Bonnes pratiques pour créer une architecture de cloud hybride avec Services AWS

AWS Directives prescriptives

AWS Directives prescriptives: Bonnes pratiques pour créer une architecture de cloud hybride avec Services AWS

Table of Contents

Bonnes pratiques pour créer une architecture de cloud hybride avec Services AWS

Amazon Web Services (contributeurs)

Juin 2025 (historique du document)

De nombreuses entreprises et organisations ont adopté le cloud computing comme élément clé de leur stratégie technologique. Ils migrent généralement leurs charges de travail AWS Cloud vers le pour accroître l'agilité, les économies de coûts, les performances, la disponibilité, la résilience et l'évolutivité. La plupart des applications peuvent être facilement migrées, mais certaines doivent rester sur site pour tirer parti de la faible latence et du traitement local des données de l'environnement sur site, pour éviter des coûts de transfert de données élevés ou pour des raisons de conformité réglementaire. En outre, un sous-ensemble d'applications devra peut-être être repensé ou modernisé avant de pouvoir être déplacé vers le cloud. Cela amène de nombreuses entreprises à rechercher des architectures cloud hybrides pour intégrer leurs opérations sur site et dans le cloud afin de prendre en charge un large éventail de cas d'utilisation. Cette approche hybride peut offrir les avantages de l'informatique sur site et dans le cloud, et peut être particulièrement utile pour les scénarios d'informatique de pointe.

Lorsque vous créez un cloud hybride avec AWS, nous vous recommandons de déterminer votre stratégie de cloud hybride et votre stratégie technique :

- Une stratégie de cloud hybride fournit des directives qui régissent la consommation de ressources dans le cloud et sur site afin de soutenir vos objectifs commerciaux. Ce guide décrit les cas d'utilisation courants pour créer un cloud hybride, tels que la prise en charge de la migration continue vers le cloud, la garantie de la continuité des activités en cas de sinistre, l'extension de l'infrastructure cloud à l'environnement sur site pour prendre en charge les applications à faible latence, ou l'extension de votre présence internationale sur. AWS La définition de cette stratégie vous aide à identifier et à définir vos objectifs commerciaux en matière de création d'un cloud hybride, et fournit des directives pour le placement des charges de travail dans le cloud hybride.
- Une stratégie technique pour le cloud hybride identifie les principes directeurs de l'architecture du cloud hybride et définit un cadre de mise en œuvre. Ce guide décrit les exigences communes relatives à une architecture de cloud hybride déployée et gérée de manière cohérente afin de vous aider à définir les principes d'une mise en œuvre planifiée du cloud hybride. Ces exigences incluent

des interfaces standardisées pour le provisionnement et la gestion des ressources au sein de votre infrastructure cloud.

Ce guide décrit un cadre d'exploitation et de gestion destiné à aider les architectes de solutions et les opérateurs à identifier les éléments de base, les meilleures pratiques, le cloud AWS hybride et les services régionaux avec AWS lesquels mettre en œuvre un cloud hybride.

De nombreuses entreprises ont utilisé les solutions décrites dans ce guide pour déployer avec succès des environnements de cloud hybride qui tirent parti de l'évolutivité, de l'agilité, de l'innovation et de l'empreinte mondiale fournies par le AWS Cloud. (Voir les études de cas.)AWS les services cloud hybrides offrent une AWS expérience cohérente, que ce soit dans le cloud, sur site ou à la périphérie. Des services tels que le AWS Outposts calcul, Zones locales AWS le stockage, les bases de données et autres sont sélectionnés à Services AWS proximité de grands centres industriels et peuplés lorsque vous avez besoin d'une faible latence entre les appareils des utilisateurs finaux ou entre les centres de données sur site et les serveurs de charge de travail existants.

Dans ce guide :

Présentation

Ce guide classe les AWS recommandations pour le cloud hybride en cinq piliers : réseau, sécurité, résilience, planification des capacités et gestion de l'infrastructure. Il fournit des directives pour vous aider à améliorer votre niveau de préparation et à développer une stratégie de migration en utilisant un service de périphérie AWS hybride tel que AWS Outposts ou Zones locales AWS. Nous vous recommandons vivement de travailler avec votre Compte AWS équipe ou de vous AWS Partner assurer qu'un spécialiste du cloud AWS hybride est disponible pour vous aider à suivre ce guide et à développer votre processus.

> **Note**
>
> Bien que AWS Outposts les Zones Locales répondent à des problèmes similaires, nous vous recommandons de passer en revue les cas d'utilisation ainsi que les services et fonctionnalités disponibles afin de choisir l'offre la mieux adaptée à vos besoins. Pour plus d'informations, consultez le billet de AWS blog Zones locales AWS et AWS Outposts le choix de la technologie adaptée à votre charge de travail périphérique.

Ateliers sur le cloud hybride

Avec l'aide d'un expert en matière de cloud AWS hybride (PME), vous pouvez organiser un atelier sur le cloud hybride afin d'évaluer le niveau de maturité de votre entreprise par rapport aux cinq piliers abordés dans ce guide.

L'atelier se concentre sur les domaines internes de votre organisation, tels que le réseau, la sécurité, la conformité DevOps, la virtualisation et les unités commerciales. Il vous aide à concevoir une architecture de cloud hybride qui répond aux exigences de votre entreprise et définit les détails de mise en œuvre, en suivant les étapes décrites dans la section Processus d'adoption du cloud hybride de ce guide.

PoCs

Si vous avez des exigences spécifiques, vous pouvez utiliser des preuves de concept (PoCs) pour valider les fonctionnalités dans les Zones Locales et par AWS Outposts rapport à ces exigences.

AWS utilise PoCs pour vous aider à tester les charges de travail que vous souhaitez déplacer vers un avant-poste ou une zone locale, afin de déterminer si les charges de travail seront fonctionnelles dans le cadre des architectures de test. Pour accéder à une zone locale à des fins de test, suivez les instructions de la documentation relative aux zones locales. Pour tester votre charge de travail AWS Outposts, travaillez avec votre Compte AWS équipe ou AWS Partner pour accéder à un laboratoire de AWS Outposts test et bénéficier des conseils d'architectes de AWS solutions. Dans tous les scénarios, le développement d'un PoC vous oblige à générer un document de test contenant :

- Services AWS à utiliser, tels qu'Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Block Store (Amazon EBS), Amazon Virtual Private Cloud (Amazon VPC) et Amazon Elastic Kubernetes Service (Amazon EKS)
- Taille et nombre d'instances à consommer (par exemple, `m5.xlarge` ou `c5.2xlarge`)
- Schéma de l'architecture de test
- Critères de réussite des tests
- Détails et objectifs de chaque test à exécuter

Piliers

La section suivante traite des prérequis et des limites liés à l'utilisation des architectures décrites dans ce guide. Les sections suivantes couvrent les détails de chaque pilier afin que le document de recommandations que vous créez lors de l'atelier sur le cloud hybride puisse refléter les détails de conception requis pour la mise en œuvre.

- Réseautage à la périphérie
- La sécurité à la périphérie
- Résilience à la périphérie
- Planification des capacités à la périphérie
- Gestion de l'infrastructure de pointe

Conditions préalables et limitations

Avant de suivre ce guide, collaborez avec votre Compte AWS équipe ou examinez les conditions préalables et les limites relatives AWS Partner à la mise en œuvre d'architectures de périphérie avec AWS Outposts des Zones Locales.

Prérequis

AWS Outposts

- Votre centre de données existant doit répondre aux AWS Outposts exigences en matière d'installations, de mise en réseau et d'alimentation. AWS Outposts est conçu pour fonctionner dans un environnement de centre de données doté d'entrées d'alimentation redondantes de 5 à 15 kVA, d'un débit d'air de 145,8 fois le kVA de pieds cubes par minute (CFM) et d'une température ambiante comprise entre 41 °F (5 °C) et 95 °F (35 °C), entre autres exigences.
- Vérifiez que le AWS Outposts service est disponible dans votre pays en consultant le AWS Outposts rack FAQs. Voir la question : Dans quels pays et territoires le rack Outposts est-il disponible ?
- Si votre entreprise a besoin de quatre AWS Outposts racks ou plus, votre centre de données doit répondre aux exigences relatives aux racks Aggrégation, Core, Edge (ACE).
- Un accès Internet ou une AWS Direct Connect liaison d'au moins 500 Mbits/s (1 Gbit/s est préférable) doivent être fournis et maintenus pour se connecter AWS Outposts au Région AWS, avec une connectivité de sauvegarde appropriée si votre cas d'utilisation l'exige. Le temps de latence aller-retour entre AWS Outposts la région et la région doit être de 175 millisecondes au maximum.
- Vous devez avoir un contrat actif pour AWS Enterprise Support ou AWS Enterprise On-Ramp.

Zones locales AWS

- Une zone AWS locale doit être disponible à proximité de vos centres de données ou de vos utilisateurs. Voir les Zones locales AWS emplacements.
- Vérifiez que vous disposez d'une connectivité réseau entre votre infrastructure sur site et la zone locale :

- Option 1 : un AWS Direct Connect lien entre votre centre de données et le AWS Direct Connect point de présence (PoP) le plus proche de la zone locale. Pour plus d'informations, consultez Direct Connect dans la documentation des Zones Locales.
- Option 2 : un lien Internet en plus d'une appliance de réseau privé virtuel (VPN) sur site et des licences nécessaires pour lancer une appliance VPN logicielle sur Amazon EC2 dans la zone locale. Pour plus d'informations, consultez la section Connexion VPN dans la documentation des Zones Locales.

Pour des options de connectivité supplémentaires, consultez la documentation sur les Zones Locales.

Limites

AWS Outposts

- Amazon Relational Database Service (Amazon RDS) AWS Outposts sur les déploiements multi-AZ nécessite des pools d'adresses IP (CoIP) appartenant au client. Pour plus d'informations, consultez la section Adresses IP appartenant au client pour Amazon RDS on. AWS Outposts
- Multi-AZ on AWS Outposts est disponible pour toutes les versions prises en charge de MySQL et PostgreSQL sur Amazon RDS on. AWS Outposts Pour plus d'informations, consultez Prise en charge d'Amazon RDS sur AWS Outposts pour les fonctions Amazon RDS. Amazon RDS on AWS Outposts prend en charge les bases de données SQL Server, Amazon RDS pour MySQL et Amazon RDS pour PostgreSQL.
- AWS Outposts n'est pas conçu pour fonctionner lorsqu'il est déconnecté d'un Région AWS. Pour plus d'informations, consultez la section Penser en termes de modes de défaillance du AWS livre blanc Considérations relatives à la conception et à l'architecture de AWS Outposts haute disponibilité.
- Amazon Simple Storage Service (Amazon S3) présente certaines AWS Outposts limites. Elles sont abordées dans la section En quoi Amazon S3 sur Outposts diffère-t-il d'Amazon S3 ? section du guide de l'utilisateur d'Amazon S3 on Outposts.
- Les équilibreurs de charge d'application activés AWS Outposts ne prennent pas en charge le protocole TLS mutuel (MTL) ni les sessions persistantes.
- Les racks ACE ne sont pas entièrement fermés et ne comprennent pas de portes avant ou arrière.
- L'outil de capacité d'instance ne s'applique qu'aux nouvelles commandes.

Zones locales AWS

- Zones Locales n'ont pas de AWS Site-to-Site VPN point de terminaison. Utilisez plutôt un VPN basé sur un logiciel sur Amazon EC2.
- Les Zones Locales ne sont pas prises en charge AWS Transit Gateway. Connectez-vous plutôt à la zone locale à l'aide d'une interface virtuelle AWS Direct Connect privée (VIF).
- Les Zones Locales ne prennent pas toutes en charge les services tels qu'Amazon RDS, Amazon FSx, Amazon EMR ou ElastiCache Amazon, ou les passerelles NAT. Pour plus d'informations, consultez la section Zones locales AWS Fonctionnalités.
- Les équilibreurs de charge des applications dans les Zones Locales ne prennent pas en charge les MTL ou les sessions persistantes.

Processus d'adoption du cloud hybride

Les sections suivantes présentent les architectures et les détails de conception de chaque pilier du cloud AWS hybride :

- Réseautage à la périphérie
- La sécurité à la périphérie
- Résilience à la périphérie
- Planification des capacités à la périphérie
- Gestion de l'infrastructure de pointe

Réseautage à la périphérie

Lorsque vous concevez des solutions qui utilisent une infrastructure AWS périphérique, telle que AWS Outposts des Zones Locales, vous devez examiner attentivement la conception du réseau. Le réseau constitue la base de la connectivité permettant d'atteindre les charges de travail déployées dans ces emplacements périphériques et est essentiel pour garantir une faible latence. Cette section décrit les différents aspects de la connectivité périphérique hybride.

Architecture VPC

Un cloud privé virtuel (VPC) couvre toutes les zones de disponibilité de son. Région AWS Vous pouvez facilement étendre n'importe quel VPC de la région aux avant-postes ou aux zones locales en utilisant la AWS console ou le AWS Command Line Interface (AWS CLI) pour ajouter un sous-réseau d'avant-poste ou de zone locale. Les exemples suivants montrent comment créer des sous-réseaux dans des zones locales AWS Outposts et dans des zones locales à l'aide de AWS CLI :

- AWS Outposts: Pour ajouter un sous-réseau Outpost à un VPC, spécifiez le nom de ressource Amazon (ARN) de l'Outpost.

```
aws ec2 create-subnet --vpc-id vpc-081ec835f3EXAMPLE \
--cidr-block 10.0.0.0/24 \
--outpost-arn arn:aws:outposts:us-west-2:11111111111:outpost/op-0e32example1 \
--tag-specifications ResourceType=subnet,Tags=[{Key=Name,Value=my-ipv4-only-subnet}]
```

  Pour plus d’informations, consultez la documentation AWS Outposts.

- Zones locales : pour ajouter un sous-réseau de zone locale à un VPC, suivez la même procédure que pour les zones de disponibilité, mais spécifiez l'ID de zone locale `<local-zone-name>` (dans l'exemple suivant).

```
aws ec2 create-subnet --vpc-id vpc-081ec835f3EXAMPLE \
--cidr-block 10.0.1.0/24 \
--availability-zone <local-zone-name> \
--tag-specifications ResourceType=subnet,Tags=[{Key=Name,Value=my-ipv4-only-subnet}]
```

  Pour plus d'informations, consultez la documentation sur les Zones Locales.

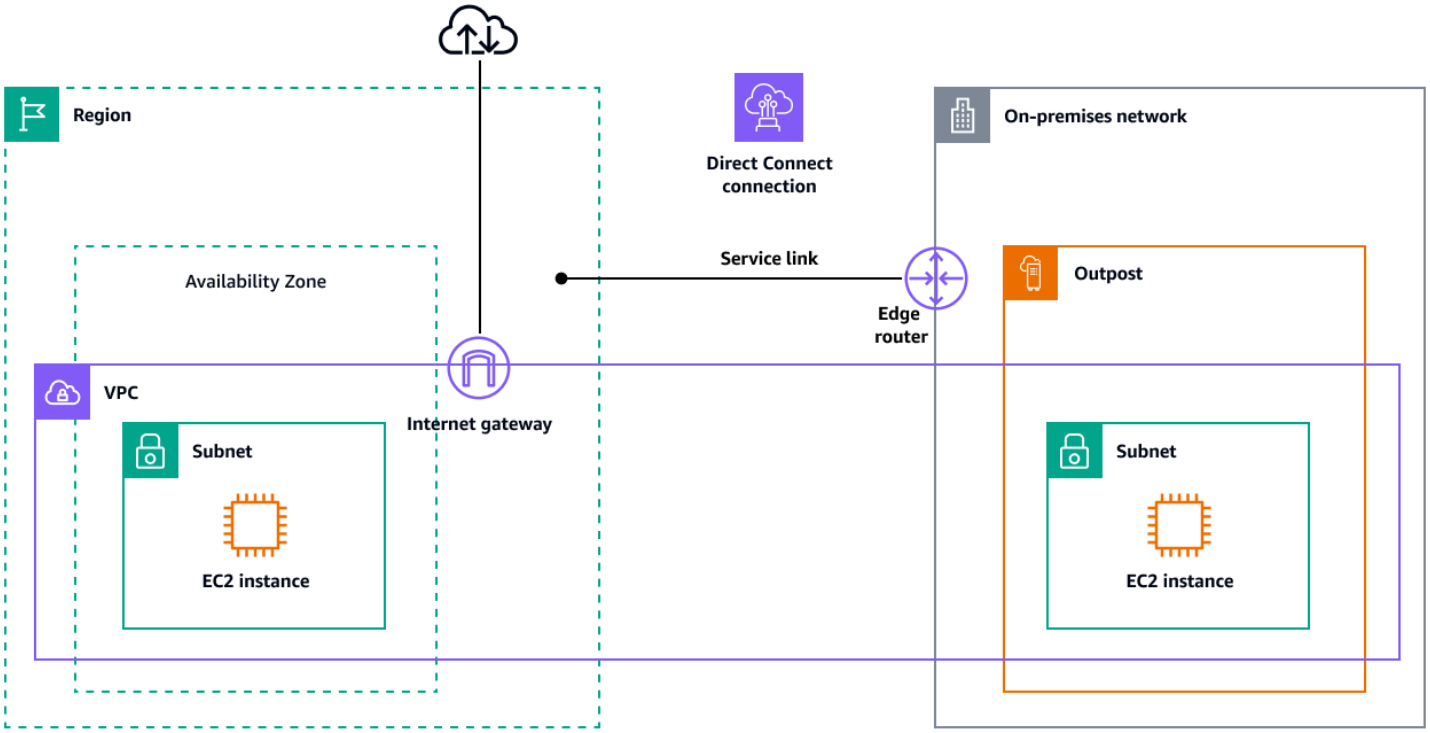
Le schéma suivant montre une AWS architecture qui inclut les sous-réseaux Outpost et Local Zone.

