

Résultats commerciaux ciblés

Ce guide est conçu pour vous aider à configurer et à utiliser ADDF en toute confiance et en toute sécurité dans des environnements de développement et de production.

Architecture et terminologie ADDF

Avant de pouvoir comprendre les sujets liés à la sécurité et aux opérations abordés dans ce guide, il est important d'avoir une excellente connaissance de la terminologie, des composants et de l'architecture Autonomous Driving Data Framework (ADDF). Cette section se compose des rubriques suivantes :

Terminologie ADDF

La terminologie clé ADDF est la suivante :

- Module ADDF : un module est une infrastructure en tant que code (IaC) qui implémente une tâche commune dans un système avancé d'assistance au pilote (ADAS, Advanced Driver-Assistance System). Les tâches courantes incluent la configuration du stockage centralisé des données, des pipelines de traitement des données, des mécanismes de visualisation, des interfaces de recherche, des charges de travail de simulation, des interfaces d'analytique et des tableaux de bord prédéfinis. Vous pouvez créer un module en fonction de vos besoins, ou vous pouvez réutiliser ou personnaliser un module existant.

  Vous pouvez utiliser l'AWS Cloud Development Kit (AWS CDK) pour définir des modules ADDF, ou vous pouvez utiliser n'importe quel cadre IaC courant, tel que Hashicorp Terraform ou AWS CloudFormation, pour implémenter les modules ADDF. Un module possède un ensemble de paramètres d'entrée. Les paramètres d'entrée peuvent dépendre des valeurs de sortie des autres modules. Un module ADDF est la plus petite unité de déploiement pour un Compte AWS cible ADDF.
- Fichier manifeste de déploiement ADDF : ce fichier définit une orchestration de modules ADDF autonomes. L'orchestration fait référence à l'ordre de déploiement des modules. Dans le fichier manifeste de déploiement ADDF, vous pouvez utiliser des groupes ADDF pour regrouper les modules associés. Dans ce fichier, vous définissez également l'Compte AWS de chaîne d'outils ADDF, les Comptes AWS de destination ADDF et les Régions AWS de destination.
- Cadre de déploiement ADDF : ce cadre déploie des modules ADDF dans des Comptes AWS de destination ADDF en fonction de l'orchestration définie dans le fichier manifeste de déploiement

ADDF. Le cadre de déploiement ADDF est mis en œuvre à l'aide des projets open source AWS suivants :

- SeedFarmer (GitHub) : SeedFarmer est l'outil de CLI utilisé pour les déploiements ADDF. Il gère l'état de chaque module, prépare et met en package le code du module, crée les stratégies de moindre privilège pour les rôles de déploiement ADDF et fournit des instructions sémantiques que CodeSeeder utilise pour le déploiement. Vous pouvez interagir directement avec SeedFarmer pour exécuter des déploiements ADDF, ou vous pouvez l'intégrer dans un pipeline d'intégration continue et de déploiement continu (CI/CD).
- CodeSeeder (GitHub) : CodeSeeder déploie une infrastructure arbitraire sous forme de packages de code via une tâche AWS CodeBuild. SeedFarmer orchestre et exécute automatiquement CodeSeeder. Seul SeedFarmer interagit directement avec CodeSeeder.

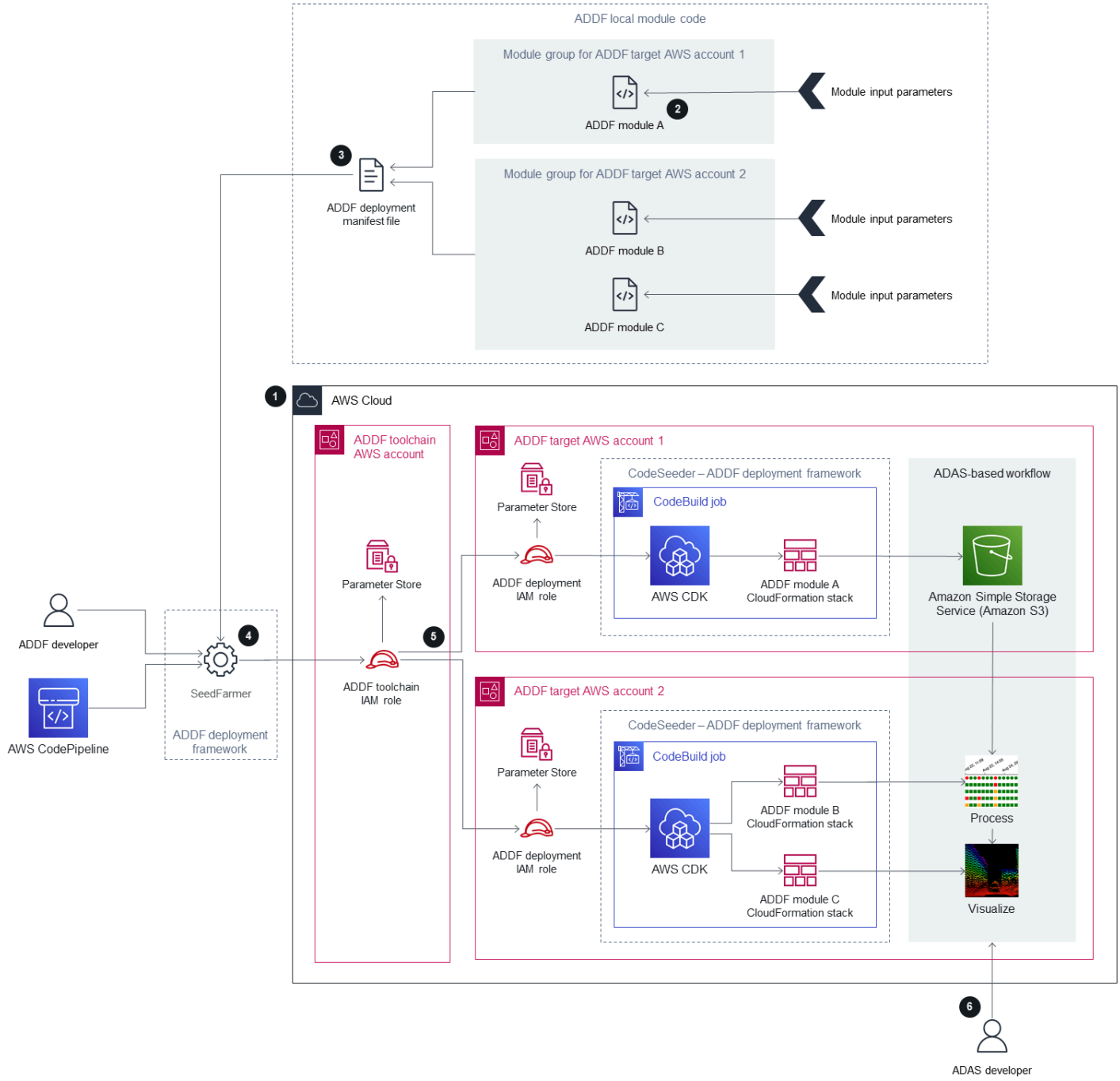
Le cadre de déploiement ADDF est conçu pour prendre en charge les déploiements dans des architectures à compte unique et à comptes multiples. En fonction des besoins de votre organisation, vous décidez si une architecture à compte unique ou à comptes multiples est requise.

- Compte AWS de chaîne d'outils ADDF : ce compte orchestre et gère le déploiement des modules dans les Comptes AWS de destination ADDF, sur la base des définitions contenues dans le fichier manifeste de déploiement ADDF. Un déploiement ADDF ne peut avoir qu'un seul Compte AWS de chaîne d'outils ADDF. Dans une architecture à compte unique, le Compte AWS de chaîne d'outils ADDF est également le Compte AWS de destination ADDF. Ce compte contient un rôle AWS Identity and Access Management (IAM), appelé rôle IAM de chaîne d'outils ADDF, qui est endossé par SeedFarmer lors du processus de déploiement ADDF. Dans ce guide, nous faisons référence à un Compte AWS de chaîne d'outils ADDF en tant que compte de chaîne d'outils.
- Comptes AWS de destination ADDF : il s'agit des comptes de destination sur lesquels vous déployez des modules ADDF. Vous pouvez avoir un ou plusieurs comptes de destination. Ces comptes contiennent les ressources et la logique d'application décrites dans le fichier manifeste de déploiement ADDF et ses modules mappés. Dans une architecture à compte unique, le Compte AWS de destination ADDF est également le Compte AWS de chaîne d'outils ADDF. Chaque compte cible ADDF contient un rôle IAM, appelé rôle IAM de déploiement ADDF, qui est endossé par CodeSeeder pendant le processus de déploiement. Dans ce guide, nous faisons référence à un Compte AWS de destination ADDF en tant que compte de destination.
- Instance ADDF : lorsque vous déployez ADDF et vos modules dans le cloud, tel que défini dans votre fichier manifeste de déploiement ADDF, cela devient une instance ADDF. Une instance ADDF peut avoir une architecture à compte unique ou à comptes multiples, et vous pouvez déployer plusieurs instances ADDF. Pour plus d'informations sur le choix du nombre d'instances

et la conception d'une architecture de compte adaptée à votre cas d'utilisation, veuillez consulter Définition de votre architecture ADDF.

