



Le guide des AWS CDK couches

AWS Conseils prescriptifs



AWS Conseils prescriptifs: Le guide des AWS CDK couches

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

Introduction	1
Constructions de couche 1	3
Le AWS CDK— CloudFormation cycle de vie des constructions L1	3
La spécification AWS CloudFormation de la ressource	4
Constructions de couche 2	7
Propriétés par défaut	9
Structures, types et interfaces	10
Méthodes statiques	10
Méthodes auxiliaires	11
Enums	13
Cours d'assistance	13
Constructions de la couche 3	15
Interactions avec les ressources	16
Extensions de ressources	18
Ressources personnalisées	19
Bonnes pratiques	28
FAQ	30
Ne puis-je pas utiliser les couches AWS CDK sans comprendre les couches ?	30
Puis-je créer des constructions L2 à partir de L1 de la même manière que je crée des constructions L3 à partir de L2 ?	30
Quelles AWS ressources n'ont pas encore de constructions L2 officielles ?	30
Puis-je créer une construction L2 ou L3 dans n'importe quelle langue prise en charge ? AWS CDK	31
Où puis-je trouver les constructions L3 existantes en dehors du ? AWS CDK	31
Ressources	32
Historique du document	33
Glossaire	34
#	34
A	35
B	38
C	40
D	43
E	47
F	50

G	52
H	53
I	55
L	57
M	58
O	63
P	65
Q	68
R	69
S	72
T	76
U	77
V	78
W	79
Z	80
.....	lxxxi

Le guide des AWS CDK couches

Steven Guggenheimer, Amazon Web Services (AWS)

Décembre 2023 ([historique du document](#))

L'un des principaux concepts sous-jacents AWS Cloud Development Kit (AWS CDK) ressemble beaucoup à celui qui sous-tend le fait de rester au chaud par temps froid. Ce concept s'appelle le layering. Par temps froid, vous enflez une chemise, une veste et parfois une veste encore plus grande selon la température. Ensuite, si vous rentrez à l'intérieur et que le chauffage brûle, vous pouvez enlever une ou les deux couches de veste pour ne pas avoir trop chaud. Il AWS CDK utilise la superposition pour fournir différents niveaux d'abstraction pour l'utilisation des composants du cloud. La superposition garantit que vous n'aurez jamais à écrire trop de code ou à accéder trop peu aux propriétés des ressources lorsque vous déployez votre infrastructure sous forme de piles de code (IAC).

Si vous n'utilisez pas le AWS CDK, vous devez écrire vos [AWS CloudFormation](#) modèles à la main, c'est-à-dire que vous n'utilisez qu'une seule couche qui vous oblige à écrire bien plus de code que ce qui est habituellement nécessaire. D'un autre côté, s' AWS CDK ils faisaient abstraction de tout ce CloudFormation que vous n'avez généralement pas besoin d'écrire, vous ne seriez pas en mesure de gérer les cas extrêmes.

Pour résoudre ce problème, le AWS CDK provisionnement des ressources est divisé en trois couches distinctes :

- Couche 1 — La CloudFormation couche : couche la plus élémentaire où la CloudFormation ressource et la AWS CDK ressource sont presque identiques.
- Couche 2 — La couche organisée : couche dans laquelle les CloudFormation ressources sont résumées en classes programmatiques qui rationalisent une grande partie de la syntaxe standard CloudFormation . Cette couche constitue la plupart des AWS CDK.
- Couche 3 — La couche de motif : couche la plus abstraite dans laquelle vous pouvez utiliser les éléments de base fournis par les couches 1 et 2 pour personnaliser le code en fonction de votre cas d'utilisation spécifique.

Chaque élément de chaque couche est une instance d'une AWS CDK classe spéciale appelée Construct a. Selon [AWS la documentation](#), les constructions sont « les éléments de base des AWS CDK applications. Une construction représente un « composant cloud » et encapsule tout ce

qui est AWS CloudFormation nécessaire pour créer le composant. » Les constructions au sein de ces couches sont appelées constructions L1, L2 et L3 selon la couche à laquelle elles appartiennent. Dans ce guide, nous allons parcourir chaque AWS CDK couche pour découvrir à quoi elles servent et pourquoi elles sont importantes.

Ce guide est destiné aux responsables techniques, aux responsables et aux développeurs qui souhaitent approfondir les concepts fondamentaux qui sous-tendent le AWS CDK travail. AWS CDK C'est un outil populaire, mais il est très courant que les équipes passent à côté d'une grande partie de ce qu'il a à offrir. Lorsque vous commencez à comprendre les concepts décrits dans ce guide, vous pouvez accéder à un tout nouveau monde de possibilités et optimiser les processus de provisionnement des ressources de vos équipes.

Dans ce guide :

- [Constructions de couche 1](#)
- [Constructions de la couche 2](#)
- [Constructions de la couche 3](#)
- [Bonnes pratiques](#)
- [FAQ](#)
- [Ressources](#)

Constructions de couche 1

Les [constructions L1 sont les](#) éléments constitutifs du AWS CDK et se distinguent facilement des autres constructions par le préfixe. Cfn Par exemple, le package Amazon DynamoDB contenu dans AWS CDK le contient Table une construction, qui est une construction L2. La construction L1 correspondante est appeléeCfnTable, et elle représente directement un CloudFormation Table DynamoDB. Il est impossible d'utiliser le AWS CDK sans accéder à cette première couche, bien qu'une AWS CDK application n'utilise généralement jamais directement une construction L1. Cependant, dans la majorité des cas, les constructions L2 et L3 que les développeurs ont l'habitude d'utiliser reposent largement sur les constructions L1. Vous pouvez donc considérer les constructions L1 comme le pont entre CloudFormation et le. AWS CDK

Le seul but du AWS CDK est de générer des CloudFormation modèles en utilisant des langages de codage standard. Une fois que vous avez exécuté la commande cdk synth CLI et que les CloudFormation modèles résultants ont été générés, le travail AWS CDK est terminé. La commande cdk deploy n'est là que pour des raisons pratiques, mais ce que vous faites lorsque vous exécutez cette commande se produit entièrement à l'intérieur CloudFormation. La pièce du puzzle qui traduit le AWS CDK code dans un format CloudFormation compréhensible est la construction L1.

Le AWS CDK— CloudFormation cycle de vie des constructions L1

Le processus de création et d'utilisation des constructions L1 comprend les étapes suivantes :

1. Le processus de AWS CDK construction convertit les CloudFormation spécifications en code programmatique sous la forme de constructions L1.
2. Les développeurs écrivent du code qui fait directement ou indirectement référence à des constructions L1 dans le cadre d'une AWS CDK application.
3. Les développeurs exécutent la commande cdk synth pour reconverter le code programmatique dans le format dicté par les CloudFormation spécifications (modèles).
4. Les développeurs exécutent la commande cdk deploy pour déployer les CloudFormation piles de ces modèles dans des environnements de AWS comptes.

Faisons un petit exercice. Accédez au [référentiel AWS CDK open source activé](#) GitHub, sélectionnez un AWS service aléatoire, puis accédez au AWS CDK package correspondant à ce service (situé dans le dossierpackages,aws-cdk-lib,aws-<servicename>,lib). Pour cet exemple,

choisissons Amazon S3, mais cela fonctionne pour n'importe quel service. Si vous regardez le [fichier `index.ts`](#) principal de ce package, vous verrez une ligne qui se lit comme suit :

```
export * from './s3.generated';
```

Cependant, vous ne verrez le `s3.generated` fichier nulle part dans le répertoire correspondant. Cela est dû au fait que les constructions L1 sont générées automatiquement à partir de la [spécification de la CloudFormation ressource](#) pendant le AWS CDK processus de construction. Vous ne le verrez donc `s3.generated` dans le package qu'après avoir exécuté la commande de AWS CDK construction pour le package.

La spécification AWS CloudFormation de la ressource

La spécification AWS CloudFormation des ressources définit l'infrastructure en tant que code (IAC) AWS et détermine comment le code contenu dans les CloudFormation modèles est converti en ressources dans un AWS compte. Cette spécification définit les AWS ressources au [format JSON](#) au niveau de chaque région. Chaque ressource reçoit un [nom de type de ressource](#) unique qui suit le format `provider::service::resource`. Par exemple, le nom du type de ressource pour un compartiment Amazon S3 serait `AWS::S3::Bucket`, et le nom du type de ressource pour un point d'accès Amazon S3 serait `AWS::S3::AccessPoint`. Ces types de ressources peuvent être affichés dans un CloudFormation modèle en utilisant la syntaxe définie dans la spécification de la AWS CloudFormation ressource. Lorsque le processus de AWS CDK génération s'exécute, chaque type de ressource devient également une construction L1.

Par conséquent, chaque construction L1 est une image miroir programmatique de sa ressource correspondante CloudFormation . Chaque propriété que vous appliqueriez dans un CloudFormation modèle est disponible lorsque vous instanciez une construction L1, et chaque CloudFormation propriété requise est également requise comme argument lorsque vous instanciez la construction L1 correspondante. Le tableau suivant compare un compartiment S3 tel que représenté dans un CloudFormation modèle avec le même compartiment S3 défini comme une construction AWS CDK L1.

CloudFormation modèle

```
"amzn-s3-demo-bucket": {
  "Type": "AWS::S3::Bucket",
  "Properties": {
```

Construction L1

```
new CfnBucket(this, "amzn-s3-demo-bucket", {
  bucketName: "amzn-s3-demo-bucket",
```

```

    "BucketName": "amzn-s3-demo-
bucket",
    "BucketEncryption": {
      "ServerSideEncryptionConfig
uration": [
        {
          "ServerSideEncrypt
ionByDefault": {
            "SSEAlgorithm": "AES256"
          }
        }
      ],
      "MetricsConfigurations": [
        {
          "Id": "myConfig"
        }
      ],
      "OwnershipControls": {
        "Rules": [
          {
            "ObjectOwnership":
"BucketOwnerPreferred"
          }
        ]
      },
      "PublicAccessBlockConfigura
tion": {
        "BlockPublicAcls": true,
        "BlockPublicPolicy": true,
        "IgnorePublicAcls": true,
        "RestrictPublicBuckets": true
      },
      "VersioningConfiguration": {
        "Status": "Enabled"
      }
    }
  }
}

```

```

    bucketEncryption: {
      serverSideEncryptionConfigu
ration: [
        {
          serverSideEncryptionByDefau
lt: {
            sseAlgorithm: "AES256"
          }
        }
      ],
      metricsConfigurations: [
        {
          id: "myConfig"
        }
      ],
      ownershipControls: {
        rules: [
          {
            objectOwnership: "BucketOw
nerPreferred"
          }
        ]
      },
      publicAccessBlockConfiguration: {
        blockPublicAcls: true,
        blockPublicPolicy: true,
        ignorePublicAcls: true,
        restrictPublicBuckets: true
      },
      versioningConfiguration: {
        status: "Enabled"
      }
    });

```

Comme vous pouvez le constater, la construction L1 est la manifestation exacte dans le code de la CloudFormation ressource. Il n'y a pas de raccourcis ni de simplifications, de sorte que la quantité de texte standard à écrire est à peu près la même. Cependant, l'un des grands avantages de l'utilisation

du AWS CDK est censé être qu'il permet d'éliminer une grande partie de cette syntaxe standard. CloudFormation Alors, comment cela se produit-il ? C'est là qu'intervient la construction L2.