Trafic d'une région à l'autre

Lorsque vous concevez une architecture hybride à l'aide de services tels que les zones locales AWS Outposts, tenez compte à la fois des flux de contrôle et des flux de trafic de données entre les infrastructures de périphérie et Régions AWS. Selon le type d'infrastructure périphérique, votre responsabilité peut varier : certaines infrastructures nécessitent que vous gériez la connexion à la région parent, tandis que d'autres s'en chargent par le biais de l'infrastructure AWS globale. Cette section explore les implications de connectivité du plan de contrôle et du plan de données pour les Zones Locales et AWS Outposts.

AWS Outposts plan de contrôle

AWS Outposts fournit une structure réseau appelée lien de service. Le lien de service est une connexion obligatoire entre AWS Outposts et la région sélectionnée Région AWS ou parent (également appelée région d'origine). Il permet la gestion de l'avant-poste et l'échange de trafic entre l'avant-poste et. Région AWS Le lien de service utilise un ensemble crypté de connexions VPN pour communiquer avec la région d'origine. Vous devez fournir une connectivité entre AWS Outposts et Région AWS soit via un lien Internet ou une interface virtuelle AWS Direct Connect publique (VIF publique), soit via une interface virtuelle AWS Direct Connect privée (VIF privée). Pour une expérience et une résilience optimales, il est AWS recommandé d'utiliser une connectivité redondante d'au moins 500 Mbits/s (1 Gbit/s est préférable) pour la connexion par liaison de service au. Région AWS La connexion par liaison de service minimale de 500 Mbits/s vous permet de lancer EC2 des instances Amazon, de connecter des volumes Amazon EBS et d'accéder à des métriques Services AWS telles qu'Amazon EKS, Amazon EMR et Amazon CloudWatch . Le réseau doit prendre en charge une unité de transmission (MTU) maximale de 1 500 octets entre l'Outpost et les points de terminaison de la liaison de service du parent. Région AWSPour plus d'informations, consultez la section AWS Outposts connectivité à Régions AWS dans la documentation des Outposts.



Pour plus d'informations sur la création d'architectures résilientes pour les liens de service qui utilisent AWS Direct Connect l'Internet public, consultez la section sur la connectivité des ancres du

AWS livre blanc Considérations relatives à la conception et à l'architecture de AWS Outposts haute disponibilité.

AWS Outposts plan de données

Le plan de données situé entre AWS Outposts et Région AWS est soutenu par la même architecture de liaison de service que celle utilisée par le plan de contrôle. La bande passante du lien de service du plan de données entre AWS Outposts et Région AWS doit être en corrélation avec la quantité de données à échanger : plus la dépendance aux données est grande, plus la bande passante de la liaison doit être importante.

Les besoins en bande passante varient en fonction des caractéristiques suivantes :

- Le nombre de AWS Outposts racks et les configurations de capacité
- Caractéristiques de la charge de travail telles que la taille de l'AMI, l'élasticité des applications et les besoins en vitesse de rafale
- Trafic VPC vers la région

Le trafic entre les EC2 instances dans AWS Outposts et EC2 les instances dans le Région AWS a une MTU de 1 300 octets. Nous vous recommandons de discuter de ces exigences avec un spécialiste du cloud AWS hybride avant de proposer une architecture qui comporte des co-dépendances entre la Région et AWS Outposts.

Plan de données des zones locales

Le plan de données entre les Zones Locales et le Région AWS est pris en charge par l'infrastructure AWS globale. Le plan de données est étendu via un VPC de la zone Région AWS à une zone locale. Les Zones Locales fournissent également une connexion sécurisée à haut débit et vous permettent de vous connecter facilement à l'ensemble des services régionaux par le biais de ces mêmes services APIs et de jeux d'outils. Région AWS

Le tableau suivant présente les options de connexion et les options associées MTUs.

À partir de	À	MTU
Amazon EC2 dans la région	Amazon EC2 dans les Zones Locales	1 300 octets

À partir de	À	MTU
AWS Direct Connect	Zones locales	1 468 octets
Passerelle Internet	Zones locales	1 500 octets
Amazon EC2 dans les Zones Locales	Amazon EC2 dans les Zones Locales	9 001 octets

Zones Locales utilisent l'infrastructure AWS globale pour se connecter Régions AWS. L'infrastructure est entièrement gérée par AWS, vous n'avez donc pas à configurer cette connectivité. Nous vous recommandons de discuter des exigences et des considérations relatives aux zones locales avec un spécialiste du cloud AWS hybride avant de concevoir une architecture comportant des co-dépendances entre la région et les zones locales.

De la périphérie au trafic sur site

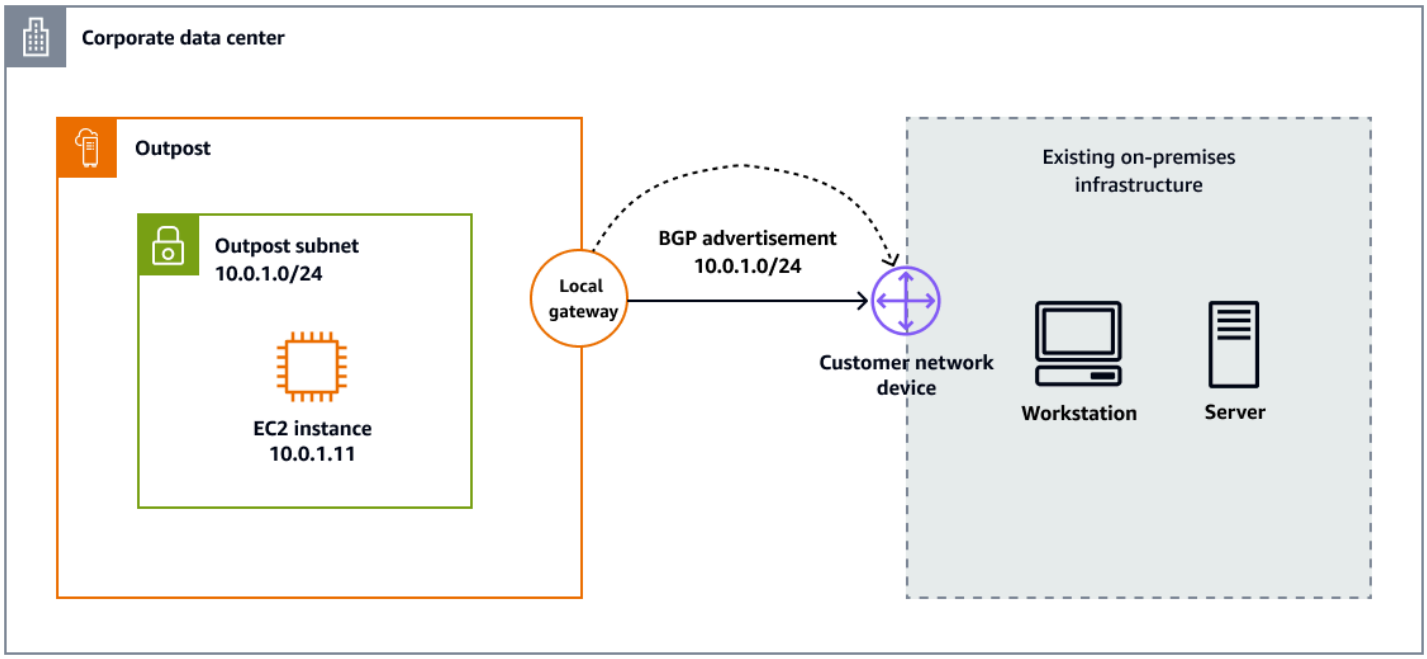
AWS les services cloud hybrides sont conçus pour répondre aux cas d'utilisation nécessitant une faible latence, un traitement local des données ou une conformité en matière de résidence des données. L'architecture réseau permettant d'accéder à ces données est importante, et elle dépend du fait que votre charge de travail s'exécute dans des zones locales AWS Outposts ou dans des zones locales. La connectivité locale nécessite également une portée bien définie, comme indiqué dans les sections suivantes.

AWS Outposts passerelle locale

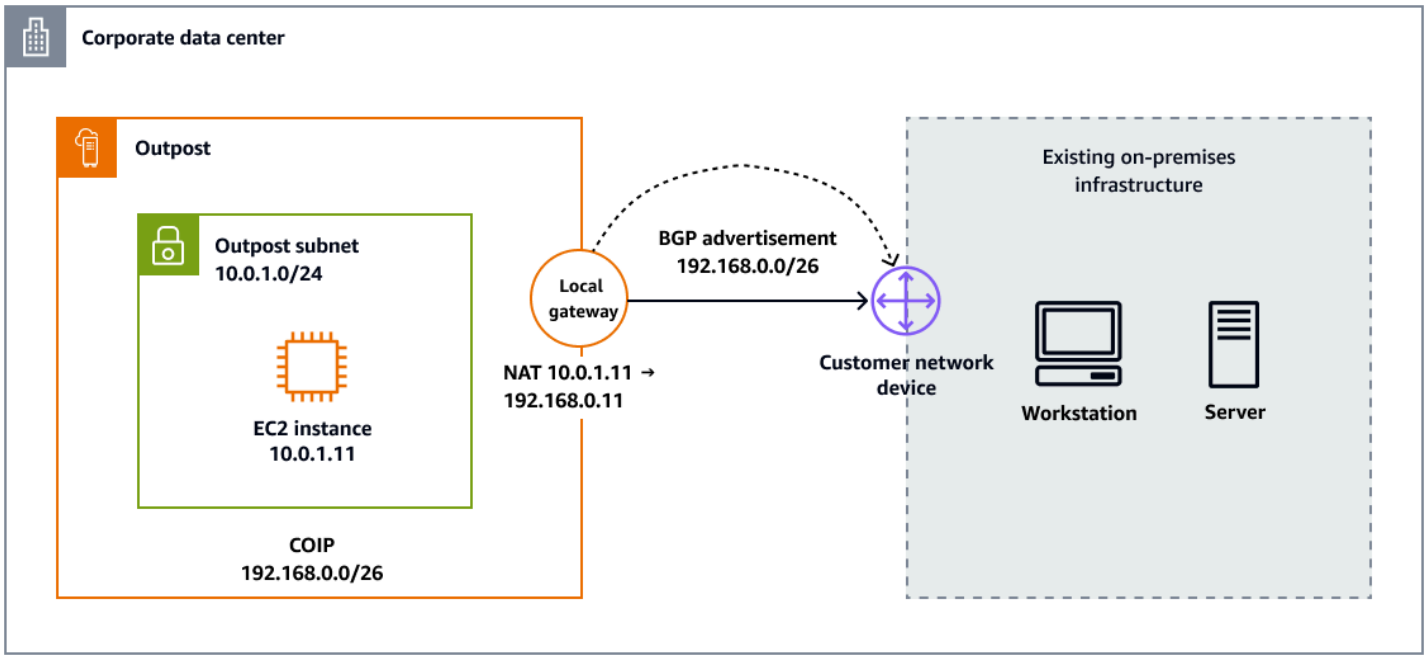
La passerelle locale (LGW) est un composant essentiel de l' AWS Outposts architecture. La passerelle locale permet la connectivité entre vos sous-réseaux Outpost et votre réseau sur site. Le rôle principal d'un LGW est de fournir une connectivité entre un avant-poste et votre réseau local sur site. Il fournit également une connectivité à Internet via votre réseau local via un routage VPC direct ou des adresses IP appartenant au client.

- Le routage VPC direct utilise l'adresse IP privée des instances de votre VPC pour faciliter la communication avec votre réseau local. Ces adresses sont publiées sur votre réseau local via le protocole BGP (Border Gateway Protocol). La publication sur BGP concerne uniquement les adresses IP privées appartenant aux sous-réseaux de votre rack Outpost. Ce type de routage est le mode par défaut pour AWS Outposts. Dans ce mode, la passerelle locale n'exécute pas le NAT pour les instances, et vous n'avez pas besoin d'attribuer d'adresses IP élastiques à vos EC2

instances. Le schéma suivant montre une passerelle AWS Outposts locale qui utilise le routage VPC direct.



- Avec les adresses IP appartenant au client, vous pouvez fournir une plage d'adresses, connue sous le nom de pool d'adresses IP appartenant au client (CoIP), qui prend en charge les plages CIDR qui se chevauchent et les autres topologies de réseau. Lorsque vous choisissez une CoIP, vous devez créer un pool d'adresses, l'attribuer à la table de routage de la passerelle locale et publier ces adresses sur votre réseau via BGP. Les adresses CoIP fournissent une connectivité locale ou externe aux ressources de votre réseau local. Vous pouvez attribuer ces adresses IP aux ressources de votre Outpost, telles que les EC2 instances, en allouant une nouvelle adresse IP élastique depuis le CoIP, puis en l'attribuant à votre ressource. Le schéma suivant montre une passerelle AWS Outposts locale qui utilise le mode CoIP.



La connectivité locale depuis AWS Outposts un réseau local nécessite certaines configurations de paramètres, telles que l'activation du protocole de routage BGP et des préfixes publicitaires entre les homologues BGP. Le MTU qui peut être pris en charge entre votre Outpost et la passerelle locale est de 1 500 octets. Pour plus d'informations, contactez un spécialiste du cloud AWS hybride ou consultez la AWS Outposts documentation.

Zones Locales et Internet

Les secteurs qui ont besoin d'une faible latence ou d'une résidence locale des données (par exemple, les jeux vidéo, le streaming en direct, les services financiers et le gouvernement) peuvent utiliser les Zones Locales pour déployer et fournir leurs applications aux utilisateurs finaux via Internet. Lors du déploiement d'une zone locale, vous devez allouer des adresses IP publiques à utiliser dans une zone locale. Lorsque vous attribuez des adresses IP élastiques, vous pouvez spécifier l'emplacement à partir duquel l'adresse IP est publiée. Cet emplacement est appelé groupe frontalier du réseau. Un groupe frontalier réseau est un ensemble de zones de disponibilité, de zones locales ou de AWS Wavelength zones à partir desquelles AWS une adresse IP publique est annoncée. Cela permet de garantir une latence ou une distance physique minimale entre le AWS réseau et les utilisateurs qui accèdent aux ressources de ces zones. Pour voir tous les groupes de bordures du réseau pour les zones locales, consultez la section Zones locales disponibles dans la documentation relative aux zones locales.

Pour exposer à Internet une charge de travail EC2 hébergée par Amazon dans une zone locale, vous pouvez activer l'option Attribuer automatiquement une adresse IP publique lorsque vous lancez l' EC2 instance. Si vous utilisez un Application Load Balancer, vous pouvez le définir comme étant connecté à Internet afin que les adresses IP publiques attribuées à la zone locale puissent être propagées par le réseau frontalier associé à la zone locale. En outre, lorsque vous utilisez des adresses IP élastiques, vous pouvez associer l'une de ces ressources à une EC2 instance après son lancement. Lorsque vous envoyez du trafic via une passerelle Internet dans les Zones Locales, les mêmes spécifications de bande passante d'instance que celles utilisées par la région sont appliquées. Le trafic réseau de la zone locale est directement dirigé vers Internet ou vers des points de présence (PoPs) sans traverser la région mère de la zone locale, afin de permettre l'accès à un calcul à faible latence.

Les Zones Locales fournissent les options de connectivité suivantes sur Internet :

- Accès public : connecte les charges de travail ou les appareils virtuels à Internet en utilisant des adresses IP élastiques via une passerelle Internet.
- Accès Internet sortant : permet aux ressources d'atteindre les points de terminaison publics par le biais d'instances de traduction d'adresses réseau (NAT) ou d'appliances virtuelles associées à des adresses IP élastiques, sans exposition directe à Internet.
- Connectivité VPN : établit des connexions privées en utilisant le VPN Internet Protocol Security (IPsec) via des appliances virtuelles associées à des adresses IP élastiques.

Pour plus d'informations, consultez la section Options de connectivité pour les zones locales dans la documentation relative aux zones locales.

Zones Locales et AWS Direct Connect

Les Zones Locales sont également compatibles AWS Direct Connect, ce qui vous permet d'acheminer votre trafic via une connexion réseau privée. Pour plus d'informations, consultez Direct Connect in Local Zones dans la documentation Local Zones.

Zones locales et passerelles de transit

AWS Transit Gateway ne prend pas en charge les attachements VPC directs aux sous-réseaux de zone locale. Cependant, vous pouvez vous connecter aux charges de travail de zone locale en créant des pièces jointes Transit Gateway dans les sous-réseaux de zone de disponibilité parents du même VPC. Cette configuration permet l'interconnectivité entre plusieurs charges de travail VPCs et celles

de votre zone locale. Pour plus d'informations, consultez la section Connexion de la passerelle de transit entre les zones locales dans la documentation relative aux zones locales.