Architecture ADDF

Le schéma suivant présente l'architecture de haut niveau d'une instance ADDF dans le AWS Cloud. Il présente une architecture à comptes multiples, comprenant un compte de chaîne d'outils dédié et deux comptes de destination. Ce guide décrit le processus de bout en bout d'utilisation d'ADDF pour déployer des ressources sur les comptes de destination.



1. Créez et amorcez les Comptes AWS ADDF.

   Pour fonctionner correctement, chaque compte doit être amorcé à ADDF et à AWS CDK. S'il s'agit d'un nouveau déploiement ADDF ou si vous ajoutez de nouveaux comptes de destination, procédez comme suit :

a. Amorcez AWS CDK dans le compte de chaîne d'outils et dans chaque compte de destination. Pour les instructions, veuillez consulter Bootstrapping (documentation AWS CDK). ADDF utilise AWS CDK pour déployer son infrastructure.

b. Amorcez ADDF dans le compte de chaîne d'outils et dans chaque compte de destination. Pour les instructions, veuillez consulter la rubrique Amorcer un ou plusieurs Compte AWS dans le Guide de déploiement ADDF. Cela permet de configurer tous les rôles IAM propres à ADDF requis par SeedFarmer et CodeSeeder.

> **Note**
>
> Vous devez effectuer cette étape uniquement si vous déployez initialement ADDF ou si vous ajoutez de nouveaux comptes de destination. Cette étape ne fait pas partie des déploiements ADDF récurrents vers des instances ADDF déjà établies.

2. Créez ou personnalisez les modules ADDF.

   Créez ou personnalisez des modules ADDF en fonction du problème spécifique que vous essayez de résoudre. Votre module doit représenter une tâche isolée ou un groupe de tâches isolé. Définissez les paramètres d'entrée du module selon les besoins et utilisez les valeurs de sortie du module comme paramètres d'entrée pour d'autres modules.

3. Définissez l'orchestration du module dans le fichier manifeste de déploiement ADDF.

   Dans le fichier manifeste ADDF, organisez les modules en groupes et définissez l'ordre de déploiement et les dépendances entre eux. Dans ce fichier, vous spécifiez également le compte de chaîne d'outils unique et les comptes de destination (y compris Régions AWS) pour chaque groupe ADDF et ses modules.

4. Évaluez le fichier manifeste de déploiement ADDF et déterminez la portée du déploiement.

   Le développeur ADDF ou un pipeline CI/CD, tel qu'AWS CodePipeline, démarre une évaluation du fichier manifeste de déploiement ADDF en appelant l'outil de CLI, SeedFarmer. Pour démarrer l'évaluation :

   - SeedFarmer utilise le fichier manifeste de déploiement ADDF comme paramètre d'entrée pour l'évaluation.
   - Pour endosser le rôle IAM de la chaîne d'outils ADDF, SeedFarmer attend le même rôle IAM ou les mêmes informations d'identification utilisateur valides que ceux définis lors du processus d'amorçage ADDF, à l'étape 1.

Si SeedFarmer ne dispose pas des informations d'identification correctes pour endosser le rôle IAM de la chaîne d'outils ADDF ou ne peut pas accéder au fichier manifeste de déploiement ADDF, l'évaluation ne démarre pas.

Si SeedFarmer peut démarrer l'évaluation, il endosse le rôle IAM de la chaîne d'outils ADDF dans le compte de chaîne d'outils. À partir de là, SeedFarmer peut accéder à n'importe quel compte de destination, en endossant le rôle IAM de déploiement ADDF dans ce compte. SeedFarmer essaie ensuite de lire toutes les métadonnées ADDF dans le compte de chaîne d'outils et les comptes de destination. L'une des situations suivantes se produit :

- S'il n'y a aucune métadonnée ADDF à lire, cela indique qu'il s'agit d'une nouvelle instance ADDF. SeedFarmer détermine que la portée du déploiement est l'intégralité du fichier manifeste de déploiement ADDF et de son contenu.
- Si des métadonnées ADDF existent, SeedFarmer compare le fichier manifeste de déploiement ADDF et son contenu aux hachages MD5 des artefacts déployés existants dans les comptes de destination. Si des modifications déployables sont détectées, ce processus se poursuit. Si aucune modification déployable n'est détectée, le processus est terminé.

5. Déployez les modules ADDF concernés sur les comptes de destination.

   CodeSeeder dispose désormais d'une liste ordonnée des déploiements à exécuter, en fonction du fichier manifeste de déploiement ADDF et des résultats de l'évaluation de l'étape précédente. Sur la base de cette liste ordonnée, CodeSeeder endosse le rôle IAM de déploiement ADDF dans chaque compte de destination associé. Il exécute ensuite CodeSeeder dans une tâche AWS CodeBuild pour créer ou mettre à jour les déploiements IaC individuels, tels que des applications AWS CDK, pour le module ADDF. Par défaut, ADDF utilise AWS CDK comme cadre IaC, mais d'autres cadres IaC courants sont également pris en charge. Une fois le processus terminé pour chaque compte de destination, vous disposez d'un flux de travail basé sur ADAS de bout en bout, entre comptes et entièrement déployé, tel que défini dans le fichier manifeste de déploiement ADDF.

   Si vous utilisez une architecture à compte unique, le compte de chaîne d'outils et les comptes de destination sont le même compte, et le seul qui possède toutes les fonctionnalités décrites.

6. Utilisez l'infrastructure déployée par ADDF.

   Un développeur ADAS peut utiliser le flux de travail basé sur ADAS déployé, tel que défini par votre cas d'utilisation.

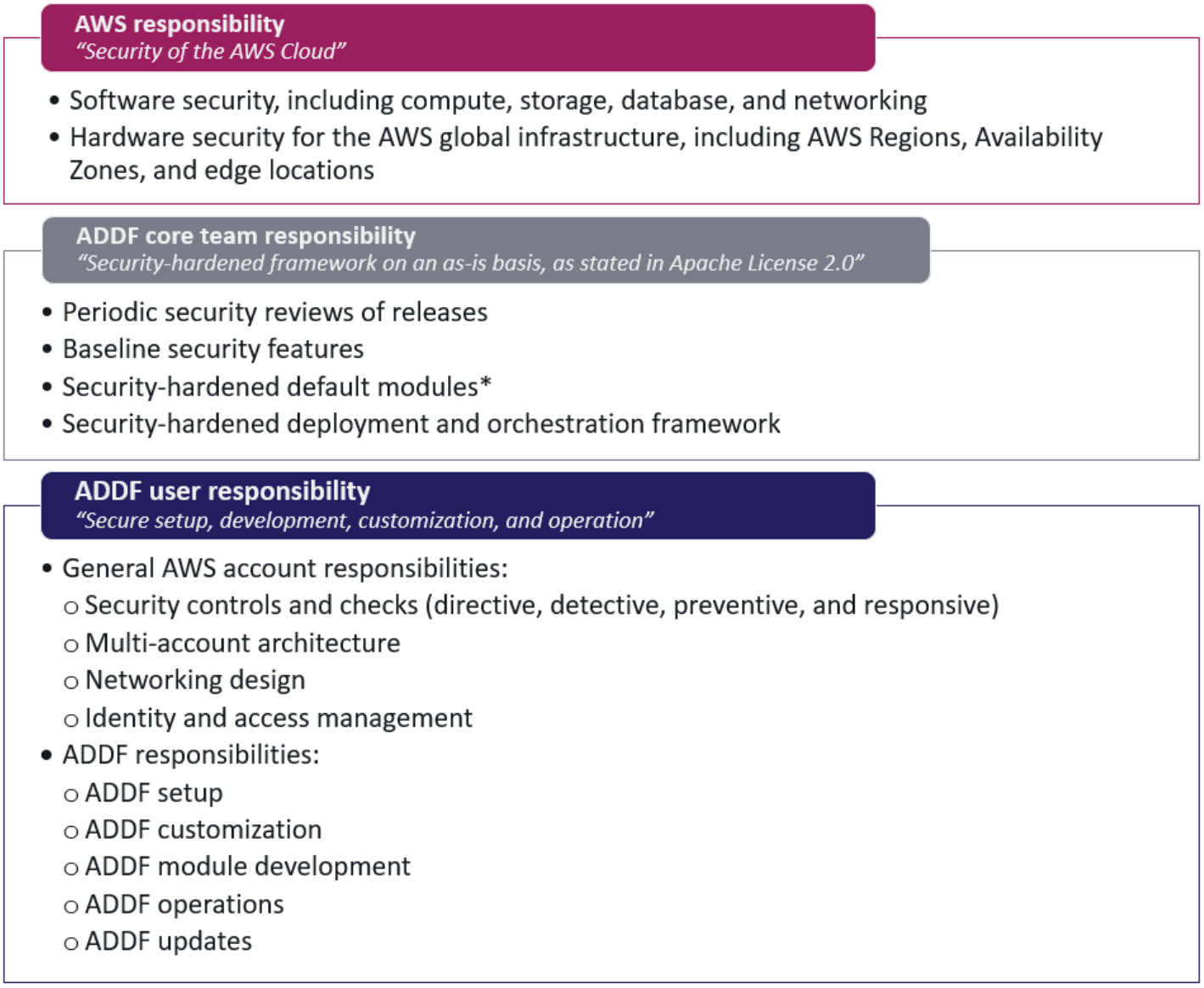
Ce flux de travail décrit l'architecture d'une instance unique d'un environnement à comptes multiples ADDF. En fonction de votre modèle de développement, de déploiement et d'opérations, nous vous recommandons d'exécuter plusieurs instances ADDF dans un environnement à plusieurs étapes. Une configuration typique peut inclure une instance ADDF dédiée avec des Comptes AWS dédiés pour chaque étape de déploiement, comme des branches pour le développement, les tests et la production. Vous pouvez également exécuter plusieurs instances ADDF dans le même environnement à compte unique ou à comptes multiples de la même Région AWS, en supposant que vous ayez créé un espace de noms de ressource unique pour chaque instance ADDF. Pour de plus amples informations, veuillez consulter Définition de votre architecture ADDF.