Constructions de couche 2

Le [référentiel AWS CDK open source](#) est écrit principalement en utilisant le langage [TypeScript](#) de programmation et se compose de nombreux packages et modules. La bibliothèque de packages principale, appelée `aws-cdk-lib`, est grossièrement divisée en un package par AWS service, bien que ce ne soit pas toujours le cas. Comme indiqué précédemment, les constructions L1 sont automatiquement générées pendant le processus de construction, alors quel est tout ce code que vous voyez lorsque vous regardez dans le référentiel ? Ce sont des [constructions L2](#), qui sont des abstractions des constructions L1.

Les packages contiennent également une collection de TypeScript types, d'énumérations et d'interfaces ainsi que des classes d'assistance qui ajoutent plus de fonctionnalités, mais ces éléments servent tous à des constructions L2. Toutes les constructions L2 appellent leurs constructions L1 correspondantes dans leurs constructeurs lors de l'instanciation, et la construction L1 résultante qui est créée est accessible depuis la couche 2 comme suit :

```
const role = new Bucket(this, "amzn-s3-demo-bucket", {/*...BucketProps*/});
const cfnBucket = role.node.defaultChild;
```

La construction L2 prend les propriétés par défaut, les méthodes pratiques et les autres sucres syntaxiques et les applique à la construction L1. Cela élimine une grande partie de la répétition et de la verbosité nécessaires pour fournir des ressources directement. CloudFormation

Toutes les constructions L2 construisent leurs constructions L1 correspondantes sous le capot. Cependant, les constructions L2 n'étendent pas réellement les constructions L1. [Les constructions L1 et L2 héritent toutes deux d'une classe spéciale appelée Construct](#). Dans la version 1 de AWS CDK la `Construct` classe était intégrée au kit de développement, mais dans la version 2, il s'agit d'un [package autonome](#) distinct. C'est ainsi que d'autres packages tels que le [Cloud Development Kit for Terraform \(CDKTF\)](#) peuvent l'inclure en tant que dépendance. Toute classe qui hérite de la `Construct` classe est une construction L1, L2 ou L3. Les constructions L2 étendent directement cette classe alors que les constructions L1 étendent une classe appelée `CfnResource`, comme indiqué dans le tableau suivant.

Arbre d'héritage L1

Construction L1

→ classe [CfnResource](#)

Arbre d'héritage L2

Construction L2

→ classe [Construct](#)

→ classe abstraite [CfnRefElement](#)

→→→ classe abstraite [CfnElement](#)

→→→ classe [Construct](#)

Si les constructions L1 et L2 héritent de la Construct classe, pourquoi les constructions L2 n'étendent-elles pas simplement L1 ? Eh bien, les classes situées entre la Construct classe et la couche 1 verrouillent la construction L1 en place en tant qu'image miroir de la CloudFormation ressource. Ils contiennent des méthodes abstraites (méthodes que les classes en aval doivent inclure)_toCloudFormation, comme celles qui obligent la construction à générer directement CloudFormation la syntaxe. Les constructions L2 ignorent ces classes et étendent directement la Construct classe. Cela leur donne la flexibilité d'abstraire une grande partie du code nécessaire aux constructions L1 en les construisant séparément dans leurs constructeurs.

La section précédente présentait une side-by-side comparaison entre un compartiment S3 issu d'un CloudFormation modèle et ce même compartiment S3 rendu sous forme de construction L1. Cette comparaison a montré que les propriétés et la syntaxe sont presque identiques et que la construction L1 n'enregistre que trois ou quatre lignes par rapport à la CloudFormation construction. Comparons maintenant la construction L1 avec la construction L2 pour le même compartiment S3 :

Construction L1 pour le compartiment S3

```
new CfnBucket(this, "amzn3demobucket", {
    bucketName: "amzn-s3-demo-bucket",
    bucketEncryption: {
        serverSideEncryptionConfiguration: [
            {
                serverSideEncryptionByDefault: {
                    sseAlgorithm: "AES256"
                }
            }
        ],
    },
    metricsConfigurations: [
        {
```

Construction L2 pour le compartiment S3

```
new Bucket(this, "amzn3demobucket",
    {
        bucketName: "amzn-s3-demo-bucket",
        encryption: BucketEncryption.S3_MANAGED,
        metrics: [
            {
                id: "myConfig"
            },
        ],
        objectOwnership: ObjectOwnership.BUCKET_OWNER_PREFERRED,
        blockPublicAccess: BlockPublicAccess.BLOCK_ALL,
        versioned: true
    });
```

```
        id: "myConfig"
    }
],
ownershipControls: {
    rules: [
        {
            objectOwnership: "BucketOwnerPreferred"
        }
    ]
},
publicAccessBlockConfiguration: {
    blockPublicAcls: true,
    blockPublicPolicy: true,
    ignorePublicAcls: true,
    restrictPublicBuckets: true
},
versioningConfiguration: {
    status: "Enabled"
}
});
```

Comme vous pouvez le constater, la construction L2 est inférieure à la moitié de la taille de la construction L1. Les constructions L2 utilisent de nombreuses techniques pour réaliser cette consolidation. Certaines de ces techniques s'appliquent à une seule construction L2, mais d'autres peuvent être réutilisées dans plusieurs constructions afin qu'elles soient séparées dans leur propre classe pour être réutilisables. Les constructions L2 consolident CloudFormation la syntaxe de plusieurs manières, comme indiqué dans les sections suivantes.

Propriétés par défaut

Le moyen le plus simple de consolider le code de provisionnement d'une ressource consiste à transformer les paramètres de propriété les plus courants en paramètres par défaut. AWS CDK II a accès à de puissants langages de programmation mais CloudFormation ne le fait pas. Ces valeurs par défaut sont donc souvent de nature conditionnelle. Il est parfois possible d'éliminer plusieurs lignes de CloudFormation configuration du AWS CDK code, car ces paramètres peuvent être déduits des valeurs d'autres propriétés transmises à la construction.

Structures, types et interfaces

Bien qu'il AWS CDK soit disponible dans plusieurs langages de programmation, il est écrit nativement TypeScript, de sorte que le système de types du langage est utilisé pour définir les types qui composent les constructions L2. L'étude approfondie de ce type de système dépasse le cadre de ce guide ; consultez la [TypeScript documentation](#) pour plus de détails. En résumé, a TypeScript type décrit le type de données que contient une variable particulière. Il peut s'agir de données de base telles que `string`, ou de données plus complexes telles que `object`. A TypeScript `interface` est une autre façon d'exprimer le type d' `TypeScript` objet, et a `struct` est un autre nom pour une interface.

TypeScript n'utilise pas le terme structure, mais si vous regardez dans la [référence de l'AWS CDK API](#), vous verrez qu'une structure n'est en fait qu'une autre TypeScript interface dans le code. La référence d'API fait également référence à certaines interfaces en tant qu'interfaces. Si les structures et les interfaces sont identiques, pourquoi la AWS CDK documentation fait-elle une distinction entre elles ?

Ce que l'on AWS CDK appelle des structures sont des interfaces qui représentent n'importe quel objet utilisé par une construction L2. Cela inclut les types d'objets pour les arguments de propriété transmis à la construction L2 lors de l'instanciation, tels que `BucketProps` pour la construction `S3 Bucket` et pour `TableProps` la construction `DynamoDB Table`, ainsi que les autres TypeScript interfaces utilisées dans le. AWS CDK En bref, s'il s'agit d'une TypeScript interface dans le AWS CDK et que son nom n'est pas préfixé par la lettre `I`, il l' AWS CDK appelle une structure.

Inversement, il AWS CDK utilise le terme interface pour représenter les éléments de base. Un objet simple devrait être considéré comme une représentation appropriée d'une construction ou d'une classe d'assistance particulière. C'est-à-dire qu'une interface décrit ce que doivent être les propriétés publiques d'une construction L2. Tous les noms AWS CDK d'interface sont les noms de structures existantes ou de classes auxiliaires préfixés par la lettre. `I` Toutes les constructions L2 étendent la `Construct` classe, mais elles implémentent également l'interface correspondante. La construction L2 `Bucket` implémente donc l'`IBucket` interface.

Méthodes statiques

Chaque instance d'une construction L2 est également une instance de son interface correspondante, mais l'inverse n'est pas vrai. Cela est important lorsque vous parcourez une structure pour voir quels types de données sont requis. Si une structure possède une propriété appelée `bucket`, qui nécessite le type de données `IBucket`, vous pouvez transmettre soit un objet contenant

les propriétés répertoriées dans l'`IBucket` interface, soit une instance d'un `Bucket` L2. L'un ou l'autre fonctionnerait. Toutefois, si cette `bucket` propriété appelait un `L2Bucket`, vous ne pouviez transmettre qu'une `Bucket` instance dans ce champ.

Cette distinction devient très importante lorsque vous importez des ressources préexistantes dans votre pile. Vous pouvez créer une construction L2 pour n'importe quelle ressource native de votre pile, mais si vous devez référencer une ressource créée en dehors de la pile, vous devez utiliser l'interface de cette construction L2. En effet, la création d'une construction L2 crée une nouvelle ressource s'il n'en existe pas déjà une dans cette pile. Les références aux ressources existantes doivent être des objets simples conformes à l'interface de cette construction L2.

