Guide de l'utilisateur pour les Outposts Racks

AWS Outposts

AWS Outposts: Guide de l'utilisateur pour les Outposts Racks

Table of Contents

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

AWS Outposts est un service entièrement géré qui étend AWS l'infrastructure APIs, les services et les outils aux locaux du client. 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 EC2 instances, 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 avant-poste à un autre avant-poste 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 consulter et gérer la capacité de votre Outpost depuis la AWS Outposts console. AWS Outposts prend en charge la gestion des capacités en libre-service que vous pouvez définir au niveau des Outposts pour reconfigurer tous les actifs d'un Outposts ou spécifiquement pour chaque actif individuel. Un actif Outpost peut être un serveur unique au sein d'un rack Outposts ou d'un serveur 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 Outposts incluent des serveurs montables en rack, des commutateurs, un panneau de brassage réseau, une étagère d'alimentation et des panneaux vierges.
- Racks ACE Outposts : le rack Aggregation, Core, Edge (ACE) fait office de point d'agrégation réseau pour les déploiements Outpost sur plusieurs racks. Le rack ACE réduit le nombre de ports réseau physiques et d'interfaces logiques requis en fournissant une connectivité entre plusieurs racks de calcul Outpost de vos Outposts logiques et de votre réseau sur site.

  Vous devez installer un rack ACE si vous disposez de quatre racks de calcul ou plus. Si vous avez moins de quatre racks de calcul mais que vous prévoyez de passer à quatre racks ou plus à l'avenir, nous vous recommandons d'installer un rack ACE au plus tôt.

  Pour plus d'informations sur les racks ACE, voir Mise à l'échelle des déploiements de AWS Outposts racks avec des racks ACE.
- 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 Outposts fournissent des services informatiques et réseau locaux aux sites dont l'espace est limité ou dont les besoins en capacité sont moindres.
- Propriétaire de l'avant-poste : titulaire du compte qui passe la AWS Outposts commande. Après AWS s'être engagé avec le client, le propriétaire peut inclure des points de contact supplémentaires. AWS communiquera avec les contacts pour clarifier les commandes, les rendez-vous d'installation, ainsi que la maintenance et le remplacement du matériel. AWS Support Centre de contact si les informations de contact changent.
- 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 Outposts et votre réseau local.
- Interface réseau locale : interface réseau qui permet la communication entre un serveur Outposts et votre réseau local.

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
EC2 Instances Amazon	 O	 Oui
Clusters Amazon ECS	 O	 Oui
Nœuds Amazon EKS	 O	 Non

Base de données et analytique

Type de ressource	Racks	Serveurs
ElastiCacheNœuds Amazon (cluster Redis, cluster Memcached)	 O	 Non
Clusters Amazon EMR	 O	 Non
Instances de base de données Amazon RDS	 O	 Non

Réseaux

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

Stockage

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

Autres Services AWS

Service	Racks	Serveurs
AWS IoT Greengrass	 O	 Oui

Tarification

Le prix est basé sur les détails de votre commande. Lorsque vous passez une commande, vous pouvez choisir parmi une variété de configurations Outpost, chacune proposant une combinaison de types d' EC2 instances Amazon et d'options de stockage. Vous choisissez également une durée contractuelle et une option de paiement. Le prix inclut les éléments suivants :

- Racks Outposts : livraison, installation, maintenance des services d'infrastructure, correctifs et mises à niveau logiciels, retrait des racks.
- Serveurs Outposts : livraison, maintenance des services d'infrastructure, correctifs et mises à niveau logiciels. Vous êtes responsable de l'installation et de l'emballage du serveur pour le retour.

Les ressources partagées et tout transfert de données de la AWS région vers l'avant-poste vous sont facturés. Vous êtes également facturé pour les transferts de données effectués dans le but AWS de maintenir la disponibilité et la sécurité.

Pour connaître la tarification basée sur l'emplacement, la configuration et l'option de paiement, consultez :

- Les tarifs d'Outposts Racks
- Tarification des serveurs Outposts

Comment AWS Outposts fonctionne

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

Le diagramme suivant illustre les deux facteurs de forme d'Outpost.

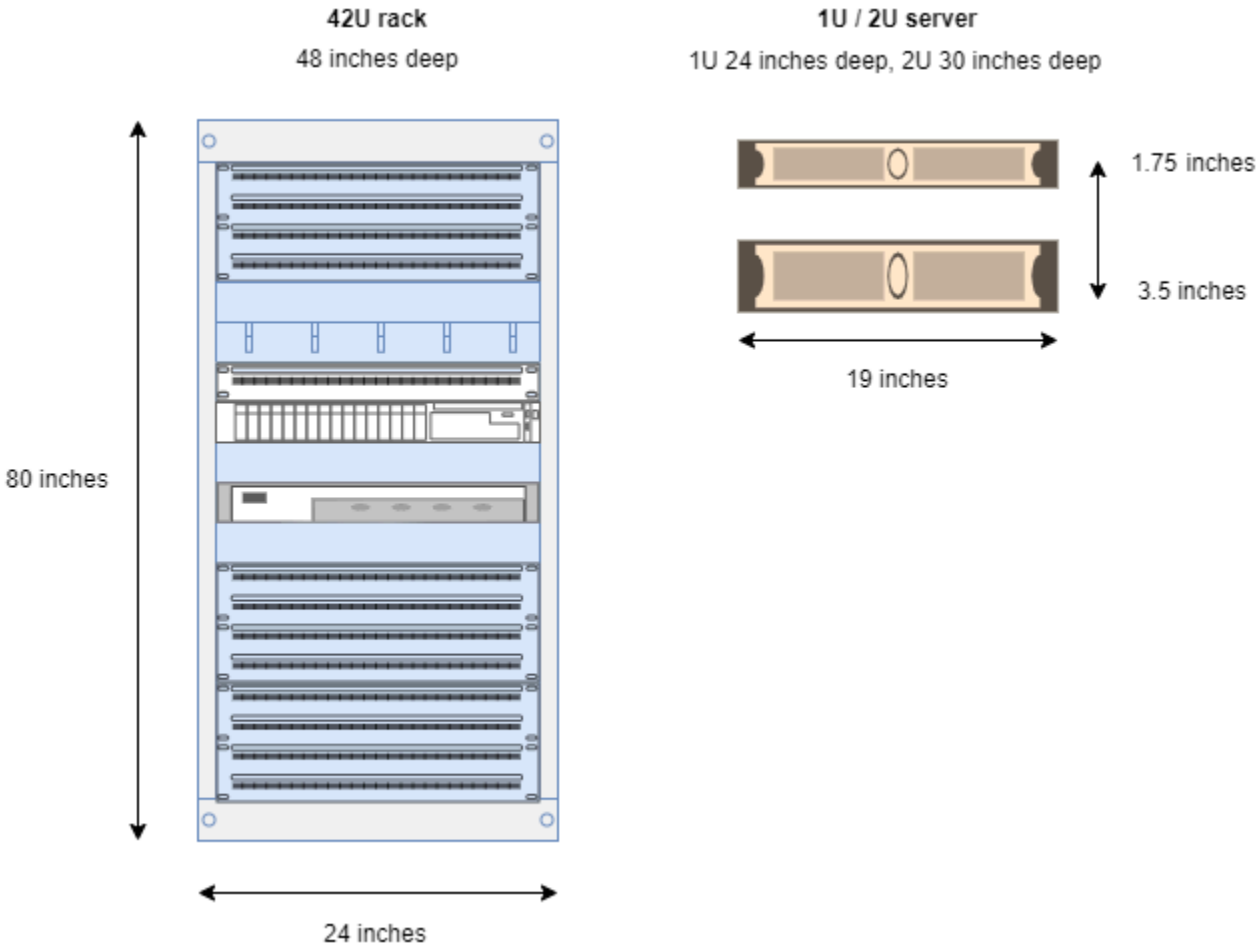


Table des matières

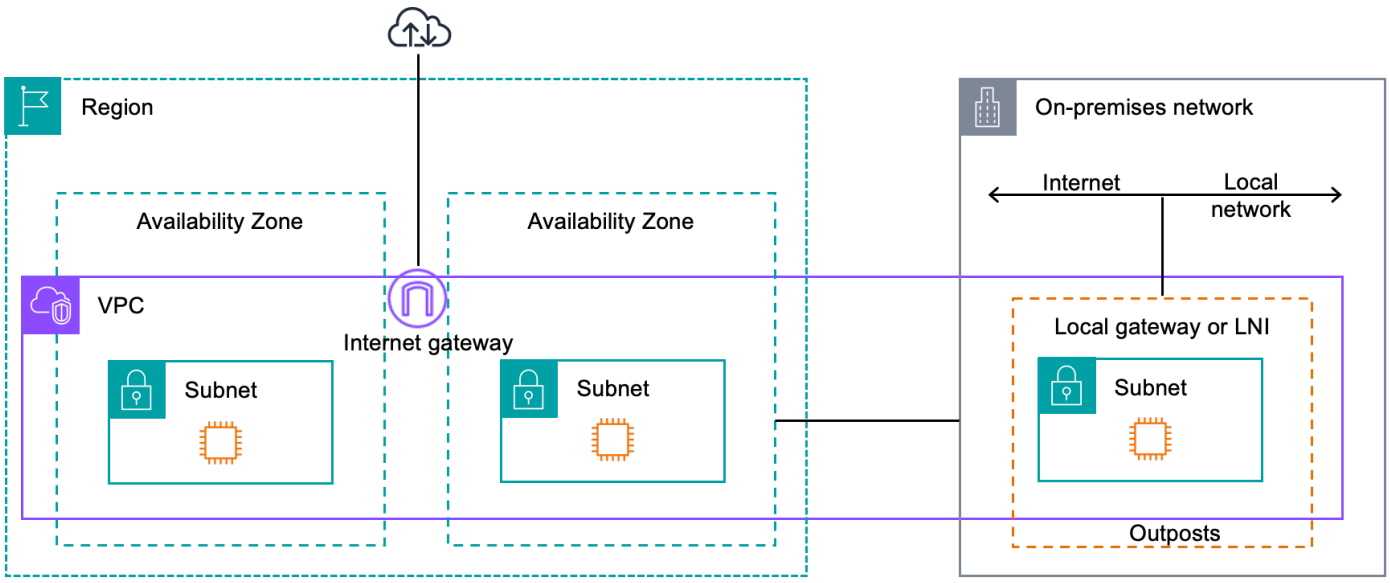
- DNS
- Liaison de service
- Passerelles locales
- Interfaces de réseau local

Composants réseau

AWS Outposts étend un Amazon VPC d'une AWS région à un avant-poste avec les composants VPC accessibles dans la région, notamment les passerelles Internet, les passerelles privées virtuelles, les passerelles de transit Amazon VPC et les points de terminaison 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 diagramme suivant illustre les composants réseau de votre Outpost.

- Un Région AWS et un réseau sur site
- Un VPC constitué de plusieurs sous-réseaux dans la région
- Un Outpost dans le réseau sur site
- La connectivité entre l'avant-poste et le réseau local a fourni :
  - Pour les Outposts : une passerelle locale
  - Pour les serveurs Outposts : une interface réseau locale (LNI)



VPCs 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'Amazon Resource Name (ARN) 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' EC2 instance lorsque vous lancez l' EC2 instance 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 en accueillir plusieurs VPCs qui peuvent avoir un ou plusieurs sous-réseaux Outpost. Pour en savoir plus sur les quotas de VPC, consultez Quotas Amazon VPC dans le Guide de l'utilisateur Amazon VPC.

Vous créez les sous-réseaux Outpost à partir de la plage CIDR du VPC dans lequel vous avez créé l'Outpost. Vous pouvez utiliser les plages d'adresses Outpost pour les ressources, telles que EC2 les instances 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 fonctionnent de la même manière pour les sous-réseaux Outpost que 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 en guise de 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 l'ensemble du trafic du VPC, y compris le sous-réseau Outpost ayant une destination dans le CIDR du VPC, continue d'être routé 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 l'ensemble du routage d'un VPC, y compris le trafic entre les instances Outpost au sein du même VPC.

- AWS Destinations 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 virtuelles AWS Transit Gateway, les passerelles Internet et le peering VPC.

  Si vous disposez d'une connexion d'appairage avec plusieurs d'entre eux VPCs sur le même avant-poste, le trafic entre les deux VPCs reste dans l'avant-poste et n'utilise pas le lien de service vers la région.
- Communication intra-VPC entre Outposts dotés d’une passerelle locale : vous pouvez établir une communication entre les sous-réseaux d’un même VPC à travers différents Outposts dotés d’une passerelle locale en utilisant le routage VPC direct. Pour plus d'informations, consultez :
  - Routage VPC direct
  - Routage vers une passerelle locale AWS Outposts

DNS

Pour les interfaces réseau connectées à un VPC, les EC2 instances 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 domaine, le routage DNS et la surveillance de l’état pour les instances s’exécutant dans votre Outpost. Les zones de disponibilité hébergées publiques et privées sont prises en charge pour le routage du 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.

Les délais de résolution DNS peuvent être plus longs avec Route 53, en fonction de la latence du chemin entre votre avant-poste et la AWS région. 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 jeux d’options DHCP pour vos serveurs DNS sur site et les associer au VPC. Vous devez également vérifier 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 Outposts dotés d'une passerelle locale. Sachant que les jeux d’options DHCP s’étendent au VPC, les instances situées dans les sous-réseaux Outpost et les sous-réseaux de zone de disponibilité du VPC essaieront d’utiliser les serveurs DNS spécifiés pour la résolution de noms DNS.

La journalisation des requêtes n’est pas prise en charge pour les requêtes DNS provenant d’un Outpost.

Liaison de 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. La liaison de service est un jeu chiffré des connexions VPN qui sont utilisées chaque fois que l'Outpost communique avec la région d'origine choisie. Vous pouvez utiliser un réseau local virtuel (VLAN) pour segmenter le trafic sur la liaison 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 liaison de service est créée au moment où votre Outpost est provisionné. Si vous disposez d'un facteur de forme de serveur, c'est vous qui créez la connexion. Si vous avez un rack, AWS crée le lien de service. Pour plus d'informations, consultez :

- AWS Outposts connectivité à Régions AWS
- Livre blanc sur le routage des applications/charges de travail dans le AWS Outposts cadre de la conception et de l'architecture de haute disponibilité AWS

Passerelles locales

Les racks Outposts incluent une passerelle locale qui fournit la connectivité à votre réseau local. Si vous avez un rack Outposts, vous pouvez inclure une passerelle locale comme cible, la destination étant votre réseau local. Les passerelles locales ne sont disponibles que pour les racks Outposts et ne peuvent être utilisées que dans les VPC et les tables de routage de sous-réseaux associées à un rack Outposts. Pour plus d'informations, consultez :

- Passerelles locales pour vos étagères Outposts
- Livre blanc sur le routage des applications/charges de travail dans le AWS Outposts cadre de la conception et de l'architecture de haute disponibilité AWS

Interfaces de réseau local

Les serveurs Outposts incluent une interface réseau locale qui fournit une connectivité à votre réseau local. Une interface de réseau local est disponible uniquement pour les serveurs Outposts s'exécutant sur un sous-réseau Outpost. Vous ne pouvez pas utiliser une interface réseau locale à partir d'une EC2 instance située sur un rack d'Outposts ou dans la AWS région. L'interface de réseau

local est réservée aux emplacements sur site. Pour plus d’informations, consultez Interface réseau locale dans le Guide de l’utilisateur AWS Outposts pour les serveurs Outposts.

Exigences du site pour les rayonnages 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, reportez-vous à la section AWS Outposts Rack FAQs. Reportez-vous à la question : Dans quels pays et territoires le rack Outposts est-il disponible ?

Cette page décrit les exigences relatives aux racks Outposts. Si vous installez un rack Aggregation, Core, Edge (ACE), votre site doit également répondre aux exigences répertoriées dansExigences du site pour les racks Outpost ACE.

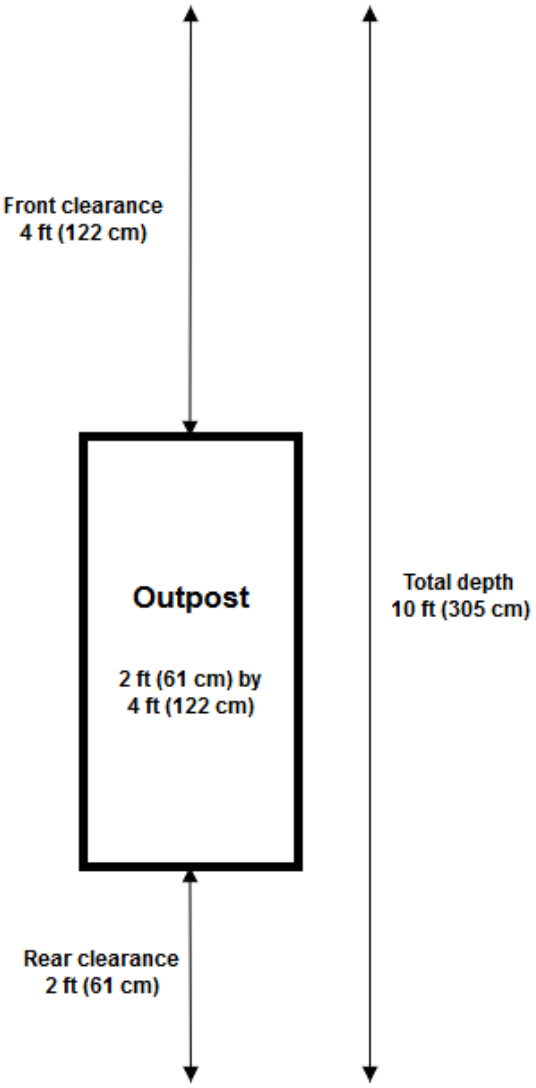
Pour connaître les exigences relatives aux serveurs Outposts, consultez Exigences du site pour les serveurs Outposts dans le Guide de l'utilisateur AWS Outposts pour les serveurs Outposts.

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. AWS fournit des supports de sol qui protègent contre une activité sismique allant jusqu'à 2,0 G avec tous les racks Outposts.
- Point de fixation — Nous vous recommandons de prévoir une liaison wire/point à la position du rack afin que votre électricien puisse coller les racks lors de l'installation, ce qui sera validé par le technicien AWS certifié.

- Accès aux installations — Vous ne modifierez pas les installations d'une manière qui nuirait à la capacité d'accéder AWS à l'avant-poste, de le desservir ou de le supprimer.
- 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.
- Fournissez une fibre monomode (SMF) avec un connecteur Lucent (LC), une fibre multimode (MMF) ou une fibre MMF avec LC. OM4
- 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, le réseau étendu et tous les appareils situés entre l'avant-poste et les destinations de trafic local, ainsi que la destination dans la AWS région.

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 OM4 MMF 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	— 40 G DE BASE - IR4 (L) LR4 — 40 G DE BASE- LR4
Application de dérivation 4 x 10 Gbit/s	MMF	— 40 G DE BASE- ESR4 — 40 G DE BASE- SR4
100 Gbit/s	SMF	— 100 G DE PSM4 MSA

Vitesse de la liaison montante	Type de fibre	Norme optique
		— 100 G DE BASE- CWDM4 — 100 G DE BASE- LR4
Application de dérivation 4 x 25 Gbit/s	MMF	— 100 G DE BASE- SR4

Agrégation de liens Outpost et VLANs

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

Les éléments suivants VLANs sont requis pour chaque périphérique réseau Outpost. Pour de plus amples informations, veuillez consulter Virtuel LANs.

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 le même VLANs ou un autre VLANs pour le lien 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 les sections Agrégation de liens et Virtual LANs.

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 appareils du réseau Outpost nécessite un CIDR et une adresse IP pour le lien de service et la passerelle locale. VLANs 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) – Adresse IP de la liaison de service	– CIDR de la passerelle locale (/30 ou /31) – 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'avant-poste et les points de terminaison des liaisons de service dans la région parent. AWS Pour plus d'informations sur la liaison de service, consultez AWS Outposts connectivité aux AWS régions.

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 AWS Direct Connect connexion ou une connexion Internet publique pour reconnecter l'avant-poste à la AWS région. 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.

Pour plus d'informations sur les exigences relatives aux liaisons de service, telles que le MTU et la latence de 175 ms, consultez la section Connectivité via une liaison de service.

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 la consommation électrique maximale de votre ressource Outpost est de 9,7 kVA, vous devez fournir des configurations d'alimentation pour 10 kVA : 4 x L6-30P ou IEC3 09, 2 gouttes vers S1 et 2 gouttes vers S2 pour une alimentation monophasée redondante. Les trois configurations d'alimentation sont décrites dans le deuxième tableau ci-dessous.

Pour connaître les besoins en énergie des différentes ressources d'Outpost, choisissez Parcourir le catalogue dans la AWS Outposts console à https://console.aws.amazon.com/outposts/l'adresse.

Exigence	Spécification de
Tension de ligne CA	Monophasé 208 à 277 VAC ; 50 ou 60 Hz Triphasé : • 208 à 250 VAC (Delta) ; 50 à 60 Hz • 346 à 480 VAC (Wye) ; 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, 32 A ou 50 A avec disjoncteur à courbe 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)	Connecteurs monophasés 3XL6-30P, P+P+E, 30A ou 3x 0309 P +N+E, 32A IEC6 IP67 Triphasé, Wye 1x IEC6 0309, 3P+N+E, position d'horloge 7, prise 30A ou 1x IEC6 0309 IP67, 3P+N+E, position d'horloge 6, prise 32A IP67 Hubbell CS8365 C triphasé, Delta 1xNEMA Twistlock, 3P+E, sol central, prise 50 A

Exigence	Spécification de
	Note La meilleure pratique consiste à associer une IP67 prise à un IP67 réceptacle. Si cela n'est pas possible, la IP67 prise sera couplée à une IP44 prise. La valeur nominale de la prise combinée 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 IEC3 09 ; 1 chute vers S1 et 1 goutte vers S2	2 x AH53 0P7W, AH532 P6W ou CS8365 C ; 1 chute vers S1 et 1 goutte vers S2	Non offert	1 x AH53 0P7W, AH532 P6W ou CS8365 C ; 1 chute vers S1
10 kVA	4 x L6-30P ou IEC3 09 ; 2 gouttes pour S1 et 2 gouttes pour S2		2 x L6-30P ou IEC3 09 ; 2 gouttes vers S1	
15 kVA	6 x L6-30P ou IEC3 09 ; 3 gouttes pour S1 et 3 gouttes pour S2		3 x L6-30P ou IEC3 09 ; 3 gouttes jusqu'à S1	

Si les fouets AC AWS fournis comme décrit précédemment 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 AWS représentant des modifications apportées à la prise secteur. Sur demande, vous fournirez 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 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. Ils placeront le rack à la position identifiée. 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 avant d'apporter des modifications au matériel ou aux installations électriques de l'Outpost. AWS Vous acceptez de fournir des AWS documents attestant de la conformité et de la sécurité de toute modification. AWS n'est pas responsable des risques créés par l'installation électrique ou le câblage électrique des installations de l'Outpost ou par toute modification. 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 lorsque vous confirmez que la capacité Amazon EC2 et Amazon EBS pour votre rack Outposts est disponible auprès de votre. Compte AWS

Exigences du site pour les racks Outpost ACE

> **Note**
>
> S'applique uniquement si vous avez besoin d'un rack ACE.

