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

AWS Conseils prescriptifs

AWS Conseils prescriptifs: 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 peut avoir besoin d'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.

Conditions préalables

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).
- Une connexion Internet ou une AWS Direct Connect liaison d'au moins 500 Mbits/s (1 Gbit/s est préférable) doit être fournie et maintenue 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 disposer d'un contrat actif pour le Support aux AWS entreprises ou d'un plan d'opérations AWS unifiées.

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 Direct Connect lien entre votre centre de données et le 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.

Limitations

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 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.

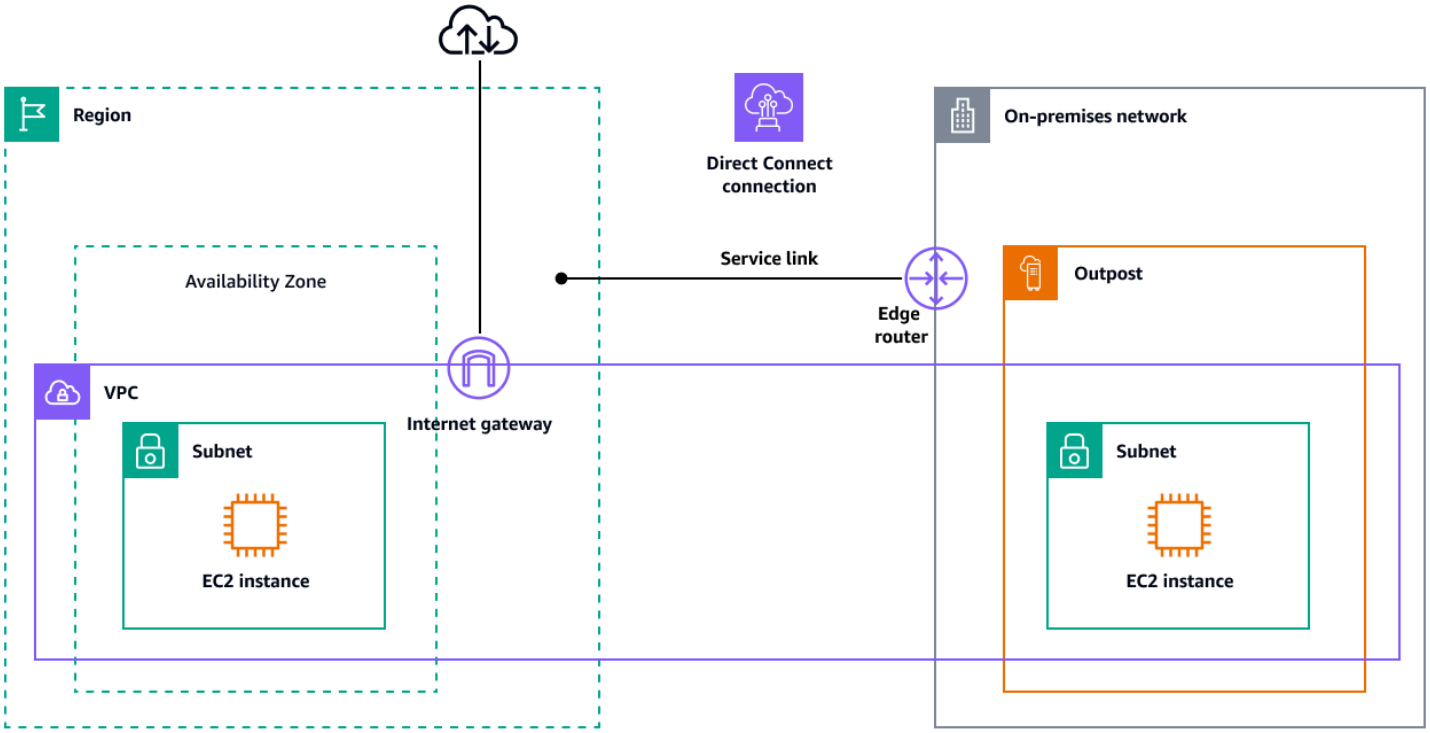
Le schéma suivant montre une AWS architecture qui inclut les sous-réseaux Outpost et Local Zone.

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 Direct Connect publique (VIF publique), soit via une interface virtuelle 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 des instances Amazon EC2, d'attacher des volumes Amazon EBS et d'accéder à Services AWS Amazon EKS, Amazon EMR et Amazon Metrics. 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 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 instances EC2 dans AWS Outposts et les instances EC2 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 via les mêmes API et ensembles d'outils. Région AWS

Le tableau suivant indique les options de connexion et les MTU associées.

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

À partir de	À	MTU
Direct Connect	Local Zones	1 468 octets
Passerelle Internet	Local Zones	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 à Régions AWS. L'infrastructure est entièrement gérée par AWS, vous n'avez donc pas besoin de 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

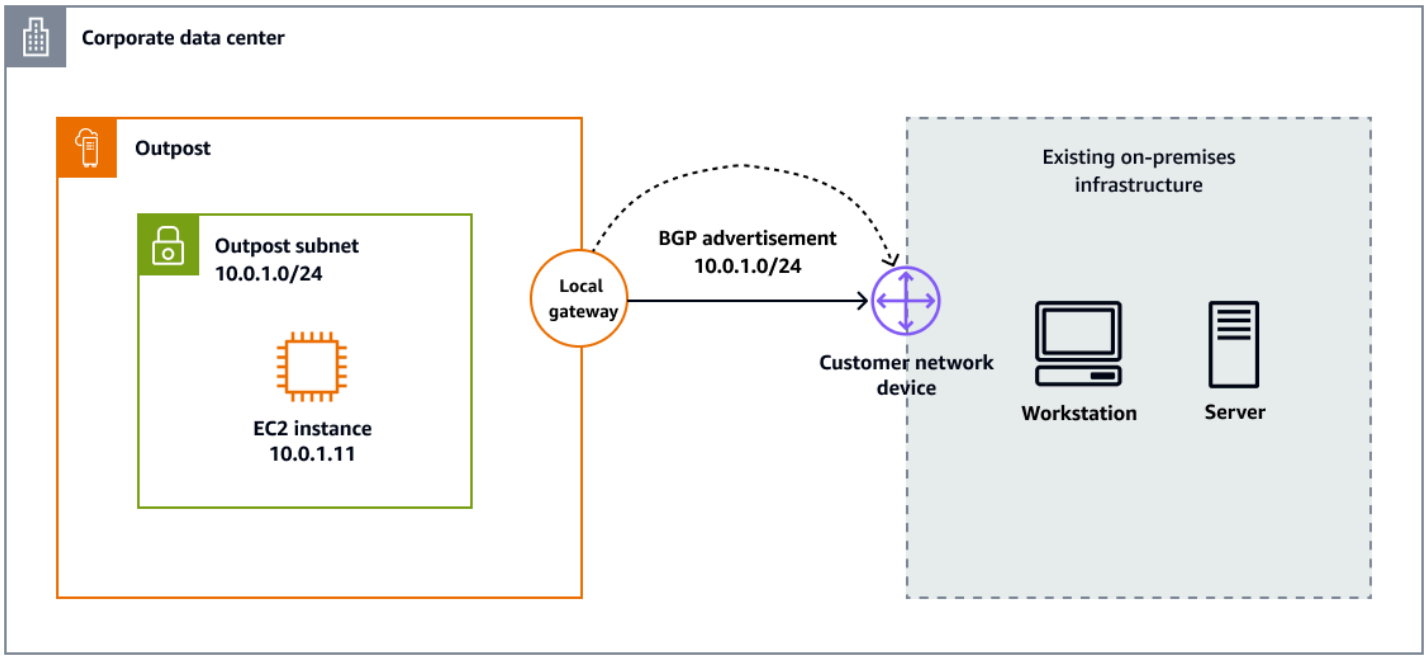
AWS les services cloud hybrides sont conçus pour répondre aux cas d'utilisation nécessitant une faible latence, un traitement local des données ou une conformité en matière de résidence des données. L'architecture réseau permettant d'accéder à ces données est importante, et elle dépend du fait que votre 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