Pour faciliter cela dans la pratique, la plupart des constructions L2 sont associées à un ensemble de méthodes statiques qui renvoient l'interface de cette construction L2. Ces méthodes statiques commencent généralement par le mot `from`. Les deux premiers arguments transmis à ces méthodes sont les mêmes `scope` et les `id` arguments sont requis pour une construction L2 standard. Cependant, le troisième argument `props` n'est qu'un petit sous-ensemble de propriétés (ou parfois une seule propriété) qui définit une interface. Pour cette raison, lorsque vous transmettez une construction L2, dans la plupart des cas, seuls les éléments de l'interface sont requis. Ainsi, vous pouvez également utiliser les ressources importées, dans la mesure du possible.

```
// Example of referencing an external S3 bucket
const preExistingBucket = Bucket.fromBucketName(this, "external-bucket", "name-of-
bucket-that-already-exists");
```

Cependant, vous ne devez pas trop vous fier aux interfaces. Vous ne devez importer des ressources et utiliser les interfaces directement que lorsque cela est absolument nécessaire, car les interfaces ne fournissent pas la plupart des propriétés, telles que les méthodes d'assistance, qui rendent une construction L2 si puissante.

Méthodes auxiliaires

Une construction L2 est une classe programmatique plutôt qu'un simple objet. Elle peut donc exposer des méthodes de classe qui vous permettent de manipuler la configuration de vos ressources après l'instanciation. La construction Gestion des identités et des accès AWS (IAM) L2 `Role` en est [un](#) bon exemple. Les extraits suivants montrent deux manières de créer le même rôle IAM à l'aide de la construction L2. `Role`

Sans méthode auxiliaire :

```
const role = new Role(this, "my-iam-role", {
  assumedBy: new FederatedPrincipal('my-identity-provider.com'),
  managedPolicies: [
    ManagedPolicy.fromAwsManagedPolicyName("ReadOnlyAccess")
  ],
  inlinePolicies: {
    lambdaPolicy: new PolicyDocument({
      statements: [
        new PolicyStatement({
          effect: Effect.ALLOW,
          actions: [ 'lambda:UpdateFunctionCode' ],
          resources: [ 'arn:aws:lambda:us-east-1:123456789012:function:my-
function' ]
        })
      ]
    })
  }
});
```

Avec une méthode auxiliaire :

```
const role = new Role(this, "my-iam-role", {
  assumedBy: new FederatedPrincipal('my-identity-provider.com')
});

role.addManagedPolicy(ManagedPolicy.fromAwsManagedPolicyName("ReadOnlyAccess"));
role.attachInlinePolicy(new Policy(this, "lambda-policy", {
  policyName: "lambdaPolicy",
  statements: [
    new PolicyStatement({
      effect: Effect.ALLOW,
      actions: [ 'lambda:UpdateFunctionCode' ],
      resources: [ 'arn:aws:lambda:us-east-1:123456789012:function:my-function' ]
    })
  ]
}));
```

La possibilité d'utiliser des méthodes d'instance pour manipuler la configuration des ressources après l'instanciation donne aux constructions L2 une flexibilité supplémentaire par rapport à la couche précédente. Les constructions L1 héritent également de certaines méthodes de ressources (telles que `addPropertyOverride`), mais ce n'est qu'à partir de la deuxième couche que vous obtenez des méthodes spécifiquement conçues pour cette ressource et ses propriétés.

Enums

CloudFormation la syntaxe vous oblige souvent à spécifier de nombreux détails afin de provisionner correctement une ressource. Cependant, la majorité des cas d'utilisation ne sont souvent couverts que par une poignée de configurations. La représentation de ces configurations à l'aide d'une série de valeurs énumérées peut réduire considérablement la quantité de code nécessaire.

Par exemple, dans l'exemple de code L2 du compartiment S3 décrit plus haut dans cette section, vous devez utiliser la `bucketEncryption` propriété du CloudFormation modèle pour fournir tous les détails, y compris le nom de l'algorithme de chiffrement à utiliser. AWS CDK II fournit plutôt l'`BucketEncryption` énumération, qui reprend les cinq formes les plus courantes de chiffrement des compartiments et vous permet d'exprimer chacune d'elles en utilisant des noms de variables uniques.

Qu'en est-il des cas extrêmes qui ne sont pas couverts par les énumérations ? L'un des objectifs d'une construction L2 est de simplifier la tâche de provisionnement d'une ressource de couche 1, de sorte que certains cas extrêmes moins courants risquent de ne pas être pris en charge dans la couche 2. Pour prendre en charge ces cas extrêmes, vous AWS CDK pouvez manipuler les propriétés CloudFormation des ressources sous-jacentes directement à l'aide de la [addPropertyOverride](#) méthode. Pour en savoir plus sur les remplacements de propriétés, consultez la section [Meilleures pratiques](#) de ce guide et la section [Abstractions et trappes d'échappement](#) de la documentation. AWS CDK

Cours d'assistance

Parfois, une énumération ne peut pas accomplir la logique de programmation nécessaire pour configurer une ressource pour un cas d'utilisation donné. Dans ces situations, il propose AWS CDK souvent un cours d'assistance à la place. Une énumération est un objet simple qui propose une série de paires clé-valeur, tandis qu'une classe auxiliaire offre toutes les fonctionnalités d'une classe. TypeScript Une classe auxiliaire peut toujours agir comme une énumération en exposant des propriétés statiques, mais ces propriétés peuvent alors avoir leurs valeurs définies en interne avec une logique conditionnelle dans le constructeur de classe auxiliaire ou dans une méthode d'assistance.

Ainsi, bien que l'`BucketEncryption` énumération puisse réduire la quantité de code nécessaire pour définir un algorithme de chiffrement sur un compartiment S3, cette même stratégie ne fonctionnerait pas pour définir des durées car les valeurs possibles sont tout simplement trop nombreuses parmi lesquelles choisir. La création d'une énumération pour chaque valeur serait bien

plus difficile qu'elle n'en vaut la peine. Pour cette raison, une classe d'assistance est utilisée pour les paramètres de configuration par défaut d'un compartiment S3 Object Lock, tels que représentés par la [ObjectLockRetention](#) classe. `ObjectLockRetention` contient deux méthodes statiques : l'une pour le maintien de la conformité et l'autre pour le maintien de la gouvernance. Les deux méthodes utilisent une instance de la [classe d'assistance Duration comme argument pour exprimer la durée](#) pendant laquelle le verrou doit être configuré.

La classe d' AWS Lambda assistance [Runtime](#) est un autre exemple. À première vue, il peut sembler que les propriétés statiques associées à cette classe puissent être gérées par une énumération. Cependant, chaque valeur de propriété représente une instance de la `Runtime` classe elle-même, de sorte que la logique exécutée dans le constructeur de la classe n'a pas pu être atteinte dans une énumération.

Constructions de la couche 3

Si les constructions L1 effectuent une traduction littérale des CloudFormation ressources en code programmatique et que les constructions L2 remplacent une grande partie de la CloudFormation syntaxe détaillée par des méthodes auxiliaires et une logique personnalisée, à quoi servent les constructions L3 ? La réponse à cette question n'est limitée que par votre imagination. Vous pouvez créer une couche 3 adaptée à n'importe quel cas d'utilisation spécifique. Si votre projet a besoin d'une ressource dotée d'un sous-ensemble spécifique de propriétés, vous pouvez créer une construction L3 réutilisable pour répondre à ce besoin.

Les constructions L3 sont appelées modèles au sein du AWS CDK. Un modèle est un objet qui étend la `Construct` classe dans le AWS CDK (ou étend une classe qui étend la `Construct` classe) pour exécuter une logique abstraite au-delà de la couche 2. Lorsque vous utilisez la AWS CDK CLI pour exécuter `cdk init` afin de démarrer un nouveau AWS CDK projet, vous devez choisir entre trois types AWS CDK d'applications : `app`, `lib`, et `sample-app`.

```
Available templates:
* app: Template for a CDK Application
  └─ cdk init app --language=[csharp|fsharp|go|java|javascript|python|typescript]
* lib: Template for a CDK Construct Library
  └─ cdk init lib --language=typescript
* sample-app: Example CDK Application with some constructs
  └─ cdk init sample-app --language=[csharp|fsharp|go|java|javascript|python|typescript]
```

`app` et `sample-app` les deux représentent AWS CDK des applications classiques dans lesquelles vous créez et déployez des CloudFormation stacks dans des environnements AWS. Lorsque vous choisissez `lib`, vous choisissez de construire une toute nouvelle construction L3. `app` et `sample-app` permettent de choisir n'importe quelle langue prise en charge par AWS CDK, mais vous ne pouvez choisir qu' TypeScript avec `lib`. Cela est dû au fait qu' AWS CDK est écrit nativement en TypeScript et utilise un système open source appelé [JSII](#) pour traduire le code original dans les autres langues prises en charge. Lorsque vous choisissez `lib` de lancer votre projet, vous choisissez de créer une extension du AWS CDK.

Toute classe qui étend la `Construct` classe peut être une construction L3, mais les cas d'utilisation les plus courants de la couche 3 sont les interactions avec les ressources, les extensions de ressources et les ressources personnalisées. La plupart des constructions L3 utilisent un ou plusieurs de ces trois cas afin d'étendre les fonctionnalités du AWS CDK.

Interactions avec les ressources

Une solution utilise généralement plusieurs services AWS qui fonctionnent ensemble. Par exemple, une CloudFront distribution Amazon utilise souvent un compartiment S3 comme origine et AWS WAF pour se protéger contre les exploits courants. AWS AppSync et Amazon API Gateway utilisent souvent des tables Amazon DynamoDB comme sources de données pour leurs applications. APIs Un pipeline utilise AWS CodePipeline souvent Amazon S3 comme source et AWS CodeBuild pour ses étapes de construction. Dans ces cas, il est souvent utile de créer une seule construction L3 qui gère le provisionnement de deux ou plusieurs constructions L2 interconnectées.

