Guide de l’utilisateur pour les serveurs

AWS Outposts

AWS Outposts: Guide de l’utilisateur pour les serveurs

Table of Contents

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

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

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

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

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

Concepts clés

Ce sont les concepts clés pour AWS Outposts.

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

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

AWS ressources sur Outposts

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

Calcul

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

Base de données et analytique

Type de ressource	Racks	Serveurs
ElastiCache Nœuds Amazon (cluster Redis, cluster Memcached)	 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	 Oui	 Non
Compartiments Amazon S3	 Oui	 Non

Autres Services AWS

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

Tarification

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

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

- AWS Outposts tarification des rayonnages

- AWS Outposts tarification des serveurs

Fonctionnement d'AWS Outposts

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

Le schéma suivant illustre les deux formats Outpost.

Table des matières

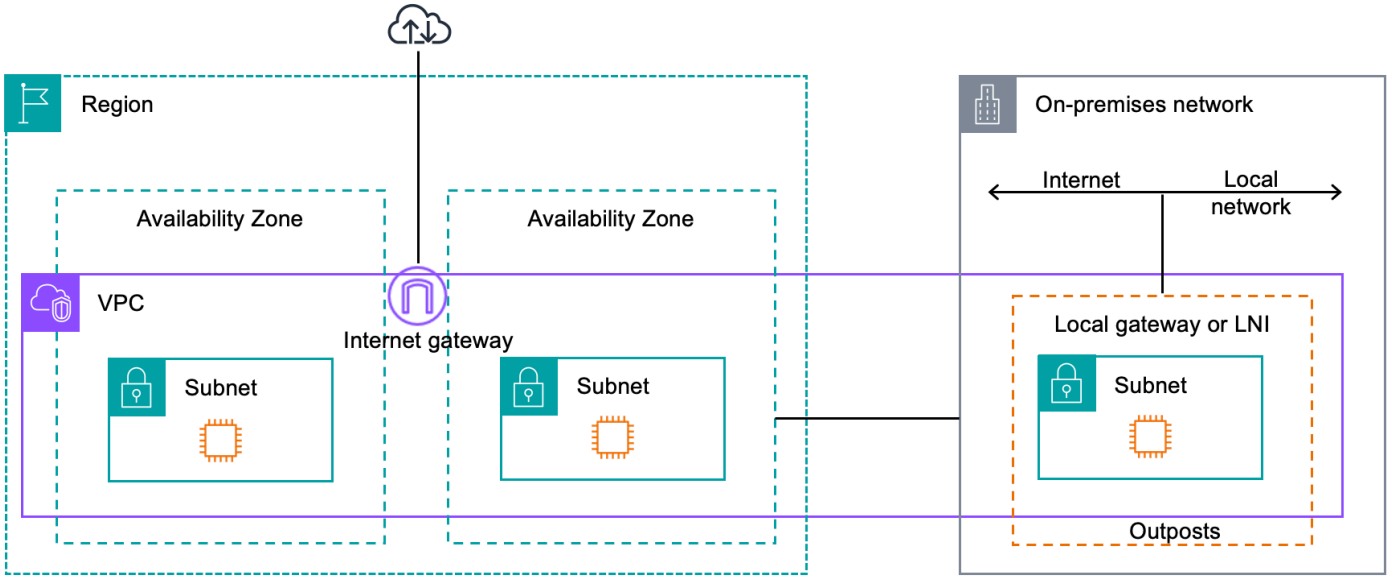
Composants du réseau

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

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

- Un Région AWS et un réseau sur site
- Un VPC avec plusieurs sous-réseaux dans la région
- Un avant-poste dans le réseau local

- Connectivité entre l'avant-poste et le réseau local assurée par une passerelle locale (racks) ou une interface réseau locale (serveurs)



VPC et sous-réseaux

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

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

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

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

Routage

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

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

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

- Plage d'adresses CIDR VPC : elle est AWS définie lors de l'installation. Il s'agit de la route locale qui s'applique à tous les routages VPC, y compris le trafic entre les instances d'Outpost d'un même VPC.
- AWSDestinations régionales : cela inclut les listes de préfixes pour Amazon Simple Storage Service (Amazon S3), les points de terminaison de la passerelle Amazon DynamoDB, les passerelles privées virtuellesAWS Transit Gateway, les passerelles Internet et le peering VPC.

  Si vous avez une connexion d'appairage avec plusieurs VPC sur le même avant-poste, le trafic entre les VPC reste dans l'avant-poste et n'utilise pas le lien de service vers la région.

DNS

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

Il se peut que vous rencontriez des temps de résolution DNS plus longs avec Route 53, en fonction de la latence du chemin entre votre Outpost et la région AWS. Dans ce cas, vous pouvez utiliser

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

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

Lien vers le service

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

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

Passerelles locales

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

Interfaces réseau locales

Les serveurs Outpost incluent une interface réseau locale qui fournit une connectivité à votre réseau local. Une interface réseau locale n'est disponible que pour les serveurs Outposts exécutés sur un

sous-réseau Outpost. Vous ne pouvez pas utiliser d'interface réseau locale à partir d'une instance EC2 sur un rack Outpost ou dans la AWS région. L'interface réseau locale est uniquement destinée aux sites locaux. Pour plus d'informations, veuillez consulter Interfaces réseau locales.

Un site Outpost est l'emplacement physique où opère votre Outpost. Les sites sont uniquement disponibles dans certains pays et territoires. Pour de plus amples informations, veuillez consulter FAQ sur les serveurs AWS Outposts. Reportez-vous à la question : Dans quels pays et territoires les serveurs Outposts sont-ils disponibles ?