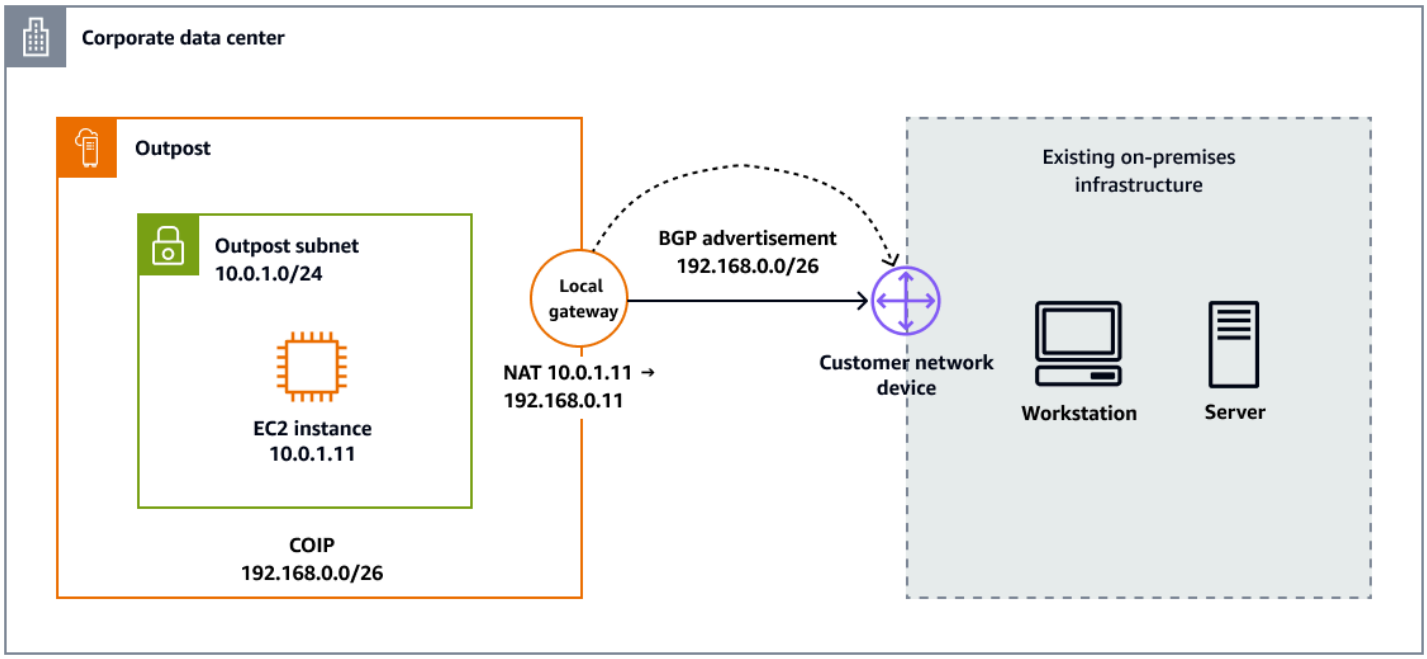
La passerelle locale (LGW) est un composant essentiel de l' AWS Outposts architecture. La passerelle locale permet la connectivité entre vos sous-réseaux Outpost et votre réseau sur site. Le rôle principal d'un LGW est de fournir une connectivité entre un avant-poste et votre réseau local sur site. Il 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 à l'aide du 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 instances

EC2. 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 instances EC2, 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 une EC2-hosted charge de travail Amazon dans une zone locale à Internet, vous pouvez activer l'option IP Auto-assign publique lorsque vous lancez l'instance EC2. 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 instance EC2 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 IPSec (Internet Protocol Security) 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 Direct Connect

Les Zones Locales sont également compatibles 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 VPC et vos charges de travail de 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 des VPC étendus aux Zones Locales. Lorsque les VPC homologues se trouvent dans la même zone locale, le trafic reste dans la zone locale et ne passe pas par la région parent.

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 essentiels 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. Third-party les auditeurs 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 Gestion des identités et des accès AWS (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 d'un chiffrement côté serveur avec des clés de chiffrement gérées par Amazon S3 (). SSE-S3 Vous pouvez éventuellement utiliser le chiffrement côté serveur avec les clés de chiffrement fournies par le client (). SSE-C Pour l'utiliser SSE-C, spécifiez une clé de chiffrement dans le cadre de vos demandes d'API d'objets. Server-side le chiffrement chiffre uniquement les données de l'objet, pas les métadonnées de l'objet.

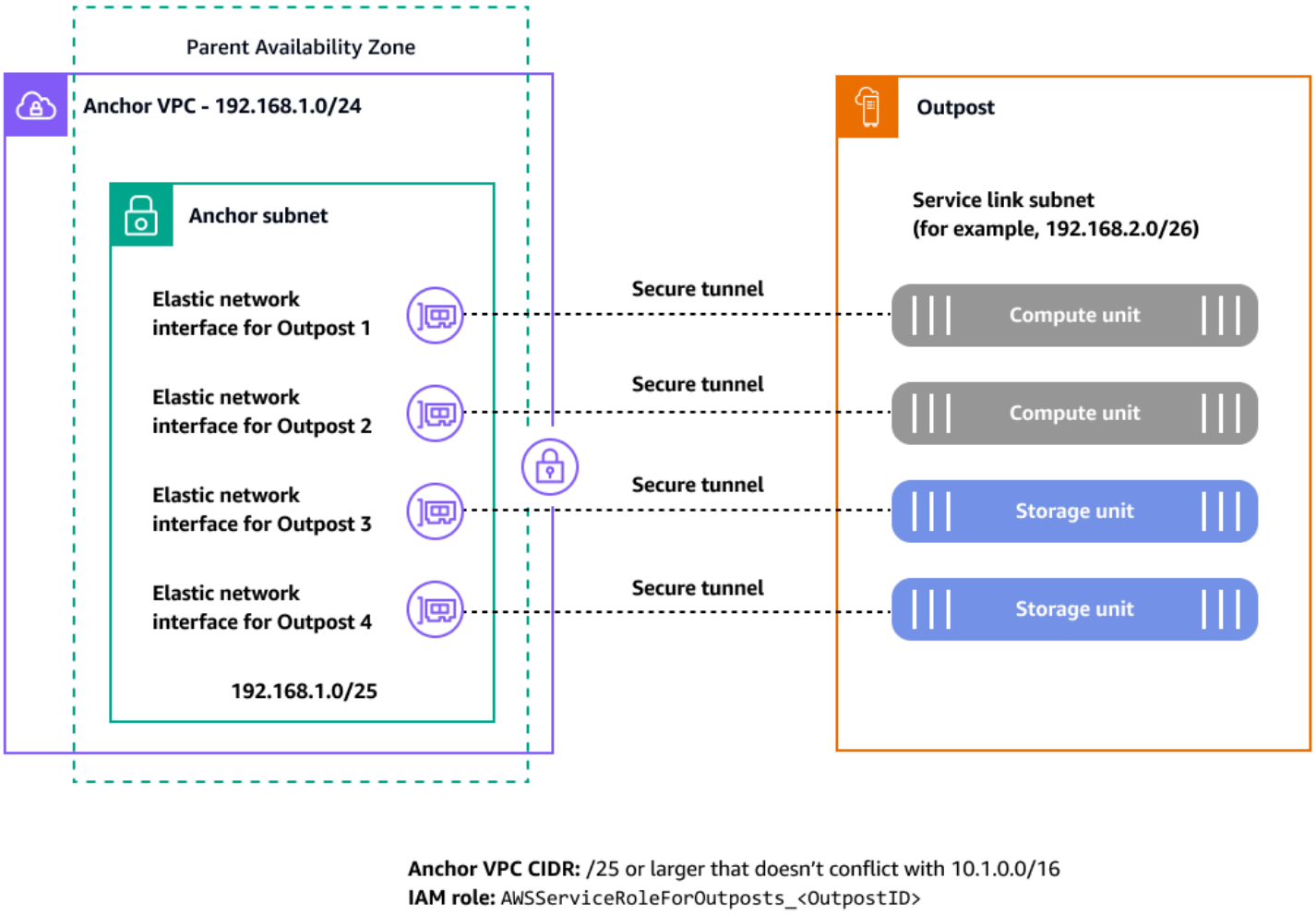
> **Note**
>
> Amazon S3 on Outposts ne prend pas en charge le chiffrement côté serveur avec des clés KMS (). SSE-KMS

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 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.