Un rack Aggregation, Core, Edge (ACE) fait office de point d'agrégation réseau pour les déploiements d'Outpost sur plusieurs racks. Vous devez installer un rack ACE si vous disposez de quatre racks de calcul ou plus. Si vous avez moins de quatre racks de calcul mais que vous prévoyez de passer à quatre racks ou plus à l'avenir, nous vous recommandons d'installer un rack ACE.

Pour installer un rack ACE, vous devez satisfaire aux exigences de cette section en plus de celles répertoriées dansExigences du site pour les rayonnages Outposts.

> **Note**
>
> Les racks ACE ne sont pas entièrement fermés et ne comportent ni porte avant ni porte arrière.

Installations

Voici les exigences relatives aux installations pour un rack ACE.

- Alimentation — Tous les racks ACE sont livrés avec un système monophasé de 10 kVA (connecteurs AA+BB, IEC6 0309 ou L6-30P Whip).
- Support de poids — Le porte-bagages ACE pèse 705 livres (320 kg).
- Dimension du dégagement et de la taille — Le rack ACE mesure 80 pouces (203 cm) de haut, 24 pouces (61 cm) de large et 42 pouces (107 cm) de profondeur.

  Si le rack ACE est doté de bras de gestion des câbles, la largeur du rack est de 36 pouces (91,5 cm).

Réseaux

Voici les exigences réseau pour un rack ACE. Pour comprendre comment le rack ACE connecte les périphériques réseau Outposts, vos périphériques réseau locaux et vos racks Outposts, voir. Connectivité au rack ACE

- Configuration requise pour le réseau en rack : assurez-vous de respecter les exigences répertoriées dans les Connectivité réseau locale pour les racks Outposts sections Liste de contrôle de préparation du réseau et, à l'exception des modifications suivantes :
  - Le rack ACE possède quatre périphériques réseau qui se connectent aux périphériques en amont, et non deux comme dans le cas d'un seul rack Outposts.
  - Les racks ACE ne prennent pas en charge les liaisons montantes de 1 Gbit/s.
- Vitesse de liaison montante — Fournissez des liaisons montantes avec des vitesses de 10 Gbit/s, 40 Gbit/s ou 100 Gbit/s. Pour les recommandations de bande passante pour la connexion par liaison de service,Recommandations concernant la bande passante de la liaison de service.

  > **Important**
  >
  > Les racks ACE ne prennent pas en charge les liaisons montantes de 1 Gbit/s.

- Fibre — Fournissez une fibre monomode (SMF) avec un connecteur Lucent (LC) ou une fibre multimode (MMF) avec un connecteur Lucent (LC). Pour obtenir la liste complète des types de fibres et des normes optiques pris en charge, consultezVitesse de liaison montante, ports et fibre.
- Appareil en amont : fournissez deux ou quatre périphériques en amont, qui peuvent être des commutateurs ou des routeurs.
- VLAN de service et VLAN de passerelle locale — Pour chacun des quatre périphériques réseau ACE, vous devez fournir un VLAN de service et un VLAN de passerelle locale différent. Vous pouvez choisir de n'en fournir que deux distincts VLANs, l'un pour le VLAN de service et l'autre pour le VLAN de passerelle local, ou d'en avoir un différent VLANs dans chaque périphérique réseau ACE pour le VLAN de service et le VLAN LGW, soit un total de 8 appareils différents. VLANs Pour plus d'informations sur l'utilisation des groupes d'agrégation de liens (LAGs) et du VLAN, reportez-vous aux sections Agrégation de liaisons etVirtuel LANs.
- CIDR et adresse IP pour le lien de service et la passerelle locale VLANs — Nous recommandons d'allouer un sous-réseau dédié à chaque périphérique réseau ACE avec un CIDR /30 ou /31. Il est également possible d'allouer un seul sous-réseau /29 dans chaque VLAN de service et de passerelle locale. Dans les deux cas, vous devez spécifier les adresses IP que les périphériques

réseau ACE doivent utiliser. Pour de plus amples informations, veuillez consulter Connectivité de la couche réseau.

- Numéro de système autonome (ASN) du client et de l'avant-poste pour le VLAN de liaison de service et un VLAN de passerelle locale — L'Outpost établit une session d'appairage BGP externe (eBGP) entre chaque périphérique rack ACE et votre périphérique réseau local pour la connectivité du lien de service via le VLAN de liaison de service. En outre, il établit une session d'appairage eBGP entre chaque périphérique réseau ACE et un périphérique réseau local pour la connectivité entre votre réseau local et la passerelle locale. Pour plus d'informations, consultez Connectivité BGP de la liaison de service et Connectivité BGP de passerelle locale.

> **Important**
>
> Sous-réseaux d'infrastructure de liens de service : un sous-réseau d'infrastructure de liens de service (doit être /26) est requis pour chaque rack de calcul inclus dans votre installation d'Outposts.

Alimentation

Voici les exigences en matière d'alimentation pour un rack ACE.

Exigence	Spécification de
Tension de ligne CA	Monophasé 200 à 240 VAC ; 50 ou 60 Hz
Consommation d'énergie	10 kVA monophasé (AA+BB)
Protection du courant alternatif (disjoncteurs en amont)	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)	IEC6Types de connecteurs à fouet 0309 ou L6-30P.

Commandez un rack Outposts pour commencer. Après avoir installé votre équipement Outpost, lancez une EC2 instance Amazon et configurez la connectivité à votre réseau local.

Tâches

- Créez une commande pour un rack Outposts
- Lancez une instance sur votre rack Outposts
- Optimisez Amazon EC2 pour AWS Outposts

Créez une commande pour un rack Outposts

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 de plus amples informations, veuillez consulter Exigences du site pour les rayonnages Outposts.
- Vous devez disposer d'un plan AWS Enterprise Support ou d'un plan AWS Enterprise On-Ramp Support.
- Déterminez Compte AWS celui que vous utiliserez pour 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
- Étape 4 : Modifier la capacité de l'instance
- 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 à AWS.
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. Spécifiez ensuite cet Outpost lorsque vous passez votre 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 de plus amples informations, veuillez consulter the section called "Prérequis".

   > **Note**
   >
   > Si vous devez supprimer la connectivité privée de votre Outpost, vous devez contacter le AWS Support Centre.

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.

> **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 ne choisissez pas de payer la totalité à l'avance, vous devrez payer des frais mensuels pendant toute la durée du contrat.

  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, contactez le AWS Support centre 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 le nom et l'adresse du lieu 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.

Étape 4 : Modifier la capacité de l'instance

Un avant-poste fournit un pool de capacités de AWS calcul et de stockage sur votre site en tant qu'extension privée d'une zone de disponibilité dans une AWS région. La capacité de calcul et de stockage disponible dans l'Outpost étant limitée et déterminée par la taille et le nombre de racks AWS installés sur votre site, vous pouvez décider de la capacité d'Amazon, Amazon EBS et Amazon S3 dont vous avez besoin pour exécuter vos charges de travail initiales, faire face à la croissance future et fournir une AWS Outposts capacité supplémentaire afin d'atténuer les pannes de serveur et les événements de maintenance. EC2

La capacité de chaque nouvelle commande Outpost est configurée avec une configuration de capacité par défaut. Vous pouvez convertir la configuration par défaut pour créer différentes instances répondant aux besoins de votre entreprise. Pour ce faire, vous créez une tâche de capacité, vous spécifiez la taille et la quantité des instances, puis vous exécutez la tâche de capacité pour implémenter les modifications.

> **Note**
>
> - Vous pouvez modifier le nombre de tailles d'instance après avoir passé commande pour vos Outposts.
> - La taille et la quantité des instances sont définies au niveau de l'avant-poste.
> - Les instances sont placées automatiquement conformément aux meilleures pratiques.

Pour modifier la capacité de l'instance

1. Dans le volet de navigation de gauche de la AWS Outposts console, sélectionnez Capacity tasks.

2. Sur la page Tâches de capacité, choisissez Créer une tâche de capacité.
3. Sur la page de démarrage, choisissez la commande.
4. Pour modifier la capacité, vous pouvez suivre les étapes de la console ou télécharger un fichier JSON.

Console steps

1. Choisissez Modifier la configuration de la capacité d'un avant-poste.
2. Choisissez Suivant.
3. Sur la page Configurer la capacité de l'instance, chaque type d'instance indique une taille d'instance avec la quantité maximale présélectionnée. Pour ajouter d'autres tailles d'instance, choisissez Ajouter une taille d'instance.
4. Spécifiez la quantité d'instance et notez la capacité affichée pour cette taille d'instance.
5. Consultez le message à la fin de chaque section sur le type d'instance qui vous indique si votre capacité est dépassée ou insuffisante. Effectuez des ajustements au niveau de la taille ou de la quantité de l'instance pour optimiser votre capacité totale disponible.
6. Vous pouvez également demander AWS Outposts à optimiser la quantité d'instances pour une taille d'instance spécifique. Pour ce faire :
   a. Choisissez la taille de l'instance.
   b. Choisissez Auto-balance à la fin de la section relative au type d'instance.
7. Pour chaque type d'instance, assurez-vous que la quantité d'instances est spécifiée pour au moins une taille d'instance.
8. Choisissez Suivant.
9. Sur la page Réviser et créer, vérifiez les mises à jour que vous demandez.
10. Choisissez Créer. AWS Outposts crée une tâche de capacité.
11. Sur la page de la tâche de capacité, surveillez l'état de la tâche.

> **Note**
>
> - AWS Outposts peut vous demander d'arrêter une ou plusieurs instances en cours d'exécution pour permettre l'exécution de la tâche de capacité. Une fois que vous aurez arrêté ces instances, la tâche AWS Outposts sera exécutée.

- Si vous devez modifier votre capacité après avoir terminé votre commande, contactez le AWS Support centre pour effectuer les modifications.

Upload a JSON file

1. Choisissez Télécharger une configuration de capacité.
2. Choisissez Suivant.
3. Sur la page Plan de configuration de la capacité de téléchargement, téléchargez le fichier JSON qui spécifie le type, la taille et la quantité de l'instance.

   Example

   Exemple de fichier JSON :

```
{
    "InstancePools": [
        {
            "InstanceType": "c5.24xlarge",
            "Count": 1
        },
        {
            "InstanceType": "m5.24xlarge",
            "Count": 2
        }
    ]
}
```

4. Passez en revue le contenu du fichier JSON dans la section Plan de configuration des capacités.
5. Choisissez Suivant.
6. Sur la page Réviser et créer, vérifiez les mises à jour que vous demandez.
7. Choisissez Créer. AWS Outposts crée une tâche de capacité.
8. Sur la page de la tâche de capacité, surveillez l'état de la tâche.

> **Note**
>
> - AWS Outposts peut vous demander d'arrêter une ou plusieurs instances en cours d'exécution pour permettre l'exécution de la tâche de capacité. Une fois que vous aurez arrêté ces instances, la tâche AWS Outposts sera exécutée.
> - Si vous devez modifier votre capacité après avoir terminé votre commande, contactez le AWS Support centre pour effectuer les modifications.
> - Pour résoudre les problèmes, consultez la section Résolution des problèmes liés aux tâches de capacité.

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

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 AWS compte.

Lancez une instance sur votre rack Outposts

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 EC2 des instances Amazon et créez des volumes Amazon EBS sur votre Outpost à l'aide d'un sous-réseau Outpost. Vous pouvez aussi créer des instantanés de volumes Amazon EBS sur votre Outpost. Pour plus d'informations, consultez les instantanés locaux d'Amazon EBS AWS Outposts dans le guide de l'utilisateur d'Amazon EBS.

Prérequis

Vous devez avoir un outpost installé sur votre site. Pour plus d'informations, consultez Créer une commande pour un rack Outposts.

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 le rack Outposts.
3. Dans le volet de navigation, choisissez Your, VPCs puis Create VPC.
4. Choisissez VPC uniquement.
5. (Facultatif) Dans le champ Name tag, entrez le nom du VPC.
6. Pour le bloc IPv4 CIDR, choisissez la saisie manuelle IPv4 CIDR et entrez la plage d' IPv4 adresses du VPC dans la IPv4 zone de texte 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 IPv6 CIDR, choisissez Aucun bloc IPv6 CIDR.
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 la section Composants réseau.

> **Note**
>
> Si vous lancez une instance dans un sous-réseau Outpost qui a été partagée avec vous par un autre Compte AWS, passez à l'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 Passerelles locales.

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

Utilisez la procédure suivante pour créer une table de routage personnalisée pour votre passerelle locale.

Pour créer une table de routage de passerelle locale 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 Table de routage de passerelle locale.
4. Choisissez Créer une table de routage de passerelle locale.
5. (Facultatif) Pour Nom, entrez un nom pour votre table de routage.
6. Pour Passerelle locale, choisissez votre passerelle locale.
7. Pour Mode, choisissez un mode de communication avec votre réseau sur site.
   - Choisissez le routage VPC direct pour utiliser les adresses IP privées de vos instances.
   - Choisissez CoIP pour utiliser les adresses des pools d'adresses IP appartenant à vos clients. Pour plus d'informations, consultez la section Création d'un pool CoIP.
8. (Facultatif) Pour ajouter une balise, choisissez Ajouter une nouvelle balise et saisissez une clé et une valeur de balise.
9. Choisissez Créer une table de routage de passerelle locale.

3b : Associer le VPC à la table de routage personnalisée

Utilisez la procédure suivante pour associer un VPC à votre table de routage de passerelle locale. Ils ne sont pas associés par défaut.

Pour associer un VPC à la table de routage personnalisée de la 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, 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) Pour ajouter une balise, choisissez Ajouter une nouvelle balise et saisissez une clé et une valeur de balise.
7. Choisissez Associate VPC (Associer un VPC).

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

Ajoutez une entrée de route dans la table de routage du sous-réseau Outpost pour activer le trafic entre les sous-réseaux Outpost et la passerelle locale.

Les sous-réseaux Outpost d'un VPC, qui est associé à une table de routage de passerelle locale, peuvent avoir un type de cible supplémentaire, 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 la passerelle locale. 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 de la passerelle locale.

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

Pour ajouter une entrée de route avec la passerelle locale comme cible dans la table de routage du sous-réseau

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 : Créez un domaine de routage de passerelle local en associant la table de routage personnalisée aux groupes VIF

Les groupes VIF sont des groupements logiques d'interfaces virtuelles (VIFs). Associez la table de routage de passerelle locale au groupe VIF pour créer un domaine de routage de passerelle local.

Pour associer la table de routage personnalisée aux groupes 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 volet de navigation, choisissez Networking puis LGW routing domain.
4. Choisissez Créer un domaine de routage LGW.
5. Entrez un nom pour le domaine de routage de la passerelle locale.
6. Choisissez la passerelle locale, le groupe VIF de passerelle locale et la table de routage de la passerelle locale.
7. Choisissez Créer un domaine de routage LGW.

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

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, consultez Adresses IP clients.

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

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 plus d'informations sur le partage d'une IPv4 adresse appartenant à un client, consultez. the section called "Partage d'une ressource Outpost"

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 votre client, la session BGP sur le VLAN de la passerelle locale est active depuis vos périphériques réseau.
- Pour le trafic allant des Outposts sur site vers les Outposts, 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 d'envoyer CNDs les publicités de routage BGP des sous-réseaux locaux 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 le CNDs 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

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 le CoIP Elastic IPs pour adresser les instances de l'Outpost, la plage d'adresses 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.

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 EC2 des instances 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 EC2 instance d'un

sous-réseau Outpost, vous pouvez spécifier une paire de clés lorsque vous lancez l'instance, comme vous le faites pour les instances d'un sous-réseau de zone de disponibilité.

Considérations

- Si vous attachez des volumes de données par blocs soutenus par des systèmes de stockage par blocs tiers compatibles pendant le processus de lancement de l'instance sur Outpost, consultez ce billet de blog Simplifier l'utilisation du stockage par blocs tiers avec. AWS Outposts
- Vous pouvez créer un groupe de placement pour influencer la manière dont Amazon EC2 doit tenter de placer des groupes d'instances interdépendantes sur le matériel des 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'instance dans la EC2 console Amazon. 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.
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 Lancer une EC2 instance dans le guide de EC2 l'utilisateur Amazon :

> **Note**
>
> Si vous ajoutez un volume Amazon EBS, vous devez utiliser le type de volume gp2.

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 Connect to your EC2 instance dans le guide de EC2 l'utilisateur Amazon.

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 EC2 console Amazon sur la page détaillée 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, consultez Connect to your EC2 instance dans le guide de EC2 l'utilisateur Amazon.