Voici un exemple de construction L3 qui fournit une CloudFront distribution avec son origine S3, et AWS WAF à placer devant elle, un enregistrement Amazon Route 53 et un certificat AWS Certificate Manager (ACM) pour ajouter un point de terminaison personnalisé avec chiffrement en transit, le tout dans une construction réutilisable :

```
// Define the properties passed to the L3 construct
export interface CloudFrontWebsiteProps {
  distributionProps: DistributionProps
  bucketProps: BucketProps
  wafProps: CfnWebAclProps
  zone: IHostedZone
}

// Define the L3 construct
export class CloudFrontWebsite extends Construct {
  public distribution: Distribution

  constructor(
    scope: Construct,
    id: string,
    props: CloudFrontWebsiteProps
  ) {
    super(scope, id);

    const certificate = new Certificate(this, "Certificate", {
      domainName: props.zone.zoneName,
      validation: CertificateValidation.fromDns(props.zone)
    });
    const defaultBehavior = {
      origin: new S3Origin(new Bucket(this, "bucket", props.bucketProps))
    }
  }
}
```

```
const waf = new CfnWebACL(this, "waf", props.wafProps);
this.distribution = new Distribution(this, id, {
  ...props.distributionProps,
  defaultBehavior,
  certificate,
  domainNames: [this.domainName],
  webAclId: waf.attrArn,
});
}
```

Notez qu'Amazon S3 CloudFront, Route 53 et ACM utilisent tous des constructions L2, mais que l'ACL Web (qui définit les règles de gestion des requêtes Web) utilise une construction L1. Cela est dû au fait qu'il s'agit d'un package open source évolutif qui n'est pas complètement complet et qu'il n'existe pas encore de construction L2. Cependant, n'importe qui peut y contribuer AWS CDK en créant de nouvelles constructions L2. Donc, jusqu'à ce qu'il AWS CDK propose une construction L2 pour `WebAcl`, vous devez utiliser une construction L1. Pour créer un nouveau site Web à l'aide de la construction `L3CloudFrontWebsite`, vous devez utiliser le code suivant :

```
const siteADotCom = new CloudFrontWebsite(stack, "siteA", siteAProps);
const siteBDotCom = new CloudFrontWebsite(stack, "siteB", siteBProps);
const siteCDotCom = new CloudFrontWebsite(stack, "siteC", siteCProps);
```

Dans cet exemple, la construction `CloudFront Distribution` L2 est exposée en tant que propriété publique de la construction L3. Dans certains cas, vous devrez toujours exposer de telles propriétés L3, si nécessaire. En fait, nous y reviendrons plus tard, dans la section [Ressources personnalisées](#).

AWS CDK II inclut quelques exemples de modèles d'interaction avec les ressources tels que celui-ci. Outre le `aws-ecs` package qui contient les constructions L2 pour Amazon Elastic Container Service (Amazon ECS), il possède un package appelé `aws-ecs-patterns`. Ce package contient plusieurs constructions L3 qui combinent Amazon ECS avec des équilibrateurs de charge d'application, des équilibrateurs de charge réseau et des groupes cibles, tout en proposant différentes versions prédéfinies pour Amazon Elastic Compute Cloud (Amazon) et EC2 AWS Fargate. Étant donné que de nombreuses applications sans serveur utilisent Amazon ECS uniquement avec Fargate, ces constructions L3 sont pratiques et permettent aux développeurs d'économiser du temps et de l'argent aux clients.

Extensions de ressources

Certains cas d'utilisation nécessitent que les ressources disposent de paramètres par défaut spécifiques qui ne sont pas natifs de la construction L2. Au niveau de la pile, cela peut être géré en utilisant des [aspects](#), mais un autre moyen pratique de donner de nouvelles valeurs par défaut à une construction L2 consiste à étendre la couche 2. Comme une construction est une classe qui hérite de la `Construct` classe et que les constructions L2 étendent cette classe, vous pouvez également créer une construction L3 en étendant directement une construction L2.

Cela peut être particulièrement utile pour une logique métier personnalisée qui répond aux besoins spécifiques d'un client. Supposons qu'une entreprise dispose d'un référentiel qui stocke l'ensemble de son code de AWS Lambda fonction dans un répertoire unique appelé `src/lambda` et que la plupart des fonctions Lambda réutilisent le même nom d'environnement d'exécution et de gestionnaire à chaque fois. Au lieu de configurer le chemin du code chaque fois que vous configurez une nouvelle fonction Lambda, vous pouvez créer une nouvelle construction L3 :

```
export class MyCompanyLambdaFunction extends Function {
  constructor(
    scope: Construct,
    id: string,
    props: Partial<FunctionProps> = {}
  ) {
    super(scope, id, {
      handler: 'index.handler',
      runtime: Runtime.NODEJS_LATEST,
      code: Code.fromAsset(`src/lambda/${props.functionName || id}`),
      ...props
    });
  }
}
```

Vous pouvez ensuite remplacer la `Function` construction L2 partout dans le référentiel comme suit :

```
new MyCompanyLambdaFunction(this, "MyFunction");
new MyCompanyLambdaFunction(this, "MyOtherFunction");
new MyCompanyLambdaFunction(this, "MyThirdFunction", {
  runtime: Runtime.PYTHON_3_11
});
```

Les valeurs par défaut vous permettent de créer de nouvelles fonctions Lambda sur une seule ligne, et la structure L3 est configurée afin que vous puissiez toujours remplacer les propriétés par défaut si nécessaire.

L'extension directe des constructions L2 fonctionne mieux lorsque vous souhaitez simplement ajouter de nouvelles valeurs par défaut aux constructions L2 existantes. Si vous avez également besoin d'une autre logique personnalisée, il est préférable d'étendre la `Construct` classe. La raison en est la `super` méthode, qui est appelée dans le constructeur. Dans les classes qui étendent d'autres classes, la `super` méthode est utilisée pour appeler le constructeur de la classe parent, et cela doit être la première chose qui se passe dans votre constructeur. Cela signifie que toute manipulation des arguments transmis ou de toute autre logique personnalisée ne peut avoir lieu qu'après la création de la construction L2 d'origine. Si vous devez exécuter l'une de ces logiques personnalisées avant d'instancier votre construction L2, il est préférable de suivre le modèle décrit précédemment dans la section Interactions avec les [ressources](#).

Ressources personnalisées

Les [ressources personnalisées](#) sont une fonctionnalité puissante CloudFormation qui vous permet d'exécuter une logique personnalisée à partir d'une fonction Lambda activée lors du déploiement de la pile. Chaque fois que vous avez besoin de processus de déploiement qui ne sont pas directement pris en charge par CloudFormation, vous pouvez utiliser une ressource personnalisée pour y parvenir. AWS CDK II propose des classes qui vous permettent également de créer des ressources personnalisées par programmation. En utilisant des ressources personnalisées dans un constructeur L3, vous pouvez créer une construction à partir de presque n'importe quoi.

L'un des avantages d'Amazon CloudFront réside dans ses puissantes capacités de mise en cache globale. Si vous souhaitez réinitialiser manuellement ce cache afin que votre site Web reflète immédiatement les nouvelles modifications apportées à votre origine, vous pouvez utiliser une [CloudFront invalidation](#). Toutefois, les invalidations sont des processus qui s'exécutent sur une CloudFront distribution au lieu d'être des propriétés d'une CloudFront distribution. Ils peuvent être créés et appliqués à une distribution existante à tout moment, de sorte qu'ils ne font pas partie intégrante du processus de provisionnement et de déploiement.

Dans ce scénario, vous souhaitez peut-être créer et exécuter une invalidation après chaque mise à jour de l'origine d'une distribution. Grâce aux ressources personnalisées, vous pouvez créer une construction L3 qui ressemble à ceci :

```
export interface CloudFrontInvalidationProps {
```

```

    distribution: Distribution
    region?: string
    paths?: string[]
  }

export class CloudFrontInvalidation extends Construct {
  constructor(
    scope: Construct,
    id: string,
    props: CloudFrontInvalidationProps
  ) {
    super(scope, id);
    const policy = AwsCustomResourcePolicy.fromSdkCalls({
      resources: AwsCustomResourcePolicy.ANY_RESOURCE
    });
    new AwsCustomResource(scope, `${id}Invalidation`, {
      policy,
      onUpdate: {
        service: 'CloudFront',
        action: 'createInvalidation',
        region: props.region || 'us-east-1',
        physicalResourceId:
PhysicalResourceId.fromResponse('Invalidation.Id'),
        parameters: {
          DistributionId: props.distribution.distributionId,
          InvalidationBatch: {
            Paths: {
              Quantity: props.paths?.length || 1,
              Items: props.paths || ['/*']
            },
            CallerReference: crypto.randomBytes(5).toString('hex')
          }
        }
      }
    }
  }
}

```

En utilisant la distribution que nous avons créée précédemment dans la construction CloudFrontWebsite L3, vous pouvez le faire très facilement :

```

new CloudFrontInvalidation(this, 'MyInvalidation', {
  distribution: siteADotCom.distribution

```

```
});
```

Cette construction L3 utilise une construction AWS CDK L3 appelée [AwsCustomResource](#) pour créer une ressource personnalisée qui exécute une logique personnalisée. `AwsCustomResource` est très pratique lorsque vous devez effectuer un seul appel au SDK AWS, car il vous permet de le faire sans avoir à écrire de code Lambda. Si vous avez des exigences plus complexes et souhaitez implémenter votre propre logique, vous pouvez utiliser directement la [CustomResource](#) classe de base.

Le [déploiement de compartiments S3](#) est un autre bon exemple d'AWS CDK utilisation d'une structure L3 de ressources personnalisées. La fonction Lambda créée par la ressource personnalisée dans le constructeur de cette construction L3 ajoute des fonctionnalités que CloudFormation ne pourraient pas être gérées autrement : elle ajoute et met à jour des objets dans un compartiment S3. Sans le déploiement du compartiment S3, vous ne pourriez pas placer de contenu dans le compartiment S3 que vous venez de créer dans le cadre de votre stack, ce qui serait très gênant.

Le meilleur exemple de l'AWS CDK élimination de la nécessité d'écrire des tonnes de CloudFormation syntaxe est le suivant : `S3BucketDeployment`

```
new BucketDeployment(this, 'BucketObjects', {
    sources: [Source.asset('./path/to/amzn-s3-demo-bucket')],
    destinationBucket: amzn-s3-demo-bucket
});
```

Comparez cela avec le CloudFormation code que vous devrez écrire pour accomplir la même chose :

```
"lambdaPolicyA5E98E09": {
  "Type": "AWS::IAM::Policy",
  "Properties": {
    "PolicyDocument": {
      "Statement": [
        {
          "Action": "lambda:UpdateFunctionCode",
          "Effect": "Allow",
          "Resource": "arn:aws:lambda:us-east-1:123456789012:function:my-function"
        }
      ],
      "Version": "2012-10-17"
    },
    "PolicyName": "lambdaPolicy",
    "Roles": [
      {
```

```

    "Ref": "myiamroleF09C7974"
  }
]
},
"Metadata": {
  "aws:cdk:path": "CdkScratchStack/lambda-policy/Resource"
}
},
"BucketObjectsAwsCliLayer8C081206": {
  "Type": "AWS::Lambda::LayerVersion",
  "Properties": {
    "Content": {
      "S3Bucket": {
        "Fn::Sub": "cdk-hnb659fds-assets-${AWS::AccountId}-${AWS::Region}"
      },
      "S3Key": "e2277687077a2abf9ae1af1cc9565e6715e2ebb62f79ec53aa75a1af9298f642.zip"
    },
    "Description": "/opt/awscli/aws"
  },
  "Metadata": {
    "aws:cdk:path": "CdkScratchStack/BucketObjects/AwsCliLayer/Resource",
    "aws:asset:path":
"asset.e2277687077a2abf9ae1af1cc9565e6715e2ebb62f79ec53aa75a1af9298f642.zip",
    "aws:asset:is-bundled": false,
    "aws:asset:property": "Content"
  }
},
"BucketObjectsCustomResourceB12E6837": {
  "Type": "Custom::CDKBucketDeployment",
  "Properties": {
    "ServiceToken": {
      "Fn::GetAtt": [
        "CustomCDKBucketDeployment8693BB64968944B69Aafb0CC9EB8756C81C01536",
        "Arn"
      ]
    }
  },
  "SourceBucketNames": [
    {
      "Fn::Sub": "cdk-hnb659fds-assets-${AWS::AccountId}-${AWS::Region}"
    }
  ],
  "SourceObjectKeys": [
    "f888a9d977f0b5bdbc04a1f8f07520ede6e00d4051b9a6a250860a1700924f26.zip"
  ],