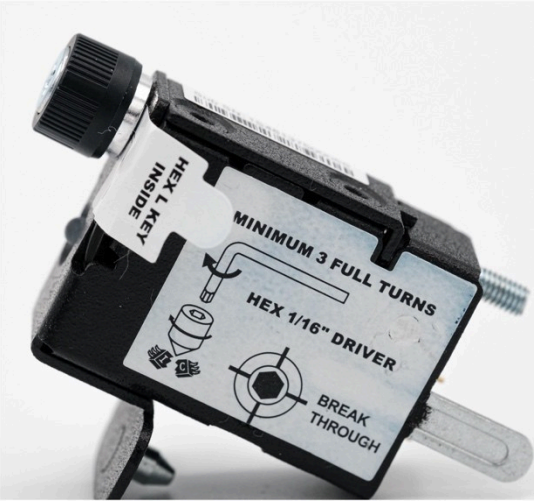
Protocole	Port source	Adresse source	Port de destination	Adresse de destination
UDP	443	AWS Outposts liaison de service /26	443	AWS Outposts Routes publiques de la région ou VPC CIDR d'ancrage
TCP	1025-65535	AWS Outposts liaison de service /26	443	AWS Outposts Routes publiques de la région ou VPC CIDR 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 Direct Connect PoPs pour accéder à une zone locale, vous pouvez activer la sécurité MAC (MACsec) entre votre routeur ou commutateur sur site et le point de terminaison. Direct Connect Pour plus d'informations, consultez le billet de AWS blog Ajouter la sécurité MacSec aux Direct Connect connexions.

Suppression de données

Lorsque vous arrêtez ou mettez fin à une instance EC2 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.



Gestion des identités et des accès

Gestion des identités et des accès AWS (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
Identity-based politiques	Oui
Resource-based politiques	Oui*
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique (spécifiques au service)	Oui
Listes de contrôle d’accès (ACL)	Non

Fonctionnalité IAM	AWS Outposts soutien
Attribute-based contrôle d'accès (ABAC) (balises dans les politiques)	Oui
Informations d’identification temporaires	Oui
Autorisations de principal	Oui
Rôles du service	Non
Service-linked rôles	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 approche de défense approfondie pour le trafic entrant et sortant. Cela inclut l'utilisation de groupes de sécurité (pare-feux d'inspection dynamique), de listes de contrôle d'accès réseau, 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 de calcul incluent les instances EC2, 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 des ressources telles que les instances EC2, 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 d'ISV et vous aider à créer des couches d'inspection dans votre zone locale, comme décrit dans le billet de AWS blog Architectures d'inspection hybrides avec Zones locales AWS.

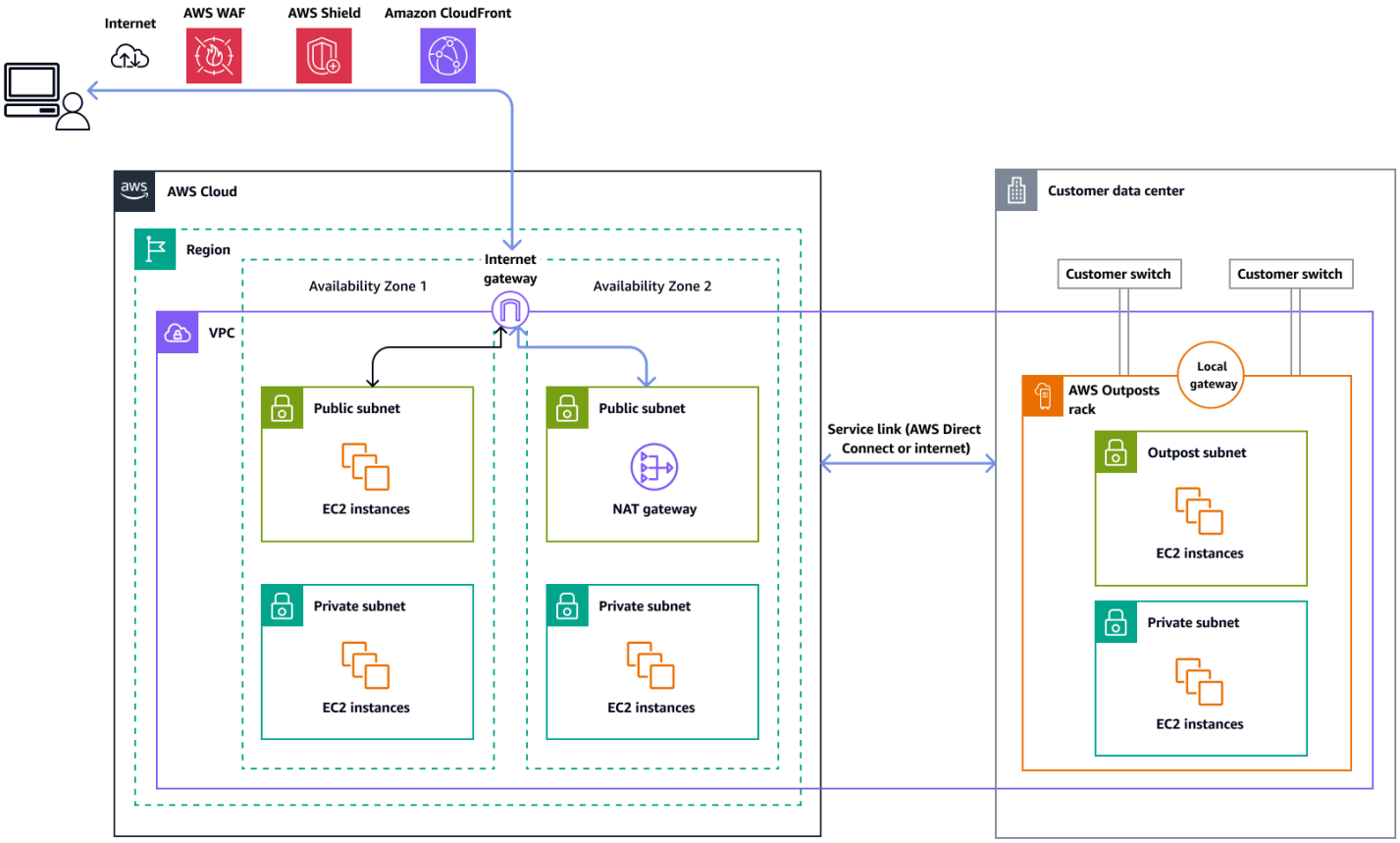
Dans AWS Outposts, si vous souhaitez utiliser la passerelle locale (LGW) pour accéder à Internet depuis votre réseau, vous devez modifier la table de routage personnalisée associée au AWS Outposts sous-réseau. La table de routage doit comporter une entrée de route par défaut (0.0.0). 0/0) qui utilise 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