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 EC2 console Amazon sur la page détaillée 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
```

Optimisez Amazon EC2 pour AWS Outposts

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

Table des matières

Hôtes dédiés sur Outposts

Un hôte EC2 dédié Amazon est un serveur physique dont la capacité d' EC2 instance est 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 la section Dedicated Hosts on AWS Outposts dans le guide de EC2 l'utilisateur Amazon.

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

Dedicated Hosts vous permet de modifier la disposition des serveurs dans votre déploiement d'Outpost sans avoir à vous contacter Support. Lorsque vous achetez de la capacité pour votre avant-poste, vous spécifiez une structure EC2 de capacité fournie par 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 la section Allocation d'un hôte dédié dans le guide de EC2 l'utilisateur Amazon.

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 possédez un rack Outposts, vous pouvez utiliser ces fonctionnalités d'hôtes dédiés pour minimiser l'impact des pannes matérielles corrélées. Pour plus d'informations sur la restauration d'instances, consultez la section Placement automatique d'hôtes dédiés et affinité d'hôte dans le guide de EC2 l'utilisateur Amazon.

Vous pouvez partager des hôtes dédiés à l'aide de AWS Resource Access Manager. Le partage d'hôtes dédiés vous permet de répartir les hôtes d'un déploiement Outpost entre plusieurs Comptes AWS. Pour de plus amples informations, veuillez consulter 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 Résilience des instances.

Groupes de placement sur Outposts

AWS Outposts soutient les groupes de placement. Utilisez les groupes de placement pour influencer la manière dont Amazon EC2 doit tenter 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 des groupes de placement de spread au niveau de l'hôte 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 des groupes de placement, consultez la section Groupes de placement et Groupes de placement AWS Outposts dans le Guide de EC2 l'utilisateur Amazon.

Pour plus d'informations sur la AWS Outposts haute disponibilité, consultez la section Considérations relatives à la conception et à l'architecture de AWS Outposts haute disponibilité.

AWS Outposts connectivité aux AWS régions

AWS Outposts prend en charge la connectivité au réseau étendu (WAN) via la connexion Service Link.

Table des matières

Connectivité via un lien de service

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

Une fois la connexion par liaison de service établie, votre avant-poste devient opérationnel et est géré par AWS. Le lien de service facilite le trafic suivant :

- Trafic VPC du client entre l'Outpost et tout ce qui y est associé. VPCs
- Outposts le trafic de gestion, tel que la gestion des ressources, la surveillance des ressources et les mises à jour des micrologiciels et des logiciels.

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

Le trafic qui passe d'une instance dans Outposts à une instance dans la région a un MTU de 1 300.

Recommandations concernant la bande passante de la liaison de service

Pour une expérience et une résilience optimales, AWS vous devez utiliser une connectivité redondante d'au moins 500 Mbits/s pour chaque rack de calcul et une latence aller-retour maximale de 175 ms pour la connexion par liaison de service à la AWS région. Vous pouvez utiliser AWS Direct Connect ou une connexion Internet pour la liaison de service. Les exigences minimales de 500 Mbits/s et de temps d'aller-retour maximales pour la connexion par liaison de service vous permettent de lancer des EC2 instances Amazon, d'attacher des volumes Amazon EBS et d'accéder à AWS des services tels qu'Amazon EKS, Amazon EMR CloudWatch et à des métriques avec des performances optimales.

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

- Nombre de AWS Outposts racks 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 concernant la bande passante de liaison de service requise pour vos besoins, contactez votre représentant AWS commercial ou votre partenaire APN.

Connexions Internet redondantes

Lorsque vous établissez une connectivité entre votre avant-poste et la AWS région, nous vous recommandons de créer plusieurs connexions pour une disponibilité et une résilience accrues. 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.

Configurez votre lien de service

Les étapes suivantes expliquent le processus de configuration des liaisons de service.

1. Choisissez une option de connexion entre vos Outposts et la région d'origine AWS . Vous pouvez choisir une connexion publique ou privée.

2. Après avoir commandé vos racks Outposts, vous AWS contacte pour collecter le VLAN, l'IP, le BGP et le sous-réseau d'infrastructure. IPs Pour de plus amples informations, veuillez consulter Connectivité réseau locale.
3. Lors de l'installation, AWS configure le lien de service sur l'Outpost en fonction des informations que vous avez fournies.
4. Vous configurez vos périphériques réseau locaux, tels que les routeurs, pour qu'ils se connectent à chaque périphérique réseau Outpost via la connectivité BGP. Pour plus d'informations sur la connectivité VLAN, IP et BGP des liaisons de service, consultez. Réseaux
5. Vous configurez vos périphériques réseau, tels que les pare-feux, pour permettre à vos Outposts d'accéder à AWS la région ou à la région d'origine. AWS Outposts utilise le sous-réseau de l'infrastructure des liaisons de service IPs pour configurer les connexions VPN et échanger le contrôle et le trafic de données avec la région. L'établissement d'une liaison de service est toujours initié depuis Outpost.

> **Note**
>
> Vous ne pourrez pas modifier la configuration du lien de service une fois la commande terminée.

Options de connectivité publique Service Link

Vous pouvez configurer le lien de service avec une connexion publique pour le trafic entre les Outposts et la région d'origine AWS . Vous pouvez choisir d'utiliser l'Internet public ou AWS Direct Connect public VIFs.

Si vous prévoyez d'inscrire uniquement AWS la région publique IPs (au lieu de 0.0.0.0/0) sur vos pare-feux, vous devez vous assurer que les règles de votre pare-feu correspondent up-to-date aux plages d'adresses IP actuelles. Pour plus d'informations, consultez les plages d'adresses AWS IP dans le guide de l'utilisateur Amazon VPC.

L'image suivante montre les deux options permettant d'établir une connexion publique par liaison de service entre vos Outposts et la AWS région :

Option 1. Connectivité publique via Internet

Cette option nécessite que le sous-réseau de l'infrastructure de liaison IPs de AWS Outposts service ait accès aux plages d'adresses IP publiques de votre AWS région ou de votre région d'origine. Vous devez autoriser AWS Region public IPs ou 0.0.0.0/0 sur les périphériques réseau tels que votre pare-feu.

Option 2. Connectivité publique par le biais AWS Direct Connect du public VIFs

Cette option nécessite que le sous-réseau IPs de l'infrastructure de liaison de AWS Outposts service ait accès aux plages d'adresses IP publiques de votre AWS région ou de votre région d'origine via le service DX. Vous devez autoriser AWS Region public IPs ou 0.0.0.0/0 sur les périphériques réseau tels que votre pare-feu.

Options de connectivité privée Service Link

Vous pouvez configurer le lien de service avec une connexion privée pour le trafic entre les Outposts et la région d'origine AWS . Vous pouvez choisir d'utiliser le transport AWS Direct Connect privé ou le transport en commun VIFs.

Sélectionnez l'option de connectivité privée lorsque vous créez votre Outpost dans la AWS Outposts console. Pour obtenir des instructions, voir Créer un avant-poste.

Lorsque vous sélectionnez l'option de connectivité privée, une connexion VPN Service Link est établie après l'installation de l'Outpost, à l'aide d'un VPC et d'un sous-réseau que vous spécifiez. Cela permet une connectivité privée via le VPC et minimise l'exposition du public à Internet.

L'image suivante montre les deux options permettant d'établir une connexion privée VPN par liaison de service entre vos Outposts et la AWS région :

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 AWS Identity and Access ManagementAWS Outposts
- Dans le même AWS compte et dans la même zone de disponibilité que votre Outpost, créez un VPC dans le seul but de garantir la connectivité privée d'Outpost avec un sous-réseau /25 ou supérieur qui n'entre pas en conflit avec 10.1.0.0/16. Par exemple, vous pouvez utiliser 10.3.0.0/16.
- Configurez le groupe de sécurité du sous-réseau pour autoriser le trafic pour les directions entrantes et sortantes UDP 443.
- Annoncez le CIDR du sous-réseau à votre réseau sur site. Vous pouvez l'utiliser AWS Direct Connect pour le faire. 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 .

> **Note**
>
> Pour sélectionner l'option de connectivité privée lorsque votre avant-poste est en attente, choisissez Outposts dans AWS Outposts la console, puis sélectionnez votre avant-poste. Choisissez Actions, Ajouter une connectivité privée, puis suivez les étapes.

Une fois que vous avez sélectionné l'option de connectivité privée pour votre Outpost, il crée AWS Outposts automatiquement un rôle lié à un service dans votre compte qui lui permet 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.

- Autorise le AWS Outposts service à associer les interfaces réseau à une instance de point de terminaison Service Link dans le compte.
- Attacher les interfaces réseau aux instances de point de terminaison de la liaison de service à partir du compte.

> **Important**
>
> Une fois votre Outpost installé, confirmez la connectivité au réseau privé IPs de votre sous-réseau depuis votre Outpost.

Option 1. Connectivité privée via le AWS Direct Connect privé VIFs

Créez une AWS Direct Connect connexion, une interface virtuelle privée et une passerelle privée virtuelle pour permettre à votre Outpost sur site d'accéder au VPC.

Pour plus d'informations, consultez les sections suivantes du guide de l'AWS Direct Connect utilisateur :

- Connexions dédiées et hébergées
- Création d'une interface virtuelle privée
- Associations de passerelles privées virtuelles

Si la AWS Direct Connect connexion se trouve dans un AWS compte différent de celui de votre VPC, consultez la section Association d'une passerelle privée virtuelle entre les comptes dans le guide de l'AWS Direct Connect utilisateur.

Option 2. Connectivité privée grâce au AWS Direct Connect transport en commun VIFs

Créez une AWS Direct Connect connexion, une interface virtuelle de transit et une passerelle de transit pour permettre à votre Outpost sur site d'accéder au VPC.

Pour plus d'informations, consultez les sections suivantes du guide de l'AWS Direct Connect utilisateur :

- Connexions dédiées et hébergées

- Création d'une interface virtuelle de transit vers la passerelle Direct Connect
- Associations de passerelles de transit

Pare-feu et liaison de service

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

Dans le schéma suivant, la configuration étend le VPC Amazon de la AWS région à l'avant-poste. Une interface virtuelle AWS Direct Connect publique est la connexion du lien de service. 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'avant-poste et tout ce qui y est associé VPCs

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.

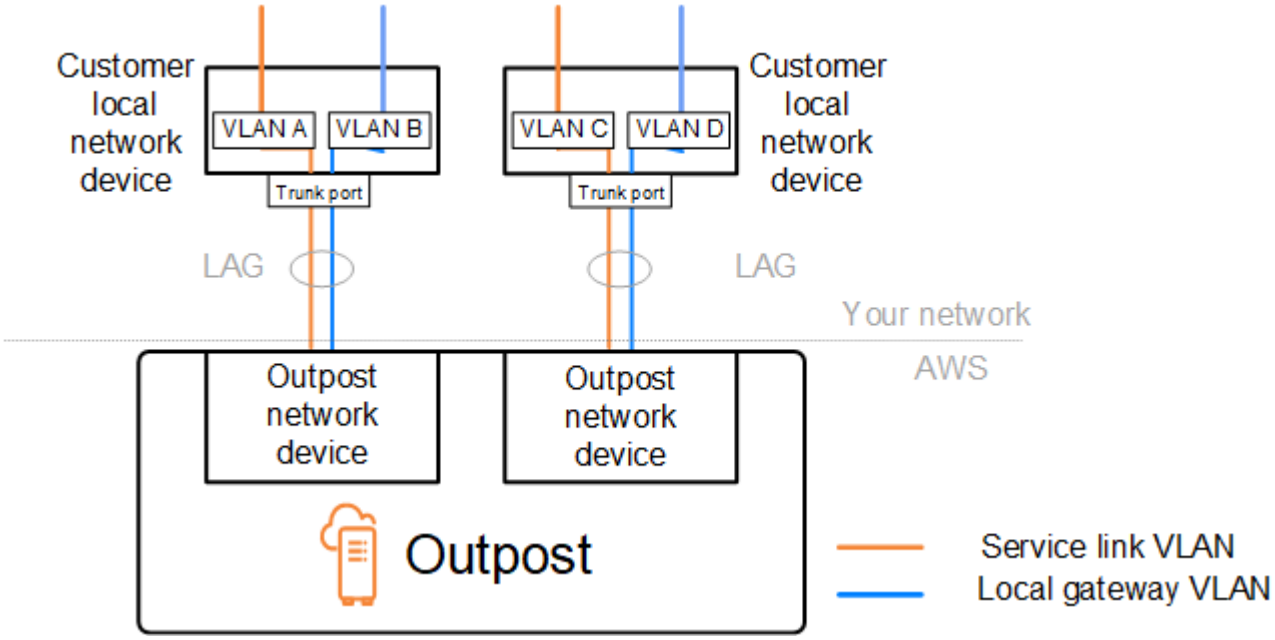
Si vous utilisez un pare-feu pour limiter la connectivité à partir du VLAN de la liaison de service, vous pouvez bloquer toutes les connexions entrantes. Vous devez autoriser les connexions sortantes vers l'avant-poste depuis la AWS région, conformément au tableau suivant. S'il s'agit d'un pare-feu avec 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	AWS Outposts liaison de service /26	443	AWS Outposts Public de la région IPs
TCP	1025-65535	AWS Outposts liaison de service /26	443	AWS Outposts Public de la région IPs

> **Note**
>
> Les instances d'un Outpost ne peuvent pas utiliser le lien 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.
> AWS Outposts les racks sont également conçus avec des équipements d'alimentation et de réseau redondants, y compris des composants de passerelle locaux. Pour plus d'informations, consultez Resilience in AWS Outposts.

Liste de vérification du dépannage du réseau Outposts Rack

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 le AWS support, en utilisant votre plan de support d'entreprise.

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 Edge connectés à AWS Direct Connect : interface virtuelle publique utilisée pour la connectivité des liaisons de service. Pour de plus amples informations, veuillez consulter AWS Direct Connect connectivité de l'interface virtuelle publique à AWS la région.
- Routeurs Edge connectés à AWS Direct Connect : interface virtuelle privée utilisée pour la connectivité des liaisons de service. Pour de plus amples informations, veuillez consulter AWS Direct Connect connectivité d'interface virtuelle privée à AWS la région.
- Routeurs Edge connectés à des fournisseurs de services Internet (ISPs) : Internet public utilisé pour la connectivité des liaisons de service. Pour de plus amples informations, veuillez consulter Connectivité de l'Internet public du FSI à la région AWS.

AWS Direct Connect connectivité de l'interface virtuelle publique à AWS la région

Utilisez la liste de contrôle suivante pour résoudre les problèmes liés aux routeurs Edge connectés AWS Direct Connect lorsqu'une interface virtuelle publique est utilisée pour la connectivité des liaisons 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. Il doit inclure les plages d'adresses IP AWS publiques ou la route par défaut.
3. Si vous ne recevez pas les plages d'adresses IP AWS publiques dans le VRF du lien de service, vérifiez les points suivants.
   a. Vérifiez l'état de la AWS Direct Connect liaison depuis le routeur Edge ou le 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 d'appairage BGP est défini`DOWN`, envoyez un ping à l'adresse AWS IP de l'homologue et vérifiez la configuration BGP dans le routeur Edge. Pour plus d'informations, consultez la section Résolution des problèmes AWS Direct Connect dans le guide de AWS Direct Connect l'utilisateur et l'état BGP de mon interface virtuelle est en panne dans la AWS console. Que dois-je faire ?

d. Si le BGP est établi et que vous ne voyez pas la route par défaut ou les plages d'adresses IP AWS publiques dans le VRF, contactez le AWS Support en utilisant votre plan de support Enterprise.

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. Si le pare-feu est statique, assurez-vous que les règles de sortie autorisent la plage d'adresses IP du lien de service de l'Outpost vers les plages d'adresses IP AWS publiques. Pour de plus amples informations, veuillez consulter AWS Outposts connectivité aux AWS régions.

   c. Si le pare-feu n'est pas dynamique, assurez-vous d'autoriser également le flux entrant (des plages d'adresses IP AWS publiques à la plage d'adresses IP du lien 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 captures de paquets MTR/traceroute/depuis votre routeur Edge vers les adresses IP AWS Direct Connect homologues. Partagez les résultats des tests avec le AWS support, en utilisant votre plan de support d'entreprise.

AWS Direct Connect connectivité d'interface virtuelle privée à AWS la région

Utilisez la liste de contrôle suivante pour résoudre les problèmes liés aux routeurs Edge connectés AWS Direct Connect lorsqu'une interface virtuelle privée est utilisée pour la connectivité des liaisons de service.

1. Si la connectivité entre le rack des Outposts et la AWS région utilise la fonctionnalité de connectivité AWS Outposts privée, vérifiez les points suivants.
   a. Envoyez un ping à l'adresse AWS IP d'appairage à distance depuis le routeur Edge et confirmez l'état de l'appairage BGP.
   b. Assurez-vous que l'appairage BGP via l'interface virtuelle AWS Direct Connect privée entre votre VPC de point de terminaison de liaison de service et l'Outpost installé dans vos locaux l'est. UP Pour plus d'informations, consultez la section Résolution des problèmes AWS Direct Connect dans le guide de AWS Direct Connect l'utilisateur. L'état BGP de mon interface virtuelle est en panne dans la AWS console. Que dois-je faire ? et Comment dépanner les problèmes de connexion BGP sur Direct Connect ?
   c. L'interface virtuelle AWS Direct Connect privée est une connexion privée à votre routeur de périphérie à l' AWS Direct Connect endroit que vous avez choisi, et elle utilise le protocole BGP pour échanger des itinéraires. 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 le réseau ACLs associé au point de terminaison privé du lien de service dans votre VPC autorise le trafic correspondant. Pour de plus amples informations, veuillez consulter 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, voir Présentation de la connectivité AWS Outposts privée.
   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 local compte plus de 100 réseaux, vous pouvez annoncer un itinéraire par défaut via la session BGP vers votre AWS 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 captures de paquets MTR/traceroute/depuis votre routeur Edge vers les adresses IP AWS Direct Connect homologues. Partagez les résultats des tests avec le AWS support, en utilisant votre plan de support d'entreprise.

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 EC2 instances ou équilibreurs de charge accessibles au public dans la région d'origine d'Outpost est accessible depuis votre appareil périphérique. Vous pouvez utiliser

une commande ping ou telnet pour vérifier la connectivité et utiliser ensuite traceroute pour vérifier le chemin réseau.

2. Si vous avez l' VRFs habitude de séparer le trafic sur votre réseau, vérifiez que le VRF de liaison de service comporte des itinéraires ou des politiques qui dirigent le trafic vers et depuis le FAI (Internet) et le 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. Vérifiez les configurations du VRFs et assurez-vous que le routage et les politiques requis pour la connectivité entre le VRF de liaison de service et le VRF du fournisseur de services Internet 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-feux locaux sont configurés pour autoriser la connectivité sortante (ports TCP 1025-65535 et UDP 443) entre les plages d'adresses IP du lien du service Outpost et les plages d'adresses IP publiques. AWS 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 ne montrent aucun problème, collectez les résultats de tous les tests (tels que MTR, telnet, traceroute, captures de paquets et journaux BGP) et contactez le support via votre plan de AWS support d'entreprise.

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 si des liaisons sont en panne ou si des modifications récentes apportées au routage (modifications des OSPF/ISIS/EIGRP métriques, modifications du plan de route BGP) dans votre réseau d'entreprise 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.

Passerelles locales pour vos étagères Outposts

La passerelle locale est un élément essentiel de l'architecture de vos racks Outposts. Une passerelle locale permet la connectivité entre vos sous-réseaux Outpost et votre réseau local. Si l'infrastructure sur site fournit un accès à Internet, les charges de travail exécutées sur des racks 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 AWS Direct Connect. Pour de plus amples informations, veuillez consulter AWS Outposts connectivité aux AWS régions.

Table des matières

Principes de base de la passerelle locale

AWS crée une passerelle locale pour chaque rack Outposts dans le cadre du processus d'installation. Un rack Outposts prend en charge une passerelle locale unique. La passerelle locale appartient au rack Compte AWS associé aux Outposts.

> **Note**
>
> Pour comprendre les limites de bande passante des instances pour le trafic passant par une passerelle locale, consultez la section Bande passante du réseau des EC2 instances Amazon dans le guide de EC2 l'utilisateur Amazon.

Une passerelle locale est dotée des composants suivants :

- Tables de routage : seul le propriétaire d'une passerelle locale peut créer des tables de routage de passerelle locales. Pour de plus amples informations, veuillez consulter the section called “Tables de routage”.

- 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 (VIFs) — La passerelle locale VIFs (interface virtuelle) est un composant d'interface logique des racks Outposts qui configure la connectivité VLAN, IP et BGP entre un périphérique réseau Outposts et un périphérique réseau sur site pour la connectivité de passerelle locale. AWS crée un VIF pour chaque LAG et ajoute les deux VIFs à un groupe VIF. La table de routage de la passerelle locale doit avoir un itinéraire par défaut vers les deux VIFs pour la connectivité au réseau local. Pour de plus amples informations, veuillez consulter Connectivité réseau locale.
- Groupes VIF : AWS ajoute VIFs ce qu'il crée à un groupe VIF. Les groupes VIF sont des groupements logiques de VIFs.
- Table de routage de passerelle locale et associations VPC — La table de routage de passerelle locale et les associations VPC vous permettent de vous connecter à des tables de routage VPCs de passerelle locales. Grâce à cette association, vous pouvez ajouter une route ciblée vers une passerelle locale dans la table de routage de votre sous-réseau Outposts. Cela permet la communication entre les ressources de votre sous-réseau Outposts et votre réseau local via la passerelle locale.
- Domaines de routage de passerelle locale — Un domaine de routage de passerelle local est l'association d'une table de routage de passerelle locale et d'un groupe VIF de passerelle local. Grâce à cette association, vous pouvez ajouter une route ciblée vers un groupe VIF de passerelle local dans votre table de routage de passerelle locale. Cela permet la communication entre les ressources de votre sous-réseau Outposts et votre réseau local via le groupe VIF sélectionné.

Lorsque vous AWS approvisionnez votre rack Outposts, 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 (VIFs) 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 pour créer un domaine de routage de passerelle local.

Routage par passerelle locale

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".

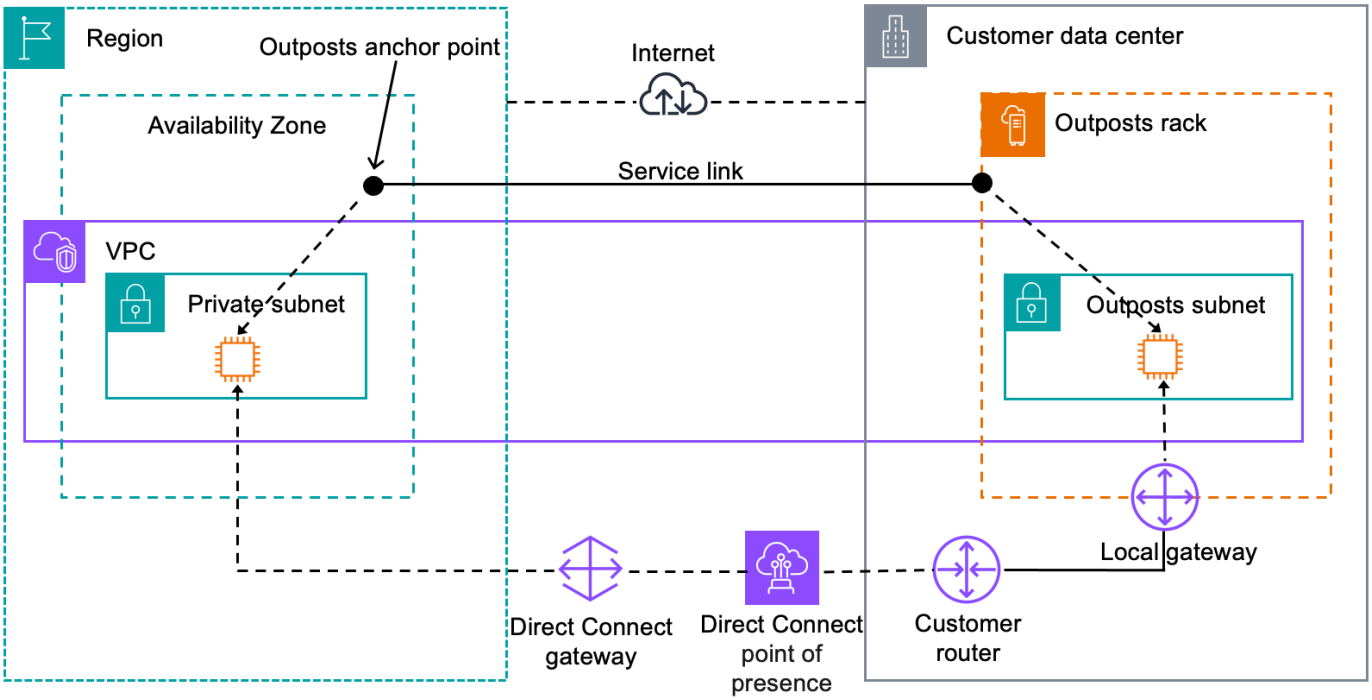
Connectivité via une passerelle locale

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, consultez 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

Dans le cadre de l'installation en rack, AWS crée la passerelle locale, les configurations VIFs et un groupe VIF. La passerelle locale appartient au AWS compte associé à l'Outpost. 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. Seul le propriétaire de la passerelle locale peut modifier la table de routage de la passerelle locale.

Les tables de routage du sous-réseau Outpost peuvent inclure un itinéraire vers les groupes VIF de passerelle locaux afin de fournir une connectivité à votre réseau local.

Les tables de routage des passerelles locales disposent d'un mode qui détermine la manière dont les instances du sous-réseau Outposts communiquent avec votre réseau local. L'option par défaut est le routage VPC direct, qui utilise les adresses IP privées des instances. L'autre option consiste à utiliser les adresses d'un pool d'adresses IP (CoIP) appartenant au client que vous fournissez. Le routage VPC direct et la CoIP sont des options mutuellement exclusives qui contrôlent le fonctionnement du routage. Pour déterminer la meilleure option pour votre Outpost, consultez Comment choisir entre les modes de routage CoIP et Direct VPC sur un rack Outposts. AWS

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 la section Utilisation de AWS Outposts ressources partagées.

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 publicité sur BGP concerne uniquement les adresses IP privées appartenant aux sous-réseaux de votre rack Outposts. Ce type de routage est le mode par défaut pour les Outposts. Dans ce mode, la passerelle locale n'exécute pas le NAT pour les instances, et vous n'avez pas besoin d'attribuer d'adresses IP élastiques à vos EC2 instances. 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 mode de routage VPC direct ne prend pas en charge les plages CIDR qui se chevauchent.

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

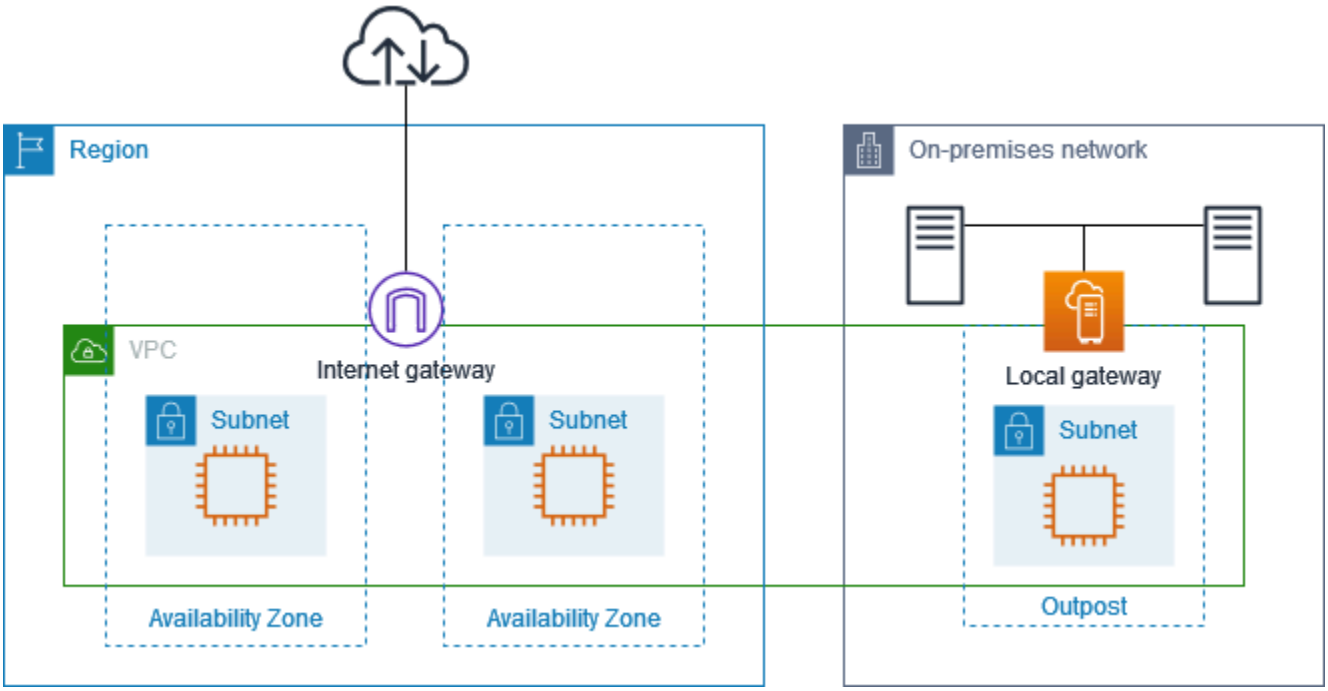
Les instances d'un sous-réseau Outpost peuvent accéder à Internet via la passerelle Internet attachée au VPC.

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 EC2 instance.
- 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
VPC CIDR	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.
on-premises network CIDR	*local-gateway-id*	Envoie le trafic destiné au réseau sur site vers la passerelle locale.

Exemple : connectivité Internet via le réseau sur site

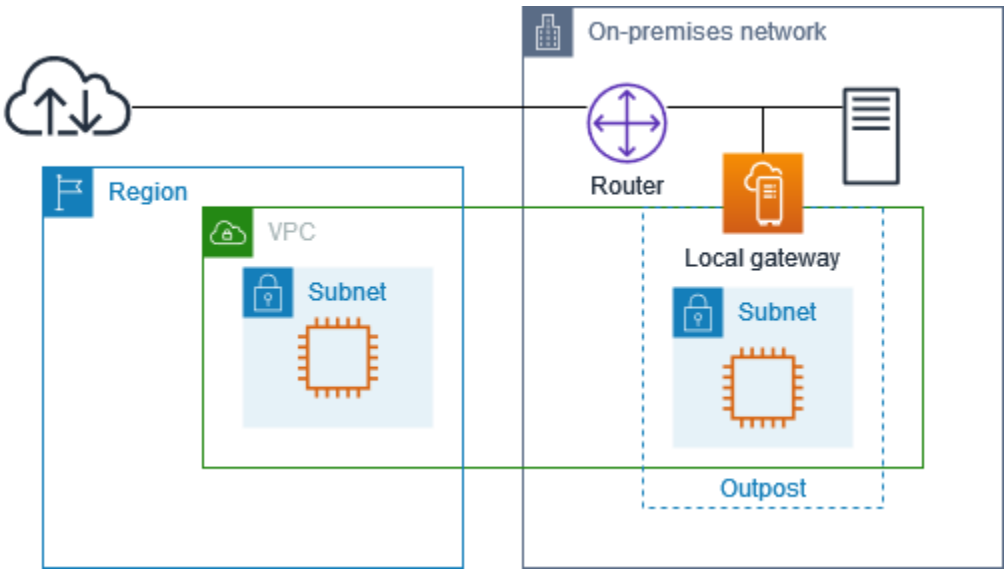
Les instances d'un sous-réseau Outpost peuvent accéder à Internet via le réseau sur site. Les instances du sous-réseau Outpost n'ont pas besoin d'adresse IP publique ou d'adresse IP Elastic.

Examinez la configuration suivante :

- Le sous-réseau Outpost possède une EC2 instance.
- 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
VPC CIDR	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 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 EC2 instances, en allouant une nouvelle adresse IP élastique issue du pool d'adresses IP appartenant au client, puis en l'attribuant à votre ressource. Pour de plus amples informations, veuillez consulter piscines CoIP.

> **Note**
>
> Pour un pool d'adresses IP appartenant au client, vous devez être en mesure de router l'adresse sur votre réseau.

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 Après avoir partagé le pool, les participants peuvent attribuer une adresse IP élastique à partir du pool d'adresses IP appartenant au client, puis l'attribuer à une EC2 instance sur l'Outpost. Pour de plus amples informations, veuillez consulter Ressources partagées.

Exemples

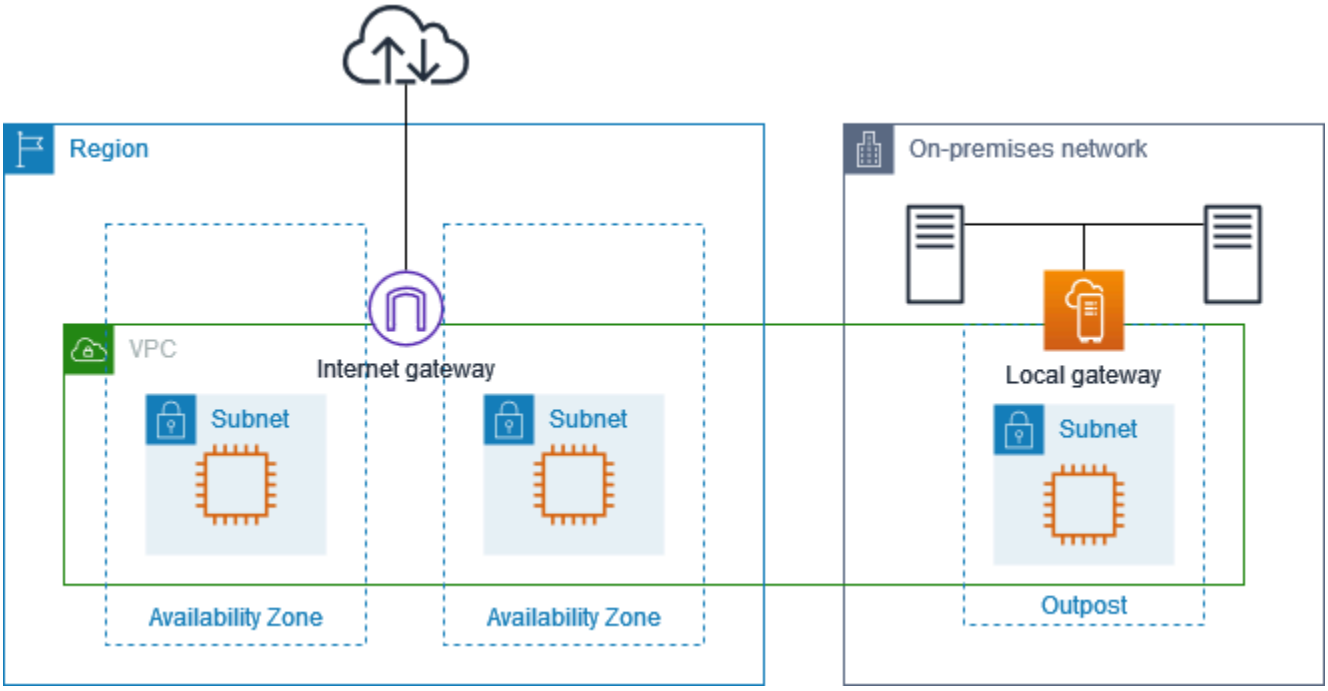
- Exemple : connectivité Internet via le VPC
- Exemple : connectivité Internet via le réseau sur site

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 EC2 instance.
- 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.

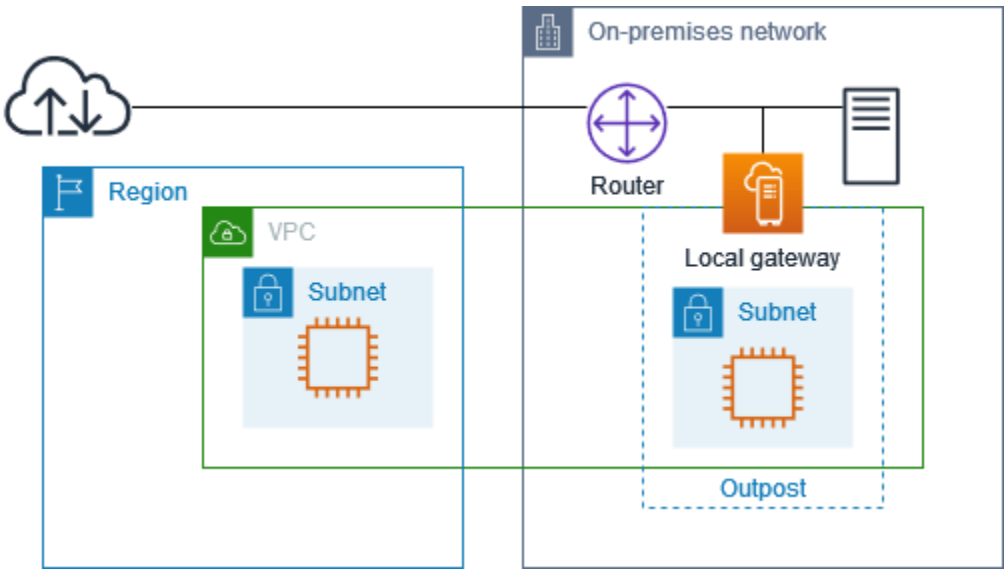
Destination	Cible	Commentaires
VPC CIDR	Local	Fournit la connectivité entre les sous-réseaux du VPC.
0.0.0.0	*internet-gateway-id*	Envoie le trafic destiné à l'Internet public vers la passerelle Internet.
On-premises network CIDR	*local-gateway-id*	Envoie le trafic destiné au réseau sur site vers la 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 possède une EC2 instance.
- 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
VPC CIDR	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' EC2 instance du sous-réseau Outpost avec une destination 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' EC2 instance du sous-réseau Outpost avec une destination du réseau local 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' EC2 instance en adresse IP appartenant au client (adresse IP élastique), 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.

Tables de routage personnalisées

Vous pouvez créer une table de routage personnalisée pour votre passerelle locale. La table de routage de la passerelle locale doit être associée à un groupe VIF et à un VPC. Pour obtenir des step-by-step instructions, voir Configurer la connectivité de la passerelle locale.

Routes de la table de routage de la passerelle locale

Vous pouvez créer des tables de routage de passerelle locales et des routes entrantes vers les interfaces réseau de votre Outpost. Vous pouvez également modifier la route entrante d'une passerelle locale existante pour modifier l'interface réseau cible.

Un itinéraire est actif uniquement lorsque son interface réseau cible est attachée à une instance en cours d'exécution. Si l'instance est arrêtée ou si l'interface est détachée, le statut de l'itinéraire passe d'actif à trou noir.

Table des matières

Exigences et limitations

Les exigences et restrictions suivantes s'appliquent :

- L'interface réseau cible doit appartenir à un sous-réseau de votre avant-poste et doit être attachée à une instance de cet avant-poste. Un itinéraire de passerelle local ne peut pas cibler une EC2 instance Amazon sur un autre Outpost ou sur le site parent Région AWS.
- Le sous-réseau doit appartenir à un VPC associé à la table de routage de passerelle locale.
- Vous ne devez pas dépasser plus de 100 itinéraires d'interface réseau dans la même table de routage.
- 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 interfaces réseau associées aux instances d'Outpost peuvent communiquer via la passerelle locale de cet Outpost. Les interfaces réseau appartenant au sous-réseau Outpost mais associées à une instance de la région ne peuvent pas communiquer via la passerelle locale de cet Outpost.
- Les interfaces gérées par le demandeur, telles que celles créées pour les points de terminaison VPC, ne sont pas accessibles depuis le réseau local via la passerelle locale. Ils ne sont accessibles qu'à partir d'instances situées dans le sous-réseau Outpost.

Les considérations NAT suivantes s'appliquent :

- La passerelle locale n'exécute pas le NAT sur le trafic correspondant à une route d'interface réseau. Au lieu de cela, l’adresse IP de destination est préservée.
- Désactivez la vérification source/destination pour l'interface réseau cible. Pour plus d'informations, consultez la section Concepts d'interface réseau dans le guide de EC2 l'utilisateur Amazon.
- Configurez le système d’exploitation pour autoriser l’interface réseau à accepter le trafic provenant du CIDR de destination.

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.

   Modifiez la table de routage de la passerelle locale pour ajouter une route statique ayant pour cible le 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.

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. Vérifiez que vous êtes dans la bonne case Région AWS.

   Pour modifier la région, 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. Vérifiez si la table de routage de la passerelle locale est associée à un groupe VIF. S'il est associé, vous devez supprimer l'association entre la table de routage de la passerelle locale et le groupe VIF.

   a. Choisissez l'ID de la table de routage de la passerelle locale.
   b. Choisissez l'onglet d'association du groupe VIF.
   c. Si un ou plusieurs groupes VIF sont associés à la table de routage de la passerelle locale, choisissez Modifier l'association de groupes VIF.
   d. Décochez la case Associer un groupe VIF.
   e. Sélectionnez Enregistrer les modifications.
5. Choisissez Supprimer la table de routage de la passerelle locale.
6. Dans la boîte de dialogue de confirmation, tapez **`delete`**, puis choisissez Supprimer.
7. (Facultatif) Créez une table de routage de passerelle locale avec un nouveau mode.

   a. Dans le panneau de navigation, choisissez Tables de routage de passerelle locale.
   b. Choisissez Créer une table de routage de passerelle locale.
   c. 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.

Création d'un pool 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.

Procédez comme suit pour créer un groupe CoIP.

Console

Pour créer un pool CoIP 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 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) Pour ajouter un bloc CIDR, choisissez Ajouter un nouveau CIDR et entrez une plage d'adresses IP appartenant au client.
9. Choisissez Créer un groupe CoIP.

AWS CLI

Pour créer un pool CoIP à l'aide du AWS CLI

1. Utilisez la create-coip-poolcommande pour créer un pool d'adresses CoIP pour la table de routage de passerelle locale spécifiée.

