Migration de serveurs locaux vers des réseaux privés AWS à l'aide de AWS Application Migration Service

AWS Conseils prescriptifs

AWS Conseils prescriptifs: Migration de serveurs locaux vers des réseaux privés AWS à l'aide de AWS Application Migration Service

Table of Contents

Migration de serveurs locaux vers desAWS réseaux privés à l'aide deAWS Application Migration Service

Mike Kuznetsov et Dipin Jain, Amazon Web Services (AWS)

Mars 2023 (historique du document)

De nombreuses entreprises migrentAWS vers des environnements réseau isolés ou semi-isolés tels que des centres de données sur site ou d'autres infrastructures cloud ou hybrides. Ces réseaux isolés n'autorisent généralement aucun trafic sortant vers des points de terminaison externes, ce qui est nécessaire pour la migration sur le réseau. D'autres entreprises autorisent le trafic de sortie HTTPS depuis leurs réseaux internes, mais n'autorisent pas les communications spécifiques sur les ports réseau requis par AWS Application Migration Service, qui sont les principauxAWS service pour les lift-and-shift migrations de grande envergure. Dans un troisième scénario, le trafic HTTPS est autorisé à la fois depuis les zones source et intermédiaire, mais le trafic de réplication des données doit passer par le canal privé pour des raisons de conformité.

Le service de migration des applications prend en charge ces cas d'utilisation et vous permet de migrer depuis des environnements isolés sécurisés en utilisant uniquement une connectivité réseau privé/public privé ou hybride. Ce guide décrit ces trois scénarios, qui vont des deux modèles hybrides public/privé au modèle totalement isolé, et se concentre sur les étapes détaillées et les exigences en matière d'infrastructure pour l'option réservée au secteur privé la plus restrictive. Il s'appuie sur le modèleAWS Prescriptive Guidance Connect to Application Migration Service, les données et les plans de contrôle via un réseau privé en fournissant :

- Informations supplémentaires sur la connectivité requise dans chaque scénario
- Explications desAWS ressources qui doivent être créées
- Options d'automatisation pour créer l'infrastructure de testAWS et la déployer pendant la phase de migration
- Options de surveillance et de résolution des problèmes de connectivité pour chaque cas d'utilisation

Pour plus d'informations sur le fonctionnement d'Application Migration Service, consultez les articles de blog suivants :

- Accélérez votre migration avecAWS Application Migration Service

- Comment utiliser le nouveauAWS Application Migration Service pour les migrations Lift-and-Shift

Scénarios

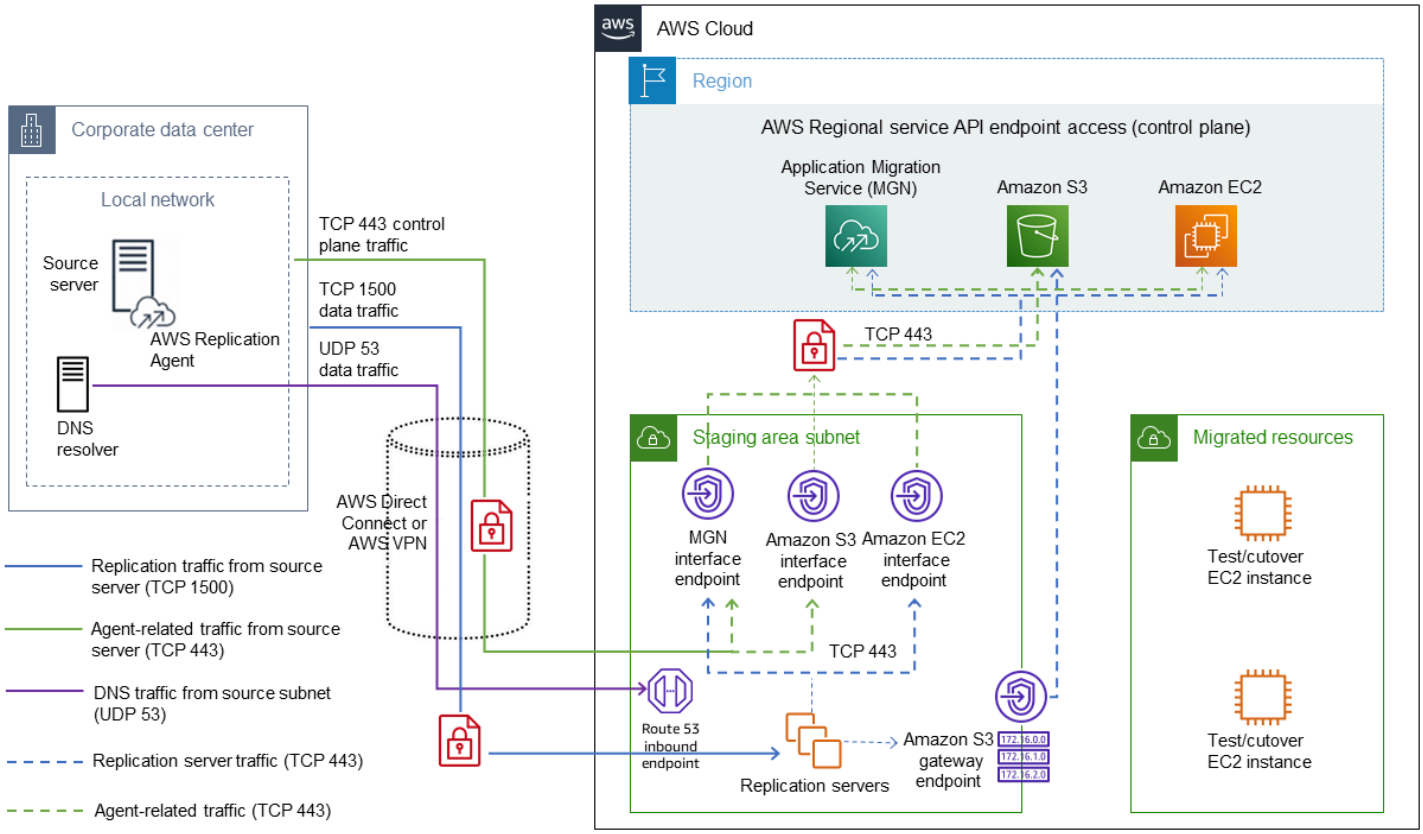
Ce guide décrit les composants d'infrastructure requis à créer pour terminer la migration selon les scénarios suivants :

- Réplication sur des réseaux privés uniquement, ce qui est le scénario le plus courant et le plus restrictif.
- Scénario hybride dans lequel la communication de sortie HTTPS est autorisée mais tout autre trafic est restreint. Ce scénario comprend deux options :
  - Sortie HTTPS publique à la source et ressources de la zone de transit privée
  - Sortie HTTPS publique à la source et ressources de la zone de transit publique

Pour chaque scénario, le guide fournit un exemple de configuration et la liste complète desAWS composants requis.

Réplication sur des réseaux privés uniquement

Le schéma suivant montre l'architecture du scénario le plus restrictif, dans lequel tout le trafic passe par le canal privé (AWS VPNouAWS Direct Connect) entre l'environnement source etAWS.



