Guide de l’utilisateur pour les racks

AWS Outposts

AWS Outposts: Guide de l’utilisateur pour les racks

Table of Contents

Qu'est-ce que c'est AWS Outposts ?

AWS Outposts est un service entièrement géré qui étend AWS l'infrastructure, les services, les API et les outils aux locaux des clients. En fournissant un accès local à l'infrastructure AWS gérée, il AWS Outposts permet aux clients de créer et d'exécuter des applications sur site en utilisant les mêmes interfaces de programmation que dans AWS les régions, tout en utilisant les ressources de calcul et de stockage locales pour réduire la latence et les besoins de traitement des données locaux.

Un avant-poste est un pool de capacités de AWS calcul et de stockage déployé sur le site d'un client. AWS exploite, surveille et gère cette capacité dans le cadre d'une AWS région. Vous pouvez créer des sous-réseaux sur votre Outpost et les spécifier lorsque vous créez des AWS ressources telles que des instances EC2, des volumes EBS, des clusters ECS et des instances RDS. Les instances des sous-réseaux Outpost communiquent avec d'autres instances de la AWS région à l'aide d'adresses IP privées, le tout au sein du même VPC.

> **Note**
>
> Vous ne pouvez pas connecter un Outpost à un autre Outpost ou à une autre zone locale appartenant au même VPC.

Pour en savoir plus, consultez la page produit d'AWS Outposts.

Concepts clés

Ce sont les concepts clés pour AWS Outposts.

- Site de l'avant-poste — Les bâtiments physiques gérés par le client où AWS sera installé votre avant-poste. Un site doit répondre aux exigences de votre Outpost en matière de locaux, de mise en réseau et d'alimentation.
- Capacité de l'Outpost : ressources de calcul et de stockage disponibles sur l'Outpost. Vous pouvez afficher et gérer la capacité de votre Outpost à partir de la console AWS Outposts .
- Équipement de l'avant-poste : matériel physique permettant d'accéder au AWS Outposts service. Le matériel comprend les racks, les serveurs, les commutateurs et le câblage détenus et gérés par. AWS

- Racks Outpost : facteur de format Outpost conforme aux normes de l'industrie en matière de rack 42U. Les racks Outpost incluent des serveurs montables en rack, des commutateurs, un panneau de correctif réseau, une étagère d'alimentation et des panneaux vierges.
- Serveurs Outpost : facteur de format Outpost conforme aux normes de l'industrie en matière de serveur 1U ou 2U, qui peut être installé dans un rack à 4 montants conforme à la norme EIA-310D 19. Les serveurs Outpost fournissent des services locaux de calcul et de mise en réseau aux sites dont l'espace est limité ou les besoins en capacité sont moindres.
- Liaison de service — Route réseau qui permet la communication entre votre avant-poste et AWS la région associée. Chaque Outpost est une extension d'une zone de disponibilité et de sa région associée.
- Passerelle locale (LGW) : routeur virtuel d'interconnexion logique qui permet la communication entre un rack Outpost et votre réseau local.
- Interface réseau locale : interface réseau qui permet la communication entre un serveur Outpost et votre réseau sur site.

AWS ressources sur Outposts

Vous pouvez créer les ressources suivantes sur votre Outpost pour prendre en charge les charges de travail à faible latence qui doivent être exécutées à proximité des données et des applications sur site :

Calcul

Type de ressource	Racks	Serveurs
Instances Amazon EC2	O	Oui
Clusters Amazon ECS	O	Oui
Nœuds Amazon EKS	O	Non

Base de données et analytique

Type de ressource	Racks	Serveurs
ElastiCache Nœuds Amazon (cluster Redis, cluster Memcached)	 Oui	 Non
Clusters Amazon EMR	 Oui	 Non
Instances de base de données Amazon RDS	 Oui	 Non

Réseaux

Type de ressource	Racks	Serveurs
Proxy App Mesh Envoy	 Oui	 Oui
Application Load Balancers	 Oui	 Non
Sous-réseaux Amazon VPC	 Oui	 Oui
Amazon Route 53	 Oui	 Non

Stockage

Type de ressource	Racks	Serveurs
Volumes Amazon EBS	 Oui	 Non
Compartiments Amazon S3	 Oui	 Non

Autres Services AWS

Service	Racks	Serveurs
AWS IoT Greengrass	 Oui	 Oui
Amazon SageMaker Edge Manager	 Oui	 Oui

Tarification

Vous pouvez choisir parmi diverses configurations Outpost, chacune offrant une combinaison de types d'instances EC2 et d'options de stockage. Le prix des configurations en rack inclut l'installation, le retrait et la maintenance. Pour les serveurs, vous devez installer et entretenir l'équipement.

Vous achetez une configuration pour une durée de 3 ans et avez le choix entre trois options de paiement : Tous les frais initiaux, Frais initiaux partiels et Aucuns frais initiaux. Si vous choisissez l'option de paiement Frais initiaux partiels ou Aucuns frais initiaux, des frais mensuels s'appliquent. Les frais initiaux sont applicables 24 heures après l'installation de votre Outpost et après la mise à disposition de la capacité de calcul et de stockage. Pour plus d'informations, consultez :

- AWS Outposts tarification des rayonnages

- AWS Outposts tarification des serveurs

Fonctionnement d'AWS Outposts

AWS Outpostsest conçu pour fonctionner avec une connexion constante et cohérente entre votre avant-poste et une AWS région. Pour établir cette connexion à la région et aux charges de travail locales de votre environnement sur site, vous devez connecter votre Outpost à votre réseau local. Votre réseau local doit fournir un accès réseau étendu (WAN) à la région et à Internet. Il doit également fournir un accès LAN ou WAN au réseau local où résident vos charges de travail ou applications sur site.

Le schéma suivant illustre les deux formats Outpost.

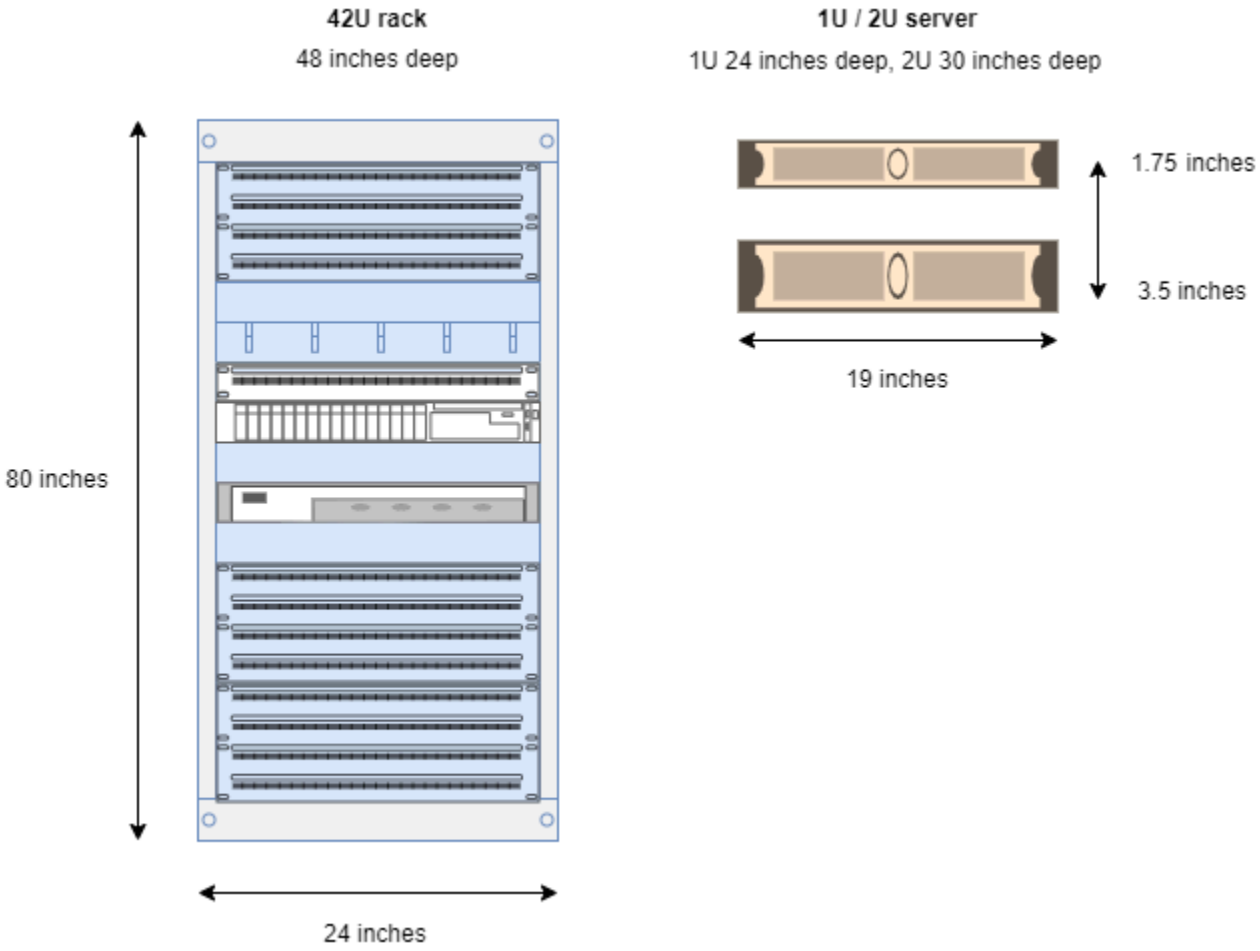


Table des matières

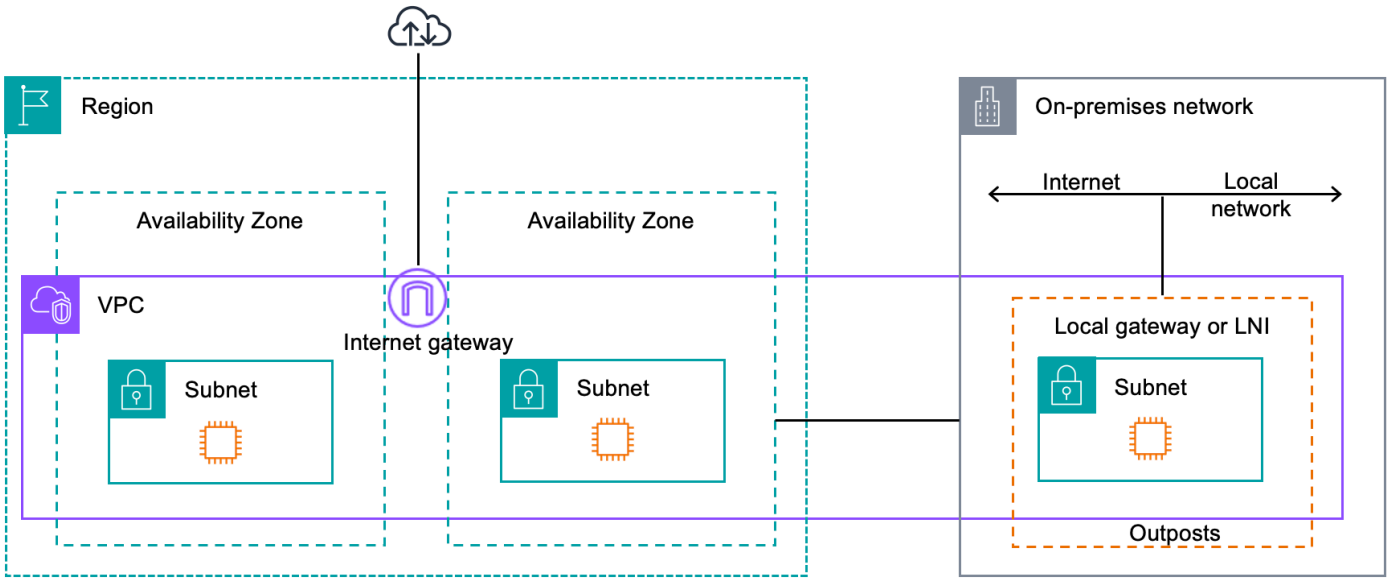
- DNS
- Lien vers le service
- Passerelles locales
- Interfaces réseau locales

Composants du réseau

AWS Outposts étend un Amazon VPC à partir d'une AWS vers un Outpost avec les composants VPC accessibles dans la Région, y compris les passerelles Internet, les passerelles privées virtuelles, les Amazon VPC Transit Gateways et les point de terminaison d'un VPC. Un Outpost est hébergé dans une zone de disponibilité dans la Région et est une extension de cette zone de disponibilité que vous pouvez utiliser pour assurer la résilience.

Le schéma suivant montre les composants du réseau de votre avant-poste.

- Un Région AWS et un réseau sur site
- Un VPC avec plusieurs sous-réseaux dans la région
- Un avant-poste dans le réseau local
- Connectivité entre l'avant-poste et le réseau local assurée par une passerelle locale (racks) ou une interface réseau locale (serveurs)



VPC et sous-réseaux

Un cloud privé virtuel (VPC) couvre toutes les zones de disponibilité de sa région. AWS Vous pouvez étendre n'importe quel VPC de la région à votre Outpost en ajoutant un sous-réseau Outpost. Pour ajouter un sous-réseau Outpost à un VPC, spécifiez l'ARN (Amazon Resource Name) de l'Outpost lorsque vous créez le sous-réseau.

Les Outposts prennent en charge plusieurs sous-réseaux. Vous pouvez spécifier le sous-réseau de l'instance EC2 lorsque vous lancez l'instance EC2 dans votre Outpost. Vous ne pouvez pas spécifier le matériel sous-jacent sur lequel l'instance est déployée, car l'Outpost est un pool de capacités de AWS calcul et de stockage.

Chaque Outpost peut prendre en charge plusieurs VPC pouvant avoir un ou plusieurs sous-réseaux Outpost. Pour plus d'informations sur les quotas VPC, consultez Amazon VPC Quotas dans le guide de l'utilisateur Amazon VPC.

Vous créez des sous-réseaux Outpost à partir de la plage d'adresses CIDR VPC du VPC dans lequel vous avez créé l'Outpost. Vous pouvez utiliser les plages d'adresses Outpost pour les ressources, telles que les instances EC2 résidant dans le sous-réseau Outpost.

Routage

Par défaut, chaque sous-réseau Outpost hérite de la table de routage principale de son VPC. Vous pouvez créer une table de routage personnalisée et l'associer à un sous-réseau Outpost.

Les tables de routage pour les sous-réseaux Outpost fonctionnent comme pour les sous-réseaux de zone de disponibilité. Vous pouvez spécifier des adresses IP, des passerelles Internet, des passerelles locales, des passerelles privées virtuelles et des connexions d'appairage comme destinations. Par exemple, chaque sous-réseau Outpost, que ce soit par le biais de la table de routage principale héritée ou d'une table personnalisée, hérite de la route locale du VPC. Cela signifie que tout le trafic du VPC, y compris le sous-réseau Outpost avec une destination dans le CIDR du VPC, reste acheminé dans le VPC.

Les tables de routage du sous-réseau Outpost peuvent inclure les destinations suivantes :

- Plage d'adresses CIDR VPC : elle est AWS définie lors de l'installation. Il s'agit de la route locale qui s'applique à tous les routages VPC, y compris le trafic entre les instances d'Outpost d'un même VPC.

- AWSDestinations régionales : cela inclut les listes de préfixes pour Amazon Simple Storage Service (Amazon S3), les points de terminaison de la passerelle Amazon DynamoDB, les passerelles privées virtuellesAWS Transit Gateway, les passerelles Internet et le peering VPC.

  Si vous avez une connexion d'appairage avec plusieurs VPC sur le même avant-poste, le trafic entre les VPC reste dans l'avant-poste et n'utilise pas le lien de service vers la région.
- Communication intra-VPC entre les Outposts avec une passerelle locale — Vous pouvez établir une communication entre les sous-réseaux d'un même VPC à travers différents Outposts grâce à des passerelles locales en utilisant le routage VPC direct. Pour plus d'informations, reportez-vous à :
  - Routage VPC direct
  - Routage vers une passerelle AWS Outposts locale

DNS

Pour les interfaces réseau connectées à un VPC, les instances EC2 des sous-réseaux Outposts peuvent utiliser le service DNS Amazon Route 53 pour convertir les noms de domaine en adresses IP. Route 53 prend en charge les fonctionnalités DNS, telles que l'enregistrement de domaines, le routage DNS et les contrôles de santé pour les instances exécutées dans votre Outpost. Les zones de disponibilité hébergées publiques et privées sont prises en charge pour acheminer le trafic vers des domaines spécifiques. Les résolveurs Route 53 sont hébergés dans la AWS région. Par conséquent, la connectivité des liaisons de service entre l'avant-poste et la AWS région doit être opérationnelle pour que ces fonctionnalités DNS fonctionnent.

Il se peut que vous rencontriez des temps de résolution DNS plus longs avec Route 53, en fonction de la latence du chemin entre votre Outpost et la région AWS. Dans ce cas, vous pouvez utiliser les serveurs DNS installés localement dans votre environnement sur site. Pour utiliser vos propres serveurs DNS, vous devez créer des ensembles d'options DHCP pour vos serveurs DNS locaux et les associer au VPC. Vous devez également vous assurer qu'il existe une connectivité IP avec ces serveurs DNS. Vous devrez peut-être également ajouter des itinéraires à la table de routage de la passerelle locale pour des raisons d'accessibilité, mais cette option n'est possible que pour les racks Outpost dotés d'une passerelle locale. Étant donné que les ensembles d'options DHCP ont une portée VPC, les instances des sous-réseaux Outpost et des sous-réseaux de zone de disponibilité du VPC essaieront d'utiliser les serveurs DNS spécifiés pour la résolution des noms DNS.

L'enregistrement des requêtes n'est pas pris en charge pour les requêtes DNS provenant d'un Outpost.

Lien vers le service

Le lien de service est une connexion entre votre Outpost et la région de votre choix ou AWS la région d'origine de l'Outpost. Le lien de service est un ensemble crypté de connexions VPN qui sont utilisées chaque fois que l'Outpost communique avec la région d'origine de votre choix. Vous utilisez un réseau local virtuel (VLAN) pour segmenter le trafic sur le lien de service. La liaison de service VLAN permet la communication entre l'avant-poste et la AWS région pour la gestion de l'avant-poste et le trafic intra-VPC entre la région et l'avant-poste. AWS

Votre lien de service est créé lorsque votre Outpost est approvisionné. Si vous avez un format de serveur, vous créez la connexion. Si vous avez un rack, AWS crée le lien de service. Pour plus d'informations, consultez la section Connectivité d'Outpost à Régions AWS.

Passerelles locales

Les racks Outpost incluent une passerelle locale qui fournit la connectivité à votre réseau local. Si vous possédez un rack Outpost, vous pouvez inclure une passerelle locale comme cible dont la destination est votre réseau local. Les passerelles locales ne sont disponibles que pour les racks Outpost et ne peuvent être utilisées que dans les tables de routage VPC et de sous-réseau associées à un rack Outpost. Pour plus d'informations, veuillez consulter Passerelle locale.

Interfaces réseau locales

Les serveurs Outpost incluent une interface réseau locale qui fournit une connectivité à votre réseau local. Une interface réseau locale n'est disponible que pour les serveurs Outposts exécutés sur un sous-réseau Outpost. Vous ne pouvez pas utiliser d'interface réseau locale à partir d'une instance EC2 sur un rack Outpost ou dans la AWS région. L'interface réseau locale est uniquement destinée aux sites locaux. Pour plus d'informations, consultez la section Interface réseau locale dans le Guide de AWS Outposts l'utilisateur pour les serveurs Outposts.

Exigences du site pour le rack Outposts

Un site Outpost est l'emplacement physique où opère votre Outpost. Les sites sont uniquement disponibles dans certains pays et territoires. Pour plus d'informations, consultez FAQ sur le rack AWS Outposts. Reportez-vous à la question : Dans quels pays et territoires le rack Outposts est-il disponible ?

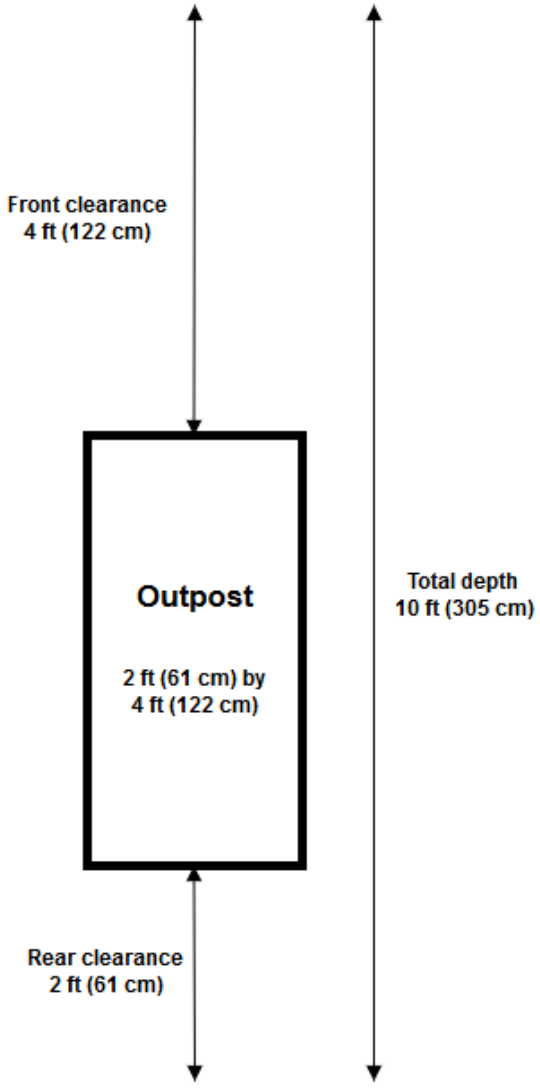
Cette page décrit les exigences relatives au rack Outposts. Pour connaître les exigences relatives aux serveurs Outposts, consultez Exigences du site pour les serveurs Outposts dans le Guide de l'utilisateur AWS Outposts pour les serveurs Outposts.

Installations

Les exigences relatives aux installations pour les racks sont décrites ci-dessous.

- Température et humidité : la température ambiante doit être comprise entre 5 et 35 °C (41 et 95 °F). L'humidité relative doit être comprise entre 8 et 80 % sans condensation.
- Débit d'air : les racks aspirent l'air froid à l'avant et évacuent l'air chaud à l'arrière. L'emplacement du rack doit fournir un débit d'air d'au moins 145,8 fois le kVA de pieds cubes par minute (pi³/min).
- Quai de chargement : votre quai de chargement doit pouvoir accueillir une caisse de 239 cm (94 pouces) de hauteur par 138 cm (54 pouces) de largeur par 130 cm (51 pouces) de profondeur.
- Support de poids : le poids varie en fonction de la configuration. Le poids de votre configuration est indiqué dans le résumé de la commande au point de chargement du rack. L'emplacement où le rack est installé et le chemin menant à cet emplacement doivent supporter le poids spécifié. Cela inclut tous les ascenseurs de fret et les ascenseurs standard situés le long du chemin.
- Espace de dégagement : le rack mesure 203 cm (80 pouces) de hauteur par 61 cm (24 pouces) de largeur par 122 cm (48 pouces) de profondeur. Les portes, les couloirs, les virages, les rampes et les ascenseurs doivent être suffisamment dégagés. En position de repos finale, il doit y avoir une zone de 61 cm (24 pouces) de largeur par 122 cm (48 pouces) de profondeur pour l'Outpost, avec un espace de dégagement supplémentaire de 122 cm (48 pouces) à l'avant et de 61 cm (24 pouces) à l'arrière. La superficie minimale totale requise pour l'Outpost est 61 cm (24 pouces) de largeur par 305 cm (10 pieds) de profondeur.

  Le schéma suivant montre la superficie minimale totale requise pour l'Outpost, espace de dégagement compris.



- Renforts sismiques — Dans la mesure requise par la réglementation ou le code, vous installerez et entretiendrez un ancrage sismique et un contreventement appropriés pour le rack pendant qu'il se trouve dans vos installations. AWSfournit des supports de sol qui protègent contre une activité sismique allant jusqu'à 2,0 G avec tous les racks Outposts.
- Point de connexion : nous vous recommandons de fournir un fil ou un point de connexion à l'emplacement du rack afin que le technicien AWS certifié puisse fixer les racks lors de l'installation.
- Accès aux installations : ne modifiez pas les installations d'une manière qui nuirait à la capacité d'AWS d'accéder à l'Outpost, de le dépanner ou de le retirer.
- Hauteur sous plafond : la hauteur sous plafond de la pièce où le rack est installé doit être inférieure à 3 050 mètres (10 005 pieds).

Réseaux

Les exigences relatives à la mise en réseau pour les racks sont décrites ci-dessous.

- Indiquez des liaisons montantes avec des vitesses de 1 Gbit/s, 10 Gbit/s, 40 Gbit/s ou 100 Gbit/s.

  Pour les recommandations relatives à la bande passante pour la connexion de la liaison de service, consultez Recommandations en matière de bande passante.
- Indiquez la fibre monomode (SMF) avec Lucent Connector (LC), la fibre multimode (MMF) ou la fibre MMF OM4 avec LC.
- Indiquez un ou deux périphériques en amont, qui peuvent être des commutateurs ou des routeurs. Nous recommandons deux périphériques pour garantir une haute disponibilité.

Liste de contrôle de préparation du réseau

Utilisez cette liste de contrôle au moment de collecter les informations nécessaires à la configuration de votre Outpost. Cela inclut le réseau local (LAN), le réseau étendu (WAN) et tous les périphériques situés entre l'Outpost et les destinations de trafic local, ainsi que la destination dans la région AWS.

Vitesse de liaison montante, ports et fibre

Vitesse de liaison montante et ports

Un Outpost possède deux périphériques réseau Outpost qui se connectent à votre réseau local. Le nombre de liaisons montantes que chaque périphérique peut prendre en charge dépend de vos besoins en bande passante et des capacités de votre routeur. Pour plus d'informations, consultez Connectivité physique.

La liste suivante indique le nombre de ports de liaison montante pris en charge par chaque périphérique réseau Outpost, en fonction de la vitesse de la liaison montante.

1 Gbit/s

1, 2, 4, 6 ou 8 liaisons montantes

10 Gbit/s

1, 2, 4, 8, 12 ou 16 liaisons montantes

40 Gbit/s ou 100 Gbit/s

1, 2 ou 4 liaisons montantes

Fibre

Les types de fibre suivants sont pris en charge :

- Fibre monomode (SMF) avec Lucent Connector (LC)
- Fibre multimode (MMF) ou MMF OM4 avec LC

En fonction de la vitesse de la liaison montante et du type de fibre que vous choisissez, les normes optiques suivantes sont prises en charge.

Vitesse de la liaison montante	Type de fibre	Norme optique
1 Gbit/s	SMF	– 1000Base-LX
1 Gbit/s	MMF	– 1000Base-SX
10 Gbit/s	SMF	– 10GBASE-IR – 10GBASE-LR
10 Gbit/s	MMF	– 10GBASE-SR
40 Gbit/s	SMF	– 40GBASE-IR4 (LR4L) – 40GBASE-LR4
Application de dérivation 4 x 10 Gbit/s	MMF	– 40GBASE-ESR4 – 40GBASE-SR4
100 Gbit/s	SMF	– 100G PSM4 MSA – 100GBASE-CWDM4 – 100GBASE-LR4
Application de dérivation 4 x 25 Gbit/s	MMF	– 100GBASE-SR4

Agrégation de liaisons Outpost et VLAN

Le protocole LACP (Link Aggregation Control Protocol) est requis entre l'Outpost et votre réseau. Vous devez utiliser le LAG dynamique avec LACP.

Les VLAN suivants sont requis pour chaque périphérique réseau Outpost. Pour plus d'informations, consultez Réseaux locaux (LAN) virtuels.

Périphérique réseau Outpost	VLAN de liaison de service	VLAN de passerelle locale
1	Valeurs valides : de 1 à 4094	Valeurs valides : de 1 à 4094
2	Valeurs valides : de 1 à 4094	Valeurs valides : de 1 à 4094

Pour chaque périphérique réseau Outpost, vous pouvez choisir d'utiliser les mêmes VLAN ou des VLAN différents pour la liaison de service et la passerelle locale. Cependant, nous recommandons que chaque périphérique réseau Outpost dispose d'un VLAN différent de celui des autres périphériques réseau Outpost. Pour plus d'informations, consultez Agrégation de liaisons et Réseaux locaux (LAN) virtuels.

Nous recommandons également une connectivité redondante de couche 2. Le protocole LACP est utilisé pour l'agrégation de liaisons et non pour la haute disponibilité. Le protocole LACP entre les périphériques réseau Outpost n'est pas pris en charge.

Connectivité IP des périphériques réseau Outpost

Chacun des deux périphériques réseau Outpost nécessite un CIDR et une adresse IP pour les VLAN de liaison de service et de passerelle locale. Nous recommandons d'allouer un sous-réseau dédié à chaque périphérique réseau avec un CIDR /30 ou /31. Spécifiez un sous-réseau et une adresse IP à partir du sous-réseau que l'Outpost doit utiliser. Pour plus d'informations, consultez Connectivité de la couche réseau.

Périphérique réseau Outpost	Exigences relatives à la liaison de service	Exigences relatives à la passerelle locale
1	– CIDR de la liaison de service (/30 ou /31)	– CIDR de la passerelle locale (/30 ou /31)

Périphérique réseau Outpost	Exigences relatives à la liaison de service	Exigences relatives à la passerelle locale
	– Adresse IP de la liaison de service	– Adresse IP de la passerelle locale
2	– CIDR de la liaison de service (/30 ou /31) – Adresse IP de la liaison de service	– CIDR de la passerelle locale (/30 ou /31) – Adresse IP de la passerelle locale

Unité de transmission maximale (MTU) d'une liaison de service

Le réseau doit prendre en charge une MTU de 1 500 octets entre l'Outpost et les points de terminaison des liaisons de service dans la région parent. AWS Pour plus d'informations sur la liaison de service, consultez Connectivité AWS Outposts avec les régions AWS.

Protocole de passerelle frontière (BGP) de la liaison de service

L'Outpost établit une session d'appairage BGP externe (eBGP) entre chaque périphérique réseau Outpost et votre périphérique réseau local pour la connectivité de liaison de service via le VLAN de liaison de service. Pour plus d'informations, consultez Connectivité BGP de la liaison de service.

Outpost	Exigences relatives au protocole BGP de la liaison de service
Votre Outpost	– Numéro de système autonome (ASN) BGP Outpost. 2 octets (16 bits) ou 4 octets (32 bits). Depuis votre plage ASN privée (64512-65534 ou 4200000000-4294967294). – CIDR de l'infrastructure (/26 requis, publié sous la forme de deux /27 contigus).

Périphérique réseau local	Exigences relatives au protocole BGP de la liaison de service
1	– Adresse IP d'appairage BGP de la liaison de service. – ASN d'appairage BGP de la liaison de service. 2 octets (16 bits) ou 4 octets (32 bits).
2	– Adresse IP d'appairage BGP de la liaison de service. – ASN d'appairage BGP de la liaison de service. 2 octets (16 bits) ou 4 octets (32 bits).

Pare-feu de la liaison de service

Les protocoles UDP et TCP 443 doivent être répertoriés par état dans le pare-feu.

Protocole	Port source	Adresse source	Port de destination	Adresse de destination
UDP	443	Liaison de service Outpost /26	443	Routes publiques de la région Outpost
TCP	1025-65535	Liaison de service Outpost /26	443	Routes publiques de la région Outpost

Vous pouvez utiliser une connexion AWS Direct Connect ou une connexion Internet publique pour reconnecter Outpost à la région AWS. Pour la connectivité de la liaison de service Outpost, vous pouvez utiliser le NAT ou le PAT au niveau de votre pare-feu ou de votre routeur périphérique. L'établissement d'une liaison de service est toujours initié depuis Outpost.

Protocole de passerelle frontière (BGP) de la passerelle locale

L'Outpost établit une session d'appairage eBGP entre chaque périphérique réseau Outpost et un périphérique réseau local pour la connectivité à la passerelle locale à partir de votre réseau local. Pour plus d'informations, consultez Connectivité BGP de passerelle locale.

Outpost	Exigences relatives au protocole BGP de la passerelle locale
Votre Outpost	– Numéro de système autonome (ASN) BGP Outpost. 2 octets (16 bits) ou 4 octets (32 bits). Depuis votre plage ASN privée (64512-65534 ou 4200000000-4294967294). – CIDR CoIP à publier (public ou privé, /26 au minimum).

Périphériques réseau local	Exigences relatives au protocole BGP de la passerelle locale
1	– Adresse IP d'appairage BGP de la passerelle locale. – ASN d'appairage BGP de la passerelle locale. 2 octets (16 bits) ou 4 octets (32 bits).
2	– Adresse IP d'appairage BGP de la passerelle locale. – ASN d'appairage BGP de la passerelle locale. 2 octets (16 bits) ou 4 octets (32 bits).

Alimentation

L'étagère d'alimentation Outposts prend en charge trois configurations d'alimentation : 5 kVA, 10 kVA ou 15 kVA. La configuration de l'étagère d'alimentation dépend de la capacité de consommation

énergétique totale de l'Outpost. Par exemple, si votre ressource Outpost possède une consommation énergétique maximale de 9,7 kVA, vous devez indiquer les configurations d'alimentation pour 10 kVA : 4 x L6-30P ou IEC309, 2 baisses vers S1 et 2 baisses vers S2 pour une alimentation redondante monophasée. Les trois configurations d'alimentation sont décrites dans le deuxième tableau ci-dessous.

Pour connaître les exigences relatives à la consommation énergétique pour les différentes ressources Outpost, choisissez Parcourir le catalogue dans la console AWS Outposts à l'adresse https://console.aws.amazon.com/outposts/.

Tension de ligne CA	Monophasée 208 à 277 VCA (50 ou 60 Hz) Triphasée 346 à 480 VCA (50 à 60 Hz)
Consommation d'énergie	5 kVA (4 kW), 10 kVA (9 kW) ou 15 kVA (13 kW)
Protection du courant alternatif (disjoncteurs en amont)	Pour les entrées 1N (non redondantes) et 2N (redondantes) : 30 A ou 32 A avec disjoncteur en D ou en K. Pour une entrées 2N (redondante) uniquement : disjoncteur en C, en D ou en K. Les disjoncteurs en B ou inférieurs ne sont pas pris en charge.
Type d'entrée CA (connecteur femelle)	Monophasée : 3xL6-30P, P+P+E, 30A ou 3xIEC60309 P+N+E, IP67, prises 32A Triphasée, Wye : 1xIEC60309, 3P+N+E, IP67, position d'horloge 7, prise 30A ou 1xIEC60309, 3P+N+E, IP67, position d'horloge 6, prise 32A Triphasée, Delta : 1xNon-NEMA twistlock Hubbell CS8365C, 3P +E, mise à la terre au centre, prise 50A **Note** La meilleure pratique consiste à associer une prise IP67 à un connecteur femelle IP67. Si cela n'est pas possible, la prise IP67 sera associée à un connecteur femelle IP44. La valeur nominale de la combinaison de la prise

	et du socket deviendra la valeur nominale inférieure (IP44).
Longueur du câble	3 m (10,25 pieds)
Câble - Entrée de câblage du rack	Depuis le dessus ou le dessous du rack

L'étagère d'alimentation possède deux entrées, S1 et S2, qui peuvent être configurées comme suit.

	Redondante, monophasée	Redondante, triphasée	Monophasée	Triphasée
5 kVA	2 x L6-30P ou IEC309, 1 baisse vers S1 et 1 baisse vers S2	2 x AH530P7W ou AH532P6W, 1 baisse vers S1 et 1 baisse vers S2	1 x L6-30P ou IEC309, 1 baisse vers S1	1 x AH530P7W ou AH532P6W, 1 baisse vers S1
10 kVA	4 x L6-30P ou IEC309, 2 baisses vers S1 et 2 baisses vers S2		2 x L6-30P ou IEC309, 2 baisses vers S1	
15 kVA	6 x L6-30P ou IEC309, 3 baisses vers S1 et 3 baisses vers S2		3 x L6-30P ou IEC309, 3 baisses vers S1	

Si les câbles CA fournis par AWS conformément à la description précédente doivent être équipés d'une autre prise d'alimentation, tenez compte des points suivants :

- Seul un électricien certifié désigné par le client peut modifier le câble CA pour l'adapter à un nouveau type de prise.
- L'installation doit être conforme à toutes les exigences nationales et locales qui s'appliquent en matière de sécurité. Elle doit être inspectée pour garantir la sécurité électrique.
- En tant que client, vous devez informer votre représentant AWS des modifications apportées à la prise du câble CA. Sur demande, vous pouvez fournir des informations sur les modifications apportées à AWS. Vous devez également inclure tous les dossiers d'inspection de sécurité émis

par l'autorité compétente. Il s'agit d'une condition requise pour valider la sécurité de l'installation avant que les employés AWS n'effectuent des travaux sur l'équipement.