Modèle de responsabilité partagée ADDF

Le modèle de responsabilité partagée qui s'applique aux Services AWS s'applique également à Autonomous Driving Data Framework (ADDF). Les entités suivantes partagent la responsabilité de sécuriser ADDF, comme indiqué dans le schéma suivant :

- AWS : le fournisseur d'infrastructure cloud proposant des Services AWS.
- Équipe principale ADDF : l'équipe principale ADDF est l'entité qui publie les versions d'ADDF dans le référentiel ADDF (GitHub).
- Utilisateur ADDF : les utilisateurs ADDF incluent, sans toutefois s'y limiter, les personnes suivantes :
  - Développeur ADDF : toute personne qui modifie, personnalise ou crée un code de module ADDF.
  - Opérateur ADDF : toute personne qui configure et gère une instance ADDF.
  - Développeur ADAS : l'utilisateur final ou le consommateur des ressources déployées par ADDF. Par exemple, un développeur ADAS peut interroger une interface de visualisation créée dans le cadre du déploiement d'ADDF.

Le schéma suivant résume la responsabilité partagée entre AWS, l'équipe principale ADDF et l'utilisateur d'ADDF.



* Excluding any modules in the ADDF **/modules/demo-only/** folder. Those modules exist only for proof-of-concept purposes and didn't receive security hardening.

Responsabilité d'AWS

AWS est responsable de la protection de l'infrastructure qui exécute tous les services proposés dans le AWS Cloud, tel que défini dans le modèle de responsabilité partagée AWS. Cette infrastructure est composée du matériel, des logiciels, du réseau et des installations exécutant les services AWS Cloud.

Responsabilité de l'équipe principale ADDF

L'équipe principale ADDF fournit un cadre sécurisé en lui-même, dans la mesure du possible, selon Licence Apache 2.0 (GitHub). L'équipe principale ADDF est responsable de ce qui suit :

- Examens de sécurité périodiques des versions
- Fonctionnalités de sécurité de base
- Modules par défaut renforcés en termes de sécurité (cela exclut tous les modules du dossier `/modules/demo-only/`. Ces modules sont uniquement destinés à des fins de preuve de concept et ne font pas l'objet d'un renforcement de la sécurité.)
- Cadre de déploiement et d'orchestration renforcé en termes de sécurité

Ces responsabilités en matière de sécurité s'étendent uniquement au cadre, tel que fourni dans le référentiel GitHub, sans aucune modification ni personnalisation. Cela inclut tous les modules ADDF, à l'exception des modules ADDF du dossier `modules/demo-only/`. Les modules ADDF dans ce dossier ne sont pas sécurisés et ne doivent pas être déployés dans des environnements de production ou dans un environnement contenant des données sensibles ou protégées. Ces modules sont inclus pour mettre en valeur les capacités du système, et vous pouvez les utiliser comme base pour créer vos propres modules personnalisés et sécurisés.

> **Note**
>
> ADDF en tant que cadre est fourni tel quel. Il n'est assorti d'aucune responsabilité ni garantie, comme indiqué dans la Licence Apache 2.0 (GitHub). Vous devez effectuer votre propre évaluation de la sécurité d'ADDF et vérifier qu'elle est conforme aux exigences de sécurité spécifiques de votre organisation.

Responsabilité de l'utilisateur ADDF

ADDF et ses modules ne sont sécurisés que si ADDF est configuré, personnalisé et exploité de manière sécurisée. L'utilisateur ADDF est entièrement responsable de la sécurité des éléments suivants :

- Responsabilités d'Compte AWS générales :
  - Contrôles et vérifications de sécurité (directifs, de détections, préventifs et réactifs)

  - Architecture à comptes multiples
  - Conception de réseaux
  - Gestion des identités et des accès
- Responsabilités propres à ADDF :
  - Configuration d'ADDF
  - Personnalisation d'ADDF
  - Développement de modules ADDF
  - Opérations ADDF
  - Mises à jour d'ADDF

Responsabilités d'Compte AWS générales

Avant de déployer des ressources liées à ADDF dans les Comptes AWS, votre Comptes AWS doit être configuré conformément aux bonnes pratiques du cadre AWS Well-Architected. Il s'agit de contrôles de sécurité directifs, de détection, préventifs et réactifs. Vous devez avoir mis en place des processus d'atténuation détaillés en cas de violation ou d'incident de sécurité. La stratégie de votre organisation doit inclure des exigences relatives à la gestion centralisée de l'identité, de l'accès et de la mise en réseau. Généralement, ces exigences et services sont gérés par une équipe dédiée à la zone de destination.

Responsabilités propres à ADDF

Configuration ADDF sécurisée

La responsabilité d'un utilisateur d'ADDF commence par la configuration ADDF sécurisée conformément à la documentation ADDF. Nous vous recommandons vivement de suivre les instructions de ADDF Deployment Guide (GitHub). Pour plus d'informations sur la configuration sécurisée d'ADDF, veuillez consulter Définition de votre architecture ADDF et Configuration initiale.

Personnalisation sécurisée d'ADDF

En cas de personnalisation des fonctionnalités de base d'ADDF, telles que CodeSeeder, SeedFarmer et les modules principaux ADDF, l'utilisateur ADDF assume l'entière responsabilité de ces modifications. Pour de plus amples informations, veuillez consulter Personnalisation du code du cadre de déploiement ADDF.

Développement de module ADDF sécurisé

L'utilisateur ADDF est entièrement responsable de tout module personnalisé déployé à l'aide d'ADDF. En outre, l'utilisateur d'ADDF est responsable de toute modification de code apportée aux modules fournis par ADDF. Pour de plus amples informations, veuillez consulter Écriture de modules personnalisés dans ADDF.

Mises à jour et opérations ADDF sécurisées

Au fur et à mesure que le cadre évolue, ADDF reçoit des mises à jour de fonctionnalités et de sécurité. Il est de la responsabilité de l'utilisateur ADDF de vérifier régulièrement les mises à jour publiées sur le référentiel GitHub et d'exploiter ADDF en toute sécurité sur le long terme. Pour plus d'informations, consultez Déploiements ADDF récurrents, Audits de sécurité récurrents, Mises à jour d'ADDF et Mise hors service.

Processus de révision de la sécurité ADDF

Autonomous Driving Data Framework (ADDF) a été conçu dans un souci de sécurité. Avant d'être mis à la disposition du public, AWS a effectué un examen de la sécurité interne initial d'ADDF et a résolu tous les problèmes de sécurité identifiés. Tant AWS que la communauté open source contribuent aux examens de la sécurité continus du cadre.