```
aws ec2 create-coip-pool --local-gateway-route-table-id lgw-rtb-
abcdefg1234567890
```

Voici un exemple de sortie.

```
{
    "CoipPool": {
        "PoolId": "ipv4pool-coip-1234567890abcdefg",
        "LocalGatewayRouteTableId": "lgw-rtb-abcdefg1234567890",
        "PoolArn": "arn:aws:ec2:us-west-2:123456789012:coip-pool/ipv4pool-
coip-1234567890abcdefg"
    }
}
```

2. Utilisez la create-coip-cidrcommande pour créer une plage d'adresses CoIP dans le pool CoIP spécifié.

```
aws ec2 create-coip-cidr --cidr 15.0.0.0/24 --coip-pool-id ipv4pool-
coip-1234567890abcdefg
```

Voici un exemple de sortie.

```
{
    "CoipCidr": {
        "Cidr": "15.0.0.0/24",
        "CoipPoolId": "ipv4pool-coip-1234567890abcdefg",
        "LocalGatewayRouteTableId": "lgw-rtb-abcdefg1234567890"
    }
}
```

Après avoir créé un pool CoIP, utilisez la procédure suivante pour attribuer une adresse à votre instance.

Console

Pour attribuer une adresse CoIP à une instance à l'aide de la console

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 le pool d' IPv4 adresses public, choisissez le pool d' IPv4 adresses appartenant au client.
6. Pour le pool d' IPv4 adresses 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 une instance à l'aide du AWS CLI

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",
}
```

Connectivité réseau locale pour les racks Outposts

Vous avez besoin des composants suivants pour connecter votre rack Outposts à votre réseau local :

- 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-pointConnectivité 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 Outposts possède deux périphériques réseau physiques qui se connectent à votre réseau local.

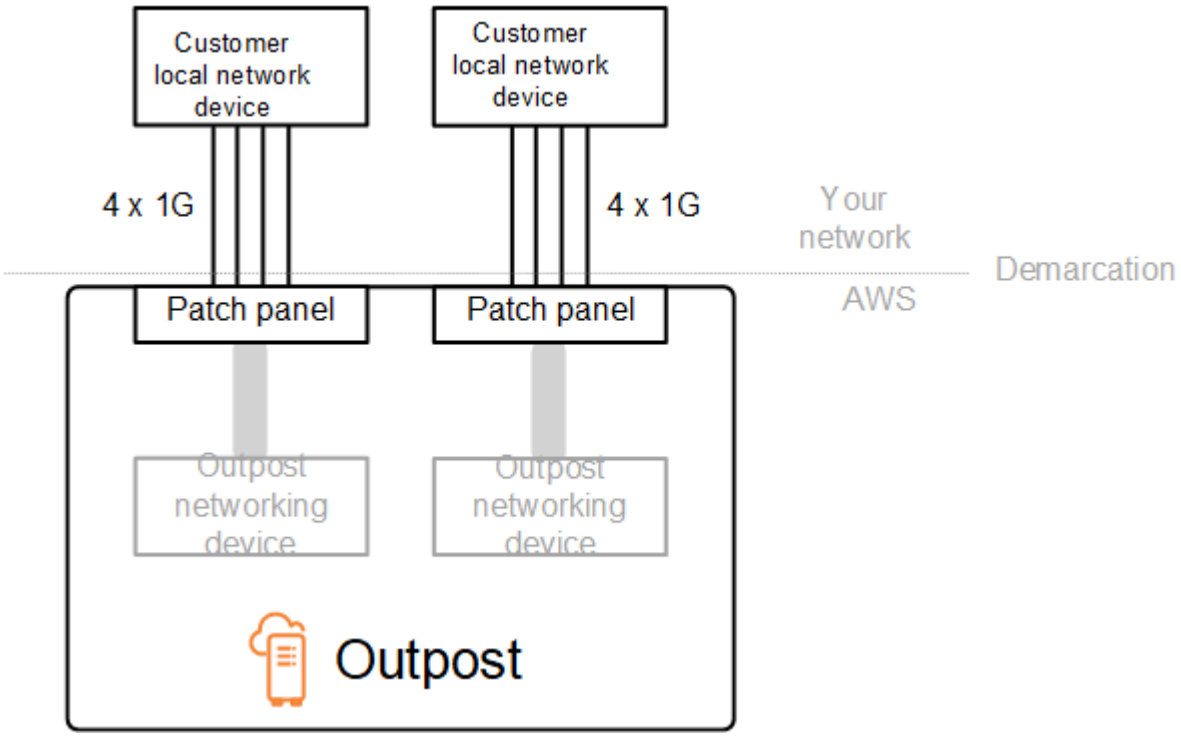
Un Outpost nécessite au moins deux liaisons physiques entre ces périphériques réseau Outpost et les périphériques de votre réseau local. Un Outpost prend en charge les vitesses et quantités de liaison montante suivantes pour chaque périphérique réseau Outpost.

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 la correction d'erreur directe (CL91FEC).