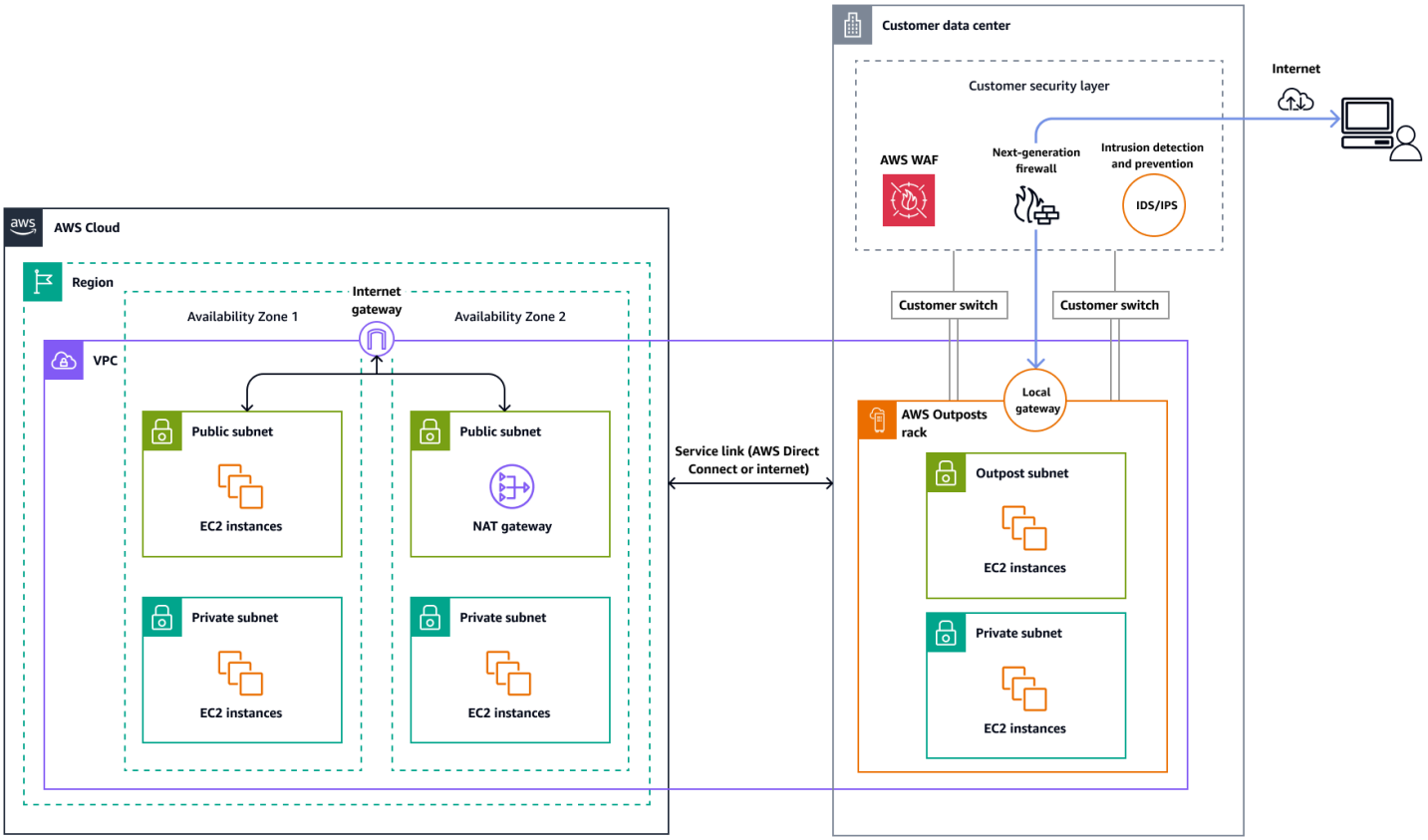
Le schéma suivant montre le trafic entre la charge de travail de l' AWS Outposts instance et Internet passant par le parent Région AWS.



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 barrières de sécurité 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 (FSI). 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 (documentation AWS Well-Architected du 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 des VPC, ainsi que 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
- Customer-owned Pools d'adresses IP (CoIP)
- Tables de routage de passerelle locale
- Outposts
- Amazon S3 sur Outposts

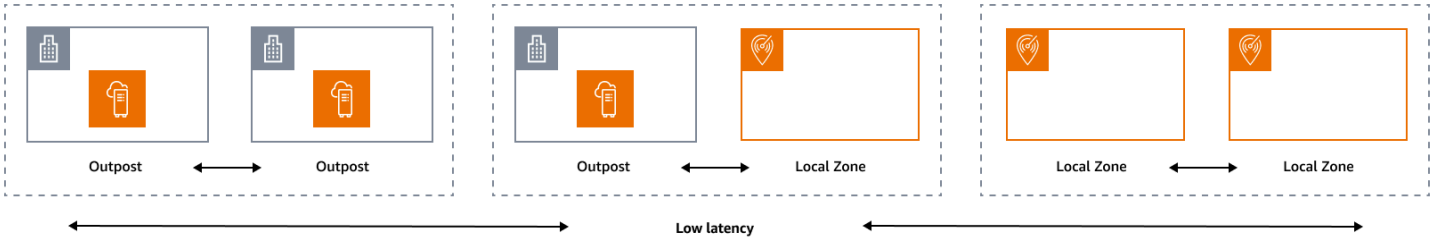
- Sites
- Subnets

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

La 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 les infrastructures que 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.

Local Zones

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 les instances EC2. 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 Services AWS, les API et 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 de créer une Multi-AZ architecture 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 :

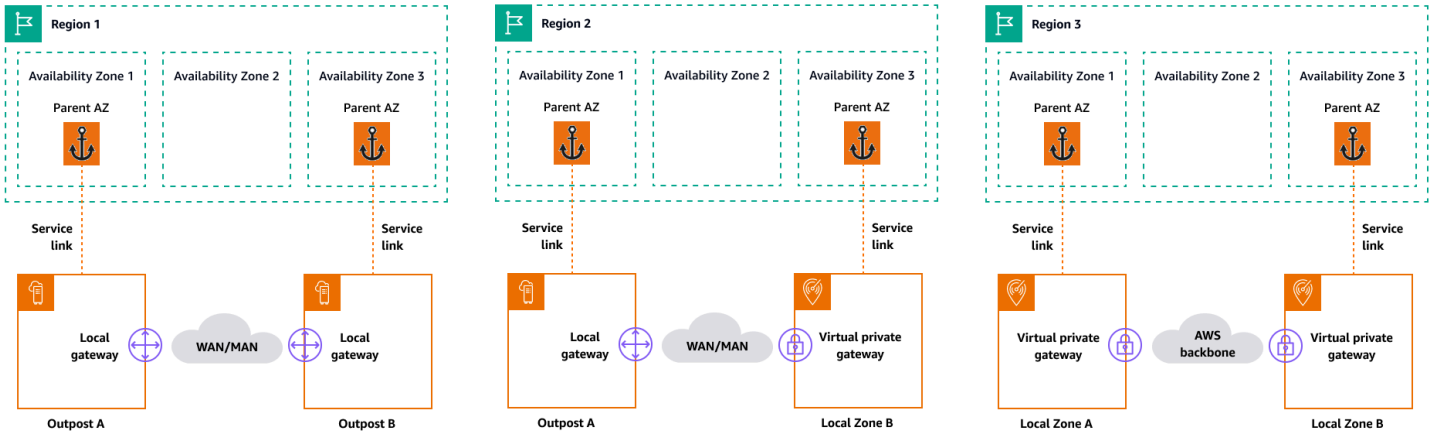
```
aws ec2 describe-availability-zones --zone-ids use1-mia1-az1
```