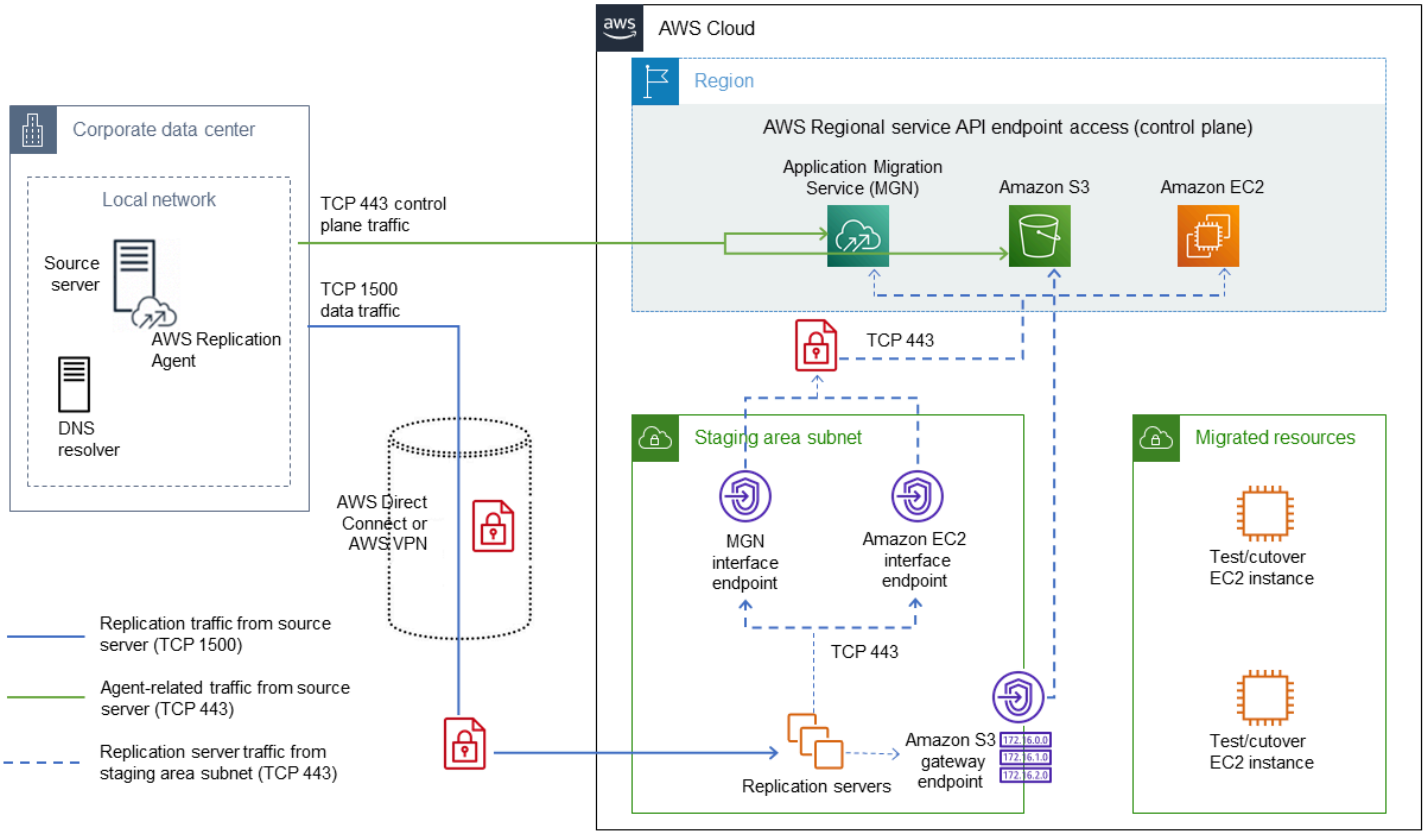
Les principaux composants de cette architecture sont les suivants :

- Environnement source dans le centre de données de l'entreprise (à gauche). Il s'agit de l'environnement à partir duquel migrer.
- Environnement intermédiaireAWS avec un cloud privé virtuel (VPC) et un sous-réseau (au milieu). Il s'agit de l'environnement que le Service de migration des applications utilisera pour créer des ressources liées à la réplication. Ces ressources peuvent inclure des serveurs de réplication, des serveurs de conversion et des volumes Amazon Elastic Block Store (Amazon EBS) associés et leurs instantanés Amazon Simple Storage Service (Amazon S3).
- Connexion VPN entre l'environnement source et le VPC intermédiaire et les sous-réseaux pour gérer trois types de trafic :
  - Port HTTPS/TCP 443 pour la communication avec l'API
  - Port TCP 1500 pour le transfert de données
  - Trafic du système de noms de domaine (DNS) via le port UDP 53

- Environnement cible dansAWS (à droite). Il peut s'agir d'un VPC complètement isolé ou d'un sous-réseau dans l'environnement intermédiaire. (Remarque : aucune connectivité réseau n'est requise entre le sous-réseau de l'environnement intermédiaire et les sous-réseaux cibles.)
- Points de terminaison d'interface Amazon VPC pour Application Migration Service, Amazon Elastic Compute Cloud (Amazon EC2) et Amazon S3 créés dans l'environnement intermédiaire, et point de terminaison de passerelle Amazon S3 VPC accessible depuis le sous-réseau intermédiaire.
- Enfin, le point de terminaison entrant du résolveur DNS dans le sous-réseau intermédiaire. Cela est nécessaire pour que les systèmes sources puissent convertir les noms de domaine complets (FQDN) des points de terminaison VPC en adresses IP privées.

Sortie HTTPS publique à la source et ressources de la zone de transit privée

Le schéma suivant illustre l'architecture du scénario hybride dans lequel le trafic de sortie HTTPS est autorisé depuis n'importe quel serveur source et est utilisé pour communiquer avec Application Migration Service et les points de terminaison Amazon S3, tandis que les données de réplication sur le port TCP 1500 passent par le canal privé (AWS VPNouAWS Direct Connect) entre l'environnement source etAWS.

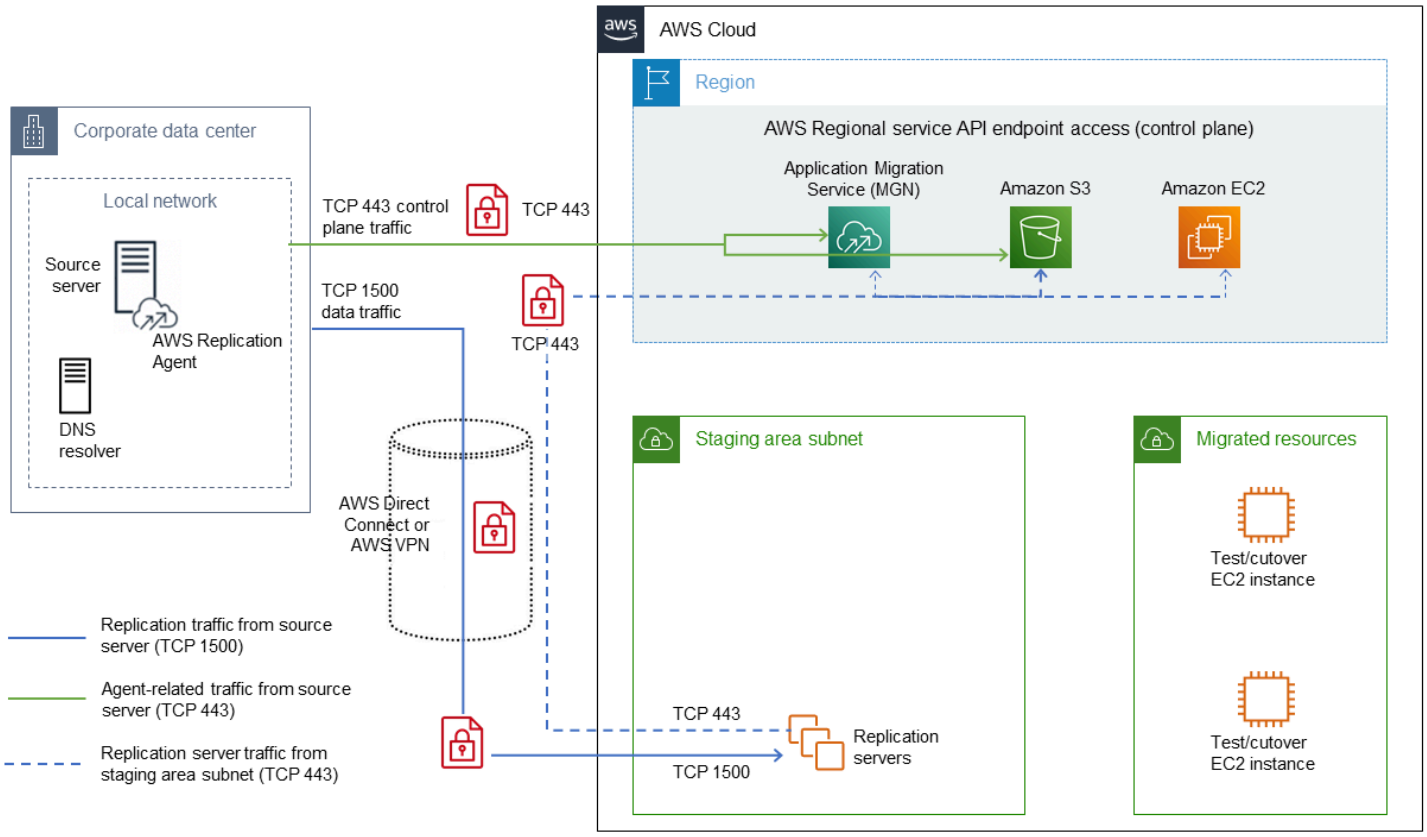


Cette architecture simplifie les exigences relatives au sous-réseau de la zone intermédiaire, car les communications HTTPS des agents ne transitent pas par le canal privé. En outre, il n'est pas nécessaire de créer des points de terminaison VPC supplémentaires pour l'interface Amazon S3 ou des points de terminaison de résolution entrant Amazon Route 53 pour le trafic DNS, car les serveurs sources utiliseront leurs serveurs DNS traditionnels pour résoudre les noms DNS publics standard d'Application Migration Service et des points de terminaison Amazon S3.