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

Installations

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

> **Note**
>
> Les spécifications concernent les serveurs fonctionnant dans des conditions normales. Par exemple, le bruit peut être plus important lors de l'installation initiale, puis s'ajuster à la puissance sonore nominale une fois l'installation terminée.

- Température : la température ambiante doit être comprise entre 5 et 35 °C (41 et 95 °F).

  Le serveur s'arrête lorsque la température se situe en dehors de cette plage et redémarre lorsqu'elle revient dans cette plage.
- Humidité : l'humidité relative doit être comprise entre 8 et 80 % sans condensation.
- Qualité de l'air : l'air doit être filtré à l'aide d'un filtre MERV8 (ou supérieur).
- Débit d'air : le serveur doit être installé de façon à assurer un espace minimum de 15 cm (6 pouces) entre lui et les murs situés devant et derrière lui, afin de permettre une circulation d'air suffisante.
- Poids : le serveur 1U pèse 11,800 kg (26 livres) et le serveur 2U 16,300 kg (36 livres). Assurez-vous que l'emplacement où vous souhaitez placer le serveur peut supporter son poids.

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

- Compatibilité avec les kits de rails : le kit de rails inclus dans votre colis est compatible avec un support de montage en L standard d'un rack de 19 pouces conforme à la norme EIA-310-D.

  > **Important**
  >
  > Le kit de rails n'est pas compatible avec un support de montage en U, comme le montre l'image suivante.

- Emplacement des racks : nous recommandons l'utilisation de racks EIA-310D standard de 19 pouces, avec une profondeur d'au moins 914 mm (36 pouces).
  - Les serveurs Outposts 2U ont besoin d'espace aux dimensions suivantes : 3,5 pouces de hauteur (88,9 mm), 17,5 pouces de largeur (447 mm), 30 pouces de profondeur (762 mm)
  - Les serveurs Outposts 1U ont besoin d'espace aux dimensions suivantes : 1,75 pouces de hauteur (44,45 mm), 17,5 pouces de largeur (447 mm), 24 pouces de profondeur (610 mm)

  > **Note**
  >
  > - Le montage vertical AWS Outposts des serveurs n'est pas pris en charge.
  > - Les serveurs Outposts 1U ont la même largeur que les serveurs Outposts 2U, mais ils sont deux fois moins hauts et moins profonds

  AWS fournit un kit de rails pour le montage en rack du serveur. Pour plus d'informations, consultez Étape 3 : Monter le rack.

  Si vous ne placez pas le serveur dans un rack, vous devez tout de même satisfaire aux autres exigences répertoriées dans cette section.

- Facilité de maintenance : la maintenance des serveurs Outposts se fait par l'avant.
- Niveau sonore : inférieur à 78 dBA à une température de 27 °C (80 °F) et conforme à la norme GR-63 CORE NEBS.
- Contreventement parasismique : dans la mesure requise par la réglementation ou le code, vous installerez et entretiendrez un ancrage et un contreventement parasismiques appropriés pour le serveur pendant qu'il se trouve dans vos installations.
- 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).

- Nettoyage : essuyez les surfaces avec des lingettes humides contenant des produits chimiques de nettoyage antistatiques approuvés.

Réseaux

Chaque serveur Outposts inclut ports physiques de liaison montante non redondants. Chaque port a ses propres exigences en matière de vitesse et de connecteurs, comme indiqué ci-dessous.

Étiquette du port	Vitesse	Connecteur sur le périphérique réseau en amont	Trafic
Port 3	10 GbE	SFP+	Trafic de liaison de service et LNI : le câble de dérivation QSFP + (10 pieds/3 m) segmente le trafic. Pour plus d'informations, consultez Configuration du réseau QSFP.

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	1024-65535	Adresse IP de la liaison de service	53	Serveur DNS fourni par DHCP
UDP	443, 1024-65535	Adresse IP de la liaison de service	443	Points de terminaison Outposts Service Link

Protocole	Port source	Adresse source	Port de destination	Adresse de destination
TCP	1024-65535	Adresse IP de la liaison de service	443	Points de terminaison d'enregistrement des Outposts

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 des liens du service Outposts, vous pouvez utiliser le NAT ou le PAT sur votre pare-feu ou votre routeur périphérique. L'établissement d'une liaison de service est toujours initié depuis Outpost.

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

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

Recommandations concernant la bande passante de la liaison de service

Pour une expérience et une résilience optimales, il est AWS recommandé d'utiliser une connectivité redondante d'au moins 500 Mbits/s pour la connexion par liaison de service vers la AWS région. L'utilisation maximale pour chaque serveur Outpost est de 500 Mbits/s. Pour accroître la vitesse de connexion, utilisez plusieurs serveurs Outpost. Par exemple, avec trois serveurs AWS Outposts , la vitesse de connexion maximale passe à 1,5 Gbit/s (1 500 Mbits/s). Pour plus d'informations, consultez Trafic de liaison de service pour les serveurs.

Les besoins en bande passante de vos liaisons de AWS Outposts service varient en fonction des caractéristiques de la charge de travail, telles que la taille de l'AMI, l'élasticité de l'application, les besoins en vitesse de rafale et le trafic Amazon VPC vers la région. Notez que les AWS Outposts serveurs ne mettent pas en cache les AMI. Les AMI sont téléchargées depuis la région à chaque lancement d'instance.

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.

La liaison de service nécessite une réponse DHCP

Le lien de service nécessite une réponse DHCP IPv4 pour configurer les paramètres réseau.

Latence maximale de la liaison de service

Les liaisons de service peuvent prendre en charge une latence réseau maximale de 250 ms à partir du serveur et de sa zone de disponibilité.

Alimentation

Les exigences en matière d'alimentation pour les serveurs Outposts sont décrites ci-dessous.