Exécution des commandes

Pour honorer la commande, AWS fixe avec vous une date et une heure. Vous recevez également une liste des éléments à vérifier ou à fournir avant l'installation.

L'équipe d'installation AWS se présente sur votre site à la date et à l'heure prévues. L'équipe fera rouler le rack jusqu'à l'emplacement identifié. Vous et votre électricien êtes responsables du raccordement électrique et de l'installation du rack.

Vous devez vous assurer que les installations électriques et toutes les modifications qui leur sont apportées sont effectuées par un électricien certifié conformément à tous les codes, lois et meilleures pratiques applicables. Vous devez obtenir une approbation écrite d'AWS avant d'apporter des modifications au matériel ou aux installations électriques de l'Outpost. Vous acceptez de fournir à AWS des documents attestant de la conformité et de la sécurité des modifications effectuées. AWS n'est pas responsable des risques créés par l'installation électrique ou le câblage électrique des installations de l'Outpost ou par les modifications. Vous ne devez apporter aucune autre modification au matériel Outposts.

Après quoi, l'équipe établit la connectivité réseau pour le rack Outposts via la liaison ascendante que vous fournissez, puis elle configure la capacité du rack.

L'installation est terminée une fois que vous avez pu constater que la capacité Amazon EC2 et Amazon EBS pour votre rack Outposts est disponible dans votre Compte AWS.

Commencez avec AWS Outposts

Commandez un Outpost pour démarrer. Après avoir installé votre équipement Outpost, lancez des instances Amazon EC2 et accédez à votre réseau sur site.

Tâches

- Création d'un Outpost et commande de capacité Outpost
- Lancez une instance sur votre rack Outpost

Création d'un Outpost et commande de capacité Outpost

Pour commencer à l'utiliser AWS Outposts, vous devez créer un avant-poste et commander une capacité d'avant-poste.

Prérequis

- Passez en revue les configurations disponibles pour vos racks Outposts.
- Un site Outpost est l'emplacement physique de votre équipement Outpost. Avant de commander de la capacité, vérifiez que votre site répond aux exigences. Pour plus d'informations, consultez Exigences du site pour le rack Outposts.
- Vous devez disposer d'un plan de Support aux AWS entreprises.
- Déterminez à qui Compte AWS appartiendra l'avant-poste. C'est à partir de ce compte que vous allez créer le site Outposts, créer l'Outpost et passer la commande. Surveillez l'e-mail associé à ce compte pour obtenir des informations provenant de AWS.

Tâches

- Étape 1 : Créer un site
- Étape 2 : Créer un Outpost
- Étape 3 : Passer la commande
- Étapes suivantes

Étape 1 : Créer un site

Créez un site pour spécifier l'adresse d'exploitation. L'adresse d'exploitation est l'emplacement physique de vos racks Outposts.

Prérequis

- Déterminez l'adresse d'exploitation.

Pour créer un site

1. Connectez-vous pour AWS utiliser le propriétaire Compte AWS de l'Outpost.
2. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.
3. Pour sélectionner le parent Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page.
4. Dans le panneau de navigation, choisissez Sites.
5. Choisissez Créer un site.
6. Pour Type de matériel pris en charge, sélectionnez Racks et serveurs.
7. Saisissez le nom, la description et l'adresse d'exploitation de votre site.
8. Pour Détails du site, fournissez les informations demandées à propos du site.
   - Poids maximum : poids maximum du rack que ce site peut supporter, en kilogrammes.
   - Puissance électrique : puissance électrique disponible à l'emplacement prévu du matériel pour le rack, en kVA.
   - Option d'alimentation : option d'alimentation que vous pouvez fournir pour le matériel.
   - Connecteur d'alimentation : connecteur d'alimentation qu' AWS doit pouvoir fournir pour les connexions au matériel.
   - Baisse de puissance : indiquez si l'alimentation électrique vient du haut ou du bas du rack.
   - Vitesse de liaison ascendante : vitesse de liaison ascendante que le rack doit prendre en charge pour la connexion à la région, en Gbit/s.
   - Nombre de liaisons ascendantes : nombre de liaisons ascendantes pour chaque appareil réseau Outpost que vous avez l'intention d'utiliser pour connecter le rack à votre réseau.
   - Type de fibre : type de fibre que vous prévoyez d'utiliser pour attacher le rack à votre réseau.
   - Norme optique : type de norme optique que vous prévoyez d'utiliser pour attacher le rack à votre réseau.

9. (Facultatif) Pour les notes sur le site, entrez toute autre information qui pourrait être utile AWS pour en savoir plus sur le site.
10. Lisez les exigences en matière d'installations, puis sélectionnez J'ai lu les exigences de l'installation.
11. Choisissez Créer un site.

Étape 2 : Créer un Outpost

Créez un Outpost pour vos racks. Vous pouvez spécifier cet Outpost au moment de passer la commande.

Prérequis

- Déterminez la zone de AWS disponibilité à associer à votre site.

Pour créer un Outpost

1. Dans le panneau de navigation, sélectionnez Outposts.
2. Choisissez Créer un Outpost.
3. Choisissez Racks.
4. Saisissez un nom et une description pour l'Outpost.
5. Choisissez une zone de disponibilité pour l'Outpost.
6. (Facultatif) Pour configurer une connectivité privée, sélectionnez Utiliser la connectivité privée. Choisissez un VPC et un sous-réseau dans la même Compte AWS zone de disponibilité que votre avant-poste. Pour plus d'informations, consultez the section called "Prérequis".
7. Pour ID du site, choisissez votre site.
8. Choisissez Créer un Outpost.

Étape 3 : Passer la commande

Passez une commande pour les racks Outposts dont vous avez besoin. Après avoir soumis la commande, un représentant AWS Outposts vous contactera.

> **Important**
>
> Sachant qu'il est impossible de modifier une commande déjà soumise, examinez attentivement tous les détails de la commande avant de la soumettre. Si vous devez modifier une commande, contactez votre responsable de AWS compte.

Prérequis

- Déterminez le mode de paiement de la commande. Vous pouvez payer la totalité à l'avance, une partie à l'avance ou rien à l'avance. Si vous choisissez de ne pas tout payer à l'avance, vous serez soumis à des frais mensuels sur une période de trois ans.

  Les prix incluent la livraison, l'installation, la maintenance des services d'infrastructure, ainsi que les mises à niveau et correctifs logiciels.
- Déterminez si l'adresse de livraison est différente de l'adresse d'exploitation que vous avez spécifiée pour le site.

Pour passer une commande

1. Dans le panneau de navigation, choisissez Commandes.
2. Choisissez Passer la commande.
3. Pour Type de matériel pris en charge, sélectionnez Racks.
4. Pour ajouter de la capacité, choisissez une configuration. Si les configurations disponibles ne répondent pas à vos besoins, vous pouvez plutôt nous contacter AWS pour demander une configuration de capacité personnalisée.
5. Choisissez Suivant.
6. Choisissez Utiliser un Outpost existant et sélectionnez votre Outpost.
7. Choisissez Suivant.
8. Sélectionnez une durée de contrat et une option de paiement.
9. Spécifiez l'adresse de livraison. Vous pouvez spécifier une nouvelle adresse ou sélectionner l'adresse d'exploitation du site. Si vous sélectionnez l'adresse d'exploitation, sachez que toute future modification de l'adresse d'exploitation du site ne se propagera pas aux commandes existantes. Si vous devez modifier l'adresse de livraison d'une commande existante, contactez votre responsable de AWS compte.

10. Choisissez Suivant.
11. Sur la page Vérifier et commander, vérifiez que vos informations sont correctes et modifiez-les si nécessaire. Vous ne pouvez pas modifier une commande déjà soumise.
12. Choisissez Passer la commande.

Étapes suivantes

Vous pouvez consulter le statut de votre commande à l'aide de la AWS Outposts console. L'état initial de votre commande est Commande reçue. Un AWS représentant vous contactera dans les trois jours ouvrables. Vous recevez un e-mail de confirmation lorsque le statut de votre commande passe à Traitement de la commande. Un AWS représentant peut vous contacter pour obtenir toute information supplémentaire AWS requise.

Si vous avez des questions concernant votre commande, contactez le AWS Support.

Pour exécuter la commande, AWS nous fixerons une date et une heure avec vous.

Vous recevez également une liste des éléments à vérifier ou à fournir avant l'installation. L'équipe AWS d'installation arrivera sur votre site à la date et à l'heure prévues. L'équipe place le rack à l'emplacement prévu et votre électricien alimente le rack. Après quoi, l'équipe établit la connectivité réseau pour le rack via la liaison ascendante que vous fournissez, puis elle configure la capacité du rack. L'installation est terminée lorsque vous confirmez que la capacité Amazon EC2 et Amazon EBS pour votre Outpost est disponible depuis votre compte. AWS

Lancez une instance sur votre rack Outpost

Dès lors que votre Outpost est installé et que la capacité de calcul et de stockage est prête à être utilisée, vous pouvez vous lancer en créant des ressources. Lancez des instances Amazon EC2 et créez des volumes Amazon EBS sur votre Outpost en utilisant un sous-réseau Outpost. Vous pouvez aussi créer des instantanés de volumes Amazon EBS sur votre Outpost. Pour plus d'informations applicables à Linux, consultez Instantanés Amazon EBS locaux sur AWS Outposts dans le Guide de l'utilisateur Amazon EC2 pour les instances Linux. Pour plus d'informations applicables à Windows, consultez Instantanés Amazon EBS locaux sur AWS Outposts dans le Guide de l'utilisateur Amazon EC2 pour les instances Windows.

Prérequis

Vous devez avoir un outpost installé sur votre site. Pour plus d'informations, consultez Création d'un Outpost et commande de capacité Outpost.

Tâches

Étape 1 : Créer un VPC

Vous pouvez étendre n'importe quel VPC de la AWS région à votre avant-poste. Ignorez cette étape si vous possédez déjà un VPC que vous pouvez utiliser.

Pour créer un VPC pour votre Outpost

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Choisissez la même région que celle du rack Outposts.
3. Dans le volet de navigation, choisissez Your VPC, puis Create VPC.
4. Choisissez VPC uniquement.
5. (Facultatif) Dans le champ Name tag, entrez le nom du VPC.
6. Pour le bloc d'adresse CIDR IPv4, choisissez la saisie manuelle d'adresse CIDR IPv4 et entrez la plage d'adresses IPv4 pour le VPC dans la zone de texte IPv4 CIDR.

   > **Note**
   >
   > Si vous souhaitez utiliser le routage VPC direct, spécifiez une plage d'adresses CIDR qui ne chevauche pas la plage d'adresses IP que vous utilisez dans votre réseau local.

7. Pour le bloc d'adresse CIDR IPv6, sélectionnez Aucun bloc d'adresse CIDR IPv6.
8. Pour Tenancy, choisissez Default.
9. (Facultatif) Pour ajouter une balise à votre VPC, choisissez Ajouter une balise, puis entrez une clé et une valeur.

10. Sélectionnez Create VPC (Créer un VPC).

Étape 2 : Création d'un sous-réseau et d'une table de routage personnalisée

Vous pouvez créer et ajouter un sous-réseau Outpost à n'importe quel VPC de la AWS région dans laquelle l'Outpost est hébergé. Lorsque vous le faites, le VPC inclut l'Outpost. Pour plus d'informations, consultez Composants du réseau.

> **Note**
>
> Si vous lancez une instance dans un sous-réseau Outpost qui a été partagée avec vous par un autre Compte AWS, passez directement à. Étape 5 : Lancer une instance sur l'Outpost

2a : Création d'un sous-réseau Outpost

Pour créer un sous-réseau Outpost

1. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.
2. Dans le panneau de navigation, choisissez Outposts.
3. Sélectionnez l'Outpost, puis choisissez Actions, Créer un sous-réseau. Vous êtes redirigé vers la console Amazon VPC où vous allez créer le sous-réseau. L'Outpost est sélectionné automatiquement ainsi que la zone de disponibilité dans laquelle il est hébergé.
4. Sélectionnez un VPC.
5. Dans les paramètres du sous-réseau, nommez éventuellement votre sous-réseau et spécifiez une plage d'adresses IP pour le sous-réseau.
6. Choisissez Create subnet (Créer un sous-réseau).
7. (Facultatif) Pour faciliter l'identification des sous-réseaux Outpost, activez la colonne Outpost ID sur la page Sous-réseaux. Pour activer la colonne, cliquez sur l'icône Préférences, sélectionnez Outpost ID, puis cliquez sur Confirmer.

2b : Création d'une table de routage personnalisée

Utilisez la procédure suivante pour créer une table de routage personnalisée avec une route à destination de la passerelle locale. Vous ne pouvez pas utiliser la même table de routage que celle des sous-réseaux de la zone de disponibilité.

Pour créer une table de routage personnalisée

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Tables de routage.
3. Choisissez Créer une table de routage.
4. (Facultatif) Pour Nom, entrez un nom pour votre table de routage.
5. Pour VPC, choisissez votre VPC.
6. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l'identification.
7. Choisissez Créer une table de routage.

2c : Associer le sous-réseau Outpost et la table de routage personnalisée

Pour appliquer des routes de table de routage à un sous-réseau spécifique, vous devez associer la table de routage au sous-réseau. Une table de routage peut être associée à plusieurs sous-réseaux. Toutefois, un sous-réseau peut être associé à une seule table de routage à la fois. Tout sous-réseau non associé explicitement à une table est associé implicitement à la table de routage principale par défaut.

Pour associer le sous-réseau Outpost et la table de routage personnalisée

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Route tables.
3. Sur l'onglet Associations de sous-réseau, choisissez Modifier les associations de sous-réseau.
4. Sélectionnez la case à cocher pour le sous-réseau à associer à la table de routage.
5. Choisissez Save associations (Enregistrer les associations).

Étape 3 : configurer la connectivité de la passerelle locale

La passerelle locale (LGW) permet la connectivité entre vos sous-réseaux Outpost et votre réseau local. Pour plus d'informations sur le LGW, consultez Passerelle locale.

Pour assurer la connectivité entre une instance du sous-réseau Outposts et votre réseau local, vous devez effectuer les tâches suivantes.

3a. Création d'une table de routage de passerelle locale personnalisée

Vous pouvez créer une table de routage personnalisée pour votre passerelle locale (LGW) à l'aide de la AWS Outposts console.

Pour créer une table de routage LGW personnalisée à l'aide de la console

1. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.
2. Pour modifier le Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page.
3. Dans le panneau de navigation, choisissez Table de routage de passerelle locale.
4. Choisissez Créer une table de routage de passerelle locale.
5. (Facultatif) Dans Nom, entrez le nom de votre table de routage LGW.
6. Pour Passerelle locale, choisissez votre passerelle locale.
7. Pour Mode, choisissez un mode de communication avec votre réseau sur site.

   - Choisissez Routage VPC direct pour utiliser l'adresse IP privée d'une instance.
   - Choisissez CoIP pour utiliser l'adresse IP client.
     - (Facultatif) Ajoutez ou supprimez des groupes CoIP et des blocs CIDR supplémentaires.

       [Ajout d'un groupe CoIP] Choisissez Ajouter un nouveau groupe et procédez comme suit :

       - Dans Nom, saisissez un nom pour votre groupe CoIP.
       - Dans CIDR, saisissez un bloc CIDR d'adresses IP clients.
     - [Ajout de blocs CIDR] Choisissez Ajouter un nouveau CIDR et entrez une plage d'adresses IP clients.
     - [Suppression d'un groupe CoIP ou d'un bloc CIDR supplémentaire] Choisissez Éliminer à droite d'un bloc CIDR ou en dessous du groupe CoIP.

       Vous pouvez spécifier jusqu'à 10 groupes CoIP et 100 blocs CIDR.

8. (Facultatif) Ajoutez ou supprimez une balise.

   [Ajouter une balise] Choisissez Ajouter une nouvelle balise et procédez comme suit :

   - Pour Clé, saisissez le nom de la clé.
   - Pour Value (Valeur), saisissez la valeur de clé.

   [Suppression d'une balise] Choisissez Éliminer à la droite de la clé et de la valeur de la balise.
9. Choisissez Créer une table de routage de passerelle locale.

3b : Associez le VPC à la table de routage LGW personnalisée

Vous devez associer les VPC à votre table de routage LGW. Ils ne sont pas associés par défaut.

Utilisez la procédure suivante pour associer un VPC à une table de routage LGW.

Vous pouvez éventuellement baliser votre association pour l'identifier ou la catégoriser en fonction des besoins de votre organisation.

AWS Outposts console

Pour associer un VPC à la table de routage LGW personnalisée

1. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.
2. Pour modifier le Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page.
3. Dans le panneau de navigation, choisissez Tables de routage de passerelle locale.
4. Sélectionnez la table de routage, puis choisissez Actions, Associer un VPC.
5. Dans ID du VPC, sélectionnez le VPC à associer à la table de routage de passerelle locale.
6. (Facultatif) Ajoutez ou supprimez une balise.

   Pour ajouter une balise, choisissez Ajouter une balise, puis procédez comme suit :

   - Pour Clé, saisissez le nom de la clé.
   - Pour Valeur, saisissez la valeur de clé.

   Pour supprimer une balise, choisissez Éliminer à droite de la clé et de la valeur de la balise.

7. Choisissez Associate VPC (Associer un VPC).

AWS CLI

Pour associer un VPC à la table de routage LGW personnalisée

Utilisez la table-vpc-association commande create-local-gateway-route-.

Exemple

```
aws ec2 create-local-gateway-route-table-vpc-association \
    --local-gateway-route-table-id lgw-rtb-059615ef7dEXAMPLE \
    --vpc-id vpc-07ef66ac71EXAMPLE
```

Sortie

```
{
    "LocalGatewayRouteTableVpcAssociation": {
        "LocalGatewayRouteTableVpcAssociationId": "lgw-vpc-assoc-0ee765bcc8EXAMPLE",
        "LocalGatewayRouteTableId": "lgw-rtb-059615ef7dEXAMPLE",
        "LocalGatewayId": "lgw-09b493aa7cEXAMPLE",
        "VpcId": "vpc-07ef66ac71EXAMPLE",
        "State": "associated"
    }
}
```

3c : Ajouter une entrée de route dans la table de routage du sous-réseau Outpost

Ajoutez une entrée d'itinéraire dans la table de routage du sous-réseau Outpost pour activer le trafic entre les sous-réseaux Outpost et LGW.

Les sous-réseaux Outpost d'un VPC, qui est associé aux tables de routage Outpost LGW, peuvent avoir un type de cible supplémentaire, à savoir un ID de passerelle Outpost Local pour leurs tables de routage. Imaginons le cas où vous souhaitez acheminer le trafic avec une adresse de destination 172.16.100.0/24 vers le réseau du client via le LGW. Pour ce faire, modifiez la table de routage du sous-réseau Outpost et ajoutez l'itinéraire suivant avec le réseau de destination et une cible du LGW (). `lgw-xxxx`

Destination	Cible
172,16.100,0/24	`lgw-id`

Pour ajouter une entrée de route en **`lgw-id`** tant que cible dans la table de routage du sous-réseau Outpost :

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Tables de routage, puis sélectionnez la table de routage que vous avez créée dans2b : Création d'une table de routage personnalisée.
3. Choisissez Actions, puis Modifier les itinéraires.
4. Pour ajouter une route, choisissez Add route (Ajouter une route).
5. Pour Destination, entrez le bloc CIDR de destination sur le réseau du client.
6. Pour Target, choisissez Outpost local Gateway ID.
7. Sélectionnez Enregistrer les modifications.

3d : Associez la table de routage LGW personnalisée aux groupes LGW VIF

Les groupes VIF sont des regroupements logiques d'interfaces virtuelles (VIF). Associez la table de routage de la passerelle locale au groupe VIF.

Pour associer la table de routage LGW personnalisée aux groupes LGW VIF

1. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.
2. Pour modifier le Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page.
3. Dans le panneau de navigation, choisissez Tables de routage de passerelle locale.
4. Choisissez la table de routage.
5. Choisissez l'onglet Association de groupe VIF dans le volet de détails, puis choisissez Modifier l'association de groupe VIF.
6. Pour les paramètres du groupe VIF, sélectionnez Associer un groupe VIF, puis choisissez un groupe VIF.
7. Sélectionnez Enregistrer les modifications.

3e : Ajouter une entrée de route dans la table de routage LGW

Modifiez la table de routage de la passerelle locale pour ajouter une route statique dont le groupe VIF est la cible et la plage d'adresses CIDR de votre sous-réseau local (ou 0.0.0.0/0) comme destination.

Destination	Cible
172,16.100,0/24	`VIF-Group-ID`

Pour ajouter une entrée de route dans la table de routage LGW

1. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.
2. Dans le panneau de navigation, choisissez Table de routage de passerelle locale.
3. Sélectionnez la table de routage de la passerelle locale, puis choisissez Actions, Modifier les itinéraires.
4. Choisissez Ajouter une route.
5. Pour Destination, entrez le bloc CIDR de destination, une adresse IP unique ou l'ID d'une liste de préfixes.
6. Pour Cible, sélectionnez l'ID de la passerelle locale.
7. Choisissez Save routes (Enregistrer les acheminements).

3f : (Facultatif) Attribuez une adresse IP appartenant au client à l'instance

Si vous avez configuré vos Outposts dans le 3a. Création d'une table de routage de passerelle locale personnalisée pour utiliser un pool d'adresses IP (CoIP) appartenant au client, vous devez allouer une adresse IP élastique à partir du pool d'adresses CoIP et associer l'adresse IP élastique à l'instance. Pour plus d'informations sur les pools CoIP, consultez Adresses IP clients.

Si vous avez configuré vos Outposts pour utiliser le routage VPC direct (DVR), ignorez cette étape.

Amazon VPC console

Pour attribuer une adresse CoIP à l'instance

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Elastic IPs.

3. Choisissez Allocate Elastic IP address (Allouer l'adresse IP Elastic).
4. Pour Groupe de bordures réseau, sélectionnez l'emplacement à partir duquel l'adresse IP est annoncée.
5. Pour Pool d'adresses IPv4 publiques, choisissez Pool d'adresses IPv4 appartenant au client.
6. Pour Pool d'adresses IPv4 appartenant au client, sélectionnez le pool que vous avez configuré.
7. Choisissez Allouer.
8. Sélectionnez l'adresse IP Elastic, puis choisissez Actions, Associer l'adresse IP Elastic.
9. Sélectionnez l'instance dans Instance, puis choisissez Associer.

AWS CLI

Pour attribuer une adresse CoIP à l'instance

1. Utilisez la describe-coip-poolscommande pour récupérer des informations sur les pools d'adresses appartenant à vos clients.

```
aws ec2 describe-coip-pools
```

Voici un exemple de sortie.

```
{
    "CoipPools": [
        {
            "PoolId": "ipv4pool-coip-0abcdef0123456789",
            "PoolCidrs":  [
                "192.168.0.0/16"
            ],
            "LocalGatewayRouteTableId": "lgw-rtb-0abcdef0123456789"
        }
    ]
}
```

2. Utilisez la commande allocate-address pour allouer une adresse IP Elastic. Utilisez l'ID de pool renvoyé à l'étape précédente.

```
aws ec2 allocate-address--address 192.0.2.128 --customer-owned-ipv4-
pool ipv4pool-coip-0abcdef0123456789
```

Voici un exemple de sortie.

```
{
    "CustomerOwnedIp": "192.0.2.128",
    "AllocationId": "eipalloc-02463d08ceEXAMPLE",
    "CustomerOwnedIpv4Pool": "ipv4pool-coip-0abcdef0123456789",
}
```

3. Utilisez la commande associate-address pour associer l'adresse IP Elastic à l'instance Outpost. Utilisez l'ID d'allocation renvoyé à l'étape précédente.

```
aws ec2 associate-address --allocation-id eipalloc-02463d08ceEXAMPLE --network-
interface-id eni-1a2b3c4d
```

Voici un exemple de sortie.

```
{
    "AssociationId": "eipassoc-02463d08ceEXAMPLE",
}
```

Pools d'adresses IP appartenant à un client en partage

Si vous souhaitez utiliser un pool d'adresses IP appartenant à un client en partage, le pool doit être partagé avant de commencer la configuration. Pour savoir comment partager une adresse IPv4 appartenant à un client, consultez Partage de vos ressources AWS dans le Guide de l'utilisateur AWS RAM .

Étape 4 : Configuration du réseau local

L'Outpost établit un peering BGP externe entre chaque périphérique réseau (OND) et un périphérique réseau local du client (CND) pour envoyer et recevoir du trafic de votre réseau sur site vers les Outposts. Pour plus d'informations, consultez la section Connectivité BGP de la passerelle locale.

Pour envoyer et recevoir du trafic depuis votre réseau local vers l'Outpost, assurez-vous que :

- Sur les appareils réseau de vos clients, la session BGP sur le VLAN de la passerelle locale est active depuis vos périphériques réseau.
- Pour le trafic allant des Outposts sur site, assurez-vous de recevoir dans votre CND les publicités BGP provenant d'Outposts. Ces publicités BGP contiennent les itinéraires que votre réseau local

doit utiliser pour acheminer le trafic depuis le réseau local vers Outpost. Assurez-vous donc que votre réseau dispose du bon routage entre les Outposts et les ressources sur site.

- Pour le trafic allant des Outposts vers le réseau local, assurez-vous que vos CND envoient les publicités de routage BGP des sous-réseaux du réseau local aux Outposts (ou 0.0.0.0/0). Vous pouvez également annoncer un itinéraire par défaut (par exemple 0.0.0.0/0) vers les Outposts. Les sous-réseaux locaux annoncés par les CND doivent avoir une plage d'adresses CIDR égale ou incluse dans la plage d'adresses CIDR que vous avez configurée. 3e : Ajouter une entrée de route dans la table de routage LGW

Exemple : publicités BGP en mode Direct VPC

Imaginons le scénario dans lequel vous avez un Outpost, configuré en mode VPC direct, avec deux périphériques réseau en rack Outposts connectés par une passerelle locale VLAN à deux périphériques réseau locaux du client. Les paramètres suivants sont configurés :

- Un VPC avec un bloc CIDR 10.0.0.0/16.
- Un sous-réseau Outpost dans le VPC avec un bloc CIDR 10.0.3.0/24.
- Un sous-réseau du réseau local avec un bloc CIDR 172.16.100.0/24
- Outposts utilise l'adresse IP privée des instances du sous-réseau Outpost, par exemple 10.0.3.0/24, pour communiquer avec votre réseau local.

Dans ce scénario, l'itinéraire annoncé par :

- La passerelle locale vers les appareils de vos clients est 10.0.3.0/24.
- Les appareils de vos clients accédant à la passerelle locale d'Outpost sont 172.16.100.0/24.

Par conséquent, la passerelle locale enverra le trafic sortant avec le réseau de destination 172.16.100.0/24 vers les appareils de vos clients. Assurez-vous que la configuration de routage de votre réseau est correcte pour acheminer le trafic vers l'hôte de destination au sein de votre réseau.

Pour connaître les commandes et la configuration spécifiques requises pour vérifier l'état des sessions BGP et les itinéraires annoncés au sein de ces sessions, consultez la documentation de votre fournisseur de réseau. Pour le dépannage, consultez la liste de contrôle de dépannage du réseau en AWS Outposts rack.

Exemple : publicités BGP en mode CoIP

Imaginons le scénario dans lequel vous avez un Outpost avec deux périphériques réseau en rack Outposts connectés par une passerelle locale VLAN à deux périphériques réseau locaux du client. Les paramètres suivants sont configurés :

- Un VPC avec un bloc CIDR 10.0.0.0/16.
- Un sous-réseau dans le VPC avec un bloc CIDR 10.0.3.0/24.
- Un groupe d'adresses IP clients (10.1.0.0/26).
- Une association d'adresses IP Elastic qui associe 10.0.3.112 à 10.1.0.2.
- Un sous-réseau du réseau local avec un bloc CIDR 172.16.100.0/24
- La communication entre votre Outpost et le réseau sur site utilisera les adresses IP Elastic CoIP pour résoudre les instances de l'Outpost, et la plage CIDR VPC n'est pas utilisée.

Dans ce scénario, l'itinéraire annoncé par :

- La passerelle locale vers les appareils de vos clients est 10.1.0.0/26.
- Les appareils de vos clients accédant à la passerelle locale d'Outpost sont 172.16.100.0/24.

Par conséquent, la passerelle locale enverra le trafic sortant avec le réseau de destination 172.16.100.0/24 vers les appareils de vos clients. Assurez-vous que votre réseau dispose de la bonne configuration de routage pour acheminer le trafic vers l'hôte de destination au sein de votre réseau.

Pour connaître les commandes et la configuration spécifiques requises pour vérifier l'état des sessions BGP et les itinéraires annoncés au sein de ces sessions, consultez la documentation de votre fournisseur de réseau. Pour le dépannage, consultez la liste de contrôle de dépannage du réseau en AWS Outposts rack.

Étape 5 : Lancer une instance sur l'Outpost

Vous pouvez lancer des instances EC2 dans le sous-réseau Outpost que vous avez créé ou dans un sous-réseau Outpost qui a été partagé avec vous. Les groupes de sécurité contrôlent le trafic entrant et sortant du VPC pour les instances d'un sous-réseau Outpost, comme ils le font pour les instances d'un sous-réseau de zone de disponibilité. Pour vous connecter à une instance EC2 d'un sous-réseau Outpost, vous pouvez spécifier une paire de clés au moment de lancer l'instance, de la même manière que vous le faites pour les instances d'un sous-réseau de zone de disponibilité.

Considérations

- Vous pouvez créer des groupes de placement pour influencer la façon dont Amazon EC2 doit placer les groupes d'instances interdépendantes sur le matériel Outposts. Vous pouvez choisir la stratégie de groupe de placement qui répond le mieux aux besoins de votre charge de travail.
- Si votre Outpost a été configuré pour utiliser un pool d'adresses IP appartenant au client (CoIP), vous devez attribuer une adresse IP appartenant au client à toutes les instances que vous lancez.

Pour lancer des instances dans votre sous-réseau Outpost

1. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.
2. Dans le panneau de navigation, choisissez Outposts.
3. Sélectionnez l'Outpost, puis choisissez Actions, Afficher les détails.
4. Sur la page Récapitulatif de l'Outpost, choisissez Lancer une instance. Vous êtes redirigé vers l'assistant de lancement d'instances dans la console Amazon EC2. Nous sélectionnons le sous-réseau Outpost pour vous et nous vous indiquons uniquement les types d'instances pris en charge par votre rack Outposts.
5. Choisissez un type d'instance compatible avec votre rack Outposts. Notez que les instances qui apparaissent grisées ne sont pas disponibles pour votre Outpost.
6. (Facultatif) Pour lancer les instances dans un groupe de placement, développez Détails avancés et faites défiler l'écran jusqu'à Groupe de placement. Vous pouvez soit sélectionner un groupe de placement existant, soit en créer un nouveau.
7. Suivez les étapes de l'assistant pour lancer l'instance dans votre sous-réseau Outpost. Pour plus d'informations, consultez les rubriques suivantes dans le Guide de l'utilisateur Amazon EC2 :
   - Linux — Lancez une instance à l'aide du nouvel assistant de lancement d'instance
   - Windows — Lancez une instance à l'aide du nouvel assistant de lancement d'instance

> **Note**
>
> Si vous créez un volume Amazon EBS, vous devez utiliser le type de volume gp2, sinon l'assistant échouera.

Étape 6 : tester la connectivité

Vous pouvez tester la connectivité en utilisant les cas d'utilisation appropriés.

Test de la connectivité entre votre réseau local et l'Outpost

Depuis un ordinateur de votre réseau local, exécutez la `ping` commande sur l'adresse IP privée de l'instance Outpost.

```
ping 10.0.3.128
```

Voici un exemple de sortie.

```
Pinging 10.0.3.128

Reply from 10.0.3.128:  bytes=32 time=<1ms TTL=128
Reply from 10.0.3.128:  bytes=32 time=<1ms TTL=128
Reply from 10.0.3.128:  bytes=32 time=<1ms TTL=128

Ping statistics for 10.0.3.128
Packets:  Sent = 3,  Received = 3,  Lost = 0 (0% lost)

Approximate round trip time in milliseconds
Minimum = 0ms,  Maximum = 0ms,  Average = 0ms
```

Test de la connectivité entre une instance Outpost et votre réseau local

Selon votre système d'exploitation, utilisez ssh ou rdp pour vous connecter à l'adresse IP privée de votre instance Outpost. Pour plus d'informations sur la connexion à une instance Linux, consultez Connexion à votre instance Linux dans le Amazon EC2 Guide de l'utilisateur pour les instances Linux. Pour en savoir plus sur la connexion à une instance Windows, consultez Connexion à votre instance Windows dans le Guide de l'utilisateur Amazon EC2 pour les instances Windows.

Une fois que l'instance s'exécute, exécutez la commande `ping` sur l'adresse IP d'un ordinateur de votre réseau local. Dans l'exemple suivant, l'adresse IP est 172.16.0.130.

```
ping 172.16.0.130
```

Voici un exemple de sortie.

```
Pinging 172.16.0.130
```

```
Reply from 172.16.0.130:  bytes=32 time=<1ms TTL=128
Reply from 172.16.0.130:  bytes=32 time=<1ms TTL=128
Reply from 172.16.0.130:  bytes=32 time=<1ms TTL=128

Ping statistics for 172.16.0.130
Packets:  Sent = 3,  Received = 3,  Lost = 0 (0% lost)

Approximate round trip time in milliseconds
Minimum = 0ms,  Maximum = 0ms,  Average = 0ms
```

Testez la connectivité entre la AWS région et l'avant-poste

Lancez une instance dans le sous-réseau de la AWS région. Par exemple, utilisez la commande run-instances.

```
aws ec2 run-instances \
    --image-id ami-abcdefghi1234567898 \
    --instance-type c5.large \
    --key-name MyKeyPair \
    --security-group-ids sg-1a2b3c4d123456787 \
    --subnet-id subnet-6e7f829e123445678
```

Une fois que l'instance s'exécute, effectuez les opérations suivantes :

1. Obtenez l'adresse IP privée de l'instance dans la AWS région. Ces informations sont disponibles dans la console Amazon EC2 sur la page de détails de l'instance.
2. Selon votre système d'exploitation, utilisez ssh ou rdp pour vous connecter à l'adresse IP privée de votre instance Outpost.
3. Exécutez la ping commande depuis votre instance Outpost, en spécifiant l'adresse IP de l'instance dans la AWS région.

   ```
   ping 10.0.1.5
   ```

   Voici un exemple de sortie.

   ```
   Pinging 10.0.1.5

   Reply from 10.0.1.5:  bytes=32 time=<1ms TTL=128
   Reply from 10.0.1.5:  bytes=32 time=<1ms TTL=128
   ```

```
Reply from 10.0.1.5:  bytes=32 time=<1ms TTL=128

Ping statistics for 10.0.1.5
Packets:  Sent = 3,  Received = 3,  Lost = 0 (0% lost)

Approximate round trip time in milliseconds
Minimum = 0ms,  Maximum = 0ms,  Average = 0ms
```

Exemples de connectivité d'adresses IP appartenant au client

Test de la connectivité entre votre réseau local et l'Outpost

À partir d'un ordinateur de votre réseau local, exécutez la commande `ping` sur l'adresse IP appartenant au client de l'instance Outpost.

```
ping 172.16.0.128
```

Voici un exemple de sortie.

```
Pinging 172.16.0.128

Reply from 172.16.0.128:  bytes=32 time=<1ms TTL=128
Reply from 172.16.0.128:  bytes=32 time=<1ms TTL=128
Reply from 172.16.0.128:  bytes=32 time=<1ms TTL=128

Ping statistics for 172.16.0.128
Packets:  Sent = 3,  Received = 3,  Lost = 0 (0% lost)

Approximate round trip time in milliseconds
Minimum = 0ms,  Maximum = 0ms,  Average = 0ms
```

Test de la connectivité entre une instance Outpost et votre réseau local

Selon votre système d'exploitation, utilisez ssh ou rdp pour vous connecter à l'adresse IP privée de votre instance Outpost. Pour plus d'informations sur la connexion à une instance Linux, consultez Connexion à votre instance Linux dans le Amazon EC2 Guide de l'utilisateur pour les instances Linux. Pour en savoir plus sur la connexion à une instance Windows, consultez Connexion à votre instance Windows dans le Guide de l'utilisateur Amazon EC2 pour les instances Windows.