Zones Locales et peering VPC

Vous pouvez étendre n'importe quel VPC d'une région parent à une zone locale en créant un nouveau sous-réseau et en l'affectant à la zone locale. Le peering VPC peut être établi entre ces deux zones et les étendre VPCs aux Zones Locales. Lorsque les pairs se VPCs trouvent dans la même zone locale, le trafic reste dans la zone locale et ne passe pas par la région mère.

La sécurité à la périphérie

Dans le AWS Cloud, la sécurité est la priorité absolue. À mesure que les entreprises adoptent l'évolutivité et la flexibilité du cloud, AWS cela les aide à faire de la sécurité, de l'identité et de la conformité des facteurs commerciaux clés. AWS intègre la sécurité dans son infrastructure de base et propose des services pour vous aider à répondre à vos exigences uniques en matière de sécurité dans le cloud. Lorsque vous étendez la portée de votre architecture dans le AWS Cloud, vous bénéficiez de l'intégration d'infrastructures telles que les Zones Locales et les Outposts dans. Régions AWS Cette intégration permet d' AWS étendre un groupe sélectionné de services de sécurité de base jusqu'à la périphérie.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilitéAWS partagée fait la différence entre la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui s'exécute Services AWS dans le AWS Cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de la AWS sécurité dans le cadre des programmes de AWS conformité.
- Sécurité dans le cloud — Votre responsabilité est déterminée par Service AWS ce que vous utilisez. Vous êtes également responsable d’autres facteurs, y compris la sensibilité de vos données, les exigences de votre entreprise, et la législation et la réglementation applicables.

Protection des données

Le modèle de responsabilité AWS partagée s'applique à la protection des données dans AWS Outposts et Zones locales AWS. Comme décrit dans ce modèle, AWS est responsable de la protection de l'infrastructure globale qui gère AWS Cloud (sécurité du cloud). Vous êtes responsable

du contrôle de votre contenu hébergé sur cette infrastructure (sécurité dans le cloud). Ce contenu inclut la configuration de la sécurité et les tâches de gestion pour le Services AWS produit que vous utilisez.

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS Identity and Access Management (IAM) ou AWS IAM Identity Center. Cela donne à chaque utilisateur uniquement les autorisations nécessaires pour accomplir ses tâches.

Chiffrement au repos

Chiffrement dans les volumes EBS

Avec AWS Outposts, toutes les données sont cryptées au repos. Le matériau clé est enveloppé d'une clé externe, la clé de sécurité Nitro (NSK), qui est stockée dans un appareil amovible. Le NSK est nécessaire pour déchiffrer les données de votre rack Outpost. Vous pouvez utiliser le chiffrement Amazon EBS pour vos volumes et instantanés EBS. Le chiffrement Amazon EBS utilise AWS Key Management Service (AWS KMS) et des clés KMS.

Dans le cas des zones locales, tous les volumes EBS sont chiffrés par défaut dans toutes les zones locales, à l'exception de la liste décrite dans la Zones locales AWS FAQ (voir la question : Quel est le comportement de chiffrement par défaut des volumes EBS dans les zones locales ?), sauf si le chiffrement est activé pour le compte.

Chiffrement dans Amazon S3 sur Outposts

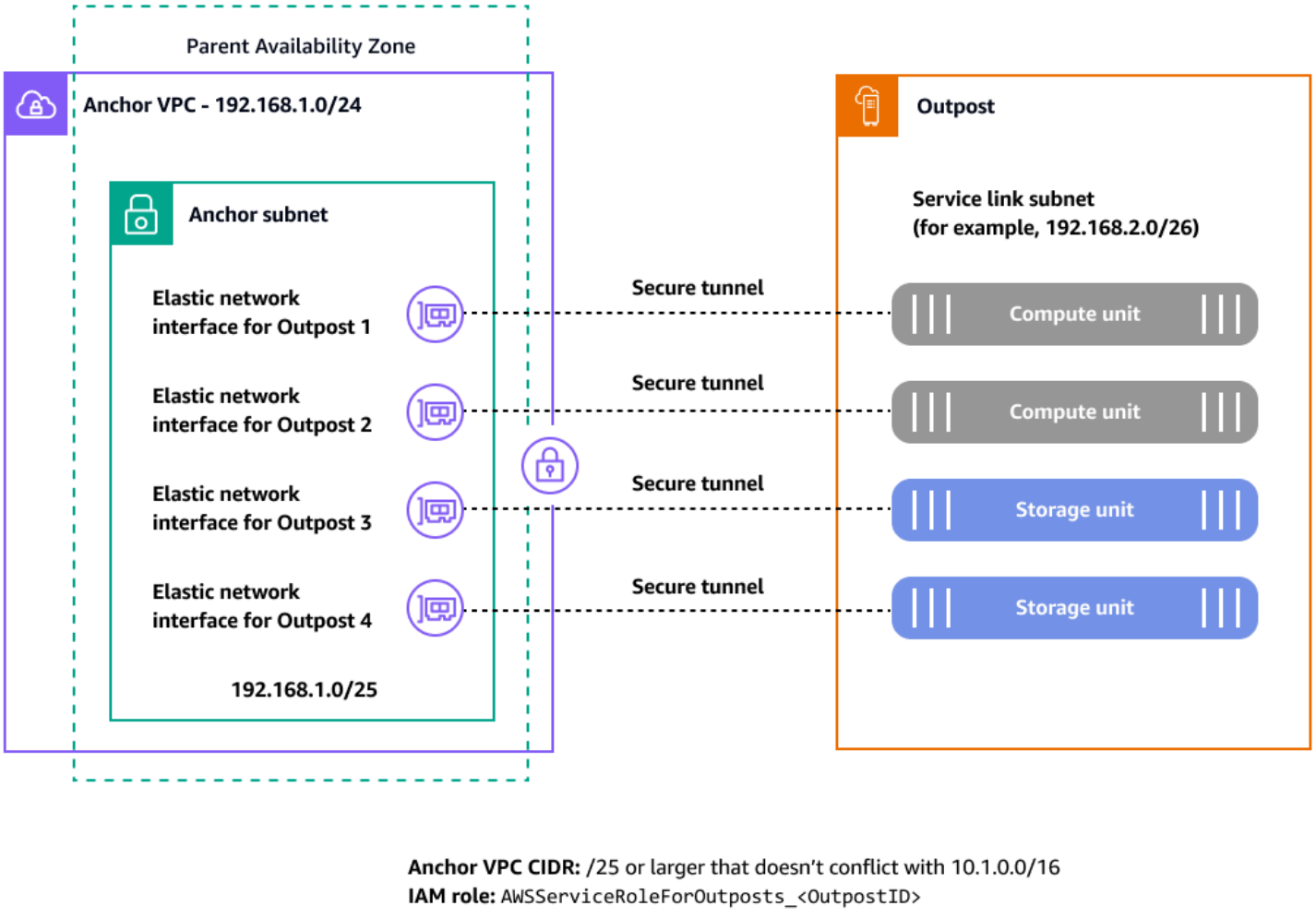
Par défaut, toutes les données stockées dans Amazon S3 sur Outposts sont chiffrées à l’aide du chiffrement côté serveur avec les clés de chiffrement gérées Amazon S3 (SSE-S3). Vous pouvez éventuellement utiliser le chiffrement côté serveur avec les clés de chiffrement fournies par le client (SSE-C). Pour utiliser SSE-C, spécifiez une clé de chiffrement dans le cadre de vos demandes d’API sur les objets. Un chiffrement côté serveur chiffre uniquement les données d’objet, pas les métadonnées d’objet.

> **Note**
>
> Amazon S3 on Outposts ne prend pas en charge le chiffrement côté serveur avec des clés KMS (SSE-KMS).

Chiffrement en transit

En AWS Outposts effet, le lien de service est une connexion nécessaire entre votre serveur Outposts et la région de votre choix Région AWS (ou de votre région d'origine) et permet la gestion de l'Outpost et l'échange de trafic vers et depuis le. Région AWS Le lien de service utilise un VPN AWS géré pour communiquer avec la région d'origine. Chaque hôte interne AWS Outposts crée un ensemble de tunnels VPN pour diviser le trafic du plan de contrôle et le trafic VPC. En fonction de la connectivité du lien de service (Internet ou AWS Direct Connect) AWS Outposts, ces tunnels nécessitent l'ouverture de ports de pare-feu pour que le lien de service puisse créer une superposition au-dessus de celui-ci. Pour obtenir des informations techniques détaillées sur la sécurité AWS Outposts et le lien de service, voir Connectivité via le lien de service et Sécurité de l'infrastructure AWS Outposts dans la AWS Outposts documentation.

Le lien AWS Outposts de service crée des tunnels chiffrés qui établissent la connectivité du plan de contrôle et du plan de données avec le parent Région AWS, comme illustré dans le schéma suivant.



Chaque AWS Outposts hôte (calcul et stockage) a besoin de ces tunnels chiffrés via des ports TCP et UDP connus pour communiquer avec sa région mère. Le tableau suivant indique les ports et adresses source et de destination pour les protocoles UDP et TCP.

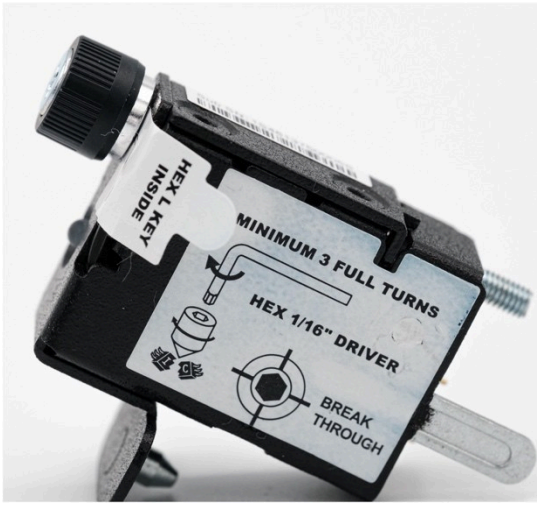
Protocole	Port source	Adresse source	Port de destination	Adresse de destination
UDP	443	AWS Outposts liaison de service /26	443	AWS Outposts Routes publiques de la région ou VPC CIDR d'ancrage
TCP	1025-65535	AWS Outposts liaison de service /26	443	AWS Outposts Routes publiques de la région ou VPC CIDR d'ancrage

Les zones Locales sont également connectées à la région mère via le backbone privé mondial redondant et à très haut débit d'Amazon. Cette connexion permet aux applications qui s'exécutent dans les Zones Locales d'accéder rapidement, de manière sécurisée et fluide aux autres Services AWS. Tant que les Zones Locales font partie de l'infrastructure AWS mondiale, toutes les données circulant sur le réseau AWS mondial sont automatiquement cryptées au niveau de la couche physique avant de quitter les installations AWS sécurisées. Si vous avez des exigences spécifiques pour chiffrer les données en transit entre vos sites locaux et AWS Direct Connect PoPs pour accéder à une zone locale, vous pouvez activer la sécurité MAC (MACsec) entre votre routeur ou commutateur local et le point de terminaison. AWS Direct Connect Pour plus d'informations, consultez le billet de AWS blog Ajouter MACsec de la sécurité aux AWS Direct Connect connexions.

Suppression de données

Lorsque vous arrêtez ou mettez fin à une EC2 instance AWS Outposts, la mémoire qui lui est allouée est nettoyée (mise à zéro) par l'hyperviseur avant d'être allouée à une nouvelle instance, et chaque bloc de stockage est réinitialisé. La suppression de données du matériel Outpost implique l'utilisation de matériel spécialisé. Le NSK est un petit appareil, illustré sur la photo suivante, qui se fixe à l'avant de chaque ordinateur ou unité de stockage d'un avant-poste. Il est conçu pour fournir un mécanisme

permettant d'empêcher l'exposition de vos données depuis votre centre de données ou votre site de colocation. Les données de l'appareil Outpost sont protégées en enveloppant le matériel de saisie utilisé pour chiffrer l'appareil et en stockant le matériel emballé sur le NSK. Lorsque vous renvoyez un hôte d'Outpost, vous détruisez le NSK en tournant une petite vis sur le jeton qui écrase le NSK et détruit physiquement le jeton. La destruction du NSK détruit les données de votre avant-poste de manière cryptographique.



Identity and Access Management

AWS Identity and Access Management (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser AWS Outposts les ressources. Si vous en avez un Compte AWS, vous pouvez utiliser IAM sans frais supplémentaires.

Le tableau suivant répertorie les fonctionnalités IAM que vous pouvez utiliser avec AWS Outposts.

Fonctionnalité IAM	AWS Outposts soutien
Politiques basées sur l’identité	Oui
Politiques basées sur les ressources	Oui*
Actions de politique	Oui
Ressources de politique	Oui

Fonctionnalité IAM	AWS Outposts soutien
Clés de condition de politique (spécifiques au service)	Oui
Listes de contrôle d'accès (ACLs)	Non
Contrôle d'accès basé sur les attributs (ABAC) (balises dans les politiques)	Oui
Informations d’identification temporaires	Oui
Autorisations de principal	Oui
Fonctions du service	Non
Rôles liés à un service	Oui

* Outre les politiques basées sur l'identité IAM, Amazon S3 on Outposts prend en charge les politiques relatives aux compartiments et aux points d'accès. Il s'agit de politiques basées sur les ressources associées à la ressource Amazon S3 on Outposts.

Pour plus d'informations sur la prise en charge de ces fonctionnalités AWS Outposts, consultez le guide de AWS Outposts l'utilisateur.

Sécurité de l'infrastructure

La protection de l’infrastructure est un aspect essentiel du programme de sécurité des informations. Il garantit que les systèmes et services de charge de travail sont protégés contre les accès involontaires et non autorisés, ainsi que contre les vulnérabilités potentielles. Par exemple, vous définissez les limites de confiance (par exemple, les limites du réseau et des comptes), la configuration et la maintenance de la sécurité du système (par exemple, renforcement, minimisation et application de correctifs), l'authentification et les autorisations du système d'exploitation (par exemple, les utilisateurs, les clés et les niveaux d'accès) et les autres points d'application des politiques appropriés (par exemple, les pare-feux d'applications Web ou les passerelles d'API).

AWS propose un certain nombre d'approches en matière de protection de l'infrastructure, comme indiqué dans les sections suivantes.

Protection des réseaux

Vos utilisateurs peuvent faire partie de votre personnel ou de vos clients, et peuvent être situés n'importe où. Pour cette raison, vous ne pouvez pas faire confiance à tous ceux qui ont accès à votre réseau. Lorsque vous appliquez le principe de sécurité à tous les niveaux, vous adoptez une approche zéro confiance. Dans le modèle de sécurité Zero Trust, les composants d'application ou les microservices sont considérés comme discrets, et aucun composant ou microservice ne fait confiance à aucun autre composant ou microservice. Pour atteindre une sécurité zéro confiance, suivez les recommandations suivantes :

- Créez des couches réseau. Les réseaux en couches permettent de regrouper de manière logique des composants réseau similaires. Ils réduisent également l'impact potentiel d'un accès non autorisé au réseau.
- Contrôlez les couches de trafic. Appliquez plusieurs contrôles avec une defense-in-depth approche à la fois pour le trafic entrant et sortant. Cela inclut l'utilisation de groupes de sécurité (pare-feux d'inspection dynamiques), de réseaux ACLs, de sous-réseaux et de tables de routage.
- Mettre en œuvre l'inspection et la protection. Inspectez et filtrez votre trafic à chaque niveau. Vous pouvez inspecter vos configurations VPC pour détecter tout accès involontaire potentiel à l'aide de l'analyseur d'accès réseau. Vous pouvez définir vos exigences en matière d'accès au réseau et identifier les chemins réseau potentiels qui ne les respectent pas.

Protection des ressources informatiques

Les ressources informatiques incluent les EC2 instances, les conteneurs, AWS Lambda les fonctions, les services de base de données, les appareils IoT, etc. Chaque type de ressource de calcul nécessite une approche différente en matière de sécurité. Cependant, ces ressources partagent des stratégies communes que vous devez prendre en compte : défense en profondeur, gestion des vulnérabilités, réduction de la surface d'attaque, automatisation de la configuration et du fonctionnement, et réalisation d'actions à distance.

Voici des conseils généraux pour protéger vos ressources informatiques pour les services clés :

- Créez et maintenez un programme de gestion des vulnérabilités. Scannez et corrigez régulièrement les ressources telles que EC2 les instances, les conteneurs Amazon Elastic Container Service (Amazon ECS) et les charges de travail Amazon Elastic Kubernetes Service (Amazon EKS).

- Automatisez la protection informatique. Automatisez vos mécanismes informatiques de protection, notamment la gestion des vulnérabilités, la réduction de la surface d'attaque et la gestion des ressources. Cette automatisation libère du temps que vous pouvez utiliser pour sécuriser d'autres aspects de votre charge de travail et contribue à réduire le risque d'erreur humaine.
- Réduisez la surface d'attaque. Réduisez votre exposition aux accès involontaires en renforçant vos systèmes d'exploitation et en minimisant les composants, les bibliothèques et les services consommables externes que vous utilisez.

En outre, pour chacune des Service AWS applications que vous utilisez, consultez les recommandations de sécurité spécifiques dans la documentation du service.