```

```

    "DestinationBucketName": {
      "Ref": "amzn-s3-demo-bucket77F80CC0"
    },
    "Prune": true
  },
  "UpdateReplacePolicy": "Delete",
  "DeletionPolicy": "Delete",
  "Metadata": {
    "aws:cdk:path": "CdkScratchStack/BucketObjects/CustomResource/Default"
  }
},
"CustomCDKBucketDeployment8693BB64968944B69AAFB0CC9EB8756CServiceRole89A01265": {
  "Type": "AWS::IAM::Role",
  "Properties": {
    "AssumeRolePolicyDocument": {
      "Statement": [
        {
          "Action": "sts:AssumeRole",
          "Effect": "Allow",
          "Principal": {
            "Service": "lambda.amazonaws.com"
          }
        }
      ],
      "Version": "2012-10-17"
    },
    "ManagedPolicyArns": [
      {
        "Fn::Join": [
          "",
          [
            "arn:",
            {
              "Ref": "AWS::Partition"
            },
            ":iam::aws:policy/service-role/AWSLambdaBasicExecutionRole"
          ]
        ]
      }
    ]
  }
},
"Metadata": {
  "aws:cdk:path": "CdkScratchStack/
Custom::CDKBucketDeployment8693BB64968944B69AAFB0CC9EB8756C/ServiceRole/Resource"

```

```

    }
  },

  "CustomCDKBucketDeployment8693BB64968944B69Aafb0CC9EB8756CServiceRoleDefaultPolicy88902FDF":
  {
    "Type": "AWS::IAM::Policy",
    "Properties": {
      "PolicyDocument": {
        "Statement": [
          {
            "Action": [
              "s3:GetBucket*",
              "s3:GetObject*",
              "s3:List*"
            ],
            "Effect": "Allow",
            "Resource": [
              {
                "Fn::Join": [
                  "",
                  [
                    "arn:",
                    {
                      "Ref": "AWS::Partition"
                    },
                    ":s3::",
                    {
                      "Fn::Sub": "cdk-hnb659fds-assets-${AWS::AccountId}-${AWS::Region}"
                    },
                    "/*"
                  ]
                ]
              }
            ],
          },
          {
            "Fn::Join": [
              "",
              [
                "arn:",
                {
                  "Ref": "AWS::Partition"
                },
                ":s3::",
                {
                  "Fn::Sub": "cdk-hnb659fds-assets-${AWS::AccountId}-${AWS::Region}"
                }
              ]
            ]
          }
        ]
      }
    }
  }
}

```

```
    }
  ]
]
}
]
},
{
  "Action": [
    "s3:Abort*",
    "s3:DeleteObject*",
    "s3:GetBucket*",
    "s3:GetObject*",
    "s3:List*",
    "s3:PutObject",
    "s3:PutObjectLegalHold",
    "s3:PutObjectRetention",
    "s3:PutObjectTagging",
    "s3:PutObjectVersionTagging"
  ],
  "Effect": "Allow",
  "Resource": [
    {
      "Fn::GetAtt": [
        "amzn3demobucket77F80CC0",
        "Arn"
      ]
    },
    {
      "Fn::Join": [
        "",
        [
          {
            "Fn::GetAtt": [
              "amzn3demobucket77F80CC0",
              "Arn"
            ]
          },
          "/"
        ]
      ]
    }
  ]
}
],
```

```

    "Version": "2012-10-17"
  },
  "PolicyName":
"CustomCDKBucketDeployment8693BB64968944B69AAFB0CC9EB8756CServiceRoleDefaultPolicy88902FDF",
  "Roles": [
    {
      "Ref":
"CustomCDKBucketDeployment8693BB64968944B69AAFB0CC9EB8756CServiceRole89A01265"
    }
  ],
  "Metadata": {
    "aws:cdk:path": "CdkScratchStack/
Custom::CDKBucketDeployment8693BB64968944B69AAFB0CC9EB8756C/ServiceRole/DefaultPolicy/
Resource"
  }
},
"CustomCDKBucketDeployment8693BB64968944B69AAFB0CC9EB8756C81C01536": {
  "Type": "AWS::Lambda::Function",
  "Properties": {
    "Code": {
      "S3Bucket": {
        "Fn::Sub": "cdk-hnb659fds-assets-${AWS::AccountId}-${AWS::Region}"
      },
      "S3Key": "9eb41a5505d37607ac419321497a4f8c21cf0ee1f9b4a6b29aa04301aea5c7fd.zip"
    },
    "Role": {
      "Fn::GetAtt": [
        "CustomCDKBucketDeployment8693BB64968944B69AAFB0CC9EB8756CServiceRole89A01265",
        "Arn"
      ]
    },
    "Environment": {
      "Variables": {
        "AWS_CA_BUNDLE": "/etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem"
      }
    },
    "Handler": "index.handler",
    "Layers": [
      {
        "Ref": "BucketObjectsAwsCliLayer8C081206"
      }
    ],
    "Runtime": "python3.9",

```

```
    "Timeout": 900
  },
  "DependsOn": [

    "CustomCDKBucketDeployment8693BB64968944B69AAFB0CC9EB8756CServiceRoleDefaultPolicy88902FDF",
    "CustomCDKBucketDeployment8693BB64968944B69AAFB0CC9EB8756CServiceRole89A01265"
  ],
  "Metadata": {
    "aws:cdk:path": "CdkScratchStack/
Custom::CDKBucketDeployment8693BB64968944B69AAFB0CC9EB8756C/Resource",
    "aws:asset:path":
"asset.9eb41a5505d37607ac419321497a4f8c21cf0ee1f9b4a6b29aa04301aea5c7fd",
    "aws:asset:is-bundled": false,
    "aws:asset:property": "Code"
  }
}
```

4 lignes contre 241 lignes, c'est une énorme différence ! Et ce n'est qu'un exemple de ce qui est possible lorsque vous utilisez la couche 3 pour personnaliser vos piles.

Bonnes pratiques

Constructions L1

- Vous ne pouvez pas toujours éviter d'utiliser directement les constructions L1, mais vous devez l'éviter autant que possible. Si une construction L2 spécifique ne convient pas à votre scénario limite, vous pouvez explorer ces deux options au lieu d'utiliser directement la construction L1 :
 - Accès `defaultChild` : Si la CloudFormation propriété dont vous avez besoin n'est pas disponible dans une construction L2, vous pouvez accéder à la construction L1 sous-jacente en utilisant `L2Construct.node.defaultChild` Vous pouvez mettre à jour toutes les propriétés publiques de la construction L1 en y accédant via cette propriété au lieu de vous donner la peine de créer vous-même la construction L1.
 - Utiliser les remplacements de propriétés : et si la propriété que vous souhaitez mettre à jour n'est pas publique ? La trappe d'évacuation ultime qui permet AWS CDK de faire tout ce qu'un CloudFormation modèle peut faire est d'utiliser une méthode disponible dans chaque construction L1 : [addPropertyOverride](#) Vous pouvez manipuler votre pile au niveau du CloudFormation modèle en transmettant le nom et la valeur de la CloudFormation propriété directement à cette méthode.

Constructions L2

- N'oubliez pas de tirer parti des méthodes d'assistance proposées souvent par les constructions L2. Avec la couche 2, vous n'avez pas à transmettre toutes les propriétés lors de l'instanciation. Les méthodes auxiliaires L2 peuvent rendre le provisionnement des ressources exponentiellement plus pratique, en particulier lorsque la logique conditionnelle est requise. L'une des méthodes d'assistance les plus pratiques est dérivée de la classe [Grant](#). Cette classe n'est pas utilisée directement, mais de nombreuses constructions L2 l'utilisent pour fournir des méthodes d'assistance qui facilitent grandement l'implémentation des autorisations. Par exemple, si vous souhaitez autoriser une fonction Lambda L2 à accéder à un compartiment L2 S3, vous pouvez `s3Bucket.grantReadWrite(lambdaFunction)` appeler au lieu de créer un nouveau rôle et une nouvelle politique.

Constructions L3

- Bien que les constructions L3 puissent être très pratiques lorsque vous souhaitez rendre vos piles plus réutilisables et personnalisables, nous vous recommandons de les utiliser avec précaution.

Déterminez le type de construction L3 dont vous avez besoin ou si vous avez vraiment besoin d'une construction L3 :

- Si vous n'interagissez pas directement avec les AWS ressources, il est souvent plus approprié de créer une classe d'assistance plutôt que d'étendre la `Construct` classe. Cela est dû au fait que la `Construct` classe effectue de nombreuses actions par défaut qui ne sont nécessaires que si vous interagissez directement avec AWS des ressources. Donc, si vous n'avez pas besoin que ces actions soient effectuées, il est plus efficace de les éviter.
- Si vous déterminez que la création d'une nouvelle construction L3 est appropriée, dans la plupart des cas, vous souhaitez étendre directement la `Construct` classe. Étendez les autres constructions L2 uniquement lorsque vous souhaitez mettre à jour les propriétés par défaut de la construction. Si d'autres constructions L2 ou une logique personnalisée sont impliquées, étendez `Construct` directement et instanciez toutes les ressources du constructeur.

FAQ

Ne puis-je pas utiliser les couches AWS CDK sans comprendre les couches ?

Tu peux absolument le faire. Mais comme c'est le cas pour les outils les plus puissants, ils le AWS CDK deviennent au fur et à mesure que vous en savez. L'apprentissage AWS CDK de la façon dont les couches interagissent ouvre un nouveau niveau de compréhension qui permet de simplifier vos déploiements de stack bien au-delà de ce que vous pouvez faire avec de simples connaissances de base AWS CDK .

Puis-je créer des constructions L2 à partir de L1 de la même manière que je crée des constructions L3 à partir de L2 ?