Les racks Outposts peuvent prendre en charge la fibre monomode (SMF) avec le connecteur Lucent (LC), la fibre multimode (MMF) ou la fibre MMF avec LC. OM4 AWS fournit les optiques compatibles avec la fibre que vous fournissez en position de 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

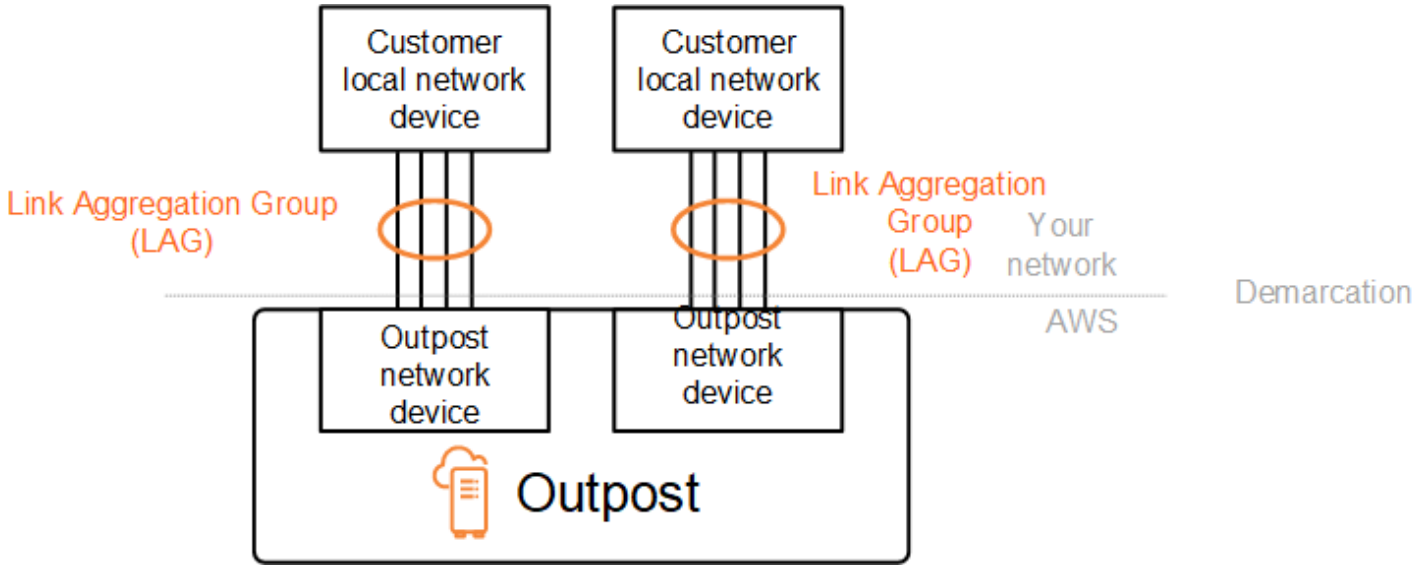
AWS Outposts utilise le protocole LACP (Link Aggrégation Control Protocol) pour établir des connexions de groupe d'agrégation de liens (LAG) entre les appareils de votre réseau Outpost et ceux de votre réseau local. Les liaisons à partir de chaque périphérique réseau Outpost sont agrégées dans un LAG Ethernet pour représenter une connexion réseau unique. Ils LAGs utilisent le LACP avec des minuteries rapides standard. Vous ne pouvez pas configurer LAGs pour utiliser des minuteries lentes.

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 en avoir quatre LAGs entre la couche d'agrégation des appareils réseau Outpost et vos appareils réseau locaux.

Le diagramme suivant présente quatre connexions physiques entre chaque périphérique réseau Outpost et son périphérique réseau local connecté. Nous utilisons Ethernet LAGs pour agréger les liens physiques reliant les appareils du réseau Outpost et les appareils du réseau local du client.



Virtuel LANs

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 VLANs pour séparer le réseau entre les chemins de données.

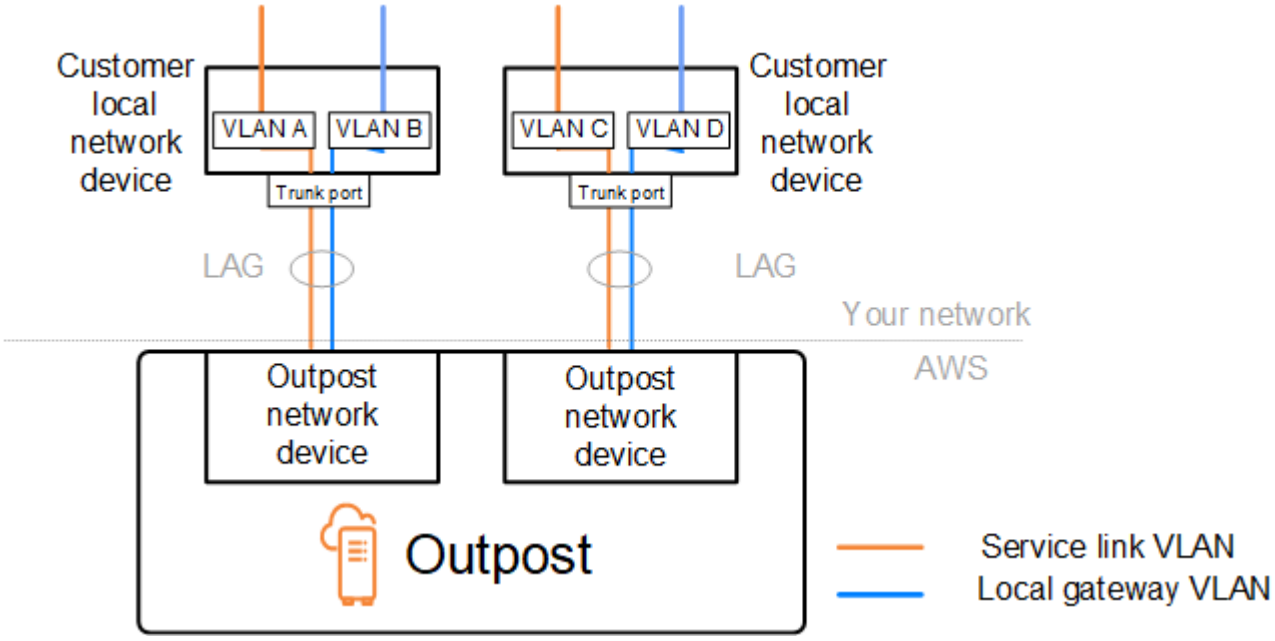
Chaque avant-poste dispose des équipements suivants VLANs pour communiquer avec les appareils de votre réseau local :

- 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 ConnectivitéAWS 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 existe au port des périphériques du réseau Outpost. AWS gère toutes les infrastructures situées du AWS côté de la connexion, et vous gérez toutes les infrastructures situées de votre côté de la ligne.



Pour intégrer votre Outpost à votre réseau local pendant l'installation et le fonctionnement en cours, vous devez répartir le matériel VLANs utilisé entre les appareils du réseau Outpost et les appareils du réseau local du client. Vous devez fournir ces informations AWS avant l'installation. Pour de plus amples informations, veuillez consulter 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 (VIFs) qui incluent l'adresse IP de chaque VLAN. Grâce à ceux-ci VIFs, les appareils AWS Outposts réseau peuvent configurer une connectivité IP et des sessions BGP avec votre équipement réseau local.

Nous vous recommandons la procédure suivante :

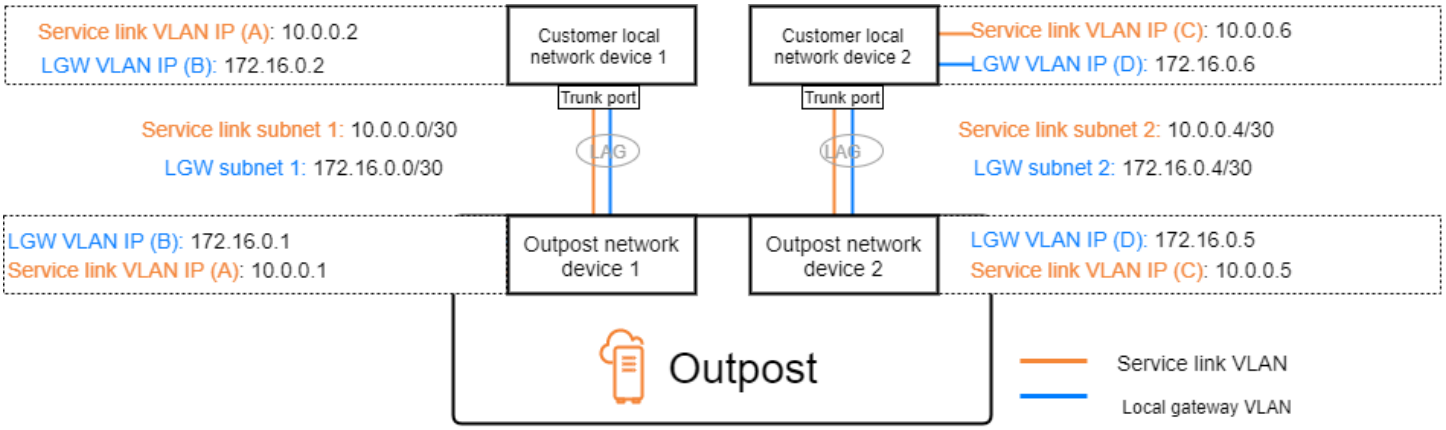
- Utilisez un sous-réseau dédié, avec un CIDR /30 ou /31, pour représenter cette connectivité logique. point-to-point
- Ne faites pas le pont VLANs entre les périphériques de votre réseau local.

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 de liaison de service (VIFs) sont utilisées pour ce chemin afin d'établir une connectivité IP et des sessions BGP entre votre avant-poste et vos périphériques réseau locaux pour la connectivité par liaison de service. Pour plus d'informations, consultez ConnectivitéAWS 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 . VIFs Des passerelles locales sont utilisées sur ce chemin pour établir une connectivité IP et des sessions BGP entre votre Outpost et les appareils 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. Il y en a quatre VLANs pour 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	AWS OND 1 IP
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	AWS OND 2 IP
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 au rack ACE

> **Note**
>
> Ignorez cette section si vous n'avez pas besoin d'un rack ACE.

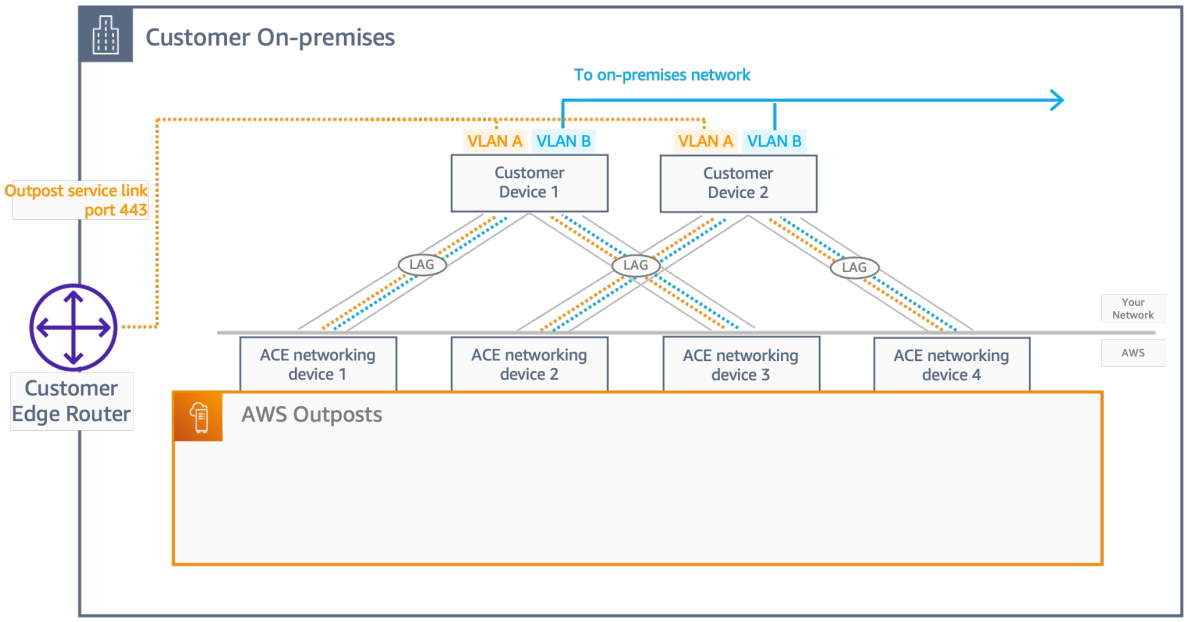
Un rack Aggregation, Core, Edge (ACE) fait office de point d'agrégation réseau pour les déploiements d'Outpost sur plusieurs racks. Vous devez utiliser un rack ACE si vous disposez de quatre racks de calcul ou plus. Si vous avez moins de quatre racks de calcul mais que vous prévoyez de passer à quatre racks ou plus à l'avenir, nous vous recommandons d'installer un rack ACE au plus tôt.

Avec un rack ACE, les périphériques réseau des Outposts ne sont plus directement connectés à vos périphériques réseau locaux. Ils sont plutôt connectés au rack ACE, qui fournit la connectivité aux racks Outposts. Dans cette topologie, AWS est propriétaire de l'allocation et de la configuration de l'interface VLAN entre les périphériques réseau Outposts et les périphériques réseau ACE.

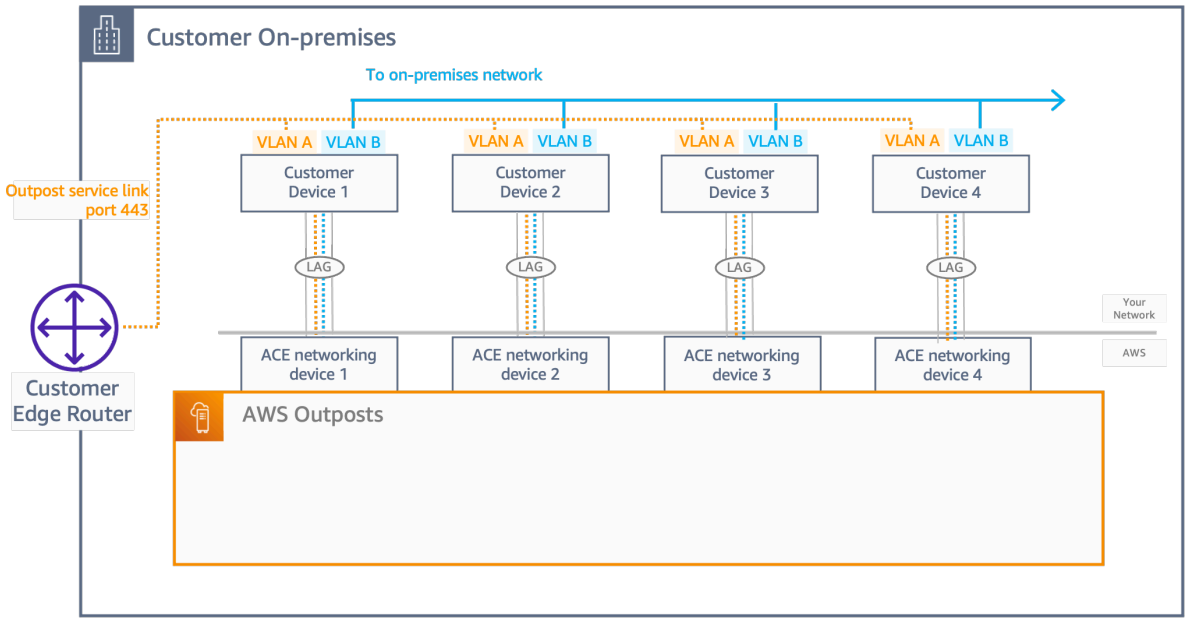
Un rack ACE comprend quatre périphériques réseau qui peuvent être connectés à deux appareils client en amont dans un réseau client sur site ou à quatre appareils client en amont pour une résilience maximale.

Les images suivantes montrent les deux topologies de réseau.

L'image suivante montre les quatre périphériques réseau ACE du rack ACE connectés à deux appareils clients en amont :



L'image suivante montre les quatre périphériques réseau ACE du rack ACE connectés à quatre appareils clients en amont :



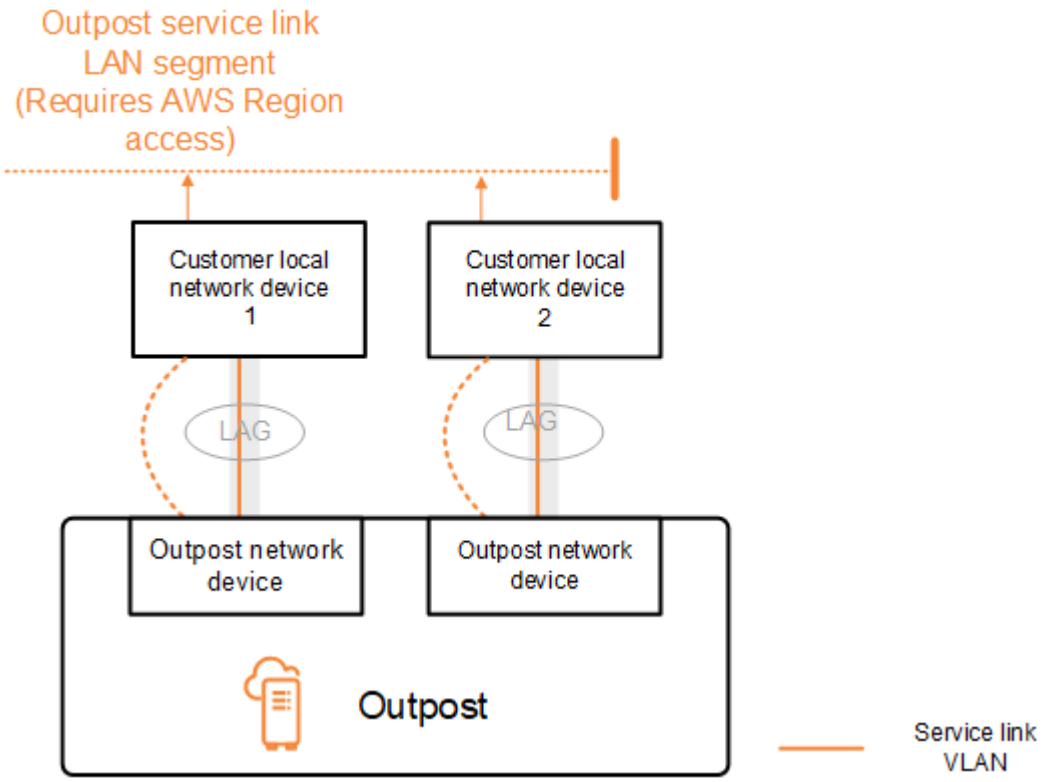
Connectivité BGP de la liaison de service

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 de peering BGP utilise un numéro de système autonome (ASN) privé sur le périphérique réseau Outpost et un ASN que vous choisissez pour les appareils réseau locaux de votre client. Dans le cadre du processus d'installation, AWS configure les attributs que vous avez fournis.

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 de plus amples informations, veuillez consulter 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 OND annonce son propre préfixe /27 avec une longueur AS-Path de 1, plus les préfixes /27 de tous les autres ONDs avec une longueur AS-Path de 4 en tant que sauvegarde.
3. Le sous-réseau est utilisé pour la connectivité entre l'avant-poste et la AWS région.

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 client doit annoncer des préfixes BGP identiques avec les mêmes attributs à tous. ONDs 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 transfert de trafic nécessite des préfixes BGP identiques de la part du client pour tous. ONDs 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 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.

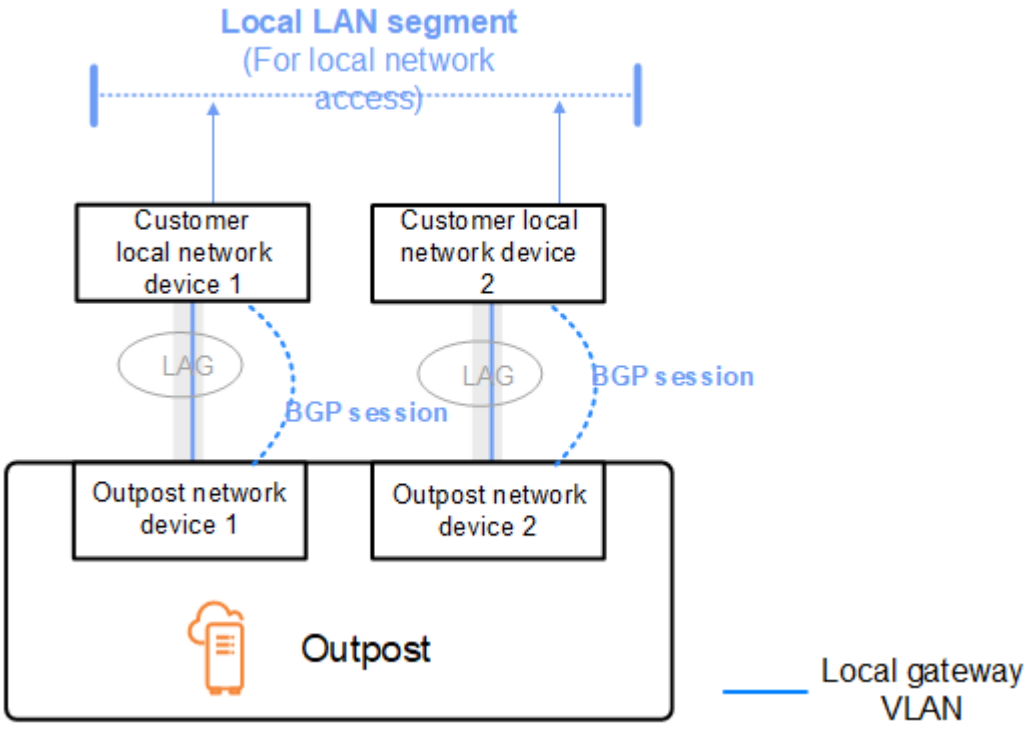
L'Outpost établit une session d'appairage BGP externe via le VLAN de passerelle locale entre chaque périphérique réseau Outpost et le périphérique réseau local connecté de son client.

La session d'appairage est établie entre le /30 ou le /31 IPs que vous avez indiqué lors de la configuration de la connectivité réseau et utilise la point-to-point connectivité entre les périphériques réseau Outpost et les périphériques réseau locaux du client. Pour de plus amples informations, veuillez consulter the section called “Connectivité de la couche réseau”.

Chaque session BGP utilise l'ASN privé du côté du périphérique réseau Outpost et un ASN que vous choisissez du côté du périphérique réseau local du client. AWS configure 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 :

- Le client 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 de plus amples informations, veuillez consulter 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 de plus amples informations, veuillez consulter 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. Le préfixe AS-Path est utilisé pour les préfixes de passerelle locale afin de détourner le trafic ONDs si une maintenance est requise. 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 client doit annoncer des préfixes BGP identiques avec les mêmes attributs à tous. ONDs 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 transfert de trafic nécessite des préfixes BGP identiques de la part du client pour tous. ONDs 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 (voir Routage VPC direct) pour faciliter la communication avec votre réseau sur site. Vous pouvez toutefois indiquer un groupe d'adresses IP clients (CoIP).