Accès Internet

Les deux, AWS Outposts ainsi que les Zones Locales, fournissent des modèles architecturaux qui permettent à vos charges de travail d'accéder à Internet et à partir de celui-ci. Lorsque vous utilisez ces modèles, considérez la consommation Internet depuis la région comme une option viable uniquement si vous l'utilisez pour appliquer des correctifs, mettre à jour, accéder à des référentiels Git externes à Git AWS, etc. Pour ce modèle architectural, les concepts d'inspection entrante centralisée et de sortie Internet centralisée s'appliquent. Ces modèles d'accès utilisent des passerelles NAT AWS Transit Gateway, des pare-feux réseau et d'autres composants résidant dans des zones locales Régions AWS, mais y étant AWS Outposts connectés, via le chemin de données entre la région et la périphérie.

Local Zones adopte une structure de réseau appelée groupe de frontières de réseau, qui est utilisée dans Régions AWS. AWS annonce les adresses IP publiques de ces groupes uniques. Un groupe frontalier du réseau est composé de zones de disponibilité, de zones locales ou de zones de longueur d'onde. Vous pouvez attribuer explicitement un pool d'adresses IP publiques à utiliser dans un groupe frontalier du réseau. Vous pouvez utiliser un groupe de bordure réseau pour étendre la passerelle Internet aux Zones Locales en autorisant le service d'adresses IP Elastic à partir du groupe. Cette option nécessite le déploiement d'autres composants pour compléter les services de base disponibles dans les Zones Locales. Ces composants peuvent provenir de votre zone locale ISVs et vous aider à créer des couches d'inspection, comme décrit dans le billet de AWS blog Architectures d'inspection hybrides avec Zones locales AWS.

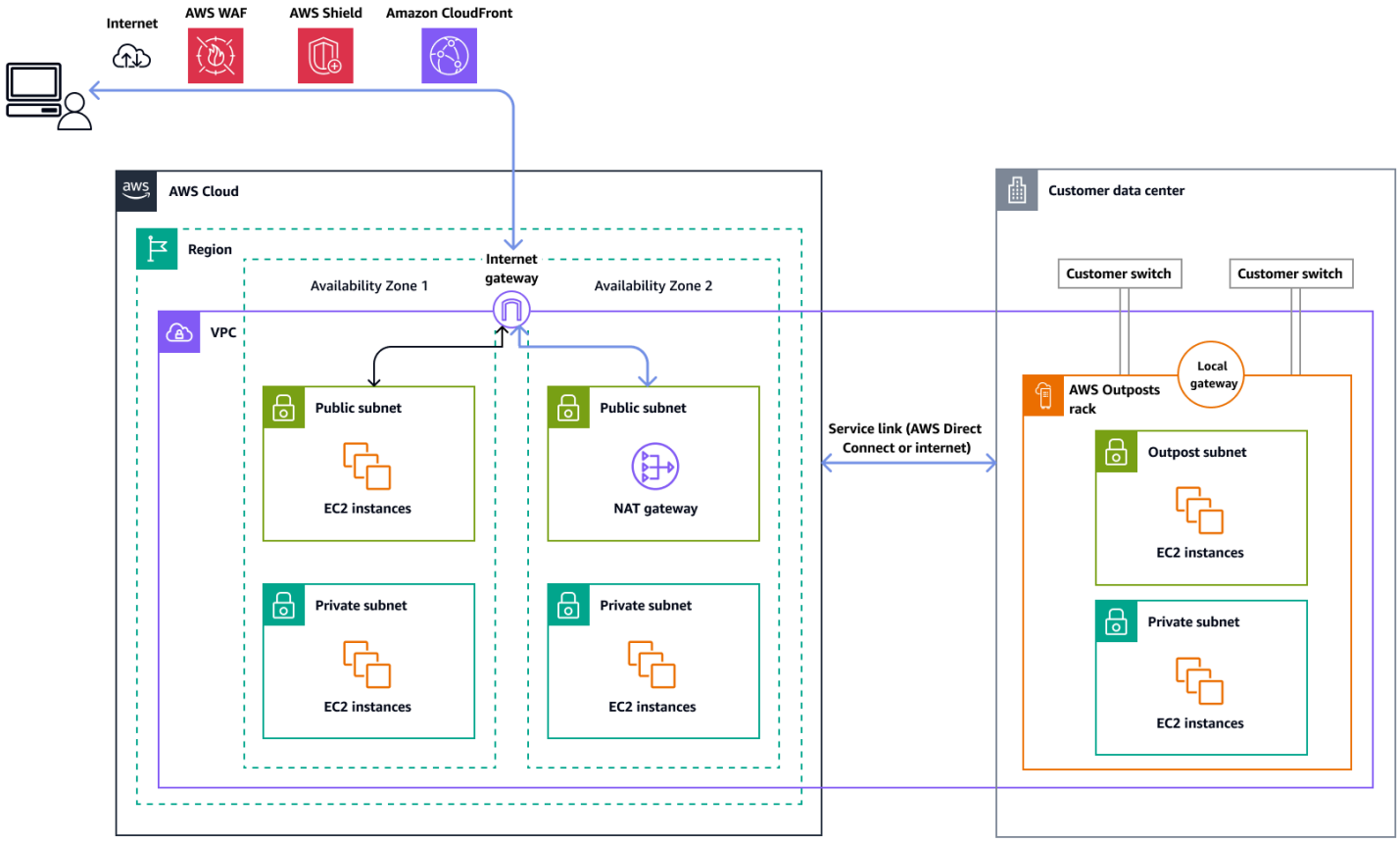
Dans AWS Outposts, si vous souhaitez utiliser la passerelle locale (LGW) pour accéder à Internet depuis votre réseau, vous devez modifier la table de routage personnalisée associée au AWS Outposts sous-réseau. La table de routage doit avoir une entrée de route par défaut (0.0.0.0/0) qui

utilise le LGW comme prochain saut. Vous êtes responsable de la mise en œuvre des contrôles de sécurité restants dans votre réseau local, y compris les défenses périmétriques telles que les pare-feux et les systèmes de prévention des intrusions ou les systèmes de détection des intrusions (IPS/IDS). Cela correspond au modèle de responsabilité partagée, qui répartit les tâches de sécurité entre vous et le fournisseur de cloud.

Accès à Internet par l'intermédiaire du parent Région AWS

Dans cette option, les charges de travail de l'Outpost accèdent à Internet via le lien de service et la passerelle Internet du parent. Région AWS Le trafic sortant vers Internet peut être acheminé via la passerelle NAT instanciée dans votre VPC. Pour renforcer la sécurité de votre trafic entrant et sortant, vous pouvez utiliser des services AWS de sécurité tels que AWS WAF, AWS Shield, et Amazon CloudFront dans le. Région AWS

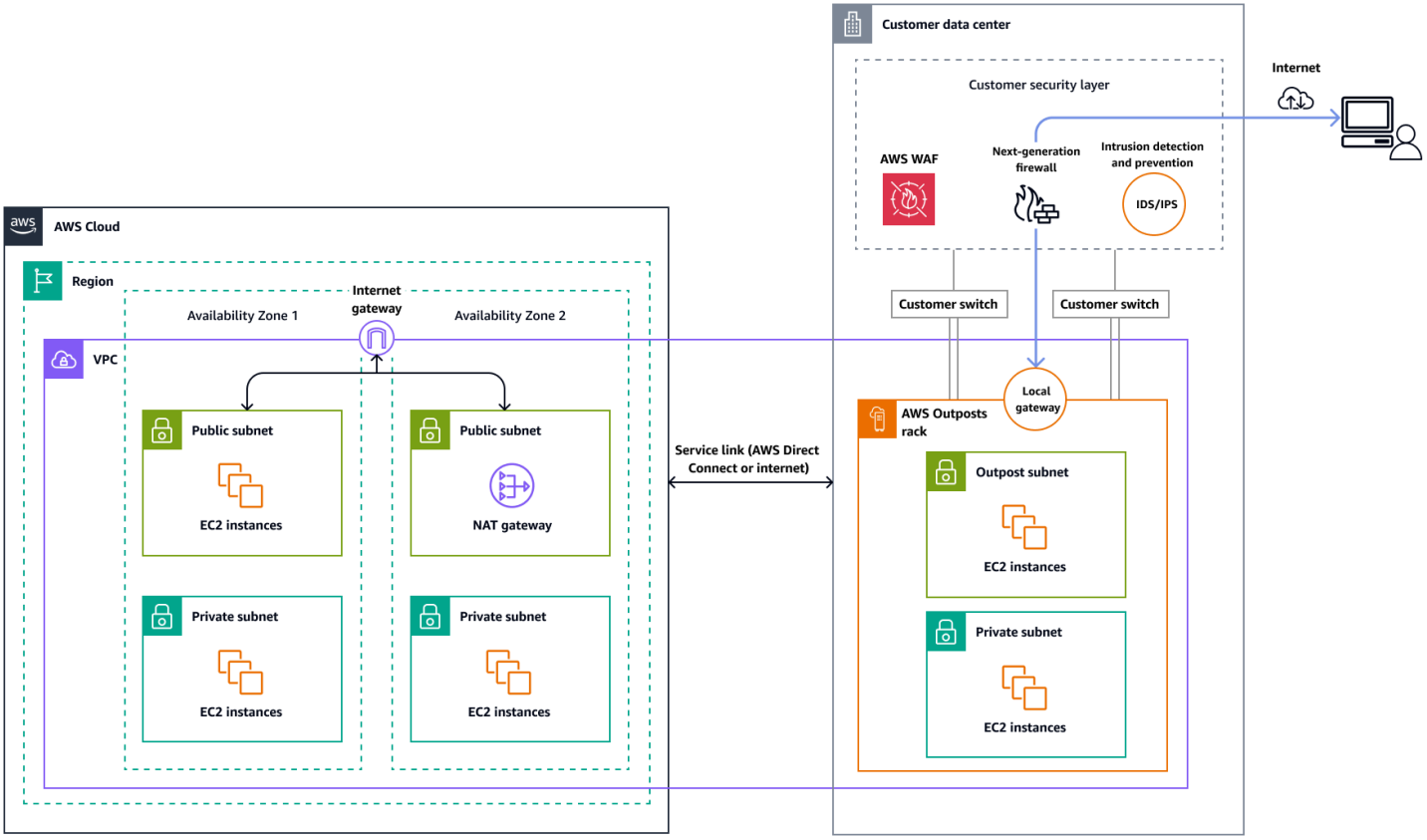
Le schéma suivant montre le trafic entre la charge de travail de l' AWS Outposts instance et Internet passant par le parent Région AWS.



Accès à Internet via le réseau de votre centre de données local

Dans cette option, les charges de travail de l'Outpost accèdent à Internet via votre centre de données local. Le trafic de charge de travail qui accède à Internet passe par votre point de présence Internet local et sort localement. Dans ce cas, l'infrastructure de sécurité réseau de votre centre de données local est chargée de sécuriser le trafic de AWS Outposts charge de travail.

L'image suivante montre le trafic entre une charge de travail du AWS Outposts sous-réseau et Internet passant par un centre de données.



Gouvernance de l'infrastructure

Que vos charges de travail soient déployées dans une zone locale ou un Région AWS avant-poste, vous pouvez les utiliser AWS Control Tower pour la gouvernance de l'infrastructure. AWS Control Tower propose un moyen simple de configurer et de gérer un environnement AWS multi-comptes, en suivant les meilleures pratiques prescriptives. AWS Control Tower orchestre les capacités de plusieurs autres Services AWS, notamment AWS Organizations AWS Service Catalog, et IAM Identity Center (voir tous les services intégrés) pour créer une zone d'atterrissage en moins d'une heure. Les ressources sont configurées et gérées en votre nom.

AWS Control Tower fournit une gouvernance unifiée dans tous les AWS environnements, y compris les régions, les zones locales (extensions à faible latence) et les Outposts (infrastructure sur site). Cela permet de garantir une sécurité et une conformité cohérentes sur l'ensemble de votre architecture de cloud hybride. Pour plus d'informations, consultez la documentation AWS Control Tower.

Vous pouvez configurer AWS Control Tower des fonctionnalités telles que des garde-corps pour vous conformer aux exigences en matière de résidence des données dans les gouvernements et les secteurs réglementés tels que les institutions de services financiers ()FSIs. Pour comprendre comment déployer des barrières de sécurité pour la résidence des données à la périphérie, consultez ce qui suit :

- Meilleures pratiques pour gérer la résidence des données lors de Zones locales AWS l'utilisation des contrôles de zone d'atterrissage (article de AWS blog)
- Architecture pour la résidence des données à l'aide de glissières de sécurité pour les AWS Outposts racks et les zones d'atterrissage (article de blog)AWS
- Résidence des données avec l'objectif des services cloud hybrides (documentationAWS Well-Architected Framework)

Partage des ressources des Outposts

Comme un avant-poste est une infrastructure limitée installée dans votre centre de données ou dans un espace de colocation, pour une gouvernance centralisée AWS Outposts, vous devez contrôler de manière centralisée les comptes avec lesquels les AWS Outposts ressources sont partagées.

Grâce au partage d'Outpost, les propriétaires d'Outposts peuvent partager leurs Outposts et leurs ressources, y compris leurs sites et sous-réseaux, avec d'autres Comptes AWS utilisateurs de la même organisation dans. AWS Organizations En tant que propriétaire d'Outpost, vous pouvez créer et gérer les ressources d'Outpost à partir d'un emplacement central, et partager les ressources entre plusieurs personnes Comptes AWS au sein de votre AWS organisation. Cela permet aux autres consommateurs d'utiliser les sites Outpost, de configurer VPCs, de lancer et d'exécuter des instances sur l'Outpost partagé.

Les ressources partageables AWS Outposts sont les suivantes :

- Hôtes dédiés alloués
- Réserves de capacité

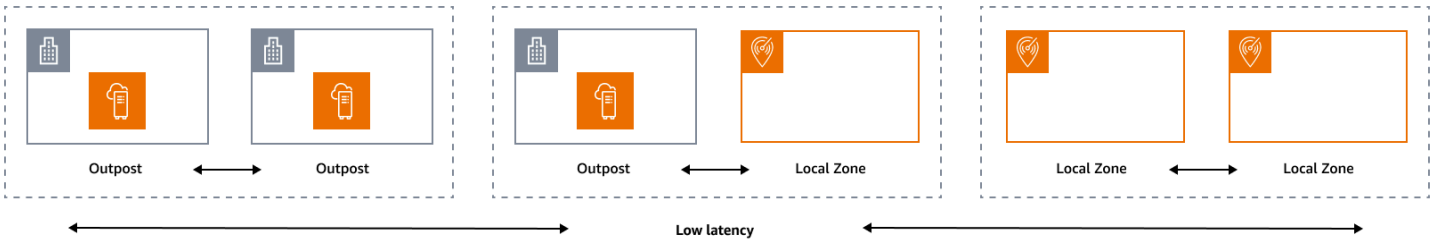
- Pools d'adresses IP appartenant au client (CoIP)
- Tables de routage de passerelle locale
- Outposts
- Amazon S3 sur Outposts
- Sites
- Sous-réseaux

Pour suivre les meilleures pratiques en matière de partage des ressources d'Outposts dans un environnement multi-comptes, consultez les articles de blog suivants : AWS

- Partage AWS Outposts dans un AWS environnement multi-comptes : partie 1
- Partage AWS Outposts dans un AWS environnement multi-comptes : partie 2

Résilience à la périphérie

Le pilier de fiabilité englobe la capacité d'une charge de travail à exécuter correctement et de manière cohérente la fonction prévue lorsqu'elle est censée le faire. Cela inclut la capacité d'exploiter et de tester la charge de travail tout au long de son cycle de vie. En ce sens, lorsque vous concevez une architecture résiliente à la périphérie, vous devez d'abord déterminer quelles infrastructures vous utiliserez pour déployer cette architecture. Il existe trois combinaisons possibles à implémenter en utilisant Zones locales AWS et AWS Outposts : avant-poste vers avant-poste, avant-poste vers zone locale et zone locale vers zone locale, comme illustré dans le schéma suivant. Bien qu'il existe d'autres possibilités pour les architectures résilientes, telles que la combinaison de services de AWS périphérie avec une infrastructure sur site traditionnelle Régions AWS, ce guide se concentre sur ces trois combinaisons qui s'appliquent à la conception de services de cloud hybride



Considérations relatives à l’infrastructure

À AWS, l'un des principes fondamentaux de la conception des services est d'éviter les points de défaillance uniques dans l'infrastructure physique sous-jacente. En raison de ce principe, les AWS

logiciels et les systèmes utilisent plusieurs zones de disponibilité et résistent à la défaillance d'une seule zone. À la périphérie, AWS propose des infrastructures basées sur les Zones Locales et les Outposts. Par conséquent, un facteur essentiel pour garantir la résilience lors de la conception de l'infrastructure consiste à définir où les ressources d'une application sont déployées.

Zones locales

Les zones locales agissent de la même manière que les zones de disponibilité qui les composent Région AWS, car elles peuvent être sélectionnées comme emplacement pour les AWS ressources zonales telles que les sous-réseaux et EC2 les instances. Cependant, ils ne sont pas situés dans un Région AWS, mais à proximité de grands centres industriels et informatiques où il n'en Région AWS existe pas aujourd'hui. Malgré cela, ils conservent des connexions sécurisées à bande passante élevée entre les charges de travail locales de la zone locale et les charges de travail exécutées dans le. Région AWS Par conséquent, vous devez utiliser les Zones Locales pour déployer les charges de travail au plus près de vos utilisateurs afin de garantir une faible latence.