Une fois que l'instance Outpost s'exécute, exécutez la commande `ping` sur l'adresse IP d'un ordinateur de votre réseau local.

```
ping 172.16.0.130
```

Voici un exemple de sortie.

```
Pinging 172.16.0.130

Reply from 172.16.0.130:  bytes=32 time=<1ms TTL=128
Reply from 172.16.0.130:  bytes=32 time=<1ms TTL=128
Reply from 172.16.0.130:  bytes=32 time=<1ms TTL=128

Ping statistics for 172.16.0.130
Packets:  Sent = 3,  Received = 3,  Lost = 0 (0% lost)

Approximate round trip time in milliseconds
Minimum = 0ms,  Maximum = 0ms,  Average = 0ms
```

Testez la connectivité entre la AWS région et l'avant-poste

Lancez une instance dans le sous-réseau de la AWS région. Par exemple, utilisez la commande run-instances.

```
aws ec2 run-instances \
    --image-id ami-abcdefghi1234567898 \
    --instance-type c5.large \
    --key-name MyKeyPair \
    --security-group-ids sg-1a2b3c4d123456787 \
    --subnet-id subnet-6e7f829e123445678
```

Une fois que l'instance s'exécute, effectuez les opérations suivantes :

1. Obtenez l'adresse IP privée de l'instance AWS Region, par exemple 10.0.0.5. Ces informations sont disponibles dans la console Amazon EC2 sur la page de détails de l'instance.
2. Selon votre système d'exploitation, utilisez ssh ou rdp pour vous connecter à l'adresse IP privée de votre instance Outpost.
3. Exécutez la `ping` commande depuis votre instance Outpost vers l'adresse IP de l'instance AWS Region.

   ```
   ping 10.0.0.5
   ```

   Voici un exemple de sortie.

```
Pinging 10.0.0.5

Reply from 10.0.0.5:  bytes=32 time=<1ms TTL=128
Reply from 10.0.0.5:  bytes=32 time=<1ms TTL=128
Reply from 10.0.0.5:  bytes=32 time=<1ms TTL=128

Ping statistics for 10.0.0.5
Packets:  Sent = 3,  Received = 3,  Lost = 0 (0% lost)

Approximate round trip time in milliseconds
Minimum = 0ms,  Maximum = 0ms,  Average = 0ms
```

Connectivité AWS Outposts avec les régions AWS

AWS Outposts prend en charge la connectivité de réseau étendu (WAN) via la connexion de la liaison de service.

Table des matières

Connectivité via les liaisons de service

La liaison de service est une connexion nécessaire entre vos Outposts et la région AWS de votre choix (ou région d'origine) et permet la gestion des Outposts et l'échange de trafic vers et en provenance de la région AWS. La liaison de service utilise un jeu chiffré de connexions VPN pour communiquer avec la région d'origine.

Pour configurer la connectivité de la liaison de service, vous ou AWS devez configurer la liaison de service physique, le réseau local virtuel (VLAN) et la connectivité de la couche réseau avec les appareils de votre réseau local pendant le provisionnement de l'Outpost. Pour plus d'informations, consultez Connectivité de réseau local pour les racks et Exigences relatives au site pour un rack Outposts.

Pour la connectivité du réseau étendu (WAN) avec la région AWS, AWS Outposts peut établir des connexions VPN de liaison de service via la connectivité publique de la région AWS. Pour cela, les Outposts doivent avoir accès aux plages d'adresses IP publiques de la région, que ce soit en empruntant l'Internet public ou des interfaces virtuelles publiques AWS Direct Connect. Pour connaître les plages d'adresses IP actuelles, consultez Plages d'adresses IP AWS dans le Guide de l'utilisateur Amazon VPC. Cette connectivité peut être activée en configurant des routes spécifiques ou par défaut (0.0.0.0/0) dans le chemin de la couche réseau de la liaison de service. Pour plus d'informations, consultez Connectivité BGP pour la liaison de service et Annonce et plage d'adresses IP de sous-réseau d'infrastructure de liaison de service.

Vous pouvez également sélectionner l'option de connectivité privé pour votre Outpost. Pour plus d'informations, consultez Connectivité privée de liaison de service utilisant un VPC.

Une fois la connexion de la liaison de service établie, votre Outpost devient opérationnel et est géré par AWS. La liaison de service est utilisée pour le trafic suivant :

- Trafic de VPC client entre l'Outpost et les VPC associés.
- Trafic de gestion des Outposts, tel que la gestion des ressources, la surveillance des ressources et les mises à jour de microprogramme et de logiciel.

Exigences relatives à l'unité de transmission maximale (MTU) pour les liaisons de service

L'unité de transmission maximale (MTU) d'une connexion réseau correspond à la taille, en octets, du paquet le plus volumineux susceptible d'être transmis via la connexion. Le réseau doit prendre en charge une MTU de 1 500 octets entre l'Outpost et les points de terminaison des liaisons de service dans la région parent. AWS Pour plus d'informations sur le MTU requis entre une instance de l'Outpost et une instance de la AWS région via le lien de service, consultez la section Unité de transmission maximale (MTU) réseau pour votre instance Amazon EC2 dans le guide de l'utilisateur Amazon EC2 pour les instances Linux.

Recommandations concernant la bande passante de la liaison de service

Pour une expérience et une résilience optimales, AWS vous recommande d'utiliser une connectivité redondante d'au moins 500 Mbits/s (1 Gbit/s est préférable) pour la connexion de la liaison de service avec la région AWS. Vous pouvez utiliser AWS Direct Connect ou une connexion Internet pour la liaison de service. 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 AWS des services tels qu'Amazon EKS, Amazon EMR et aux métriques. CloudWatch

Les besoins en bande passante de la liaison de service Outposts varient en fonction des caractéristiques suivantes :

- Nombre de racks AWS Outposts et configurations de capacité
- Caractéristiques de la charge de travail (taille d'AMI, élasticité de l'application, besoins en vitesse en rafale, trafic Amazon VPC vers la région, etc.)

Pour recevoir une recommandation personnalisée qui tienne compte de vos besoins en bande passante de la liaison de service, contactez votre représentant commercial AWS ou votre partenaire APN.

Pare-feu et liaison de service

Cette section traite des configurations de pare-feu et de la connexion de la liaison de service.

Dans la configuration présentée dans le diagramme suivant, le VPC Amazon s'étend de la région AWS à l'Outpost. La connexion de la liaison de service utilise une interface virtuelle publique AWS Direct Connect. Le trafic suivant transite par la liaison de service et la connexion AWS Direct Connect :

- Trafic de gestion à destination de l'Outpost via la liaison de service
- Trafic entre l'Outpost et les VPC associés

Si vous utilisez un pare-feu avec état avec votre connexion Internet afin de limiter la connectivité de l'Internet public vers le VLAN de la liaison de service, vous pouvez bloquer toutes les connexions entrantes initiées depuis Internet. En effet, le VPN de la liaison de service s'initie uniquement de l'Outpost vers la région, et non de la région vers l'Outpost.

Si vous utilisez un pare-feu pour limiter la connectivité à partir du VLAN de la liaison de service, vous pouvez bloquer toutes les connexions entrantes. Vous devez autoriser les connexions sortantes retournant vers l'Outpost depuis la région AWS selon les indications du tableau ci-dessous. S'il s'agit d'un pare-feu avec état, les connexions sortantes autorisées en provenance de l'Outpost, c'est-à-dire initiées depuis l'Outpost, doivent être autorisées à revenir en entrée.

Protocole	Port source	Adresse source	Port de destination	Adresse de destination
UDP	443	Liaison de service AWS Outposts /26	443	Routes publiques de la région AWS Outposts
TCP	1025-65535	Liaison de service AWS Outposts /26	443	Routes publiques de la région AWS Outposts

> **Note**
>
> Les instances contenues dans un Outpost ne peuvent pas utiliser la liaison de service pour communiquer avec les instances d'un autre Outpost. Pour permettre la communication entre les Outposts, optez pour un routage via la passerelle locale ou l'interface de réseau local. Les racks AWS Outposts ont également été conçus avec des équipements d'alimentation et de réseau redondants, notamment des composants de passerelle locale. Pour plus d'informations, consultez Résilience dans AWS Outposts.

Connectivité privée de la liaison de service avec VPC

Vous pouvez sélectionner l'option de connectivité privée dans la console au moment de créer votre Outpost. Dans ce cas, une connexion VPN de liaison de service est établie après l'installation de l'Outpost en utilisant un VPC et le sous-réseau que vous spécifiez. Ainsi, vous bénéficiez d'une connectivité privée grâce au VPC et d'une exposition à l'Internet public réduite au minimum.

Prérequis

Vous devez remplir les prérequis suivants avant de pouvoir configurer la connectivité privée pour votre Outpost :

- Vous devez configurer les autorisations d'une entité IAM (utilisateur ou rôle) pour permettre à l'utilisateur ou au rôle de créer le rôle lié à un service pour la connectivité privée. L'entité IAM a besoin d'une autorisation pour accéder aux actions suivantes :
  - `iam:CreateServiceLinkedRole` sur `arn:aws:iam::*:role/aws-service-role/outposts.amazonaws.com/AWSServiceRoleForOutposts*`
  - `iam:PutRolePolicy` sur `arn:aws:iam::*:role/aws-service-role/outposts.amazonaws.com/AWSServiceRoleForOutposts*`
  - `ec2:DescribeVpcs`
  - `ec2:DescribeSubnets`

  Pour plus d'informations, consultez Gestion des identités et des accès (IAM) pour AWS Outposts et Utilisation des rôles liés aux services pour AWS Outposts.
- Dans le même compte AWS et dans la même zone de disponibilité que votre Outpost, créez un VPC à la seule fin de la connectivité privée de l'Outpost avec un sous-réseau /25 ou plus grand qui ne soit pas en conflit avec 10.1.0.0/16. Par exemple, vous pouvez utiliser 10.2.0.0/16.

- Créez une connexion AWS Direct Connect, une interface virtuelle privée et une passerelle privée virtuelle pour permettre à votre Outpost sur site d'accéder au VPC. Si la connexion AWS Direct Connect se trouve dans un compte AWS différent de celui de votre VPC, consultez Association d'une passerelle privée virtuelle entre comptes dans le Guide de l'utilisateur AWS Direct Connect.
- Annoncez le CIDR du sous-réseau à votre réseau sur site. Pour ce faire, vous pouvez utiliser AWS Direct Connect. Pour plus d'informations, consultez Interfaces virtuelles AWS Direct Connect et Utilisation de passerelles AWS Direct Connect dans le Guide de l'utilisateur AWS Direct Connect.

Vous pouvez sélectionner l'option de connectivité privée au moment de créer votre Outpost dans la console AWS Outposts. Pour obtenir des instructions, veuillez consulter Création d'un Outpost et commande de capacité Outpost.

> **Note**
>
> Pour sélectionner l'option de connectivité privée lorsque votre Outpost a le statut EN ATTENTE, choisissez Outposts dans la console, puis sélectionnez votre Outpost. Choisissez Actions, Ajouter une connectivité privée, puis suivez les étapes.

Une fois que vous avez sélectionné l'option de connectivité privée pour votre Outpost, AWS Outposts crée automatiquement un rôle lié à un service dans votre compte qui permet à celui-ci d'effectuer les tâches suivantes en votre nom :

- Créer des interfaces réseau dans le sous-réseau et le VPC que vous spécifiez, et créer un groupe de sécurité pour les interfaces réseau.
- Accorder au service AWS Outposts l'autorisation d'attacher les interfaces réseau à une instance de point de terminaison de la liaison de service dans le compte.
- Attacher les interfaces réseau aux instances de point de terminaison de la liaison de service à partir du compte.

Pour de plus amples informations sur le rôle lié à un service, veuillez consulter Utilisation des rôles liés aux services pour AWS Outposts.

> **Important**
>
> Une fois votre Outpost installé, vérifiez la connectivité entre l'Outpost et les adresses IP privées de votre sous-réseau.

Connexions Internet redondantes

Lorsque vous établissez une connectivité entre votre Outpost et la région AWS, nous vous recommandons de créer plusieurs connexions afin d'accroître la disponibilité et la résilience. Pour plus d'informations, consultez Recommandations relatives à la résilience AWS Direct Connect.

Si vous avez besoin d'une connectivité vers l'Internet public, vous pouvez utiliser des connexions Internet redondantes et plusieurs fournisseurs Internet, comme vous le feriez pour vos charges de travail sur site existantes.

Outposts et sites

Gérez les Outposts et les sites pour. AWS Outposts

Vous pouvez baliser les Outposts et les sites pour vous aider à les identifier ou à les catégoriser en fonction des besoins de votre organisation. Pour plus d'informations sur le balisage, consultez la section AWS Ressources relatives au balisage dans le Références générales AWS Guide.

Rubriques

Gestion des Outposts

AWS Outposts inclut des ressources matérielles et virtuelles connues sous le nom d'Outposts. Cette section vous explique comment créer et gérer les Outposts, notamment comment changer leur nom et comment ajouter ou afficher des détails ou des balises.

Pour créer un Outpost

1. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.
2. Pour modifier le Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page.
3. Dans le panneau de navigation, choisissez Outposts.
4. Choisissez Créer un Outpost.
5. Choisissez un type de matériel pour cet Outpost.
6. Saisissez un nom et une description pour l'Outpost.
7. Choisissez une zone de disponibilité pour l'Outpost.
8. (Facultatif) Choisissez Option de connectivité privée. Pour le VPC et le sous-réseau, sélectionnez un VPC et un sous-réseau dans le même AWS compte et la même zone de disponibilité que votre avant-poste.

> **Note**
>
> Si vous avez besoin d'annuler la connectivité privée pour votre Outpost, vous devez contacter AWS Enterprise Support.

9. À partir d'ID du site, effectuez l'une des opérations suivantes :

   - Pour sélectionner un site existant, choisissez-le.
   - Pour créer un site, choisissez Créer un site, cliquez sur Suivant, puis saisissez les informations relatives à votre site dans la nouvelle fenêtre.

     Après avoir créé le site, retournez dans cette fenêtre pour sélectionner le site. Vous devrez peut-être actualiser la liste des sites pour voir le nouveau site. Pour actualiser vos données, choisissez l'icône d'actualisation ().

     Pour plus d'informations, consultez the section called "Sites".

10. Choisissez Créer un Outpost.

> **Tip**
>
> Pour ajouter de la capacité à votre nouvel Outpost, vous devez passer une commande.

Effectuez les étapes suivantes pour modifier le nom et la description d'un Outpost.

Pour modifier le nom et la description de l'Outpost

1. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.
2. Pour modifier le Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page.
3. Dans le panneau de navigation, choisissez Outposts.
4. Sélectionnez l'Outpost, puis choisissez Actions, Modifier l'Outpost.
5. Modifiez le nom et la description.

   Dans Nom, saisissez le nom.

Dans Description, saisissez la description.

6. Sélectionnez Enregistrer les modifications.

Effectuez les étapes suivantes pour afficher les détails d'un Outpost.

Pour afficher les détails de l'Outpost

1. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.
2. Pour modifier le Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page.
3. Dans le panneau de navigation, choisissez Outposts.
4. Sélectionnez l'Outpost, puis choisissez Actions, Afficher les détails.

Vous pouvez également utiliser le AWS CLI pour consulter les détails de l'Outpost.

Pour consulter les informations relatives à Outpost à l'aide du AWS CLI

- Utilisez la commande get-outpost AWS CLI .

Effectuez les étapes suivantes pour gérer les balises sur un Outpost.

Pour gérer les balises de l'Outpost

1. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.
2. Pour modifier le Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page.
3. Dans le panneau de navigation, choisissez Outposts.
4. Sélectionnez l'Outpost, puis choisissez Actions, Gérer les balises.
5. Ajoutez ou supprimez une balise.

   Pour ajouter une balise, choisissez Ajouter une balise, puis procédez comme suit :

   - Pour Clé, saisissez le nom de la clé.
   - Pour Valeur, saisissez la valeur de clé.

Pour supprimer une balise, choisissez Éliminer à droite de la clé et de la valeur de la balise.

6. Sélectionnez Enregistrer les modifications.

Gestion des sites Outpost

Les bâtiments physiques gérés par le client où AWS sera installé votre avant-poste. Un site doit répondre aux exigences en matière d'installations, de réseau et d'alimentation pour votre Outpost. Pour plus d'informations, consultez Prérequis.

Pour créer un site Outpost

1. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.
2. Pour modifier le Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page.
3. Dans le panneau de navigation, choisissez Sites.
4. Choisissez Créer un site.
5. Choisissez un type de matériel pris en charge pour le site.
6. Saisissez le nom, la description et l'adresse d'exploitation de votre site. Si vous avez choisi de prendre en charge des racks sur le site, saisissez les informations suivantes :

   - Poids maximum : spécifiez le poids maximum du rack que ce site peut supporter.
   - Puissance électrique : spécifiez en kVA la puissance électrique disponible à l'emplacement prévu du matériel pour le rack.
   - Option d'alimentation : spécifiez l'option d'alimentation que vous pouvez fournir pour le matériel.
   - Connecteur d'alimentation : spécifiez le connecteur d'alimentation qui AWS doit être prévu pour les connexions au matériel.
   - Baisse de puissance : précisez si l'alimentation électrique vient du haut ou du bas du rack.
   - Vitesse de liaison ascendante : spécifiez la vitesse de liaison ascendante que le rack doit prendre en charge pour la connexion à la région.
   - Nombre de liaisons ascendantes : spécifiez le nombre de liaisons ascendantes pour chaque appareil réseau Outpost que vous avez l'intention d'utiliser pour connecter le rack à votre réseau.

- Type de fibre : spécifiez le type de fibre que vous prévoyez d'utiliser pour attacher l'Outpost à votre réseau.
- Norme optique : spécifiez le type de norme optique que vous prévoyez d'utiliser pour attacher l'Outpost à votre réseau.
- Remarques : formulez des remarques sur un site.

7. Lisez les exigences en matière d'installations, puis choisissez J'ai lu les exigences de l'installation.
8. Choisissez Créer un site.

Effectuez les étapes suivantes pour modifier un site Outpost.

Pour modifier un site

1. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.
2. Pour modifier le Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page.
3. Dans le panneau de navigation, choisissez Sites.
4. Sélectionnez le site, puis Actions, Modifier le site.
5. Vous pouvez modifier le nom, la description, l'adresse d'exploitation et les détails du site.

   Si vous modifiez l'adresse d'exploitation, sachez que ces modifications ne se propageront pas aux commandes existantes.
6. Sélectionnez Enregistrer les modifications.

Effectuez les étapes suivantes pour afficher les détails d'un site Outpost.

Pour afficher les détails du site

1. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.
2. Pour modifier le Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page.
3. Dans le panneau de navigation, choisissez Sites.
4. Sélectionnez le site, puis choisissez Actions, Afficher les détails.

Effectuez les étapes suivantes pour gérer les balises sur un site Outpost.

Pour gérer les balises du site

1. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.
2. Pour modifier le Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page.
3. Dans le panneau de navigation, choisissez Sites.
4. Sélectionnez le site, puis choisissez Actions, Gérer les balises.
5. Ajoutez ou supprimez une balise.

   Pour ajouter une balise, choisissez Ajouter une balise, puis procédez comme suit :

   - Pour Clé, saisissez le nom de la clé.
   - Pour Valeur, saisissez la valeur de clé.

   Pour supprimer une balise, choisissez Éliminer à droite de la clé et de la valeur de la balise.
6. Sélectionnez Enregistrer les modifications.

Passerelle locale

La passerelle locale est un composant essentiel de l'architecture des Outposts. La passerelle locale permet la connectivité entre vos sous-réseaux Outpost et votre réseau sur site. Si l'infrastructure sur site fournit un accès à Internet, les charges de travail exécutées sur les Outposts peuvent également tirer parti de la passerelle locale pour communiquer avec les services régionaux ou les charges de travail régionales. Cette connectivité peut être réalisée soit en utilisant une connexion publique (Internet), soit en utilisant Direct Connect. Pour de plus amples informations, veuillez consulter Connectivité AWS Outposts avec les régions AWS.

Table des matières

Principes de base de la passerelle locale

Chaque Outpost prend en charge une seule passerelle locale. Une passerelle locale est dotée des composants suivants :

- Tables de routage : vous les utilisez pour créer des tables de routage de passerelle locale. Pour de plus amples informations, veuillez consulter the section called “Tables de routage de passerelle locale”.
- Groupes CoIP : (facultatif) vous pouvez utiliser les plages d'adresses IP dont vous êtes propriétaire pour faciliter la communication entre le réseau sur site et les instances de votre VPC. Pour de plus amples informations, veuillez consulter the section called “Adresses IP clients”.
- Interfaces virtuelles (VIF) : AWS crée un VIF pour chaque LAG et ajoute les deux VIF à un groupe VIF. La table de routage de passerelle locale doit avoir une route par défaut vers les deux VIF pour réaliser la connectivité au réseau local. Pour de plus amples informations, veuillez consulter Connectivité réseau locale.
- Associations de groupes VIF : AWS ajoute les VIF qu'il crée à un groupe VIF. Les groupes VIF sont des regroupements logiques d'interfaces virtuelles. Pour de plus amples informations, veuillez consulter the section called “Associations de groupe d'interfaces virtuelles”.

- Associations de VPC : vous les utilisez pour créer des associations de VPC avec vos VPC et la table de routage de passerelle locale. Les tables de routage VPC associées aux sous-réseaux résidant sur un Outpost peuvent utiliser la passerelle locale comme cible de routage. Pour de plus amples informations, veuillez consulter the section called “Associations de VPC”.

Lorsque vous AWS approvisionnez votre rack Outpost, nous créons certains composants et vous êtes responsable de la création d'autres.

AWS responsabilités

- Fournit le matériel.
- Crée la passerelle locale.
- Crée les interfaces virtuelles (VIF) et un groupe VIF.

Vos responsabilités

- Créez la table de routage de passerelle locale.
- Associez un VPC à la table de routage de passerelle locale.
- Associez un groupe VIF à la table de routage de passerelle locale.

Routage

Les instances de votre sous-réseau Outpost peuvent utiliser l'une des options suivantes pour communiquer avec votre réseau sur site via la passerelle locale :

- Adresses IP privées : la passerelle locale utilise les adresses IP privées des instances de votre sous-réseau Outpost pour faciliter la communication avec votre réseau sur site. Il s'agit de l'option par défaut.
- Adresses IP clients : la passerelle locale effectue la traduction d'adresses réseau (NAT) pour les adresses IP clients que vous attribuez aux instances du sous-réseau Outpost. Cette option prend en charge les plages CIDR qui se chevauchent et les autres topologies de réseau.

Pour de plus amples informations, veuillez consulter the section called “Tables de routage de passerelle locale”.

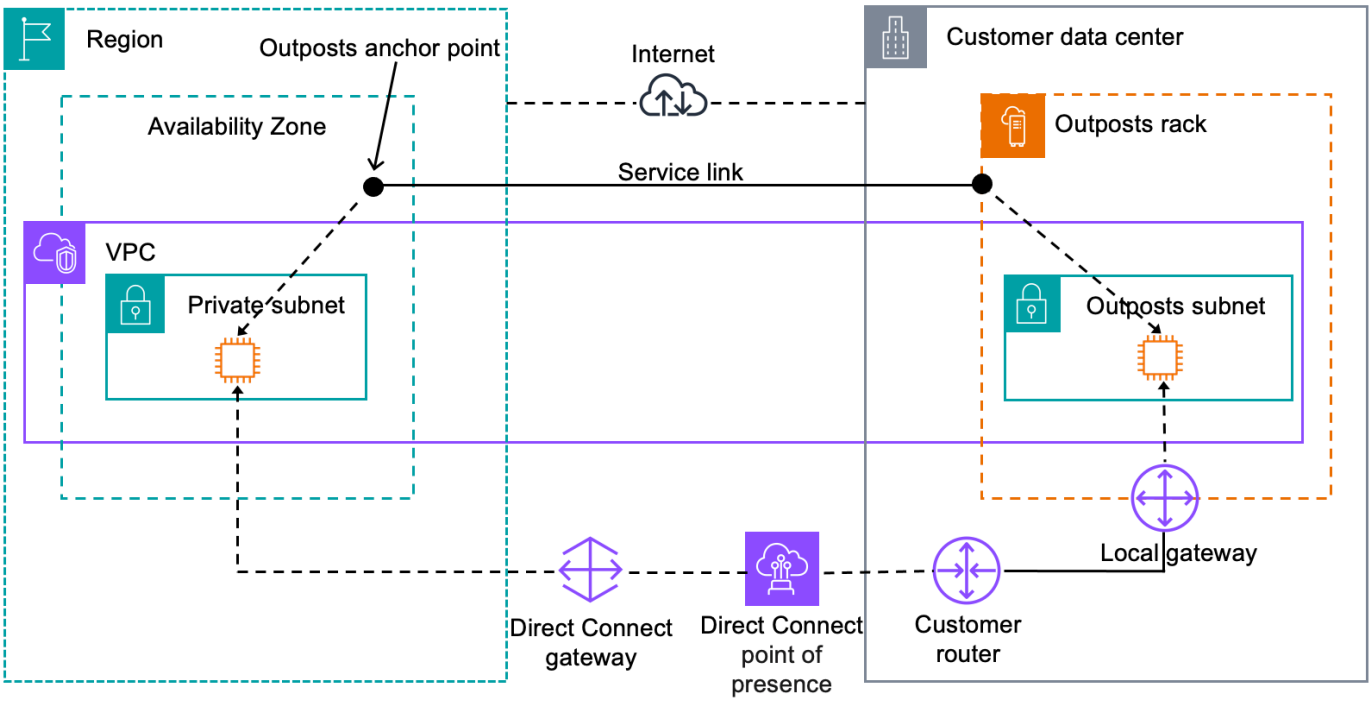
Connectivité via la passerelle locale

Le rôle principal d'une passerelle locale vise à établir une connectivité entre un Outpost et votre réseau sur site local. Elle fournit également une connectivité à Internet via votre réseau sur site. Pour obtenir des exemples, veuillez consulter the section called "Routage VPC direct" et the section called "Adresses IP clients".

La passerelle locale peut également fournir un chemin de plan de données vers la AWS région. Le chemin du plan de données pour la passerelle locale part de l'Outpost, passe par la passerelle locale et atteint le segment LAN de votre passerelle locale privée. Il suivrait ensuite un chemin privé pour revenir aux points de terminaison du service AWS dans la région. Notez que le chemin du plan de contrôle utilise toujours la connectivité de la liaison de service, quel que soit le chemin du plan de données que vous utilisiez.

Vous pouvez connecter votre infrastructure Outposts sur site Services AWS à celle de la région en privé. AWS Direct Connect Pour plus d'informations, consultez Connectivité privée AWS Outposts.

L'image suivante illustre la connectivité via la passerelle locale :



Tables de routage de passerelle locale

Les tables de routage de sous-réseau Outpost sur un rack peuvent inclure une route vers votre réseau sur site. La passerelle locale achemine ce trafic pour un routage à faible latence vers le réseau sur site.

Par défaut, Outposts utilise l'adresse IP privée des instances de l'Outpost pour communiquer avec votre réseau sur site. C'est ce que l'on appelle le routage VPC direct pour AWS Outposts (ou routage VPC direct). Toutefois, vous pouvez fournir une plage d'adresses, appelée groupe d'adresses IP clients (CoIP), et demander aux instances de votre réseau d'utiliser ces adresses pour communiquer avec votre réseau sur site. Le routage VPC direct et CoIP sont des options qui s'excluent mutuellement et le routage fonctionne différemment en fonction de votre choix.

Table des matières

Routage VPC direct

Le routage VPC direct utilise l'adresse IP privée des instances de votre VPC pour faciliter la communication avec votre réseau sur site. Ces adresses sont publiées sur votre réseau sur site via BGP. 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 les Outposts. Dans ce mode, la passerelle locale n'exécute pas la NAT pour les instances, et vous n'avez pas besoin d'attribuer d'adresses IP Elastic à vos instances EC2. Vous avez la possibilité d'utiliser votre propre espace d'adressage au lieu du mode de routage VPC direct. Pour de plus amples informations, veuillez consulter Adresses IP clients.

Le routage VPC direct n'est pris en charge que pour les interfaces réseau des instances. Avec les interfaces réseau AWS créées en votre nom (appelées interfaces réseau gérées par les demandeurs), leurs adresses IP privées ne sont pas accessibles depuis votre réseau local. Par exemple, les points de terminaison d'un VPC ne sont pas directement accessibles depuis votre réseau sur site.

Les exemples suivants illustrent le routage VPC direct.

Exemples

Exemple : connectivité Internet via le VPC

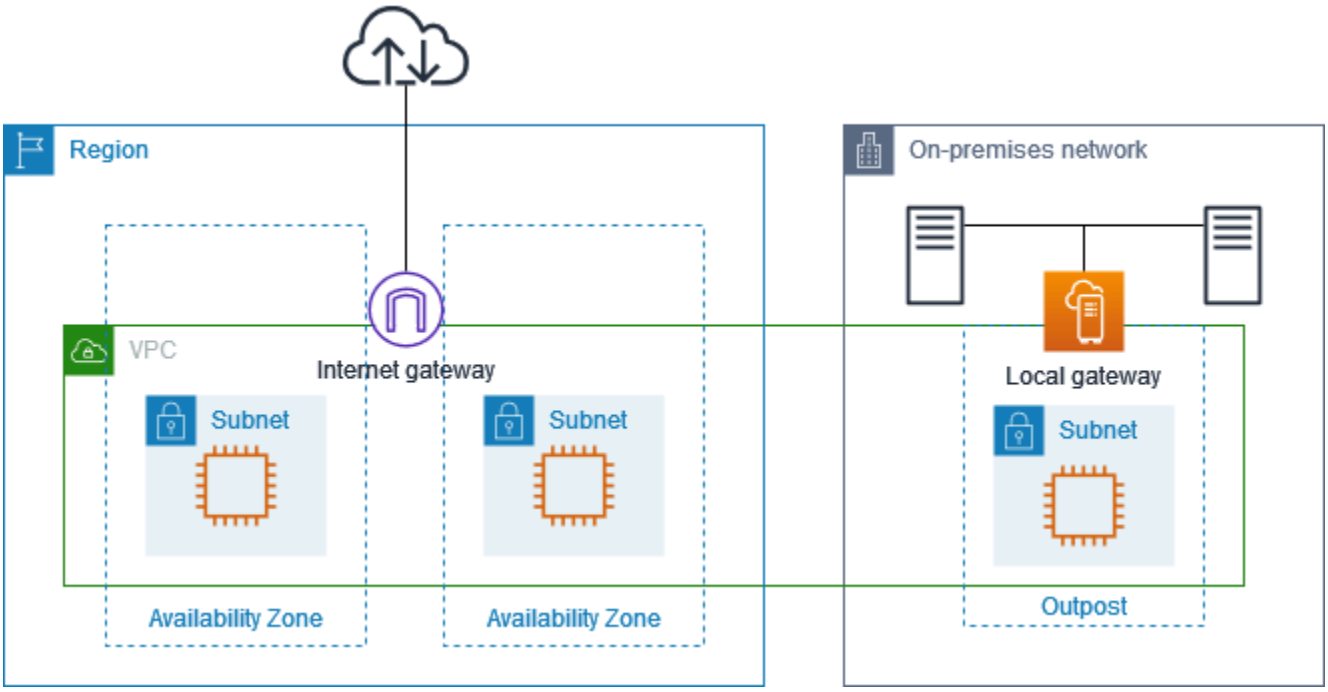
Les instances d'un sous-réseau Outpost peuvent accéder à Internet via la passerelle Internet attachée au VPC.

Examinez la configuration suivante :

- Le VPC parent couvre deux zones de disponibilité, avec un sous-réseau dans chacune d'elles.
- L'Outpost possède un sous-réseau.
- Chaque sous-réseau possède une instance EC2.
- La passerelle locale utilise la publication BGP pour publier les adresses IP privées du sous-réseau Outpost sur le réseau sur site.

> **Note**
>
> La publication BGP n'est prise en charge que pour les sous-réseaux d'un Outpost dont la route a pour destination la passerelle locale. Les autres sous-réseaux ne sont pas publiés via BGP.

Dans le diagramme suivant, le trafic provenant de l'instance du sous-réseau Outpost peut utiliser la passerelle Internet pour que le VPC accède à Internet.



Pour établir une connectivité Internet via la région parent, la table de routage du sous-réseau Outpost doit comporter les routes suivantes.

Destination	Cible	Commentaires
Bloc d'adresse du VPC	Local	Fournit la connectivité entre les sous-réseaux du VPC.
0.0.0.0	*internet-gateway-id*	Envoie le trafic destiné à Internet vers la passerelle Internet.
CIDR du réseau sur site	*local-gateway-id*	Envoie le trafic destiné au réseau sur site vers la passerelle locale.

Exemple : connectivité Internet via le réseau sur site

Les instances d'un sous-réseau Outpost peuvent accéder à Internet via le réseau sur site. Les instances du sous-réseau Outpost n'ont pas besoin d'adresse IP publique ou d'adresse IP Elastic.

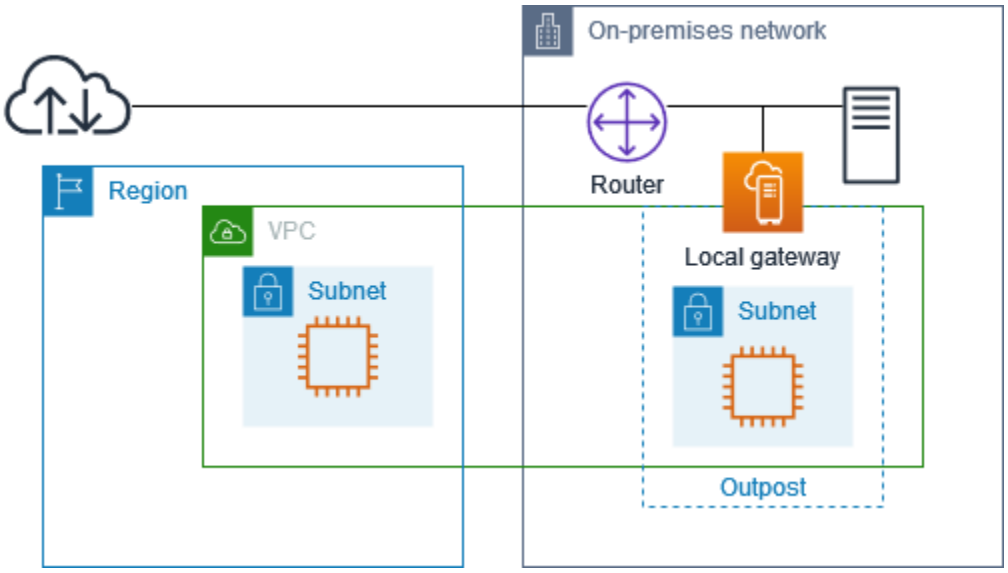
Examinez la configuration suivante :

- Le sous-réseau Outpost dispose d'une instance EC2.

- Le routeur du réseau sur site effectue la traduction d'adresses réseau (NAT).
- La passerelle locale utilise la publication BGP pour publier les adresses IP privées du sous-réseau Outpost sur le réseau sur site.

> **Note**
>
> La publication BGP n'est prise en charge que pour les sous-réseaux d'un Outpost dont la route a pour destination la passerelle locale. Les autres sous-réseaux ne sont pas publiés via BGP.

Dans le diagramme suivant, le trafic provenant de l'instance du sous-réseau Outpost peut utiliser la passerelle locale pour accéder à Internet ou au réseau sur site. Le trafic provenant du réseau sur site utilise la passerelle locale pour accéder à l'instance du sous-réseau Outpost.