Prérequis

- Soutien en alimentation
- Consommation énergétique
- Câble d'alimentation
- Redondance de l'alimentation

Soutien en alimentation

Les serveurs peuvent être alimentés en courant alternatif jusqu'à 1 600 W 90-264 Vca 47/63 Hz.

Consommation énergétique

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

Câble d'alimentation

Le serveur est livré avec un câble d'alimentation CEI C14-C13.

Câblage d'alimentation entre le serveur et le rack

Utilisez le câble d'alimentation CEI C14-C13 fourni pour relier le serveur au rack.

Câblage d'alimentation entre le serveur et la prise murale

Pour relier le serveur à une prise murale standard, vous devez utiliser un adaptateur pour l'entrée C14 ou un cordon d'alimentation spécifique au pays.

Assurez-vous de disposer de l'adaptateur ou du câble d'alimentation adapté à votre région afin de gagner du temps lors de l'installation du serveur.

- Aux États-Unis, vous avez besoin d'un câble d'alimentation CEI C13 vers NEMA 5-15P.
- Dans certaines régions d'Europe, vous pourriez avoir besoin d'un câble d'alimentation CEI C13 vers CEE 7/7.
- En Inde, vous avez besoin d'un câble d'alimentation CEI C13 vers IS1293.

Redondance de l'alimentation

Les serveurs sont dotés de plusieurs connexions électriques et sont fournis avec des câbles pour permettre un fonctionnement redondant. Nous recommandons la redondance de l'alimentation, mais aucune redondance n'est requise.

Les serveurs ne sont pas équipés d'une alimentation sans interruption (UPS).

Exécution des commandes

Pour exécuter la commande, l'équipement du serveur Outposts, y compris les supports de rail et les câbles d'alimentation et de réseau nécessaires, AWS sera expédié à l'adresse que vous avez fournie. Les dimensions de la boîte dans laquelle le serveur est expédié sont les suivantes :

- Boîte avec serveur 2U :
  - Longueur : 44 pouces/111,8 cm
  - Hauteur : 67,3 cm/26,5 pouces
  - Largeur : 43,2 cm/17 pouces
- Boîte avec serveur 1U :
  - Longueur : 87,6 cm/34,5 pouces
  - Hauteur : 61 cm/24 pouces
  - Largeur : 22,9 cm/9 pouces

Votre équipe ou un fournisseur tiers doit installer l'équipement. Pour plus d'informations, consultez Installation du serveur Outpost.

L'installation est terminée lorsque vous confirmez que la capacité Amazon EC2 pour votre serveur Outposts est disponible depuis votre compte. AWS

Commencez avec AWS Outposts

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

Tâches

- Création d’un Outpost et commande de capacité Outpost
- Installation du serveur Outpost
- Lancez une instance sur votre serveur Outpost

Création d’un Outpost et commande de capacité Outpost

Pour commencer à l'utiliser AWS Outposts, connectez-vous avec le AWS compte qui possédera l'Outpost. Créez un site et un Outpost. Passez ensuite une commande pour les serveurs Outposts dont vous avez besoin.

Prérequis

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

Tâches

- Étape 1 : Créer un site
- Étape 2 : Création d’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'endroit où vous allez installer et exécuter vos serveurs Outposts. Après avoir créé le site, AWS Outposts attribuez-lui un identifiant. Vous devez spécifier ce site lorsque vous créez un Outpost.

Prérequis

- Déterminez l'adresse d'exploitation.

Pour créer un site

1. Connectez-vous pour AWS utiliser le propriétaire Compte AWS de l'Outpost.
2. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.
3. Pour sélectionner le parent Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page.
4. Dans le panneau de navigation, choisissez Sites.
5. Choisissez Créer un site.
6. Pour Type de matériel pris en charge, choisissez Serveurs uniquement.
7. Saisissez le nom, la description et l'adresse d'exploitation de votre site.
8. (Facultatif) Pour les notes sur le site, entrez toute autre information qui pourrait être utile AWS pour en savoir plus sur le site.
9. Choisissez Créer un site.

Étape 2 : Création d'un Outpost

Créez un Outpost pour chaque serveur. Un Outpost ne peut être associé qu'à un seul serveur. Vous spécifierez cet Outpost au moment de passer la commande.

Prérequis

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

Pour créer un Outpost

1. Dans le panneau de navigation, sélectionnez Outposts.

2. Choisissez Créer un Outpost.
3. Choisissez Serveurs.
4. Saisissez un nom et une description pour votre Outpost.
5. Choisissez une zone de disponibilité pour l'Outpost.
6. Pour ID du site, choisissez votre site.
7. Choisissez Créer un Outpost.

Étape 3 : Passer la commande

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

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

Prérequis

- Déterminez le mode de paiement de la commande. Vous pouvez payer la totalité à l'avance, une partie à l'avance ou rien à l'avance. Si vous choisissez l'option Frais initiaux partiels ou Aucuns frais initiaux, vous serez soumis à des frais mensuels pendant trois ans.

  Les prix incluent la livraison, 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, choisissez Serveurs.

4. Pour ajouter de la capacité, choisissez une configuration.
5. Choisissez Suivant.
6. Choisissez Utiliser un Outpost existant et sélectionnez votre Outpost.
7. Choisissez Suivant.
8. Sélectionnez une durée de contrat et une option de paiement.
9. Spécifiez l'adresse de livraison. Vous pouvez spécifier une nouvelle adresse ou sélectionner l'adresse d'exploitation du site. Si vous sélectionnez l'adresse d'exploitation, sachez que toute future modification de l'adresse d'exploitation du site ne se propagera pas aux commandes existantes. Si vous devez modifier l'adresse de livraison d'une commande existante, contactez votre responsable de AWS compte.
10. Choisissez Suivant.
11. Sur la page Vérifier et commander, vérifiez que vos informations sont correctes et modifiez-les si nécessaire. Vous ne pouvez pas modifier une commande déjà soumise.
12. Choisissez Passer la commande.