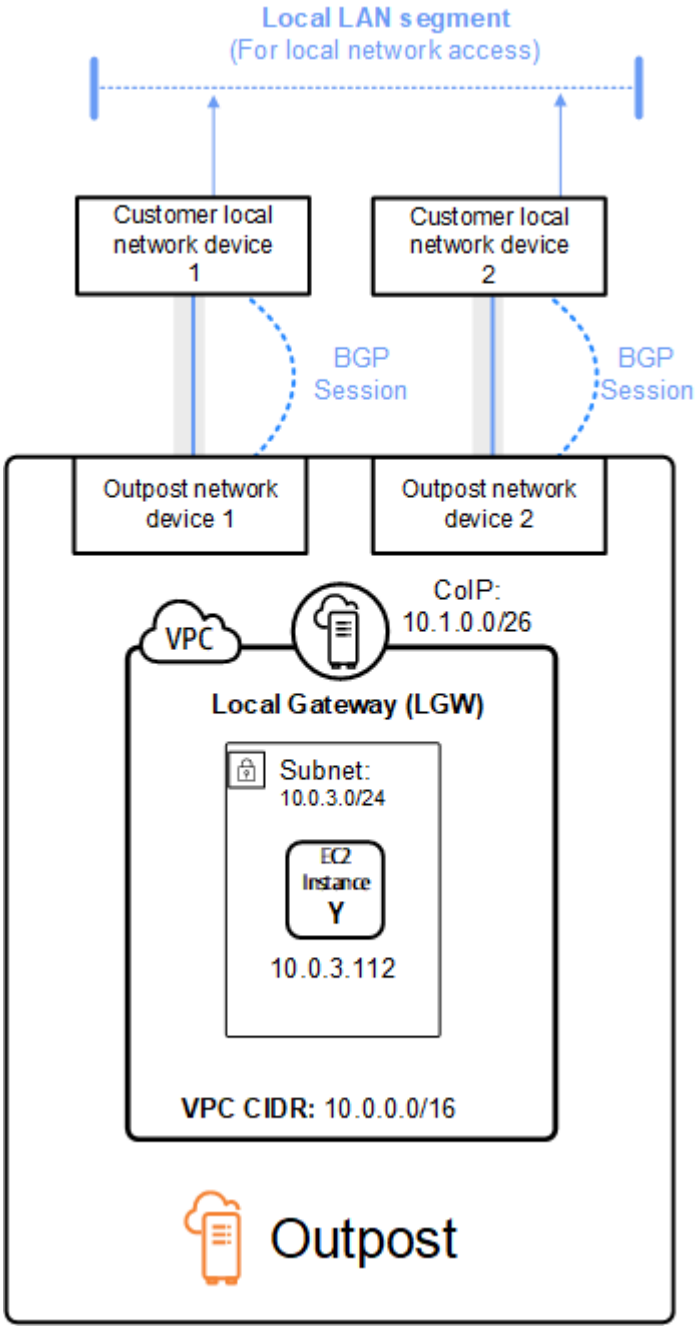
Vous pouvez créer des adresses IP élastiques à partir de ce pool, puis les attribuer aux ressources de votre Outpost, telles que EC2 les instances.

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 EC2 instance du 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 le CoIP Elastic IPs pour adresser les instances de l'Outpost, la plage d'adresses 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

Gestion des capacités pour AWS Outposts

Un avant-poste fournit un pool de capacités de AWS calcul et de stockage sur votre site en tant qu'extension privée d'une zone de disponibilité dans une AWS région. La capacité de calcul et de stockage disponible dans l'Outpost étant limitée et déterminée par la taille et le nombre d'actifs AWS installés sur votre site, vous pouvez décider de la AWS Outposts capacité d'Amazon, Amazon EBS et Amazon S3 dont vous avez besoin pour exécuter vos charges de travail initiales, faire face à la croissance future et fournir une capacité supplémentaire afin d'atténuer les pannes de serveur et les événements de maintenance. EC2

Rubriques

Afficher la AWS Outposts capacité

Vous pouvez consulter la configuration des capacités au niveau de l'instance ou de l'avant-poste.

Pour consulter la configuration de la capacité de votre avant-poste à l'aide de la console

1. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.
2. Dans le volet de navigation de gauche, choisissez Outposts.
3. Choisissez l'Outpost.
4. Sur la page de détails de l'Outpost, sélectionnez la vue Instance ou la vue Rack.
    - Vue des instances : fournit des informations sur les instances configurées sur les Outposts et sur la répartition des instances par taille et par famille.
    - Vue en rack : permet de visualiser les instances de chaque actif au sein de chaque avant-poste et de sélectionner Modifier la capacité des instances pour modifier la capacité des instances.

Modifier la capacité de l' AWS Outposts instance

La capacité de chaque nouvelle commande Outpost est configurée avec une configuration de capacité par défaut. Vous pouvez convertir la configuration par défaut pour créer différentes instances répondant aux besoins de votre entreprise. Pour ce faire, vous devez créer une tâche de capacité, choisir un Outposts ou un actif unique, spécifier la taille et la quantité des instances, puis exécuter la tâche de capacité pour implémenter les modifications.

Considérations

Tenez compte des points suivants avant de modifier la capacité de l'instance :

- Les tâches de capacité ne peuvent être exécutées que par le AWS compte propriétaire des ressources de l'Outpost (propriétaire). Les consommateurs ne peuvent pas exécuter de tâches liées à la capacité. Pour plus d'informations sur les propriétaires et les consommateurs, voir Partager vos AWS Outposts ressources.
- Les tailles et quantités des instances peuvent être définies au niveau de l'avant-poste ou au niveau d'un actif individuel.
- La capacité est configurée automatiquement pour un actif ou pour tous les actifs d'un avant-poste en fonction des configurations possibles et des meilleures pratiques.
- Pendant qu'une tâche de capacité est en cours d'exécution, les actifs associés à l'avant-poste sélectionné peuvent être isolés. C'est pourquoi nous vous recommandons de créer une tâche de capacité uniquement lorsque vous ne comptez pas lancer de nouvelles instances sur vos Outposts.
- Vous pouvez choisir d'exécuter la tâche de capacité instantanément ou de continuer à essayer régulièrement au cours des prochaines 48 heures. Le choix d'une exécution instantanée nécessite moins de temps d'isolation des actifs, mais la tâche peut échouer si les instances doivent être arrêtées pour exécuter la tâche. Le choix d'une exécution périodique permet de disposer de plus de temps pour arrêter les instances avant que la tâche n'échoue, mais les actifs peuvent être isolés plus longtemps.
- Il est possible que des configurations de capacité valides n'utilisent pas tous les vCPU disponibles sur un actif. Dans ce cas, un message à la fin de la section Type d'instance vous informera que votre capacité est insuffisante, mais permettra d'appliquer la configuration comme demandé.
- Lorsque vous modifiez un Outpost dans la console, toutes les instances prises en charge ne sont pas affichées car le mélange d'instances sauvegardées sur disque avec des instances n'est pas totalement pris en charge non-disk-backed dans la console. Pour accéder à toutes les instances possibles, utilisez l'StartCapacityTaskAPI.

- Lors de la définition de la capacité d'un avant-poste, toutes les familles et tous les types d'instances seront inclus dans la reconfiguration, sauf s'ils sont répertoriés comme des instances à éviter.
- Vous ne pouvez modifier la configuration de capacité de vos Outposts existante que pour utiliser des tailles d' EC2instance Amazon valides issues de familles d'instances prises en charge par votre modèle d'actif respectif.
- Si vous avez des instances en cours d'exécution sur votre avant-poste et que vous ne souhaitez pas les arrêter pour exécuter une tâche de capacité, sélectionnez leur ID d'instance respectif dans la section Instances à conserver telles quelles — facultatif et assurez-vous de conserver la quantité nécessaire de cette taille d'instance dans votre configuration de capacité mise à jour. Cela permettra de conserver les instances utilisées pour prendre en charge les charges de travail de production pendant l'exécution d'une tâche de capacité.
- Lorsque vous configurez un actif avec plusieurs tailles d'instance au sein d'une même famille d'instances, utilisez Auto-balance pour vous assurer que vous n'essayez pas de surprovisionner ou de sous-approvisionner votre droplet. Le surprovisionnement n'est pas pris en charge et entraînera une défaillance de la tâche de capacité.
- Si vous souhaitez reconfigurer complètement une famille d'instances sur votre avant-poste sans conserver les tailles d'instance de la configuration de capacité d'origine, vous devez arrêter toutes les instances de cette famille en cours d'exécution sur votre avant-poste avant d'exécuter la tâche de capacité. Si l'instance appartient à un autre compte ou est utilisée par un service en couches exécuté sur l'Outpost, vous devez utiliser le compte du propriétaire de l'instance pour arrêter l'instance ou l'instance de service.
- Plusieurs tâches de capacité peuvent être exécutées en parallèle tant qu'elles s'appliquent à des ensembles d'actifs qui s'excluent mutuellementIDs. Par exemple, vous pouvez créer plusieurs tâches de capacité au niveau des actifs pour différents actifs IDs en même temps. Toutefois, si une tâche de niveau Outpost est en cours d'exécution, vous ne pouvez pas créer une autre tâche au niveau de l'Outpost ou de l'actif en même temps. De même, si une tâche au niveau de l'actif est en cours d'exécution, vous ne pouvez pas créer une tâche au niveau Outpost ou une tâche au niveau de l'actif sur le même AssetID en même temps.

Pour modifier la configuration de capacité de votre avant-poste à l'aide de la console

1. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.
2. Dans le volet de navigation de gauche, sélectionnez Capacity tasks.
3. Sur la page Tâches de capacité, choisissez Créer une tâche de capacité.
4. Sur la page de démarrage, choisissez la commande, l'Outpost ou l'actif à configurer.

5. Pour modifier la capacité, spécifiez une option pour Méthode de modification : e steps dans la console ou téléchargez un fichier JSON.

   - Modifiez le plan de configuration de la capacité pour suivre les étapes de la console
   - Téléchargez un plan de configuration de capacité pour télécharger un fichier JSON

> **Note**
>
> - Pour empêcher la gestion de la capacité de recommander l'arrêt d'instances spécifiques, spécifiez les instances qui ne doivent pas être arrêtées. Ces instances seront exclues de la liste des instances à arrêter.

Console steps

1. Choisissez la vue Instance ou la vue Rack.
2. Choisissez Modifier la configuration de la capacité d'un avant-poste ou Modifier sur un seul actif.
3. Choisissez un avant-poste ou un actif s'il est différent de la sélection actuelle.
4. Choisissez d'exécuter cette tâche de capacité immédiatement ou régulièrement pendant 48 heures.
5. Choisissez Suivant.
6. Sur la page Configurer la capacité de l'instance, chaque type d'instance indique une taille d'instance avec la quantité maximale présélectionnée. Pour ajouter d'autres tailles d'instance, choisissez Ajouter une taille d'instance.
7. Spécifiez la quantité d'instance et notez la capacité affichée pour cette taille d'instance.
8. Consultez le message à la fin de chaque section sur le type d'instance qui vous indique si votre capacité est dépassée ou insuffisante. Effectuez des ajustements au niveau de la taille ou de la quantité de l'instance pour optimiser votre capacité totale disponible.
9. Vous pouvez également demander AWS Outposts à optimiser la quantité d'instances pour une taille d'instance spécifique. Pour ce faire :

   a. Choisissez la taille de l'instance.

   b. Choisissez Auto-balance à la fin de la section sur le type d'instance correspondante.

10. Pour chaque type d'instance, assurez-vous que la quantité d'instances est spécifiée pour au moins une taille d'instance.
11. Choisissez éventuellement les instances à conserver telles quelles.
12. Choisissez Suivant.
13. Sur la page Réviser et créer, vérifiez les mises à jour que vous demandez.
14. Choisissez Créer. AWS Outposts crée une tâche de capacité.
15. Sur la page de la tâche de capacité, surveillez l'état de la tâche.

Upload a JSON file

1. Choisissez Télécharger une configuration de capacité.
2. Choisissez Suivant.
3. Sur la page Plan de configuration de la capacité de téléchargement, téléchargez le fichier JSON qui spécifie le type, la taille et la quantité de l'instance. Vous pouvez éventuellement spécifier les TaskActionOnBlockingInstancesparamètres InstancesToExclude, et dans le fichier JSON.

   Example

   Exemple de fichier JSON :

```
{
  "InstancePools": [
    {
      "InstanceType": "c5.24xlarge",
      "Count": 1
    },
    {
      "InstanceType": "m5.24xlarge",
      "Count": 2
    }
  ],
  "InstancesToExclude": {
    "AccountIds": [
      "111122223333"
    ],
    "Instances": [
      "i-1234567890abcdef0"
    ],
```

```
    "Services": [
      "ALB"
    ]
  },
  "TaskActionOnBlockingInstances": "WAIT_FOR_EVACUATION"
}
```

4. Passez en revue le contenu du fichier JSON dans la section Plan de configuration des capacités.
5. Choisissez Suivant.
6. Sur la page Réviser et créer, vérifiez les mises à jour que vous demandez.
7. Choisissez Créer. AWS Outposts crée une tâche de capacité.
8. Sur la page de la tâche de capacité, surveillez l'état de la tâche.

Résolution des problèmes liés aux tâches de capacité

Passez en revue les problèmes connus suivants pour résoudre un problème lié à la gestion des capacités dans un nouvel ordre. Si votre problème n'apparaît pas dans la liste, contactez Support.

*oo-xxxxxx*La commande n'est pas associée à Outpost ID *op-xxxxx*

Ce problème se produit lorsque vous utilisez l'API AWS CLI or pour exécuter le `StartCapacityTask`et que l'identifiant d'avant-poste indiqué dans la demande ne correspond pas à l'identifiant d'avant-poste de la commande.

Pour résoudre ce problème :

1. Connectez-vous à AWS.
2. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.
3. Dans le volet de navigation, sélectionnez Commandes.
4. Sélectionnez la commande et vérifiez que le statut de la commande est l'un des suivants : `PREPARINGIN_PROGRESS`, ou`ACTIVE`.
5. Notez l'ID de l'Outpost dans la commande.
6. Entrez l'identifiant Outpost correct dans la demande `StartCapacityTask` d'API.

Le plan de capacité inclut les types d'instances qui ne sont pas pris en charge

Ce problème se produit lorsque vous utilisez l'API AWS CLI or pour créer ou modifier la tâche de capacité et que la demande contient des types d'instances non pris en charge.

Pour résoudre ce problème, utilisez la console ou la CLI.

Utilisation de la console

1. Connectez-vous à AWS.
2. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.
3. Dans le volet de navigation, choisissez Capacity task.
4. Utilisez l'option Télécharger une configuration de capacité pour télécharger un fichier JSON avec la même liste de types d'instances.
5. La console affiche un message d'erreur avec la liste des types d'instances pris en charge.
6. Corrigez la demande de suppression des types d'instances non pris en charge.
7. Créez ou modifiez la tâche de capacité sur la console à l'aide du JSON corrigé ou utilisez la CLI ou l'API avec cette liste corrigée de types d'instances.

Utilisation de l'interface de ligne de commande

1. Utilisez la GetOutpostSupportedInstanceTypescommande pour voir la liste des types d'instances pris en charge.
2. Créez ou modifiez la tâche de capacité avec la liste correcte de types d'instances.

Aucun avant-poste avec identifiant d'avant-poste *op-xxxxx*

Ce problème se produit lorsque vous utilisez l'API AWS CLI or pour exécuter le `StartCapacityTask`et que la demande contient un identifiant Outpost non valide pour l'une des raisons suivantes :

- L'avant-poste se trouve dans une autre AWS région.
- Vous n'êtes pas autorisé à accéder à cet avant-poste.
- L'identifiant de l'Outpost est incorrect.

Pour résoudre ce problème :

1. Notez la AWS région que vous avez utilisée dans la demande `StartCapacityTask` d'API.
2. Utilisez l'action `ListOutposts`API pour obtenir la liste des Outposts que vous possédez dans la AWS région.
3. Vérifiez si l'identifiant de l'Outpost est répertorié.
4. Entrez l'ID Outpost correct dans la `StartCapacityTask` demande.
5. Si vous ne trouvez pas l'identifiant de l'avant-poste, utilisez à nouveau l'action de l'`ListOutposts`API pour vérifier si l'avant-poste existe dans une autre AWS région.

CapacityTaskCasquette active- *XXXX* déjà trouvée pour Outpost op- *XXXX*

Ce problème se produit lorsque vous utilisez la AWS Outposts console ou l'API pour exécuter StartCapacityTaskun Outpost alors qu'une tâche de capacité d'exécution existe déjà pour l'Outpost. Une tâche de capacité est considérée comme en cours d'exécution si elle possède l'un des états suivants :`REQUESTED`, `IN_PROGRESSWAITING_FOR_EVACUATION`, ou`CANCELLATION_IN_PROGRESS`.

Pour résoudre ce problème, utilisez la AWS Outposts console ou la CLI.

Utilisation de la console

1. Connectez-vous à AWS.
2. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.
3. Dans le volet de navigation, sélectionnez Capacity tasks.
4. Assurez-vous qu'aucune tâche de capacité d'exécution n'est prévue pour le OutpostId.
5. Si des tâches de capacité sont en cours d'exécution pour le OutpostId, attendez qu'elles se terminent ou annulez-les si vous le souhaitez.
6. Lorsqu'aucune tâche de capacité n'est en cours pour la demande OutpostId, réessayez de créer la tâche de capacité.

Utilisation de l'interface de ligne de commande

1. Utilisez la ListCapacityTaskscommande pour rechercher les tâches relatives à la capacité de fonctionnement de l'avant-poste.

2. Attendez que toutes les tâches de capacité en cours soient terminées ou annulez-les si vous le souhaitez.
3. Lorsqu'aucune tâche de capacité n'est en cours pour la demande OutpostId, réessayez de créer la tâche de capacité.

CapacityTaskCasquette active : *XXXX* déjà trouvée pour Asset *XXXX* on Outpost OP-xxxx

Ce problème se produit lorsque vous utilisez la AWS Outposts console ou l'API pour exécuter StartCapacityTaskune ressource et qu'une tâche de capacité d'exécution existe déjà pour cette ressource. Une tâche de capacité est considérée comme en cours d'exécution si elle possède l'un des états suivants :`REQUESTED`, `IN_PROGRESSWAITING_FOR_EVACUATION`, ou`CANCELLATION_IN_PROGRESS`.

Pour résoudre ce problème, utilisez la AWS Outposts console ou la CLI.

Utilisation de la console

1. Connectez-vous à AWS.
2. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.
3. Dans le volet de navigation, sélectionnez Capacity tasks.
4. Assurez-vous qu'il n'y a aucune tâche de capacité d'exécution pour le OutpostId et qu'aucune tâche de capacité au niveau des actifs n'est en cours d'exécution pour le. AssetId
5. Si des tâches de capacité sont en cours d'exécution, attendez qu'elles se terminent ou annulez-les si vous le souhaitez.
6. Lorsqu'aucune tâche de capacité n'est en cours d'exécution, réessayez de créer la tâche de capacité.

Utilisation de l'interface de ligne de commande

1. Utilisez la ListCapacityTaskscommande pour rechercher les tâches de capacité d'exécution pour OutpostID et AssetID.
2. Assurez-vous qu'aucune tâche de capacité au niveau de l'Outpost n'est en cours d'exécution pour le OutpostId, et qu'aucune tâche de capacité au niveau des actifs n'est en cours d'exécution pour le. AssetId

3. Si des tâches de capacité sont en cours d'exécution, attendez qu'elles se terminent ou annulez-les si vous le souhaitez.
4. Réessayez votre demande pour créer la tâche de capacité.

AssetId= n'*XXXX*est pas valide pour Outpost=OP- *XXXX*

Ce problème se produit lorsque vous utilisez la AWS Outposts console ou l'API pour exécuter StartCapacityTaskune ressource et que l'AssetID n'est pas valide pour l'une des raisons suivantes :

- L'actif n'est pas associé à l'avant-poste.
- L'actif est isolé.

Pour résoudre ce problème, utilisez la AWS Outposts console ou la CLI.

Utilisation de la console

1. Connectez-vous à AWS.
2. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.
3. Choisissez Rack view pour l'Outpost.
4. Vérifiez que la demande AssetId est associée à l'avant-poste et qu'elle n'est pas marquée comme hôte isolé.
    a. Si l'actif est isolé, cela peut être dû au fait qu'une tâche de capacité est en cours d'exécution sur celui-ci. Vous pouvez accéder au panneau des tâches de capacité et vérifier si des tâches au niveau de l'avant-poste ou des actifs sont en cours d'exécution pour le et. OutpostId AssetId Si tel est le cas, attendez que la tâche soit terminée et que la ressource soit de nouveau disponible.
    b. S'il n'existe aucune tâche de capacité d'exécution pour un actif isolé, celui-ci peut être dégradé.
5. Après avoir vérifié que l'actif existe et est dans un état valide, réessayez votre demande pour créer la tâche de capacité.

Utilisation de l'interface de ligne de commande

1. Utilisez la ListAssetscommande pour rechercher les actifs associés à l'OutpostID.
2. Vérifiez que la demande AssetId est associée à l'avant-poste et que son état l'est`ACTIVE`.

a. Si l'état de l'actif n'est pas ACTIF, cela peut être dû au fait qu'une tâche de capacité est en cours d'exécution sur celui-ci. Utilisez la ListCapacityTaskscommande pour déterminer si des tâches Outpost ou au niveau des actifs sont en cours d'exécution pour le et. OutpostId AssetId Si tel est le cas, attendez que la tâche se termine et que l'actif redevienne ACTIF.

b. S'il n'existe aucune tâche de capacité d'exécution pour un actif isolé, celui-ci peut être dégradé.

3. Après avoir vérifié que l'actif existe et est dans un état valide, réessayez votre demande pour créer la tâche de capacité.

Partagez vos AWS Outposts ressources

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 VPCs, de lancer et d'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 partagés avec eux comme ils le feraient sur des Outposts créés dans leur propre compte. Le propriétaire est responsable de la gestion de l'Outpost 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 réserves de capacité, les propriétaires peuvent également afficher, modifier et supprimer des ressources que les consommateurs créent sur des Outposts partagés. Les propriétaires ne peuvent pas modifier les instances que les consommateurs lancent dans Capacity Reservations qu'ils ont partagées.