Toutefois, dans ce scénario, les ressources du sous-réseau de la zone de transit s'exécutent toujours sur un réseau privé et totalement isolé et n'ont aucun accès public à aucun point de terminaison HTTPS. Elles doivent donc créer à la fois des points de terminaison Application Migration Service et d'interface Amazon EC2 ainsi qu'un point de terminaison de passerelle Amazon S3.

Sortie HTTPS publique à la source et ressources de la zone de transit publique

Dans les cas où les ressources de la zone de transit ne doivent pas nécessairement se trouver sur un sous-réseau totalement isolé, vous pouvez utiliser l'alternative hybride présentée dans le schéma suivant.



Dans ce scénario, seul le trafic de réplication de données sur le port TCP 1500 passe par le canal privé. Le reste de la communication, à la fois depuis le sous-réseau source et le sous-réseau intermédiaire, s'effectue via le réseau public, vers des points de terminaison HTTPS publics standard.

Composants de l'architecture et exigences pour une réplication restreinte

Cette section fournit une description détaillée du scénario le plus restrictif, dans lequel toutes les communications se font uniquement via le canal privé, et inclut une explication détaillée des exigences et des composants correspondants à créer pour chaque zone.

Sous-réseau intermédiaire

Le sous-réseau intermédiaire est la partie la plus importante de l'infrastructure de réplication. C'est ici que tous les serveurs de réplication du service de migration des applications seront lancés, et il contient les adresses IP vers lesquelles le trafic de réplication sera dirigé. Pour la réplication des données privées entrantes, configurez les paramètres du serveur de réplication pour Application Migration Service à l'aide de l'option Utiliser une adresse IP privée.

Pour les besoins sortants, vous pouvez utiliser l'option Créer une adresse IP publique pour choisir si les serveurs de réplication communiqueront avec lesAWS services requis (Amazon S3, Application Migration Service, Amazon EC2) via une adresse IP privée ou publique. Les options standard pour fournir une connectivité Internet sortante sont répertoriées dans la documentation du service de migration des applications : adresse IP publique avec une passerelle Internet ou adresse IP privée avec une passerelle NAT. Les deux options vous permettent de mettre en œuvre un scénario hybride simplifié dans lequel le trafic de réplication de données passe par une connexion privée (AWS VPNouAWS Direct Connect) tandis que les serveurs de réplication communiquent avec lesAWS services via le réseau public.

Cependant, il est généralement interdit de disposer d'une connectivité sortante publique dans les environnements d'entreprise fermés. Il s'agit du scénario le plus restrictif décrit dans la section suivante. Dans ce cas, vous utilisezAWS PrivateLink et configurez les points de terminaison VPC suivants dans des sous-réseaux intermédiaires pour les serveurs de réplication :

- le point de terminaison de la passerelle VPC pour communiquer avec Amazon S3
- Points de terminaison de l'interface VPC pour communiquer avec Application Migration Service et Amazon EC2

Pour plus d'informations sur les points de terminaison VPC, consultez Appair VPC dans la AWS PrivateLinkdocumentation.

Sous-réseau source

Le sous-réseau source est n'importe quel sous-réseau à partir duquel vous effectuez une réplication. C'est ici que se trouvent vos serveurs sources et que vous allez installer l'agent deAWS réplication sur ces serveurs. La configuration réseau requise pour un agent est la suivante :

- Communiquer via le port HTTPS/TCP 443 avecAWS services notamment Amazon S3 et Application Migration Service
- Communication avec l'adresse IP du serveur de réplication (privée ou publique, en fonction de ses paramètres)

L'agent prend également en charge les scénarios hybrides dans lesquels la communicationAWS services peut se faire via le réseau public (à l'aide du trafic HTTPS standard) tandis que les données de réplication sont envoyées via des réseaux privés vers l'adresse IP privée du serveur de réplication.

Ce guide se concentre sur un scénario plus restrictif dans lequel même le trafic HTTPS en provenance des systèmes sourcesAWS services n'est pas autorisé. Les points de terminaison suivants sont donc configurés dans le sous-réseau intermédiaire :

- Points de terminaison d'interface VPC pour Application Migration Service et Amazon S3 (point de terminaison d'interface régional, et non le point de terminaison de passerelle requis pour les serveurs de réplication)
- Un point de terminaison de résolution DNS entrant, permettant aux sources locales et aux serveurs DNS de résoudre les adresses IP privées pour les points de terminaison VPC, situés dans le sous-réseau intermédiaire

le sous-réseau cible

Le sous-réseau cible est tout sous-réseau dans lequel vous prévoyez de lancer vos serveurs, y compris les instances de test et de transition. Ces sous-réseaux n'ont aucune exigence de connectivité réseau et peuvent être situés dans n'importe quel autre VPC de la mêmeCompte AWS région. En effet, Application Migration Service utilise les API Amazon EC2 pour créer de nouvelles instances de test ou de transfert (c'est pourquoi les serveurs de réplication du sous-réseau intermédiaire nécessitent une connectivité HTTPS sortante vers Amazon EC2) et accède aux instantanés S3 régionaux créés à partir de volumes EBS répliqués. Aucune de ces opérations ne

nécessite un accès direct au réseau depuis ou vers le sous-réseau cible. Il peut donc même s'agir d'un sous-réseau privé complètement isolé.

Toutefois, Application Migration Service installe également automatiquement plusieurs outils tels que EC2Config ouAWS Systems Manager des agents (agents SSM) sur des instances cibles, et ces activités nécessitent une connectivité sortante HTTPS/TCP port 443 à partir des instances et des sous-réseaux cibles.

Bonnes pratiques de configuration

Cette section fournit une description détaillée du scénario le plus restrictif, dans lequel toutes les communications se font uniquement via le canal privé, et inclut une explication détaillée des exigences et des composants correspondants à créer pour chaque zone.

Cette section décrit la configuration pour le scénario le plus restrictif (réplication sur des réseaux privés uniquement), comme indiqué dans le premier diagramme, sur la base des considérations évoquées précédemment. Vous pouvez configurer les deux scénarios hybrides en ignorant certaines parties de la configuration la plus restrictive :

- Pour le scénario hybride qui prend en charge la sortie HTTPS publique au niveau de la source et les ressources de la zone de transit privée, le point de terminaison VPC de l'interface Amazon S3 n'est pas requis.
- Dans le scénario hybride qui prend en charge la sortie HTTPS publique à la source et les ressources de la zone intermédiaire publique, aucun point de terminaison VPC dans le sous-réseau de la zone intermédiaire n'est requis.

Les sections suivantes supposent que la configuration initiale du service de migration des applications est déjà terminée, comme décrit dans les articles de blog (Accélérez votre migration avecAWS Application Migration Service et Comment utiliser le nouveauAWS Application Migration Service pour les migrations Lift-and-Shift). Cette discussion se concentre sur les composants spécifiques au scénario restrictif et suppose un sous-réseau intermédiaire privé qui n'est pas connecté à Internet.