Étape 4 : Modifier la capacité de l'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 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 AWS Outposts 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 une nouvelle configuration de capacité d'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 sur le type d'instance correspondante.
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.

Upload 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 :

   ```
   {
       "RequestedInstancePools": [
           {
               "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.

Étapes suivantes

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

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

Pour exécuter la commande, AWS fixera une date de livraison.

Vous êtes responsable de toutes les tâches d'installation, y compris l'installation physique et la configuration réseau. Vous pouvez confier ces tâches à un prestataire tiers. Que vous réalisiez vous-même l'installation ou que vous la confiiez à un tiers, l'installation a besoin des informations d'identification IAM du Compte AWS qui contient l'Outpost pour vérifier l'identité du nouvel appareil. Il vous incombe de fournir et de gérer cet accès. Pour plus d'informations, consultez the section called "Installation du serveur Outpost".

L'installation est terminée une fois que la capacité Amazon EC2 de votre Outpost est disponible dans votre compte Compte AWS. Dès que la capacité est disponible, vous pouvez lancer des instances Amazon EC2 sur votre serveur Outpost. Pour plus d'informations, consultez the section called "Lancer une instance ".

Installation du serveur Outpost

Lorsque vous commandez un serveur Outpost, vous êtes responsable de l'installation, que vous la réalisiez vous-même ou que vous la confiiez à un tiers. Les intervenants chargés de l'installation ont besoin d'autorisations spécifiques pour vérifier l'identité du nouvel appareil. Pour plus d'informations, consultez Accorder des autorisations.

Prérequis

Vous devez disposer d'un facteur de forme de serveur Outpost sur votre site. Pour plus d'informations, consultez Création d'un Outpost et commande de capacité Outpost.

> **Note**
>
> Nous vous recommandons de visionner la vidéo de formation sur l'installation de AWS Outposts serveurs avant et pendant le processus d'installation. Pour accéder à la formation, vous devez vous connecter ou créer un compte sur AWS Skill Builder.