Outposts

AWS Outposts est un service entièrement géré qui étend AWS l'infrastructure et Services AWS APIs les outils à votre centre de données. La même infrastructure matérielle que celle utilisée dans le AWS Cloud est installée dans votre centre de données. Les Outposts sont ensuite connectés aux plus proches. Région AWS Vous pouvez utiliser les Outposts pour prendre en charge vos charges de travail nécessitant une faible latence ou nécessitant un traitement local des données.

Zones de disponibilité pour les parents

Chaque zone locale ou avant-poste possède une région parent (également appelée région d'origine). La région parent est l'endroit où le plan de contrôle de l'infrastructure AWS périphérique (avant-poste ou zone locale) est ancré. Dans le cas des zones locales, la région parent est un composant architectural fondamental d'une zone locale et ne peut pas être modifiée par les clients. AWS Outposts l'étend AWS Cloud à votre environnement sur site. Vous devez donc sélectionner une région et une zone de disponibilité spécifiques lors du processus de commande. Cette sélection ancre le plan de contrôle de votre déploiement d'Outposts à l' AWS infrastructure choisie.

Lorsque vous développez des architectures de haute disponibilité en périphérie, la région parent de ces infrastructures, telle que les Outposts ou les Zones Locales, doit être identique, afin qu'un VPC puisse être étendu entre elles. Ce VPC étendu est à la base de la création de ces architectures à haute disponibilité. Lorsque vous définissez une architecture hautement résiliente, vous devez donc

valider la région parent et la zone de disponibilité de la région dans laquelle le service sera (ou est) ancré. Comme illustré dans le schéma suivant, si vous souhaitez déployer une solution de haute disponibilité entre deux Outposts, vous devez choisir deux zones de disponibilité différentes pour ancrer les Outposts. Cela permet une architecture multi-AZ du point de vue du plan de contrôle. Si vous souhaitez déployer une solution à haute disponibilité incluant une ou plusieurs zones locales, vous devez d'abord valider la zone de disponibilité parent dans laquelle l'infrastructure est ancrée. Pour cela, utilisez la AWS CLI commande suivante :

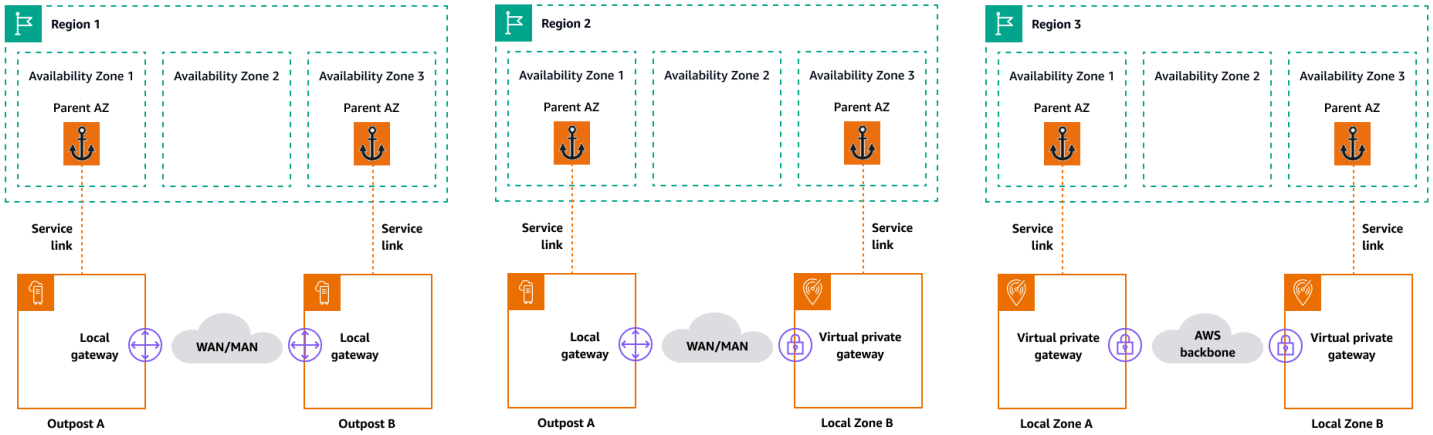
```
aws ec2 describe-availability-zones --zone-ids use1-mia1-az1
```

Résultat de la commande précédente :

```
{     "AvailabilityZones": [
          {
             "State": "available",
             "OptInStatus": "opted-in",
             "Messages": [],
             "RegionName": "us-east-1",
             "ZoneName": "us-east-1-mia-1a",
             "ZoneId": "use1-mia1-az1",
             "GroupName": "us-east-1-mia-1",
             "NetworkBorderGroup": "us-east-1-mia-1",
             "ZoneType": "local-zone",
             "ParentZoneName": "us-east-1d",
             "ParentZoneId": "use1-az2"
          }
     ]
 }
```

Dans cet exemple, la zone locale de Miami (`us-east-1d-mia-1a1`) est ancrée dans la zone de `us-east-1d-az2` disponibilité. Par conséquent, si vous devez créer une architecture résiliente à la périphérie, vous devez vous assurer que l'infrastructure secondaire (Outposts ou Zones Locales) est ancrée dans une zone de disponibilité autre que. **`us-east-1d-az2`** Par exemple, `us-east-1d-az1` serait valide.

Le schéma suivant fournit des exemples d'infrastructures périphériques à haute disponibilité.



Considérations relatives au réseau

Cette section décrit les considérations initiales relatives à la mise en réseau en périphérie, principalement pour les connexions permettant d'accéder à l'infrastructure périphérique. Il passe en revue les architectures valides qui fournissent un réseau résilient pour le lien de service.

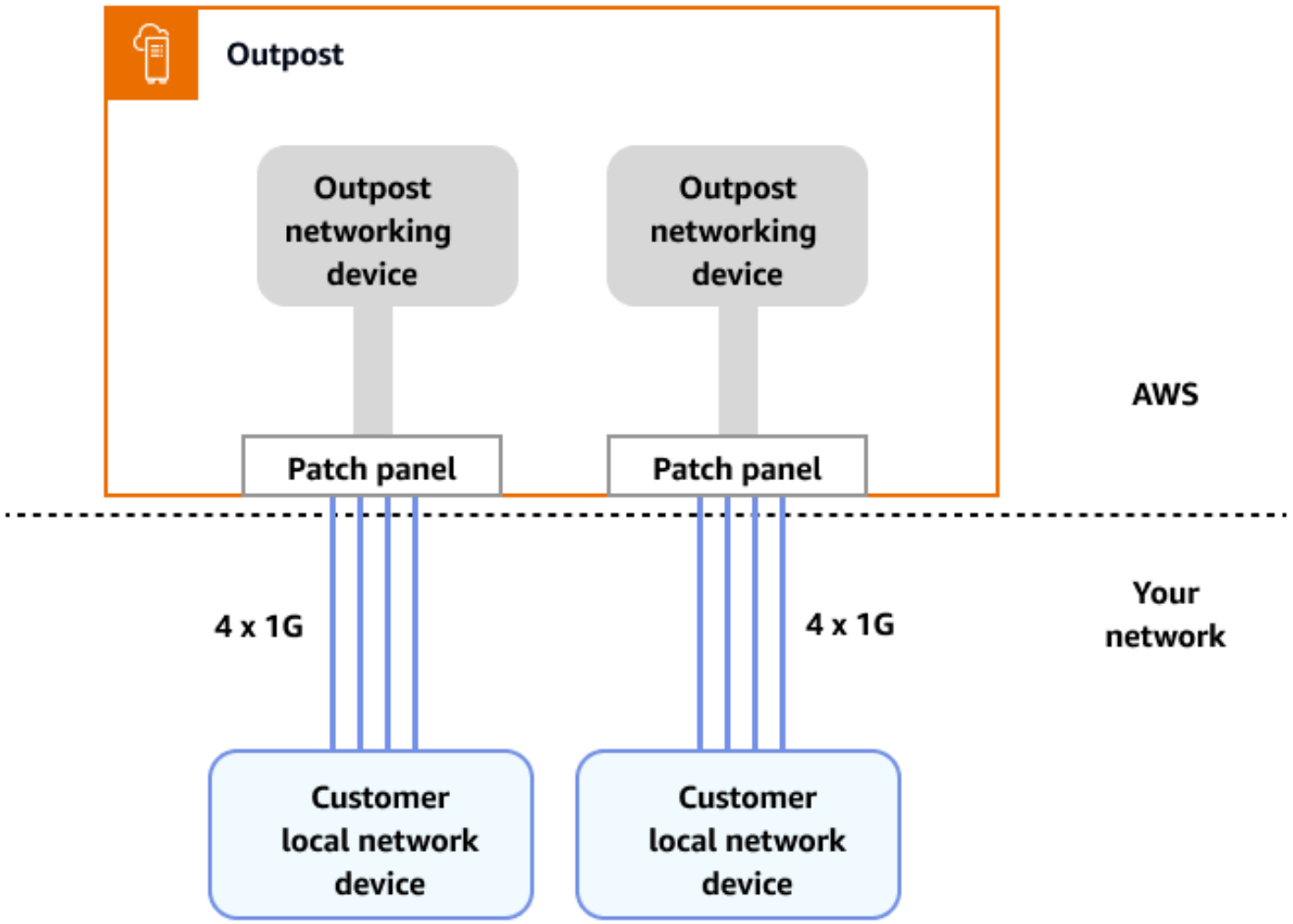
Réseau de résilience pour les Zones Locales

Les Zones Locales sont connectées à la région mère par de multiples liaisons haut débit sécurisées et redondantes qui vous permettent d'utiliser n'importe quel service régional, tel qu'Amazon S3 et Amazon RDS, de manière fluide. Vous êtes responsable de fournir la connectivité entre votre environnement local ou vos utilisateurs et la zone locale. Quelle que soit l'architecture de connectivité que vous choisissez (par exemple, VPN ou AWS Direct Connect), la latence qui doit être atteinte via les liens réseau doit être équivalente pour éviter tout impact sur les performances de l'application en cas de défaillance d'une liaison principale. Si vous l'utilisez AWS Direct Connect, les architectures de résilience applicables sont les mêmes que celles permettant d'accéder à un Région AWS, comme indiqué dans les recommandations de AWS Direct Connect résilience. Cependant, certains scénarios s'appliquent principalement aux Zones Locales internationales. Dans le pays où la zone locale est activée, le fait de n'avoir qu'un AWS Direct Connect seul PoP rend impossible la création des architectures recommandées pour AWS Direct Connect la résilience. Si vous n'avez accès qu'à un seul AWS Direct Connect emplacement ou si vous avez besoin d'une résilience allant au-delà d'une simple connexion, vous pouvez créer une appliance VPN sur Amazon EC2 et AWS Direct Connect, comme illustré et expliqué dans le billet de AWS blog Activer la connectivité hautement disponible sur site vers Zones locales AWS.

Réseau de résilience pour les Outposts

Contrairement aux Zones Locales, les Outposts disposent d'une connectivité redondante pour accéder aux charges de travail déployées dans les Outposts depuis votre réseau local. Cette redondance est obtenue grâce à deux périphériques réseau Outposts (). ONDs Chaque OND nécessite au moins deux connexions par fibre optique à 1 Gbit/s, 10 Gbit/s, 40 Gbit/s ou 100 Gbit/s vers votre réseau local. Ces connexions doivent être configurées en tant que groupe d'agrégation de liens (LAG) pour permettre l'ajout évolutif de liens supplémentaires.

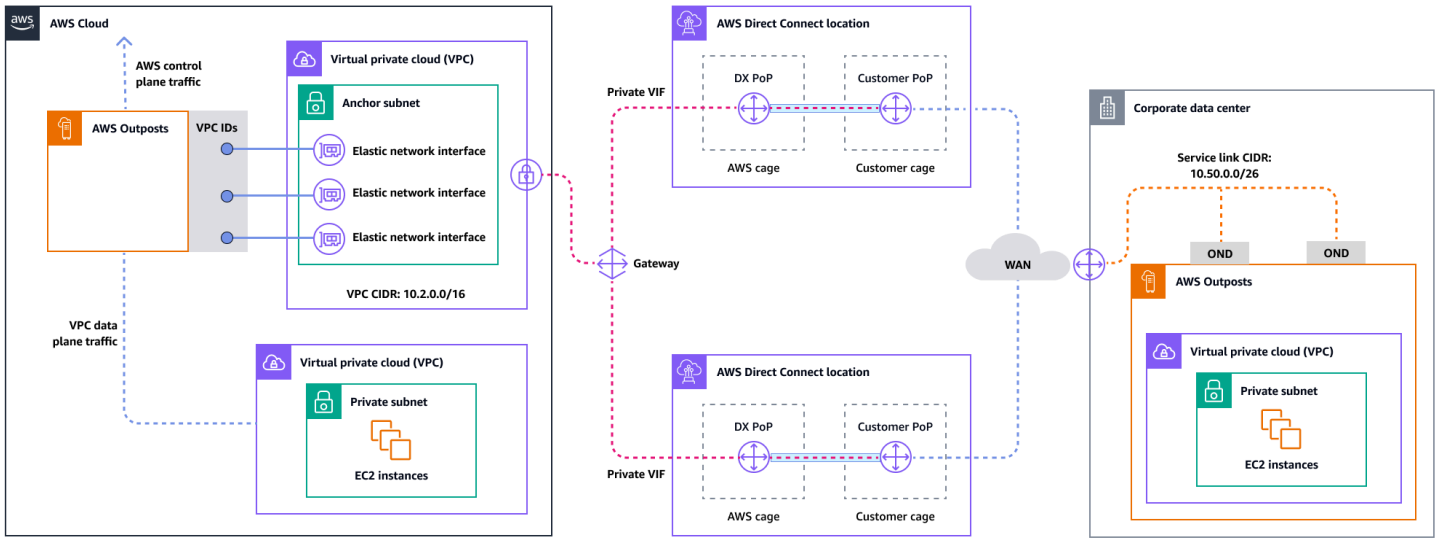
Vitesse de la liaison montante	Nombre de liaisons montantes
1 Gbit/s	1, 2, 4, 6 ou 8
10 Gbit/s	1, 2, 4, 8, 12 ou 16
40 ou 100 Gbit/s	1, 2 ou 4



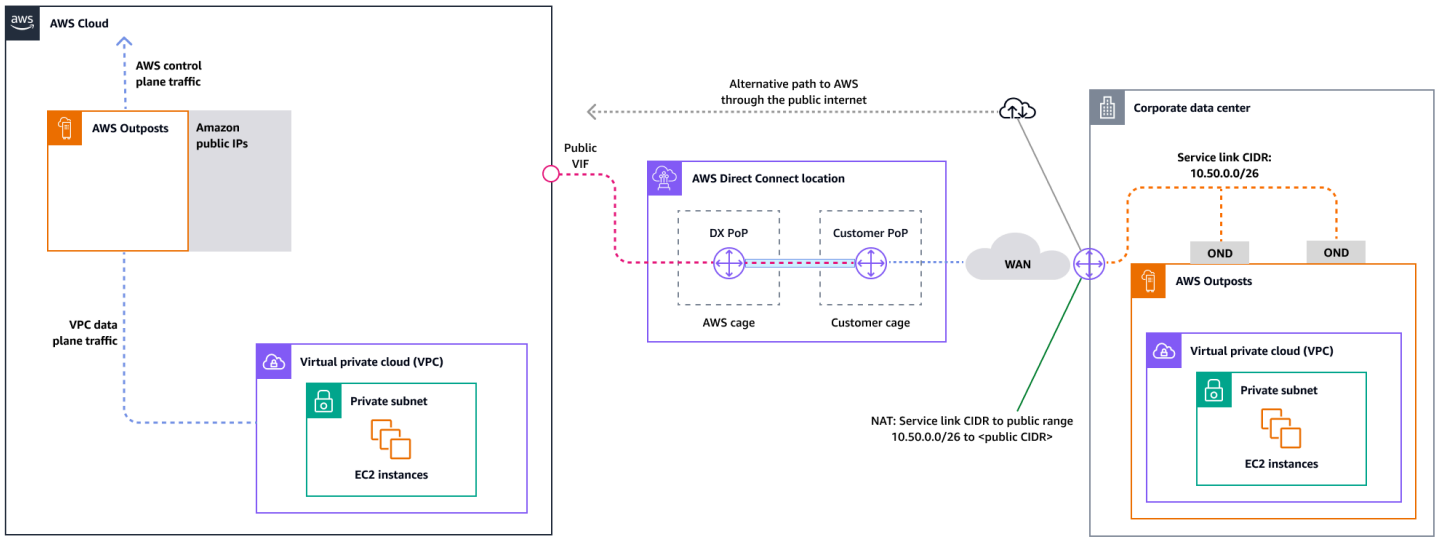
Pour plus d'informations sur cette connectivité, consultez la section Connectivité réseau locale pour les Outposts Racks dans la documentation. AWS Outposts

Pour une expérience et une résilience optimales, il est AWS recommandé d'utiliser une connectivité redondante d'au moins 500 Mbit/s (1 Gbit/s est préférable) pour la connexion par liaison de service au. Région AWS Vous pouvez utiliser AWS Direct Connect une connexion Internet pour le lien de service. Ce minimum vous permet de lancer des EC2 instances, d'attacher des volumes EBS et d'y accéder Services AWS, comme Amazon EKS, Amazon EMR et des métriques. CloudWatch

Le schéma suivant illustre cette architecture pour une connexion privée à haute disponibilité.