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

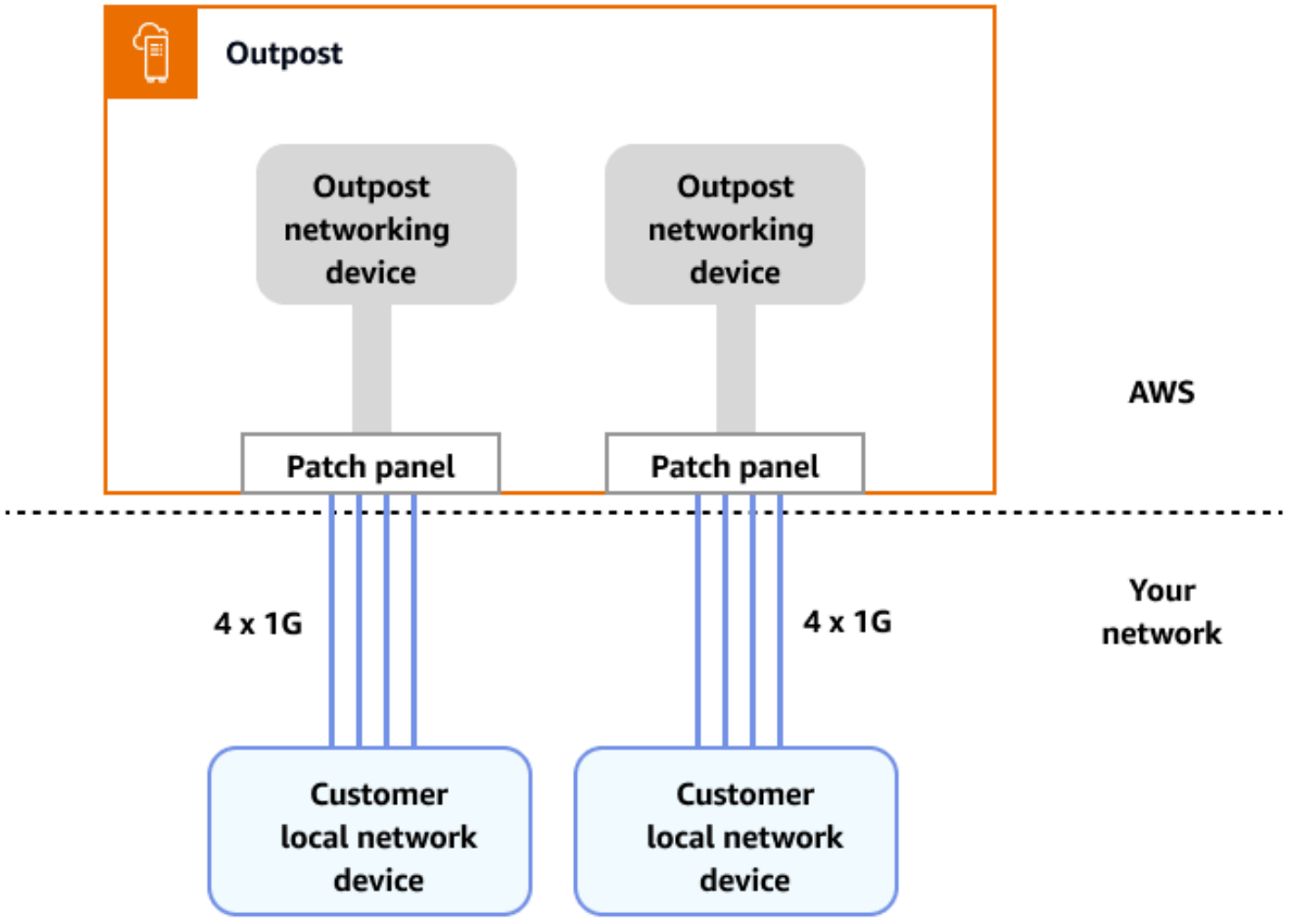
Les Zones Locales sont connectées à la région mère par de multiples liaisons haut débit sécurisées et redondantes qui vous permettent d'utiliser n'importe quel service régional, tel qu'Amazon S3 et Amazon RDS, de manière fluide. Vous êtes responsable de fournir la connectivité entre votre environnement local ou vos utilisateurs et la zone locale. Quelle que soit l'architecture de connectivité que vous choisissez (par exemple, VPN ou 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 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 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 Direct Connect seul PoP rend impossible la création des architectures recommandées pour Direct Connect la résilience. Si vous n'avez accès qu'à un seul 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 Direct Connect et, comme illustré et expliqué dans AWS le billet de 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 (OND). 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.

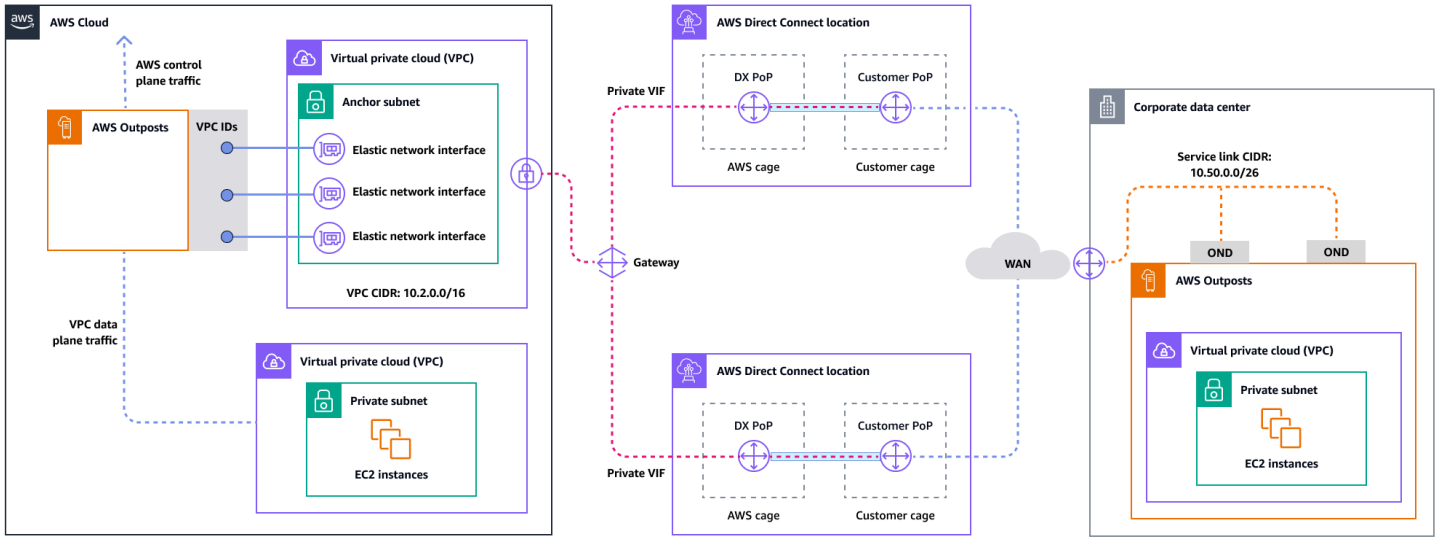
Vitesse de la liaison montante	Nombre de liaisons montantes
1 Gbit/s	1, 2, 4, 6 ou 8
10 Gbit/s	1, 2, 4, 8, 12 ou 16
40 ou 100 Gbit/s	1, 2 ou 4