Tâches

Étape 1 : Accorder des autorisations

Pour vérifier l'identité du nouvel appareil, vous devez disposer d'informations d'identification IAM dans le Compte AWS qui contient l'Outpost. La politique AWSOutpostsAuthorizeServerPolicy accorde les autorisations nécessaires pour installer un serveur Outpost. Pour plus d'informations, consultez the section called "Gestion des identités et des accès".

Considérations

- Si vous utilisez un tiers qui n'a pas accès à votre compte Compte AWS, vous devez fournir un accès temporaire.
- AWS Outposts prend en charge l'utilisation d'informations d'identification temporaires. Vous pouvez configurer des informations d'identification temporaires d'une durée maximale de 36 heures. Veillez à accorder suffisamment de temps à l'installateur pour effectuer toutes les étapes nécessaires à l'installation du serveur. Pour plus d'informations, consultez the section called "Informations d'identification temporaires".

Étape 2 : Inspecter

Pour effectuer une inspection de l’équipement Outposts, vérifiez que le colis de livraison n’est pas endommagé, déballez-le, puis localisez la clé de sécurité Nitro (NSK). Au moment d’inspecter le serveur, tenez compte des informations suivantes :

- Des capteurs de choc sont présents sur les deux plus grands côtés du colis de livraison.
- Le rabat intérieur du colis contient des instructions pour déballer le serveur et localiser la clé NSK.
- La clé NSK est un module de chiffrement. Pour effectuer l’inspection, localisez la clé NSK. Vous devrez l’attacher au serveur dans une étape ultérieure.

Vérification du colis de livraison

Pour inspecter le colis de livraison

- Avant d’ouvrir le colis, vérifiez si les deux capteurs de choc ont été activés. Si tel est le cas, il est possible que l’appareil ait été endommagé. Passez à l’installation en prenant le temps de relever les autres dommages éventuels sur le serveur ou les accessoires. Si une partie du système est manifestement endommagée ou si l'installation ne se déroule pas comme prévu, contactez le AWS Support pour obtenir des conseils sur le remplacement de votre serveur Outposts.

Si la barre au milieu du capteur est rouge, cela signifie qu’il a été activé.

Déballage du colis de livraison

Pour déballer le colis de livraison

- Ouvrez le colis et vérifiez qu’il contient les éléments suivants :