Examens de la sécurité réguliers effectués par AWS

ADDF est publié sous l'organisation GitHub awslabs qui appartient à AWS. AWS effectue des examens de la sécurité automatiques et manuels réguliers du code dans cette organisation, afin de vérifier la sécurité dans les meilleures conditions. Conformément à la stratégie AWS, AWS ne divulgue aucune information sur la fréquence des examens de la sécurité, l'approche ou les outils utilisés. En outre, AWS ne publie aucun rapport d'audit interne concernant ADDF. Cependant, tous les résultats de sécurité identifiés sont corrigés et publiés par le biais d'une demande d'extraction, en toute urgence.

> **Note**
>
> ADDF en tant que cadre est fourni « TEL QUEL », SANS GARANTIE NI CONDITION D'AUCUNE SORTE, tant expresse qu'implicite, y compris, sans s'y limiter, toute garantie ou condition de titre, de non-contrefaçon, de qualité marchande ou d'adéquation à un usage particulier, comme indiqué dans la licence Apache 2.0 (GitHub). Vous devez effectuer votre propre évaluation de la sécurité d'ADDF et vérifier s'il est conforme aux exigences de sécurité propres à votre organisation. Comme indiqué dans la licence Apache 2.0, il vous incombe à vous seul de déterminer la pertinence de l'utilisation ou de la redistribution d'ADDF et vous assumez tous les risques associés à l'exercice ou aux autorisations que vous avez accordées en vertu de cette licence.

Examens de la sécurité open source et contributions

ADDF est un projet open source qui accepte les contributions. Nous invitons tous les utilisateurs à effectuer leur propre examen de la sécurité du cadre et à y contribuer en signalant tout résultat lié à la sécurité. Si vous trouvez un problème dans le code, veuillez suivre les instructions de Security issue notifications (documentation ADDF).

Fonctionnalités de sécurité intégrées ADDF

Autonomous Driving Data Framework (ADDF) dispose de diverses fonctionnalités de sécurité intégrées. Par défaut, ces fonctionnalités sont conçues pour vous aider à configurer un cadre sécurisé et à aider votre organisation à répondre aux exigences de sécurité d'entreprise les plus courantes.

Les fonctionnalités de sécurité intégrées sont les suivantes :

- Moindre privilège pour le code de module ADDF
- Infrastructure en tant que code
- Contrôles de sécurité automatisés pour IaC
- Stratégie de moindre privilège personnalisée pour le rôle de déploiement AWS CDK
- Politique de moindre privilège pour le fichier deployspec du module
- Chiffrement des données
- Stockage des informations d'identification à l'aide de Secrets Manager
- Examens de sécurité de SeedFarmer et CodeSeeder
- Prise en charge des limites des autorisations pour le rôle AWS CodeBuild pour CodeSeeder
- Architecture à comptes multiples AWS
- Autorisations de moindre privilège pour les déploiements de comptes multiples

Moindre privilège pour le code de module ADDF

Le moindre privilège est la bonne pratique de sécurité qui consiste à accorder les autorisations minimales nécessaires à l'exécution d'une tâche. Pour en savoir plus, veuillez consulter Appliquer les autorisations de moindre privilège. Les modules fournis par ADDF suivent rigoureusement le principe du moindre privilège dans leur code et dans les ressources déployées, comme suit :

- Toutes les politiques (IAM) AWS Identity and Access Management générées pour un module ADDF disposent des autorisations minimales requises pour le cas d'utilisation.
- Les Services AWS sont configurés et déployés selon le principe du moindre privilège. Les modules fournis par ADDF utilisent uniquement les services et fonctionnalités de service requis pour un cas d'utilisation spécifique.

Infrastructure en tant que code

ADDF, en tant que cadre, est conçu pour déployer des modules ADDF sous forme d'infrastructure en tant que code (IaC). L'IaC élimine les processus de déploiement manuel et aide à prévenir les erreurs et les mauvaises configurations qui peuvent résulter des processus manuels.

ADDF est conçu pour orchestrer et déployer des modules à l'aide de n'importe quel cadre IaC courant. Cela inclut, mais sans s'y limiter :

- AWS Cloud Development Kit (AWS CDK)
- AWS CloudFormation
- Hashicorp Terraform

Vous pouvez utiliser différents cadres IaC pour écrire différents modules, puis utiliser ADDF pour les déployer.

Le cadre IaC par défaut utilisé par les modules ADDF est AWS CDK. AWS CDK est une abstraction orientée objet de haut niveau que vous pouvez utiliser pour définir des ressources AWS de manière impérative. AWS CDK applique déjà les bonnes pratiques de sécurité par défaut pour divers services et scénarios. Avec AWS CDK, le risque lié aux mauvaises configurations de sécurité est réduit.

Contrôles de sécurité automatisés pour IaC

L'utilitaire cdk-nag open source (GitHub) est intégré dans ADDF. Cet utilitaire vérifie automatiquement que les modules ADDF basés sur AWS CDK respectent les bonnes pratiques générales et de sécurité. L'utilitaire cdk-nag utilise des règles et des packs de règles pour détecter et signaler le code qui enfreint les bonnes pratiques. Pour plus d'informations sur les règles et une liste complète, voir Règles cdk-nag (GitHub).

Stratégie de moindre privilège personnalisée pour le rôle de déploiement AWS CDK

L'ADDF utilise largement AWS CDK v2. Il est nécessaire d'amorcer tous les Comptes AWS ADDF sur AWS CDK. Pour plus d'informations, veuillez consulter Bootstrapping (documentation AWS CDK).

Par défaut, AWS CDK assigne la stratégie gérée par AWS AdministratorAccess permissive au rôle de déploiement AWS CDK créé dans des comptes amorcés. Le nom complet de ce rôle est `cdk-`

`[CDK_QUALIFIER]-cfn-exec-role-[AWS_ACCOUNT_ID]-[REGION]`. AWS CDK utilise ce rôle pour déployer des ressources dans le Compte AWS amorcé dans le cadre du processus de déploiement d'AWS CDK.

En fonction des exigences de sécurité de votre organisation, la stratégie `AdministratorAccess` peut être trop permissive. Dans le cadre du processus d'amorçage d'AWS CDK, vous pouvez personnaliser la stratégie et les autorisations en fonction de vos besoins. Vous pouvez modifier la stratégie en réamorçant le compte avec une nouvelle stratégie définie à l'aide du paramètre `--cloudformation-execution-policies`. Pour plus d'informations, veuillez consulter Personnalisation du bootstrapping (documentation AWS CDK).

> **Note**
>
> Bien que cette fonctionnalité de sécurité ne soit pas propre à ADDF, elle est répertoriée dans cette section, car elle peut améliorer la sécurité globale de votre déploiement ADDF.

Politique de moindre privilège pour le fichier deployspec du module

Chaque module contient un fichier de spécifications de déploiement appelé deployspec.yaml. Ce fichier définit les instructions de déploiement du module. CodeSeeder l'utilise pour déployer le module défini dans le compte de destination à l'aide d'AWS CodeBuild. CodeSeeder attribue une fonction du service par défaut à CodeBuild pour déployer les ressources, comme indiqué dans le fichier de spécifications de déploiement. Cette fonction du service est conçue selon le principe du moindre privilège. Elle inclut toutes les autorisations requises pour le déploiement d'applications AWS CDK, car tous les modules fournis par ADDF sont créés en tant qu'applications AWS CDK.

Toutefois, si vous devez exécuter des commandes d'étape en dehors d'AWS CDK, vous devez créer une politique IAM personnalisée au lieu d'utiliser la fonction du service par défaut pour CodeBuild. Par exemple, si vous utilisez un autre cadre de déploiement IaC qu'AWS CDK, comme Terraform, vous devez créer une politique IAM qui accorde des autorisations suffisantes pour que ce cadre spécifique fonctionne. Un autre scénario qui nécessite une politique IAM dédiée est celui où vous incluez les appels directs AWS Command Line Interface (AWS CLI) vers d'autres Services AWS dans les commandes d'étape `install`, `pre_build`, `build` ou `post_build`. Par exemple, vous avez besoin d'une stratégie personnalisée si votre module inclut une commande Amazon Simple Storage Service (Amazon S3) pour charger des fichiers dans un compartiment S3. La politique IAM personnalisée offre un contrôle précis pour toute commande AWS en dehors du déploiement d'AWS CDK. Pour un exemple de politique IAM personnalisée, voir ModuleStack (documentation

SeedFarmer). Lorsque vous créez une politique IAM personnalisée pour votre module ADDF, assurez-vous d'appliquer les autorisations de moindre privilège.

Chiffrement des données

ADDF stocke et traite des données potentiellement sensibles. Pour renforcer la protection de ces données, les modules fournis par SeedFarmer, CodeSeeder et ADDF chiffrent les données au repos et en transit pour tous les Services AWS utilisés (sauf indication contraire explicite pour les modules du dossier `demo-only`).