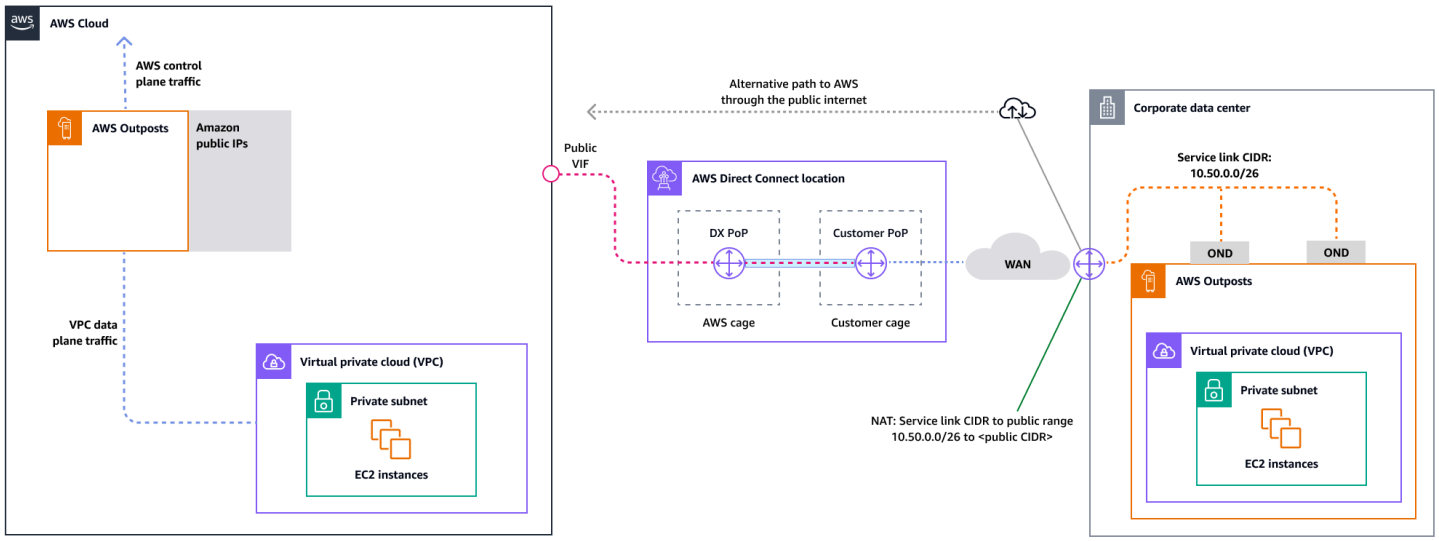
Pour plus d'informations sur cette connectivité, consultez la section Connectivité réseau locale pour les Outposts Racks dans la documentation. AWS Outposts

Pour une expérience et une résilience optimales, il est AWS recommandé d'utiliser une connectivité redondante d'au moins 500 Mbits/s (1 Gbit/s est préférable) pour la connexion par liaison de service au. Région AWS Vous pouvez utiliser Direct Connect une connexion Internet pour le lien de service. Ce minimum vous permet de lancer des instances EC2, 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.

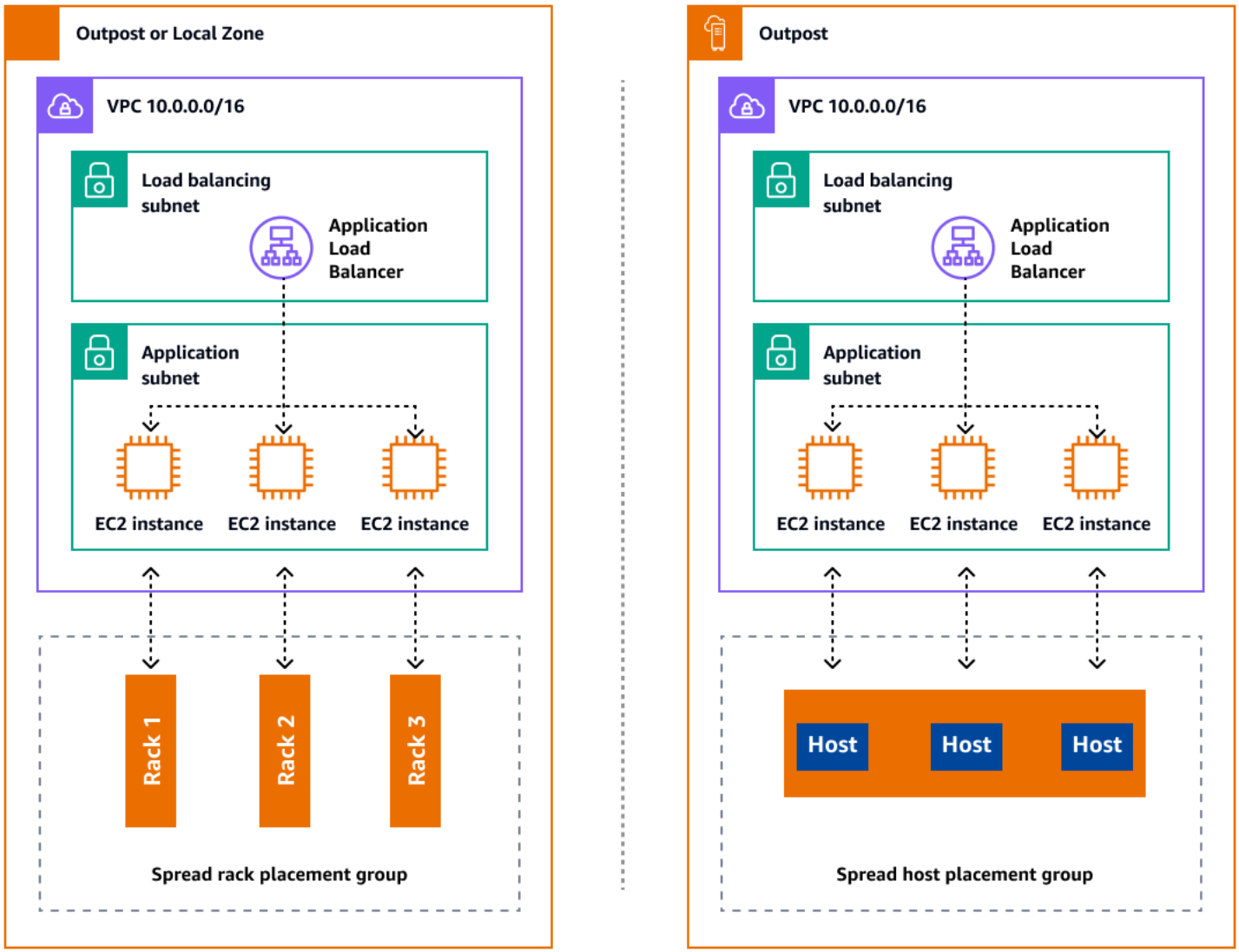


Expansion des déploiements en rack d'Outposts avec des racks ACE

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 de l'alimentation, 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 dans Multi-AZ AWS Outposts