  - Serveur
  - Clé de sécurité Nitro (module de chiffrement) – emballage sur lequel figure « NSK » en rouge. Pour savoir comment trouver la clé NSK dans le colis, consultez la procédure suivante.
  - Kit d’installation du rack (2 rails intérieurs, 2 rails extérieurs et vis)
  - Brochure d’installation
  - Kit d’accessoires
    - Paire de câbles d’alimentation C13/14 – 3 mètres (10 pieds)
    - Câble de dérivation QSFP – 3 mètres (10 pieds)
    - Câble USB, micro-USB vers USB-C – 3 mètres (10 pieds)

- Cache de protection

Recherche de la clé NSK

La clé NSK se trouve à l'intérieur de la boîte A qui contient les accessoires du serveur.

> **Important**
>
> Pendant l'installation, n'utilisez pas la clé NSK pour détruire les données présentes sur le serveur.

Cette clé est nécessaire pour activer le serveur. Elle permet également de détruire les données présentes sur le serveur avant de le retourner. Lors de cette étape d'installation, ne tenez pas compte des instructions figurant sur le corps de la clé NSK ; elles visent à détruire les données.

Étape 3 : Monter le rack

Pour effectuer cette étape, vous devez fixer les rails intérieurs sur le serveur, les rails extérieurs sur le rack, puis monter le serveur sur le rack. Vous avez besoin ici d'un tournevis cruciforme.

Solutions de remplacement au montage du rack

Vous n'est pas tenu de monter le serveur dans un rack. Si vous ne montez pas le serveur dans un rack, tenez compte des informations suivantes :

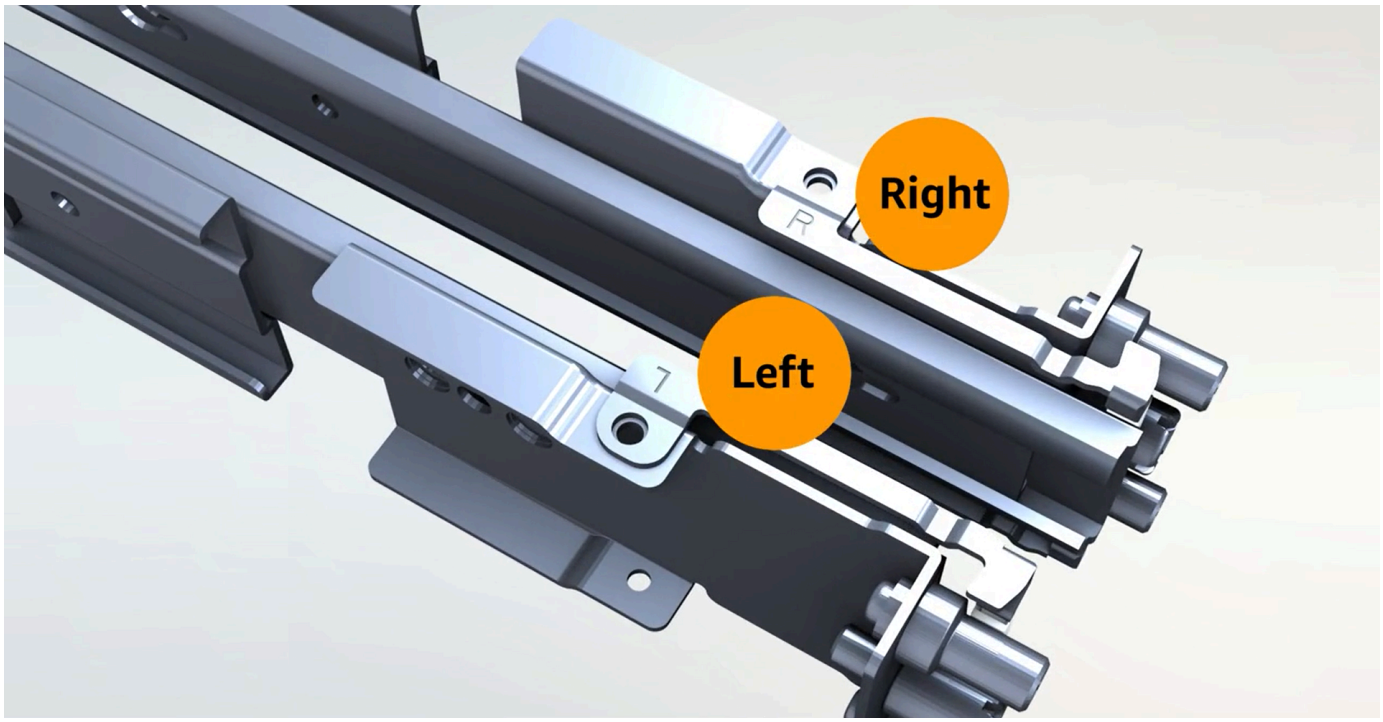
- Veillez à laisser un espace d'au moins 15 cm (6 pouces) entre le serveur et les murs devant et derrière le serveur pour favoriser l'évacuation de l'air chaud.
- Placez le serveur sur une surface stable exempte de risques mécaniques tels que l'humidité ou la chute d'objets.
- Pour utiliser les câbles réseau fournis avec le serveur, vous devez placer le serveur à moins de 3 m (10 pieds) de votre appareil réseau situé en amont.
- Suivez les directives locales en matière de renforcement et de collage parasismiques.

Identification des côtés et des extrémités

Pour faire la distinction entre la gauche et la droite, l'avant et l'arrière

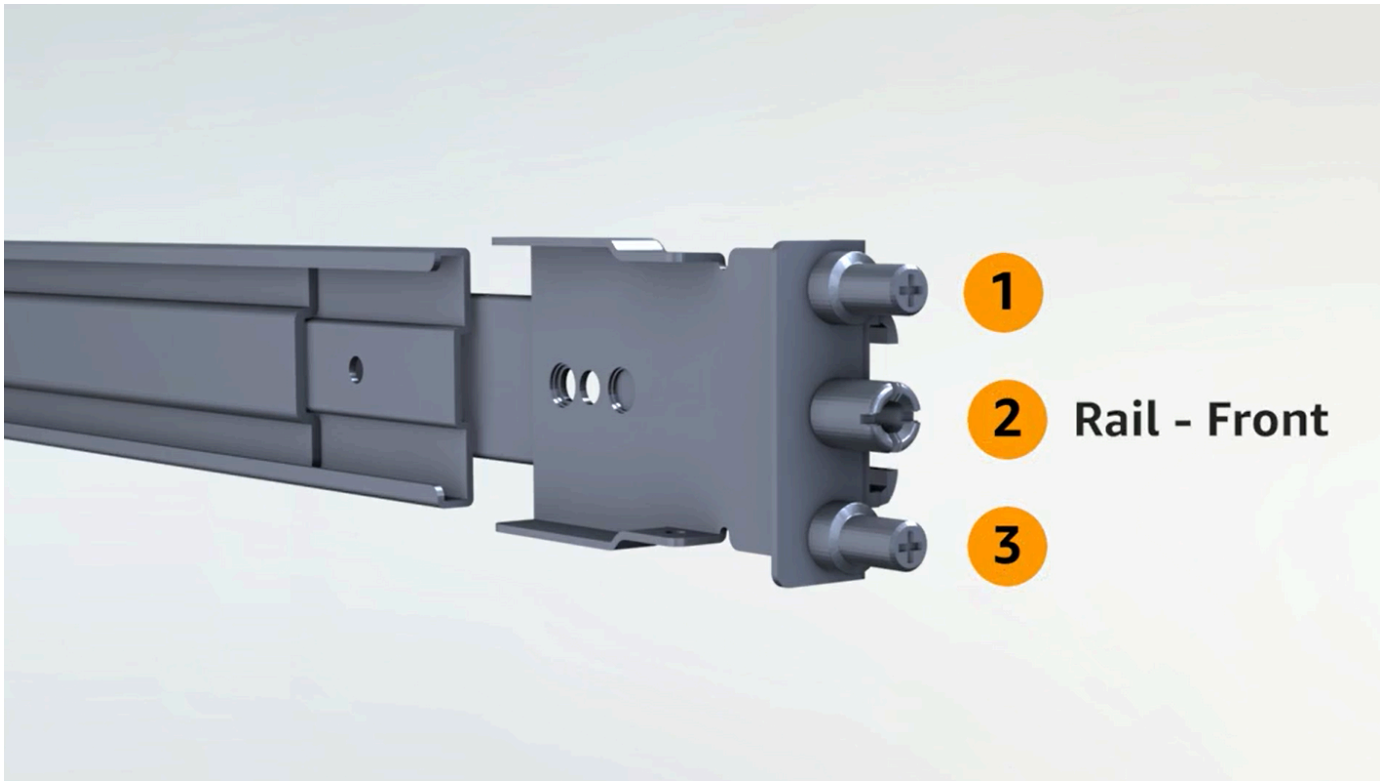
1. Localisez et ouvrez le carton contenant les rails du rack qui accompagnait le serveur.

2. Sur les rails, vous trouverez des marques identifiant les rails gauche et droit. Ces marques indiquent sur quel côté du serveur chaque rail doit être fixé.