Pour établir une connectivité Internet via le réseau sur site, la table de routage du sous-réseau Outpost doit comporter les routes suivantes.

Destination	Cible	Commentaires
Bloc d'adresse du VPC	Local	Fournit la connectivité entre les sous-réseaux du VPC.

Destination	Cible	Commentaires	
0.0.0.0/0	*local-gateway-id*	Envoie le trafic destiné à Internet vers la passerelle locale.	

Accès sortant à Internet

Le trafic initié depuis l'instance du sous-réseau Outpost à destination d'Internet utilise la route 0.0.0.0/0 pour acheminer le trafic vers la passerelle locale. La passerelle locale envoie le trafic au routeur. Le routeur utilise la NAT pour traduire l'adresse IP privée en adresse IP publique sur le routeur, puis envoie le trafic vers la destination.

Accès sortant au réseau sur site

Le trafic initié depuis l'instance du sous-réseau Outpost à destination du réseau sur site utilise la route 0.0.0.0/0 pour acheminer le trafic vers la passerelle locale. La passerelle locale envoie le trafic vers la destination du réseau sur site.

Accès entrant depuis le réseau sur site

Le trafic provenant du réseau sur site à destination de l'instance du sous-réseau Outpost utilise l'adresse IP privée de l'instance. Lorsque le trafic atteint la passerelle locale, cette dernière l'envoie vers la destination du VPC.

Adresses IP clients

Par défaut, la passerelle locale utilise les adresses IP privées des instances de votre VPC pour faciliter la communication avec votre réseau sur site. Cependant, vous pouvez fournir une plage d'adresses, appelée groupe d'adresses IP clients (CoIP), qui prend en charge les plages CIDR qui se chevauchent et les autres topologies de réseau.

Si vous choisissez CoIP, vous devez créer un groupe d'adresses, l'attribuer à la table de routage de passerelle locale et republier ces adresses sur votre réseau client via BGP. Toutes les adresses IP clients associées à votre table de routage de passerelle locale apparaissent dans la table de routage sous forme de routes propagées.

Les adresses IP clients fournissent une connectivité locale ou externe aux ressources de votre réseau sur site. Vous pouvez attribuer ces adresses IP aux ressources de votre Outpost, telles que les instances EC2, en allouant une nouvelle adresse IP Elastic issue du groupe d'adresses IP clients,

puis en l'attribuant à votre ressource. Pour de plus amples informations, veuillez consulter the section called “3f : (Facultatif) Attribuez une adresse IP appartenant au client à l'instance”.

Les exigences suivantes s'appliquent au groupe d'adresses IP clients :

- Vous devez être en mesure d'acheminer l'adresse sur votre réseau
- Le bloc CIDR doit être au moins égal à /26

Lorsque vous allouez une adresse IP Elastic à partir de votre groupe d'adresses IP clients, vous continuez à être propriétaire des adresses IP figurant dans votre groupe d'adresses IP clients. Vous êtes responsable de leur publication sur vos réseaux internes ou votre réseau étendu (WAN) selon les besoins.

Vous pouvez éventuellement partager votre pool appartenant à des clients avec plusieurs membres de votre organisation Comptes AWS à l'aide de. AWS Resource Access Manager Une fois que vous avez partagé le groupe, les participants peuvent attribuer une adresse IP Elastic provenant du groupe d'adresses IP clients, puis l'attribuer à une instance EC2 sur l'Outpost. Pour plus d'informations, consultez Partage de vos ressources AWS dans le Guide de l'utilisateur AWS RAM .

Exemples

- Exemple : connectivité Internet via le VPC
- Exemple : connectivité Internet via le réseau sur site

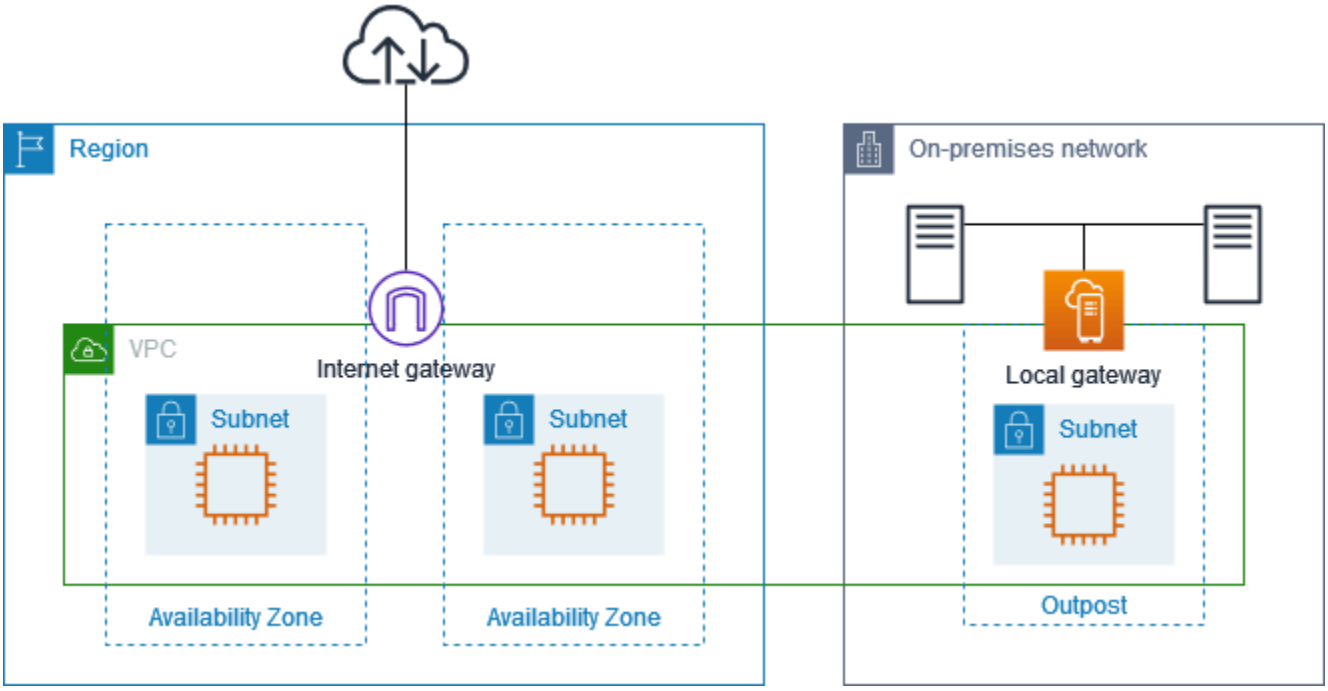
Exemple : connectivité Internet via le VPC

Les instances d'un sous-réseau Outpost peuvent accéder à Internet via la passerelle Internet attachée au VPC.

Examinez la configuration suivante :

- Le VPC parent couvre deux zones de disponibilité, avec un sous-réseau dans chacune d'elles.
- L'Outpost possède un sous-réseau.
- Chaque sous-réseau possède une instance EC2.
- Il existe un groupe d'adresses IP clients.
- L'instance du sous-réseau Outpost possède une adresse IP Elastic provenant du groupe d'adresses IP clients.

- La passerelle locale utilise la publication BGP pour publier le groupe d'adresses IP clients sur le réseau sur site.



Pour établir une connectivité Internet via la région, la table de routage du sous-réseau Outpost doit comporter les routes suivantes.

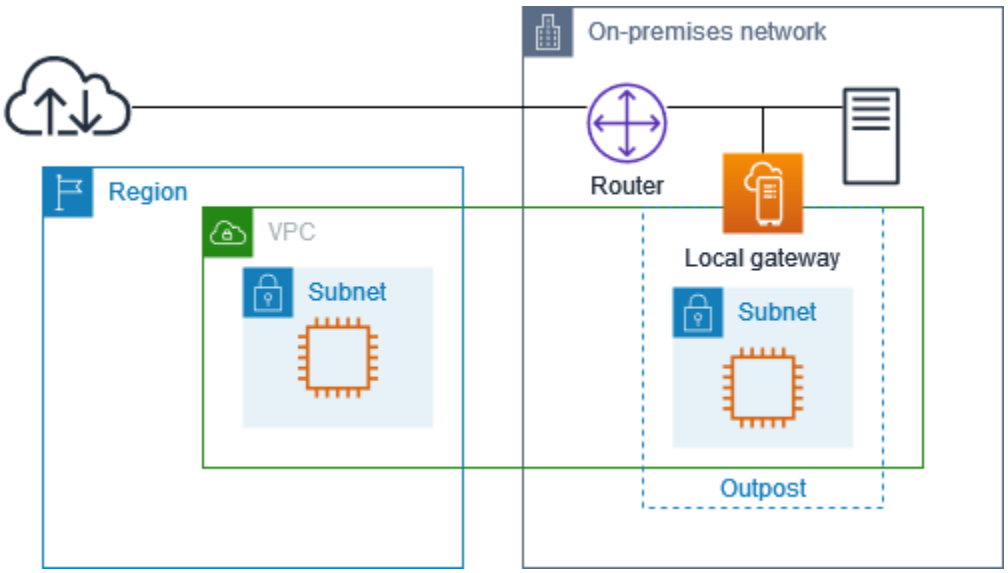
Destination	Cible	Commentaires
Bloc d'adresse du VPC	Local	Fournit la connectivité entre les sous-réseaux du VPC.
0.0.0.0	*internet-gateway-id*	Envoie le trafic destiné à l'Internet public vers la passerelle Internet.
CIDR du réseau sur site	*local-gateway-id*	Envoie le trafic destiné au réseau sur site vers la passerelle locale.

Exemple : connectivité Internet via le réseau sur site

Les instances d'un sous-réseau Outpost peuvent accéder à Internet via le réseau sur site.

Examinez la configuration suivante :

- Le sous-réseau Outpost dispose d'une instance EC2.
- Il existe un groupe d'adresses IP clients.
- La passerelle locale utilise la publication BGP pour publier le groupe d'adresses IP clients sur le réseau sur site.
- Une association d'adresses IP Elastic mappe 10.0.3.112 à 10.1.0.2.
- Le routeur du réseau sur site client exécute la NAT.



Pour établir une connectivité Internet via la passerelle locale, la table de routage du sous-réseau Outpost doit comporter les routes suivantes.

Destination	Cible	Commentaires
Bloc d'adresse du VPC	Local	Fournit la connectivité entre les sous-réseaux du VPC.
0.0.0.0/0	*local-gateway-id*	Envoie le trafic destiné à Internet vers la passerelle locale.

Accès sortant à Internet

Le trafic initié depuis l'instance EC2 du sous-réseau Outpost à destination d'Internet utilise la route 0.0.0.0/0 pour acheminer le trafic vers la passerelle locale. La passerelle locale mappe l'adresse IP privée de l'instance à l'adresse IP client, puis envoie le trafic au routeur. Le routeur utilise la NAT

pour traduire l'adresse IP client en adresse IP publique sur le routeur, puis envoie le trafic vers la destination.

Accès sortant au réseau sur site

Le trafic initié depuis l'instance EC2 du sous-réseau Outpost à destination du réseau sur site utilise la route 0.0.0.0/0 pour acheminer le trafic vers la passerelle locale. La passerelle locale traduit l'adresse IP de l'instance EC2 en adresse IP client (adresse IP Elastic), puis envoie le trafic vers la destination.

Accès entrant depuis le réseau sur site

Le trafic provenant du réseau sur site à destination de l'instance du sous-réseau Outpost utilise l'adresse IP client (adresse IP Elastic) de l'instance. Lorsque le trafic atteint la passerelle locale, cette dernière mappe l'adresse IP client (adresse IP Elastic) à l'adresse IP de l'instance, puis envoie le trafic vers la destination dans le VPC. En outre, la table de routage de passerelle locale évalue toutes les routes qui ciblent les interfaces réseau Elastic. Si l'adresse de destination correspond au CIDR de destination d'une route statique, le trafic est envoyé vers cette interface réseau Elastic. Lorsque le trafic suit une route statique vers une interface réseau Elastic, l'adresse de destination est préservée et n'est pas traduite en adresse IP privée de l'interface réseau.

Utilisation des tables de routage de passerelle locale

Dans le cadre de l'installation en rack, AWS crée la passerelle locale, configure les VIF et un groupe VIF. Vous créez la table de routage de passerelle locale. Une table de routage de passerelle locale doit être associée à un groupe VIF et à un VPC. Vous créez et gérez l'association du groupe VIF et du VPC. Tenez compte des informations suivantes concernant les tables de routage de passerelle locale :

- Les groupes VIF et les tables de routage des passerelles locales doivent avoir une one-to-one relation.
- La passerelle locale appartient au AWS compte associé à l'Outpost et seul le propriétaire peut modifier la table de routage de la passerelle locale.
- Vous pouvez partager la table de routage de la passerelle locale avec d'autres AWS comptes ou unités organisationnelles à l'aide de AWS Resource Access Manager. Pour plus d'informations, consultez Utilisation de ressources AWS Outposts partagées.
- Les tables de routage de passerelle locale disposent d'un mode qui détermine si l'adresse IP privée des instances doit être utilisée pour communiquer avec votre réseau sur site (routage VPC direct) ou avec un groupe d'adresses IP clients (CoIP). Le routage VPC direct et CoIP sont des options

qui s'excluent mutuellement et le routage fonctionne différemment en fonction de votre choix. Pour de plus amples informations, veuillez consulter ???.

- Le mode de routage VPC direct ne prend pas en charge les plages CIDR qui se chevauchent.

Tâches

- Affichage des détails de la table de routage de passerelle locale
- Création de tables de routage de passerelle locale personnalisées
- Gestion des routes de la table de routage de passerelle locale
- Gestion des balises de la table de routage de passerelle locale
- Changement de mode de la table de routage de passerelle locale ou suppression d'une table de routage de passerelle locale
- Gestion des groupes CoIP
- Associations de groupe d'interfaces virtuelles
- Associations de VPC

Affichage des détails de la table de routage de passerelle locale

Vous pouvez afficher les détails des tables de routage de votre passerelle locale à l'aide de la console ou de l' AWS CLI.

AWS Outposts console

Pour afficher les détails de la table de routage de passerelle locale

1. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.
2. Pour modifier le Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page.
3. Dans le panneau de navigation, choisissez Table de routage de passerelle locale.
4. Sélectionnez la table de routage de passerelle locale, puis choisissez Actions, Afficher les détails.

AWS CLI

Pour afficher les détails de la table de routage de passerelle locale

Utilisez la AWS CLI commande describe-local-gateway-route-tables.

Exemple

```
aws ec2 describe-local-gateway-route-tables --region us-west-2
```

Sortie

```
{
    "LocalGatewayRouteTables": [
        {
            "LocalGatewayRouteTableId": "lgw-rtb-059615ef7deEXAMPLE",
            "LocalGatewayId": "lgw-09b493aa7cEXAMPLE",
            "OutpostArn": "arn:aws:outposts:us-west-2:111122223333:outpost/
op-0dc11b66edEXAMPLE",
            "State": "available",
            "Tags": []
        }
    ]
}
```

> **Note**
>
> Si la table de routage de passerelle locale par défaut que vous consultez utilise le mode CoIP, la table de routage de passerelle locale est configurée avec une route par défaut vers chacune des interfaces virtuelles et une route propagée vers chaque adresse IP client associée du groupe CoIP.

Création de tables de routage de passerelle locale personnalisées

Vous pouvez créer une table de routage personnalisée pour votre passerelle locale à l'aide de la console AWS Outposts .

Pour créer une table de routage de passerelle locale personnalisée à l'aide de la console

1. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.
2. Pour modifier le Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page.

3. Dans le panneau de navigation, choisissez Table de routage de passerelle locale.
4. Choisissez Créer une table de routage de passerelle locale.
5. (Facultatif) Dans Nom, saisissez un nom pour votre table de routage de passerelle locale.
6. Pour Passerelle locale, choisissez votre passerelle locale.
7. (Facultatif) Choisissez Associer le groupe VIF et choisissez votre Groupe VIF.
8. Pour Mode, choisissez un mode de communication avec votre réseau sur site.

   - Choisissez Routage VPC direct pour utiliser l'adresse IP privée d'une instance.
   - Choisissez CoIP pour utiliser l'adresse IP client.
     - (Facultatif) Ajoutez ou supprimez des groupes CoIP et des blocs CIDR supplémentaires.

       [Ajout d'un groupe CoIP] Choisissez Ajouter un nouveau groupe et procédez comme suit :

       - Dans Nom, saisissez un nom pour votre groupe CoIP.
       - Dans CIDR, saisissez un bloc CIDR d'adresses IP clients.
     - [Ajout de blocs CIDR] Choisissez Ajouter un nouveau CIDR et entrez une plage d'adresses IP clients.
     - [Suppression d'un groupe CoIP ou d'un bloc CIDR supplémentaire] Choisissez Éliminer à droite d'un bloc CIDR ou en dessous du groupe CoIP.

       Vous pouvez spécifier jusqu'à 10 groupes CoIP et 100 blocs CIDR.
9. (Facultatif) Ajoutez ou supprimez une balise.

   [Ajouter une balise] Choisissez Ajouter une nouvelle balise et procédez comme suit :

   - Pour Clé, saisissez le nom de la clé.
   - Pour Value (Valeur), saisissez la valeur de clé.

   [Suppression d'une balise] Choisissez Éliminer à la droite de la clé et de la valeur de la balise.
10. Choisissez Créer une table de routage de passerelle locale.

Gestion des routes de la table de routage de passerelle locale

Vous pouvez créer des tables de routage de passerelle locale et des routes entrantes à destination des interfaces réseau Elastic sur votre Outpost. Vous pouvez également modifier la route entrante d'une passerelle locale existante pour changer l'interface réseau Elastic cible.

Une route est à l'état actif uniquement lorsque son interface réseau Elastic cible est attachée à une instance en cours d'exécution. Si l'instance est arrêtée ou que l'interface est détachée, la route passe de l'état actif à l'état Blackhole.

Les exigences et les limitations suivantes s'appliquent à une passerelle locale :

- L'interface réseau Elastic cible doit appartenir à un sous-réseau de votre Outpost et doit être attachée à une instance de cet Outpost. Une route de passerelle locale ne peut pas cibler une instance Amazon EC2 d'un autre Outpost ou de la Région AWS parent.
- Le sous-réseau doit appartenir à un VPC associé à la table de routage de passerelle locale.
- Une table de routage ne doit pas contenir plus de 100 routes d'interface réseau Elastic.
- AWS donne la priorité à l'itinéraire le plus spécifique, et si les itinéraires correspondent, nous donnons la priorité aux itinéraires statiques par rapport aux itinéraires propagés.
- Les points de terminaison de VPC d'interface ne sont pas pris en charge.
- La publication BGP est destinée uniquement aux sous-réseaux d'un Outpost qui comportent une route ciblant la passerelle locale dans la table de routage. Si les sous-réseaux ne comportent pas de route qui cible la passerelle locale dans la table de routage, ils ne sont pas publiés avec BGP.
- Seules les ENI attachées aux instances Outpost peuvent communiquer via la passerelle locale de cet Outpost. Les ENI qui appartiennent au sous-réseau Outpost mais qui sont attachées à une instance de la région ne peuvent pas communiquer via la passerelle locale de cet Outpost.
- Les interfaces gérées telles que les points de terminaison ou les interfaces VPCE ne sont pas accessibles sur site via la passerelle locale. Elles ne sont accessibles qu'à partir des instances situées dans l'Outpost.

Les considérations suivantes s'appliquent à la traduction d'adresses réseau (NAT).

- La passerelle locale n'effectue pas de NAT sur le trafic correspondant à une route d'interface réseau Elastic. Au lieu de cela, l'adresse IP de destination est préservée.
- Désactivez la vérification de la source/destination pour l'interface réseau Elastic cible. Pour plus d'informations, consultez Notions fondamentales concernant l'interface réseau dans le Guide de l'utilisateur Amazon EC2 pour les instances Linux.
- Configurez le système d'exploitation pour autoriser l'interface réseau à accepter le trafic provenant du CIDR de destination.

AWS Outposts console

Pour éditer une route de la table de routage de passerelle locale

1. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.
2. Pour modifier le Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page.
3. Dans le panneau de navigation, choisissez Table de routage de passerelle locale.
4. Sélectionnez la table de routage de passerelle locale, puis choisissez Actions, Modifier les routages.
5. Pour ajouter une route, choisissez Add route (Ajouter une route). Pour Destination, entrez le bloc CIDR de destination, une adresse IP unique ou l'ID d'une liste de préfixes.
6. Pour modifier une route existante, pour Destination, remplacez le bloc d'adresse CIDR de destination ou l'adresse IP unique. Pour Cible, choisissez une cible.
7. Choisissez Save routes (Enregistrer les acheminements).

AWS CLI

Pour créer une route de la table de routage de passerelle locale

- Utilisez la create-local-gateway-route AWS CLI commande.

Exemple

```
aws ec2 create-local-gateway-route \
    --local-gateway-route-table-id lgw-rtb-059615ef7dEXAMPLE \
    --network-interface-id eni-03e612f0a1EXAMPLE \
    --destination-cidr-block 192.0.2.0/24
```

Sortie

```
{
    "Route": {
        "DestinationCidrBlock": "192.0.2.0/24",
        "NetworkInterfaceId": "eni-03e612f0a1EXAMPLE",
        "Type": "static",
        "State": "active",
        "LocalGatewayRouteTableId": "lgw-rtb-059615ef7dEXAMPLE",
```

```
        "LocalGatewayRouteTableArn": "arn:aws:ec2:us-west-2:111122223333:local-
gateway-route-table/lgw-rtb-059615ef7dEXAMPLE",
        "OwnerId": "111122223333"
    }
}
```

Pour modifier une route de la table de routage de passerelle locale

Vous pouvez modifier l'interface réseau Elastic ciblée par une route existante. Pour utiliser l'opération de modification, la table de routage doit déjà comporter une route avec le bloc CIDR de destination spécifié.

- Utilisez la modify-local-gateway-route AWS CLI commande.

Exemple

```
aws ec2 modify-local-gateway-route \
    --local-gateway-route-table-id lgw-rtb-059615ef7dEXAMPLE \
    --network-interface-id eni-12a345b6c7EXAMPLE \
    --destination-cidr-block 192.0.2.0/24
```

Sortie

```
{
    "Route": {
        "DestinationCidrBlock": "192.0.2.0/24",
        "NetworkInterfaceId": "eni-12a345b6c7EXAMPLE",
        "Type": "static",
        "State": "active",
        "LocalGatewayRouteTableId": "lgw-rtb-059615ef7dEXAMPLE",
        "LocalGatewayRouteTableArn": "arn:aws:ec2:us-west-2:111122223333:local-
gateway-route-table/lgw-rtb-059615ef7dEXAMPLE",
        "OwnerId": "111122223333"
    }
}
```

Gestion des balises de la table de routage de passerelle locale

Vous pouvez baliser les tables de routage de votre passerelle locale afin de les identifier ou de les classer en fonction des besoins de votre organisation.

Pour gérer les balises de la table de routage de passerelle locale

1. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.
2. Pour modifier le Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page.
3. Dans le panneau de navigation, choisissez Tables de routage de passerelle locale.
4. Sélectionnez la table de routage de passerelle locale, puis choisissez Actions, Gérer les balises.
5. Ajoutez ou supprimez une balise.

   Pour ajouter une balise, choisissez Ajouter une balise, puis procédez comme suit :

   - Pour Clé, saisissez le nom de la clé.
   - Pour Valeur, saisissez la valeur de clé.

   Pour supprimer une balise, choisissez Éliminer à droite de la clé et de la valeur de la balise.
6. Sélectionnez Enregistrer les modifications.

Changement de mode de la table de routage de passerelle locale ou suppression d'une table de routage de passerelle locale

Vous devez supprimer et recréer la table de routage de passerelle locale pour changer de mode. La suppression de la table de routage de passerelle locale entraîne une interruption du trafic réseau.

Pour changer de mode ou supprimer une table de routage de passerelle locale

1. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.
2. Pour modifier le Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page.
3. Dans le panneau de navigation, choisissez Tables de routage de passerelle locale.
4. Sélectionnez la table de routage de passerelle locale, puis choisissez Actions, Supprimer la table de routage de passerelle locale.
5. Dans la boîte de dialogue de confirmation, tapez **`delete`**, puis choisissez Supprimer.
6. (Facultatif) Créez une table de routage de passerelle locale avec un nouveau mode.

   a. Choisissez Créer une table de routage de passerelle locale.

b. Configurez la table de routage de passerelle locale en utilisant le nouveau mode. Pour plus d'informations, consultez Création de tables de routage de passerelle locale personnalisées.

Gestion des groupes CoIP

Vous pouvez fournir des plages d'adresses IP pour faciliter la communication entre votre réseau sur site et les instances de votre VPC. Pour plus d'informations, consultez Adresses IP clients.

Des groupes d'adresses IP clients sont disponibles pour les tables de routage de passerelle locale en mode CoIP. Pour passer d'un mode de table de routage de passerelle locale à un autre, consultez Changement de mode de la table de routage de passerelle locale.

Procédez comme suit pour créer un groupe CoIP.

Pour créer un groupe CoIP

1. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.
2. Pour modifier le Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page.
3. Dans le panneau de navigation, choisissez Tables de routage de passerelle locale.
4. Choisissez la table de routage.
5. Choisissez l'onglet Groupes CoIP dans le volet de détails, puis choisissez Créer un groupe CoIP.
6. (Facultatif) Dans Nom, saisissez un nom pour votre groupe CoIP.
7. Choisissez Ajouter un nouveau CIDR et entrez une plage d'adresses IP clients.
8. (Facultatif) Ajout ou suppression de blocs CIDR

   [Ajout d'un bloc CIDR] Choisissez Ajouter un nouveau CIDR et entrez une plage d'adresses IP clients.

   [Suppression d'un bloc CIDR] Choisissez Éliminer à droite d'un bloc CIDR.
9. Choisissez Créer un groupe CoIP.

Procédez comme suit pour modifier un groupe CoIP.

Pour modifier un groupe CoIP

1. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.

2. Pour modifier le Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page.
3. Dans le panneau de navigation, choisissez Tables de routage de passerelle locale.
4. Choisissez la table de routage.
5. Choisissez l'onglet Groupes CoIP dans le volet de détails, puis choisissez un groupe CoIP.
6. Choisissez Actions, Modifier le groupe CoIP.
7. Choisissez Ajouter un nouveau CIDR et entrez une plage d'adresses IP clients.
8. (Facultatif) Ajout ou suppression de blocs CIDR

   [Ajout d'un bloc CIDR] Choisissez Ajouter un nouveau CIDR et entrez une plage d'adresses IP clients.

   [Suppression d'un bloc CIDR] Choisissez Éliminer à droite d'un bloc CIDR.
9. Sélectionnez Enregistrer les modifications.

Procédez comme suit pour gérer les balises ou ajouter une balise de nom à un groupe CoIP.

Pour gérer les balises dans un groupe CoIP

1. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.
2. Pour modifier le Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page.
3. Dans le panneau de navigation, choisissez Tables de routage de passerelle locale.
4. Choisissez la table de routage.
5. Choisissez l'onglet Groupes CoIP dans le volet de détails, puis choisissez un groupe CoIP.
6. Choisissez Actions, Gérer les balises.
7. Ajoutez ou supprimez une balise.

   Pour ajouter une balise, choisissez Ajouter une balise, puis procédez comme suit :

   - Pour Clé, saisissez le nom de la clé.
   - Pour Valeur, saisissez la valeur de clé.

   Pour supprimer une balise, choisissez Éliminer à droite de la clé et de la valeur de la balise.
8. Sélectionnez Enregistrer les modifications.

Procédez comme suit pour supprimer un groupe CoIP.

Pour supprimer un groupe CoIP

1. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.
2. Pour modifier le Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page.
3. Dans le panneau de navigation, choisissez Tables de routage de passerelle locale.
4. Choisissez la table de routage.
5. Choisissez l'onglet Groupes CoIP dans le volet de détails, puis choisissez un groupe CoIP.
6. Choisissez Actions, Supprimer le groupe CoIP.
7. Dans la boîte de dialogue de confirmation, tapez **`delete`**, puis choisissez Supprimer.

Associations de groupe d'interfaces virtuelles

Les groupes VIF sont des regroupements logiques d'interfaces virtuelles (VIF). Vous pouvez modifier la table de routage de passerelle locale à laquelle le groupe VIF est associé. Lorsque vous dissociez un groupe VIF d'une table de routage de passerelle locale, vous supprimez toutes les routes de la table de routage et vous interrompez le trafic réseau.

Pour modifier l'association d'un groupe VIF

1. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.
2. Pour modifier le Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page.
3. Dans le panneau de navigation, choisissez Tables de routage de passerelle locale.
4. Choisissez la table de routage.
5. Choisissez l'onglet Association de groupe VIF dans le volet de détails, puis choisissez Modifier l'association de groupe VIF.
6. Pour Paramètres du groupe VIF, effectuez l'une des actions suivantes :

   - Pour associer le groupe VIF à la table de routage de passerelle locale, sélectionnez Associer le groupe VIF, puis choisissez un groupe VIF.
   - Pour dissocier le groupe VIF de la table de routage de passerelle locale, désélectionnez Associer le groupe VIF.

> **Important**
>
> La dissociation d'un groupe VIF de la table de routage de passerelle locale supprime automatiquement toutes les routes et interrompt le trafic réseau.

7. Sélectionnez Enregistrer les modifications.

Associations de VPC

Vous devez associer les VPC à la table de routage de votre passerelle locale. Ils ne sont pas associés par défaut.

Création d'une association de VPC

Procédez comme suit pour associer un VPC à une table de routage de passerelle locale.

Vous pouvez éventuellement baliser votre association pour l'identifier ou la catégoriser en fonction des besoins de votre organisation.

AWS Outposts console

Pour associer un VPC

1. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.
2. Pour modifier le Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page.
3. Dans le panneau de navigation, choisissez Tables de routage de passerelle locale.
4. Sélectionnez la table de routage, puis choisissez Actions, Associer un VPC.
5. Dans ID du VPC, sélectionnez le VPC à associer à la table de routage de passerelle locale.
6. (Facultatif) Ajoutez ou supprimez une balise.

   Pour ajouter une balise, choisissez Ajouter une balise, puis procédez comme suit :

   - Pour Clé, saisissez le nom de la clé.
   - Pour Valeur, saisissez la valeur de clé.

   Pour supprimer une balise, choisissez Éliminer à droite de la clé et de la valeur de la balise.

7. Choisissez Associate VPC (Associer un VPC).

AWS CLI

Pour associer un VPC

Utilisez la table-vpc-association commande create-local-gateway-route-.

Exemple

```
aws ec2 create-local-gateway-route-table-vpc-association \
    --local-gateway-route-table-id lgw-rtb-059615ef7dEXAMPLE \
    --vpc-id vpc-07ef66ac71EXAMPLE
```

Sortie

```
{
    "LocalGatewayRouteTableVpcAssociation": {
        "LocalGatewayRouteTableVpcAssociationId": "lgw-vpc-assoc-0ee765bcc8EXAMPLE",
        "LocalGatewayRouteTableId": "lgw-rtb-059615ef7dEXAMPLE",
        "LocalGatewayId": "lgw-09b493aa7cEXAMPLE",
        "VpcId": "vpc-07ef66ac71EXAMPLE",
        "State": "associated"
    }
}
```

Suppression d'une association de VPC

Procédez comme suit pour dissocier un VPC d'une table de routage de passerelle locale.

AWS Outposts console

Pour dissocier un VPC

1. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.
2. Pour modifier le Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page.
3. Dans le panneau de navigation, choisissez Tables de routage de passerelle locale.
4. Sélectionnez la table de routage, puis choisissez Actions, Afficher les détails.

5. Dans Associations de VPC, sélectionnez le VPC à dissocier, puis choisissez Dissocier.
6. Choisissez Dissocier.

AWS CLI

Pour dissocier un VPC

Utilisez la table-vpc-association commande delete-local-gateway-route-.

Exemple

```
aws ec2 delete-local-gateway-route-table-vpc-association \
    --local-gateway-route-table-id lgw-rtb-059615ef7dEXAMPLE \
    --vpc-id vpc-07ef66ac71EXAMPLE
```

Sortie

```
{
    "LocalGatewayRouteTableVpcAssociation": {
        "LocalGatewayRouteTableVpcAssociationId": "lgw-vpc-assoc-0ee765bcc8EXAMPLE",
        "LocalGatewayRouteTableId": "lgw-rtb-059615ef7dEXAMPLE",
        "LocalGatewayId": "lgw-09b493aa7cEXAMPLE",
        "VpcId": "vpc-07ef66ac71EXAMPLE",
        "State": "associated"
    }
}
```

Connectivité réseau locale pour les racks

Vous avez besoin des composants suivants pour connecter votre rack Outpost à votre réseau sur site :

- Connectivité physique entre le panneau de répartition Outpost et les périphériques du réseau local de votre client.
- Protocole LACP (Link Aggregation Control Protocol) pour établir deux connexions de groupe d'agrégation de liaisons (LAG) vers les périphériques de votre réseau Outpost et vers les périphériques de votre réseau local.
- Connectivité de réseau local virtuel (VLAN) entre l'Outpost et les périphériques du réseau local de votre client.
- point-to-point Connectivité de couche 3 pour chaque VLAN.
- Protocole de passerelle frontière (BGP) pour la publication de la route entre l'Outpost et votre liaison de service sur site.
- BGP pour la publication de la route entre l'Outpost et votre périphérique réseau local sur site pour la connectivité à la passerelle locale.

Table des matières

Connectivité physique

Un rack Outpost possède deux périphériques réseau physiques qui se connectent à votre réseau local.

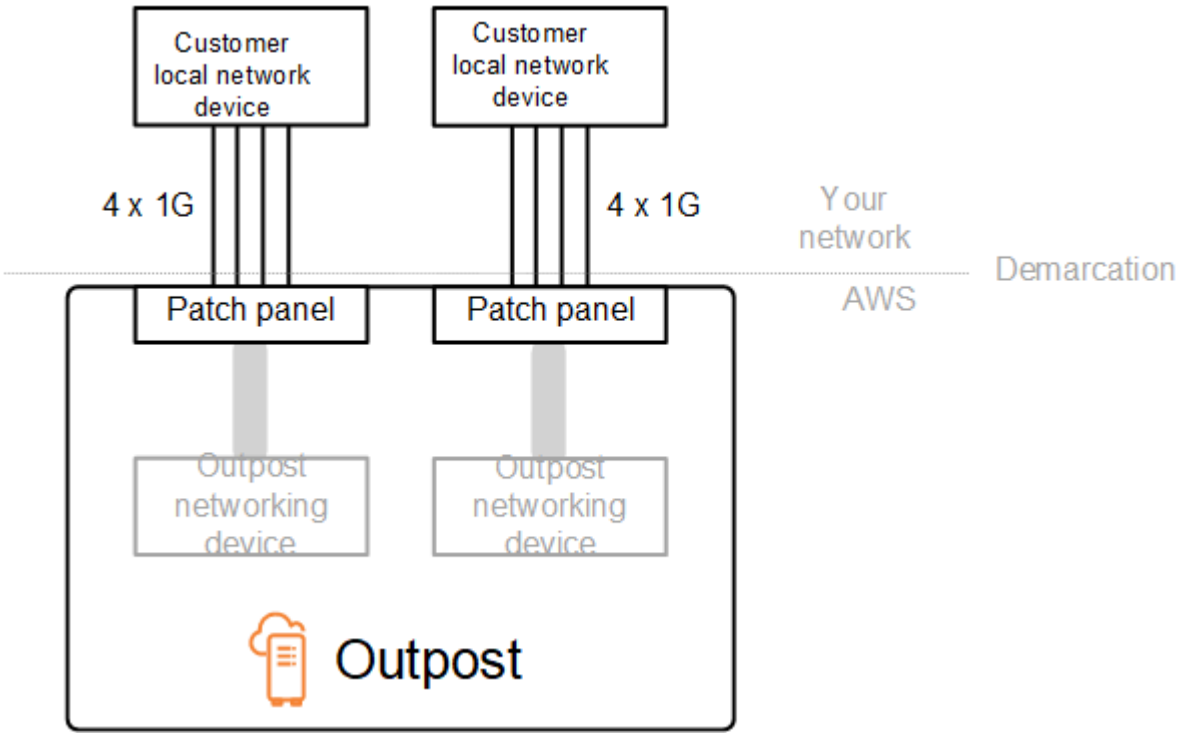
Un Outpost nécessite au moins deux liaisons physiques entre ces périphériques réseau Outpost et les périphériques de votre réseau local. Un Outpost prend en charge les vitesses et quantités de liaison montante suivantes pour chaque périphérique réseau Outpost.