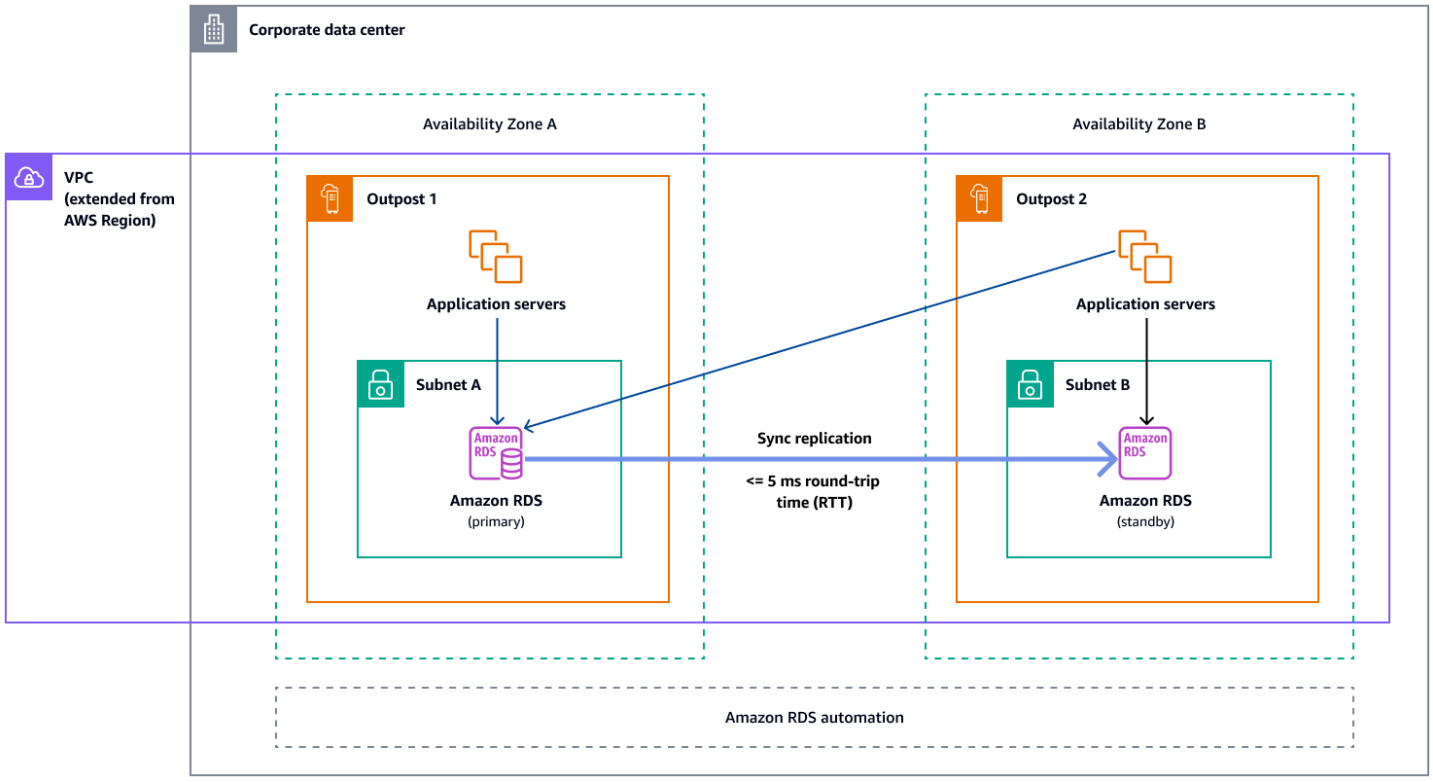
Lorsque vous utilisez des déploiements d' Multi-AZ instances sur des Outposts, Amazon RDS crée deux instances de base de données sur deux Outposts. Chaque avant-poste fonctionne sur sa propre infrastructure physique et se connecte aux différentes zones de disponibilité d'une région pour une haute disponibilité. 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 Multi-AZ déploiements, Amazon RDS crée une instance de base de données principale sur un avant-poste et réplique les données de manière synchrone sur une instance de base de données de secours sur un autre avant-poste. Multi-AZ les

déploiements sur les Outposts fonctionnent Multi-AZ comme les déploiements Régions AWS dans 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 les adresses Customer-owned IP d'Amazon RDS AWS Outposts dans la documentation Amazon RDS.
- La réplication fonctionne sur votre réseau local.

Multi-AZ les déploiements 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 Multi-AZ déploiements.