Si une ressource possède déjà une construction L2, nous vous recommandons d'utiliser cette construction et d'effectuer vos personnalisations dans la couche 3. En effet, de nombreuses recherches ont déjà été menées pour déterminer les meilleurs moyens de configurer les constructions L2 existantes pour une ressource particulière. Cependant, il existe plusieurs constructions L1 dont les constructions L2 n'existent pas encore. Dans ces cas, nous vous encourageons à créer vos propres constructions L2 et à les partager avec d'autres en devenant contributeur à la bibliothèque AWS CDK open source. Vous trouverez tout ce dont vous avez besoin pour commencer dans les [directives de contribution](#) du AWS CDK.

Quelles AWS ressources n'ont pas encore de constructions L2 officielles ?

[Le nombre de AWS ressources qui n'ont pas de construction L2 diminue de jour en jour, mais si vous souhaitez participer à la création d'une construction L2 pour l'une de ces ressources, consultez la AWS CDK référence des API.](#) Consultez la liste des ressources dans le volet de gauche. Les ressources dont le nom est indiqué en exposant 1 n'ont pas de construction L2 officielle.

Puis-je créer une construction L2 ou L3 dans n'importe quelle langue prise en charge ? AWS CDK

Il AWS CDK prend en charge plusieurs langages de programmation TypeScript JavaScript, notamment Python, Java, C# et Go. Vous pouvez créer vos propres constructions L3 en utilisant le AWS CDK code compilé dans le langage approprié. Toutefois, si vous souhaitez contribuer AWS CDK ou créer des AWS CDK constructions natives, vous devez utiliser TypeScript. C' TypeScript est parce que c'est la seule langue native du AWS CDK. Les AWS CDK versions pour les autres langues sont créées à partir du TypeScript code natif à l'aide d'une AWS bibliothèque appelée [JSii](#).

Où puis-je trouver les constructions L3 existantes en dehors du ? AWS CDK

Il y a trop d'emplacements à partager ici, mais vous pouvez trouver la plupart des constructions les plus populaires sur le site Web de [AWS Solutions Constructs](#) et dans la AWS CDK section du [Construct Hub](#).

Ressources

- [AWS CDK Référence API](#)
- [AWS CloudFormation spécification des ressources](#)
- [AWS CDK construit de la documentation](#)
- [AWS CDK abstractions et trappes d'évacuation](#)
- [Tirez parti des structures L2 pour réduire la complexité de votre AWS CDK application](#) (AWS article de blog)
- [AWS CloudFormation ressources personnalisées](#)
- [AWS Solutions et constructions](#)
- [Construire un hub](#)
- [AWS CDK Exemples](#) (GitHub référentiel)

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	—	4 décembre 2023

AWS Glossaire des directives prescriptives

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

Nombres

7 R

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

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

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

A

ABAC

Voir contrôle [d'accès basé sur les attributs](#).

services abstraits

Consultez la section [Services gérés](#).

ACIDE

Voir [atomicité, consistance, isolation, durabilité](#).

migration active-active

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

migration active-passive

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

fonction d'agrégation

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

AI

Voir [intelligence artificielle](#).

AIOps

Voir les [opérations d'intelligence artificielle](#).

anonymisation

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

anti-motif

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

contrôle des applications

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

portefeuille d'applications

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

intelligence artificielle (IA)

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

opérations d'intelligence artificielle (AIOps)

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

chiffrement asymétrique

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

atomicité, cohérence, isolement, durabilité (ACID)

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

contrôle d'accès par attributs (ABAC)

Pratique qui consiste à créer des autorisations détaillées en fonction des attributs de l'utilisateur, tels que le service, le poste et le nom de l'équipe. Pour plus d'informations, consultez [ABAC pour AWS](#) dans la documentation Gestion des identités et des accès AWS (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'une Région AWS réseau isolé des défaillances dans d'autres zones de disponibilité et fournissant une connectivité réseau peu coûteuse et à faible latence aux autres zones de disponibilité de la même région.

AWS Cadre d'adoption du cloud (AWS CAF)

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

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

Outil qui évalue les charges de travail liées à la migration des bases de données, recommande des stratégies de migration et fournit des estimations de travail. AWS Le WQF est inclus avec

AWS Schema Conversion Tool (AWS SCT). Il analyse les schémas de base de données et les objets de code, le code d'application, les dépendances et les caractéristiques de performance, et fournit des rapports d'évaluation.

B

mauvais bot

Un [bot](#) destiné à perturber ou à nuire à des individus ou à des organisations.

BCP

Consultez la section [Planification de la continuité des activités](#).

graphique de comportement

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

système de poids fort

Système qui stocke d'abord l'octet le plus significatif. Voir aussi [endianité](#).

classification binaire

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

filtre de Bloom

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

déploiement bleu/vert

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

bot

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

botnet

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

branche

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

accès par brise-vitre

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

stratégie existante (brownfield)

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

cache de tampon

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

capacité métier

Ce que fait une entreprise pour générer de la valeur (par exemple, les ventes, le service client ou le marketing). Les architectures de microservices et les décisions de développement

peuvent être dictées par les capacités métier. Pour plus d'informations, veuillez consulter la section [Organisation en fonction des capacités métier](#) du livre blanc [Exécution de microservices conteneurisés sur AWS](#).

planification de la continuité des activités (BCP)

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

C

CAF

Voir le [cadre d'adoption du AWS cloud](#).

déploiement de Canary

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

CCo E

Voir [le Centre d'excellence du cloud](#).

CDC

Voir [capture des données de modification](#).

capture des données de modification (CDC)

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

ingénierie du chaos

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

CI/CD

Découvrez [l'intégration continue et la livraison continue](#).

classification

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

chiffrement côté client

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

Centre d'excellence du cloud (CCoE)

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

cloud computing

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

modèle d'exploitation du cloud

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

étapes d'adoption du cloud

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

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

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

CMDB

Consultez la base de [données de gestion des configurations](#).

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 Bitbucket Cloud. Chaque version du code est appelée branche. Dans une structure de microservice, chaque référentiel est consacré à une seule fonctionnalité. Un seul pipeline CI/CD peut utiliser plusieurs référentiels.

cache passif

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

données gelées

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

vision par ordinateur (CV)

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

dérive de configuration

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

base de données de gestion des configurations (CMDB)

Référentiel qui stocke et gère les informations relatives à une base de données et à son environnement informatique, y compris les composants matériels et logiciels ainsi que leurs

configurations. Vous utilisez généralement les données d'une CMDB lors de la phase de découverte et d'analyse du portefeuille de la migration.

pack de conformité

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

intégration continue et livraison continue (CI/CD)

Processus d'automatisation des étapes de source, de construction, de test, de préparation et de production du processus de publication du logiciel. CI/CD est communément décrit comme un pipeline. CI/CD peut vous aider à automatiser les processus, à améliorer la productivité, à améliorer la qualité du code et à accélérer les livraisons. Pour plus d'informations, veuillez consulter [Avantages de la livraison continue](#). CD peut également signifier déploiement continu. Pour plus d'informations, veuillez consulter [Livraison continue et déploiement continu](#).

CV

Voir [vision par ordinateur](#).

D

données au repos

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

classification des données

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

dérive des données

Une variation significative entre les données de production et les données utilisées pour entraîner un modèle ML, ou une modification significative des données d'entrée au fil du temps. La dérive

des données peut réduire la qualité, la précision et l'équité globales des prédictions des modèles ML.

données en transit

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

maillage de données

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

minimisation des données

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

périmètre de données

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

prétraitement des données

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

provenance des données

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

sujet des données

Personne dont les données sont collectées et traitées.

entrepôt des données

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

langage de définition de base de données (DDL)

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

langage de manipulation de base de données (DML)

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

DDL

Voir [langage de définition de base](#) de données.

ensemble profond

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

deep learning

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

defense-in-depth

Approche de la sécurité de l'information dans laquelle une série de mécanismes et de contrôles de sécurité sont judicieusement répartis sur l'ensemble d'un réseau informatique afin de protéger la confidentialité, l'intégrité et la disponibilité du réseau et des données qu'il contient. Lorsque vous adoptez cette stratégie AWS, vous ajoutez plusieurs contrôles à différentes couches de la AWS Organizations structure afin de sécuriser les ressources. Par exemple, une defense-in-depth approche peut combiner l'authentification multifactorielle, la segmentation du réseau et le chiffrement.

administrateur délégué

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

déploiement

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

environnement de développement

Voir [environnement](#).

contrôle de détection

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

cartographie de la chaîne de valeur du développement (DVSM)

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

jumeau numérique

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

tableau des dimensions

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

catastrophe

Un événement qui empêche une charge de travail ou un système d'atteindre ses objectifs commerciaux sur son site de déploiement principal. Ces événements peuvent être des

catastrophes naturelles, des défaillances techniques ou le résultat d'actions humaines, telles qu'une mauvaise configuration involontaire ou une attaque de logiciel malveillant.

reprise après sinistre (DR)

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

DML

Voir [langage de manipulation de base](#) de données.

conception axée sur le domaine

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

DR

Voir [reprise après sinistre](#).

détection de dérive

Suivi des écarts par rapport à une configuration de référence. Par exemple, vous pouvez l'utiliser AWS CloudFormation pour [détecter la dérive des ressources du système](#) ou AWS Control Tower pour [détecter les modifications de votre zone d'atterrissage](#) susceptibles d'affecter le respect des exigences de gouvernance.

DVSM

Voir la [cartographie de la chaîne de valeur du développement](#).

E

EDA

Voir [analyse exploratoire des données](#).

EDI

Voir échange [de données informatisé](#).

informatique de périphérie

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

échange de données informatisé (EDI)

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

chiffrement

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

clé de chiffrement

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

endianisme

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

point de terminaison

Voir [point de terminaison de service](#).

service de point de terminaison

Service que vous pouvez héberger sur un cloud privé virtuel (VPC) pour le partager avec d'autres utilisateurs. Vous pouvez créer un service de point de terminaison avec AWS PrivateLink et accorder des autorisations à d'autres Comptes AWS ou à Gestion des identités et des accès AWS (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).

environnement

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

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

épopée

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

ERP

Voir [Planification des ressources d'entreprise](#).

analyse exploratoire des données (EDA)

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

F

tableau des faits

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

échouer rapidement

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

limite d'isolation des défauts

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

branche de fonctionnalités

Voir [succursale](#).

fonctionnalités

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

importance des fonctionnalités

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

transformation de fonctionnalité

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

invitation en quelques coups

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

FGAC

Découvrez le [contrôle d'accès détaillé](#).

contrôle d'accès détaillé (FGAC)

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

migration instantanée (flash-cut)

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

FM

Voir le [modèle de fondation](#).

modèle de fondation (FM)

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

G

IA générative

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

blocage géographique

Voir les [restrictions géographiques](#).

restrictions géographiques (blocage géographique)

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

Flux de travail Gitflow

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

image dorée

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

stratégie inédite

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

barrière de protection

Règle de haut niveau qui permet de régir les ressources, les politiques et la conformité au sein des unités organisationnelles (OUs). Les barrières de protection préventives appliquent des politiques pour garantir l'alignement sur les normes de conformité. Elles sont mises en œuvre à l'aide de politiques de contrôle des services et de limites des autorisations IAM. Les barrières de protection de détection détectent les violations des politiques et les problèmes de conformité, et génèrent des alertes pour y remédier. Ils sont implémentés à l'aide d'Amazon AWS Config AWS Security Hub CSPM GuardDuty AWS Trusted Advisor, d'Amazon Inspector et de AWS Lambda contrôles personnalisés.