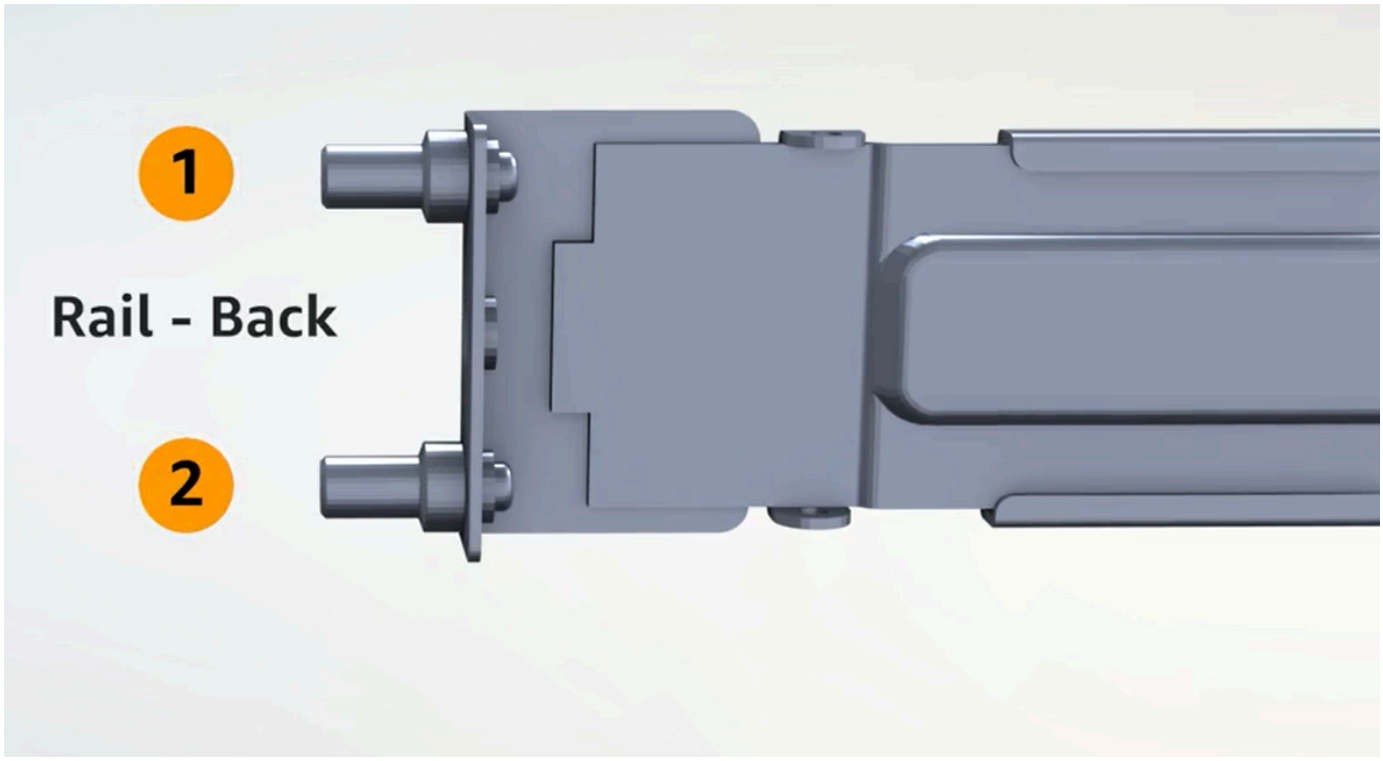


3. Examinez les tenons situés à chaque extrémité des rails pour déterminer leur positionnement, à l’avant ou à l’arrière.

   La partie avant compte trois tenons.



La partie arrière comporte deux tenons.



Fixation des rails intérieurs

Pour fixer les rails intérieurs sur le serveur

1. Détachez le rail intérieur du rail extérieur pour les deux rails. Vous disposez ainsi de quatre rails.
2. Fixez le rail intérieur droit sur le côté droit du serveur à l'aide d'une vis. Veillez à bien orienter le rail par rapport au serveur. Présentez la partie avant du rail à l'avant du serveur.
3. Fixez le rail intérieur gauche sur le côté gauche du serveur à l'aide d'une vis.

Fixation des rails extérieurs

Pour fixer les rails extérieurs sur le rack

1. Placez-vous devant le rack et utilisez le rail présentant la marque R sur le côté droit du rack. Fixez d'abord l'arrière du rail sur le rack, puis déployez le rail jusqu'en butée à l'avant du rack.

   > **Tip**
   >
   > Faites attention à l'orientation des rails. Utilisez éventuellement les entretoises incluses si nécessaire.

2. Répétez l'opération avec le rail gauche sur le côté gauche.

Montage du serveur

Pour monter le serveur dans le rack

- Faites glisser le serveur sur les rails extérieurs que vous avez installés sur le rack à l'étape précédente, puis fixez-le à l'avant avec les deux vis fournies.

  > **Tip**
  >
  > Cette opération doit se faire à deux personnes.

Étape 4 : Mettre sous tension

Pour effectuer la mise sous tension, branchez la clé NSK, connectez le serveur à une source d'alimentation, puis vérifiez que le serveur s'est allumé. Au moment de mettre le serveur sous tension, tenez compte des informations suivantes :

- Le serveur fonctionne avec une seule source d'alimentation, mais il est AWS recommandé d'utiliser deux sources d'alimentation pour assurer la redondance.
- Connectez les câbles d'alimentation avant de connecter les câbles réseau.
- Utilisez la paire de câbles d'alimentation à connecteur mâle C13 et à connecteur femelle C14 pour connecter le serveur à une alimentation sur le rack. Si vous n'utilisez pas le câble d'alimentation à connecteur femelle C14 pour connecter le serveur à une alimentation sur le rack, vous devez prévoir des adaptateurs pour les connecteurs femelles C14 qui se connectent à une source d'alimentation.