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

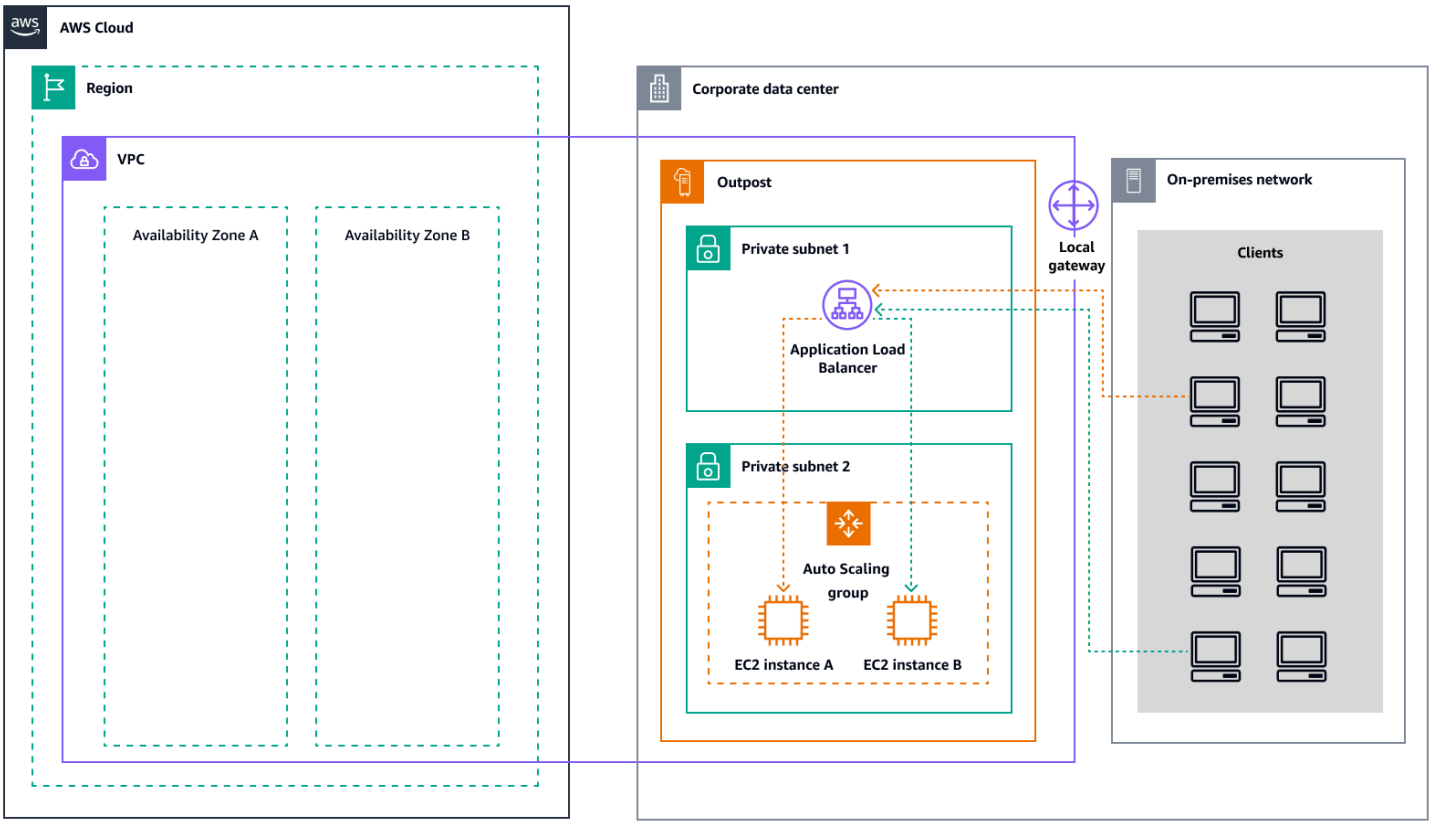


Mécanismes de basculement

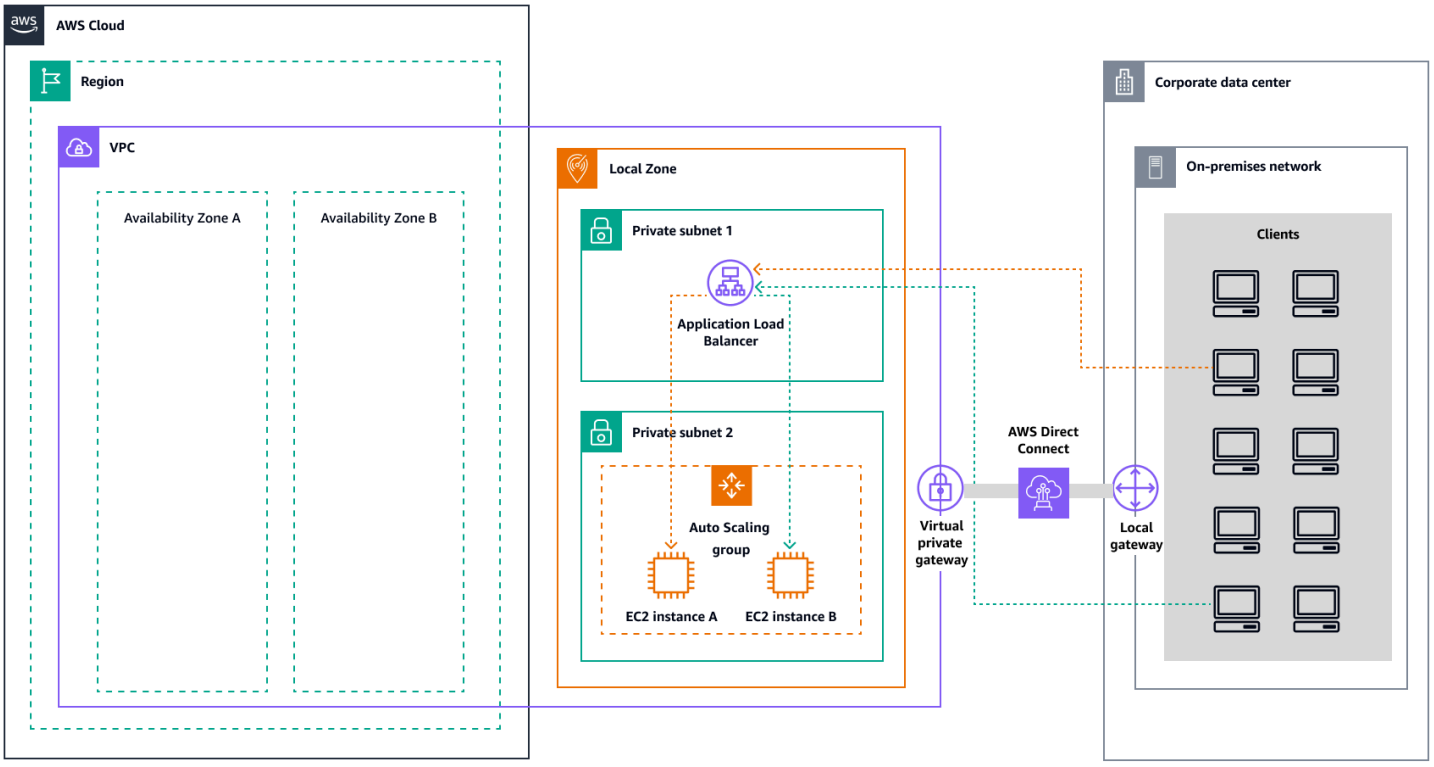
Équilibrage de charge et dimensionnement automatique

Elastic Load Balancing (ELB) répartit automatiquement le trafic applicatif entrant sur toutes les instances EC2 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 instances EC2 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 EC2 dans. AWS Outposts



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

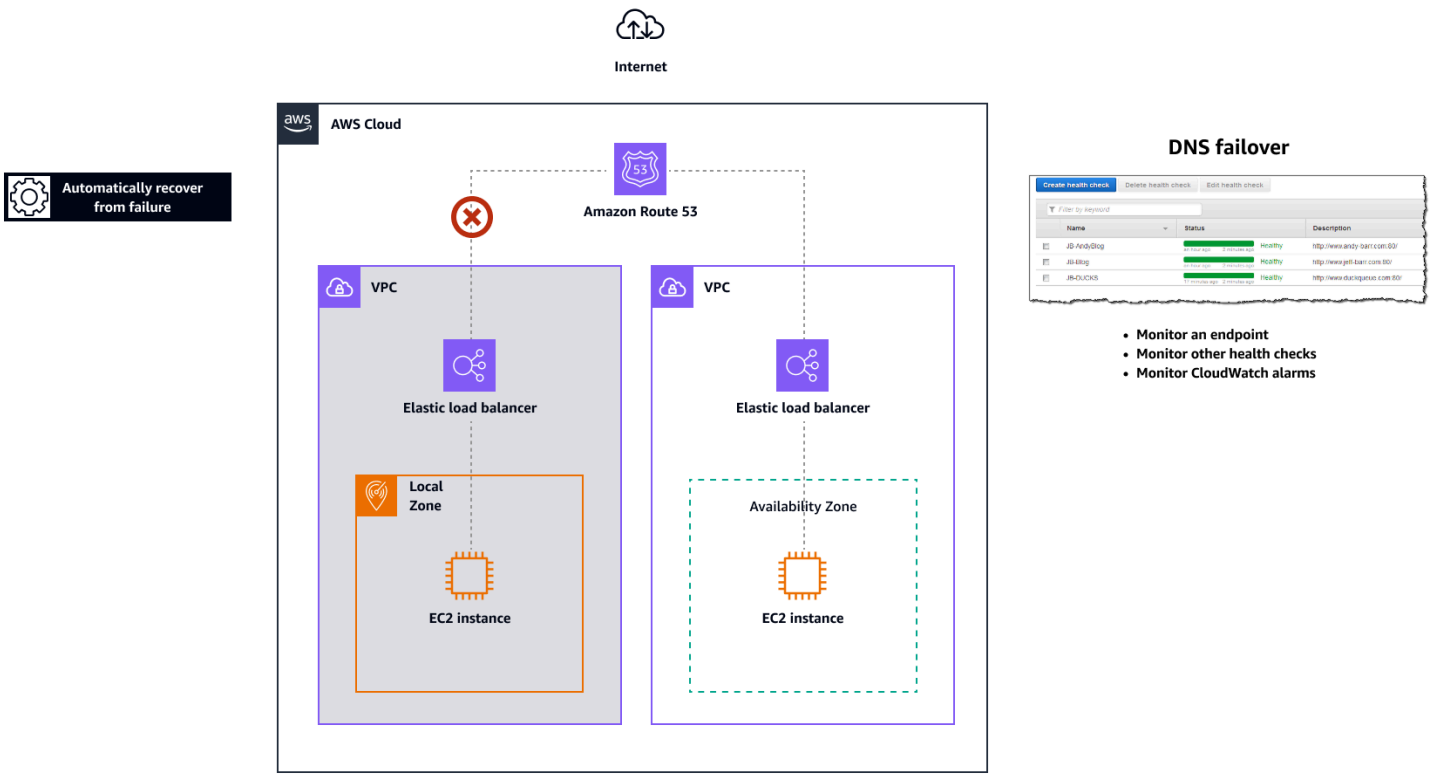


> **Note**
>
> Les équilibreurs de charge d'application sont disponibles à la fois dans les Zones Locales AWS Outposts et dans les Zones Locales. Toutefois, pour utiliser un Application Load Balancer AWS Outposts, vous devez dimensionner la capacité Amazon EC2 afin de fournir l'évolutivité requise par 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) des adresses IP publiques 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 Outposts-hosted application.

Amazon Route 53 Resolver on 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 nécessitant 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 VPC Outposts 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 les VPC 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
Reprise après sinistre AWS Elastic	Travailler avec Reprise après sinistre AWS Elastic et AWS Outposts	Non disponible
AWS Transform MGN	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 pour 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

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.