H

HA

Découvrez [la haute disponibilité](#).

migration de base de données hétérogène

Migration de votre base de données source vers une base de données cible qui utilise un moteur de base de données différent (par exemple, Oracle vers Amazon Aurora). La migration hétérogène fait généralement partie d'un effort de réarchitecture, et la conversion du schéma peut s'avérer une tâche complexe. [AWS propose AWS SCT](#) qui facilite les conversions de schémas.

haute disponibilité (HA)

Capacité d'une charge de travail à fonctionner en continu, sans intervention, en cas de difficultés ou de catastrophes. Les systèmes HA sont conçus pour basculer automatiquement, fournir constamment des performances de haute qualité et gérer différentes charges et défaillances avec un impact minimal sur les performances.

modernisation des historiens

Approche utilisée pour moderniser et mettre à niveau les systèmes de technologie opérationnelle (OT) afin de mieux répondre aux besoins de l'industrie manufacturière. Un historien est un type de base de données utilisé pour collecter et stocker des données provenant de diverses sources dans une usine.

données de rétention

Partie de données historiques étiquetées qui n'est pas divulguée dans un ensemble de données utilisé pour entraîner un modèle d'[apprentissage automatique](#). Vous pouvez utiliser les données de blocage pour évaluer les performances du modèle en comparant les prévisions du modèle aux données de blocage.

migration de base de données homogène

Migration de votre base de données source vers une base de données cible qui partage le même moteur de base de données (par exemple, Microsoft SQL Server vers Amazon RDS for SQL Server). La migration homogène s'inscrit généralement dans le cadre d'un effort de réhébergement ou de replateforme. Vous pouvez utiliser les utilitaires de base de données natifs pour migrer le schéma.

données chaudes

Données fréquemment consultées, telles que les données en temps réel ou les données translationnelles récentes. Ces données nécessitent généralement un niveau ou une classe de stockage à hautes performances pour fournir des réponses rapides aux requêtes.

correctif

Solution d'urgence à un problème critique dans un environnement de production. En raison de son urgence, un correctif est généralement créé en dehors du flux de travail de DevOps publication habituel.

période de soins intensifs

Immédiatement après le basculement, période pendant laquelle une équipe de migration gère et surveille les applications migrées dans le cloud afin de résoudre les problèmes éventuels. En règle générale, cette période dure de 1 à 4 jours. À la fin de la période de soins intensifs, l'équipe de migration transfère généralement la responsabilité des applications à l'équipe des opérations cloud.

I

laC

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.

Ilo T

Voir [Internet industriel des objets](#).

infrastructure immuable

Modèle qui déploie une nouvelle infrastructure pour les charges de travail de production au lieu de mettre à jour, d'appliquer des correctifs ou de modifier l'infrastructure existante. Les infrastructures immuables sont intrinsèquement plus cohérentes, fiables et prévisibles que les infrastructures [mutables](#). Pour plus d'informations, consultez les meilleures pratiques de [déploiement à l'aide d'une infrastructure immuable](#) dans le AWS Well-Architected Framework.

VPC entrant (d'entrée)

Dans une architecture AWS multi-comptes, un VPC qui accepte, inspecte et achemine les connexions réseau depuis l'extérieur d'une application. L'[architecture AWS de référence de sécurité](#) recommande de configurer votre compte réseau avec les fonctions entrantes, sortantes et d'inspection VPCs afin de protéger l'interface bidirectionnelle entre votre application et l'Internet en général.

migration incrémentielle

Stratégie de basculement dans le cadre de laquelle vous migrez votre application par petites parties au lieu d'effectuer un basculement complet unique. Par exemple, il se peut que vous ne transfériez que quelques microservices ou utilisateurs vers le nouveau système dans un premier temps. Après avoir vérifié que tout fonctionne correctement, vous pouvez transférer

I

progressivement des microservices ou des utilisateurs supplémentaires jusqu'à ce que vous puissiez mettre hors service votre système hérité. Cette stratégie réduit les risques associés aux migrations de grande ampleur.

Industry 4.0

Terme introduit par [Klaus Schwab](#) en 2016 pour désigner la modernisation des processus de fabrication grâce aux avancées en matière de connectivité, de données en temps réel, d'automatisation, d'analyse et d'IA/ML.

infrastructure

Ensemble des ressources et des actifs contenus dans l'environnement d'une application.

infrastructure en tant que code (IaC)

Processus de mise en service et de gestion de l'infrastructure d'une application via un ensemble de fichiers de configuration. IaC est conçue pour vous aider à centraliser la gestion de l'infrastructure, à normaliser les ressources et à mettre à l'échelle rapidement afin que les nouveaux environnements soient reproductibles, fiables et cohérents.

Internet industriel des objets (IIoT)

L'utilisation de capteurs et d'appareils connectés à Internet dans les secteurs industriels tels que la fabrication, l'énergie, l'automobile, les soins de santé, les sciences de la vie et l'agriculture. Pour plus d'informations, voir [Élaboration d'une stratégie de transformation numérique de l'Internet des objets \(IIoT\) industriel](#).

VPC d'inspection

Dans une architecture AWS multi-comptes, un VPC centralisé qui gère les inspections du trafic réseau VPCs entre (identique ou Régions AWS différent), Internet et les réseaux locaux. L'[architecture AWS de référence de sécurité](#) recommande de configurer votre compte réseau avec les fonctions entrantes, sortantes et d'inspection VPCs afin de protéger l'interface bidirectionnelle entre votre application et l'Internet en général.

Internet des objets (IoT)

Réseau d'objets physiques connectés dotés de capteurs ou de processeurs intégrés qui communiquent avec d'autres appareils et systèmes via Internet ou via un réseau de communication local. Pour plus d'informations, veuillez consulter la section [Qu'est-ce que l'IoT ?](#).

interprétabilité

Caractéristique d'un modèle de machine learning qui décrit dans quelle mesure un être humain peut comprendre comment les prédictions du modèle dépendent de ses entrées. Pour plus d'informations, voir [Interprétabilité du modèle d'apprentissage automatique avec AWS](#).

IoT

Voir [Internet des objets](#).

Bibliothèque d'informations informatiques (ITIL)

Ensemble de bonnes pratiques pour proposer des services informatiques et les aligner sur les exigences métier. L'ITIL constitue la base de l'ITSM.

gestion des services informatiques (ITSM)

Activités associées à la conception, à la mise en œuvre, à la gestion et à la prise en charge de services informatiques d'une organisation. Pour plus d'informations sur l'intégration des opérations cloud aux outils ITSM, veuillez consulter le [guide d'intégration des opérations](#).

ITIL

Consultez la [bibliothèque d'informations informatiques](#).

ITSM

Voir [Gestion des services informatiques](#).

L

contrôle d'accès basé sur des étiquettes (LBAC)

Une implémentation du contrôle d'accès obligatoire (MAC) dans laquelle une valeur d'étiquette de sécurité est explicitement attribuée aux utilisateurs et aux données elles-mêmes. L'intersection entre l'étiquette de sécurité utilisateur et l'étiquette de sécurité des données détermine les lignes et les colonnes visibles par l'utilisateur.

zone de destination

Une zone d'atterrissage est un AWS environnement multi-comptes bien conçu, évolutif et sécurisé. Il s'agit d'un point de départ à partir duquel vos entreprises peuvent rapidement lancer et déployer des charges de travail et des applications en toute confiance dans leur environnement de sécurité et d'infrastructure. Pour plus d'informations sur les zones de destination, veuillez consulter [Setting up a secure and scalable multi-account AWS environment](#).

grand modèle de langage (LLM)

Un modèle d'[intelligence artificielle basé](#) sur le deep learning qui est préentraîné sur une grande quantité de données. Un LLM peut effectuer plusieurs tâches, telles que répondre à des questions, résumer des documents, traduire du texte dans d'autres langues et compléter des phrases. Pour plus d'informations, voir [Que sont LLMs](#).

migration de grande envergure

Migration de 300 serveurs ou plus.

LBAC

Voir contrôle d'[accès basé sur des étiquettes](#).

principe de moindre privilège

Bonne pratique de sécurité qui consiste à accorder les autorisations minimales nécessaires à l'exécution d'une tâche. Pour plus d'informations, veuillez consulter la rubrique [Accorder les autorisations de moindre privilège](#) dans la documentation IAM.

lift and shift

Voir [7 Rs](#).

système de poids faible

Système qui stocke d'abord l'octet le moins significatif. Voir aussi [endianité](#).

LLM

Voir le [grand modèle de langage](#).

environnements inférieurs

Voir [environnement](#).

M

machine learning (ML)

Type d'intelligence artificielle qui utilise des algorithmes et des techniques pour la reconnaissance et l'apprentissage de modèles. Le ML analyse et apprend à partir de données enregistrées, telles que les données de l'Internet des objets (IoT), pour générer un modèle statistique basé sur des modèles. Pour plus d'informations, veuillez consulter [Machine Learning](#).

branche principale

Voir [succursale](#).

malware

Logiciel conçu pour compromettre la sécurité ou la confidentialité de l'ordinateur. Les logiciels malveillants peuvent perturber les systèmes informatiques, divulguer des informations sensibles ou obtenir un accès non autorisé. Parmi les malwares, on peut citer les virus, les vers, les rançongiciels, les chevaux de Troie, les logiciels espions et les enregistreurs de frappe.

services gérés

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

système d'exécution de la fabrication (MES)

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

MAP

Voir [Migration Acceleration Program](#).

mécanisme

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

compte membre

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

MAILLES

Voir le [système d'exécution de la fabrication](#).