Sous-réseaux et configurations de routage

Dans le scénario restrictif, vous configurez lesAWS ressources requises dans le sous-réseau privé d'un VPC intermédiaire. Ce sous-réseau n'est pas connecté à Internet (aucune passerelle Internet n'est connectée à la table de routage en tant que route par défaut). Au lieu de cela, il utilise soit une passerelle virtuelle associée à une AWS Site-to-Site VPNpasserelle (connectée via un tunnel IPsec à une passerelle sur site), soit il est connecté à une passerelle de transfert ou à desAWS Direct Connect services fournissant une interconnectivité privée aux centres de données locaux.

Vous utiliserez ce sous-réseau privé comme sous-réseau intermédiaire pour les ressources liées à la réplication gérées par Application Migration Service, et vous configurerez tous les accès réseau

requis via ce sous-réseau à l'aide de points de terminaison VPC, comme indiqué dans la section suivante.

VPC

Vous devez désormais créer des points de terminaison VPC dans le sous-réseau intermédiaire afin de fournir la connectivité aux serveurs de réplication et aux agents du service de migration d'applications à partir de sous-réseaux locaux.

Voici la liste complète des points de terminaison VPC dont vous avez besoin :

- Les points de terminaison d'interface Application Migration Service et Amazon EC2, qui fournissent leurs propres interfaces réseau élastiques avec des adresses IP privées et des noms DNS privés à utiliser à la fois par les serveurs de réplication et les agents. (Les agents utiliseront uniquement le point de terminaison du service de migration des applications.)
- Point de terminaison de passerelle Amazon S3 qui fournit un itinéraire spécifique dans la table de routage du sous-réseau (via une liste de préfixes). Il sera utilisé par les serveurs de réplication.
- Point de terminaison de l'interface Amazon S3 qui fournit une elastic network interface spécifique avec une adresse IP privée dédiée dans le sous-réseau privé. Les agents du service de migration des applications utiliseront cette adresse via un nom DNS spécifique.

Les sections suivantes décrivent plus en détail le fonctionnement des points de terminaison VPC. Le tableau suivant répertorie tous les points de terminaison créés pour le sous-réseau privé intermédiaire. (Notez qu'aucune interface réseau n'est configurée sur le point de terminaison de la passerelle Amazon S3, mais que des listes de préfixes spécifiques sont fournies dans la table de routage du sous-réseau, comme cela sera décrit plus loin dans ce guide.)

AWS service	VPC endpoint type	Private DNS	Related subnet
Amazon EC2	utilisateur	Activé	Mise en réseau privé
Application	utilisateur	Activé	Mise en réseau privé
Amazon S3	utilisateur	Non disponible	Mise en réseau privé

AWS service	VPC endpoint type	Private DNS	Related subnet
Amazon S3	Passerelle	Non disponible	Connect à la table de routage du sous-rése au privé intermédiaire

Vous pouvez créer des points de terminaison VPC facultatifs pour permettre l'accès aux instances EC2 sur des sous-réseaux privés isolés viaAWS Systems Manager, comme indiqué dans la section Création de points de terminaison VPC dans la documentation de Systems Manager.

AWS service	VPC endpoint type	Private DNS	Related subnet
Systems Manager	utilisateur	Activé	Mise en réseau privé
messages ssm	utilisateur	Activé	Mise en réseau privé
messages ec2	utilisateur	Activé	Mise en réseau privé
AWS Key Management Service (AWS KMS)	utilisateur	Activé	Mise en réseau privé
Journaux	utilisateur	Activé	Mise en réseau privé

Points de terminaison de l'interface d'un VPC

La création d'un point de terminaison d'interface crée également une elastic network interface spécifique pour chaque sous-réseau pour lequel le point de terminaison d'interface donné est provisionné. Par exemple, le point de terminaison de l'interface Application Migration Service est configuré dans un sous-réseau privé du VPC intermédiaire avec une elastic network interface associée à l'adresse IP au sein de ce sous-réseau, et il possède également trois noms DNS pouvant être résolus depuis le sous-réseau vers cette adresse IP :

- Un nom DNS privé,`mgn.<region>.amazonaws.com`
- Deux noms DNS basés sur l'ID du point de terminaison (`vpce-xxx`), avec et sans la région incluse dans le nom :`vpce-xxx-<region>.<service-name>` et`vpce-xxx.<service-name>`

Cela permet à toute instance exécutée dans le sous-réseau qui utilise la configuration définie par défaut du protocole DHCP (Dynamic Host Configuration Protocol) dans le VPC, et dont les attributsenableDnsHostnames DNS sontenableDnsSupport activés, de :

- Résolvez le nom DNS d'Application Migration Service (`mgn.<region>.amazonaws.com`) en une adresse IP privée attribuée à l'elastic network interface.
- Connect au service de migration des applications en utilisant le réseau local uniquement.

Cela corrige la connectivité de toutes les instances exécutées dans le sous-réseau intermédiaire (comme le serveur de réplication ou le serveur de conversion d'applications) pour toutes les instancesAWS service dont les points de terminaison d'interface sont provisionnés dans le sous-réseau (comme Amazon EC2, Application Migration ServiceAWS KMS, Systems Manager, etc.).

Points de terminaison d'un VPC

Pour des services tels qu'Amazon S3, aucun nom DNS fixe ne peut être provisionné car chaque compartiment possède son propre nom DNS. Pour ce scénario, vous utiliserez des points de terminaison de passerelle VPC.

La création d'un point de terminaison de passerelle Amazon S3 crée également un objet de liste de préfixes spécifique avec une liste de destinations de sous-réseau (en notation CIDR), qui peut être ajouté dans la table de routage des sous-réseaux. Ainsi, les noms DNS des compartiments S3 résolus en adresses IP incluses dans cette liste seraient accessibles via une connectivité interne.

Lorsque vous provisionnez un point de terminaison de passerelle Amazon S3, vous pouvez spécifier les sous-réseaux dans les tables de routage qui doivent inclure cet ID de liste de préfixes (`PL-<id>`). La table de routage résultante pour le sous-réseau privé intermédiaire doit inclure cet ID de liste de préfixes, comme dans cet exemple de table de routage :

Destination	Target
`pl-<id>`	`vpce-<id-of-S3-Gateway-VPC-endpoint>`
Toute autre route (par exemple, les CIDR du sous-réseau source)	Toutes les cibles telles que les identifiants de passerelle virtuelle

Destination	Target
CIdu du réseau local	`"local"`

Points de terminaison entrants du résolveur DNS

La configuration décrite dans la section précédente est suffisante pour les instances qui s'exécutent dans lesAWS sous-réseaux, car elles sont déjà configurées pour utiliser des serveurs DNS Amazon Route 53 internes. Toutefois, les serveurs sources locaux nécessitent des étapes supplémentaires pour pouvoir communiquerAWS services en privé. En particulier, Application Migration Service Agent doit télécharger le programme d'installation depuis Amazon S3, puis communiquer avec Application Migration Service en utilisant les noms DNS fournis dans la documentation. Les serveurs locaux utilisent leurs serveurs DNS par défaut pour résoudre ces noms DNS, ce qui génère des adresses IP publiques. Les communications avec ces adresses via le port HTTPS/TCP 443 sont finalement bloquées par les pare-feux de l'entreprise.

Pour éviter cela, vous devez configurer les serveurs sources ou leurs serveurs DNS par défaut à utiliser Amazon Route 53 Resolverpour la résolution de ces noms DNS spécifiques ou d'une zone de sous-domaine (c'est-à-dire la`*.<region>.amazonaws.com` zone complète). Cela peut être configuré en créant un point de terminaison entrant du résolveur Route 53 qui, comme un point de terminaison d'interface VPC, possède une elastic network interface dédiée créée dans le sous-réseau privé dédié surAWS, et est donc capable de transférer les demandes DNS versAmazon Route 53 Resolver.

Points de terminaison d'interface réseau réseau réseau réseau réseau

Chaque elastic network interface est associée à un groupe de sécurité dédié, qui doit autoriser le trafic attendu pour cette elastic network interface et le point de terminaison correspondant. Ainsi, le groupe de sécurité du point de terminaison du résolveur DNS doit autoriser le port UDP 53 entrant (et parfois le port TCP 53) pour les demandes DNS, et les groupes de sécurité du point de terminaison pour la plupart des autres services (Application Migration Service, Amazon EC2, Systems Manager, etc.) doivent être activés sur le port HTTPS/TCP 443 entrant.