Stockage des informations d'identification à l'aide de Secrets Manager

ADDF gère divers secrets pour différents services, tels que Docker Hub, JupyterHub et Amazon Redshift. ADDF utilise AWS Secrets Manager pour stocker tous les secrets liés à ADDF. Cela vous permet de supprimer les données sensibles du code source.

Les secrets de Secrets Manager sont uniquement stockés dans les comptes de destination, dans la mesure où ils sont nécessaires au bon fonctionnement de ces comptes. Par défaut, le compte de chaîne d'outils ne contient aucun secret.

Examens de sécurité de SeedFarmer et CodeSeeder

SeedFarmer et CodeSeeder (référentiels GitHub) sont utilisés pour déployer ADDF et ses modules ADDF. Ces projets open source sont soumis au même processus d'examen de sécurité interne AWS régulier qu'ADDF, tel que décrit dans Processus de révision de la sécurité ADDF.

Prise en charge des limites des autorisations pour le rôle AWS CodeBuild pour CodeSeeder

Les limites des autorisations IAM sont un mécanisme de sécurité courant qui définit les autorisations maximales qu'une politique basée sur l'identité peut accorder à une entité IAM. SeedFarmer et CodeSeeder prennent en charge une limite des autorisations IAM pour chaque compte de destination. La limite des autorisations limite les autorisations maximales de toute fonction du service utilisée par CodeBuild lorsque CodeSeeder déploie des modules. Les limites des autorisations IAM doivent être créées en dehors d'ADDF par une équipe de sécurité. Les pièces jointes à la stratégie

de limite des autorisations IAM sont acceptées en tant qu'attributs dans le fichier manifeste de déploiement ADDF, deployment.yaml. Pour plus d'informations, veuillez consulter Permissions boundary support (documentation SeedFarmer).

Le flux de travail est le suivant :

1. Votre équipe de sécurité définit et crée une limite des autorisations IAM en fonction de vos exigences de sécurité. La limite des autorisations IAM doit être créée individuellement dans chaque Compte AWS ADDF. Le résultat est une liste Amazon Resource Name (ARN) des stratégies de limite des autorisations.
2. L'équipe de sécurité partage la liste ARN des stratégies avec votre équipe de développement ADDF.
3. L'équipe de développement ADDF intègre la liste ARN des stratégies dans le fichier manifeste. Pour un exemple de cette intégration, voir sample-permissionboundary.yaml (GitHub) et Deployment manifest (documentation SeedFarmer).
4. Une fois le déploiement réussi, la limite des autorisations est jointe à toutes les fonctions du service utilisées par CodeBuild pour déployer des modules.
5. L'équipe de sécurité veille à ce que les limites des autorisations soient appliquées selon les besoins.

Architecture à comptes multiples AWS

Tel que défini dans le pilier de sécurité du cadre AWS Well-Architected, il est considéré comme une bonne pratique de séparer les ressources et les charges de travail en plusieurs Comptes AWS, en fonction des exigences de votre organisation. Cela s'explique par le fait qu'un Compte AWS sert de limite d'isolement. Pour plus d'informations, veuillez consulter Gestion et séparation de Compte AWS. La mise en œuvre de ce concept est appelée architecture à comptes multiples. Une architecture à comptes multiples AWS bien conçue permet de catégoriser les charges de travail et de réduire l'impact en cas de faille de sécurité, par rapport à une architecture à compte unique.

ADDF prend en charge de manière native les architectures à comptes multiples AWS. Vous pouvez répartir vos modules ADDF sur autant d'Comptes AWS que nécessaire pour répondre aux exigences de votre organisation en matière de sécurité et de séparation des tâches. Vous pouvez déployer ADDF dans un seul Compte AWS, en combinant les fonctions de la chaîne d'outils et du compte de destination. Vous pouvez également créer des comptes de destination individuels pour les modules ou les groupes de modules ADDF.

La seule restriction que vous devez prendre en compte est qu'un module ADDF représente la plus petite unité de déploiement pour chaque Compte AWS.

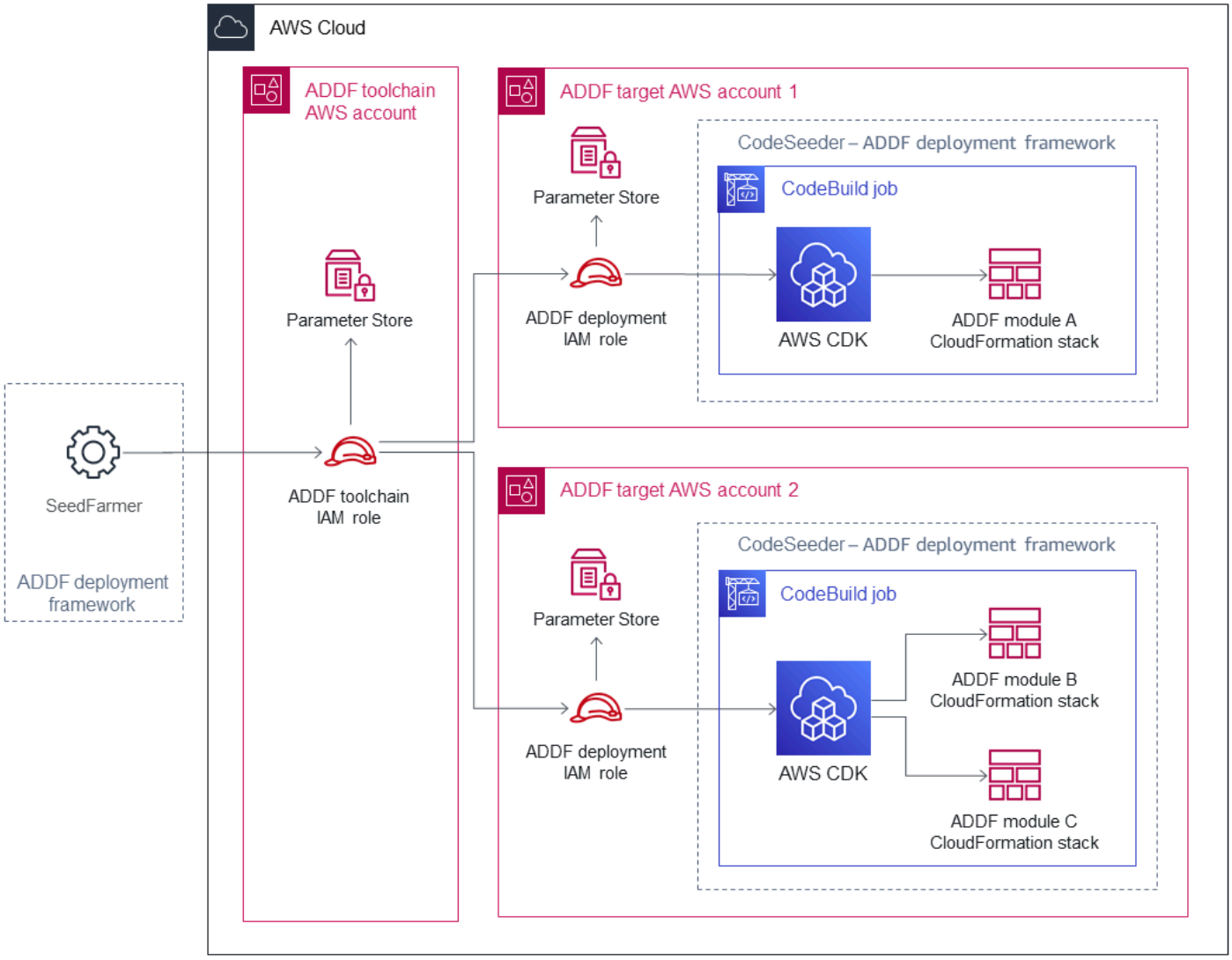
Pour les environnements de production, il est recommandé d'utiliser une architecture à comptes multiples composée d'un compte de chaîne d'outils et d'au moins un compte de destination. Pour de plus amples informations, veuillez consulter Architecture ADDF.

Autorisations de moindre privilège pour les déploiements de comptes multiples

Si vous utilisez une architecture à comptes multiples, SeedFarmer doit accéder aux comptes de destination pour effectuer les trois actions suivantes :

1. Écrire les métadonnées du module ADDF dans le compte de chaîne d'outils et les comptes de destination.
2. Lire les métadonnées du module ADDF en cours à partir du compte chaîne d'outils et des comptes de destination.
3. Lancer des tâches AWS CodeBuild dans les comptes de destination, dans le but de déployer ou de mettre à jour des modules.

La figure suivante montre les relations entre comptes, y compris les opérations permettant d'endosser les rôles AWS Identity and Access Management (IAM) propres à ADDF.



Ces actions entre comptes sont réalisées à l'aide d'opérations assume-role bien définies.