Les consommateurs sont responsables de la gestion des ressources qu'ils créent sur des Outposts partagés avec eux, y compris les ressources consommant des réserves de capacité. Les consommateurs ne peuvent pas afficher ou modifier les ressources appartenant à d'autres consommateurs ou au 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 Outpost avec :

- AWS Comptes spécifiques au sein de son organisation en AWS Organizations.
- Une unité organisationnelle au sein de son organisation dans AWS Organizations.
- L'ensemble de son organisation dans AWS Organizations.

Table des matières

Ressources Outpost partageables

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

- Hôtes dédiés alloués : les consommateurs ayant accès à cette ressource peuvent :
  - Lancez et exécutez EC2 des instances sur un hôte dédié.
- Réserves de capacité : les consommateurs ayant accès à cette ressource peuvent :
  - Identifier les réserves de capacité partagées avec eux.
  - Lancer et gérer les instances qui consomment des réserves de capacité.
- Pools d’adresses IP clients (CoIP) : les consommateurs ayant accès à cette ressource peuvent :
  - Allouer et associer des adresses IP clients à des instances.
- Tables de routage de passerelle locale : les consommateurs ayant accès à cette ressource peuvent :
  - Créer et gérer des associations VPC à une passerelle locale.
  - Afficher les configurations des tables de routage de passerelle locale et des interfaces virtuelles.
- Outposts : les consommateurs ayant accès à cette ressource peuvent :
  - Créer et gérer des sous-réseaux sur l’Outpost.
  - Créer et gérer des volumes EBS sur l’Outpost.
  - Utilisez l' AWS Outposts API pour consulter les informations relatives à l'Outpost.
- S3 on Outposts : les consommateurs ayant accès à cette ressource peuvent :
  - Créer et gérer des compartiments, des points d’accès et des points de terminaison S3 sur l’Outpost.
- Sites : les consommateurs ayant accès à cette ressource peuvent :
  - Créer, gérer et contrôler un Outpost sur le site.

- Sous-réseaux : les consommateurs ayant accès à cette ressource peuvent :
  - Afficher des informations sur les sous-réseaux.
  - Lancez et exécutez EC2 des instances dans des sous-réseaux.

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

Conditions préalables requises pour le partage de ressources Outposts

- Pour partager une ressource Outpost avec votre organisation ou une unité organisationnelle dans AWS Organizations, vous devez activer le partage avec AWS Organizations. Pour plus d'informations, consultez 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 qui se trouve dans votre organisation.

Services connexes

Le partage de ressources Outpost s'intègre à AWS Resource Access Manager (AWS RAM). AWS RAM est un service qui vous permet de partager vos AWS ressources avec n'importe quel AWS compte ou via AWS 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 entière AWS Organizations.

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

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, il est possible que la zone `us-east-1a` de disponibilité de votre AWS compte ne soit pas la même que celle `us-east-1a` d'un autre AWS compte.

Pour identifier l'emplacement de votre ressource Outpost par rapport à vos comptes, vous devez utiliser l'ID de zone de disponibilité. L'AZ ID est un identifiant unique et cohérent pour une zone de disponibilité pour tous les AWS comptes. Par exemple, `use1-az1` il s'agit d'un identifiant AZ pour la `us-east-1` région et il s'agit du même emplacement dans tous les AWS comptes.

Pour consulter les IDs zones de disponibilité de votre compte

1. Accédez à la AWS RAM console dans la AWS RAM console.
2. L'AZ IDs de la région actuelle s'affiche dans le panneau Your AZ ID sur le côté droit de l'écran.

> **Note**
>
> Les tables de routage de passerelle locale se trouvant dans la même zone de disponibilité que leur Outpost, il n'est pas nécessaire de spécifier un ID de zone de disponibilité pour les tables de routage.

Partage d'une ressource Outpost

Lorsqu'un propriétaire partage un Outpost avec un consommateur, ce dernier peut créer des ressources sur l'Outpost comme il le ferait sur des Outposts créés dans son propre compte. Les consommateurs ayant accès à des tables de routage de passerelle locale partagées peuvent créer et gérer des associations VPC. Pour plus d'informations, consultez Ressources Outpost partageables.

Pour partager une ressource Outpost, vous devez l'ajouter à un partage de ressources. Un partage de ressources est une AWS RAM ressource qui vous permet de partager vos ressources entre différents AWS comptes. 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 préalablement créer le partage de ressources à l'aide de la console AWS RAM.

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 bénéficient d'un 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 du AWS CLI.

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

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 Partages de ressources.
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 qui vous appartient, utilisez également la procédure suivante.

Pour partager un Outpost ou une table de routage de passerelle locale qui vous appartient 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

Lorsque vous annulez le partage de votre Outpost avec un consommateur, celui-ci ne peut plus effectuer les opérations suivantes :

- Affichez l'Outpost dans la AWS Outposts console.
- Créez de nouveaux sous-réseaux sur l'Outpost.
- Créez de nouveaux volumes Amazon EBS sur l'Outpost.

- Consultez les détails de l'Outpost et les types d'instances à l'aide de la AWS Outposts console ou du AWS CLI.

Les sous-réseaux, volumes ou instances créés par le consommateur pendant la période partagée ne sont pas supprimés et le consommateur peut continuer à effectuer les opérations suivantes :

- Accédez à ces ressources et modifiez-les.
- Lancez de nouvelles instances sur un sous-réseau existant créé par le consommateur.

Pour empêcher le consommateur d'accéder à ses ressources et de lancer de nouvelles instances sur votre Outpost, demandez-lui de supprimer ses ressources.

Lorsqu'une table de routage de passerelle locale partagée n'est plus partagée, le consommateur ne peut plus créer de nouvelles associations VPC avec celle-ci. Toutes les associations VPC existantes créées par le consommateur restent associées à la table de routage. Les ressources qu'ils contiennent VPCs peuvent continuer à acheminer le trafic vers la passerelle locale. Pour éviter cela, demandez au consommateur de supprimer les associations VPC.

Pour annuler le partage d’une ressource Outpost qui vous appartient, vous devez la supprimer du partage de ressources. Vous pouvez le faire à l'aide de la AWS RAM console ou du 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.

Identification d’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 de passerelle locale partagées à l’aide de l’ AWS CLI.

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

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 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 Outpost partagées

Autorisations accordées aux propriétaires

Les propriétaires sont responsables de la gestion de l'Outpost et des ressources qu'il y crée. 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 partagés avec eux comme ils le feraient sur des Outposts créés dans leur propre compte. Les consommateurs sont responsables de la gestion des ressources qu'ils lancent sur les Outposts partagés avec eux. Les consommateurs ne peuvent ni afficher ni modifier les ressources appartenant à d'autres consommateurs ou au propriétaire de l'Outpost, et ils ne peuvent pas modifier les Outposts qui sont partagés avec eux.

Facturation et mesures

Les propriétaires sont facturés pour les Outposts et les ressources d'Outpost 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

Le partage de tables de routage de passerelle locale n'entraîne pas de frais supplémentaires. 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 d'application 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 du partage de VPC, consultez Limites dans le Guide de l'utilisateur 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 plus d'informations 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).

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 Amazon EBS Encryption dans le guide de l'utilisateur Amazon EBS.

Chiffrement en transit

AWS chiffre les données en transit entre votre avant-poste et sa région. AWS Pour de plus amples informations, veuillez consulter Connectivité via un lien 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 mettez fin à une EC2 instance, la mémoire qui lui est allouée est nettoyée (mise à zéro) par l'hyperviseur avant d'être allouée à une nouvelle instance, et chaque bloc de stockage est réinitialisé.

La 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

Fonctionnalité 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
Clés de condition de politique (spécifiques au service)	Oui
ACLs	Non
ABAC (étiquettes dans les politiques)	Oui
Informations d’identification temporaires	Oui

Fonctionnalité IAM	AWS Soutien aux Outposts
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 groupe d'utilisateurs 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, consultez Définition d'autorisations IAM personnalisées avec des politiques gérées par le client 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

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 politique 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 auxquels 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-les ARNs par des virgules.

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

Pour consulter la liste des types de ressources des AWS Outposts et de leurs caractéristiques ARNs, 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

ABAC avec Outposts AWS

Prise en charge d'ABAC (balises 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 ABAC, consultez Définition d'autorisations avec l'autorisation 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 par 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 Passage d’un rôle utilisateur à un rôle IAM (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 sessions d’accès direct (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, vous pouvez effectuer une action qui initie 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.

Rôles liés à un service pour les Outposts AWS

Prend en charge les rôles liés aux services : 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. Rôles liés à un service 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 peut 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 IAM (console) 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 ARNs de chaque type de ressource, 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 plus d'informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Accordez 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 d'IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utilisez 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 l'Analyseur d'accès IAM pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : l'Analyseur d'accès IAM 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 plus d'informations, consultez Validation de politiques avec 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 la MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Sécurisation de l'accès aux API avec 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"
    }
  ]
}
```

Rôles liés à un service 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 de rôle de service directement lié à. AWS Outposts AWS Outposts définit les rôles liés aux services et inclut toutes les autorisations nécessaires 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.

Autorisations de rôle liées à un service pour AWS Outposts

AWS Outposts utilise le rôle lié au service nommé AWSService RoleForOutposts _. ***`OutpostID`*** Ce rôle accorde aux Outposts l'autorisation de gérer les ressources réseau afin d'activer la connectivité privée en votre nom. Ce rôle permet également aux Outposts de créer et de configurer des interfaces réseau, de gérer des groupes de sécurité et d'associer des interfaces aux instances de point de terminaison Service Link. Ces autorisations sont nécessaires pour établir et maintenir la connexion sécurisée et privée entre votre Outpost sur site et les AWS services, afin de garantir le fonctionnement fiable de votre déploiement Outpost.

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

- `outposts.amazonaws.com`

Politiques relatives aux rôles liés aux services

Le rôle *`OutpostID`* lié au service AWSService RoleForOutposts _ inclut les politiques suivantes :

- AWSOutpostsServiceRolePolicy
- AWSOutpostsPrivateConnectivityPolicy_*`OutpostID`*

AWSOutpostsServiceRolePolicy

La `AWSOutpostsServiceRolePolicy` politique 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 toutes les AWS ressources
- Action : `ec2:DescribeSecurityGroups` sur toutes les AWS ressources
- Action : `ec2:DescribeSubnets` sur toutes les AWS ressources

- Action : `ec2:DescribeVpcEndpoints` sur toutes les AWS ressources
- Action : `ec2:CreateNetworkInterface` sur les AWS ressources suivantes :

```
"arn:*:ec2:*:*:vpc/*",
"arn:*:ec2:*:*:subnet/*",
"arn:*:ec2:*:*:security-group/*"
```

- Action : `ec2:CreateNetworkInterface` sur la AWS ressource `"arn:*:ec2:*:*:network-interface/*"` qui répond à la condition suivante :

```
"ForAnyValue:StringEquals" : { "aws:TagKeys": [ "outposts:private-
connectivity-resourceId" ] }
```

- Action : `ec2:CreateSecurityGroup` sur les AWS ressources suivantes :

```
"arn:*:ec2:*:*:vpc/*"
```

- Action : `ec2:CreateSecurityGroup` sur la AWS ressource `"arn:*:ec2:*:*:security-group/*"` qui répond à la condition suivante :

```
"ForAnyValue:StringEquals": { "aws:TagKeys": [ "outposts:private-
connectivity-resourceId" ] }
```

AWSOutpostsPrivateConnectivityPolicy_OutpostID

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

- Action : `ec2:AuthorizeSecurityGroupIngress` sur toutes les AWS ressources qui répondent à la condition suivante :

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

- Action : `ec2:AuthorizeSecurityGroupEgress` sur toutes les AWS ressources qui répondent à la condition suivante :

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

- Action : `ec2:CreateNetworkInterfacePermission` sur toutes les AWS ressources qui répondent à la condition suivante :

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

- Action : `ec2:CreateTags` sur toutes les AWS ressources qui répondent à la condition suivante :

```
{ "StringLike" : { "aws:RequestTag/outposts:private-connectivity-resourceId" :
 "{{OutpostId}}*"}},
"StringEquals": {"ec2:CreateAction" : ["CreateSecurityGroup",
 "CreateNetworkInterface"]}
```

- Action : `ec2:RevokeSecurityGroupIngress` sur toutes les AWS ressources qui répondent à la condition suivante :

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

- Action : `ec2:RevokeSecurityGroupEgress` sur toutes les AWS ressources qui répondent à la condition suivante :

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

- Action : `ec2:DeleteNetworkInterface` sur toutes les AWS ressources qui répondent à la condition suivante :

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

- Action : `ec2:DeleteSecurityGroup` sur toutes les AWS ressources qui répondent à la condition suivante :

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

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 Autorisations de rôles liés à un service dans le Guide de l'utilisateur IAM.

Créez 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 de plus amples informations, veuillez consulter Options de connectivité privée Service Link.

Modifier un rôle lié à un service pour AWS Outposts

AWS Outposts ne vous permet pas de modifier le rôle *`OutpostID`* lié au service AWSService RoleForOutposts _. 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 au rôle. Néanmoins, vous pouvez modifier la description du rôle à l’aide d’IAM. Pour plus d'informations, voir Mettre à jour un rôle lié à un service dans le Guide de l'utilisateur IAM.

Supprimer 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.

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.

Vous devez supprimer votre Outpost avant de pouvoir supprimer le rôle lié au *`OutpostID`* service AWSService RoleForOutposts _.

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, voir Annulation du partage d'une ressource Outpost partagée.

Pour supprimer AWS Outposts les ressources utilisées par le AWSService RoleForOutposts _ ***`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

Pour plus d'informations, voir Supprimer un rôle lié à un service dans le Guide de l'utilisateur IAM.

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

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 les FAQs racks pour 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 Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

AWS politique gérée : AWSOutposts ServiceRolePolicy

Cette politique est associée à un rôle lié à un service qui permet aux AWS Outposts d'effectuer des actions en votre nom. Pour de plus amples informations, veuillez consulter Rôles liés à un service.

AWS Outposts met à jour les politiques gérées AWS

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

Modification	Description	Date
Mises à jour du AWS Identity and Access Management rôle lié au service	Les autorisations de rôle AWSServiceRoleForOutposts_	18 avril 2025

Modification	Description	Date
_ AWSService RoleForOutposts *OutpostID*	***OutpostID*** liées au service sont mises à jour pour affiner la gestion des ressources AWS Outposts réseau pour la connectivité privée, avec des contrôles plus précis sur l'interface réseau et les opérations des groupes de sécurité nécessaires pour les instances de point de terminaison Service Link.	
AWS Outposts ont commencé à suivre les changements	AWS Outposts a commencé à suivre les modifications apportées à ses politiques AWS 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 EC2 instances et les volumes EBS exécutés sur votre Outpost, consultez la section Sécurité de l'infrastructure sur 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 Outposts sont 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 métriques 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 de plus amples informations, veuillez consulter Groupes de placement sur Outposts.

Vous pouvez lancer des instances dans Outposts à l'aide d'Amazon EC2 Auto Scaling et créer un Application Load Balancer pour 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 :

- Conformité et gouvernance de la sécurité : ces guides de mise en œuvre de solutions traitent des considérations architecturales et fournissent les étapes à suivre afin de déployer des fonctionnalités de sécurité et de conformité.
- Référence des services éligibles HIPAA : liste les services éligibles HIPAA. Tous ne Services AWS sont pas éligibles à la loi HIPAA.
- 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 plusieurs 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.
- Amazon GuardDuty — Cela Service AWS détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité, telles que la norme PCI DSS, en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.
- 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 les tarifs Amazon EC2 On-Demand.
- 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 Outposts n'entrent CIDRs pas en conflit avec les Outposts sur site. CIDRs
- 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.

AWS Outposts s'intègre aux services suivants qui offrent des fonctionnalités de surveillance et de journalisation :

CloudWatch métriques

Utilisez Amazon CloudWatch pour récupérer des statistiques sur les points de données de votre rack 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 de plus amples informations, veuillez consulter CloudWatch .

CloudTrail journaux

AWS CloudTrail À utiliser pour capturer des informations détaillées sur les appels passés à AWS APIs. 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 pour AWS Outposts. Ils contiennent également des informations relatives aux appels à des actions d'API provenant de services présents sur un Outpost, tels qu'Amazon EC2 et Amazon EBS. Pour de plus amples informations, veuillez consulter Enregistrez les appels d'API à l'aide de 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 de votre serveur Outposts out-of-band vers des dispositifs de sécurité et de surveillance. Vous pouvez utiliser le trafic en miroir pour inspecter le contenu, surveiller les menaces ou résoudre les problèmes. Pour plus d'informations, consultez le guide Amazon VPC Traffic Mirroring.

AWS Health Dashboard

AWS Health Dashboard Affiche les informations et les notifications déclenchées par des modifications de l'état de santé des AWS ressources. 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. Une partie du AWS Health service ne AWS Health Dashboard nécessite aucune configuration et peut être consultée par tout utilisateur authentifié dans votre compte. Pour plus d'informations, consultez Démarrer avec le AWS Health Dashboard.

CloudWatch

AWS Outposts publie 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 à1, 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 `ConnectedStatus` problème, nous vous recommandons de vérifier la connectivité à la AWS région depuis votre réseau local et de contacter le 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

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 Outposts Virtual Interfaces VIFs () 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 de la passerelle locale VIFs (lgw-vif) :`OutpostsId`, et `VirtualInterfaceGroupId` `VirtualInterfaceId`

Dimensions du lien de service VIFs (sl-vif) : et `OutpostsId` `VirtualInterfaceId`

`IfTrafficOut`

Débit de données que les Outposts Virtual Interfaces VIFs () transfèrent aux périphériques du réseau local connectés.

Unité : bits par seconde

Résolution maximale : 5 minutes

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

Dimensions de la passerelle locale VIFs (lgw-vif) :`OutpostsId`, et `VirtualInterfaceGroupId` `VirtualInterfaceId`

Dimensions du lien de service VIFs (sl-vif) : et `OutpostsId` `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 inclut le `AvailableReservedInstances` nombre.

Pour déterminer le nombre d'instances que vous pouvez réserver, soustrayez le `AvailableReservedInstances` nombre du `AvailableInstanceType_Count` nombre.

```
Number of instances that you can reserve = AvailableInstanceType_Count
 - AvailableReservedInstances
```

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`

Le nombre d'instances disponibles pour le lancement dans la capacité de calcul réservée à l'aide des réservations de capacité.

Cette métrique n'inclut pas les instances EC2 réservées Amazon.

Cette métrique n'inclut pas le nombre d'instances que vous pouvez réserver. Pour déterminer le nombre d'instances que vous pouvez réserver, soustrayez le `AvailableReservedInstances` nombre du `AvailableInstanceType_Count` nombre.

```
Number of instances that you can reserve = AvailableInstanceType_Count
 - AvailableReservedInstances
```

Unité : nombre

Résolution maximale : 5 minutes

Dimensions : `InstanceType` et `OutpostId`

`UsedReservedInstances`

Le nombre d'instances qui s'exécutent dans la capacité de calcul réservée à l'aide des réservations de capacité. Cette métrique n'inclut pas les instances EC2 réservées Amazon.

Unité : nombre

Résolution maximale : 5 minutes

Dimensions : `InstanceType` et `OutpostId`

`TotalReservedInstances`

Le nombre total d'instances, en cours d'exécution et disponibles pour le lancement, fourni par la capacité de calcul réservée à l'aide des réservations de capacité. Cette métrique n'inclut pas les instances EC2 réservées Amazon.

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 métriques

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.

Vous pouvez consulter les CloudWatch statistiques de votre rack Outposts 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 le champ de recherche.

Pour consulter les statistiques à l'aide du AWS CLI

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

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

Pour obtenir les statistiques d'une métrique à l'aide du 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
```

Enregistrez les appels AWS Outposts d'API à l'aide de AWS CloudTrail

AWS Outposts est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service. CloudTrail capture les appels d'API AWS Outposts sous forme d'événements. Les appels capturés incluent des appels provenant de la AWS Outposts console et des appels de code vers les opérations de l' AWS Outposts API. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite AWS Outposts, l'adresse IP à partir de laquelle la demande a été faite, la date à laquelle elle a été faite et des informations supplémentaires.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l’identité permettent de déterminer :

- Si la demande a été effectuée avec des informations d’identification d’utilisateur root ou d’utilisateur root.
- Si la demande a été faite au nom d'un utilisateur du centre d'identité IAM.

- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la requête a été effectuée par un autre Service AWS.

CloudTrail est actif sur votre AWS compte lorsque vous le créez, et vous avez automatiquement accès à l'historique des CloudTrail événements. L'historique des CloudTrail événements fournit un enregistrement consultable, consultable, téléchargeable et immuable des 90 derniers jours des événements de gestion enregistrés dans un. Région AWS Pour plus d'informations, consultez la section Utilisation de l'historique des CloudTrail événements dans le guide de AWS CloudTrail l'utilisateur. La consultation de CloudTrail l'historique des événements est gratuite.

Pour un enregistrement continu des événements de vos 90 Compte AWS derniers jours, créez un magasin de données sur les événements de Trail ou CloudTrail Lake.

CloudTrail sentiers

Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Tous les sentiers créés à l'aide du AWS Management Console sont multirégionaux. Vous ne pouvez créer un journal de suivi en une ou plusieurs régions à l'aide de l' AWS CLI. Il est recommandé de créer un parcours multirégional, car vous capturez l'activité dans l'ensemble Régions AWS de votre compte. Si vous créez un journal de suivi pour une seule région, il convient de n'afficher que les événements enregistrés dans le journal de suivi pour une seule région Région AWS. Pour plus d'informations sur les journaux de suivi, consultez Créez un journal de suivi dans vos Compte AWS et Création d'un journal de suivi pour une organisation dans le AWS CloudTrail Guide de l'utilisateur.

Vous pouvez envoyer une copie de vos événements de gestion en cours dans votre compartiment Amazon S3 gratuitement CloudTrail en créant un journal. Toutefois, des frais de stockage Amazon S3 sont facturés. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification. Pour obtenir des informations sur la tarification Amazon S3, consultez Tarification Amazon S3.