Installation de l'agent Application Migration Service sur les serveurs sources

Pour installer Application Migration Service Agent sur des serveurs sources, vous devez fournir les noms DNS du service de migration des applications et des points de terminaison de l'interface Amazon S3 dans les paramètres de ligne de commande de l'agent (voir Installation de l'agent sur un réseau sécurisé dans la documentation du service de migration des applications).

Pour le point de terminaison du service de migration des applications, vous pouvez utiliser n'importe quel nom DNS qui lui est associé (un champ DNS privé (`mgn.<region>.amazonaws.com`) ou un nom DNS spécifique au VPC (`vpce-<VPC-id>-<suffix>.mgn.<region>.vpce.amazonaws.com`), et fournir un argument :`--endpoint <FQDN>`. En fait, si vous ignorez cet argument, l'agent utilise le nom de domaine spécifiéRégion AWS pour reconstruire le nom de domaine complet du DNS par défaut (`mgn.<region>.amazonaws.com`) et utilise le nom de domaine complet pour accéder au plan de contrôle du service de migration des applications. Dans la plupart des cas, ce comportement par défaut devrait suffire, à condition que le nom de domaine complet soit correctement transféré du serveur source à l'adresse IP privée de l'elastic network interface du point de terminaison VPC Application Migration Service créé dans le sous-réseau intermédiaire.

Le point de terminaison de l'interface Amazon S3 n'aura pas de nom DNS privé unique (car chaque compartiment S3 aura le sien). Cette option n'est donc pas prise en charge. Toutefois, un point de terminaison d'interface Amazon S3 est toujours associé à une elastic network interface. Il possède également une adresse IP privée spécifique et des noms DNS génériques (au format`.vpce-<VPC-ID>-<suffix>.s3.<region>.vpce.amazonaws.com` ou à la région). `vpce-<VPC-ID>-<suffix>-<region>.s3.<region>.vpce.amazonaws.com`) qui peuvent être résolus avec cette adresse IP privée.

Ce nom DNS générique peut être utilisé pour l'`--s3-endpoint`argument, comme suit :

```
aws-replication-installer-init.py --region <region> --aws-access-key-id
 <MGN_IAM_ACCESS_KEY>  --aws-secret-access-key <MGN_IAM_SECRET> --no-prompt \
   --endpoint vpce-<VPC-id>-<suffix>.mgn.<region>.vpce.amazonaws.com --s3-endpoint
 vpce-<VPC-ID>-<suffix>-<region>.s3.<region>.vpce.amazonaws.com
```

La section suivante fournit un exemple de configuration du service de migration d'applications, y compris tous les points de terminaison VPC requis, et de déploiement des agents à l'aide de points

de terminaison VPC sur des serveurs sources Windows et Linux. Cette section couvre à la fois le déploiement manuel et automatisé.

Déploiement de l'environnement PoC

De nombreux utilisateurs préfèrent tester minutieusement tous les canaux de communication et les étapes de migration à l'avance. Tester la migration à partir de réseaux isolés peut s'avérer difficile. Pour répondre à ce besoin,AWS propose deux options :

- Un CloudFormation modèle qui prépare toutes les ressources requises surAWS. Le modèle crée un environnement de preuve de concept (PoC) qui émule les composants de l'environnement du centre de données et configure l'AWSinfrastructure. Il inclut des VPC sources et cibles isolés, des sous-réseaux et des points de terminaison VPC.
- Un atelier dédié (Migrate the Well-Architected Way) contenant des step-by-step instructions détaillées pour créer votre environnement de test (voir l'étape Créer des points de terminaison VPC).

Vous pouvez également déployer votre environnement PoC en suivant les étapes décrites dans les sections suivantes.

Déploiement manuel

La liste suivante décrit les principales étapes des déploiements manuels dans votre environnement. Pour plus d'informations, consultez le modèle d'orientationAWS prescriptive Connect aux données et aux plans de contrôle du service de migration des applications via un réseau privé.

1. Créez le VPC source et le VPC de la zone de transit avec un sous-réseau privé.
2. Créez les points de terminaison VPC suivants dans le sous-réseau de la zone intermédiaire :
    - Service de migration des applications et activez le nom DNS privé (partagé par le serveur de réplication et le serveur source).
    - Amazon EC2, et activez le nom DNS privé (partagé par le serveur de réplication et le serveur source).
    - Amazon S3 (nom DNS privé non pris en charge). Les points de terminaison d'interface sont pris en charge via Direct Connect et le peering VPC.AWS VPN Par conséquent, cela n'est requis que pour les serveurs sources (et peuvent être situés sur site) pour se connecter au plan de contrôle du service de migration des applications via un réseau privé.

> **Note**
>
> Les points de terminaison ssm et ssmmessages sont facultatifs et sont actuellement créés pour connecter le serveur source via le gestionnaire de session SSM.

- Point de terminaison de la passerelle Amazon S3 dans le sous-réseau de la zone de transit. Ceci est requis par le serveur de réplication pour se connecter à Amazon S3. Vous devez mettre à jour les itinéraires pour le sous-réseau de la zone de transit.

3. Créez un point de terminaison de résolution entrant dans la zone intermédiaire VPC pour permettre la résolution de l'enregistrement DNS privé (pour les points de terminaison de l'interface VPC) à partir du VPC source.
4. Mettez à jour les options DHCP du VPC source avec le point de terminaison du résolveur entrant du VPC de la zone de transit en tant qu'adresse IP du serveur DNS.
5. Activez le peering entre le VPC source et le VPC intermédiaire, et mettez à jour les deux tables de routage des VPC.
6. Créez un groupe de sécurité dans les VPC source et intermédiaire pour autoriser les ports suivants.

Source	Destination	Port	Description
Centre de données source	URL des services Amazon S3	443 (TCP)	Communication via le port TCP 443
Centre de données source	Adresse de consoleRégion AWS spécifique au service de migration des applications	443 (TCP)	Communication entre les serveurs sources et le service de migration des applications via le port TCP 443
Centre de données source	Sous-réseau de la zone de transit	1500 (TCP)	Communication entre les serveurs source et le sous-réseau de la zone intermédiaire via le port TCP 1500

Source	Destination	Port	Description
Sous-réseau de la zone intermédiaire	Adresse de consoleRégion AWS spécifique au service de migration des applications	443 (TCP)	Communication entre le sous-réseau de la zone de transit et le service de migration des applications via le port TCP 443
Sous-réseau de la zone intermédiaire	URL des services Amazon S3	443 (TCP)	Communication via le port TCP 443
Sous-réseau de la zone intermédiaire	Point de terminais on Amazon EC2 de sonRégion AWS	443 (TCP)	Communication via le port TCP 443

7. Initialisez le service de migration des applications dans la zone intermédiaire enRégion AWS mettant à jour les détails du sous-réseau de la zone intermédiaire et en activant la communication via une adresse IP privée.
8. Créez un rôleAWS Identity and Access Management (IAM) pour installer Application Migration Service Agent. Attachez des politiques gérées et générez des clés d'accès et une clé secrète.
9. Créez un profil IAM pour connecter Amazon EC2 via le gestionnaire de session SSM.
10. Installez un agent sur les machines sources.

Automatiser les déploiements d'agents avec Cloud Migration Factory

La Cloud Migration Factory onAWS automatise le déploiement de l'agent de service de migration des applications pour le scénario des réseaux privés, avec des paramètres de ligne de commande supplémentaires. Lorsque vous déployez cette solution (voir les options de déploiement automatique), vous pouvez utiliser ces scripts et l'une des options suivantes :

- Exécutez ces scripts manuellement à partir de la ligne de commande, comme décrit dans la section Exécuter des automatisations à partir d'une invite de commande du Guide de mise en œuvre de Cloud Migration Factory.