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 Gbit/s ou 100 Gbit/s	1, 2 ou 4

La vitesse et la quantité de liaison montante sont symétriques sur chaque périphérique réseau Outpost. Si vous utilisez 100 Gbit/s comme vitesse de liaison montante, vous devez configurer la liaison avec correction d'erreurs sans voie de retour (FEC CL91).

Les racks Outpost peuvent prendre en charge la fibre monomode (SMF) avec Lucent Connector (LC), la fibre multimode (MMF) ou MMF OM4 avec LC. AWS fournit les dispositifs optiques compatibles avec la fibre que vous indiquez à l'emplacement du rack.

Dans le diagramme suivant, la démarcation physique est le panneau de répartition en fibres de chaque Outpost. Vous fournissez les câbles en fibres nécessaires pour connecter l'Outpost au panneau de répartition.



Agrégation de liaisons

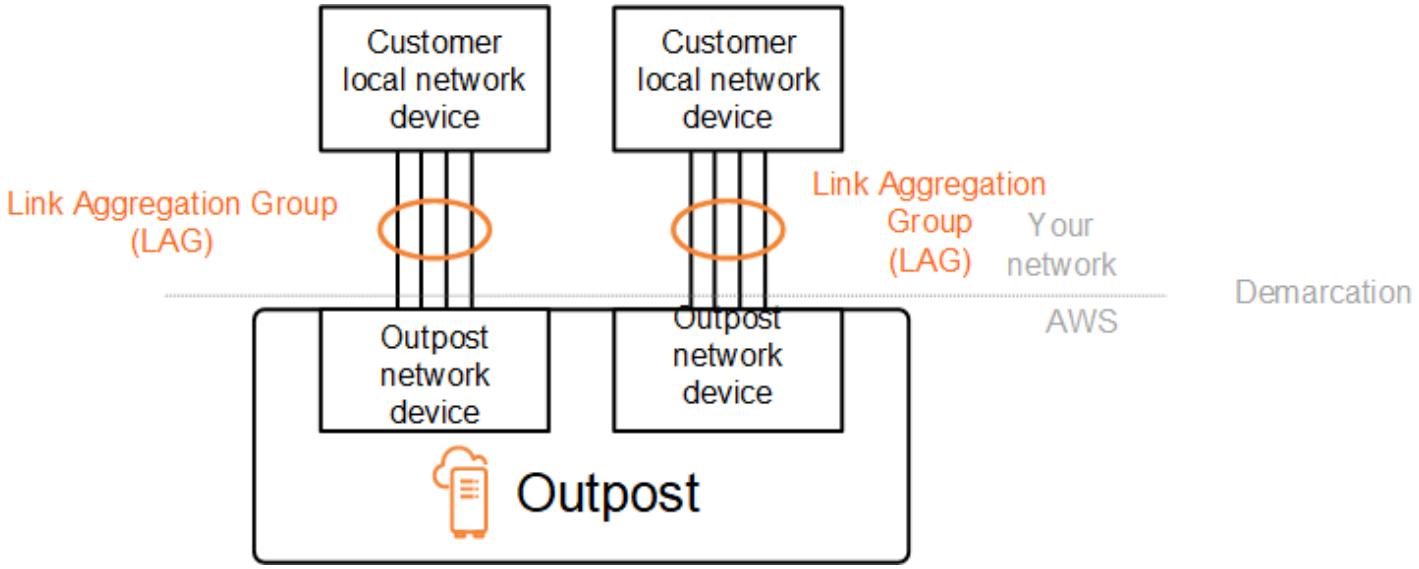
AWS Outposts utilise le protocole LACP (Link Aggregation Control Protocol) pour établir deux connexions de groupe d'agrégation de liaisons (LAG), une entre chaque périphérique réseau Outpost et chaque périphérique réseau local. Les liaisons à partir de chaque périphérique réseau Outpost sont agrégées dans un LAG Ethernet pour représenter une connexion réseau unique. Ces LAG utilisent le protocole LACP avec des minuteurs rapides standard. Vous ne pouvez pas configurer les LAG pour utiliser des minuteurs lents.

Pour activer une installation Outpost sur votre site, vous devez configurer les connexions LAG de votre côté sur vos périphériques réseau.

D'un point de vue logique, ignorez les panneaux de répartition Outpost comme point de démarcation et utilisez les périphériques réseau Outpost.

Pour les déploiements comportant plusieurs racks, un Outpost doit disposer de quatre LAG entre la couche d'agrégation des périphériques réseau Outpost et les périphériques de votre réseau local.

Le diagramme suivant présente quatre connexions physiques entre chaque périphérique réseau Outpost et son périphérique réseau local connecté. Nous utilisons des LAG Ethernet pour agréger les liaisons physiques reliant les périphériques réseau Outpost et les périphériques du réseau local du client.



Réseaux locaux (LAN) virtuels

Chaque LAG entre un périphérique réseau Outpost et un périphérique réseau local doit être configuré en tant que jonction Ethernet IEEE 802.1q. Cela permet d'utiliser plusieurs VLAN pour séparer le réseau entre les chemins de données.

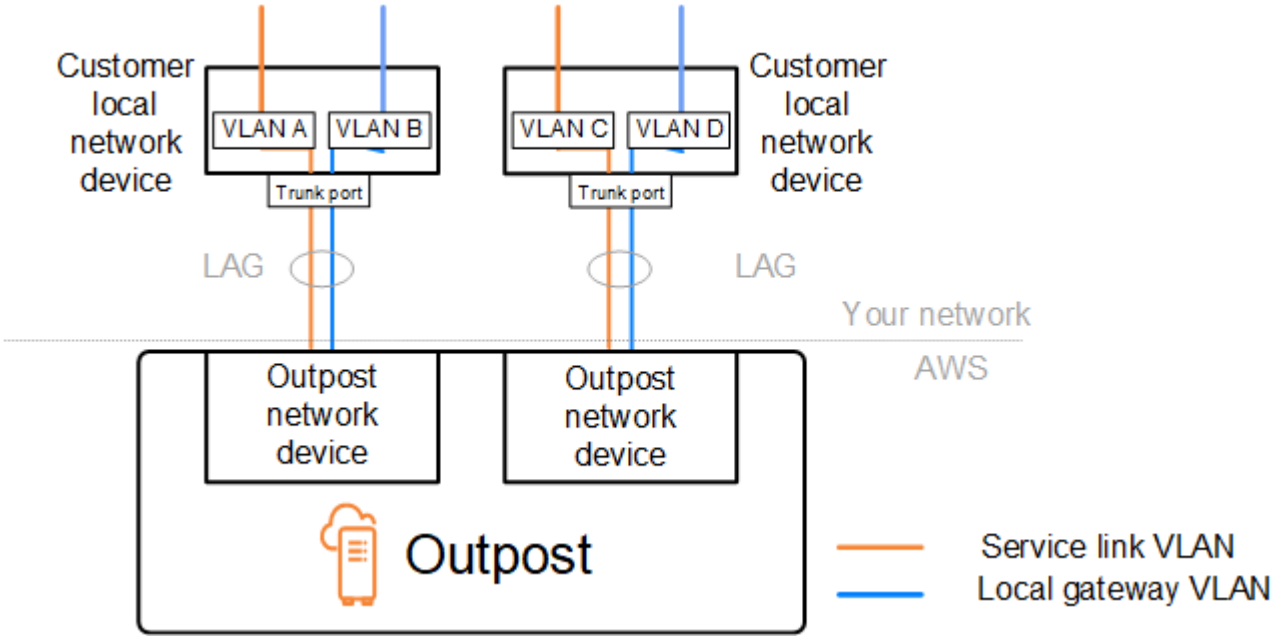
Chaque Outpost dispose des VLAN suivants pour communiquer avec les périphériques de votre réseau local :

- VLAN de liaison de service : permet la communication entre votre Outpost et les périphériques de votre réseau local afin d'établir un chemin de liaison de service pour la connectivité de la liaison de service. Pour plus d'informations, consultez Connectivité AWS Outposts aux régions AWS.
- VLAN de passerelle locale : permet la communication entre votre Outpost et les périphériques de votre réseau local afin d'établir un chemin de passerelle locale pour connecter vos sous-réseaux Outpost et votre réseau local. La passerelle locale Outpost utilise ce VLAN pour fournir à vos instances la connectivité à votre réseau sur site, ce qui peut inclure un accès Internet via votre réseau. Pour plus d'informations, consultez Passerelle locale.

Vous pouvez configurer le VLAN de liaison de service et le VLAN de passerelle locale uniquement entre l'Outpost et les périphériques du réseau local de votre client.

Un Outpost est conçu pour séparer les chemins de données de la liaison de service et de la passerelle locale en deux réseaux isolés. Cela vous permet de choisir lequel de vos réseaux peut communiquer avec les services exécutés sur l'Outpost. Il vous permet également de faire de la

liaison de service un réseau isolé du réseau de passerelle locale en utilisant plusieurs tables de routage sur le périphérique réseau local de votre client, communément appelées instances de routage et de transfert virtuels (VRF). La ligne de démarcation se trouve à l'emplacement du port des périphériques réseau Outpost. AWS gère toutes les infrastructures situées du côté AWS de la connexion, tandis que vous gérez toutes les infrastructures situées de votre côté de la ligne.



Pour intégrer votre Outpost à votre réseau sur site pendant l'installation et le fonctionnement continu, vous devez allouer les VLAN utilisés entre les périphériques réseau Outpost et les périphériques réseau local du client. Vous devez fournir ces informations à AWS avant l'installation. Pour plus d'informations, consultez the section called “Liste de contrôle de préparation du réseau”.

Connectivité de la couche réseau

Pour établir la connectivité de la couche réseau, chaque périphérique réseau Outpost est configuré avec des interfaces virtuelles (VIF) qui incluent l'adresse IP de chaque VLAN. Grâce à ces VIF, les périphériques réseau AWS Outposts peuvent configurer une connectivité IP et des sessions BGP avec votre équipement réseau local.

Nous vous recommandons la procédure suivante :

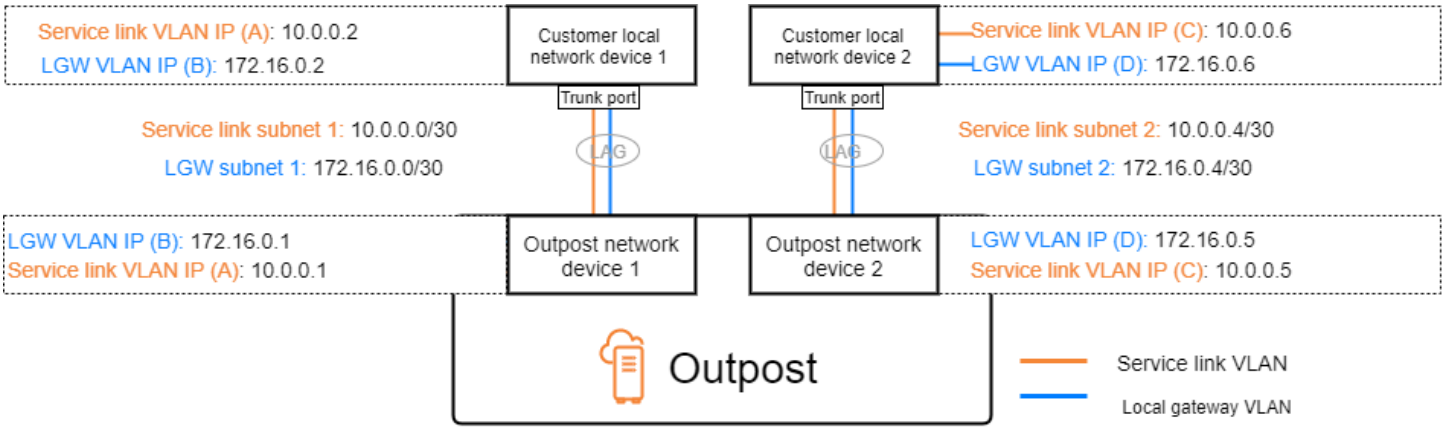
- Utilisez un sous-réseau dédié, avec un CIDR /30 ou /31, pour représenter cette connectivité logique. point-to-point
- Ne connectez pas les VLAN entre les périphériques de votre réseau local.

Pour la connectivité de la couche réseau, vous devez définir deux chemins :

- Chemin de liaison de service : pour définir ce chemin, spécifiez un sous-réseau VLAN avec une plage de /30 ou /31 et une adresse IP pour chaque VLAN de liaison de service sur le périphérique réseau AWS Outposts. Les interfaces virtuelles (VIF) de liaison de service sont utilisées pour que ce chemin établisse une connectivité IP et des sessions BGP entre votre Outpost et les périphériques de votre réseau local pour la connectivité de la liaison de service. Pour plus d'informations, consultez Connectivité AWS Outposts aux régions AWS.
- Chemin de passerelle locale : pour définir ce chemin, spécifiez un sous-réseau VLAN avec une plage de /30 ou /31 et une adresse IP pour le VLAN de passerelle locale sur le périphérique réseau AWS Outposts. Les VIF de passerelle locale sont utilisés sur ce chemin pour établir une connectivité IP et des sessions BGP entre votre Outpost et les périphériques de votre réseau local pour la connectivité de vos ressources locales.

Le diagramme suivant présente les connexions entre chaque périphérique réseau Outpost et le périphérique réseau local du client pour le chemin de liaison de service et le chemin de passerelle locale. Quatre VLAN sont indiqués dans cet exemple :

- Le VLAN A est destiné au chemin de liaison de service qui connecte le périphérique réseau Outpost 1 au périphérique réseau local 1 du client.
- Le VLAN B est destiné au chemin de passerelle locale qui connecte le périphérique réseau Outpost 1 au périphérique réseau local 1 du client.
- Le VLAN C est destiné au chemin de liaison de service qui connecte le périphérique réseau Outpost 2 au périphérique réseau local 2 du client.
- Le VLAN D est destiné au chemin de passerelle locale qui connecte le périphérique réseau Outpost 2 au périphérique réseau local 2 du client.



Le tableau suivant présente des exemples de valeurs pour les sous-réseaux qui connectent le périphérique réseau Outpost 1 au périphérique réseau local 1 du client.

VLAN	Sous-réseau	Adresse IP du périphérique client 1	Adresse IP AWS OND 1
A	10,0.0.0/30	10,0.0.2	10,0.0.1
B	172,16,0,0/30	172,16,0.2	172,16,0.1

Le tableau suivant présente des exemples de valeurs pour les sous-réseaux qui connectent le périphérique réseau Outpost 2 au périphérique réseau local 2 du client.

VLAN	Sous-réseau	Adresse IP du périphérique client 2	Adresse IP AWS OND 2
C	10,0.0.4/30	10.0.0.6	10.0.0.5
D	172,16,0,4/30	172,16,0.6	172.16.0.5

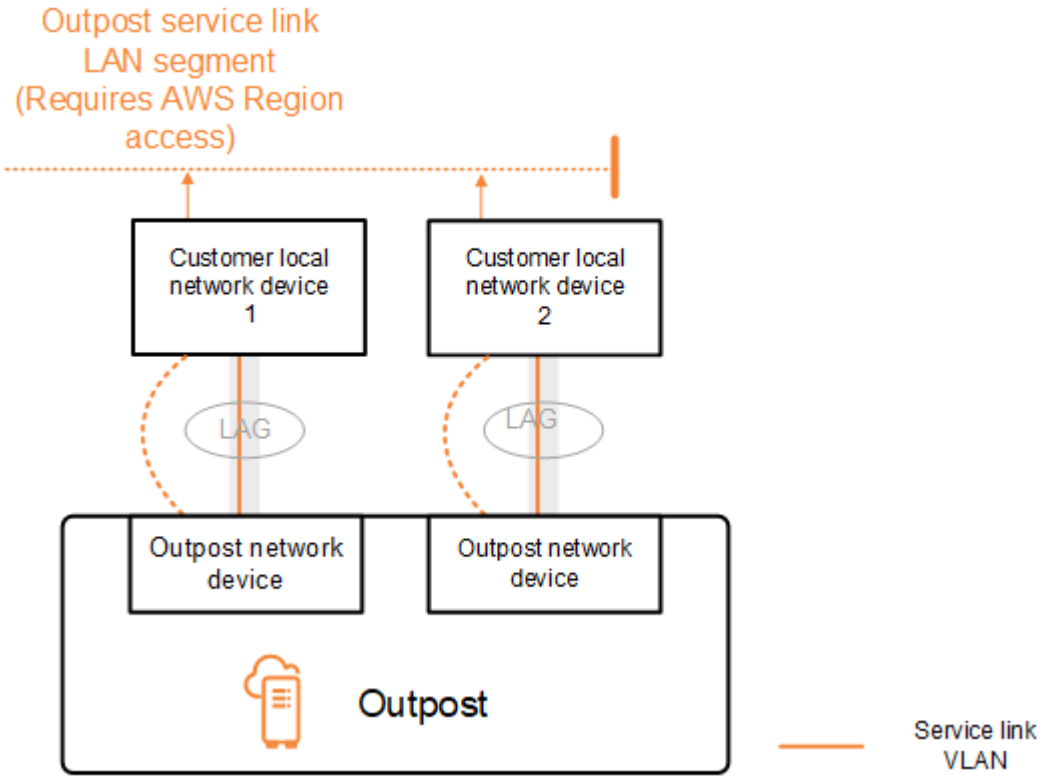
Connectivité BGP de la liaison de service

L'Outpost établit une session d'appairage BGP externe entre chaque périphérique réseau Outpost et le périphérique réseau local du client pour la connectivité de liaison de service via le VLAN de liaison de service. La session d'appairage BGP est établie entre les adresses IP /30 ou /31 fournies pour le VLAN. point-to-point Chaque session d'appairage BGP utilise un numéro de système

autonome (ASN) privé sur le périphérique réseau Outpost et un ASN que vous choisissez pour les périphériques réseau local de votre client. AWS fournit les attributs dans le cadre du processus d'installation.

Imaginons le scénario dans lequel vous avez un Outpost avec deux périphériques réseau Outpost connectés par un VLAN de liaison de service à deux périphériques réseau local du client. Vous configurez l'infrastructure suivante et les attributs ASN BGP du périphérique réseau local du client pour chaque liaison de service :

- L'ASN BGP de la liaison de service. 2 octets (16 bits) ou 4 octets (32 bits). Les valeurs valides sont 64512 à 65535 ou 4200000000 à 4294967294.
- Le CIDR d'infrastructure. Il doit s'agir d'un CIDR /26 par rack.
- L'adresse IP de l'appairage BGP de la liaison de service du périphérique réseau local 1 du client.
- L'ASN de l'appairage BGP de la liaison de service du périphérique réseau local 1 du client. Les valeurs valides sont 1 à 4294967294.
- L'adresse IP de l'appairage BGP de la liaison de service du périphérique réseau local 2 du client.
- L'ASN de l'appairage BGP de la liaison de service du périphérique réseau local 2 du client. Les valeurs valides sont 1 à 4294967294. Pour plus d'informations, consultez RFC4893.



L'Outpost établit une session d'appairage BGP externe via le VLAN de liaison de service en utilisant le processus suivant :

1. Chaque périphérique réseau Outpost utilise l'ASN pour établir une session d'appairage BGP avec son périphérique réseau local connecté.
2. Les périphériques réseau Outpost publient la plage CIDR /26 sous la forme de deux plages CIDR /27 pour prendre en charge les pannes de liaison et de périphérique. Chaque périphérique réseau Outpost (OND) publie son propre préfixe /27 avec une longueur AS-Path de 1, plus les préfixes /27 de tous les autres OND avec une longueur AS-Path de 4 en tant que sauvegarde.
3. Le sous-réseau est utilisé pour la connectivité entre l'Outpost et la région AWS.

Nous vous recommandons de configurer l'équipement réseau du client de sorte qu'il reçoive les annonces BGP d'Outposts sans modification des attributs BGP. Le réseau du client doit privilégier les routes en partance d'Outposts d'une longueur AS-Path de 1 plutôt que les routes d'une longueur AS-Path de 4.

Le réseau du client doit annoncer à tous les appareils OND les mêmes préfixes BGP avec les mêmes attributs. Par défaut, le réseau Outpost équilibre la charge du trafic sortant entre toutes les liaisons ascendantes. Si une maintenance est nécessaire, les politiques de routage sont utilisées côté Outpost pour détourner le trafic d'un appareil OND. Ce détournement de trafic nécessite des préfixes BGP identiques côté client sur tous les appareils OND. Si une maintenance est nécessaire sur le réseau du client, nous vous recommandons d'utiliser l'ajout en préfixe de AS-Path pour détourner temporairement le trafic de certaines liaisons ascendantes.

Publication de sous-réseau d'infrastructure de liaison de service et plage d'adresses IP

Vous fournissez une plage CIDR /26 lors du processus de pré-installation du sous-réseau d'infrastructure de liaison de service. L'infrastructure de l'Outpost utilise cette plage pour établir une connectivité avec la région par le biais de la liaison de service. Le sous-réseau de liaison de service est la source Outpost, qui initie la connectivité.

Les périphériques réseau Outpost publient la plage CIDR /26 sous la forme de deux blocs CIDR /27 pour prendre en charge les pannes de liaison et de périphérique.

Vous devez indiquer un ASN BGP de liaison de service et un CIDR de sous-réseau d'infrastructure (/26) pour l'Outpost. Pour chaque périphérique réseau Outpost, indiquez l'adresse IP d'appairage BGP sur le VLAN du périphérique réseau local et l'ASN BGP du périphérique réseau local.

Si le déploiement est effectué sur plusieurs racks, vous devez disposer d'un sous-réseau /26 par rack.

Connectivité BGP de passerelle locale

L'Outpost établit un appairage BGP externe entre chaque périphérique réseau Outpost et un périphérique réseau local pour la connectivité à la passerelle locale. Il utilise un numéro de système autonome (ASN) privé que vous attribuez afin d'établir les sessions BGP externes. Chaque périphérique réseau Outpost possède un seul appairage BGP externe vers un périphérique réseau local à l'aide de son VLAN de passerelle locale.

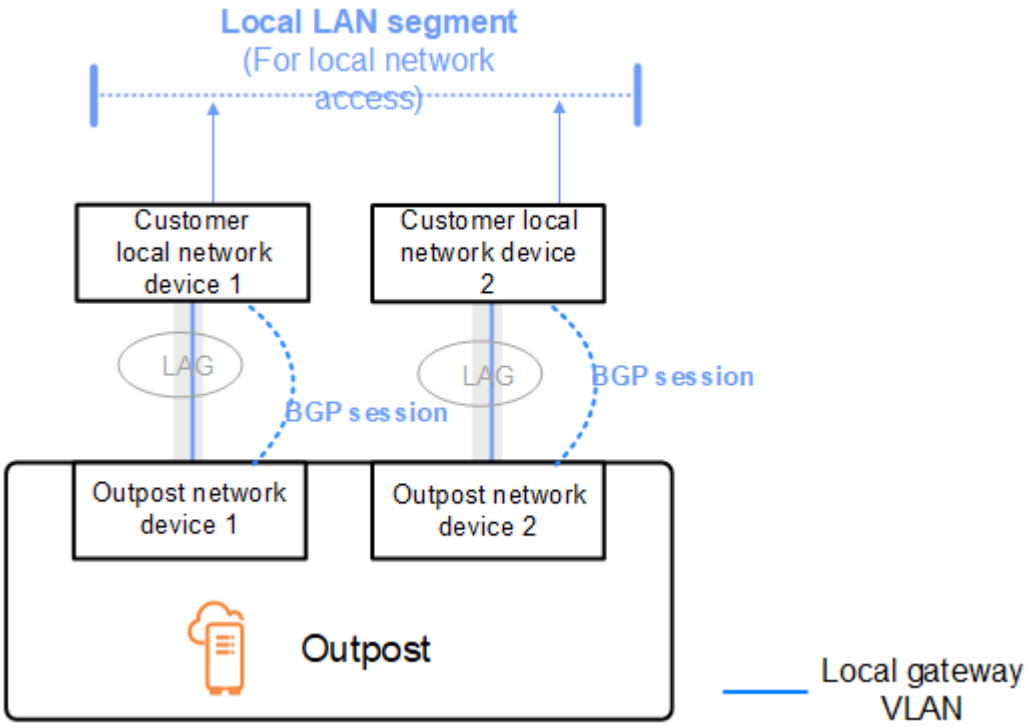
L'Outpost établit une session d'appairage BGP externe via le VLAN de passerelle locale entre chaque périphérique réseau Outpost et le périphérique réseau local connecté de son client. La session d'appairage est établie entre les adresses IP /30 ou /31 que vous avez fournies lors de la configuration de la connectivité réseau et utilise la point-to-point connectivité entre les appareils réseau Outpost et les appareils réseau locaux du client. Pour plus d'informations, consultez the section called "Connectivité de la couche réseau".

Chaque session BGP utilise l'ASN privé pour le périphérique réseau Outpost et un ASN que vous choisissez pour le périphérique réseau local du client. AWS fournit les attributs dans le cadre du processus de pré-installation.

Imaginons le scénario dans lequel vous avez un Outpost avec deux périphériques réseau Outpost connectés par un VLAN de liaison de service à deux périphériques réseau local du client. Vous configurez la passerelle locale suivante et les attributs ASN BGP du périphérique réseau local du client pour chaque liaison de service :

- AWS fournit l'ASN BGP de la passerelle locale. 2 octets (16 bits) ou 4 octets (32 bits). Les valeurs valides sont 64512 à 65535 ou 4200000000 à 4294967294.
- (Facultatif) Vous indiquez le CIDR client qui est publié (public ou privé, /26 minimum).
- Vous indiquez l'adresse IP d'appairage BGP de la passerelle locale du périphérique réseau local 1 du client.
- Vous indiquez l'ASN d'appairage BGP de la passerelle locale du périphérique réseau local 1 du client. Les valeurs valides sont 1 à 4294967294. Pour plus d'informations, consultez RFC4893.

- Vous indiquez l'adresse IP d'appairage BGP de la passerelle locale du périphérique réseau local 2 du client.
- Vous indiquez l'ASN d'appairage BGP de la passerelle locale du périphérique réseau local 2 du client. Les valeurs valides sont 1 à 4294967294. Pour plus d'informations, consultez RFC4893.



Nous vous recommandons de configurer l'équipement réseau du client de sorte qu'il reçoive les annonces BGP d'Outposts sans modification des attributs BGP, et d'activer le multichemin/l'équilibrage de charge BGP afin de bénéficier de flux de trafic entrant optimaux. L'ajout de AS-Path est utilisé pour les préfixes de passerelles locales afin de détourner le trafic des appareils OND dans le cas où une maintenance est nécessaire. Le réseau du client doit privilégier les routes en partance d'Outposts d'une longueur AS-Path de 1 plutôt que les routes d'une longueur AS-Path de 4.

Le réseau du client doit annoncer à tous les appareils OND les mêmes préfixes BGP avec les mêmes attributs. Par défaut, le réseau Outpost équilibre la charge du trafic sortant entre toutes les liaisons ascendantes. Si une maintenance est nécessaire, les politiques de routage sont utilisées côté Outpost pour détourner le trafic d'un appareil OND. Ce détournement de trafic nécessite des préfixes BGP identiques côté client sur tous les appareils OND. Si une maintenance est nécessaire sur le réseau du client, nous vous recommandons d'utiliser l'ajout en préfixe de AS-Path pour détourner temporairement le trafic de certaines liaisons ascendantes.

Publication de sous-réseau IP client de passerelle locale

Par défaut, la passerelle locale utilise les adresses IP privées des instances de votre VPC pour faciliter la communication avec votre réseau sur site. Vous pouvez toutefois indiquer un groupe d'adresses IP clients (CoIP).

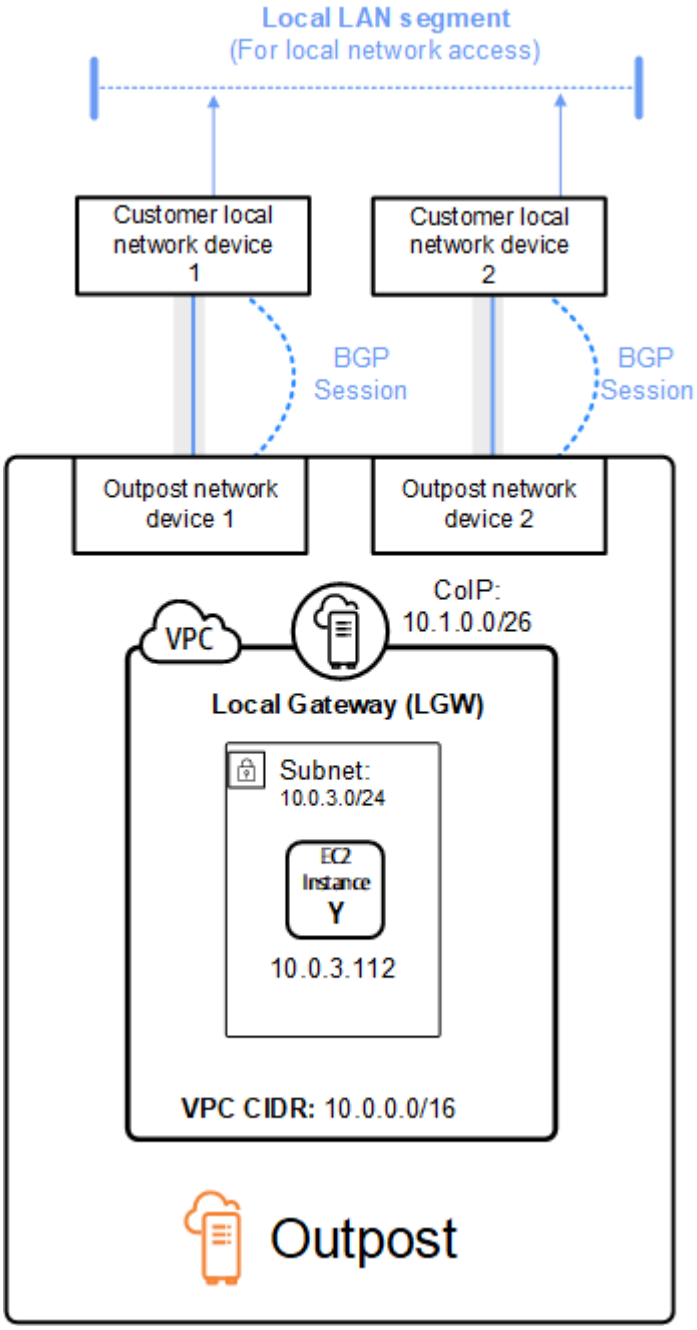
Si vous choisissez CoIP, AWS crée le groupe à partir des informations que vous fournissez lors du processus d'installation. Vous pouvez créer des adresses IP Elastic à partir de ce groupe, puis les attribuer aux ressources de votre Outpost, telles que les instances EC2.

La passerelle locale traduit l'adresse IP Elastic en adresse du groupe client. La passerelle locale publie l'adresse traduite dans votre réseau sur site et dans tout autre réseau communiquant avec l'Outpost. Les adresses sont publiées sur les deux sessions BGP de passerelle locale vers les périphériques réseau local.

> **Tip**
>
> Si vous n'utilisez pas CoIP, BGP publie les adresses IP privées de tous les sous-réseaux de votre Outpost qui ont une route ciblant la passerelle locale dans la table de routage.

Imaginons le scénario dans lequel vous avez un Outpost avec deux périphériques réseau Outpost connectés par un VLAN de liaison de service à deux périphériques réseau local du client. Les paramètres suivants sont configurés :

- Un VPC avec un bloc CIDR 10.0.0.0/16.
- Un sous-réseau dans le VPC avec un bloc CIDR 10.0.3.0/24.
- Une instance EC2 dans le sous-réseau avec une adresse IP privée 10.0.3.112.
- Un groupe d'adresses IP clients (10.1.0.0/26).
- Une association d'adresses IP Elastic qui associe 10.0.3.112 à 10.1.0.2.
- Une passerelle locale qui utilise BGP pour publier 10.1.0.0/26 sur le réseau sur site via les périphériques locaux.
- La communication entre votre Outpost et le réseau sur site utilisera les adresses IP Elastic CoIP pour résoudre les instances de l'Outpost, et la plage CIDR VPC n'est pas utilisée.


Local LAN segment
(For local network access)
Customer local network device 1
Customer local network device 2
BGP Session
BGP Session
Outpost network device 1
Outpost network device 2
CoIP: 10.1.0.0/26
VPC
Local Gateway (LGW)
Subnet: 10.0.3.0/24
EC2 Instance Y
10.0.3.112
VPC CIDR: 10.0.0.0/16
Outpost

Utilisation de AWS Outposts ressources partagées

Grâce au partage d'Outpost, les propriétaires d'Outposts peuvent partager leurs Outposts et leurs ressources, y compris leurs sites et sous-réseaux Outpost, avec d'autres comptes appartenant à la même organisation. AWS AWS En tant que propriétaire d'Outpost, vous pouvez créer et gérer les ressources d'Outpost de manière centralisée, et partager les ressources entre plusieurs AWS comptes au sein de votre AWS organisation. Cela permet aux autres consommateurs d'utiliser les sites Outpost, de configurer des VPC et de lancer et exécuter des instances sur l'Outpost partagé.

Dans ce modèle, le AWS compte propriétaire des ressources Outpost (propriétaire) partage les ressources avec d'autres AWS comptes (consommateurs) de la même organisation. Les consommateurs peuvent créer des ressources sur des Outposts qui sont partagées avec eux de la même manière qu'ils créeraient des ressources sur des Outposts qu'ils créent sur leur propre compte. Le propriétaire est responsable de la gestion de l'avant-poste et des ressources qu'il y crée. Les propriétaires peuvent modifier ou révoquer l'accès partagé à tout moment. À l'exception des instances qui consomment des réservations de capacité, les propriétaires peuvent également consulter, modifier et supprimer les ressources créées par les consommateurs sur des Outposts partagés. Les propriétaires ne peuvent pas modifier les instances lancées par les consommateurs dans des réservations de capacité qu'ils ont partagées.

Les consommateurs sont responsables de la gestion des ressources qu'ils créent sur les Outposts partagés avec eux, y compris les ressources consommant des réservations de capacité. Les consommateurs ne peuvent pas consulter ou modifier les ressources détenues par d'autres consommateurs ou par le propriétaire de l'Outpost. Ils ne peuvent pas non plus modifier les Outposts partagés avec eux.

Le propriétaire d'un Outpost peut partager les ressources de l'Outpost avec :

- AWSComptes spécifiques au sein de son organisation enAWS Organizations.
- Une unité organisationnelle au sein de son organisation enAWS Organizations.
- Toute son organisation enAWS Organizations.

Table des matières

- Partage sur plusieurs zones de disponibilité
- Partage d'une ressource Outpost
- Annulation du partage d'une ressource Outpost
- Identifier une ressource Outpost partagée
- Autorisations relatives aux ressources Shared Outpost
- Facturation et mesures
- Limites

Ressources Outpost partageables

Le propriétaire d'un Outpost peut partager les ressources d'Outpost répertoriées dans cette section avec les consommateurs.

Voici les ressources disponibles pour les rack Outpost. Pour les ressources du serveur, consultez la section Utilisation AWS Outposts des ressources partagées dans le Guide de AWS Outposts l'utilisateur pour les serveurs Outposts.

- Hôtes dédiés alloués — Les consommateurs ayant accès à cette ressource peuvent :
  - Lancez et exécutez des instances EC2 sur un hôte dédié.
- Réservations de capacité — Les consommateurs ayant accès à cette ressource peuvent :
  - Identifiez les réservations de capacité partagées avec eux.
  - Lancez et gérez les instances qui consomment des réservations de capacité.
- Pools d'adresses IP appartenant au client (CoIP) — Les consommateurs ayant accès à cette ressource peuvent :
  - Allouez et associez les adresses IP appartenant aux clients aux instances.
- Tables de routage des passerelles locales — Les consommateurs ayant accès à cette ressource peuvent :
  - Créez et gérez des associations VPC avec une passerelle locale.
  - Affichez les configurations des tables de routage des passerelles locales et des interfaces virtuelles.
- Outposts — Les consommateurs ayant accès à cette ressource peuvent :
  - Créez et gérez des sous-réseaux sur l'Outpost.
  - Créez et gérez des volumes EBS sur l'Outpost.