- Le rôle IAM de la chaîne d'outils ADDF est déployé dans le compte de chaîne d'outils. SeedFarmer endosse ce rôle. Ce rôle est autorisé à exécuter une action `iam:AssumeRole` et peut endosser le rôle IAM de déploiement ADDF dans chaque compte de destination. En outre, le rôle IAM de la chaîne d'outils ADDF peut exécuter des opérations AWS Systems Manager Parameter Store locales.
- Le rôle IAM de déploiement ADDF est déployé dans chaque compte de destination. Ce rôle ne peut être endossé qu'à partir du compte de chaîne d'outils en utilisant le rôle IAM de la chaîne d'outils ADDF. Ce rôle est autorisé à exécuter des opérations AWS Systems Manager Parameter Store locales et des actions AWS CodeBuild qui initient et décrivent des tâches CodeBuild via CodeSeeder.

Ces rôles IAM propres à ADDF sont créés dans le cadre du processus d'amorçage d'ADDF. Pour plus d'informations, veuillez consulter Bootstrap Compte AWS(s) dans le Guide de déploiement d'ADDF (GitHub).

Toutes les autorisations de comptes multiples sont définies selon le principe du moindre privilège. Si un compte de destination est compromis, l'impact sur les autres Comptes AWS ADDF est minime ou nul.

Dans le cas d'une architecture à compte unique pour ADDF, les relations entre les rôles restent les mêmes. Elles se fondent simplement dans un Compte AWS unique.

Configuration et fonctionnement sécurisés d'ADDF

Autonomous Driving Data Framework (ADDF) doit être considéré comme un logiciel personnalisé qui nécessite une maintenance et des soins continus par une équipe DevOps et de sécurité dédiée au sein de votre organisation. Cette section décrit les tâches courantes liées à la sécurité qui vous aident à configurer et à utiliser ADDF tout au long de son cycle de vie.

Cette section comprend les tâches suivantes :

- Définition de votre architecture ADDF
- Configuration initiale
- Personnalisation du code du cadre de déploiement ADDF
- Écriture de modules personnalisés dans ADDF
- Déploiements ADDF récurrents
- Audits de sécurité récurrents
- Mises à jour d'ADDF
- Mise hors service

Définition de votre architecture ADDF

Une instance ADDF n'est aussi sûre que l'environnement d'Compte AWS dans lequel elle est déployée. Cet environnement Compte AWS doit être conçu pour répondre aux besoins opérationnels et de sécurité de votre cas d'utilisation spécifique. Par exemple, les tâches et considérations liées à la sécurité et aux opérations relatives à la configuration d'une instance ADDF dans un environnement de preuve de concept (PoC) sont différentes de celles relatives à la configuration d'ADDF dans un environnement de production.

Exécution d'ADDF dans un environnement de PoC

Si vous avez l'intention d'utiliser ADDF dans un environnement de PoC, nous vous recommandons de créer un Compte AWS dédié pour ADDF qui ne contient aucune autre charge de travail. Cela permet de sécuriser votre compte pendant que vous découvrez ADDF et ses fonctionnalités. Les avantages de cette approche sont les suivants :

- En cas de grave erreur de configuration d'ADDF, aucune autre charge de travail n'est affectée.

- Il n'y a aucun risque d'autre erreur de configuration de la charge de travail susceptible de nuire à la configuration d'ADDF.

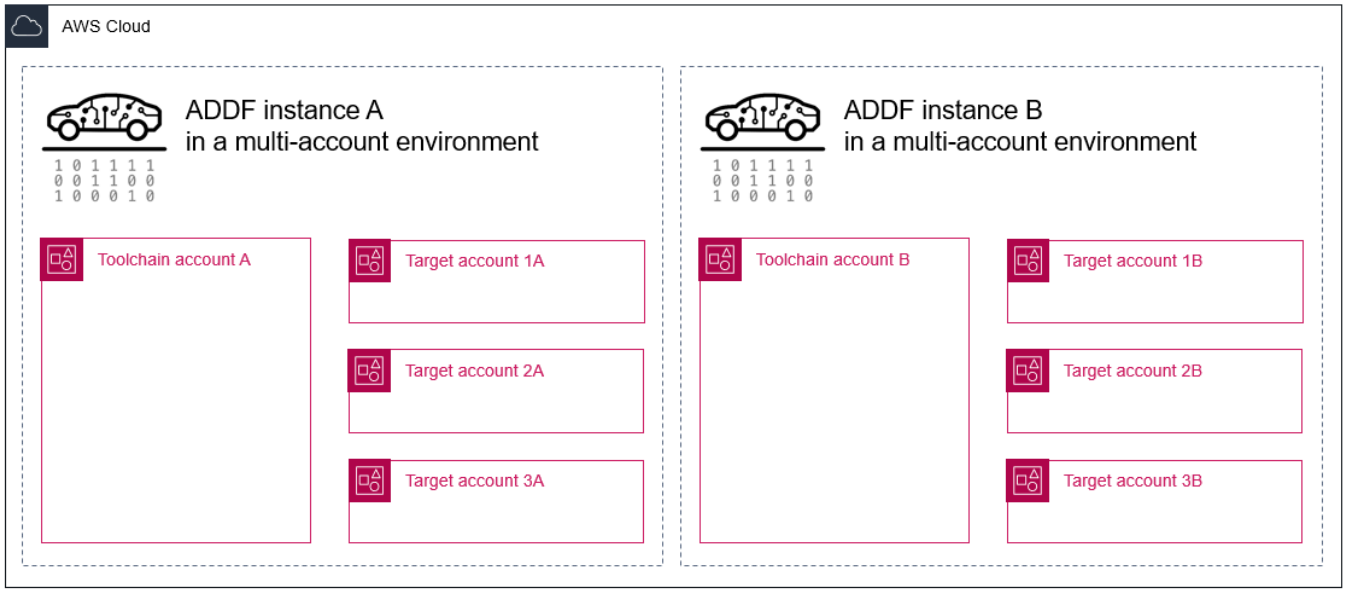
Même pour un environnement PoC, nous vous recommandons de suivre les bonnes pratiques répertoriées dans Exécution d'ADDF dans un environnement de production dans la mesure du possible.

Exécution d'ADDF dans un environnement de production

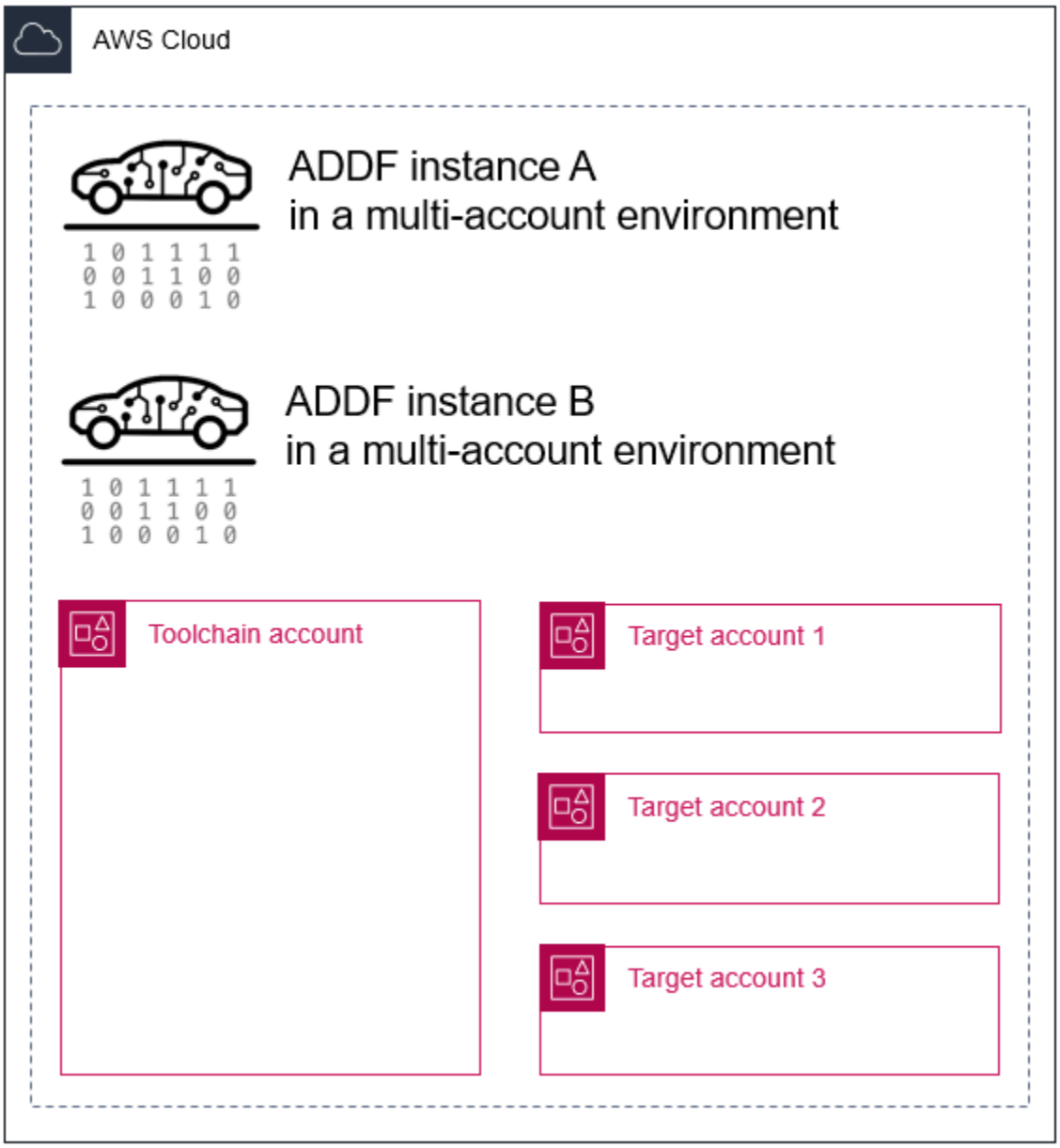
Si vous avez l'intention d'utiliser ADDF dans un environnement de production d'entreprise, nous vous recommandons vivement de prendre en compte les bonnes pratiques de sécurité de votre organisation et d'implémenter ADDF en conséquence. Outre les bonnes pratiques de sécurité de votre entreprise, nous vous recommandons d'implémenter les mesures suivantes :