- Ajoutez les scripts à Migration Factory en suivant les instructions de la section Gestion des scripts pour une intégration complète à Cloud Migration Factory

Ces scripts automatisent les opérations suivantes :

- Installation de l'agent Application Migration Service sur un serveur Windows à l'aide de points de terminaison privés
- Installation de l'agent de service de migration des applications sur des serveurs Linux à l'aide de points de terminaison privés

Surveillance et dépannage

Vous pouvez surveiller le service de migration des applications en utilisant Amazon CloudWatch EventBridge, Amazon et AWS CloudTrail, qui collectent des données brutes et les transforment en near-real-time mesures lisibles. Pour plus d'informations, consultez la section Surveillance du service de migration des applications dans laAWS documentation.

Si vous rencontrez des problèmes et souhaitez lancer de nouvelles instances de test ou de transfert, vous pouvez annuler l'action de test ou de transfert. Cela ramènera l'état du cycle de vie de vos serveurs sources à l'étape précédente, indiquant que ces serveurs n'ont pas subi de transition. Lors d'une restauration, vous aurez également la possibilité de supprimer vos instances de test ou de transfert à des fins de réduction des coûts. Pour plus d'informations, consultez la section dans la documentation dans la documentation dans la documentation dans la documentation du service.

Une fois l'agent installé, le serveur source apparaît sur la console du service de migration des applications et vous pouvez consulter les détails du serveur pour vérifier la progression de la réplication.

Tester la connectivité et la résolution des noms depuis le serveur source

Connectez-vous au serveur source à l'aide du protocole RDP (Windows Remote Desktop Protocol), de Secure Shell (SSH) ou du gestionnaire deAWS sessions, et testez les éléments suivants :

- Connectivité via HTTPS sur le port TCP 443 vers le point de terminaison du service de migration des applications.
  - Sous Windows (en PowerShell) :

```
Test-NetConnection -ComputerName mgn.<aws_region>.amazonaws.com -Port 443
```

  - Sous Linux ou Windows (cmd) :

```
Telnet mgn.<aws_region>.amazonaws.com 443
```

- Connectivité via HTTPS sur le port TCP 443 vers le point de terminaison Amazon S3.
  - Sous Windows (en PowerShell) :

```
Test-NetConnection -ComputerName <s3_endpoint_name> -Port 443
```

- Sous Linux ou Windows (cmd) :

```
Telnet <s3_endpoint_name> 443
```

- Connectivité du port TCP 1500 à l'adresse IP du serveur de réplication :
  - Sous Windows (en PowerShell) :

```
Test-NetConnection -ComputerName <Replication_Server_Private_IP> -Port 1500
```

  - Sous Linux ou Windows (cmd) :

```
Telnet <Replication_Server_Private_IP> 1500
```

En outre, assurez-vous que les points de terminaison des API Amazon EC2 et Application Migration Service sont convertis en adresses IP privées à l'aide des commandes suivantes. (Vous pouvez utiliser les mêmes commandes sous Windows et Linux.)

- `nslookup ec2.<aws_region>.amazonaws.com`
- `nslookup mgn.<aws_region>.amazonaws.com`

Tester la connectivité et la résolution des noms à partir du réseau intermédiaire

Pour tester la connectivité depuis la zone intermédiaire, lancez temporairement une instance EC2 dans le sous-réseau intermédiaire et testez les éléments suivants :

- Connectivité via HTTPS sur le port TCP 443 vers le point de terminaison du service de migration des applications.
  - Sous Windows (en PowerShell) :

```
Test-NetConnection -ComputerName mgn.<aws_region>.amazonaws.com -Port 443
```

  - Sous Linux ou Windows (cmd) :

```
Telnet mgn.<aws_region>.amazonaws.com 443
```

- Connectivité via HTTPS sur le port TCP 443 vers le point de terminaison Amazon EC2.
  - Sous Windows (en PowerShell) :

```
Test-NetConnection -ComputerName ec2.<aws_region>.amazonaws.com -Port 443
```

  - Sous Linux ou Windows (cmd) :

```
Telnet ec2.<aws_region>.amazonaws.com 443
```

Si l'initialisation de la réplication s'arrête à l'étape « Téléchargement du logiciel de réplication » après l'installation de l'agent sur le serveur source, vérifiez les points suivants.

- Résolution

```
nslookup s3.<aws_region>.amazonaws.com
```

> **Note**
>
> Le point de terminaison Amazon S3 mais la connexion en privé via le point de terminaison de la passerelle Amazon S3 mais la connexion en privé via le point de terminaison de la passerelle Amazon S3.

- Connectivité via le protocole HTTPS sur le port TCP/443.
  - Sous Windows :

```
Test-NetConnection -ComputerName s3.<aws_region>.amazonaws.com -Port 443
```

  - Sous Linux :

```
Telnet s3.<aws_region>.amazonaws.com 443
```

Conclusion

Ce guide couvrait les exigences et fournissait un exemple de configuration pour l'utilisation d'Application lift-and-shift Migration Service pour la migration de serveurs depuis des réseaux locaux sécurisés versAWS une connectivité privée (AWS VPNouAWS Direct Connect). Il s'agit d'un scénario typique pour de nombreuses migrations d'entreprise. Le guide fournit également des conseils sur les méthodes de test à l'aide d'un déploiement automatique ou manuel, ainsi que sur la surveillance et la résolution des problèmes de connectivité s'ils surviennent.

Ressources

Articles du blog

- Accélérez votre migration avecAWS Application Migration Service
- Comment utiliser le nouveauAWS Application Migration Service pour les migrations Lift-and-Shift

Guides et modèles

- Connect aux donnéesAWS MGN et aux avions de contrôle via un réseau privé
- AWSstratégie de migration à grande échelle et meilleures pratiques
- Automatiser les migrations de serveurs à grande échelle avec Cloud Migration Factory

Des solutions

- Coordonnez et automatisez les migrations à grande échelle vers laAWS solution Cloud Migration FactoryAWS Cloud

Historique du document

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

Modification	Description	Date
Publication initiale	—	10 mars 2023

AWS Glossaire des directives prescriptives

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

Nombres

7 R

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

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

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

A

ABAC

Voir contrôle d'accès basé sur les attributs.

services abstraits

Consultez la section Services gérés.

ACIDE

Voir atomicité, consistance, isolation, durabilité.

migration active-active

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

migration active-passive

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

fonction d'agrégation

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

AI

Voir intelligence artificielle.

AIOps

Voir les opérations d'intelligence artificielle.

anonymisation

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

anti-motif

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

contrôle des applications

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

portefeuille d'applications

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

intelligence artificielle (IA)

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

opérations d'intelligence artificielle (AIOps)

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

chiffrement asymétrique

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

atomicité, cohérence, isolement, durabilité (ACID)

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

contrôle d'accès par attributs (ABAC)

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

source de données faisant autorité

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

Zone de disponibilité

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

AWS Cadre d'adoption du cloud (AWS CAF)

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

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

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

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

B

mauvais bot

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

BCP

Consultez la section Planification de la continuité des activités.

graphique de comportement

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

système de poids fort

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

classification binaire

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

filtre de Bloom

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

déploiement bleu/vert

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

bot

Application logicielle qui exécute des tâches automatisées sur Internet et simule l'activité ou l'interaction humaine. Certains robots sont utiles ou bénéfiques, comme les robots d'exploration Web qui indexent des informations sur Internet. D'autres robots, connus sous le nom de mauvais robots, sont destinés à perturber ou à nuire à des individus ou à des organisations.

botnet

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

branche

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

accès par brise-vitre

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

stratégie existante (brownfield)

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

cache de tampon

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

capacité métier

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

planification de la continuité des activités (BCP)

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

C

CAF

Voir le cadre d'adoption du AWS cloud.

déploiement de Canary

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

CCoE

Voir le Centre d'excellence du cloud.