  - Utilisez l'AWS OutpostsAPI pour consulter les informations relatives à l'Outpost.
- S3 on Outposts — Les consommateurs ayant accès à cette ressource peuvent :
  - Créez et gérez des compartiments, des points d'accès et des points de terminaison S3 sur l'Outpost.
- Sites — Les consommateurs ayant accès à cette ressource peuvent :
  - Créez, gérez et contrôlez un avant-poste sur le site.
- Sous-réseaux — Les consommateurs ayant accès à cette ressource peuvent :
  - Afficher les informations relatives aux sous-réseaux.
  - Lancez et exécutez des instances EC2 dans des sous-réseaux.

  Utilisez la console Amazon VPC pour partager un sous-réseau Outpost. Pour plus d'informations, consultez la section Partage d'un sous-réseau dans le guide de l'utilisateur Amazon VPC.

Conditions préalables au partage des ressources des Outposts

- Pour partager une ressource Outpost avec votre organisation ou une unité organisationnelle dansAWS Organizations, vous devez activer le partage avecAWS Organizations. Pour plus d'informations, veuillez consulter Activation du partage avec AWS Organizations dans le Guide de l'utilisateur AWS RAM.
- Pour partager une ressource Outpost, vous devez la posséder dans votre AWS compte. Vous ne pouvez pas partager une ressource Outpost qui a été partagée avec vous.
- Pour partager une ressource Outpost, vous devez la partager avec un compte appartenant à votre organisation.

Services connexes

Le partage de ressources Outpost s'intègre à AWS Resource Access Manager (AWS RAM). AWS RAMest un service qui vous permet de partager vos AWS ressources avec n'importe quel AWS compte ou viaAWS Organizations. Avec AWS RAM, vous pouvez partager des ressources dont vous êtes propriétaire en créant un partage de ressources. Un partage de ressources spécifie les ressources à partager, ainsi que les consommateurs avec qui elles seront partagées. Les consommateurs peuvent être AWS des comptes individuels, des unités organisationnelles ou une organisation entièreAWS Organizations.

Pour plus d'informations sur AWS RAM, consultez le Guide de l'utilisateur AWS RAM.

Partage sur plusieurs zones de disponibilité

Pour garantir que les ressources sont réparties entre les zones de disponibilité d'une région, nous mappons indépendamment les zones de disponibilité aux noms de chaque compte. Cela peut entraîner des différences de nom de zone de disponibilité entre les comptes. Par exemple, la zone de disponibilité `us-east-1a` pour votre compte AWS peut avoir un emplacement autre que `us-east-1a` pour un autre compte AWS.

Pour identifier l'emplacement de votre ressource Outpost par rapport à vos comptes, vous devez utiliser l'ID de zone de disponibilité (AZ ID). L'ID de zone de disponibilité est un identifiant unique et cohérent pour une zone de disponibilité entre tous les comptes AWS. Par exemple, `use1-az1` est l'ID de zone de disponibilité de la région `us-east-1` et dont l'emplacement est identique dans chaque compte AWS.

Pour afficher les ID de zone de disponibilité pour votre compte

1. Ouvrez la console AWS RAM à l'adresse https://console.aws.amazon.com/ram.
2. Les ID de zone de disponibilité pour la région actuelle sont affichés dans le volet Your AZ ID (Votre ID de zone de disponibilité) dans la partie droite de l'écran.

> **Note**
>
> Les tables de routage des passerelles locales se trouvent dans la même zone AZ que leur avant-poste. Il n'est donc pas nécessaire de spécifier un ID AZ pour les tables de routage.

Partage d'une ressource Outpost

Lorsqu'un propriétaire partage un Outpost avec un consommateur, celui-ci peut créer des ressources sur l'Outpost de la même manière qu'il créerait des ressources sur des Outposts qu'il créerait sur son propre compte. Les consommateurs ayant accès à des tables de routage de passerelles locales partagées peuvent créer et gérer des associations VPC. Pour plus d'informations, veuillez consulter Ressources Outpost partageables.

Pour partager une ressource Outpost, vous devez l'ajouter à un partage de ressources. Un partage de ressources est une ressource AWS RAM qui vous permet de partager vos ressources entre

des comptes AWS. Un partage de ressources spécifie les ressources à partager, ainsi que les consommateurs avec qui elles seront partagées. Lorsque vous partagez une ressource Outpost à l'aide de la AWS Outposts console, vous l'ajoutez à un partage de ressources existant. Pour ajouter la ressource Outpost à un nouveau partage de ressources, vous devez d'abord créer le partage de ressources à l'aide de la AWS RAMconsole.

Si vous faites partie d'une organisation AWS Organizations et que le partage au sein de votre organisation est activé, vous pouvez autoriser les clients de votre organisation à accéder à la ressource Outpost partagée depuis la AWS RAM console. Dans le cas contraire, les consommateurs reçoivent une invitation à rejoindre le partage de ressources et ont accès à la ressource Outpost partagée après avoir accepté l'invitation.

Vous pouvez partager une ressource Outpost dont vous êtes propriétaire à l'aide de la AWS Outposts console, de AWS RAM la console ou duAWS CLI.

Pour partager un Outpost dont vous êtes propriétaire à l'aide de la console AWS Outposts

1. Ouvrez la console AWS Outposts à l'adresse https://console.aws.amazon.com/outposts/.
2. Dans le volet de navigation, choisissez Outposts.
3. Sélectionnez l'avant-poste, puis choisissez Actions, Afficher les détails.
4. Sur la page récapitulative d'Outpost, sélectionnez Resource shares.
5. Choisissez Créer une ressource.

Vous êtes redirigé vers la AWS RAM console pour terminer le partage de l'Outpost en suivant la procédure suivante. Pour partager une table de routage de passerelle locale dont vous êtes le propriétaire, suivez également la procédure suivante.

Pour partager une table de routage d'Outpost ou de passerelle locale dont vous êtes propriétaire à l'aide de la console AWS RAM

Consultez Création d'un partage de ressources dans le Guide de l'utilisateur AWS RAM.

Pour partager une table de routage d'Outpost ou de passerelle locale dont vous êtes propriétaire à l'aide du AWS CLI

Utilisez la commande create-resource-share.

Annulation du partage d'une ressource Outpost

Lorsqu'un avant-poste partagé n'est plus partagé, les consommateurs ne peuvent plus voir l'avant-poste dans la console. AWS Outposts Ils ne peuvent pas créer de nouveaux sous-réseaux sur l'Outpost, créer de nouveaux volumes EBS sur l'Outpost ou consulter les détails de l'Outpost et les types d'instances à l'aide de la console ou du. AWS Outposts AWS CLI Les sous-réseaux, volumes ou instances existants créés par les consommateurs ne sont pas supprimés. Tous les sous-réseaux existants créés par les consommateurs sur l'Outpost peuvent toujours être utilisés pour lancer de nouvelles instances.

Lorsqu'une table de routage de passerelle locale partagée n'est plus partagée, les consommateurs ne peuvent plus créer de nouvelles associations VPC avec celle-ci. Toutes les associations VPC existantes créées par les consommateurs restent associées à la table de routage. Les ressources de ces VPC peuvent continuer à acheminer le trafic vers la passerelle locale.

Pour annuler le partage d'une ressource Outpost dont vous êtes propriétaire, vous devez la supprimer du partage de ressources. Pour ce faire, vous pouvez utiliser soit la console AWS RAM, soit l'AWS CLI.

Pour annuler le partage d'une ressource Outpost partagée dont vous êtes propriétaire à l'aide de la console AWS RAM

Consultez Mise à jour d'un partage de ressources dans le Guide de l'utilisateur AWS RAM.

Pour annuler le partage d'une ressource Outpost partagée dont vous êtes propriétaire à l'aide du AWS CLI

Utilisez la commande disassociate-resource-share.

Identifier une ressource Outpost partagée

Les propriétaires et les consommateurs peuvent identifier les Outposts partagés à l'aide de la AWS Outposts console et. AWS CLI Ils peuvent identifier les tables de routage des passerelles locales partagées à l'aide duAWS CLI.

Pour identifier un avant-poste partagé à l'aide de la console AWS Outposts

1. Ouvrez la console AWS Outposts à l'adresse https://console.aws.amazon.com/outposts/.
2. Dans le volet de navigation, choisissez Outposts.

3. Sélectionnez l'avant-poste, puis choisissez Actions, Afficher les détails.
4. Sur la page récapitulative de l'Outpost, consultez l'ID du propriétaire pour identifier le numéro de AWS compte du propriétaire de l'Outpost.

Pour identifier une ressource Outpost partagée à l'aide du AWS CLI

Utilisez les commandes list-outposts et describe-local-gateway-route -tables. Ces commandes renvoient les ressources Outpost que vous possédez et les ressources Outpost partagées avec vous. `OwnerId`indique l'ID de AWS compte du propriétaire de la ressource Outpost.

Autorisations relatives aux ressources Shared Outpost

Autorisations accordées aux propriétaires

Les propriétaires sont responsables de la gestion de l'avant-poste et des ressources qu'ils y créent. Les propriétaires peuvent modifier ou révoquer l'accès partagé à tout moment. Ils peuvent les utiliser AWS Organizations pour afficher, modifier et supprimer les ressources créées par les consommateurs sur des Outposts partagés.

Autorisations accordées aux consommateurs

Les consommateurs peuvent créer des ressources sur des Outposts qui sont partagées avec eux de la même manière qu'ils créeraient des ressources sur des Outposts qu'ils créent sur leur propre compte. Les consommateurs sont responsables de la gestion des ressources qu'ils lancent sur les Outposts et qu'ils partagent avec eux. Les consommateurs ne peuvent pas consulter ou modifier les ressources détenues par d'autres consommateurs ou par le propriétaire de l'Outpost, et ils ne peuvent pas modifier les Outposts partagés avec eux.

Facturation et mesures

Les propriétaires sont facturés pour les Outposts et les ressources des Outposts qu'ils partagent. Les frais de transfert de données associés au trafic VPN de la liaison de service de leur Outpost en provenance de la Région leur sont également facturés. AWS

Aucuns frais supplémentaires ne sont facturés pour le partage des tables de routage des passerelles locales. Pour les sous-réseaux partagés, le propriétaire du VPC est facturé pour les ressources de niveau VPC AWS Direct Connect telles que les connexions VPN, les passerelles NAT et les connexions de liaison privée.

Les consommateurs sont facturés pour les ressources applicatives qu'ils créent sur des Outposts partagés, telles que les équilibreurs de charge et les bases de données Amazon RDS. Les consommateurs sont également facturés pour les transferts de données payants depuis la AWS Région.

Limites

Les restrictions suivantes s'appliquent à l'utilisation du AWS Outposts partage :

- Les limites relatives aux sous-réseaux partagés s'appliquent à l'utilisation du AWS Outposts partage. Pour plus d'informations sur les limites de partage VPC, consultez la section Limitations du guide de l'utilisateur d'Amazon Virtual Private Cloud.
- Les quotas de service sont appliqués à chaque compte individuel.

Sécurité dans AWS Outposts

La sécurité AWS est la priorité absolue. En tant que AWS client, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit ceci comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services 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 notre sécurité dans le cadre des programmes de AWS conformité Programmes de de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS Outposts, voir AWS Services concernés par programme de conformitéAWS .
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Pour plus d'informations sur la sécurité et la conformité des serveurs AWS Outposts, consultez la FAQ sur en AWS Outposts rack.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de son utilisation AWS Outposts. Elle vous montre comment atteindre vos objectifs en matière de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos ressources.

Table des matières

Protection des données dans AWS Outposts

Le modèle de responsabilité AWS partagée de s'applique à la protection des données dans AWS Outposts. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. 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 IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches.

Pour en savoir plus sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

Chiffrement au repos

Avec AWS Outposts, toutes les données sont cryptées au repos. Les éléments de clé sont encapsulés dans une clé externe stockée dans un dispositif amovible : la clé de sécurité Nitro (NSK). La clé NSK est nécessaire pour déchiffrer les données sur vos serveurs 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. Pour plus d'informations, consultez Chiffrement Amazon EBS dans le Guide de l'utilisateur Amazon EC2.

Chiffrement en transit

AWS chiffre les données en transit entre votre avant-poste et sa région. AWS Pour plus d'informations, consultez Connectivité via les liaisons de service.

Vous pouvez utiliser un protocole de chiffrement, tel que TLS (Transport Layer Security), pour chiffrer les données sensibles en transit via la passerelle locale à destination de votre réseau local.

Suppression de données

Lorsque vous arrêtez ou résiliez une instance EC2, la mémoire qui lui est allouée est nettoyée (remise à zéro) par l'hyperviseur avant d'être allouée à une nouvelle instance, et chaque bloc de stockage est réinitialisé.

La destruction par chiffrement de la clé de sécurité Nitro déchiquette les données sur votre Outpost.

Gestion des identités et des accès (IAM) pour AWS Outposts

AWS Identity and Access Management (IAM) est un AWS service 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. Vous pouvez utiliser IAM sans frais supplémentaires.

Table des matières

Comment AWS Outposts fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès aux AWS Outposts, découvrez quelles fonctionnalités IAM peuvent être utilisées avec Outposts. AWS

Fonctionnalités IAM que vous pouvez utiliser avec Outposts AWS

Fonction IAM	AWS Soutien aux Outposts
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Oui

Fonction IAM	AWS Soutien aux Outposts
Clés de condition de politique (spécifiques au service)	Oui
ACL	Non
ABAC (étiquettes dans les politiques)	Oui
Informations d'identification temporaires	Oui
Autorisations de principal	Oui
Fonctions du service	Non
Rôles liés à un service	Oui

Politiques basées sur l'identité pour les Outposts AWS

Prend en charge les politiques basées sur l'identité	Oui

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un Groupes d'utilisateurs IAM ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, veuillez consulter Création de politiques IAM dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité car celle-ci s'applique à l'utilisateur ou au rôle auquel elle est attachée. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Exemples de politiques basées sur l'identité pour les Outposts AWS

Pour voir des exemples de politiques basées sur l'identité AWS des Outposts, consultez. AWS Exemples de politiques relatives aux Outposts

Politiques basées sur les ressources au sein d'Outposts AWS

Prend en charge les politiques basées sur les ressources	Non

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment Amazon S3. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. L'ajout d'un principal entre comptes à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource sont différents Comptes AWS, un administrateur IAM du compte sécurisé doit également accorder à l'entité principale (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur une identité à l'entité. Toutefois, si une politique basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. Pour plus d'informations, consultez Différence entre les rôles IAM et les politiques basées sur une ressource dans le Guide de l'utilisateur IAM.

Actions politiques pour les AWS Outposts

Prend en charge les actions de politique	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Les actions de stratégie portent généralement le même nom que l'opération AWS d'API associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une stratégie afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des actions d' AWS Outposts, consultez la section Actions définies par AWS Outposts dans la référence d'autorisation de service.

Les actions politiques dans AWS Outposts utilisent le préfixe suivant avant l'action :

```
outposts
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

```
"Action": [
    "outposts:action1",
    "outposts:action2"
]
```

Vous pouvez aussi spécifier plusieurs actions à l'aide de caractères génériques (*). Par exemple, pour spécifier toutes les actions qui commencent par le mot `List`, incluez l'action suivante :

```
"Action": "outposts:List*"
```

Ressources politiques pour les AWS Outposts

Prend en charge les ressources de politique	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets pour lesquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Certaines actions de l'API AWS Outposts prennent en charge plusieurs ressources. Pour spécifier plusieurs ressources dans une seule instruction, séparez leurs ARN par des virgules.

```
"Resource": [
    "resource1",
    "resource2"
]
```

Pour consulter la liste des types de ressources des AWS Outposts et de leurs ARN, consultez la section Types de ressources définis par AWS Outposts dans la référence d'autorisation de service. Pour savoir grâce à quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez Actions définies par AWS Outposts.

Clés de conditions politiques pour les AWS Outposts

Prend en charge les clés de condition de politique spécifiques au service	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une `OR` opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour plus d'informations, consultez Éléments d'une politique IAM : variables et identifications dans le Guide de l'utilisateur IAM.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

Pour consulter la liste des clés de condition des AWS Outposts, voir Clés de condition pour AWS Outposts la référence d'autorisation de service. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez la section Actions définies par AWS Outposts.

Pour voir des exemples de politiques basées sur l'identité AWS des Outposts, consultez. AWS Exemples de politiques relatives aux Outposts

ACL dans les Outposts AWS

Prend en charge les listes ACL	Non

Les listes de contrôle d'accès (ACL) vérifient quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

ABAC avec Outposts AWS

Prend en charge ABAC (étiquettes dans les politiques)	Oui

Le contrôle d'accès par attributs (ABAC) est une stratégie d'autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et à de nombreuses AWS ressources. L'étiquetage des entités et des ressources est la première étape d'ABAC. Vous concevez ensuite des politiques ABAC pour autoriser des opérations quand l'identification du principal correspond à celle de la ressource à laquelle il tente d'accéder.

L'ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas où la gestion des politiques devient fastidieuse.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informations sur l'ABAC, consultez Qu'est-ce que le contrôle d'accès basé sur les attributs (ABAC) ? dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez Utilisation du contrôle d'accès basé sur les attributs (ABAC) dans le Guide de l'utilisateur IAM.

Utiliser des informations d'identification temporaires avec AWS Outposts

Prend en charge les informations d'identification temporaires	Oui

Certains Services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui Services AWS fonctionnent avec des informations d'identification temporaires, consultez Services AWS la section relative à l'utilisation d'IAM dans le guide de l'utilisateur d'IAM.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez Changement de rôle (console) dans le Guide de l'utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l' AWS API AWS CLI or. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires dans IAM.

Autorisations principales interservices pour les Outposts AWS

Prend en charge les transmissions de sessions d'accès (FAS)	Oui

Lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, l'action que vous effectuez est susceptible de lancer une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transmission des sessions d'accès.

Fonctions du service pour AWS Outposts

Prend en charge les fonctions de service	Non

Une fonction du service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM.

Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

Rôles liés à un service pour les Outposts AWS

Prend en charge les rôles liés à un service.	Oui

Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Pour plus de détails sur la création ou la gestion des AWS rôles liés aux services Outposts, consultez. Utilisation des rôles liés aux services pour AWS Outposts

AWS Exemples de politiques relatives aux Outposts

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier les ressources d' AWS Outposts. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l'API AWS Management Console, AWS Command Line Interface (AWS CLI) ou de AWS l'API. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM doit créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques dans l'onglet JSON dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par AWS Outposts, y compris le format des ARN pour chacun des types de ressources, voir Actions, ressources et clés de condition AWS Outposts dans la référence d'autorisation de service.

Table des matières

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer des ressources AWS Outposts dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour de plus amples informations, consultez Politiques gérées AWS ou Politiques gérées AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Accorder les autorisations de moindre privilège - Lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation de IAM pour appliquer des autorisations, consultez Politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utiliser des conditions dans les politiques IAM pour restreindre davantage l'accès - Vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez IAM Access Analyzer pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles - IAM Access Analyzer valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour de plus amples informations, consultez Validation de politique IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue.

Compte AWS Pour exiger le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour de plus amples informations, consultez Configuration de l'accès aux API protégé par MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Exemple : Utilisation d'autorisations au niveau des ressources

L'exemple suivant utilise des autorisations au niveau des ressources pour accorder l'autorisation d'obtenir des informations sur l'Outpost spécifié.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "outposts:GetOutpost",
      "Resource": "arn:aws:outposts:region:12345678012:outpost/op-1234567890abcdef0"
    }
  ]
}
```

L'exemple suivant utilise des autorisations au niveau des ressources pour accorder l'autorisation d'obtenir des informations sur le site spécifié.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "outposts:GetSite",
      "Resource": "arn:aws:outposts:region:12345678012:site/os-0abcdef1234567890"
    }
  ]
}
```

Utilisation des rôles liés aux services pour AWS Outposts

AWS Outposts utilise des AWS Identity and Access Management rôles liés à un service (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à. AWS Outposts Les rôles liés au

service sont prédéfinis par AWS Outposts et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom.

Un rôle lié à un service rend votre configuration AWS Outposts plus efficace, car vous n'avez pas à ajouter manuellement les autorisations nécessaires. AWS Outposts définit les autorisations associées à ses rôles liés aux services et, sauf indication contraire, seul AWS Outposts peut assumer ses rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable des ressources connexes. Cela protège vos AWS Outposts ressources car vous ne pouvez pas supprimer par inadvertance l'autorisation d'accès aux ressources.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés aux services, consultez Services AWS fonctionnant avec IAM et recherchez les services où Oui figure dans la colonne Rôle lié à un service. Sélectionnez un Oui ayant un lien pour consulter la documentation du rôle lié à un service, pour ce service.

Autorisations des rôles liés à un service pour AWS Outposts

AWS Outposts utilise le rôle lié au service nommé AWSServiceRoleForOutposts_ ***OutpostID – Permet aux Outposts*** d' AWS accéder aux ressources pour une connectivité privée en votre nom. Ce rôle lié à un service permet de configurer la connectivité privée, de créer des interfaces réseau et de les attacher à des instances de point de terminaison de la liaison de service.

Le rôle lié au service AWSServiceRoleForOutposts _ *OutpostID* fait confiance aux services suivants pour assumer le rôle :

- `outposts.amazonaws.com`

Le rôle lié au service AWSServiceRoleForOutposts_ ***OutpostID*** inclut les politiques suivantes :

- AWSOutpostsServiceRolePolicy
- AWSOutpostsPrivateConnectivityPolicy_ ***OutPostID***

La AWSOutpostsServiceRolePolicypolitique est une politique de rôle liée au service qui permet d'accéder aux AWS ressources gérées par. AWS Outposts

Cette politique permet AWS Outposts d'effectuer les actions suivantes sur les ressources spécifiées :

- Action : `ec2:DescribeNetworkInterfaces` sur `all AWS resources`
- Action : `ec2:DescribeSecurityGroups` sur `all AWS resources`
- Action : `ec2:CreateSecurityGroup` sur `all AWS resources`
- Action : `ec2:CreateNetworkInterface` sur `all AWS resources`

La politique AWSOutpostsPrivateConnectivityPolicy_ ***OutpostID*** permet d' AWS Outposts effectuer les actions suivantes sur les ressources spécifiées :

- Action : `ec2:AuthorizeSecurityGroupIngress` sur `all AWS resources that match the following Condition:`

```
{ "StringLike" : { "ec2:ResourceTag/outposts:private-connectivity-resourceId" :
 "OutpostID" }} and { "StringEquals" : { "ec2:Vpc" : "vpcArn" }}
```

- Action : `ec2:AuthorizeSecurityGroupEgress` sur `all AWS resources that match the following Condition:`

```
{ "StringLike" : { "ec2:ResourceTag/outposts:private-connectivity-resourceId" :
 "OutpostID" }} and { "StringEquals" : { "ec2:Vpc" : "vpcArn" }}
```

- Action : `ec2:CreateNetworkInterfacePermission` sur `all AWS resources that match the following Condition:`

```
{ "StringLike" : { "ec2:ResourceTag/outposts:private-connectivity-resourceId" :
 "OutpostID" }} and { "StringEquals" : { "ec2:Vpc" : "vpcArn" }}
```

- Action : `ec2:CreateTags` sur `all AWS resources that match the following Condition:`

```
{ "StringLike" : { "aws:RequestTag/outposts:private-connectivity-resourceId" :
 "{{OutpostId}}*"}}
```

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez Service-Linked Role Permissions (autorisations du rôle lié à un service) dans le IAM User Guide (guide de l'utilisateur IAM).

Création d'un rôle lié à un service pour AWS Outposts

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous configurez la connectivité privée pour votre Outpost dans le AWS Management Console, AWS Outposts crée le rôle lié au service pour vous.

Pour plus d'informations, consultez Connectivité privée de la liaison de service avec VPC.

Modification d'un rôle lié à un service pour AWS Outposts

AWS Outposts ne vous permet pas de modifier le rôle lié au AWSServiceRoleForOutposts service _ *`OutpostID`*. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, consultez Editing a Service-Linked Role (Modification d'un rôle lié à un service) dans le Guide de l'utilisateur IAM.

Suppression d'un rôle lié à un service pour AWS Outposts

Si vous n'avez plus besoin d'utiliser une fonctionnalité ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous évitez d'avoir une entité inutilisée non surveillée ou non gérée activement. Cependant, vous devez nettoyer les ressources de votre rôle lié à un service avant de pouvoir les supprimer manuellement.

> **Note**
>
> Si le AWS Outposts service utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression risque d'échouer. Si cela se produit, patientez quelques minutes et réessayez.

> **Warning**
>
> Vous devez supprimer votre Outpost avant de pouvoir supprimer le rôle lié au service AWSServiceRoleForOutposts _ *`OutpostID`*. La procédure suivante permet de supprimer votre Outpost.

Avant de commencer, assurez-vous que votre Outpost n'est pas partagé à l'aide de AWS Resource Access Manager (AWS RAM). Pour plus d'informations, consultez Annulation du partage d'une ressource Outpost.

Pour supprimer les AWS Outposts ressources utilisées par le AWSServiceRoleForOutposts _ ***OutpostID***

- Contactez le Support aux AWS entreprises pour supprimer votre Outpost.

Pour supprimer manuellement le rôle lié à un service à l'aide d'IAM

Utilisez la console IAM, le AWS CLI, ou l' AWS API pour supprimer le rôle lié au service AWSServiceRoleForOutposts _ *OutpostID*. Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles liés à un service AWS Outposts

AWS Outposts prend en charge l'utilisation de rôles liés au service dans toutes les régions où le service est disponible. Pour plus d'informations, consultez Points de terminaison et quotas AWS Outposts.

AWS politiques gérées pour AWS Outposts

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les politiques gérées sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont accessibles à tous les AWS clients. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWS est le plus susceptible de mettre à jour une politique AWS gérée lorsqu'une nouvelle Service AWS est lancée ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

Pour plus d'informations, consultez la section Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

AWS politique gérée : AWSOutpostsServiceRolePolicy

Cette politique est associée à un rôle lié à un service qui permet d' AWS Outposts effectuer des actions en votre nom. Pour plus d'informations, consultez Utilisation des rôles liés aux services.

AWS politique gérée : AWSOutpostsPrivateConnectivityPolicy

Cette politique est associée à un rôle lié à un service qui permet d' AWS Outposts effectuer des actions en votre nom. Pour plus d'informations, consultez Utilisation des rôles liés aux services.

AWS Outposts mises à jour des politiques AWS gérées

Consultez les détails des mises à jour des politiques AWS gérées AWS Outposts depuis que ce service a commencé à suivre ces modifications.

Modification	Description	Date
AWS Outposts a commencé à suivre les modifications	AWS Outposts a commencé à suivre les modifications apportées AWS à ses politiques gérées.	3 décembre 2019

Sécurité de l'infrastructure dans AWS Outposts

En tant que service géré, AWS Outposts est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section Sécurité du AWS cloud. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder aux AWS Outposts via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Pour plus d'informations sur la sécurité de l'infrastructure fournie pour les instances EC2 et les volumes EBS s'exécutant sur votre Outpost, consultez Sécurité de l'infrastructure dans Amazon EC2.

Les journaux de flux VPC fonctionnent de la même manière que dans une AWS région. Cela signifie qu'ils peuvent être publiés sur CloudWatch Logs, Amazon S3 ou Amazon à des GuardDuty fins d'analyse. Les données doivent être renvoyées à la région pour publication auprès de ces services, afin qu'elles ne soient pas visibles depuis CloudWatch ou vers d'autres services lorsque l'avant-poste est déconnecté.

Surveillance des altérations sur les équipements AWS Outposts

Assurez-vous que personne ne modifie, n'altère, ne fait d'ingénierie inverse ou n'altère l'équipement. AWS Outposts AWS Outposts l'équipement peut être équipé d'un système de surveillance des altérations afin de garantir le respect des conditions AWS de service.

Résilience dans AWS Outposts

AWS Outposts est conçu pour être hautement disponible. Les racks Outpost ont été conçus avec des équipements d'alimentation et de réseau redondants. Pour une résilience accrue, nous vous recommandons de prévoir deux sources d'alimentation et une connectivité réseau redondante pour votre Outpost.

Pour bénéficier d'une haute disponibilité, vous pouvez provisionner une capacité intégrée supplémentaire toujours active sur le rack Outposts. Les configurations de capacité Outpost ont été conçues pour être exploitées dans des environnements de production et prennent en charge N+1 instances pour chaque famille d'instances lorsque vous provisionnez de la capacité à cet effet. AWS recommande d'allouer une capacité supplémentaire suffisante pour vos applications critiques, afin de permettre une récupération et un basculement en cas de problème sur l'hôte sous-jacent. Vous pouvez utiliser les indicateurs de disponibilité des CloudWatch capacités d'Amazon et définir des alarmes pour surveiller l'état de vos applications, créer des CloudWatch actions pour configurer les options de restauration automatique et surveiller l'utilisation de la capacité de vos Outposts au fil du temps.

Lorsque vous créez un avant-poste, vous sélectionnez une zone de disponibilité AWS dans une région. Cette zone de disponibilité prend en charge les opérations de plan de contrôle, notamment la réponse aux appels d'API, la surveillance de l'Outpost et sa mise à jour. Pour bénéficier de la résilience offerte par les zones de disponibilité, vous pouvez déployer des applications sur plusieurs Outposts, qui sont chacun rattachés à une zone de disponibilité différente. Cela vous permet de renforcer la résilience des applications et d'éviter de dépendre d'une seule zone de disponibilité. Pour plus d'informations sur les régions et les zones de disponibilité, consultez Infrastructure mondiale AWS.

Vous pouvez utiliser un groupe de placement avec une stratégie d'extension pour faire en sorte que les instances soient placées sur des racks Outposts distincts. Cela peut contribuer à réduire les défaillances corrélées. Pour plus d'informations, consultez Groupes de placement sur Outposts.

Vous pouvez lancer des instances dans les Outposts à l'aide d'Amazon EC2 Auto Scaling et créer un Application Load Balancer afin de répartir le trafic entre les instances. Pour plus d'informations, consultez Configuration d'un Application Load Balancer sur AWS Outposts.

Validation de conformité pour AWS Outposts

Pour savoir si un programme Services AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultez Services AWS la section de conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de AWS conformité Programmes AWS de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir Téléchargement de rapports dans AWS Artifact .

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Guides de démarrage rapide sur la sécurité et la conformité : ces guides de déploiement abordent les considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de base axés sur AWS la sécurité et la conformité.
- Architecture axée sur la sécurité et la conformité HIPAA sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent créer des applications AWS conformes à la loi HIPAA.

> **Note**
>
> Tous ne Services AWS sont pas éligibles à la loi HIPAA. Pour plus d'informations, consultez le HIPAA Eligible Services Reference.

- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- AWS Guides de conformité destinés aux clients — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation Services AWS et décrivent les directives relatives aux contrôles de sécurité dans de nombreux cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).
- Évaluation des ressources à l'aide des règles du guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub— Cela Service AWS fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez Référence des contrôles Security Hub.
- AWS Audit Manager— Cela vous Service AWS permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Accès à Internet pour les charges AWS Outposts de travail

Cette section explique comment les AWS Outposts charges de travail peuvent accéder à Internet de la manière suivante :

- Par le biais de la AWS région mère
- Par le biais du réseau de votre centre de données local

Accès à Internet par le biais de la AWS région mère

Dans cette option, les charges de travail des Outposts accèdent à Internet via le lien de service, puis via la passerelle Internet (IGW) de la région parent. AWS Le trafic sortant vers Internet peut passer par 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 la AWS région.

Pour le paramétrage de la table de routage sur le sous-réseau Outposts, consultez la section Tables de routage des passerelles locales.

Considérations

- Utilisez cette option dans les cas suivants :
  - Vous avez besoin de flexibilité pour sécuriser le trafic Internet grâce AWS aux multiples services de la AWS Région.
  - Vous n'avez pas de point de présence Internet dans votre centre de données ou dans votre installation de colocation.
- Dans cette option, le trafic doit traverser la AWS région parent, ce qui introduit de la latence.
- Tout comme les frais de transfert de données dans AWS les régions, le transfert de données depuis la zone de disponibilité parent vers l'avant-poste entraîne des frais. Pour en savoir plus sur le transfert de données, consultez la tarification à la demande d'Amazon EC2.
- L'utilisation de la bande passante des liaisons de service augmentera.

L'image suivante montre le trafic entre la charge de travail de l'instance Outposts et Internet passant par la région parent AWS .

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

Dans cette option, les charges de travail résidant dans les Outposts accèdent à Internet via votre centre de données local. Le trafic de charge de travail accédant à Internet passe par votre point de présence Internet local et sort localement. La couche de sécurité du réseau de votre centre de données local est chargée de sécuriser le trafic de charge de travail des Outposts.

Pour le paramétrage de la table de routage sur le sous-réseau Outposts, consultez la section Tables de routage des passerelles locales.

Considérations

- Utilisez cette option dans les cas suivants :
  - Vos charges de travail nécessitent un accès à faible latence aux services Internet.
  - Vous préférez éviter de payer des frais de transfert de données sortants (DTO).
  - Vous souhaitez préserver la bande passante des liaisons de service pour le trafic du plan de contrôle.
- Votre couche de sécurité est chargée de sécuriser le trafic de charge de travail des Outposts.
- Si vous optez pour le routage VPC direct (DVR), vous devez vous assurer que les CIDR des Outposts n'entrent pas en conflit avec les CIDR locaux.
- Si la route par défaut (0/0) est propagée via la passerelle locale (LGW), les instances risquent de ne pas être en mesure d'accéder aux points de terminaison du service. Vous pouvez également choisir des points de terminaison VPC pour accéder au service souhaité.

L'image suivante montre le trafic entre la charge de travail de l'instance Outposts et Internet passant par votre centre de données local.

Surveillance de votre Outpost

AWS Outposts s'intègre avec les services suivants offrant des capacités de surveillance et de journalisation :

CloudWatch métriques

Utilisez Amazon CloudWatch pour récupérer des statistiques sur les points de données de vos Outposts sous la forme d'un ensemble ordonné de séries chronologiques, appelées métriques. Vous pouvez utiliser ces métriques pour vérifier que le système fonctionne comme prévu. Pour plus d'informations, consultez CloudWatch métriques pour AWS Outposts.

CloudTrail journaux

Utilisez AWS CloudTrail pour capturer des informations détaillées sur les appels effectués aux API AWS. Vous pouvez stocker ces appels sous forme de fichiers journaux dans Amazon S3. Vous pouvez utiliser ces CloudTrail journaux pour déterminer des informations telles que l'appel a été effectué, l'adresse IP source d'où provient l'appel, l'auteur de l'appel et la date de l'appel.

Les CloudTrail journaux contiennent des informations sur les appels aux actions d'API pourAWS Outposts. Ils contiennent également des informations relatives aux appels aux actions d'API depuis des services d'un Outpost, tels qu'Amazon EC2 et Amazon EBS. Pour plus d'informations, consultez AWS Outpostsinformations dans CloudTrail.

Journaux de flux VPC

Utilisez les journaux de flux VPC pour capturer des informations détaillées sur le trafic entrant ou sortant de votre Outpost et au sein de votre Outpost. Pour plus d'informations, consultez la rubrique Journaux de flux VPC dans le Guide de l'utilisateur Amazon VPC.

Mise en miroir du trafic

Utilisez la mise en miroir du trafic pour copier et transférer le trafic réseau d'Outpost vers les dispositifs de out-of-band sécurité et de surveillance d'Outpost. Vous pouvez utiliser le trafic en miroir pour inspecter le contenu, surveiller les menaces ou résoudre les problèmes. Pour plus d'informations, consultez Guide de mise en miroir du trafic pour Amazon VPC.

AWS Health Dashboard

Le AWS Health Dashboard affiche des informations et des notifications qui sont initiées par des changements d'intégrité des ressources AWS. Les informations sont présentées de deux

manières : sur un tableau de bord qui montre les événements récents et à venir organisés par catégorie, et dans un journal des événements complet qui contient tous les événements des 90 derniers jours. Par exemple, un problème de connectivité sur la liaison de service déclencherait un événement qui apparaîtrait sur le tableau de bord et dans le journal des événements, puis resterait dans ce dernier pendant 90 jours. Dans le cadre du service AWS Health, le AWS Health Dashboard ne nécessite aucune configuration et peut être affiché par n'importe quel utilisateur authentifié dans votre compte. Pour plus d'informations, consultez Démarrer avec le AWS Health Dashboard.

CloudWatch métriques pour AWS Outposts

AWS Outpostspublie des points de données sur Amazon CloudWatch pour vos Outposts. CloudWatch vous permet de récupérer des statistiques sur ces points de données sous la forme d'un ensemble ordonné de séries chronologiques, appelées métriques. Considérez une métrique comme une variable à surveiller, et les points de données comme les valeurs de cette variable au fil du temps. Par exemple, vous pouvez surveiller la capacité d'instance disponible pour votre Outpost sur une période spécifiée. Un horodatage et une unité de mesure facultative sont associés à chaque point de données.

Vous pouvez utiliser les métriques pour vérifier que le système fonctionne comme prévu. Par exemple, vous pouvez créer une CloudWatch alarme pour surveiller la `ConnectedStatus` métrique. Si la métrique moyenne est inférieure à`1`, CloudWatch vous pouvez lancer une action, telle que l'envoi d'une notification à une adresse e-mail. Vous pouvez ensuite étudier les éventuels problèmes de réseau sur site ou par liaison montante susceptibles d'avoir un impact sur les opérations de votre Outpost. Parmi les problèmes courants, citons les modifications récentes de la configuration réseau sur site apportées aux règles de pare-feu et NAT, ou les problèmes de connexion Internet. En cas de problème `ConnectedStatus`, nous vous recommandons de vérifier la connectivité à la région AWS depuis votre réseau sur site et de contacter AWS Support si le problème persiste.

Pour plus d'informations sur la création d'une CloudWatch alarme, consultez la section Utilisation d'Amazon CloudWatch Alarms dans le guide de CloudWatch l'utilisateur Amazon. Pour plus d'informations CloudWatch, consultez le guide de CloudWatch l'utilisateur Amazon.

Table des matières

Métriques Outpost

L'espace de noms `AWS/Outposts` inclut les métriques suivantes.

`ConnectedStatus`

État de la connexion de la liaison de service d'un Outpost. Si la statistique moyenne est inférieure à 1, la connexion est perturbée.

Unité : nombre

Résolution maximale : 1 minute

Statistics : la statistique la plus utile est `Average`.

Dimensions : `OutpostId`

`CapacityExceptions`

Nombre d'erreurs liées à une capacité insuffisante lors des lancements d'instance.

Unité : nombre

Résolution maximale : 5 minutes

Statistiques : les statistiques les plus utiles sont `Maximum` et `Minimum`.

Dimensions : `InstanceType` et `OutpostId`

`IfTrafficIn`

Débit de données que les interfaces virtuelles (VIF) d'Outposts reçoivent des périphériques du réseau local connectés.

Unité : bits par seconde

Résolution maximale : 5 minutes

Statistiques : les statistiques les plus utiles sont `Max` et `Min`.

Dimensions pour les VIF de passerelle locale (lgw-vif) : `OutpostsId`, `VirtualInterfaceGroupId` et `VirtualInterfaceId`

Dimensions pour les VIF de liaison de service (sl-vif) : `OutpostsId` et `VirtualInterfaceId`

`IfTrafficOut`

Débit de données que les interfaces virtuelles (VIF) d'Outposts (VIF) transfèrent vers les périphériques du réseau local connectés.

Unité : bits par seconde

Résolution maximale : 5 minutes

Statistiques : les statistiques les plus utiles sont `Max` et `Min`.

Dimensions pour les VIF de passerelle locale (lgw-vif) : `OutpostsId`, `VirtualInterfaceGroupId` et `VirtualInterfaceId`

Dimensions pour les VIF de liaison de service (sl-vif) : `OutpostsId` et `VirtualInterfaceId`

`InstanceFamilyCapacityAvailability`

Pourcentage de capacité d'instance disponible. Cette métrique n'inclut pas de capacité pour les hôtes dédiés configurés sur l'Outpost.

Unité : pourcentage

Résolution maximale : 5 minutes

Statistics : les statistiques les plus utiles sont `Average` et `pNN.NN` (percentiles).

Dimensions : `InstanceFamily` et `OutpostId`

`InstanceFamilyCapacityUtilization`

Pourcentage de capacité d'instance en cours d'utilisation. Cette métrique n'inclut pas de capacité pour les hôtes dédiés configurés sur l'Outpost.

Unité : pourcentage

Résolution maximale : 5 minutes

Statistics : les statistiques les plus utiles sont `Average` et `pNN.NN` (percentiles).

Dimensions : `Account`, `InstanceFamily` et `OutpostId`

`InstanceTypeCapacityAvailability`

Pourcentage de capacité d'instance disponible. Cette métrique n'inclut pas de capacité pour les hôtes dédiés configurés sur l'Outpost.

Unité : pourcentage

Résolution maximale : 5 minutes

Statistics : les statistiques les plus utiles sont `Average` et `pNN.NN` (percentiles).

Dimensions : `InstanceType` et `OutpostId`

`InstanceTypeCapacityUtilization`

Pourcentage de capacité d'instance en cours d'utilisation. Cette métrique n'inclut pas de capacité pour les hôtes dédiés configurés sur l'Outpost.

Unité : pourcentage

Résolution maximale : 5 minutes

Statistics : les statistiques les plus utiles sont `Average` et `pNN.NN` (percentiles).

Dimensions : `Account`, `InstanceType` et `OutpostId`

`UsedInstanceType_Count`

Nombre de types d'instances actuellement utilisés, y compris les types d'instances utilisés par des services gérés tels qu'Amazon Relational Database Service (Amazon RDS) ou Application Load Balancer. Cette métrique n'inclut pas de capacité pour les hôtes dédiés configurés sur l'Outpost.

Unité : nombre

Résolution maximale : 5 minutes

Dimensions : `Account`, `InstanceType` et `OutpostId`

`AvailableInstanceType_Count`

Nombre de types d'instances disponibles. Cette métrique n'inclut pas de capacité pour les hôtes dédiés configurés sur l'Outpost.

Unité : nombre

Résolution maximale : 5 minutes

Dimensions : `InstanceType` et `OutpostId`

`AvailableReservedInstances`

Nombre d'instances disponibles sur l'Outpost pour les réserves de capacité à la demande (ODCR). Cette métrique ne mesure pas les instances réservées Amazon EC2.

Unité : nombre

Résolution maximale : 5 minutes

Dimensions : `InstanceType` et `OutpostId`

`UsedReservedInstances`

Nombre d'instances disponibles sur l'Outpost pour les réserves de capacité à la demande (ODCR). Cette métrique ne mesure pas les instances réservées Amazon EC2.

Unité : nombre

Résolution maximale : 5 minutes

Dimensions : `InstanceType` et `OutpostId`

`TotalReservedInstances`

Nombre d'instances disponibles sur l'Outpost pour les réserves de capacité à la demande (ODCR). Cette métrique ne mesure pas les instances réservées Amazon EC2.

Unité : nombre

Résolution maximale : 5 minutes

Dimensions : `InstanceType` et `OutpostId`

`EBSVolumeTypeCapacityUtilization`

Pourcentage de la capacité du type de volume EBS utilisée.

Unité : pourcentage

Résolution maximale : 5 minutes

Statistics : les statistiques les plus utiles sont `Average` et `pNN.NN` (percentiles).

Dimensions : `VolumeType` et `OutpostId`

`EBSVolumeTypeCapacityAvailability`

Pourcentage de la capacité du type de volume EBS disponible.

Unité : pourcentage

Résolution maximale : 5 minutes

Statistics : les statistiques les plus utiles sont `Average` et `pNN.NN` (percentiles).

Dimensions : `VolumeType` et `OutpostId`

`EBSVolumeTypeCapacityUtilizationGB`

Nombre de gigaoctets utilisés pour le type de volume EBS.

Unité : gigaoctet

Résolution maximale : 5 minutes

Statistics : les statistiques les plus utiles sont `Average` et `pNN.NN` (percentiles).

Dimensions : `VolumeType` et `OutpostId`

`EBSVolumeTypeCapacityAvailabilityGB`

Capacité disponible (en gigaoctets) pour le type de volume EBS.

Unité : gigaoctet

Résolution maximale : 5 minutes

Statistics : les statistiques les plus utiles sont `Average` et `pNN.NN` (percentiles).

Dimensions : `VolumeType` et `OutpostId`

Dimensions des métriques Outpost

Pour filtrer les métriques pour votre Outpost, utilisez les dimensions suivantes.

Dimension	Description
`Account`	Compte ou service qui utilise la capacité.
`InstanceFamily`	Famille de l'instance.
`InstanceType`	Type d'instance.
`OutpostId`	L'ID de l'Outpost.
`VolumeType`	Type du volume EBS.
`VirtualInterfaceId`	ID de l'interface virtuelle (VIF) de la passerelle locale ou de la liaison de service.
`VirtualInterfaceGroupId`	ID du groupe d'interfaces virtuelles pour l'interface virtuelle (VIF) de la passerelle locale.

Afficher CloudWatch les statistiques de votre avant-poste

Vous pouvez consulter les CloudWatch métriques de vos équilibreurs de charge à l'aide de la CloudWatch console.

Pour afficher les métriques à l'aide de la CloudWatch console

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le panneau de navigation, sélectionnez Métriques.
3. Sélectionnez l'espace de noms Outposts.
4. (Facultatif) Pour afficher une métrique pour toutes les dimensions, entrez son nom dans la zone de recherche.

Pour afficher les métriques à l'aide de la AWS CLI

Utilisez la commande list-metrics suivante pour répertorier les métriques disponibles :