Le schéma suivant illustre cette architecture pour une connexion publique à haute disponibilité.



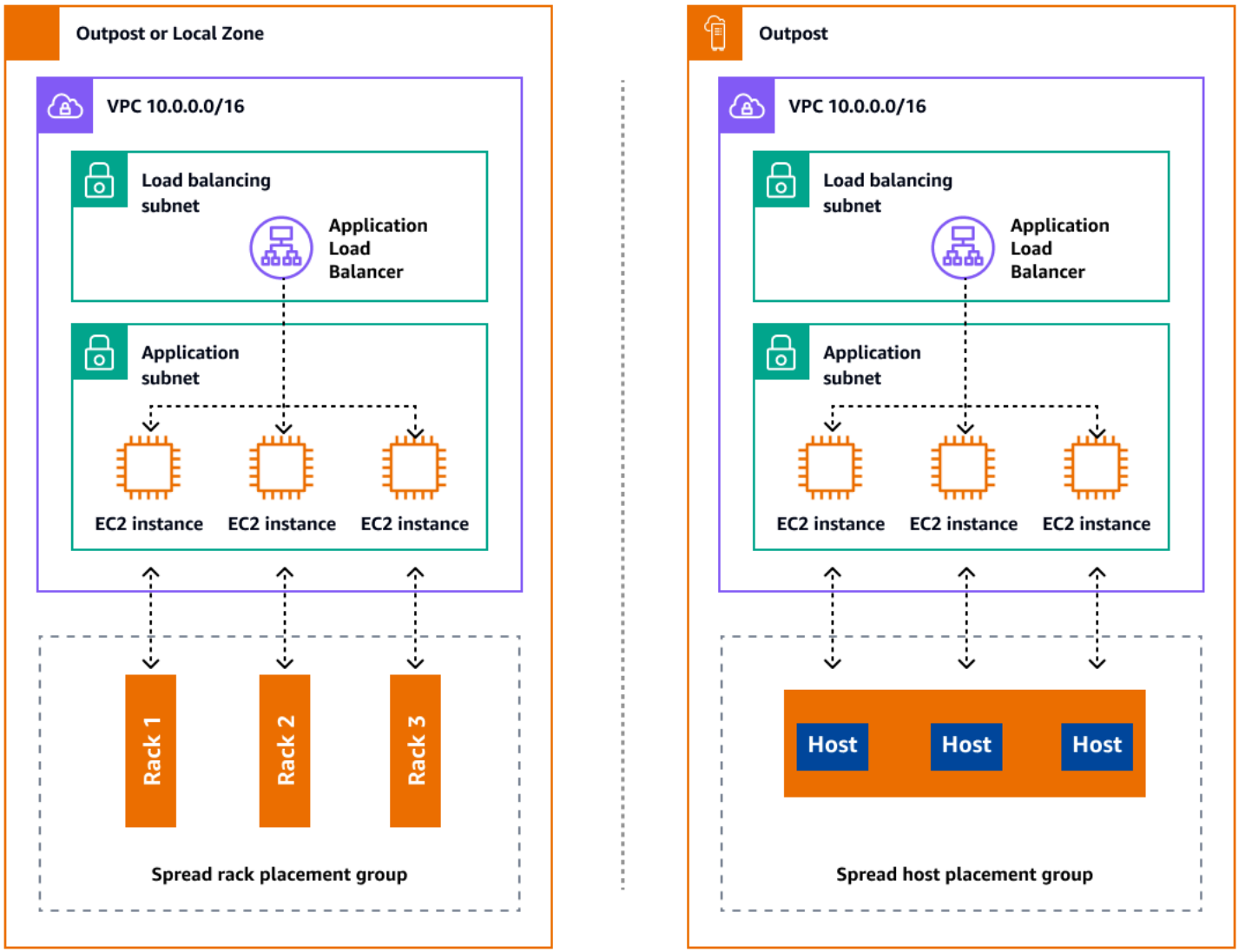
Expansion des déploiements en rack d'Outposts avec des racks ACE

Le rack Aggregation, Core, Edge (ACE) constitue un point d'agrégation essentiel pour les déploiements AWS Outposts multirack et est principalement recommandé pour les installations comportant plus de trois racks ou pour la planification d'une future extension. Chaque rack ACE comprend quatre routeurs qui prennent en charge les connexions 10 Gbit/s, 40 Gbit/s et 100 Gbit/s (100 Gbit/s est optimal). Chaque rack peut se connecter à un maximum de quatre appareils clients en amont pour une redondance maximale. Les racks ACE consomment jusqu'à 10 kVA d'énergie et pèsent jusqu'à 705 livres. Les principaux avantages incluent la réduction des exigences en matière de réseau physique, la réduction des liaisons montantes de câblage en fibre optique et la diminution des interfaces virtuelles VLAN. AWS surveille ces racks par le biais de données de télémétrie via

des tunnels VPN et travaille en étroite collaboration avec les clients lors de l'installation pour garantir une disponibilité électrique, une configuration réseau et un placement optimal. L'architecture en rack ACE apporte une valeur croissante à mesure que les déploiements évoluent et simplifie efficacement la connectivité tout en réduisant la complexité et les exigences en matière de ports physiques dans les grandes installations. Pour plus d'informations, consultez le billet de AWS blog Scaling AWS Outposts rack deployments with ACE Rack.

Répartition des instances entre les Outposts et les Zones Locales

Les Outposts et les Zones Locales disposent d'un nombre limité de serveurs informatiques. Si votre application déploie plusieurs instances associées, ces instances peuvent être déployées sur le même serveur ou sur des serveurs du même rack, sauf si elles sont configurées différemment. Outre les options par défaut, vous pouvez répartir les instances sur les serveurs afin de limiter le risque lié à l'exécution d'instances associées sur la même infrastructure. Vous pouvez également répartir les instances sur plusieurs racks en utilisant des groupes de placement de partitions. C'est ce qu'on appelle le modèle de distribution par rayonnage. Utilisez la distribution automatique pour répartir les instances sur les partitions du groupe ou déployez des instances sur des partitions cibles sélectionnées. En déployant des instances sur des partitions cibles, vous pouvez déployer des ressources sélectionnées sur le même rack tout en répartissant les autres ressources entre les racks. Outposts propose également une autre option appelée spread host qui vous permet de répartir votre charge de travail au niveau de l'hôte. Le schéma suivant montre les options de distribution du rack de diffusion et de l'hôte de diffusion.



Amazon RDS Multi-AZ dans AWS Outposts

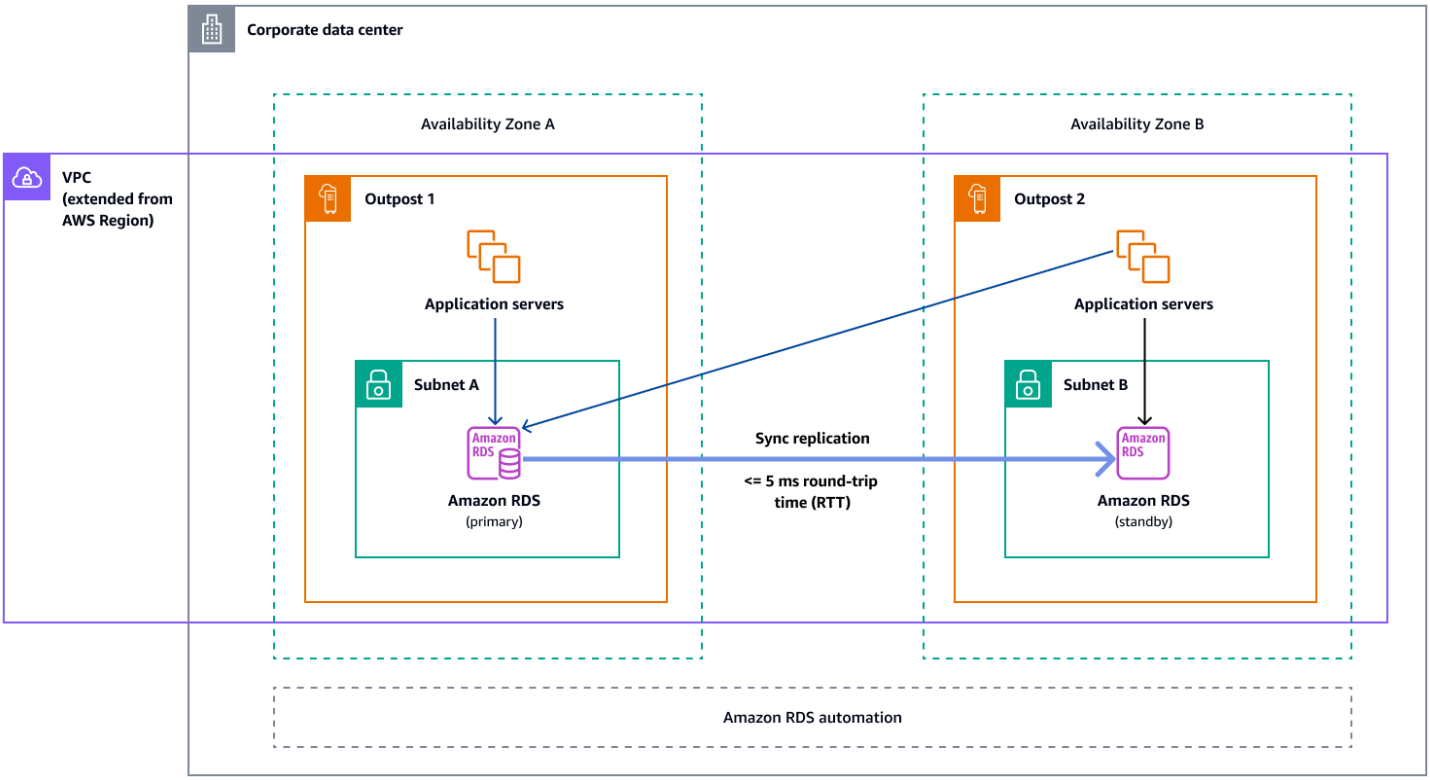
Lorsque vous utilisez des déploiements d'instances multi-AZ sur des Outposts, Amazon RDS crée deux instances de base de données sur deux Outposts. Chaque avant-poste fonctionne sur sa propre infrastructure physique et se connecte aux différentes zones de disponibilité d'une région pour une haute disponibilité. Lorsque deux Outposts sont connectés via une connexion locale gérée par le client, Amazon RDS gère la réplication synchrone entre les instances de base de données principale et de secours. En cas de défaillance du logiciel ou de l'infrastructure, Amazon RDS place automatiquement l'instance de secours au rôle principal et met à jour l'enregistrement DNS pour qu'il pointe vers la nouvelle instance principale. Pour les déploiements Multi-AZ, Amazon RDS crée une instance de base de données principale sur un Outpost et réplique de manière synchrone les données vers une instance de base de données en veille sur un Outpost différent. Les déploiements

multi-AZ sur les Outposts fonctionnent comme les déploiements multi-AZ dans Régions AWS les Outposts, avec les différences suivantes :

- Ils nécessitent une connexion locale entre deux Outposts ou plus.
- Ils ont besoin de pools d'adresses IP (CoIP) appartenant au client. Pour plus d'informations, consultez la section Adresses IP appartenant au client pour Amazon RDS dans AWS Outposts la documentation Amazon RDS.
- La réplication fonctionne sur votre réseau local.

Les déploiements multi-AZ sont disponibles pour toutes les versions prises en charge de MySQL et PostgreSQL sur Amazon RDS on Outposts. Les sauvegardes locales ne sont pas prises en charge pour les déploiements multi-AZ.

Le schéma suivant montre l'architecture des configurations multi-AZ d'Amazon RDS on Outposts.

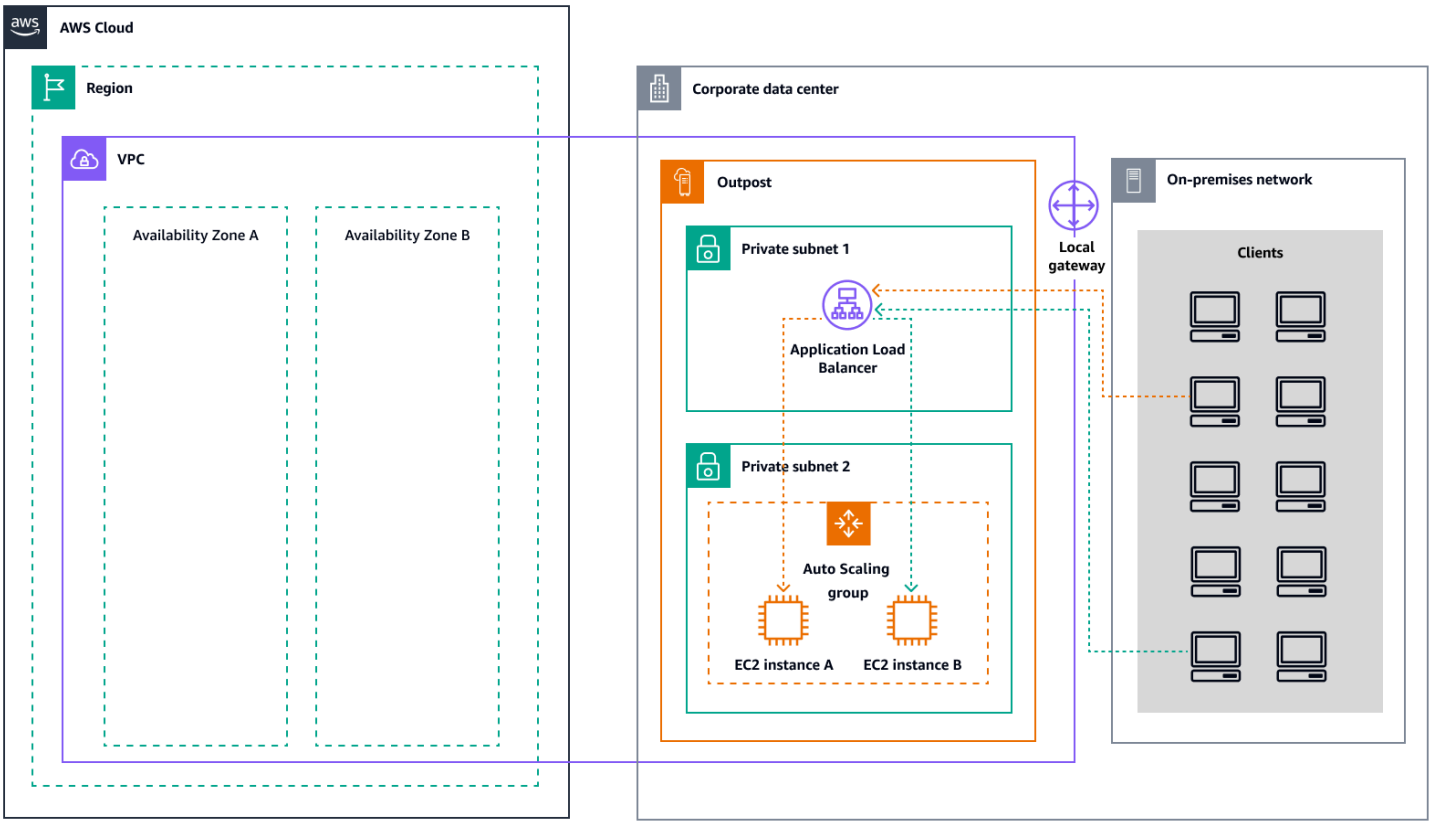


Mécanismes de basculement

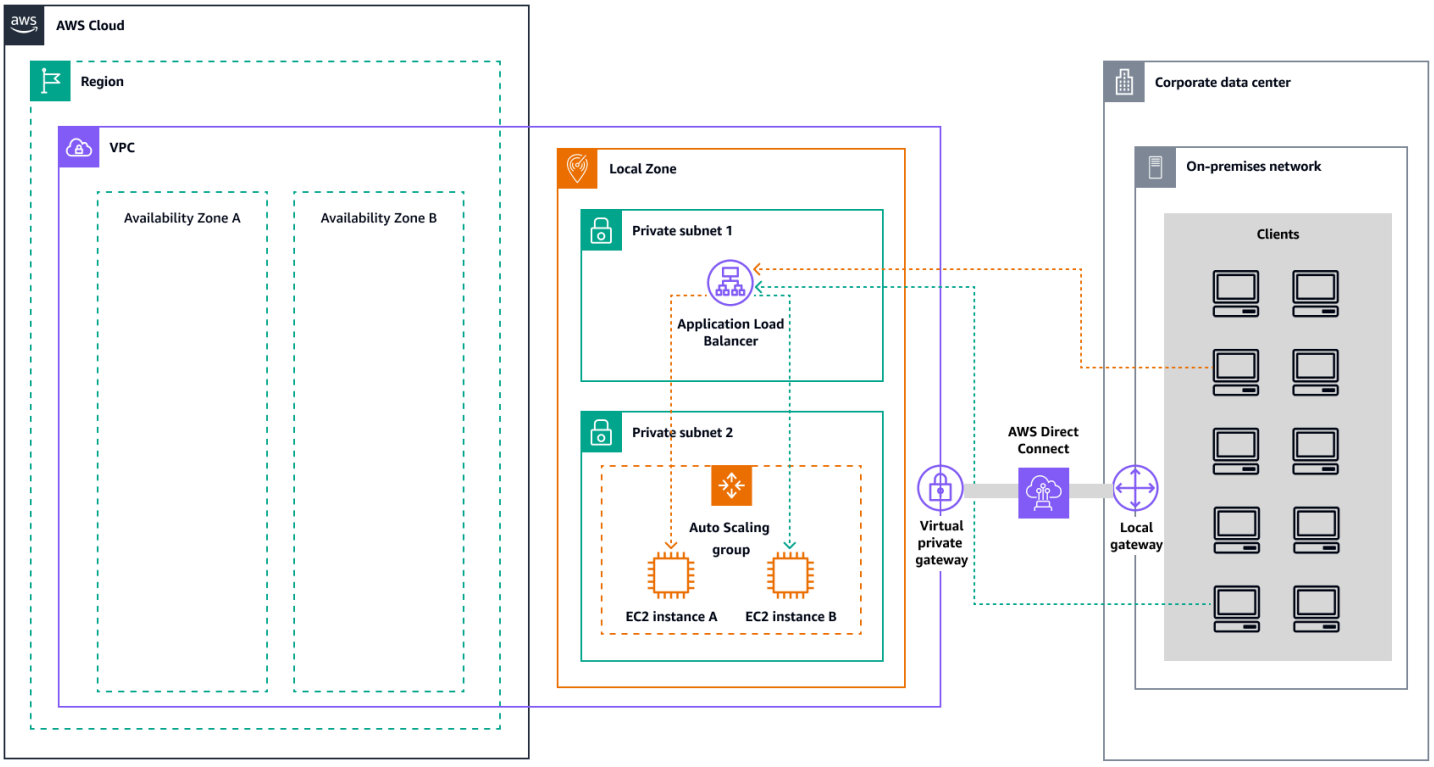
Équilibrage de charge et dimensionnement automatique