CDC

Consultez la section Capture des données de modification.

capture des données de modification (CDC)

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

ingénierie du chaos

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

CI/CD

Découvrez l'intégration continue et la livraison continue.

classification

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

chiffrement côté client

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

Centre d'excellence cloud (CCoE)

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

cloud computing

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

modèle d'exploitation du cloud

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

étapes d'adoption du cloud

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

- Projet : exécution de quelques projets liés au cloud à des fins de preuve de concept et d'apprentissage
- Base : réaliser des investissements fondamentaux pour mettre à l'échelle l'adoption du cloud (par exemple, en créant une zone de destination, en définissant un CCoE ou en établissant un modèle opérationnel)
- Migration : migration d'applications individuelles
- Réinvention : optimisation des produits et services et innovation dans le cloud

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

CMDB

Voir base de données de gestion de configuration.

référentiel de code

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

cache passif

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

données gelées

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

vision par ordinateur (CV)

Domaine de l'IA qui utilise l'apprentissage automatique pour analyser et extraire des informations à partir de formats visuels tels que des images numériques et des vidéos. Par exemple, AWS

Panorama propose des appareils qui ajoutent des CV aux réseaux de caméras locaux, et Amazon SageMaker fournit des algorithmes de traitement d'image pour les CV.

dérive de configuration

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

base de données de gestion des configurations (CMDB)

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

pack de conformité

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

intégration continue et livraison continue (CI/CD)

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

CV

Voir vision par ordinateur.

D

données au repos

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

classification des données

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

dérive des données

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

données en transit

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

maillage de données

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

minimisation des données

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

périmètre de données

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

prétraitement des données

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

provenance des données

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

sujet des données

Personne dont les données sont collectées et traitées.

entrepôt des données

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

langage de définition de base de données (DDL)

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

langage de manipulation de base de données (DML)

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

DDL

Voir langage de définition de base de données.

ensemble profond

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

deep learning

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

defense-in-depth

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

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

administrateur délégué

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

déploiement

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

environnement de développement

Voir environnement.

contrôle de détection

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

cartographie de la chaîne de valeur du développement (DVSM)

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

jumeau numérique

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

tableau des dimensions

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

catastrophe

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

reprise après sinistre (DR)

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

DML

Voir langage de manipulation de base de données.

conception axée sur le domaine

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

DR

Consultez la section Reprise après sinistre.

détection de dérive

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

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

DVSM

Voir la cartographie de la chaîne de valeur du développement.

E

EDA

Voir analyse exploratoire des données.

informatique de périphérie

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

chiffrement

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

clé de chiffrement

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

endianisme

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

point de terminaison

Voir point de terminaison de service.

service de point de terminaison

Service que vous pouvez héberger sur un cloud privé virtuel (VPC) pour le partager avec d'autres utilisateurs. Vous pouvez créer un service de point de terminaison avec AWS PrivateLink et accorder des autorisations à d'autres principaux Comptes AWS ou à AWS Identity and Access Management (IAM) principaux. Ces comptes ou principaux peuvent se connecter à votre

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

planification des ressources d'entreprise (ERP)

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

chiffrement d'enveloppe

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

environment

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

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

épopée

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

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

ERP

Voir Planification des ressources d'entreprise.

analyse exploratoire des données (EDA)

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

F

tableau des faits

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

échouer rapidement

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

limite d'isolation des défauts

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

branche de fonctionnalités

Voir la succursale.

fonctionnalités

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

importance des fonctionnalités

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

transformation de fonctionnalité

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

FGAC

Découvrez le contrôle d'accès détaillé.

contrôle d'accès détaillé (FGAC)

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

migration instantanée (flash-cut)

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

G

blocage géographique

Voir les restrictions géographiques.

restrictions géographiques (blocage géographique)

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

Flux de travail Gitflow

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

stratégie inédite

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

barrière de protection

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

H

HA

Découvrez la haute disponibilité.

migration de base de données hétérogène

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

haute disponibilité (HA)

Capacité d'une charge de travail à fonctionner en continu, sans intervention, en cas de difficultés ou de catastrophes. Les systèmes HA sont conçus pour basculer automatiquement, fournir

constamment des performances de haute qualité et gérer différentes charges et défaillances avec un impact minimal sur les performances.

modernisation de l'historien

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

migration de base de données homogène

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

données chaudes

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

correctif

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

période de soins intensifs

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

I

IaC

Considérez l'infrastructure comme un code.

politique basée sur l’identité

Politique attachée à un ou plusieurs principaux IAM qui définit leurs autorisations au sein de l' AWS Cloud environnement.

application inactive

Application dont l'utilisation moyenne du processeur et de la mémoire se situe entre 5 et 20 % sur une période de 90 jours. Dans un projet de migration, il est courant de retirer ces applications ou de les retenir sur site.

IIoT

Voir Internet industriel des objets.

infrastructure immuable

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

VPC entrant (d'entrée)

Dans une architecture AWS multi-comptes, un VPC qui accepte, inspecte et achemine les connexions réseau depuis l'extérieur d'une application. L'architecture de référence de sécuritéAWS recommande de configurer votre compte réseau avec des VPC entrants, sortants et d'inspection afin de protéger l'interface bidirectionnelle entre votre application et Internet en général.

migration incrémentielle

Stratégie de basculement dans le cadre de laquelle vous migrez votre application par petites parties au lieu d'effectuer un basculement complet unique. Par exemple, il se peut que vous ne transfériez que quelques microservices ou utilisateurs vers le nouveau système dans un

premier temps. Après avoir vérifié que tout fonctionne correctement, vous pouvez transférer progressivement des microservices ou des utilisateurs supplémentaires jusqu'à ce que vous puissiez mettre hors service votre système hérité. Cette stratégie réduit les risques associés aux migrations de grande ampleur.

Industry 4.0

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

infrastructure

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

infrastructure en tant que code (IaC)

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

internet industriel des objets (IIoT)

L'utilisation de capteurs et d'appareils connectés à Internet dans les secteurs industriels tels que la fabrication, l'énergie, l'automobile, les soins de santé, les sciences de la vie et l'agriculture. Pour plus d'informations, veuillez consulter Building an industrial Internet of Things (IIoT) digital transformation strategy.

VPC d'inspection

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

Internet des objets (IoT)

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

interprétabilité

Caractéristique d'un modèle de machine learning qui décrit dans quelle mesure un être humain peut comprendre comment les prédictions du modèle dépendent de ses entrées. Pour plus d'informations, veuillez consulter Machine learning model interpretability with AWS.

IoT

Voir Internet des objets.

Bibliothèque d'informations informatiques (ITIL)

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

gestion des services informatiques (ITSM)

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

ITIL

Consultez la bibliothèque d'informations informatiques.

ITSM

Consultez la section Gestion des services informatiques.

L

contrôle d'accès basé sur des étiquettes (LBAC)

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

zone de destination

Une zone d'atterrissage est un AWS environnement multi-comptes bien conçu, évolutif et sécurisé. Il s'agit d'un point de départ à partir duquel vos entreprises peuvent rapidement lancer et déployer des charges de travail et des applications en toute confiance dans leur environnement

de sécurité et d'infrastructure. Pour plus d'informations sur les zones de destination, veuillez consulter Setting up a secure and scalable multi-account AWS environment.

migration de grande envergure

Migration de 300 serveurs ou plus.

LBAC

Voir contrôle d'accès basé sur des étiquettes.

principe de moindre privilège

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

lift and shift

Voir 7 Rs.

système de poids faible

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

environnements inférieurs

Voir environnement.

M

machine learning (ML)

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

branche principale

Voir la succursale.

malware

Logiciel conçu pour compromettre la sécurité ou la confidentialité de l'ordinateur. Les logiciels malveillants peuvent perturber les systèmes informatiques, divulguer des informations sensibles

ou obtenir un accès non autorisé. Parmi les malwares, on peut citer les virus, les vers, les rançongiciels, les chevaux de Troie, les logiciels espions et les enregistreurs de frappe.

services gérés

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

système d'exécution de la fabrication (MES)

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

MAP

Voir Migration Acceleration Program.

mécanisme

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

compte membre

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

MAILLES

Voir le système d'exécution de la fabrication.