```
aws cloudwatch list-metrics --namespace AWS/Outposts
```

Pour obtenir les statistiques pour une métrique à l'aide de l'AWS CLI

Utilisez la get-metric-statisticscommande suivante pour obtenir des statistiques pour la métrique et la dimension spécifiées. CloudWatch traite chaque combinaison unique de dimensions comme une métrique distincte. Vous ne pouvez pas récupérer les statistiques à l'aide de combinaisons de dimensions qui n'ont pas été spécialement publiées. Vous devez spécifier les mêmes dimensions que celles utilisées lorsque les mesures ont été créées.

```
aws cloudwatch get-metric-statistics --namespace AWS/Outposts \
--metric-name InstanceTypeCapacityUtilization --statistics Average  --period 3600 \
--dimensions Name=OutpostId,Value=op-01234567890abcdef \
Name=InstanceType,Value=c5.xlarge \
--start-time 2019-12-01T00:00:00Z --end-time 2019-12-08T00:00:00Z
```

Journalisation des appels d'API AWS Outposts à l'aide d'AWS CloudTrail

AWS Outpostsest intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dansAWS Outposts. CloudTrail capture tous les appels d'API AWS Outposts sous forme d'événements. Les appels capturés incluent des appels de la console AWS Outposts et les appels de code vers les opérations d'API AWS Outposts. Si vous créez un suivi, vous pouvez activer la diffusion continue des CloudTrail événements vers un compartiment S3, y compris les événements pourAWS Outposts. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faiteAWS Outposts, l'adresse IP à partir de laquelle la demande a été faite, qui a fait la demande, quand elle a été faite et des détails supplémentaires.

Pour plus d'informations CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

AWS Outpostsinformations dans CloudTrail

CloudTrail est activé sur votre AWS compte lorsque vous le créez. Lorsqu'une activité se produit dansAWS Outposts, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez afficher, rechercher et télécharger les événements récents dans votre compte AWS. Pour plus d'informations, consultez la section Affichage des événements avec l'historique des CloudTrail événements.

Pour enregistrer en continu les événements dans votre compte AWS, y compris les événements d'AWS Outposts, créez un journal d'activité. Un journal permet CloudTrail de fournir des fichiers

journaux à un compartiment S3 du parentRégion AWS. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions AWS. Le journal d'activité consigne les événements de toutes les régions dans la partition AWS et livre les fichiers journaux dans le compartiment S3 de votre choix. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour en savoir plus, consultez les ressources suivantes :

- Présentation de la création d'un journal de suivi
- CloudTrail Services et intégrations pris en charge
- Configuration des notifications Amazon SNS pour CloudTrail
- Réception de fichiers CloudTrail journaux de plusieurs régions et réception de fichiers CloudTrail journaux de plusieurs comptes

Toutes les AWS Outposts actions sont enregistrées par CloudTrail. Elles sont décrites dans la Référence des API AWS Outposts. Par exemple, les appels aux `CreateOutpost`GetOutpostInstanceTypes, et `ListSites` les actions génèrent des entrées dans les fichiers CloudTrail journaux.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations d'identité vous aident à déterminer si la demande a été effectuée :

- avec des informations d'identification racine ou d'utilisateur ;
- avec des informations d'identification de sécurité temporaires correspondant à un rôle ou un utilisateur fédéré ;
- par un autre Service AWS.

Pour de plus amples informations, veuillez consulter l'élément userIdentity CloudTrail .

Présentation des entrées des fichiers journaux AWS Outposts

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique d'une source quelconque. Il inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'`CreateOutpost`action.


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAIOSFODNN7EXAMPLE:jdoe",
        "arn": "arn:aws:sts::111122223333:assumed-role/example/jdoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAIOSFODNN7EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/example",
                "accountId": "111122223333",
                "userName": "example"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2020-08-14T16:28:16Z"
            }
        }
    },
    "eventTime": "2020-08-14T16:32:23Z",
    "eventSource": "outposts.amazonaws.com",
    "eventName": "SetSiteAddress",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "XXX.XXX.XXX.XXX",
    "userAgent": "userAgent",
    "requestParameters": {
        "SiteId": "os-123ab4c56789de01f",
        "Address": "***"
    },
    "responseElements": {
        "Address": "***",
        "SiteId": "os-123ab4c56789de01f"
    },
    "requestID": "1abcd23e-f4gh-567j-klm8-9np01q234r56",
    "eventID": "1234a56b-c78d-9e0f-g1h2-34jk56m7n890",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
```

```
}
```

Maintenance d'un Outpost

En vertu du modèle de responsabilité partagée, AWS est responsable du matériel et des logiciels exécutant les services AWS. Cela s'applique à AWS Outposts, de la même façon que cela s'applique à une région AWS. Par exemple, AWS gère les correctifs de sécurité, met à jour le microprogramme et assure la maintenance de l'équipement Outpost. De même, AWS surveille les performances, l'état et les métriques de votre Outpost et détermine si une quelconque maintenance est nécessaire.

> **Warning**
>
> Si le lecteur de disque sous-jacent rencontre une défaillance ou si l'instance s'arrête, se met en veille prolongée ou est résiliée, les données stockées sur les volumes de stockage d'instances sont perdues. Pour éviter toute perte de données, nous vous recommandons de sauvegarder les données à long terme stockées sur des volumes de stockage d'instances sur un système de stockage persistant, tel qu'un compartiment Amazon S3, un volume Amazon EBS ou un dispositif de stockage de votre réseau sur site.

Table des matières

Maintenance matérielle

Si AWS détecte un problème irréparable sur le matériel hébergeant les instances Amazon EC2 s'exécutant sur votre Outpost, nous informons le propriétaire de l'Outpost et le propriétaire des instances que les instances concernées sont vouées à être retirées. Pour plus d'informations, consultez Retrait d'instances dans le Guide de l'utilisateur Amazon EC2.

Le propriétaire de l'Outpost et le propriétaire des instances peuvent tâcher de résoudre le travail conjointement. Le propriétaire des instances peut arrêter et démarrer une instance affectée pour la

migrer vers de la capacité disponible. Les propriétaires d'instances peuvent arrêter et démarrer les instances concernées à leur convenance. Sinon, AWS arrête et redémarre les instances concernées à la date prévue de leur retrait. S'il n'y a pas de capacité supplémentaire sur l'Outpost, l'instance reste à l'état arrêté. Le propriétaire de l'Outpost peut essayer de libérer de la capacité utilisée ou de demander de la capacité supplémentaire pour l'Outpost de façon à mener à bien la migration.

Si une maintenance matérielle s'avère nécessaire, AWS contacte le gestionnaire du site Outpost pour confirmer la date et l'heure de visite de l'équipe d'installation AWS. Il est possible de programmer une intervention en deux jours ouvrables à compter du moment où le gestionnaire du site contacte l'équipe AWS.

Une fois arrivée sur site, l'équipe d'installation AWS remplace les hôtes, les commutateurs ou les éléments de rack non sains et met la nouvelle capacité en service. Sur place, elle n'effectue aucun diagnostic ni aucune réparation sur le matériel. Si le remplacement d'un hôte est nécessaire, elle supprime et détruit la clé de sécurité physique conforme au NIST, ce qui a pour effet d'effacer effectivement les données qui pourraient rester sur le matériel. Vous avez ainsi l'assurance qu'aucune donnée ne quitte votre site. En cas de remplacement d'un appareil réseau Outpost, il est possible que des informations de configuration réseau soient présentes sur l'appareil au moment où il est retiré du site. Ces informations peuvent inclure les adresses IP et les numéros ASN utilisés pour établir des interfaces virtuelles en vue de configurer le chemin menant à votre réseau local ou retournant à la région.

Mises à jour du microprogramme

Normalement, la mise à jour du microprogramme Outpost n'affecte pas les instances de votre Outpost. Dans les rares cas où nous devrons redémarrer l'équipement Outpost pour installer une mise à jour, vous recevrez un avis de retrait pour les instances utilisant cette capacité.

Maintenance de l'équipement réseau

La maintenance des appareils réseau Outpost (OND) n'affecte pas les opérations et le trafic réguliers de l'Outpost. Si une maintenance est nécessaire, le trafic est détourné des appareils OND. Il se peut que vous notiez des changements temporaires dans les annonces BGP, telles que l'ajout en préfixe de AS-Path, ainsi que les changements correspondants dans les modèles de trafic des liaisons ascendantes Outpost. Lors des mises à jour du microprogramme des appareils OND, il est possible que vous constatiez une instabilité du protocole BGP.

Nous vous recommandons de configurer l'équipement réseau du client de sorte qu'il reçoive les annonces BGP d'Outposts sans modification des attributs BGP, et d'activer le multichemin/l'équilibrage de charge BGP afin de bénéficier de flux de trafic entrant optimaux. L'ajout de AS-Path est utilisé pour les préfixes de passerelles locales afin de détourner le trafic des appareils OND dans le cas où une maintenance est nécessaire. Le réseau du client doit privilégier les routes en partance d'Outposts d'une longueur AS-Path de 1 plutôt que les routes d'une longueur AS-Path de 4.

Le réseau du client doit annoncer à tous les appareils OND les mêmes préfixes BGP avec les mêmes attributs. Par défaut, le réseau Outpost équilibre la charge du trafic sortant entre toutes les liaisons ascendantes. Si une maintenance est nécessaire, les politiques de routage sont utilisées côté Outpost pour détourner le trafic d'un appareil OND. Ce détournement de trafic nécessite des préfixes BGP identiques côté client sur tous les appareils OND. Si une maintenance est nécessaire sur le réseau du client, nous vous recommandons d'utiliser l'ajout en préfixe de AS-Path pour détourner temporairement le trafic de certaines liaisons ascendantes.

Bonnes pratiques concernant les événements liés à l'alimentation et au réseau AWS Outposts

Comme indiqué dans les conditions de service AWS pour les clients AWS Outposts, l'installation qui accueille l'équipement Outposts doit répondre aux exigences minimales en matière d'alimentation et de réseau pour pouvoir servir de base à l'installation, à la maintenance et à l'utilisation de l'équipement Outposts. Pour bien fonctionner, un rack Outposts doit disposer d'une alimentation et d'une connectivité réseau sans interruptions.

Événements liés à l'alimentation

En cas de panne d'électricité totale, il existe intrinsèquement un risque qu'une ressource AWS Outposts ne puisse pas se remettre en service automatiquement. Outre le déploiement de solutions d'alimentation redondante et d'alimentation de secours, nous vous recommandons de prendre les mesures suivantes pour vous préparer aux pires scénarios :

- Déplacez vos services et applications en dehors de l'équipement Outposts de manière contrôlée, en procédant à des changements d'équilibrage de charge extérieurs au rack ou basés sur DNS.
- Arrêtez les conteneurs, les instances et les bases de données de manière incrémentielle et ordonnée et restaurez-les dans l'ordre inverse.
- Testez des solutions permettant de déplacer ou d'arrêter les services de manière contrôlée.
- Sauvegardez les données et les configurations critiques et stockez-les en dehors des Outposts.

- Limitez les coupures de courant au minimum.
- Évitez de changer plusieurs fois les alimentations (off-on-off-on) pendant la maintenance.
- Prévoyez du temps supplémentaire dans la fenêtre de maintenance pour faire face aux imprévus.
- Gérez les attentes de vos utilisateurs et de vos clients en leur communiquant une fenêtre de maintenance plus grande que le temps dont vous auriez normalement besoin.

Événements liés à la connectivité réseau

En général, la connexion de la liaison de service entre votre Outpost et la région AWS ou la région d'origine Outposts se rétablit automatiquement en cas d'interruption réseau ou de problèmes susceptibles de se produire sur les appareils de votre réseau d'entreprise en amont ou sur le réseau d'un fournisseur de connectivité tiers une fois la maintenance réseau terminée. Pendant que la connexion de la liaison de service est hors service, vos opérations Outposts sont limitées aux activités du réseau local. Pour plus d'informations, consultez Que se passe-t-il en cas d'interruption de la connexion réseau de mon installation ? sur la page FAQ sur le rack AWS Outposts.

Si la liaison de service est inopérante en raison d'un problème d'alimentation sur site ou d'une perte de connectivité réseau, le AWS Health Dashboard envoie une notification au compte propriétaire des Outposts. Ni vous ni AWS ne peuvent supprimer la notification d'une interruption de la liaison de service, même si l'interruption est prévue. Pour plus d'informations, consultez Premiers pas avec le AWS Health Dashboard dans le Guide de l'utilisateur AWS Health.

Dans le cas d'une maintenance de service planifiée qui va perturber la connectivité réseau, prenez les mesures proactives suivantes pour limiter l'impact de scénarios potentiellement problématiques :

- Si votre rack Outposts se connecte à la région AWS parente via Internet ou une interface virtuelle publique Direct Connect, capturez un trace-route avant la maintenance planifiée. Le fait de disposer d'un chemin réseau fonctionnel (post-network-maintenance) et d'un chemin réseau problématique () pour identifier les différences faciliterait le dépannage. pre-network-maintenance Si vous faites remonter un problème postérieur à la maintenance à AWS ou à votre fournisseur de services Internet (FSI), vous pouvez inclure ces informations.

  Capturez un trace-route entre :

  - Les adresses IP publiques de l'emplacement Outposts et l'adresse IP renvoyée par `outposts.region.amazonaws.com`. Remplacez *`region`* par le nom de la région AWS parente.

  - Toute instance présente dans la région parente dotée d'une connexion Internet publique et les adresses IP publiques à l'emplacement Outposts.
- Si vous êtes responsable de la maintenance réseau, limitez la durée du temps d'arrêt de la liaison de service. Prévoyez une étape supplémentaire dans votre processus de maintenance pour vérifier que le réseau a été rétabli.
- Si vous n'êtes pas responsable de la maintenance réseau, surveillez le temps d'arrêt de la liaison de service par rapport à la fenêtre de maintenance annoncée et faites rapidement remonter l'information à la personne en charge de la maintenance réseau planifiée si la liaison de service n'est pas rétablie à la fin de la fenêtre de maintenance annoncée.

Ressources

Voici quelques ressources se rapportant à la surveillance qui peuvent vous rassurer quant au fonctionnement normal des Outposts après un événement lié à l'alimentation ou au réseau, qu'il soit planifié ou non :

- Le billet de blog AWS Monitoring best practices for AWS Outposts aborde les bonnes pratiques en matière d'observabilité et de gestion des événements propres à Outposts.
- Le AWS blog sur l'outil de débogage pour la connectivité réseau d'Amazon VPC explique l'outil VPC AWSSupport-SetupIP MonitoringFrom. Cet outil est un document AWS Systems Manager (SSM) qui crée une instance de surveillance Amazon EC2 dans un sous-réseau que vous avez spécifié et qui surveille les adresses IP cibles. Le document exécute des tests de diagnostic ping, MTR, TCP trace-route et trace-path et stocke les résultats dans Amazon CloudWatch Logs qui peuvent être visualisés dans un CloudWatch tableau de bord (latence, perte de paquets, par exemple). Pour la surveillance d'Outposts, l'instance de surveillance doit se trouver dans un sous-réseau de la région AWS parente et être configurée pour surveiller une ou plusieurs de vos instances Outpost en utilisant sa/leurs adresses IP privées. Vous obtiendrez ainsi des graphiques sur la perte de paquets et des informations sur la latence entre AWS Outposts et la région AWS parente.
- Le AWS blog Déploiement d'un CloudWatch tableau de bord Amazon automatisé AWS Outposts à utiliser AWS CDK décrit les étapes du déploiement d'un tableau de bord automatisé.
- Si vous avez des questions ou si vous souhaitez obtenir des informations supplémentaires, consultez Création d'un dossier de support dans le Guide de l'utilisateur AWS Support.

Optimisation d'Amazon EC2 pour AWS Outposts

À la différence de la Région AWS, la capacité Amazon Elastic Compute Cloud (Amazon EC2) est limitée sur un Outpost. Vous êtes contraint par le volume total de capacité de calcul que vous avez commandée. Cette rubrique vous présente les bonnes pratiques et des stratégies d'optimisation pour vous aider à tirer le meilleur parti de votre capacité Amazon EC2 dans AWS Outposts.

Table des matières

Hôtes dédiés sur Outposts

Un hôte dédié Amazon EC2 est un serveur physique avec une capacité d'instance EC2 entièrement dédiée à votre utilisation. Si votre Outpost vous procure déjà du matériel dédié, les hôtes dédiés vous permettent d'utiliser des licences logicielles existantes avec des restrictions de licence par socket, par cœur ou par machine virtuelle sur un même hôte. Pour plus d'informations, consultez Hôtes dédiés sur AWS Outposts dans le Guide de l'utilisateur Amazon EC2 pour les instances Linux. Pour Windows, consultez Hôtes dédiés sur AWS Outposts dans le Guide de l'utilisateur Amazon EC2 pour les instances Windows.

Au-delà des licences, les propriétaires d'Outposts peuvent utiliser des hôtes dédiés de deux façons différentes pour optimiser les serveurs dans leurs déploiements d'Outposts, à savoir :

- Modifier la structure de la capacité d'un serveur
- Contrôler le placement des instances au niveau du matériel

Modification de la structure de la capacité d'un serveur

Les hôtes dédiés vous offrent la possibilité de modifier la structure des serveurs de votre déploiement Outpost sans avoir à contacter AWS Support. Lorsque vous achetez de la capacité pour votre Outpost, vous spécifiez la structure de la capacité EC2 que fournit chaque serveur. Chaque serveur prend en charge une seule famille de types d'instance. Une structure peut offrir un ou plusieurs types d'instance. Les hôtes dédiés vous permettent de modifier les choix que vous avez effectués pour cette structure initiale. Si vous allouez un hôte de façon à prendre en charge un seul type

d'instance pour la capacité totale, vous ne pouvez lancer qu'un seul type d'instance à partir de cet hôte. L'illustration suivante présente un serveur m5.24xlarge avec une structure homogène :

Vous pouvez allouer la même capacité à plusieurs types d'instance. Lorsque vous allouez un hôte de façon à prendre en charge plusieurs types d'instance, vous disposez d'une structure hétérogène qui ne nécessite pas de structure de capacité explicite. L'illustration suivante présente un serveur m5.24xlarge avec une structure hétérogène à pleine capacité :

Pour plus d'informations, consultez Allocation d'hôtes dédiés dans le Guide de l'utilisateur Amazon EC2 pour les instances Linux ou Allocation d'hôtes dédiés dans le Guide de l'utilisateur Amazon EC2 pour les instances Windows.

Contrôle du placement des instances au niveau du matériel

Vous pouvez utiliser des hôtes dédiés pour contrôler le placement des instances au niveau du matériel. Utilisez le placement automatique pour laisser les hôtes dédiés déterminer si les instances doivent être lancées sur un hôte spécifique ou sur tout hôte disponible ayant la configuration correspondante. Utilisez l'affinité de l'hôte pour établir une relation entre une instance et un hôte dédié. Si vous disposez d'un rack Outpost, vous pouvez utiliser ces fonctionnalités d'hôtes dédiés pour minimiser l'impact des pannes matérielles corrélées. Pour plus d'informations sur la récupération d'instances, consultez Compréhension du placement automatique et de l'affinité dans le Guide de l'utilisateur Amazon EC2 pour les instances Linux ou Compréhension du placement automatique et de l'affinité dans le Guide de l'utilisateur Amazon EC2 pour les instances Windows.

Vous pouvez partager des hôtes dédiés à l'aide d'AWS Resource Access Manager. Le partage d'hôtes dédiés vous permet de répartir les hôtes d'un déploiement Outpost entre plusieurs Comptes AWS. Pour plus d'informations, consultez Utilisation de ressources partagées.

Configuration de la récupération d'instances

Les instances de votre Outpost qui basculent dans un état non sain en raison d'une défaillance matérielle doivent être migrées vers un hôte sain. Vous pouvez configurer la récupération automatique de sorte que cette migration s'effectue automatiquement en fonction des vérifications du statut des instances. Pour plus d'informations, consultez Récupération de votre instance Linux ou Récupération de votre instance Windows.

Groupes de placement sur Outposts

AWS Outposts prend en charge les groupes de placement. Utilisez des groupes de placement pour influencer la manière dont Amazon EC2 tente de placer les groupes d'instances interdépendantes que vous lancez sur le matériel sous-jacent. Vous pouvez utiliser différentes stratégies (cluster, partition ou extension) pour répondre aux besoins des différentes charges de travail. Si vous disposez d'un Outpost à un seul rack, vous pouvez utiliser la stratégie d'extension pour placer les instances sur des hôtes plutôt que sur des racks.

Groupes de placement étendu

Utilisez un groupe de placement étendu pour répartir une même instance entre des équipements matériels distincts. Le lancement d'instances dans un groupe de placement étendu réduit les risques de défaillances simultanées qui peuvent se produire quand des instances partagent un même équipement. Les groupes de placement peuvent répartir des instances sur des racks ou des hôtes. Vous pouvez utiliser les groupes de placement par répartition sur les hôtes uniquement avec AWS Outposts.

Groupes de placement par répartition sur des racks

Votre groupe de placement étendu sur des racks peut contenir autant d'instances qu'il y a de racks dans votre déploiement Outpost. L'illustration suivante montre un déploiement Outpost à trois racks exécutant trois instances dans un groupe de placement étendu sur des racks.

Groupes de placement étendu sur des hôtes

Votre groupe de placement étendu sur des hôtes peut contenir autant d'instances qu'il y a d'hôtes dans votre déploiement Outpost. L'illustration suivante montre un déploiement Outpost à un seul rack exécutant trois instances dans un groupe de placement étendu sur des hôtes.

Groupes de placement de partitions

Utilisez un groupe de placement de partitions pour répartir plusieurs instances entre des racks dotés de partitions. Chaque partition peut contenir plusieurs instances. Vous pouvez utiliser la répartition automatique pour répartir des instances entre des partitions ou déployer des instances sur des partitions cibles. L'illustration suivante montre un groupe de placement de partitions avec une répartition automatique.

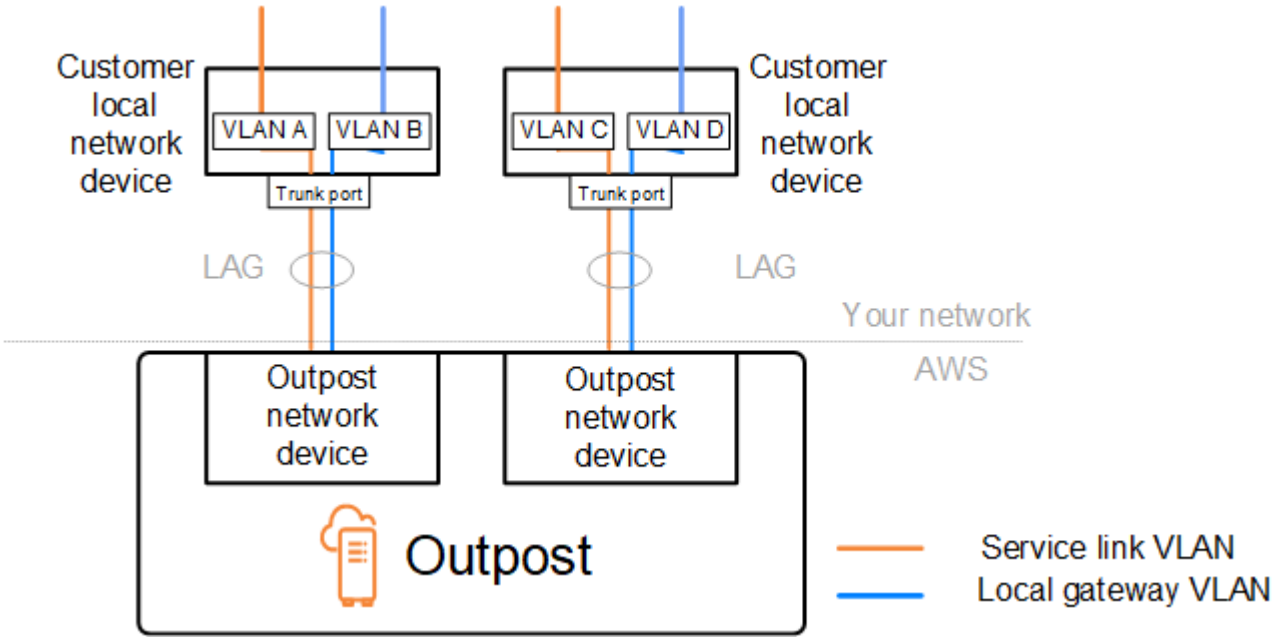
Vous pouvez également déployer des instances sur des partitions cibles. L'illustration suivante montre un groupe de placement de partitions avec une répartition ciblée.

Pour plus d'informations sur l'utilisation de groupes de placement, consultez Groupes de placement et Groupes de placement sur AWS Outposts dans le Guide de l'utilisateur Amazon EC2 pour les instances Linux. Pour Windows, consultez Groupes de placement et Groupes de placement sur AWS Outposts dans le Guide de l'utilisateur Amazon EC2 pour les instances Windows.

Pour plus d'informations sur la haute disponibilité avec AWS Outposts, consultez Considérations concernant l'architecture et la haute disponibilité avec AWS Outposts.

Liste de contrôle pour la résolution des problèmes liés aux réseaux de racks AWS Outposts

Utilisez cette liste de contrôle pour résoudre les problèmes liés à une liaison de service dont le statut est `DOWN`.



Connectivité avec les appareils du réseau Outpost

Vérifiez le statut de l'appairage BGP sur les appareils du réseau local du client qui sont connectés aux appareils du réseau Outpost. Si le statut de l'appairage BGP est `DOWN`, suivez ces étapes :

1. Envoyez une commande ping à l'adresse IP du pair distant sur les appareils du réseau Outpost à partir des appareils du client. Vous pouvez trouver l'adresse IP du pair dans la configuration BGP de votre appareil. Vous pouvez également vous reporter à la Liste de contrôle de préparation du réseau qui vous a été communiquée au moment de l'installation.
2. En cas d'échec de la commande ping, contrôlez la connexion physique et vérifiez que le statut de connectivité est UP.
   a. Vérifiez le statut LACP des appareils du réseau local du client.
   b. Examinez le statut de l'interface sur l'appareil. Si le statut est UP, passez à l'étape 3.
   c. Sur les appareils du réseau local du client, vérifiez que le module optique fonctionne.
   d. Remplacez les fibres défectueuses et vérifiez que les voyants (Tx/Rx) se situent dans une plage acceptable.
3. Si la commande ping aboutit, vérifiez sur les appareils du réseau local du client que les configurations BGP suivantes sont correctes.
   a. Vérifiez que le numéro ASN (Autonomous System Number) local (ASN du client) est correctement configuré.
   b. Vérifiez que le numéro ASN distant (ASN de l'Outpost) est correctement configuré.
   c. Vérifiez que l'adresse IP de l'interface et les adresses IP des pairs distants sont correctement configurées.
   d. Vérifiez que les routes annoncés et reçues sont correctes.
4. Si votre session BGP alterne entre l'état actif et l'état de connexion, vérifiez que le port TCP 179 et les autres ports éphémères pertinents ne sont pas bloqués sur les appareils du réseau local du client.
5. Si vous avez besoin d'un dépannage plus approfondi, vérifiez les points suivants sur les appareils du réseau local du client :
   a. Journaux de débogage BGP et TCP
   b. Journaux BGP
   c. Capture de paquets
6. Si le problème persiste, effectuez des tests MTR, traceroute ou des captures de paquets entre le routeur connecté à l'Outpost et les adresses IP des appareils pairs du réseau Outpost. Partagez les résultats des tests avec AWS Support par l'intermédiaire de votre plan Enterprise Support.