- Créer une équipe DevOps ADDF engagée à long terme : ADDF doit être considéré comme un logiciel personnalisé. Il nécessite une maintenance et des soins continus par une équipe DevOps dédiée. Avant de commencer à exécuter ADDF dans un environnement de production, une équipe DevOps de taille et de capacités suffisantes doit être définie avec un engagement total en termes de ressources, jusqu'à la fin de vie du déploiement d'ADDF.
- Utiliser une architecture à comptes multiples : chaque instance ADDF doit être déployée dans son propre environnement à comptes multiples AWS dédié, sans aucune autre charge de travail indépendante. Tel que défini dans la gestion et séparation des comptes AWS (cadre AWS Well-Architected), il est considéré comme une bonne pratique de séparer les ressources et les charges de travail en plusieurs Comptes AWS, en fonction des exigences de votre organisation. Cela s'explique par le fait qu'un Compte AWS sert de limite d'isolement. Une architecture à comptes multiples AWS bien conçue permet de catégoriser les charges de travail et de réduire l'impact en cas de faille de sécurité, par rapport à une architecture à compte unique. L'utilisation d'une architecture à comptes multiples permet également à vos comptes de respecter leurs quotas de Service AWS. Répartissez vos modules ADDF sur autant d'Comptes AWS que nécessaire pour répondre aux exigences de votre organisation en matière de sécurité et de séparation des tâches.
- Déployer plusieurs instances ADDF : configurez autant d'instances ADDF distinctes que nécessaire afin de développer, tester et déployer correctement les modules ADDF conformément aux processus de développement logiciel de votre organisation. Lorsque vous configurez plusieurs instances ADDF, vous pouvez utiliser l'une des approches suivantes :
  - Plusieurs instances ADDF dans différents environnements à comptes multiples AWS : vous pouvez utiliser des Comptes AWS distincts pour isoler différentes instances ADDF. Par exemple,

si votre organisation dispose d'étapes de développement, de test et de production dédiées, vous pouvez créer des instances ADDF distinctes et des comptes dédiés pour chaque étape. Cela présente de nombreux avantages, tels que la réduction du risque de propagation des erreurs entre les étapes, l'aide à l'implémentation d'un processus d'approbation et la restriction de l'accès des utilisateurs à certains environnements uniquement. L'image suivante montre deux instances ADDF déployées dans des environnements à comptes multiples distincts.



- Plusieurs instances ADDF dans le même environnement AWS à comptes multiples : vous pouvez créer plusieurs instances ADDF qui partagent le même environnement AWS à comptes multiples. Cela crée efficacement des branches isolées dans les mêmes Comptes AWS. Par exemple, si différents développeurs travaillent en parallèle, un développeur peut créer une instance ADDF dédiée dans les mêmes Comptes AWS. Cela permet aux développeurs de travailler dans des branches isolées à des fins de développement et de test. Si vous utilisez cette approche, pour chaque instance ADDF, vos ressources ADDF doivent avoir des noms de ressources uniques. Ceci est pris en charge par défaut dans les modules préalablement fournis par ADDF. Vous pouvez utiliser cette approche tant que vous ne dépassez pas les quotas Service AWS. L'image suivante montre deux instances ADDF déployées dans un environnement à comptes multiples partagé.



- Plusieurs instances ADDF dans le même environnement AWS à compte unique : cette architecture est très similaire à l'exemple précédent. La différence est que les différentes instances ADDF sont déployées dans un environnement à compte unique plutôt que dans un environnement à comptes multiples. Cette architecture peut s'adapter à des cas d'utilisation ADDF très simples dont la portée est très limitée et où plusieurs développeurs travaillent simultanément sur différentes branches.

SeedFarmer étant le seul outil qui contrôle les déploiements d'une instance ADDF, vous pouvez créer n'importe quel environnement et architecture de compte adaptés à la stratégie de déploiement et aux processus CI/CD de votre organisation.

- Personnaliser le processus d'amorçage AWS Cloud Development Kit (AWS CDK) en fonction des exigences de sécurité de votre organisation : par défaut, AWS CDK assigne la stratégie gérée par AWS AdministratorAccess pendant le processus d'amorçage. Cette stratégie accorde des privilèges administratifs complets. Si cette stratégie est trop permissive pour les besoins en sécurité de votre organisation, vous pouvez personnaliser les stratégies qui seront appliquées. Pour de plus amples informations, veuillez consulter Stratégie de moindre privilège personnalisée pour le rôle de déploiement AWS CDK.
- Respecter les bonnes pratiques lors de la configuration de l'accès dans IAM : établissez une solution d'accès AWS Identity and Access Management (IAM) structurée qui permet à vos utilisateurs d'accéder aux Comptes AWS ADDF. Le cadre d'ADDF est conçu pour adhérer au principe du moindre privilège. Votre modèle d'accès IAM doit également respecter le principe du

moindre privilège, être conforme aux exigences de votre organisation et respecter les bonnes pratiques de sécurité dans IAM (documentation IAM).

- Configurer la mise en réseau conformément aux bonnes pratiques de votre organisation : ADDF inclut une pile AWS CloudFormation de mise en réseau facultative qui crée un cloud privé virtuel (VPC) public ou privé de base. Selon la configuration de votre organisation, ce VPC peut exposer des ressources directement à Internet. Nous vous recommandons de suivre les bonnes pratiques de mise en réseau de votre entreprise et de créer un module réseau personnalisé et renforcé en termes de sécurité.
- Déployez des mesures de prévention de sécurité, de détection et d'atténuation au niveau du Compte AWS : AWS propose divers services de sécurité, tels qu'Amazon GuardDuty, AWS Security Hub, Amazon Detective et AWS Config. Activez ces services dans votre Compte AWS ADDF et intégrez les processus de prévention, de détection, d'atténuation et de gestion des incidents liés à la sécurité de votre organisation. Nous vous recommandons de suivre Bonnes pratiques pour la sécurité, l'identité et la conformité (AWS Architecture Center) et toutes les recommandations spécifiques à un service contenues dans la documentation de ce service. Pour en savoir plus, veuillez consulter Documentation de sécurité AWS.

ADDF n'aborde aucun de ces sujets, car les détails d'implémentation et de configuration dépendent fortement des exigences et des processus propres à votre organisation. Il est plutôt de la responsabilité fondamentale de votre organisation d'aborder ces sujets. Généralement, l'équipe qui gère votre zone de destination AWS vous aide à planifier et à implémenter votre environnement ADDF.

Configuration initiale

Configurez ADDF conformément à ADDF Deployment Guide (GitHub). Le point de départ de tout déploiement est le dossier `/manifest` dans le référentiel GitHub autonomous-driving-data-framework. Le dossier `/manifest/example-dev` contient un exemple de déploiement à des fins de démonstration. Utilisez cet exemple comme point de départ pour la conception de votre propre déploiement. Dans ce répertoire, il existe un fichier manifeste de déploiement ADDF appelé deployment.yaml. Il contient toutes les informations permettant à SeedFarmer de gérer, de déployer ou de supprimer ADDF et ses ressources dans le AWS Cloud. Vous pouvez créer des groupes de modules ADDF dans des fichiers dédiés. Le fichier core-modules.yaml est un exemple du groupe de modules principaux, et il inclut tous les modules principaux fournis par ADDF. Pour résumer, le fichier

deployment.yaml contient toutes les références aux groupes et modules qui seront déployés sur leurs comptes de destination et spécifie l'ordre de déploiement.