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

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

microservice

Petit service indépendant qui communique via des API bien définies et qui est généralement détenu par de petites équipes autonomes. Par exemple, un système d'assurance peut inclure des microservices qui mappent à des capacités métier, telles que les ventes ou le marketing, ou

à des sous-domaines, tels que les achats, les réclamations ou l'analytique. Les avantages des microservices incluent l'agilité, la flexibilité de la mise à l'échelle, la facilité de déploiement, la réutilisation du code et la résilience. Pour plus d'informations, consultez la section Intégration de microservices à l'aide de services AWS sans serveur.

architecture de microservices

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

Programme d'accélération des migrations (MAP)

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

migration à grande échelle

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

usine de migration

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

métadonnées de migration

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

modèle de migration

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

Évaluation du portefeuille de migration (MPA)

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

Évaluation de la préparation à la migration (MRA)

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

stratégie de migration

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

ML

Voir apprentissage automatique.

modernisation

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

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

évaluation de la préparation à la modernisation

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

applications monolithiques (monolithes)

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

MPA

Voir Évaluation du portefeuille de migration.

MQTT

Voir Message Queuing Telemetry Transport.

classification multi-classes

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

infrastructure mutable

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

O

OAC

Voir Contrôle d'accès à l'origine.

OAI

Voir l'identité d'accès à l'origine.

OCM

Voir gestion du changement organisationnel.

migration hors ligne

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

OI

Consultez la section Intégration des opérations.

OLA

Voir l'accord au niveau opérationnel.

migration en ligne

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

OPC-UA

Voir Open Process Communications - Architecture unifiée.

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

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

accord au niveau opérationnel (OLA)

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

examen de l'état de préparation opérationnelle (ORR)

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

technologie opérationnelle (OT)

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

intégration des opérations (OI)

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

journal de suivi d'organisation

Un parcours créé par AWS CloudTrail qui enregistre tous les événements pour tous les membres Comptes AWS d'une organisation dans AWS Organizations. Ce journal de suivi est créé dans chaque Compte AWS qui fait partie de l'organisation et suit l'activité de chaque compte. Pour plus d'informations, consultez la section Création d'un suivi pour une organisation dans la CloudTrail documentation.

gestion du changement organisationnel (OCM)

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

contrôle d'accès d'origine (OAC)

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

identité d'accès d'origine (OAI)

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

OU

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

DE

Voir technologie opérationnelle.

VPC sortant (de sortie)

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

P

limite des autorisations

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

informations personnelles identifiables (PII)

Informations qui, lorsqu'elles sont consultées directement ou associées à d'autres données connexes, peuvent être utilisées pour déduire raisonnablement l'identité d'une personne. Les

exemples d'informations personnelles incluent les noms, les adresses et les informations de contact.

PII

Voir les informations personnelles identifiables.

manuel stratégique

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

PLC

Voir contrôleur logique programmable.

PLM

Consultez la section Gestion du cycle de vie des produits.

politique

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

persistance polyglotte

Choix indépendant de la technologie de stockage de données d'un microservice en fonction des modèles d'accès aux données et d'autres exigences. Si vos microservices utilisent la même technologie de stockage de données, ils peuvent rencontrer des difficultés d'implémentation ou présenter des performances médiocres. Les microservices sont plus faciles à mettre en œuvre, atteignent de meilleures performances, ainsi qu'une meilleure capacité de mise à l'échelle s'ils utilisent l'entrepôt de données le mieux adapté à leurs besoins. Pour plus d'informations, veuillez consulter Enabling data persistence in microservices.

évaluation du portefeuille

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

predicate

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

prédicat pushdown

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

contrôle préventif

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

principal

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

Confidentialité dès la conception

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

zones hébergées privées

Conteneur qui contient des informations concernant la façon dont vous souhaitez qu'Amazon Route 53 réponde aux requêtes DNS pour un domaine et ses sous-domaines dans un ou plusieurs VPC. Pour plus d'informations, veuillez consulter Working with private hosted zones dans la documentation Route 53.

contrôle proactif

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

gestion du cycle de vie des produits (PLM)

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

environnement de production

Voir environnement.

contrôleur logique programmable (PLC)

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

pseudonymisation

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

publier/souscrire (pub/sub)

Modèle qui permet des communications asynchrones entre les microservices afin d'améliorer l'évolutivité et la réactivité. Par exemple, dans un MES basé sur des microservices, un microservice peut publier des messages d'événements sur un canal auquel d'autres microservices peuvent s'abonner. Le système peut ajouter de nouveaux microservices sans modifier le service de publication.

Q

plan de requête

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

régression du plan de requêtes

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

R

Matrice RACI

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

rançongiciel

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

Matrice RASCI

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

RCAC

Voir contrôle d'accès aux lignes et aux colonnes.

réplica en lecture

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

réarchitecte

Voir 7 Rs.

objectif de point de récupération (RPO)

Durée maximale acceptable depuis le dernier point de récupération des données. Cela permet de déterminer ce qui est considéré comme une perte de données acceptable entre le dernier point de restauration et l'interruption du service.

objectif de temps de récupération (RTO)

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

refactoriser

Voir 7 Rs.

Région

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

régression

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

réhéberger

Voir 7 Rs.

version

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

déplacer

Voir 7 Rs.

replateforme

Voir 7 Rs.

rachat

Voir 7 Rs.

résilience

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

politique basée sur les ressources

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

matrice responsable, redevable, consulté et informé (RACI)

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

contrôle réactif

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

retain

Voir 7 Rs.

se retirer

Voir 7 Rs.

rotation

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

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

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

RPO

Voir l'objectif du point de récupération.

RTO

Voir l'objectif en matière de temps de rétablissement.

runbook

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

S

SAML 2.0

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

un utilisateur dans IAM pour tous les membres de votre organisation. Pour plus d'informations sur la fédération SAML 2.0, veuillez consulter À propos de la fédération SAML 2.0 dans la documentation IAM.

SCADA

Voir Contrôle de supervision et acquisition de données.

SCP

Voir la politique de contrôle des services.

secret

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

contrôle de sécurité

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

renforcement de la sécurité

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

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

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

automatisation des réponses de sécurité

Action prédéfinie et programmée conçue pour répondre automatiquement à un événement de sécurité ou y remédier. Ces automatisations servent de contrôles de sécurité détectifs ou réactifs

qui vous aident à mettre en œuvre les meilleures pratiques AWS de sécurité. Parmi les actions de réponse automatique, citons la modification d'un groupe de sécurité VPC, l'application de correctifs à une instance Amazon EC2 ou la rotation des informations d'identification.

chiffrement côté serveur

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

Politique de contrôle des services (SCP)

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

point de terminaison du service

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

contrat de niveau de service (SLA)

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

indicateur de niveau de service (SLI)

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

objectif de niveau de service (SLO)

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

modèle de responsabilité partagée

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

SIEM

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

point de défaillance unique (SPOF)

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

SLA

Voir le contrat de niveau de service.

SLI

Voir l'indicateur de niveau de service.

SLO

Voir l'objectif de niveau de service.

split-and-seed modèle

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

SPOF

Voir point de défaillance unique.

schéma en étoile

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

modèle de figuier étrangleur

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

un moyen de gérer les risques lors de la réécriture de systèmes monolithiques. Pour obtenir un exemple d'application de ce modèle, veuillez consulter Modernizing legacy Microsoft ASP.NET (ASMX) web services incrementally by using containers and Amazon API Gateway.

sous-réseau

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

contrôle de supervision et acquisition de données (SCADA)

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

chiffrement symétrique

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

tests synthétiques

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

T

balises

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

variable cible

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

liste de tâches

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

environnement de test

Voir environnement.

entraînement

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

passerelle de transit

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

flux de travail basé sur jonction

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

accès sécurisé

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

réglage

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

équipe de deux pizzas

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

U

incertitude

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

tâches indifférenciées

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

environnements supérieurs

Voir environnement.

V

mise à vide

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

contrôle de version

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

Appairage de VPC

Connexion entre deux VPC qui vous permet d'acheminer le trafic à l'aide d'adresses IP privées. Pour plus d'informations, veuillez consulter la rubrique Qu'est-ce que l'appairage de VPC ? dans la documentation Amazon VPC.

vulnérabilités

Défaut logiciel ou matériel qui compromet la sécurité du système.

W

cache actif

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

données chaudes

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

fonction de fenêtre

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

charge de travail

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

flux de travail

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

VER

Voir écrire une fois, lire plusieurs.

WQF

Consultez le cadre de qualification des charges de travail AWS.

écrire une fois, lire plusieurs (WORM)

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

Z

exploit Zero-Day

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

vulnérabilité de type « jour zéro »

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

application zombie

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

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