CloudTrail Stockages de données sur les événements du lac

CloudTrail Lake vous permet d'exécuter des requêtes SQL sur vos événements. CloudTrail Lake convertit les événements existants au format JSON basé sur les lignes au format Apache ORC. ORC est un format de stockage en colonnes qui est optimisé pour une récupération rapide des données. Les événements sont agrégés dans des magasins de données d'événement. Ceux-ci constituent des collections immuables d'événements basées sur des critères que vous

sélectionnez en appliquant des sélecteurs d'événements avancés. Les sélecteurs que vous appliquez à un magasin de données d'événement contrôlent les événements qui persistent et que vous pouvez interroger. Pour plus d'informations sur CloudTrail Lake, consultez la section Travailler avec AWS CloudTrail Lake dans le guide de AWS CloudTrail l'utilisateur.

CloudTrail Les stockages et requêtes de données sur les événements de Lake entraînent des coûts. Lorsque vous créez un magasin de données d'événement, vous choisissez l'option de tarification que vous voulez utiliser pour le magasin de données d'événement. L'option de tarification détermine le coût d'ingestion et de stockage des événements, ainsi que les périodes de conservation par défaut et maximale pour le magasin de données d'événement. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification.

AWS Outposts événements de gestion dans CloudTrail

Les événements de gestion fournissent des informations sur les opérations de gestion effectuées sur les ressources de votre Compte AWS. Ils sont également connus sous le nom opérations de plan de contrôle. Par défaut, CloudTrail enregistre les événements de gestion.

AWS Outposts enregistre toutes les opérations du plan de contrôle des AWS Outposts en tant qu'événements de gestion. Pour une liste des opérations du plan de contrôle AWS Outposts auxquelles Outposts se connecte, CloudTrail consultez le Guide de référence de l'API AWSAWS Outposts.

AWS Outposts exemples d'événements

L'exemple suivant montre un CloudTrail événement illustrant l'`SetSiteAddress`opération.


```
{
    "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"
}
```

Dans le cadre du modèle de responsabilité partagée de responsabilité partagée AWS est responsable du matériel et des logiciels qui exécutent AWS les services. Cela s'applique à une région AWS Outposts, tout comme cela s'applique à une AWS région. Par exemple, AWS gère les correctifs de sécurité, met à jour le microprogramme et assure la maintenance de l'équipement Outpost. AWS surveille également les performances, l'état de santé et les indicateurs de votre rack Outposts et détermine si une 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

Mettre à jour les coordonnées

Si le propriétaire de l'Outpost change, contactez le AWS Support Centre en indiquant le nom et les coordonnées du nouveau propriétaire.

Maintenance matérielle

Si un problème matériel irréparable est AWS détecté pendant le processus de mise en service du serveur ou lors de l'hébergement d' EC2 instances Amazon exécutées sur votre rack Outposts, nous informerons le propriétaire de l'Outpost et le propriétaire des instances que les instances concernées

sont censées être retirées. Pour plus d'informations, consultez la section Retrait d'instance dans le guide de EC2 l'utilisateur Amazon.

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 de mise hors service de l'instance. 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 du matériel est requise, AWS contactera le propriétaire de l'Outpost pour confirmer la date et l'heure de la visite de AWS l'équipe d'installation. Les visites peuvent être planifiées dans un délai de deux jours ouvrables à compter du moment où le propriétaire de l'avant-poste a parlé à l' AWS équipe.

Lorsque l'équipe AWS d'installation arrive sur place, elle remplace les hôtes, les commutateurs ou les éléments de rack défectueux et met en service la nouvelle capacité. 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 des adresses IP et être ASNs utilisées pour établir des interfaces virtuelles afin de configurer le chemin d'accès à votre réseau local ou de retour vers 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. Le préfixe AS-Path est utilisé pour les préfixes de passerelle locale afin de détourner le trafic ONDs si une maintenance est requise. 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 client doit annoncer des préfixes BGP identiques avec les mêmes attributs à tous. ONDs 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 transfert de trafic nécessite des préfixes BGP identiques de la part du client pour tous. ONDs 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

Comme indiqué dans les conditions de AWS service destinées AWS Outposts aux clients, l'installation où se trouve l'équipement Outposts doit répondre aux exigences minimales en matière d'alimentation et de réseau pour prendre en charge l'installation, la maintenance et l'utilisation de l'équipement Outposts. Un rack Outposts ne peut fonctionner correctement que lorsque l'alimentation et la connectivité réseau ne sont pas interrompues.

Événements liés à l'alimentation

En cas de panne de courant complète, il existe un risque inhérent qu'une AWS Outposts ressource ne soit pas remise 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.
- Une fois l'alimentation rétablie, créez un dossier au AWS Support centre pour demander à vérifier que les services associés sont en cours d'exécution AWS Outposts et que les services associés sont en cours d'exécution.

Événements liés à la connectivité réseau

La liaison de service entre votre Outpost et la AWS région ou la région d'origine de l'Outpost se rétablit généralement automatiquement en cas d'interruption du réseau ou de problèmes susceptibles de survenir sur les appareils réseau de votre entreprise en amont ou sur le réseau de tout fournisseur de connectivité tiers une fois la maintenance du réseau terminée. Pendant que la connexion de la liaison de service est hors service, vos opérations Outposts sont limitées aux activités du réseau local.

EC2 Les instances Amazon, la passerelle locale et les volumes Amazon EBS sur les Outposts continueront de fonctionner normalement et seront accessibles localement via le réseau local. De même, les ressources de AWS service telles que les nœuds de travail Amazon ECS continuent de s'exécuter localement. Cependant, la disponibilité de l'API sera dégradée. Par exemple, les commandes run, start, stop et terminate APIs risquent de ne pas fonctionner. Les statistiques et les journaux des instances continueront d'être mis en cache localement pendant 7 jours au maximum et seront transmis à la AWS région lorsque la connectivité sera rétablie. Une déconnexion au-delà de 7 jours peut entraîner la perte de statistiques et de journaux.

Pour plus d'informations, consultez la question Que se passe-t-il en cas de panne de la connexion réseau de mon établissement ? sur la FAQs page du AWS Outposts rack.

Si la liaison de service est interrompue en raison d'un problème d'alimentation sur site ou d'une perte de connectivité réseau, le service AWS Health Dashboard envoie une notification au compte

propriétaire des Outposts. Ni vous ni ne AWS pouvez supprimer la notification d'une interruption de 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 AWS région parent via Internet ou une connexion directe publique, enregistrez un trace-itinéraire avant toute 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 signalez un problème post-maintenance à AWS ou à votre fournisseur de services Internet, 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 AWS région parent.
  - 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 AWS blog Monitoring best practices for AWS Outposts couvre les meilleures pratiques en matière d'observabilité et de gestion des événements spécifiques aux Outposts.

- Le AWS blog sur l'outil de débogage pour la connectivité réseau d'Amazon VPC explique AWSSupport-SetupIPMonitoringFromVPCcet outil. Cet outil est un AWS Systems Manager document (document SSM) qui crée une instance Amazon EC2 Monitor 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 des Outposts, l'instance de surveillance doit se trouver dans un sous-réseau de la AWS région parent et être configurée pour surveiller une ou plusieurs de vos instances Outpost à l'aide de ses adresses IP privées. Cela fournira des graphiques de perte de paquets et de latence entre AWS Outposts et la région parent. AWS
- 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.

Options de rack pour Outposts end-of-term

À la fin de votre AWS Outposts mandat, vous devez choisir entre les options suivantes :

- Renouvelez votre abonnement et conservez vos étagères Outposts existantes.
- Mettez fin à votre abonnement et préparez vos racks Outposts pour le retour.
- Passez à un month-to-month abonnement et conservez vos étagères Outposts existantes.

Renouvellement de votre abonnement

Vous devez effectuer les étapes suivantes au moins 30 jours avant la fin de l'abonnement en cours pour vos Outposts racks.

Pour renouveler votre abonnement et conserver vos racks Outposts existants

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.

AWS Support client lancera le processus de renouvellement de l'abonnement. Votre nouvel abonnement débutera le lendemain de la fin de votre abonnement actuel.

Si vous n'indiquez pas que vous souhaitez renouveler votre abonnement ou retourner votre rack Outposts, vous serez automatiquement converti en month-to-month abonnement. Votre rack Outposts sera renouvelé tous les mois au taux de l'option de paiement No Upfront correspondant à votre configuration. AWS Outposts Votre nouvel abonnement mensuel débutera le lendemain de la fin de votre abonnement actuel.

Fin de votre abonnement et préparation des racks pour le retour

Vous devez effectuer les étapes suivantes au moins 30 jours avant la fin de l'abonnement actuel à votre rack Outposts. AWS vous ne pouvez pas démarrer le processus de retour tant que vous ne l'avez pas fait.

> **Important**
>
> AWS vous ne pouvez pas arrêter le processus de retour une fois que vous avez ouvert un dossier d'assistance pour mettre fin à votre abonnement.

Pour mettre fin à votre abonnement

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.

AWS Le Support client vous contactera pour coordonner la récupération.

Pour préparer vos AWS Outposts rayonnages en vue du retour :

> **⚠ Important**
>
> Ne mettez pas le rack des Outposts hors tension tant qu' AWS il n'est pas sur place pour la récupération planifiée.

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 AWS RAM console. Pour plus d'informations, consultez Mise à jour d'un partage de ressources dans le Guide de l'utilisateur AWS RAM .
   - Utilisez le AWS CLI pour exécuter la disassociate-resource-sharecommande.

   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 mettre fin aux instances, suivez les instructions de la section Résiliation de votre instance dans le guide de EC2 l'utilisateur Amazon.

> **Note**
>
> Certains services AWS gérés exécutés sur votre Outpost, tels que les équilibreurs de charge d'application ou Amazon Relational Database Service (RDS), consomment de la capacité. EC2 Cependant, leurs instances associées ne sont pas visibles sur le tableau de EC2 bord Amazon. Vous devez mettre fin aux ressources liées à ces services pour libérer de la capacité. Pour plus d'informations, consultez Pourquoi certaines capacités d'EC2instance manquent-elles sur mon Outpost ? .

3. Vérifiez instance-capacity-availability les EC2 instances Amazon de votre AWS compte.

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

   b. Choisissez Outposts.

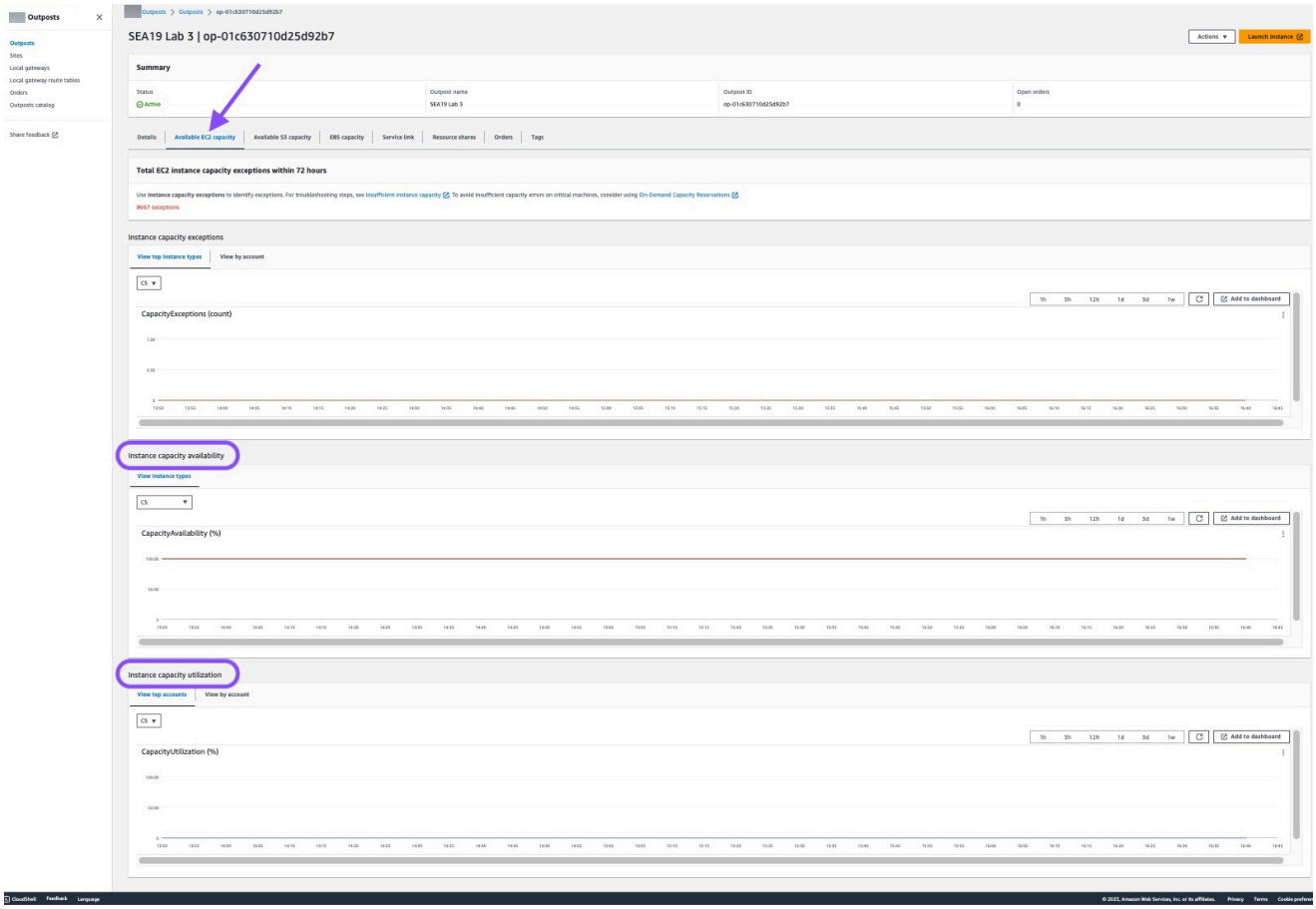
   c. Choisissez l'Outpost spécifique que vous retournez.

   d. Sur la page de l'avant-poste, choisissez l'onglet EC2 Capacité disponible.

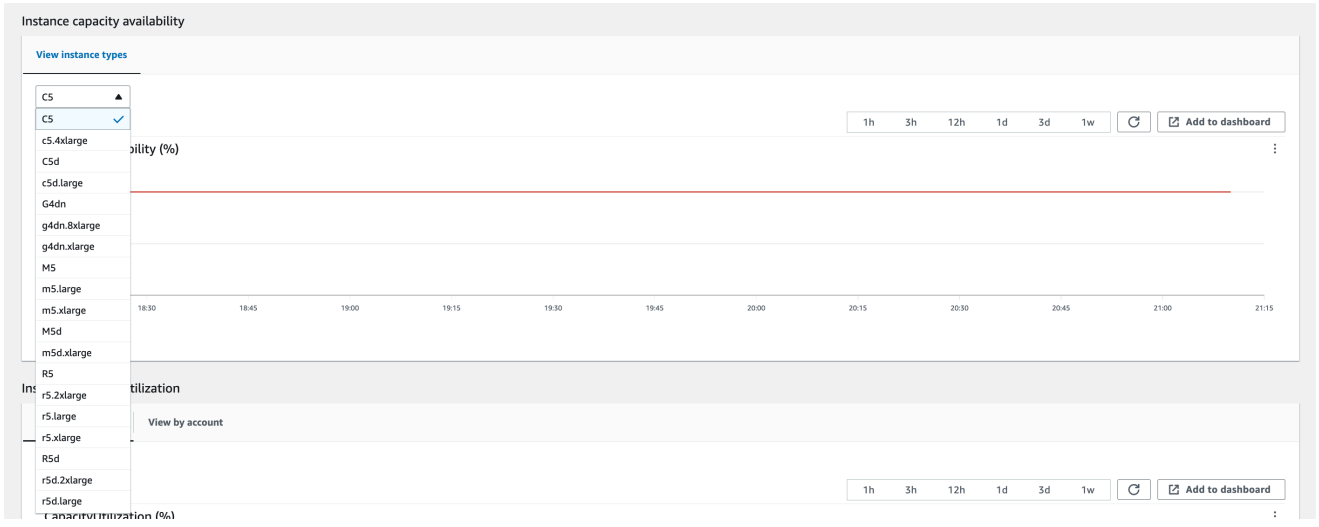
   e. Assurez-vous que l'option Disponibilité de la capacité d'instance est définie sur 100 % pour chaque famille d'instances.

   f. Assurez-vous que l'option Utilisation de la capacité d'instance est définie sur 0 % pour chaque famille d'instances.

      L'image suivante montre les graphiques de disponibilité de la capacité d'instance et d'utilisation de la capacité d'instance dans l'onglet EC2 Capacité disponible.



L'image suivante présente la liste des types d'instance.



4. Créez des sauvegardes de vos EC2 instances Amazon et de vos volumes de serveurs. Pour créer les sauvegardes, suivez les instructions de la section Backup and recovery for Amazon EC2 with EBS volumes du guide AWS prescriptif.
5. Supprimez les volumes Amazon EBS associés à votre Outpost.

a. Ouvrez la EC2 console Amazon à l'adresse 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 EC2 console Amazon à l'adresse 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 rack Outposts. Pour supprimer les compartiments, suivez les instructions de la section Supprimer votre compartiment Amazon S3 on Outposts dans le guide de l'utilisateur d'Amazon S3 on Outposts.
8. Supprimez toutes les associations VPC et tous les pools d'adresses IP (CoIP) CIDRs appartenant au client associés à votre Outpost.

Une équipe AWS de récupération mettra le rack hors tension. Une fois hors tension, vous pouvez détruire la clé de sécurité AWS Nitro ou l'équipe chargée de la AWS récupérer peut le faire à votre place.

Convertir en month-to-month abonnement

Pour passer à un month-to-month abonnement et conserver vos racks Outposts existants, aucune action n'est nécessaire. Si vous avez des questions, ouvrez un cas de support pour la facturation.

Vos racks Outposts seront renouvelés tous les mois au taux de l'option de paiement No Upfront correspondant à votre configuration Outposts. Votre nouvel abonnement mensuel commence le lendemain de la fin de votre abonnement actuel.

Quotas pour AWS Outposts

Vous Compte AWS disposez de quotas par défaut, anciennement appelés limites, pour chacun d'entre eux Service AWS. Sauf indication contraire, chaque quota est spécifique à la région. Vous pouvez demander l'augmentation de certains quotas, mais pas de tous les quotas.

Pour consulter les quotas pour AWS Outposts, ouvrez la console 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.

Vous Compte AWS disposez des quotas suivants relatifs à AWS Outposts.

Ressource	Par défaut	Ajustable	Commentaires
Sites Outpost	100	Oui	Un site Outpost est le bâtiment physique géré par le client dans lequel vous alimentez et reliez votre équipement Outpost au réseau. Vous pouvez avoir 100 sites Outposts dans chaque région de votre AWS compte.
Outposts par site	10	Oui	AWS Outposts inclut des ressources matérielles et virtuelles, connues sous le nom d'Outposts. Ce quota limite les ressources virtuelles de votre Outpost. Vous pouvez avoir 10 Outposts dans chaque site Outpost.

AWS Outposts et les quotas pour les autres services

AWS Outposts repose sur les 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.

Modification	Description	Date
Mises à jour de la stabilité statique	En cas d'interruption de votre réseau, les métriques et les journaux de l'instance seront mis en cache localement pendant 7 jours au maximum. Auparavant, les Outposts pouvaient mettre en cache les journaux pendant quelques heures seulement.	1er mai 2025
Mises à jour du AWS Identity and Access Management rôle lié au service _ AWSService RoleForOutposts *OutpostID*	Les autorisations de rôle AWSServiceRoleForOutposts_ ***OutpostID*** liées au service sont mises à jour pour affiner la gestion des ressources AWS Outposts réseau pour la connectivité privée, avec des contrôles plus précis sur l'interface réseau et les opérations des groupes de sécurité nécessaires pour les instances de point de terminaison Service Link.	17 avril 2025
Gestion des capacités au niveau des actifs	Vous pouvez modifier la configuration de la capacité au niveau de l'actif.	31 mars 2025
Connectivité privée utilisant le AWS Direct Connect réseau VIF de transit	Vous pouvez désormais configurer le lien de service pour utiliser un VIF de AWS Direct Connect transit afin de permettre une connectivité	11 décembre 2024

	privée entre les Outposts et la région d'origine AWS .	
Volumes de blocs externes soutenus par un système de stockage tiers	Vous pouvez désormais associer des volumes de données par blocs soutenus par des systèmes de stockage par blocs tiers compatibles pendant le processus de lancement de l'instance sur Outpost.	1er décembre 2024
Gestion des capacités	Vous pouvez modifier la configuration de capacité d'une instance.	11 novembre 2024
Gestion des capacités	Vous pouvez modifier la configuration de capacité par défaut pour votre nouvelle commande d'Outposts.	16 avril 2024
AWS Outposts le rack prend en charge les mesures de débit de l'interface Service Link	Vous pouvez désormais surveiller l'utilisation du débit entre les interfaces virtuelles de vos Outposts Rack Service Link VIFs () et les périphéri ques de votre réseau local, en `IfTrafficIn` tirant parti `IfTrafficOut` Amazon CloudWatch des métriques.	17 novembre 2023
Communication intra-VPC via AWS Outposts 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

End-of-term options pour les AWS Outposts racks	À la fin de votre AWS Outposts période, vous pouvez renouveler, résilier ou convertir votre abonnement.	1er août 2023
Amazon Route 53 on Outposts est disponible sur AWS Outposts racks.	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 un résolveur Outpost et un résolveur DNS sur site lorsque vous déployez des points de terminaison entrants et sortants.	20 juillet 2023
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 AWS Outposts l'utilisateur créé pour les Outposts Racks	AWS Outposts Le guide de l'utilisateur a été divisé en guides distincts pour le rack 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. Gère les associations de groupe d'interfaces virtuelles (VIF).	14 septembre 2022
Groupes de placement sur AWS Outposts	Les groupes de placement qui utilisent une stratégie d'extension 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 AWS comptes 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	Mise à disposition d'une liste de contrôle pour la résolution des problèmes de réseau.	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
AWS Outposts Ressources 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 AWS comptes 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
Support pour le partage des adresses appartenant aux clients IPv4	AWS Resource Access Manager À utiliser pour partager les adresses appartenant aux clients IPv4 .	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 version initiale de 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.