Pour une configuration sécurisée et conforme, en particulier dans un environnement non destiné à la preuve de concept, nous vous recommandons de consulter le code source de chaque module que vous souhaitez déployer. Conformément aux bonnes pratiques de renforcement de la sécurité, vous devez déployer uniquement les modules requis pour le cas d'utilisation prévu.

> **Note**
>
> Les modules ADDF dans le dossier `modules/demo-only/` ne sont pas sécurisés et ne doivent pas être déployés dans des environnements de production ou dans un environnement contenant des données sensibles ou protégées. Ces modules sont inclus pour mettre en valeur les capacités du système, et vous pouvez les utiliser comme base pour créer vos propres modules personnalisés et sécurisés.

Personnalisation du code du cadre de déploiement ADDF

Le cadre de déploiement ADDF et sa logique d'orchestration et de déploiement peuvent être entièrement personnalisés pour répondre à toutes les exigences. Cependant, nous vous suggérons de ne pas personnaliser ou de minimiser vos modifications pour les raisons suivantes :

- Maintenir la compatibilité en amont : la compatibilité en amont facilite la mise à jour d'ADDF pour bénéficier des dernières fonctionnalités et mises à jour de sécurité. La modification du cadre rompt la rétrocompatibilité native avec SeedFarmer, CodeSeeder et tous les modules principaux ADDF.
- Conséquences pour la sécurité : la modification du cadre de déploiement ADDF peut être une tâche complexe susceptible d'avoir des conséquences imprévues en matière de sécurité. Dans le pire des cas, les modifications du cadre peuvent donner lieu à des vulnérabilités de sécurité.

Dans la mesure du possible, créez et personnalisez votre propre code de module au lieu de modifier le cadre de déploiement ADDF et le code du module principal ADDF.

> **Note**
>
> Si vous pensez que certaines parties du cadre de déploiement d'ADDF doivent être améliorées ou renforcées davantage en matière de sécurité, veuillez apporter vos

modifications au référentiel ADDF par le biais d'une demande d'extraction. Pour de plus amples informations, veuillez consulter Examens de la sécurité open source et contributions.

Écriture de modules personnalisés dans ADDF

La création d'un module ADDF ou l'extension d'un module existant est un concept fondamental d'ADDF. Lors de la création ou de la personnalisation de modules, nous vous suggérons de suivre les bonnes pratiques générales en matière de sécurité AWS et les bonnes pratiques de votre organisation en matière de codage sécurisé. En outre, nous vous recommandons de procéder à des examens de sécurité techniques internes ou externes initiaux et périodiques, en fonction des exigences de sécurité de votre organisation, afin de réduire davantage le risque de problèmes de sécurité.

Déploiements ADDF récurrents

Déployez ADDF et ses modules comme décrit dans ADDF Deployment Guide (GitHub). Pour prendre en charge les déploiements ADDF récurrents qui ajoutent, mettent à jour ou suppriment des ressources dans vos comptes de destination, SeedFarmer utilise des hachages MD5, stockés dans le Parameter Store de votre chaîne d'outils et de vos comptes de destination, pour comparer l'infrastructure actuellement déployée à l'infrastructure définie dans les fichiers manifestes de votre base de code locale.

Cette approche suit le paradigme GitOps, selon lequel votre référentiel source (la base de code locale dans laquelle vous utilisez SeedFarmer) est la source de vérité, et l'infrastructure déclarée explicitement dans celui-ci est le résultat souhaité de votre déploiement. Pour plus d'informations sur GitOps, veuillez consulter What is GitOps (site Web GitLab).

Audits de sécurité récurrents

Comme tout autre logiciel de votre organisation, intégrez ADDF et votre code de module ADDF personnalisé dans votre cycle de gestion des risques de sécurité, d'examen de sécurité et d'audit de sécurité.

Mises à jour d'ADDF

ADDF reçoit des mises à jour régulières dans le cadre de ses efforts de développement continus. Cela inclut les mises à jour des fonctionnalités, ainsi que les améliorations et correctifs liés à la sécurité. Nous vous recommandons de vérifier régulièrement les nouvelles versions du cadre et d'appliquer les mises à jour en temps opportun. Pour plus d'informations, veuillez consulter Steps to update ADDF (documentation ADDF).

Mise hors service

Si ADDF n'est plus nécessaire, supprimez-le avec toutes ses ressources associées de votre Comptes AWS. Toute infrastructure non surveillée et inutilisée entraîne des coûts inutiles et présente un risque de sécurité potentiel. Pour plus d'informations, veuillez consulter Steps to destroy ADDF (documentation ADDF).

Étapes suivantes

Ce guide examine les bonnes pratiques et considérations en matière de sécurité et d'opérations lors du déploiement d'Autonomous Driving Data Framework (ADDF) dans votre environnement AWS Cloud. Ce guide se penche sur le modèle de responsabilité partagée entre l'utilisateur d'ADDF, l'équipe principale ADDF et AWS afin que vous compreniez votre rôle et vos responsabilités en matière de configuration et d'exploitation d'ADDF en toute sécurité. Il inclut également des recommandations d'exploitation d'ADDF en toute sécurité tout au long de son cycle de vie, y compris des recommandations propres à l'environnement.

Nous vous recommandons de vous familiariser avec les ressources de la section Ressources. Lorsque vous êtes prêt, vous pouvez configurer ADDF en fonction des instructions contenues dans ADDF Deployment Guide (GitHub).

Lorsque vous configurez et utilisez ADDF, si vous pensez que le cadre de déploiement doit être amélioré ou renforcé davantage au niveau de la sécurité, veuillez apporter vos modifications au référentiel ADDF par le biais d'une demande d'extraction. Pour de plus amples informations, veuillez consulter Examens de la sécurité open source et contributions.

Ressources

Documentation AWS

- Develop and deploy a customized workflow using ADDF on AWS (billet de blog AWS)
- Documentation sur le service de sécurité AWS
- Bonnes pratiques de sécurité dans IAM
- Gestion et séparation des comptes AWS
- Bootstrapping for AWS CDK
- Modèle de responsabilité partagée AWS
- Cadre AWS Well-Architected

Ressources open source

- ADDF repository (GitHub)
- ADDF Deployment Guide (GitHub)
- CodeSeeder repository (GitHub)
- SeedFarmer repository (GitHub)

Avis

Il incombe aux clients de procéder à une évaluation indépendante des informations contenues dans le présent document. Ce document : (a) est fourni à titre informatif uniquement, (b) représente les offres de produits et les pratiques AWS actuelles, qui sont sujettes à modification sans préavis, et (c) ne donne lieu à aucun engagement ni aucune assurance de la part d'AWS et de ses sociétés apparentées, fournisseurs ou concédants de licence. Les produits ou services AWS sont fournis « tels quels » sans garantie, représentation ou condition d'aucune sorte, tant expresse qu'implicite.

Les responsabilités et obligations d'AWS vis-à-vis de ses clients sont régies par les contrats AWS. Le présent document ne fait partie d'aucun, et ne modifie aucun, contrat entre AWS et ses clients.

Historique du document

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

Modification	Description	Date
Publication initiale	—	15 novembre 2022

AWS Glossaire des directives prescriptives

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

Nombres

7 R

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

- Refactorisation/réarchitecture : transférez une application et modifiez son architecture en tirant pleinement parti des fonctionnalités natives cloud pour améliorer l'agilité, les performances et la capacité de mise à l'échelle. Cela implique généralement le transfert du système d'exploitation et de la base de données. Exemple : migrez votre base de données Oracle sur site vers l'édition compatible avec Amazon Aurora PostgreSQL.
- Replateformer (déplacer et remodeler) : transférez une application vers le cloud et introduisez un certain niveau d'optimisation pour tirer parti des fonctionnalités du cloud. Exemple : migrez votre base de données Oracle sur site vers Amazon Relational Database Service (Amazon RDS) pour Oracle dans le. AWS Cloud
- Racheter (rachat) : optez pour un autre produit, généralement en passant d'une licence traditionnelle à un modèle SaaS. Exemple : migrez votre système de gestion de la relation client (CRM) vers Salesforce.com.
- Réhéberger (lift and shift) : transférez une application vers le cloud sans apporter de modifications pour tirer parti des fonctionnalités du cloud. Exemple : migrez votre base de données Oracle 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.