Elastic Load Balancing (ELB) répartit automatiquement le trafic entrant de votre application sur toutes les EC2 instances que vous exécutez. ELB aide à gérer les demandes entrantes en acheminant le trafic de manière optimale afin qu'aucune instance ne soit débordée. Pour utiliser ELB avec votre groupe Amazon EC2 Auto Scaling, associez l'équilibreur de charge à votre groupe Auto Scaling. Cela enregistre le groupe auprès de l'équilibreur de charge, qui agit comme un point de contact unique pour tout le trafic Web entrant dans votre groupe. Lorsque vous utilisez ELB avec votre groupe Auto Scaling, il n'est pas nécessaire d'enregistrer des EC2 instances individuelles auprès de l'équilibreur de charge. Les instances qui sont lancées par votre groupe Auto Scaling sont automatiquement enregistrées auprès de l'équilibreur de charge. De même, les instances mises hors service par votre groupe Auto Scaling sont automatiquement désenregistrées de l'équilibreur de charge. Après avoir attaché un équilibreur de charge à votre groupe Auto Scaling, vous pouvez configurer votre groupe pour utiliser les métriques ELB (telles que le nombre de demandes d'Application Load Balancer par cible) afin d'adapter le nombre d'instances du groupe en fonction des fluctuations de la demande. Vous pouvez éventuellement ajouter des tests de santé ELB à votre groupe Auto Scaling afin qu'Amazon EC2 Auto Scaling puisse identifier et remplacer les instances défectueuses sur la base de ces tests de santé. Vous pouvez également créer une CloudWatch alarme Amazon qui vous avertit si le nombre d'hôtes sains du groupe cible est inférieur au nombre autorisé.

Le schéma suivant illustre comment un Application Load Balancer gère les charges de travail sur Amazon dans. EC2 AWS Outposts



Le schéma suivant illustre une architecture similaire pour Amazon EC2 dans les Zones Locales.

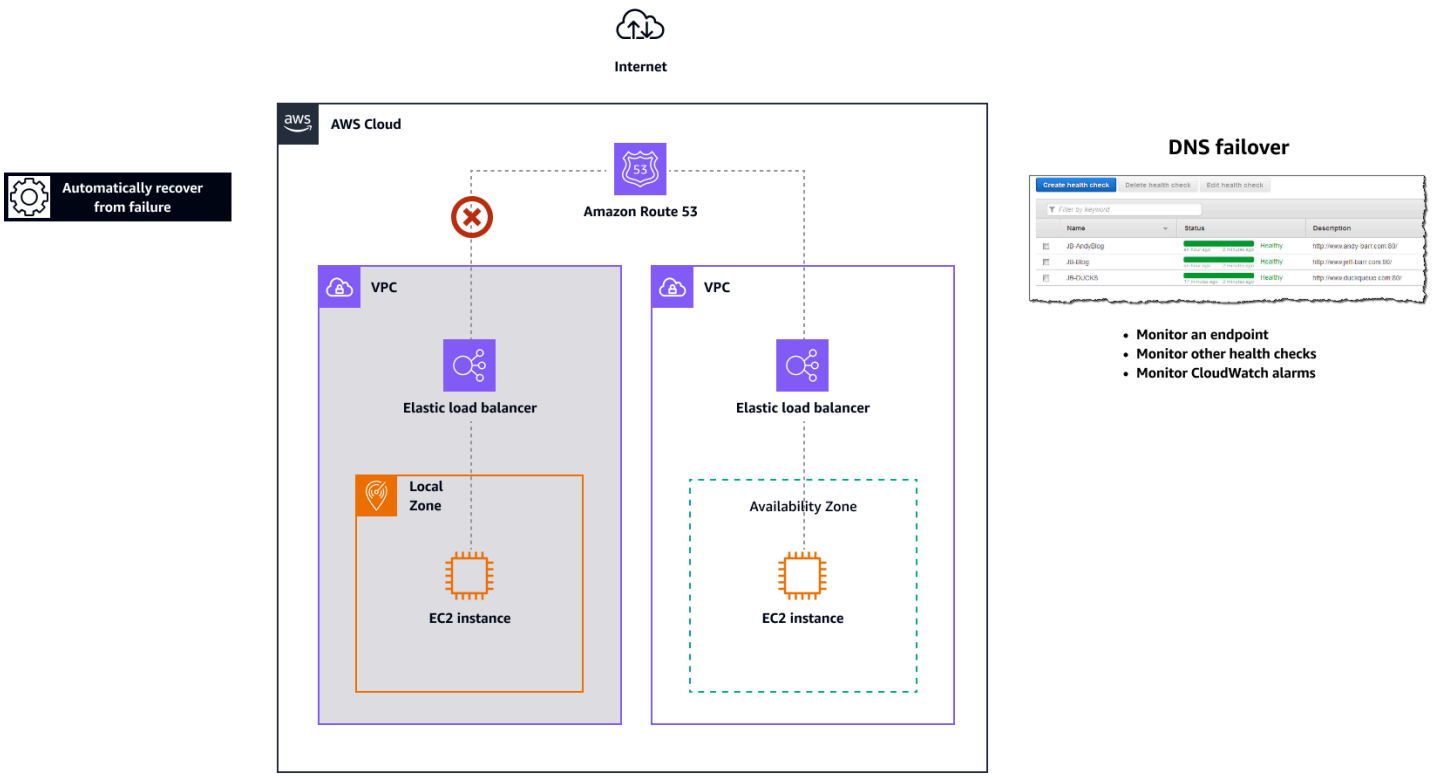


> **Note**
>
> Les équilibreurs de charge d'application sont disponibles à la fois dans les Zones Locales AWS Outposts et dans les Zones Locales. Toutefois, pour utiliser un Application Load Balancer AWS Outposts, vous devez dimensionner la EC2 capacité Amazon afin de fournir l'évolutivité requise par l'équilibreur de charge. Pour plus d'informations sur le dimensionnement d'un équilibreur de charge AWS Outposts, consultez le billet de AWS blog Configuring an Application Load Balancer on. AWS Outposts

Amazon Route 53 pour le basculement du DNS

Lorsque plusieurs ressources exécutent la même fonction, par exemple plusieurs serveurs HTTP ou de messagerie, vous pouvez configurer Amazon Route 53 pour vérifier l'état de vos ressources et répondre aux requêtes DNS en utilisant uniquement les ressources saines. Supposons, par exemple, que votre site Web soit hébergé sur deux serveurs. `example.com` Un serveur se trouve dans une zone locale et l'autre dans un avant-poste. Vous pouvez configurer Route 53 pour vérifier l'état de ces serveurs et pour répondre aux requêtes DNS en `example.com` utilisant uniquement les serveurs actuellement sains. Si vous utilisez des enregistrements d'alias pour acheminer le trafic vers AWS des ressources sélectionnées, telles que les équilibreurs de charge ELB, vous pouvez configurer Route 53 pour évaluer l'état de la ressource et acheminer le trafic uniquement vers les ressources saines. Lorsque vous configurez un enregistrement d'alias pour évaluer l'état d'une ressource, il n'est pas nécessaire de créer un bilan de santé pour cette ressource.

Le schéma suivant illustre les mécanismes de basculement de Route 53.



Remarques

- Si vous créez des enregistrements de basculement dans une zone hébergée privée, vous pouvez créer une CloudWatch métrique, associer une alarme à la métrique, puis créer un bilan de santé basé sur le flux de données de l'alarme.
- Pour rendre une application accessible au public à AWS Outposts l'aide d'un Application Load Balancer, configurez des configurations réseau qui permettent la traduction des adresses réseau de destination (DNAT) du nom de domaine public IPs vers le nom de domaine complet (FQDN) de l'équilibreur de charge, et créez une règle de basculement Route 53 avec des contrôles de santé pointant vers l'adresse IP publique exposée. Cette combinaison garantit un accès public fiable à votre application hébergée par Outposts.

Amazon Route 53 Resolver sur AWS Outposts

Amazon Route 53 Resolverest disponible sur les supports Outposts. Il fournit à vos services et applications sur site une résolution DNS locale directement depuis Outposts. Les points de terminaison Local Route 53 Resolver permettent également la résolution DNS entre les Outposts et

votre serveur DNS local. Route 53 Resolver on Outposts permet d'améliorer la disponibilité et les performances de vos applications sur site.

L'un des cas d'utilisation typiques des Outposts consiste à déployer des applications qui nécessitent un accès à faible latence aux systèmes sur site, tels que les équipements d'usine, les applications de trading à haute fréquence et les systèmes de diagnostic médical.

Lorsque vous choisissez d'utiliser les résolveurs Route 53 locaux sur les Outposts, les applications et les services continueront de bénéficier de la résolution DNS locale pour découvrir d'autres services, même en cas de perte de connectivité avec un Région AWS parent. Les résolveurs locaux aident également à réduire le temps de latence pour les résolutions DNS, car les résultats des requêtes sont mis en cache et diffusés localement depuis les Outposts, ce qui élimine les allers-retours inutiles vers le parent. Région AWS Toutes les résolutions DNS pour les applications des Outposts VPCs qui utilisent un DNS privé sont servies localement.

Outre l'activation des résolveurs locaux, ce lancement active également les points de terminaison des résolveurs locaux. Les points de terminaison sortants Route 53 Resolver permettent aux résolveurs Route 53 de transférer les requêtes DNS aux résolveurs DNS que vous gérez, par exemple sur votre réseau local. En revanche, les points de terminaison entrants Route 53 Resolver transmettent les requêtes DNS qu'ils reçoivent de l'extérieur du VPC au résolveur qui s'exécute sur Outposts. Il vous permet d'envoyer des requêtes DNS pour des services déployés sur un VPC Outposts privé depuis l'extérieur de ce VPC. Pour plus d'informations sur les points de terminaison entrants et sortants, consultez la section Résolution des requêtes DNS entre VPCs et votre réseau dans la documentation Route 53.

Planification des capacités à la périphérie

La phase de planification des capacités consiste à collecter les besoins en matière de vCPU, de mémoire et de stockage pour déployer votre architecture. Dans le pilier d'optimisation des coûts du AWS Well-Architected Framework, le dimensionnement correct est un processus continu qui commence par la planification. Vous pouvez utiliser AWS des outils pour définir des optimisations basées sur la consommation de ressources internes. AWS

La planification de la capacité périphérique dans les Zones Locales est la même que dans Régions AWS. Vous devez vérifier que vos instances sont disponibles dans chaque zone locale, car certains types d'instances peuvent différer des types présents dans Régions AWS. Pour les Outposts, vous devez planifier la capacité en fonction de vos exigences en matière de charge de travail. Les

Outposts sont dotés d'un nombre fixe d'instances par hôte et peuvent être relocalisés selon les besoins. Si vos charges de travail nécessitent une capacité de réserve, prenez-en compte lorsque vous planifiez vos besoins en capacité.

Planification des capacités sur les Outposts

AWS Outposts la planification des capacités nécessite des informations spécifiques pour un dimensionnement régional approprié, ainsi que des facteurs spécifiques à la périphérie qui affectent la disponibilité, les performances et la croissance des applications. Pour obtenir des conseils détaillés, consultez la section Planification des capacités dans le AWS livre blanc Considérations relatives à la conception et à l'architecture de AWS Outposts haute disponibilité.

Planification des capacités pour les Zones Locales

Une zone locale est une extension d'une Région AWS zone géographiquement proche de vos utilisateurs. Les ressources créées dans une zone locale peuvent desservir les utilisateurs locaux avec des communications à très faible latence. Pour activer une zone locale dans votre Compte AWS, consultez Getting started with Zones locales AWS dans la AWS documentation. Chaque zone locale dispose de différents emplacements disponibles pour les familles d' EC2 instances. Validez les instances disponibles dans chaque zone locale avant de les utiliser. Pour confirmer les EC2 instances disponibles, exécutez la AWS CLI commande suivante :

```
aws ec2 describe-instance-type-offerings \
--location-type "availability-zone" \
--filters Name=location,Values=<local-zone-name>
```

Sortie attendue :

```
{
  "InstanceTypeOfferings": [
      {
          "InstanceType": "m5.2xlarge",
          "LocationType": "availability-zone",
          "Location": "<local-zone-name>"
      },
      {
          "InstanceType": "t3.micro",
          "LocationType": "availability-zone",
          "Location": "local.zone-name"
```

```
      },
      ...
  ]
}
```

Gestion de l'infrastructure de pointe

AWS fournit des services entièrement gérés qui étendent AWS l'infrastructure, les services et les outils au plus près de vos utilisateurs finaux et de vos centres de données. APIs Les services disponibles dans les Outposts et les Zones Locales sont les mêmes que ceux disponibles dans Régions AWS. Vous pouvez donc gérer ces services à l'aide de la même AWS console AWS CLI, ou. AWS APIs Pour les services pris en charge, consultez le AWS Outposts tableau comparatif des Zones locales AWS fonctionnalités et les fonctionnalités.

Déploiement de services à la périphérie

Vous pouvez configurer les services disponibles dans les Zones Locales et les Outposts de la même manière que vous les configurez Régions AWS : en utilisant la AWS console AWS CLI, ou. AWS APIs La principale différence entre les déploiements régionaux et périphériques réside dans les sous-réseaux dans lesquels les ressources seront provisionnées. La section Mise en réseau à la périphérie décrit comment les sous-réseaux sont déployés dans les Outposts et les Zones Locales. Après avoir identifié les sous-réseaux Edge, vous utilisez l'ID du sous-réseau Edge comme paramètre pour déployer le service dans les Outposts ou les Zones Locales. Les sections suivantes fournissent des exemples de déploiement de services de périphérie.

Amazon EC2 à la pointe

L'`run-instances`exemple suivant lance une instance unique de type `m5.2xlarge` dans le sous-réseau Edge de la région actuelle. La paire de clés est facultative si vous ne prévoyez pas de vous connecter à votre instance en utilisant SSH sous Linux ou le protocole RDP (Remote Desktop Protocol) sous Windows.

```
aws ec2 run-instances \
    --image-id ami-id \
    --instance-type m5.2xlarge \
    --subnet-id <subnet-edge-id> \
    --key-name MyKeyPair
```

Équilibreurs de charge des applications à la périphérie

L'`create-load-balancer`exemple suivant crée un Application Load Balancer interne et active les zones Locales ou les Outposts pour les sous-réseaux spécifiés.

```
aws elbv2 create-load-balancer \
    --name my-internal-load-balancer \
    --scheme internal \
    --subnets <subnet-edge-id>
```

Pour déployer un Application Load Balancer connecté à Internet sur un sous-réseau d'un Outpost, vous devez définir `internet-facing` l'indicateur dans l'option et fournir un ID `--scheme` de pool CoIP, comme indiqué dans cet exemple :

```
aws elbv2 create-load-balancer \
    --name my-internal-load-balancer \
    --scheme internet-facing \
    --customer-owned-ipv4-pool <coip-pool-id>
    --subnets <subnet-edge-id>
```

Pour plus d'informations sur le déploiement d'autres services en périphérie, suivez ces liens :

Service	AWS Outposts	Zones locales AWS
Amazon EKS	Déployez Amazon EKS sur site avec AWS Outposts	Lancez des clusters EKS à faible latence avec Zones locales AWS
Amazon ECS	Amazon ECS sur AWS Outposts	Applications Amazon ECS dans des sous-réseaux partagés, des zones Locales et des zones de longueur d'onde
Amazon RDS	Amazon RDS sur AWS Outposts	Sélectionnez le sous-réseau de la zone locale
Amazon S3	Commencer à utiliser Amazon S3 sur Outposts	Non disponible

Service	AWS Outposts	Zones locales AWS
Amazon ElastiCache	Utiliser Outposts avec ElastiCache	Utilisation de Zones Locales avec ElastiCache
Amazon EMR	Clusters EMR sur AWS Outposts	Clusters EMR sur Zones locales AWS
Amazon FSx	Non disponible	Sélectionnez le sous-réseau de la zone locale
AWS Elastic Disaster Recovery	Travailler avec AWS Elastic Disaster Recovery et AWS Outposts	Non disponible
AWS Application Migration Service	Non disponible	Sélectionnez le sous-réseau de zone locale comme sous-réseau intermédiaire

CLI et SDK spécifiques à Outposts

AWS Outposts comporte deux groupes de commandes et permet APIs de créer un ordre de service ou de manipuler les tables de routage entre la passerelle locale et votre réseau local.