Si le statut de l'appairage BGP est UP entre les appareils du réseau local du client et les appareils du réseau Outpost, mais que la liaison de service est toujours DOWN, vous pouvez aller plus loin dans

le dépannage en vérifiant les appareils suivants sur le réseau local de votre client. Utilisez l'une des listes de contrôle suivantes en fonction du provisionnement de la connectivité de la liaison de service.

- Routeurs de périphérie connectés avec AWS Direct Connect : interface virtuelle publique utilisée pour la connectivité de la liaison de service. Pour plus d'informations, consultez Connectivité de l'interface virtuelle publique AWS Direct Connect à la région AWS.
- Routeurs de périphérie connectés avec AWS Direct Connect : interface virtuelle privée utilisée pour la connectivité de la liaison de service. Pour plus d'informations, consultez Connectivité de l'interface virtuelle privée AWS Direct Connect à la région AWS.
- Routeurs de périphérie connectés avec des fournisseurs de services Internet (FSI) : Internet public utilisé pour la connectivité de la liaison de service. Pour plus d'informations, consultez Connectivité de l'Internet public du FSI à la région AWS.

Connectivité de l'interface virtuelle publique AWS Direct Connect à la région AWS

Utilisez la liste de contrôle suivante pour résoudre les problèmes liés aux routeurs de périphérie connectés avec AWS Direct Connect lorsqu'une interface virtuelle publique est utilisée pour la connectivité de la liaison de service.

1. Vérifiez que les appareils se connectant directement avec les appareils du réseau Outpost reçoivent bien les plages d'adresses IP de la liaison de service via BGP.
   a. Vérifiez les routes qui sont reçues via BGP en provenance de votre appareil.
   b. Vérifiez la table de routage de l'instance de routage et de transfert virtuels (VRF) de la liaison de service. Elle doit indiquer que la plage d'adresses IP est utilisée.
2. Pour assurer la connectivité de la région, vérifiez l'instance VRF de la liaison de service dans la table de routage. Elle doit inclure les plages d'adresses IP publiques AWS ou la route par défaut.
3. Si vous ne recevez pas les plages d'adresses IP publiques AWS dans l'instance VRF de la liaison de service, vérifiez les points suivants.
   a. Vérifiez le statut de la liaison AWS Direct Connect sur le routeur de périphérie ou la AWS Management Console.
   b. Si la liaison physique est `UP`, vérifiez le statut de l'appairage BGP sur le routeur de périphérie.
   c. Si le statut de l'appairage BGP est `DOWN`, envoyez une commande ping à l'adresse IP AWS du pair et vérifiez la configuration BGP au niveau du routeur de périphérie. Pour plus d'informations, consultez Résolution des problèmes liés à AWS Direct Connect dans le Guide

de l'utilisateur AWS Direct Connect et L'état BGP de mon interface virtuelle est en panne dans la console AWS. Que dois-je faire ?

d. Si BGP est en place mais que vous ne voyez pas la route par défaut ou les plages d'adresses IP publiques AWS dans l'instance VRF, contactez AWS Support par l'intermédiaire de votre plan Enterprise Support.

4. Si vous disposez d'un pare-feu sur site, vérifiez les points suivants.

   a. Vérifiez que les ports nécessaires à la connectivité de la liaison de service sont autorisés sur les pare-feu du réseau. Utilisez traceroute sur le port 443 ou tout autre outil de résolution des problèmes réseau pour confirmer la connectivité via les pare-feu et les appareils de votre réseau. Les ports suivants doivent être configurés dans les politiques de pare-feu pour la connectivité de la liaison de service.

      - Protocole TCP – Port source : TCP 1025-65535, port de destination : 443.
      - Protocole UDP – Port source : TCP 1025-65535, port de destination : 443.

   b. S'il s'agit d'un pare-feu avec état, vérifiez que les règles de trafic sortant autorisent le trafic vers les plages d'adresses IP publiques AWS à partir de la plage d'adresses IP de la liaison de service de l'Outpost. Pour plus d'informations, consultez Connectivité AWS Outposts avec les régions AWS.

   c. S'il ne s'agit pas d'un pare-feu avec état, veillez à autoriser également le flux entrant (des plages d'adresses IP publiques AWS vers la plage d'adresses IP de la liaison de service).

   d. Si vous avez configuré un routeur virtuel au niveau des pare-feu, vérifiez que le routage configuré pour le trafic entre l'Outpost et la région AWS est approprié.

5. Si vous avez configuré le NAT sur le réseau sur site afin que les plages d'adresses IP de la liaison de service de l'Outpost soient traduites dans vos propres adresses IP publiques, vérifiez les points suivants.

   a. Vérifiez que le périphérique NAT n'est pas surchargé et qu'il a des ports libres à allouer pour de nouvelles sessions.

   b. Vérifiez que le périphérique NAT est correctement configuré pour assurer la traduction d'adresses.

6. Si le problème persiste, effectuez des tests MTR, traceroute ou des captures de paquets entre le routeur de périphérie et les adresses IP des pairs AWS Direct Connect. Partagez les résultats des tests avec AWS Support par l'intermédiaire de votre plan Enterprise Support.

Connectivité de l'interface virtuelle privée AWS Direct Connect à la région AWS

Utilisez la liste de contrôle suivante pour résoudre les problèmes liés aux routeurs de périphérie connectés avec AWS Direct Connect lorsqu'une interface virtuelle privée est utilisée pour la connectivité de la liaison de service.

1. Si la connectivité entre le rack Outpost et la région AWS utilise la fonctionnalité de connectivité privée d'AWS Outposts, vérifiez les points suivants.
   a. Envoyez une commande ping à l'adresse IP AWS d'appairage à distance à partir du routeur de périphérie et vérifiez le statut de l'appairage BGP.
   b. Vérifiez que l'appairage BGP via l'interface virtuelle privée AWS Direct Connect entre les points de terminaison de la liaison de service du VPC et l'Outpost installé dans vos locaux présente le statut UP. Pour plus d'informations, consultez Résolution des problèmes liés à AWS Direct Connect dans le Guide de l'utilisateur AWS Direct Connect et L'état BGP de mon interface virtuelle est en panne dans la console AWS. Que dois-je faire ? et Comment dépanner les problèmes de connexion BGP sur Direct Connect ?
   c. L'interface virtuelle privée AWS Direct Connect est une connexion privée à votre routeur de périphérie à l'emplacement AWS Direct Connect que vous avez choisi ; elle utilise le protocole BGP pour échanger les routes. La plage CIDR de votre cloud privé virtuel (VPC) est annoncée à votre routeur de périphérie par l'intermédiaire de cette session BGP. De même, la plage d'adresses IP de la liaison de service Outpost est annoncée à la région via BGP à partir de votre routeur de périphérie.
   d. Vérifiez que les listes ACL réseau associées au point de terminaison privé de la liaison de service de votre VPC autorisent le trafic approprié. Pour plus d'informations, consultez Liste de contrôle de préparation du réseau.
   e. Si vous disposez d'un pare-feu sur site, vérifiez qu'il dispose de règles de trafic sortant qui autorisent les plages d'adresses IP de la liaison de service et les points de terminaison du service Outpost (adresses IP de l'interface réseau) situés dans le VPC ou le CIDR du VPC. Vérifiez que les ports TCP 1025-65535 et UDP 443 ne sont pas bloqués. Pour plus d'informations, consultez Introducing AWS Outposts private connectivity.
   f. S'il ne s'agit pas d'un pare-feu avec état, vérifiez qu'il dispose de règles et de politiques autorisant le trafic entrant dans l'Outpost en provenance des points de terminaison du service Outpost du VPC.

2. Si votre réseau sur site compte plus de 100 réseaux, vous pouvez annoncer une route par défaut via la session BGP à AWS sur votre interface virtuelle privée. Si vous ne souhaitez pas annoncer de route par défaut, résumez les routes de sorte que le nombre de routes annoncées soit inférieur à 100.
3. Si le problème persiste, effectuez des tests MTR, traceroute ou des captures de paquets entre le routeur de périphérie et les adresses IP des pairs AWS Direct Connect. Partagez les résultats des tests avec AWS Support par l'intermédiaire de votre plan Enterprise Support.

Connectivité de l'Internet public du FSI à la région AWS

Utilisez la liste de contrôle suivante pour résoudre les problèmes liés aux routeurs de périphérie connectés via un FSI lorsque l'Internet public est utilisé pour la connectivité de la liaison de service.

- Vérifiez que la liaison Internet est opérationnelle.
- Vérifiez que les serveurs publics sont accessibles à partir de vos appareils de périphérie connectés via un FSI.

Si Internet ou les serveurs publics ne sont pas accessibles via les liaisons du FSI, effectuez les étapes suivantes.

1. Contrôlez si le statut de l'appairage BGP avec les routeurs du FSI est établi.
   a. Vérifiez que le protocole BGP n'est pas instable.
   b. Vérifiez que le protocole BGP reçoit et annonce les routes nécessaires à partir du FSI.
2. Dans le cas d'une configuration de route statique, vérifiez que la route par défaut est correctement configurée sur l'appareil de périphérie.
3. Vérifiez si vous pouvez accéder à Internet en utilisant la connexion d'un autre FSI.
4. Si le problème persiste, effectuez des tests MTR, traceroute ou des captures de paquets sur votre routeur de périphérie. Partagez les résultats avec l'équipe de support technique de votre FSI pour un dépannage plus approfondi.

Si Internet et les serveurs publics sont accessibles via les liaisons du FSI, effectuez les étapes suivantes.

1. Vérifiez si l'une de vos instances EC2 ou l'un de vos équilibreurs de charge accessibles publiquement dans la région d'origine de l'Outpost sont accessibles depuis votre appareil de

périphérie. Vous pouvez utiliser une commande ping ou telnet pour vérifier la connectivité et utiliser ensuite traceroute pour vérifier le chemin réseau.

2. Si vous utilisez des instances VRF pour séparer le trafic sur votre réseau, vérifiez que l'instance VRF de la liaison de service dispose de routes ou de politiques qui dirigent le trafic à destination et en provenance du FSI (Internet) et de l'instance VRF. Examinez les points de contrôle suivants.
   a. Routeurs de périphérie connectés avec le FSI. Examinez la table de routage VRF du FSI sur les routeurs de périphérie pour vérifier la présence de la plage d'adresses IP de la liaison de service.
   b. Appareils du réseau local du client connectés avec l'Outpost. Examinez la configuration des instances VRF et vérifiez que le routage et les politiques nécessaires à la connectivité entre l'instance VRF de la liaison de service et l'instance VRF du FSI sont correctement configurés. En règle générale, une route par défaut est envoyée de l'instance VRF du FSI vers l'instance VRF de la liaison de service pour le trafic à destination d'Internet.
   c. Si vous avez configuré un routage en fonction de la source sur les routeurs connectés à votre Outpost, vérifiez que la configuration est correcte.
3. Assurez-vous que les pare-feu sur site sont configurés pour autoriser la connectivité sortante (ports TCP 1025-65535 et UDP 443) entre les plages d'adresses IP de la liaison de service Outpost et les plages d'adresses IP AWS publiques. S'il ne s'agit pas de pare-feu avec état, vérifiez que la connectivité entrante à destination de l'Outpost est également configurée.
4. Vérifiez que le NAT est configuré sur le réseau sur site afin que les plages d'adresses IP de la liaison de service de l'Outpost soient traduites dans vos propres adresses IP publiques. Vérifiez également les points suivants.
   a. Le périphérique NAT n'est pas surchargé et a des ports libres à allouer pour de nouvelles sessions.
   b. Le périphérique NAT est correctement configuré pour assurer la traduction d'adresses.

Si le problème persiste, effectuez des tests MTR, traceroute ou des captures de paquets.

- Si les résultats montrent que des paquets sont abandonnés ou bloqués dans le réseau sur site, contactez votre équipe réseau ou technique pour obtenir des conseils supplémentaires.
- Si les résultats montrent que l'abandon ou le blocage des paquets se produisent dans le réseau du FSI, contactez l'équipe de support technique du FSI.

- Si les résultats n'indiquent aucun problème, collectez les résultats de tous les tests (MTR, telnet, traceroute, captures de paquets et journaux BGP) et contactez AWS Support par l'intermédiaire de votre plan Enterprise Support.

Outposts se trouve derrière deux pare-feux

Si vous avez placé votre Outpost derrière une paire de pare-feux synchronisés à haute disponibilité ou deux pare-feux autonomes, un routage asymétrique du lien de service peut se produire. Cela signifie que le trafic entrant peut passer par le pare-feu-1, tandis que le trafic sortant passe par le pare-feu-2. Utilisez la liste de contrôle suivante pour identifier le routage asymétrique potentiel du lien de service, en particulier s'il fonctionnait correctement auparavant.

- Vérifiez si des modifications récentes ou une maintenance continue ont été apportées à la configuration du routage du réseau de votre entreprise qui auraient pu entraîner un routage asymétrique de la liaison de service à travers les pare-feux.
  - Utilisez les graphiques du trafic du pare-feu pour vérifier les modifications des modèles de trafic correspondant au début du problème de liaison de service.
  - Vérifiez s'il s'agit d'une défaillance partielle du pare-feu ou d'un scénario de paire de pare-feux à cerveau divisé qui aurait pu empêcher vos pare-feux de synchroniser leurs tables de connexion entre eux.
  - Vérifiez s'il existe des liaisons en panne ou des modifications récentes apportées au routage (modifications des métriques OSPF/ISIS/EIGRP, modifications de la feuille de route BGP) dans votre réseau d'entreprise qui correspondent au début du problème de liaison de service.
- Si vous utilisez une connexion Internet publique pour le lien de service vers la région d'origine, la maintenance d'un fournisseur de services peut avoir entraîné un routage asymétrique du lien de service à travers les pare-feux.
  - Consultez les graphiques du trafic pour voir s'il existe des liens vers votre ou vos fournisseurs de services Internet afin de détecter les modifications des modèles de trafic correspondant au début du problème de lien de service.
- Si vous utilisez la AWS Direct Connect connectivité pour le lien de service, il est possible qu'une maintenance AWS planifiée ait déclenché un routage asymétrique du lien de service.
  - Vérifiez les notifications de maintenance planifiée sur vos AWS Direct Connect services.
  - Notez que si vous disposez de AWS Direct Connect services redondants, vous pouvez tester de manière proactive le routage du lien de service Outposts sur chaque chemin réseau probable dans des conditions de maintenance. Cela vous permet de tester si une interruption de l'un de

vos AWS Direct Connect services peut entraîner un routage asymétrique du lien de service. La résilience de la AWS Direct Connect partie de la connectivité end-to-end réseau peut être testée par le kit d'outils AWS Direct Connect Resiliency with Resiliency. Pour plus d'informations, voir Tester AWS Direct Connect la résilience avec le Resiliency Toolkit — Failover Testing.

Après avoir passé en revue la liste de contrôle précédente et identifié le routage asymétrique du lien de service comme cause possible, vous pouvez prendre un certain nombre d'autres mesures :

- Restaurez le routage symétrique en annulant toute modification apportée au réseau de l'entreprise ou en attendant la fin de la maintenance planifiée par le fournisseur.
- Connectez-vous à un pare-feu ou aux deux et effacez toutes les informations relatives à l'état des flux depuis la ligne de commande (si le fournisseur du pare-feu les prend en charge).
- Filtrez temporairement les annonces BGP via l'un des pare-feu ou fermez les interfaces d'un pare-feu afin de forcer le routage symétrique à travers l'autre pare-feu.
- Redémarrez chaque pare-feu à tour de rôle pour éliminer toute corruption potentielle dans le suivi de l'état du flux du trafic des liaisons de service dans la mémoire du pare-feu.
- Contactez votre fournisseur de pare-feu pour vérifier ou assouplir le suivi de l'état du flux UDP pour les connexions UDP provenant du port 443 et destinées au port 443.

AWS Outposts end-of-term options

À la fin de votre contrat AWS Outposts, trois options s'offrent à vous :

- Renouvelez votre abonnement et conservez votre Outpost existant.
- Mettez fin à votre abonnement et préparez vos racks Outpost pour le retour.
- Passez à un month-to-month abonnement et conservez votre Outpost existant.

Si vous n'indiquez pas que vous souhaitez renouveler votre abonnement ou retourner votre Outpost, vous serez converti en month-to-month abonnement.

Rubriques

Renouvellement de votre abonnement

Pour renouveler votre abonnement et conserver votre Outpost existant :

Effectuez les étapes suivantes au moins 30 jours avant la fin du contrat de votre Outpost :

1. Connectez-vous à la console du Centre AWS Support.
2. Choisissez Create case (Créer une demande).
3. Choisissez Compte et facturation.
4. Pour Service, choisissez Facturation.
5. Pour Catégorie, choisissez Autres questions de facturation.
6. Pour Gravité, choisissez Question importante.
7. Choisissez Next step: Additional information (Étape suivante : informations supplémentaires).
8. Dans la page Informations supplémentaires, pour Objet, entrez votre demande de renouvellement, telle que **`Renew my Outpost subscription`**.
9. Pour Description, entrez l'une des options de paiement suivantes :

    - Sans frais initiaux

- Frais initiaux partiels
- Tous les frais initiaux

Pour la tarification, consultez Tarification des racks AWS Outposts. Vous pouvez également demander un devis.

10. Choisissez Next step: Solve now or contact us (Étape suivante : résolvez maintenant ou contactez-nous).
11. Sur la page Contact us (Contactez-nous), choisissez votre langue préférée.
12. Choisissez votre méthode de contact préférée.
13. Vérifiez les détails de votre cas et choisissez Submit (Envoyer). Votre numéro d'ID de dossier et votre résumé apparaissent.

Le support client AWS lancera le processus de renouvellement de l'abonnement. Votre nouvel abonnement débutera le lendemain de la fin de votre abonnement actuel.

Fin de votre abonnement et préparation des racks pour le retour

> **Important**
>
> AWS ne peut pas commencer le processus de retour tant que vous n'avez pas effectué les procédures suivantes. Nous ne pouvons pas arrêter le processus de retour une fois que vous avez ouvert un cas de support pour mettre fin à votre abonnement.

Pour mettre fin à votre abonnement :

Effectuez les étapes suivantes au moins 30 jours avant la fin du contrat de votre Outpost :

1. Connectez-vous à la console du Centre AWS Support.
2. Choisissez Create case (Créer une demande).
3. Choisissez Compte et facturation.
4. Pour Service, choisissez Facturation.
5. Pour Catégorie, choisissez Autres questions de facturation.
6. Pour Gravité, choisissez Question importante.

7. Choisissez Next step: Additional information (Étape suivante : informations supplémentaires).
8. Dans la page Informations supplémentaires, pour Objet, entrez une demande claire, telle que **`End my Outpost subscription`**.
9. Pour Description, entrez la date à laquelle vous préférez que l'Outpost soit récupéré.
10. Choisissez Next step: Solve now or contact us (Étape suivante : résolvez maintenant ou contactez-nous).
11. Sur la page Contact us (Contactez-nous), choisissez votre langue préférée.
12. Choisissez votre méthode de contact préférée.
13. Vérifiez les détails de votre cas et choisissez Submit (Envoyer). Votre numéro d'ID de dossier et votre résumé apparaissent.

Le support client AWS vous contactera pour coordonner la récupération.

Pour préparer vos racks AWS Outposts pour le retour :

> **Important**
>
> Ne mettez pas le rack Outpost hors tension tant qu'AWS n'est pas sur site pour la récupération prévue.

1. Si les ressources de l'Outpost sont partagées, vous devez annuler le partage de ces ressources.

   Vous pouvez annuler le partage d'une ressource Outpost de l'une des manières suivantes :

   - Utilisez la console AWS RAM. Pour plus d'informations, consultez Mise à jour d'un partage de ressources dans le Guide de l'utilisateur AWS RAM.
   - Utilisez l'interface AWS CLI pour exécuter la commande disassociate-resource-share.

   Pour consulter la liste des ressources Outpost qui peuvent être partagées, consultez Ressources Outpost partageables.
2. Résiliez les instances actives associées aux sous-réseaux sur votre Outpost. Pour résilier les instances, suivez les instructions de Résilier une instance dans le Guide de l'utilisateur Amazon EC2 pour les instances Linux.
3. Vérifiez le instance-capacity-availability nombre de vos instances Amazon EC2 dans votre AWS compte.

a. Ouvrez la console AWS Outposts à l'adresse https://console.aws.amazon.com/outposts/.

b. Choisissez Outposts.

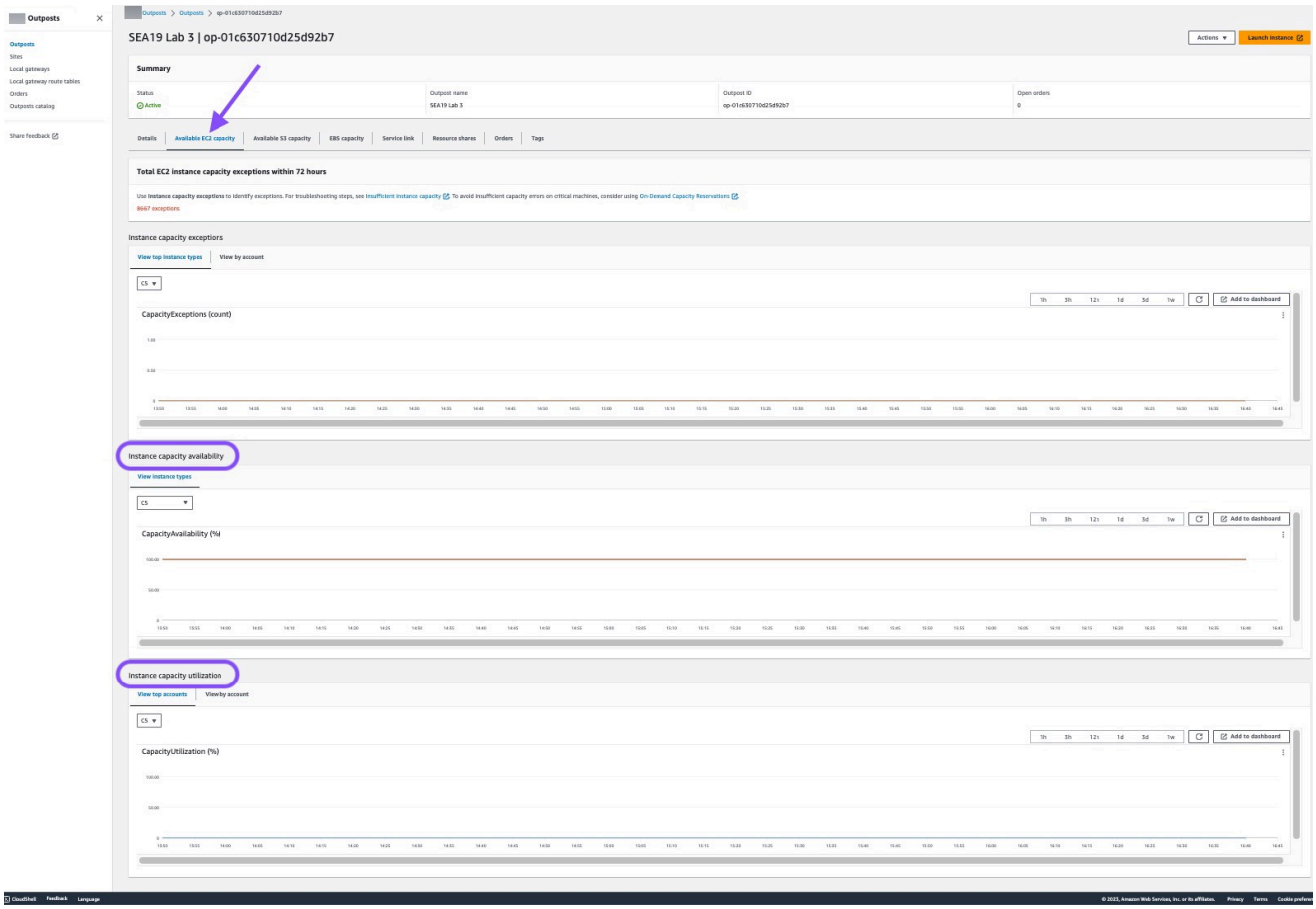
c. Choisissez l'Outpost spécifique que vous retournez.

d. Dans la page de l'Outpost, choisissez l'onglet Capacité EC2 disponible.

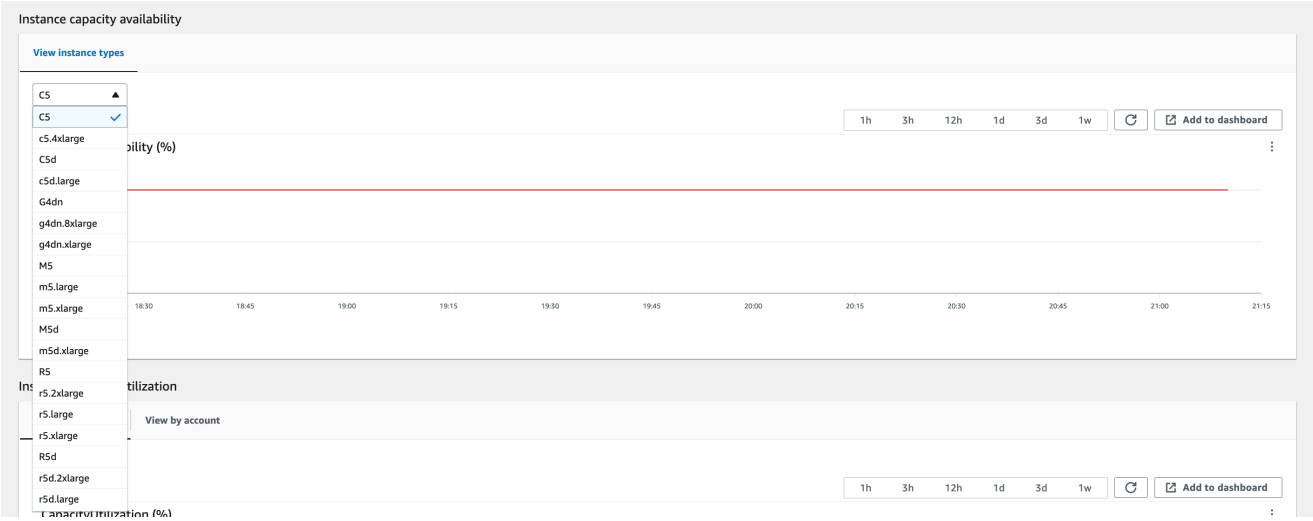
e. Assurez-vous que l'option Disponibilité de la capacité d'instance est définie sur 100 % pour chaque famille d'instances.

f. Assurez-vous que l'option Utilisation de la capacité d'instance est définie sur 0 % pour chaque famille d'instances.

L'image suivante présente les graphiques Disponibilité de la capacité d'instance et Utilisation de la capacité d'instance dans l'onglet Capacité EC2 disponible.



L'image suivante présente la liste des types d'instance.



4. Créez des sauvegardes de vos instances Amazon EC2 et de vos volumes de serveur. Pour créer les sauvegardes, suivez les instructions de Sauvegarde et restauration d'Amazon EC2 avec des volumes EBS dans le guide Recommandations AWS.
5. Supprimez les volumes Amazon EBS associés à votre Outpost.
   a. Ouvrez la console Amazon EC2 sur https://console.aws.amazon.com/ec2/.
   b. Dans le panneau de navigation, choisissez Volumes.
   c. Choisissez Actions, puis Supprimer le volume.
   d. Dans la boîte de dialogue de confirmation, choisissez Delete (Supprimer).
6. Si Amazon S3 on Outposts est installé, supprimez tous les instantanés locaux sur les Outposts.
   a. Ouvrez la console Amazon EC2 sur https://console.aws.amazon.com/ec2/.
   b. Dans le volet de navigation, choisissez Snapshots (Instantanés).
   c. Sélectionnez les instantanés dotés d'un ARN Outpost.
   d. Choisissez Actions, puis Supprimer les instantanés.
   e. Dans la boîte de dialogue de confirmation, choisissez Delete (Supprimer).
7. Supprimez tous les compartiments Amazon S3 associés à votre Outpost. Pour supprimer les compartiments, suivez les instructions de Suppression de votre compartiment Amazon S3 on Outposts dans le Guide de l'utilisateur Amazon Simple Storage Service.
8. Supprimez les associations de VPC et les CIDR de groupe d'adresses IP clients (CoIP) associés à votre Outpost.

Une équipe AWS chargée de la récupération mettra le rack hors tension. Une fois qu'il est hors tension, vous pouvez détruire la clé de sécurité Nitro AWS ou l'équipe AWS chargée de la récupération peut le faire à votre place.

Convertir en month-to-month abonnement

Pour passer à un month-to-month abonnement et conserver votre Outpost existant, aucune action n'est nécessaire. Si vous avez des questions, ouvrez un cas de support pour la facturation.

Votre Outpost sera renouvelé sur une base mensuelle au taux de l'option de paiement Aucuns frais initiaux correspondant à votre configuration AWS Outposts. Votre nouvel abonnement mensuel débutera le lendemain de la fin de votre abonnement actuel.

Quotas pour AWS Outposts

VotreCompte AWS dispose de des dispose de, anciennement appelés limites, pour chaque dispose deService AWS. Sauf indication contraire, chaque quota est spécifique à la région. Vous pouvez demander des augmentations pour certains quotas, et ne peuvent pas être augmentés.

Pour afficher les quotas pourAWS Outposts, ouvrez la boîte de dialogue Service Quotas. Dans le volet de navigation, choisissez Services AWS, puis sélectionnez AWS Outposts.

Pour demander une augmentation de quota, consultez Demande d'augmentation de quota dans le Guide de l'utilisateur Service Quotas.

Les quotas de votre Compte AWS concernant AWS Outposts sont les suivants :

Ressource	Par défaut	Ajustable	Commentaires
Sites d'avant-poste	100	Oui	Un site Outpost est le bâtiment physique géré par le client dans lequel vous alimentez et connectez votre équipement Outpost au réseau. Vous pouvez avoir 100 sites Outposts dans chaque région de votreAWS compte.
Outposts par site	10	Oui	AWS Outpostsinclut des ressource s matérielles et virtuelles, appelées Outposts. Ce quota limite les ressources virtuelles de votre Outpost. Vous pouvez avoir 10 Outposts dans chaque site d'avant-poste.

AWS Outpostset les quotas pour les autres services

AWS Outpostsdépend des ressources d'autres services et ces services peuvent avoir leurs propres quotas par défaut. Par exemple, votre quota pour les interfaces réseau locales provient du quota Amazon VPC pour les interfaces réseau.

Historique du document

Le tableau suivant décrit les modifications importantes apportées au Guide de l'utilisateur AWS Outposts.

Modification	Description	Date
Le rack AWS Outposts prend en charge les mesures de débit de l'interface de liaison de service	Vous pouvez désormais surveiller l'utilisation du débit entre les interfaces virtuelles (VIF) des liaisons de service de votre rack Outpost et les périphériques de votre réseau local, en tirant parti des métriques Amazon CloudWatch `IfTrafficIn` et `IfTrafficOut` .	17 novembre 2023
Communication intra-VPC dans AWS Outposts avec une passerelle locale	Vous pouvez établir une communication entre des sous-réseaux qui sont dans le même VPC à travers différents Outposts avec des passerelles locales.	30 août 2023
nd-of-term Options E pour les AWS Outposts racks	À la fin de votre contrat AWS Outposts, vous pouvez renouveler, résilier ou convertir votre abonnement.	1er août 2023
Amazon Route 53 sur Outposts est désormais disponible sur des racks AWS Outposts.	Amazon Route 53 sur Outposts inclut un résolveur qui met en cache toutes les requêtes DNS provenant de AWS Outposts. Vous pouvez également configurer une connectivité hybride entre	20 juillet 2023

	un résolveur Outpost et un résolveur DNS sur site lorsque vous déployez des points de terminaison entrants et sortants.	
Routes entrantes de la passerelle locale	Vous pouvez créer et modifier les routes entrantes des passerelles locales vers des interfaces réseau Elastic sur votre Outpost.	15 septembre 2022
Présentation du routage VPC direct pour AWS Outposts	Utilise l'adresse IP privée des instances de votre VPC pour faciliter la communication avec votre réseau sur site.	14 septembre 2022
Guide de l'utilisateur AWS Outposts créé pour les racks Outposts	Le guide de l'utilisateur AWS Outposts a été divisé en deux pour les racks et les serveurs.	14 septembre 2022
Créez et gérez des tables de routage de passerelles locales	Créez et modifiez des tables de routage de passerelles locales et des pools CoIP. Gérez les associations du groupe d'interfaces virtuelles.	14 septembre 2022
Groupes de placement sur AWS Outposts	Les groupes de placement qui utilisent une stratégie de répartition peuvent répartir les instances entre les hôtes.	30 juin 2022
Hôtes dédiés sur AWS Outposts	Vous pouvez désormais utiliser des hôtes dédiés sur Outposts.	31 mai 2022

Sites Outpost partagés	Créez et gérez des sites Outpost et partagez-les avec d'autres comptes AWS de votre organisation.	18 octobre 2021
Une nouvelle CloudWatch dimension	Une nouvelle CloudWatch dimension pour les métriques dans l'espace de AWS Outposts noms.	13 octobre 2021
Partagez des compartiments S3	Partagez et gérez des compartiments S3 sur votre Outpost.	5 août 2021
Prise en charge de certains groupes de placement	Vous pouvez utiliser des stratégies de placement en cluster, en partition ou de répartition comme vous le feriez dans une région.	28 juillet 2021
CloudWatch Métriques supplémentaires	Des CloudWatch métriques supplémentaires sont disponibles pour les instances réservées.	24 mai 2021
Liste de contrôle de dépannage réseau	cUne liste de contrôle de dépannage réseau est disponible.	22 février 2021
CloudWatch Métriques supplémentaires	Des CloudWatch mesures supplémentaires pour les volumes EBS sont disponibles.	2 février 2021
Mise à jour des commandes de la console	Le processus de commande de la console est mis à jour.	14 janvier 2021

Connectivité privée	Vous pouvez configurer la connectivité privée pour votre Outpost lorsque vous le créez dans la console AWS Outposts.	21 décembre 2020
Liste de contrôle de disponibilité du réseau	Utilisez la liste de contrôle de disponibilité du réseau lorsque vous collectez les informations nécessaires à la configuration de votre Outpost.	28 octobre 2020
Ressources AWS Outposts partagées	Grâce au partage d'Outpost , les propriétaires d'Outpost s peuvent partager leurs Outposts et leurs ressource s, y compris les tables de routage des passerelles locales, avec d'autres comptes AWS appartenant à la même organisation AWS.	15 octobre 2020
CloudWatch Métriques supplémentaires	Des CloudWatch mesures supplémentaires concernant le nombre de types d'instances sont disponibles.	21 septembre 2020
CloudWatch Métrique supplémentaire	Une CloudWatch métrique supplémentaire concernant l'état de connexion du lien de service est disponible.	11 septembre 2020
Prise en charge du partage des adresses IPv4 appartenant aux clients	Utilisez AWS Resource Access Manager pour partager les adresses IPv4 appartenant aux clients.	20 avril 2020

CloudWatch Métriques supplémentaires	Des CloudWatch mesures supplémentaires pour les volumes EBS sont disponibles.	4 avril 2020
Première version	Il s'agit de la première version d’AWS Outposts.	3 décembre 2019

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.