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

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

microservice

Un petit service indépendant qui communique via un réseau bien défini APIs et qui est généralement détenu par de petites équipes autonomes. Par exemple, un système d'assurance peut inclure des microservices qui mappent à des capacités métier, telles que les ventes ou le marketing, ou à des sous-domaines, tels que les achats, les réclamations ou l'analytique. Les avantages des microservices incluent l'agilité, la flexibilité de la mise à l'échelle, la facilité de déploiement, la réutilisation du code et la résilience. Pour plus d'informations, consultez la section [Intégration de microservices à l'aide de services AWS sans serveur](#).

architecture de microservices

Approche de création d'une application avec des composants indépendants qui exécutent chaque processus d'application en tant que microservice. Ces microservices communiquent via une interface bien définie en utilisant Lightweight. APIs Chaque microservice de cette architecture peut être mis à jour, déployé et mis à l'échelle pour répondre à la demande de fonctions spécifiques d'une application. Pour plus d'informations, consultez la section [Implémentation de microservices sur AWS](#).

Programme d'accélération des migrations (MAP)

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

migration à grande échelle

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

usine de migration

Équipes interfonctionnelles qui rationalisent la migration des charges de travail grâce à des approches automatisées et agiles. Les équipes de Migration Factory comprennent généralement des responsables des opérations, des analystes commerciaux et des propriétaires, des ingénieurs de migration, des développeurs et DevOps des professionnels travaillant dans le cadre de sprints.

Entre 20 et 50 % du portefeuille d'applications d'entreprise est constitué de modèles répétés qui peuvent être optimisés par une approche d'usine. Pour plus d'informations, veuillez consulter la rubrique [discussion of migration factories](#) et le [guide Cloud Migration Factory](#) dans cet ensemble de contenus.

métadonnées de migration

Informations relatives à l'application et au serveur nécessaires pour finaliser la migration.

Chaque modèle de migration nécessite un ensemble de métadonnées de migration différent. Les exemples de métadonnées de migration incluent le sous-réseau cible, le groupe de sécurité et le AWS compte.

modèle de migration

Tâche de migration reproductible qui détaille la stratégie de migration, la destination de la migration et l'application ou le service de migration utilisé. Exemple : réorganisez la migration vers Amazon EC2 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, à évaluer, à prévenir ou à 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 peuvent accéder au contenu d'un compartiment S3 uniquement via une distribution spécifique CloudFront . Voir également [OAC](#), qui fournit un contrôle d'accès plus précis et amélioré.

ORR

Voir l'[examen de l'état de préparation opérationnelle](#).

DE

Voir [technologie opérationnelle](#).

VPC sortant (de sortie)

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

P

limite des autorisations

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

informations personnelles identifiables (PII)

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

PII

Voir les [informations personnelles identifiables](#).

manuel stratégique

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

PLC

Voir [contrôleur logique programmable](#).

PLM

Consultez la section [Gestion du cycle de vie des produits](#).

policy

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.

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

zones hébergées privées

Conteneur contenant des informations sur la manière dont vous souhaitez qu'Amazon Route 53 réponde aux requêtes DNS pour un domaine et ses sous-domaines au sein d'un ou de plusieurs VPCs domaines. Pour plus d'informations, veuillez consulter [Working with private hosted zones](#) dans la documentation Route 53.

contrôle proactif

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

gestion du cycle de vie des produits (PLM)

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

environnement de production

Voir [environnement](#).

contrôleur logique programmable (PLC)

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

chaînage rapide

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

pseudonymisation

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

publish/subscribe (pub/sub)

Modèle qui permet les 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 \(RACI\)](#).

RAG

Voir [Retrieval Augmented Generation](#).

rançongiciel

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

Matrice RASCI

Voir [responsable, responsable, consulté, informé \(RACI\)](#).

RCAC

Voir [contrôle d'accès aux lignes et aux colonnes](#).

réplica en lecture

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

réarchitecte

Voir [7 Rs](#).

objectif de point de récupération (RPO)

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

objectif de temps de récupération (RTO)

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

refactoriser

Voir [7 Rs](#).

Région

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

régression

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

réhéberger

Voir [7 Rs](#).

version

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

déplacer

Voir [7 Rs](#).

replateforme

Voir [7 Rs](#).

rachat

Voir [7 Rs](#).

résilience

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

politique basée sur les ressources

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

matrice responsable, redevable, consulté et informé (RACI)

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

contrôle réactif

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

retain

Voir [7 Rs](#).

se retirer

Voir [7 Rs](#).

Génération augmentée de récupération (RAG)

Technologie d'[IA générative](#) dans laquelle un [LLM](#) fait référence à une source de données faisant autorité qui se trouve en dehors de ses sources de données de formation avant de générer une réponse. Par exemple, un modèle RAG peut effectuer une recherche sémantique dans la base de connaissances ou dans les données personnalisées d'une organisation. Pour plus d'informations, voir [Qu'est-ce que RAG ?](#)

rotation

Processus de mise à jour périodique d'un [secret](#) pour empêcher un attaquant d'accéder aux informations d'identification.

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

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

RPO

Voir l'[objectif du point de récupération](#).

RTO

Voir l'[objectif 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 de l' AWS API sans que vous ayez à créer un utilisateur dans IAM pour tous les membres de votre organisation. Pour plus d'informations sur la fédération SAML 2.0, veuillez consulter [À propos de la fédération SAML 2.0](#) dans la documentation IAM.

SCADA

Voir [Contrôle de supervision et acquisition de données](#).

SCP

Voir la [politique de contrôle des services](#).

secret

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

sécurité dès la conception

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

contrôle de sécurité

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

renforcement de la sécurité

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

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

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

automatisation des réponses de sécurité

Action prédéfinie et programmée conçue pour répondre automatiquement à un événement de sécurité ou y remédier. Ces automatisations servent de contrôles de sécurité [détectifs ou réactifs](#) qui vous aident à mettre en œuvre les meilleures pratiques en matière 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 fournit un contrôle centralisé des autorisations pour tous les comptes d'une organisation dans AWS Organizations. SCPs définissent des garde-fous ou des limites aux actions qu'un administrateur peut déléguer à des utilisateurs ou à des rôles. Vous pouvez les utiliser SCPs comme listes d'autorisation ou de refus pour spécifier les services ou les actions autorisés ou interdits. Pour plus d'informations, consultez la section [Politiques de contrôle des services](#) dans la AWS Organizations documentation.

point de terminaison du service

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

contrat de niveau de service (SLA)

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

indicateur de niveau de service (SLI)

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

objectif de niveau de service (SLO)

Mesure cible qui représente l'état d'un service, tel que mesuré par un indicateur de [niveau de service](#).

modèle de responsabilité partagée

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

SIEM

Consultez les [informations de sécurité et le système de gestion des événements](#).

point de défaillance unique (SPOF)

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

SLA

Voir le contrat [de niveau de service](#).

SLI

Voir l'indicateur de [niveau de service](#).

SLO

Voir l'objectif de [niveau de service](#).

split-and-seed modèle

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

SPOF

Voir [point de défaillance unique](#).

schéma en étoile

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

modèle de figuier étrangleur

Approche de modernisation des systèmes monolithiques en réécrivant et en remplaçant progressivement les fonctionnalités du système jusqu'à ce que le système hérité puisse être mis hors service. Ce modèle utilise l'analogie d'un figuier de vigne qui se développe dans un arbre existant et qui finit par supplanter son hôte. Le schéma a été [présenté par Martin Fowler](#) comme un moyen de gérer les risques lors de la réécriture de systèmes monolithiques. Pour obtenir un exemple d'application de ce modèle, veuillez consulter [Modernizing legacy Microsoft ASP.NET \(ASMX\) web services incrementally by using containers and Amazon API Gateway](#).

sous-réseau

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

contrôle de supervision et acquisition de données (SCADA)

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

chiffrement symétrique

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

tests synthétiques

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

invite du système

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

T

tags

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

variable cible

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

liste de tâches

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

environnement de test

Voir [environnement](#).

entraînement

Pour fournir des données à partir desquelles votre modèle de ML peut apprendre. Les données d'entraînement doivent contenir la bonne réponse. L'algorithme d'apprentissage identifie des modèles dans les données d'entraînement, qui mettent en correspondance les attributs des données d'entrée avec la cible (la réponse que vous souhaitez prédire). Il fournit un modèle de ML

qui capture ces modèles. Vous pouvez alors utiliser le modèle de ML pour obtenir des prédictions sur de nouvelles données pour lesquelles vous ne connaissez pas la cible.

passerelle de transit

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

flux de travail basé sur jonction

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

accès sécurisé

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

réglage

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

équipe de deux pizzas

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

U

incertitude

Un concept qui fait référence à des informations imprécises, incomplètes ou inconnues susceptibles de compromettre la fiabilité des modèles de ML prédictifs. Il existe deux types

d'incertitude : l'incertitude épistémique est causée par des données limitées et incomplètes, alors que l'incertitude aléatoire est causée par le bruit et le caractère aléatoire inhérents aux données. Pour plus d'informations, veuillez consulter le guide [Quantifying uncertainty in deep learning systems](#).

tâches indifférenciées

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

environnements supérieurs

Voir [environnement](#).

V

mise à vide

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

contrôle de version

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

Appairage de VPC

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

vulnérabilités

Défaut logiciel ou matériel qui compromet la sécurité du système.

W

cache actif

Cache tampon qui contient les données actuelles et pertinentes fréquemment consultées.

L'instance de base de données peut lire à partir du cache tampon, ce qui est plus rapide que la lecture à partir de la mémoire principale ou du disque.

données chaudes

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

fonction de fenêtre

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

charge de travail

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

flux de travail

Groupes fonctionnels d'un projet de migration chargés d'un ensemble de tâches spécifique. Chaque flux de travail est indépendant, mais prend en charge les autres flux de travail du projet. Par exemple, le flux de travail du portefeuille est chargé de prioriser les applications, de planifier les vagues et de collecter les métadonnées de migration. Le flux de travail du portefeuille fournit ces actifs au flux de travail de migration, qui migre ensuite les serveurs et les applications.

VER

Voir [écrire une fois, lire plusieurs](#).

WQF

Voir le [cadre AWS de qualification de la charge](#) de travail.

écrire une fois, lire plusieurs (WORM)

Modèle de stockage qui écrit les données une seule fois et empêche leur suppression ou leur modification. Les utilisateurs autorisés peuvent lire les données autant de fois que nécessaire,

mais ils ne peuvent pas les modifier. Cette infrastructure de stockage de données est considérée comme [immuable](#).

Z

exploit Zero-Day

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

vulnérabilité « jour zéro »

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

invite Zero-Shot

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

application zombie

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

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