Processus de commande d'Outposts

Vous pouvez utiliser le AWS CLIou les Outposts APIs pour créer un site Outposts, pour créer un Outpost et pour créer une commande Outposts. Nous vous recommandons de travailler avec un spécialiste du cloud hybride lors de votre processus de AWS Outposts commande afin de garantir une sélection appropriée des ressources IDs et une configuration optimale pour vos besoins de mise en œuvre. Pour une liste complète des identifiants de ressources, consultez la page de tarification AWS Outposts des racks.

Gestion des passerelles locales

La gestion et le fonctionnement de la passerelle locale (LGW) dans Outposts nécessitent la connaissance des commandes et AWS CLI du SDK disponibles pour cette tâche. Vous pouvez

utiliser le AWS CLI et AWS SDKs pour créer et modifier des itinéraires LGW, entre autres tâches. Pour plus d'informations sur la gestion du LGW, consultez les ressources suivantes :

- AWS CLI pour Amazon EC2
- EC2.Client dans le AWS SDK for Python (Boto)
- Ec2Client dans le AWS SDK pour Java

CloudWatch métriques et journaux

Pour Services AWS qu'ils soient disponibles à la fois dans les Outposts et les Zones Locales, les métriques et les journaux sont gérés de la même manière que dans les Régions. Amazon CloudWatch fournit des statistiques dédiées à la surveillance des Outposts dans les dimensions suivantes :

Dimension	Description
`Account`	Le compte ou le service utilisant la capacité
`InstanceFamily`	La famille d'instances
`InstanceType`	Le type d'instance
`OutpostId`	L'identifiant de l'avant-poste
`VolumeType`	Type de volume EBS
`VirtualInterfaceId`	L'ID de la passerelle locale ou de l'interface virtuelle de liaison de service (VIF)
`VirtualInterfaceGroupId`	L'ID du groupe VIF pour la passerelle locale (VIF)

Pour plus d'informations, consultez CloudWatch les statistiques relatives aux racks Outposts dans la documentation Outposts.

Ressources

AWS références

- Cloud hybride avec AWS
- AWS Outposts Guide de l'utilisateur pour les Outposts Racks
- Guide de l'utilisateur Zones locales AWS
- AWS Outposts Famille
- Zones locales AWS
- Étendre un VPC à une zone locale, à une zone de longueur d'onde ou à un avant-poste (documentation Amazon VPC)
- Instances Linux dans les Zones Locales (EC2 documentation Amazon)
- Instances Linux dans Outposts (documentation Amazon EC2)
- Commencez à déployer des applications à faible latence avec Zones locales AWS (tutoriel)

AWS articles de blog

- Gestion de AWS l'infrastructure sur site avec Amazon EC2
- Création d'applications modernes avec Amazon EKS sur Amazon EC2
- Comment choisir entre les modes de routage CoIP et VPC direct sur Amazon Rack EC2
- Sélection de commutateurs réseau pour votre Amazon EC2
- Conserver une copie locale de vos données dans Zones locales AWS
- Amazon ECS sur Amazon EC2
- Gestion du maillage de services adapté aux périphériques avec Amazon EKS pour Zones locales AWS
- Déploiement du routage d'entrée par passerelle locale sur Amazon EC2
- Automatiser les déploiements de vos charges de travail dans Zones locales AWS
- Partage d'Amazon EC2 dans un AWS environnement multi-comptes : partie 1
- Partage d'Amazon EC2 dans un AWS environnement multi-comptes : partie 2
- AWS Direct Connect et modèles Zones locales AWS d'interopérabilité

- Déployez Amazon RDS sur Amazon EC2 avec une haute disponibilité multi-AZ

Collaborateurs

Les personnes suivantes ont contribué à ce guide.

Conception

- Leonardo Solano, architecte principal des solutions de cloud hybride, AWS
- Len Gomes, architecte de solutions pour les partenaires, AWS
- Matt Price, ingénieur principal du support aux entreprises, AWS
- Tom Gadomski, architecte de solutions, AWS
- Obed Gutierrez, architecte de solutions, AWS
- Dionysios Kakaletris, responsable des comptes techniques, AWS
- Vamsi Krishna, spécialiste principal des Outposts, AWS

Révision

- David Filiatrault, conseiller en livraison, AWS

Rédaction technique

- Handan Selamoglu, responsable principal de la documentation, AWS

Historique du document

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

Modification	Description	Date
Publication initiale	—	10 juin 2025

AWS Glossaire des directives prescriptives

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

Nombres

7 R

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

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

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

A

ABAC

Voir contrôle d'accès basé sur les attributs.

services abstraits

Consultez la section Services gérés.

ACIDE

Voir atomicité, consistance, isolation, durabilité.

migration active-active

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

migration active-passive

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

fonction d'agrégation

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

AI

Voir intelligence artificielle.

AIOps

Voir les opérations d'intelligence artificielle.

anonymisation

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

anti-motif

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

contrôle des applications

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

portefeuille d'applications

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

intelligence artificielle (IA)

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

opérations d'intelligence artificielle (AIOps)

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

chiffrement asymétrique

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

atomicité, cohérence, isolement, durabilité (ACID)

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

contrôle d'accès par attributs (ABAC)

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

source de données faisant autorité

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

Zone de disponibilité

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

AWS Cadre d'adoption du cloud (AWS CAF)

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

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

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

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

B

mauvais bot

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

BCP

Consultez la section Planification de la continuité des activités.

graphique de comportement

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

système de poids fort

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

classification binaire

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

filtre de Bloom

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

déploiement bleu/vert

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

bot

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

botnet

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

branche

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

accès par brise-vitre

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

stratégie existante (brownfield)

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

cache de tampon

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

capacité métier

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

planification de la continuité des activités (BCP)

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

C

CAF

Voir le cadre d'adoption du AWS cloud.

déploiement de Canary

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

CCo E

Voir le Centre d'excellence du cloud.

CDC

Voir capture des données de modification.

capture des données de modification (CDC)

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

ingénierie du chaos

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

CI/CD

Découvrez l'intégration continue et la livraison continue.

classification

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

chiffrement côté client

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

Centre d'excellence du cloud (CCoE)

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

cloud computing

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

modèle d'exploitation du cloud

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

étapes d'adoption du cloud

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

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

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

CMDB

Voir base de données de gestion de configuration.

référentiel de code

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

cache passif

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

données gelées

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

vision par ordinateur (CV)

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

dérive de configuration

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

base de données de gestion des configurations (CMDB)

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

pack de conformité

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

intégration continue et livraison continue (CI/CD)

Processus d'automatisation des étapes de source, de construction, de test, de préparation et de production du processus de publication du logiciel. CI/CD 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 .

deployment

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.

EDI

Voir échange de données informatisé.

informatique de périphérie

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

échange de données informatisé (EDI)

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

chiffrement

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

clé de chiffrement

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

endianisme

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

point de terminaison

Voir point de terminaison de service.

service de point de terminaison

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

planification des ressources d'entreprise (ERP)

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

chiffrement d'enveloppe

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

environment

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

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

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

époppée

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

ERP

Voir Planification des ressources d'entreprise.

analyse exploratoire des données (EDA)

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

F

tableau des faits

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

échouer rapidement

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

limite d'isolation des défauts

Dans le AWS Cloud, une limite telle qu'une zone de disponibilité Région AWS, un plan de contrôle ou un plan de données qui limite l'effet d'une panne et contribue à améliorer la résilience des

charges de travail. Pour plus d'informations, consultez la section Limites d'isolation des AWS pannes.

branche de fonctionnalités

Voir succursale.

fonctionnalités

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

importance des fonctionnalités

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

transformation de fonctionnalité

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

invitation en quelques coups

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

FGAC

Découvrez le contrôle d'accès détaillé.

contrôle d'accès détaillé (FGAC)

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

migration instantanée (flash-cut)

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

FM

Voir le modèle de fondation.

modèle de fondation (FM)

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

G

IA générative

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

blocage géographique

Voir les restrictions géographiques.

restrictions géographiques (blocage géographique)

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

Flux de travail Gitflow

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

image dorée

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

stratégie inédite

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

barrière de protection

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

H

HA

Découvrez la haute disponibilité.

migration de base de données hétérogène

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

haute disponibilité (HA)

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

modernisation des historiens

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

données de rétention

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

migration de base de données homogène

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

données chaudes

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

correctif

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

période de soins intensifs

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

I

IaC

Considérez l'infrastructure comme un code.

politique basée sur l'identité

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

application inactive

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

IIo T

Voir Internet industriel des objets.

infrastructure immuable

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

VPC entrant (d'entrée)

Dans une architecture AWS multi-comptes, un VPC qui accepte, inspecte et achemine les connexions réseau depuis l'extérieur d'une application. L'architecture AWS de référence de sécurité recommande de configurer votre compte réseau avec les fonctions entrantes, sortantes

et d'inspection VPCs afin de protéger l'interface bidirectionnelle entre votre application et l'Internet en général.

migration incrémentielle

Stratégie de basculement dans le cadre de laquelle vous migrez votre application par petites parties au lieu d'effectuer un basculement complet unique. Par exemple, il se peut que vous ne transfériez que quelques microservices ou utilisateurs vers le nouveau système dans un premier temps. Après avoir vérifié que tout fonctionne correctement, vous pouvez transférer progressivement des microservices ou des utilisateurs supplémentaires jusqu'à ce que vous puissiez mettre hors service votre système hérité. Cette stratégie réduit les risques associés aux migrations de grande ampleur.

Industry 4.0

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

infrastructure

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

infrastructure en tant que code (IaC)

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

Internet industriel des objets (IIoT)

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

VPC d'inspection

Dans une architecture AWS multi-comptes, un VPC centralisé qui gère les inspections du trafic réseau VPCs entre (identique ou Régions AWS différent), Internet et les réseaux locaux. L'architecture AWS de référence de sécurité recommande de configurer votre compte réseau

avec les fonctions entrantes, sortantes et d'inspection VPCs afin de protéger l'interface bidirectionnelle entre votre application et l'Internet en général.

Internet des objets (IoT)

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

interprétabilité

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

IoT

Voir Internet des objets.

Bibliothèque d'informations informatiques (ITIL)

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

gestion des services informatiques (ITSM)

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

ITIL

Consultez la bibliothèque d'informations informatiques.

ITSM

Voir Gestion des services informatiques.

L

contrôle d'accès basé sur des étiquettes (LBAC)

Une implémentation du contrôle d'accès obligatoire (MAC) dans laquelle une valeur d'étiquette de sécurité est explicitement attribuée aux utilisateurs et aux données elles-mêmes. L'intersection

entre l'étiquette de sécurité utilisateur et l'étiquette de sécurité des données détermine les lignes et les colonnes visibles par l'utilisateur.

zone de destination

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

grand modèle de langage (LLM)

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

migration de grande envergure

Migration de 300 serveurs ou plus.

LBAC

Voir contrôle d'accès basé sur des étiquettes.

principe de moindre privilège

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

lift and shift

Voir 7 Rs.

système de poids faible

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

LLM

Voir le grand modèle de langage.

environnements inférieurs

Voir environnement.

M

machine learning (ML)

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

branche principale

Voir succursale.

malware

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

services gérés

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

système d'exécution de la fabrication (MES)

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

MAP

Voir Migration Acceleration Program.

mécanisme

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

compte membre

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

MAILLES

Voir le système d'exécution de la fabrication.

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

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

microservice

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

architecture de microservices

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

Programme d'accélération des migrations (MAP)

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

migration à grande échelle

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

usine de migration

Équipes interfonctionnelles qui rationalisent la migration des charges de travail grâce à des approches automatisées et agiles. Les équipes de Migration Factory comprennent généralement 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 avec le service de migration AWS d'applications.

Évaluation du portefeuille de migration (MPA)

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

Évaluation de la préparation à la migration (MRA)

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

stratégie de migration

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

ML

Voir apprentissage automatique.

modernisation

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

évaluation de la préparation à la modernisation

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

applications monolithiques (monolithes)

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

MPA

Voir Évaluation du portefeuille de migration.

MQTT

Voir Message Queuing Telemetry Transport.

classification multi-classes

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

infrastructure mutable

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

O

OAC

Voir Contrôle d'accès à l'origine.

OAI

Voir l'identité d'accès à l'origine.

OCM

Voir gestion du changement organisationnel.

migration hors ligne

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

OI

Voir Intégration des opérations.

OLA

Voir l'accord au niveau opérationnel.

migration en ligne

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

OPC-UA

Voir Open Process Communications - Architecture unifiée.

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

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

accord au niveau opérationnel (OLA)

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

examen de l'état de préparation opérationnelle (ORR)

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

technologie opérationnelle (OT)

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

intégration des opérations (OI)

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

journal de suivi d'organisation

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

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

gestion du changement organisationnel (OCM)

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

contrôle d'accès d'origine (OAC)

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

identité d'accès d'origine (OAI)

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

ORR

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

DE

Voir technologie opérationnelle.

VPC sortant (de sortie)

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

P

limite des autorisations

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

informations personnelles identifiables (PII)

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

PII

Voir les informations personnelles identifiables.

manuel stratégique

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

PLC

Voir contrôleur logique programmable.

PLM

Consultez la section Gestion du cycle de vie des produits.

politique

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

persistance polyglotte

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

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

évaluation du portefeuille

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

predicate

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

prédicat pushdown

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

contrôle préventif

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

principal

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

confidentialité dès la conception

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

zones hébergées privées

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

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

contrôle proactif

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

gestion du cycle de vie des produits (PLM)

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

environnement de production

Voir environnement.

contrôleur logique programmable (PLC)

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

chaînage rapide

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

pseudonymisation

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

publish/subscribe (pub/sub)

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

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

Q

plan de requête

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

régression du plan de requêtes

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

R

Matrice RACI

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

CHIFFON

Voir Retrieval Augmented Generation.

rançongiciel

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

Matrice RASCI

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

RCAC

Voir contrôle d'accès aux lignes et aux colonnes.

réplica en lecture

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

réarchitecte

Voir 7 Rs.

objectif de point de récupération (RPO)

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

objectif de temps de récupération (RTO)

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

refactoriser

Voir 7 Rs.

Region (Région)

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

régression

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

réhéberger

Voir 7 Rs.

version

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

déplacer

Voir 7 Rs.

replateforme

Voir 7 Rs.

rachat

Voir 7 Rs.

résilience

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

politique basée sur les ressources

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

matrice responsable, redevable, consulté et informé (RACI)

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

contrôle réactif

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

retain

Voir 7 Rs.

se retirer

Voir 7 Rs.

Génération augmentée de récupération (RAG)

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

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

rotation

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

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

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

RPO

Voir l'objectif du point de récupération.

RTO

Voir l'objectif relatif au temps de rétablissement.

runbook

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

S

SAML 2.0

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

SCADA

Voir Contrôle de supervision et acquisition de données.

SCP

Voir la politique de contrôle des services.

secret

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

sécurité dès la conception

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

contrôle de sécurité

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

renforcement de la sécurité

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

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

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

automatisation des réponses de sécurité

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

chiffrement côté serveur

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

Politique de contrôle des services (SCP)

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

point de terminaison du service

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

contrat de niveau de service (SLA)

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

indicateur de niveau de service (SLI)

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

objectif de niveau de service (SLO)

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

modèle de responsabilité partagée

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

SIEM

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

point de défaillance unique (SPOF)

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

SLA

Voir le contrat de niveau de service.

SLI

Voir l'indicateur de niveau de service.

SLO

Voir l'objectif de niveau de service.

split-and-seed modèle

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

SPOF

Voir point de défaillance unique.

schéma en étoile

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

modèle de figuier étrangleur

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

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

sous-réseau

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

contrôle de supervision et acquisition de données (SCADA)

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

chiffrement symétrique

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

tests synthétiques

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

invite du système

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

T

balises

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

variable cible

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

liste de tâches

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

environnement de test

Voir environnement.

entraînement

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

passerelle de transit

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

flux de travail basé sur jonction

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

accès sécurisé

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

réglage

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

équipe de deux pizzas

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

U

incertitude

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

tâches indifférenciées

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

environnements supérieurs

Voir environnement.

V

mise à vide

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

contrôle de version

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

Appairage de VPC

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

vulnérabilités

Défaut logiciel ou matériel qui compromet la sécurité du système.

W

cache actif

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

données chaudes

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

fonction de fenêtre

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

charge de travail

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

flux de travail

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

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

VER

Voir écrire une fois, lire plusieurs.

WQF

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

écrire une fois, lire plusieurs (WORM)

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

Z

exploit Zero-Day

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

vulnérabilité 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.

invite Zero-Shot

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

application zombie

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

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