Branchement de la clé NSK

Vous devez brancher la clé NSK sur le serveur pour permettre le déchiffrement des données présentes sur ce dernier pendant son fonctionnement.

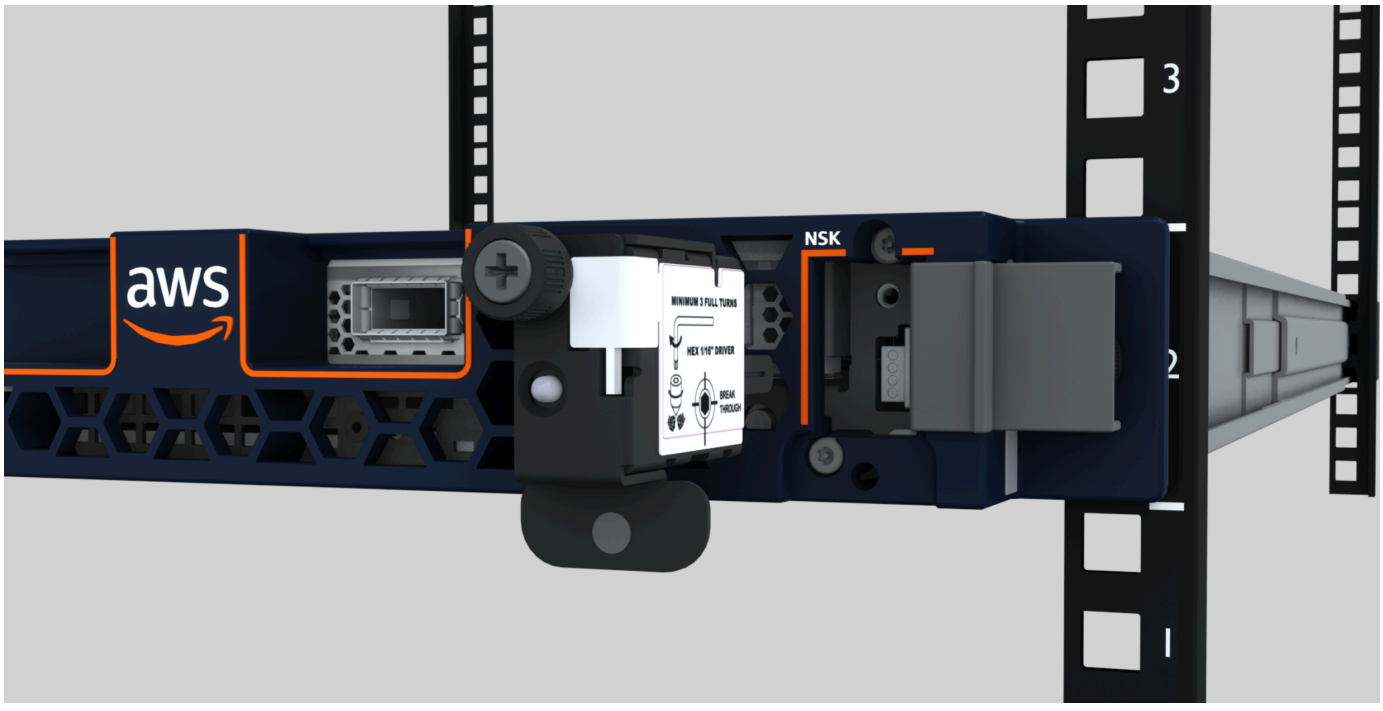
> **Important**
>
> - Sur le côté de la clé NSK, vous trouverez les instructions pour la détruire. Ne suivez pas ces instructions maintenant. Ces instructions ne sont à suivre qu'au moment de retourner le serveur à AWS, ceci afin de déchiqueter par chiffrement les données du serveur.
> - Si vous installez plusieurs serveurs en même temps, veillez à ne pas mélanger les clés NSK. Vous devez brancher la clé NSK sur le serveur qu'elle accompagnait. Si vous utilisez une clé NSK différente, le serveur ne démarrera pas.

Pour brancher la clé NSK

1. Sur le côté avant droit du serveur, ouvrez le compartiment NSK.

   L'image suivante montre une clé NSK branchée sur un serveur 2U.

L'image suivante montre une clé NSK branchée sur un serveur 1U.

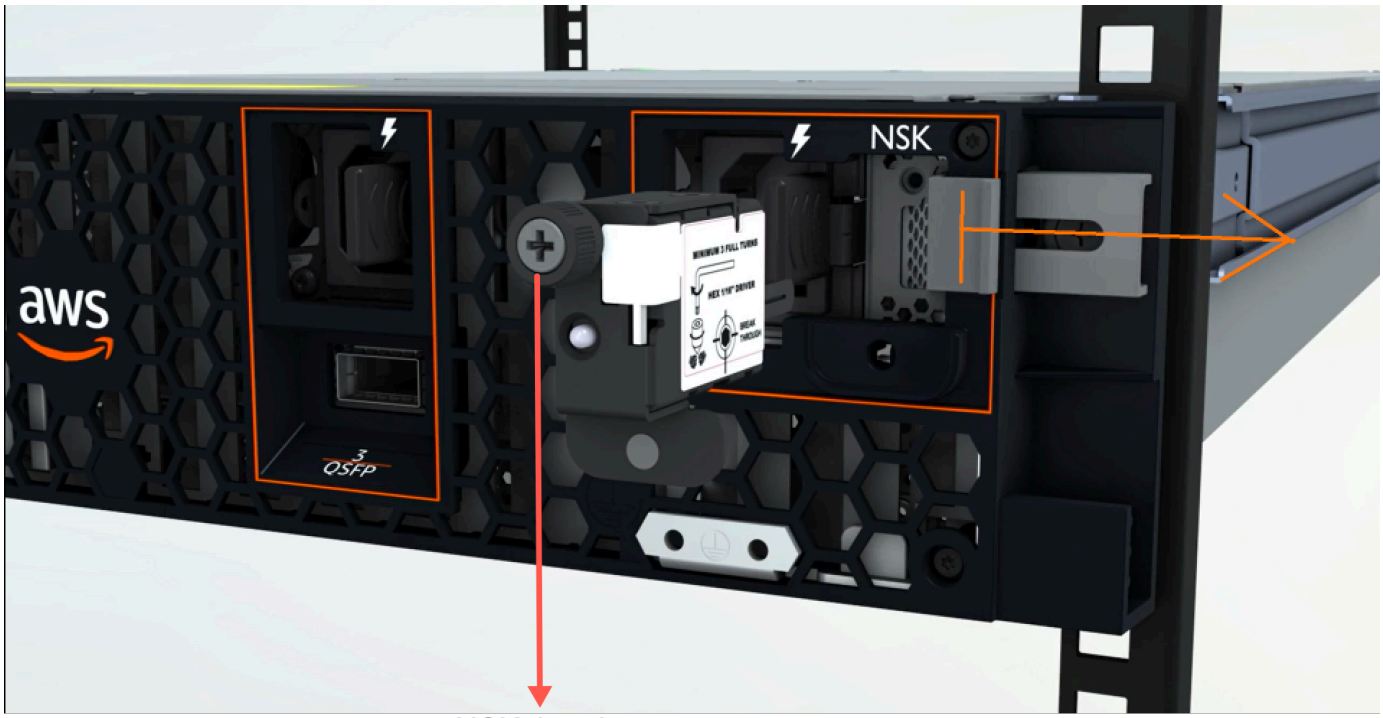


2. Vérifiez que le numéro de série (SN) indiqué sur la clé NSK correspond à celui inscrit sur la languette d'extraction du compartiment NSK du serveur.

L'image suivante montre le numéro SN sur la clé NSK et sur la languette d'extraction du panneau :

3. Insérez la clé NSK dans le logement prévu à cet effet.
4. Serrez correctement la vis de serrage à la main ou à l'aide d'un tournevis (0,7 Nm/0,52 lb-pi). Évitez d'utiliser une visseuse électrique, vous risqueriez de dépasser le couple de serrage préconisé et endommager la clé NSK.

L'image suivante montre l'emplacement de la vis de serrage.



NSK thumbscrew

L'image suivante montre le type de tournevis que vous pouvez utiliser pour attacher la clé NSK au serveur.

Mise sous tension

Pour connecter le serveur à l’alimentation

1. Localisez la paire de câbles d’alimentation C13/C14 fournis avec le serveur.
2. Connectez l’extrémité C14 des deux câbles à votre source d’alimentation.
3. Connectez l’extrémité C13 des deux câbles aux ports situés à l’avant du serveur.

Vérifiez l'alimentation du serveur

Pour vérifier que le serveur est alimenté

1. Vérifiez que vous entendez le serveur fonctionner.

   > **Tip**
   >
   > Le niveau de bruit diminue une fois que le serveur a terminé son provisionnement.

2. Vérifiez que les voyants d’alimentation LED situés au-dessus des ports d’alimentation sont allumés.

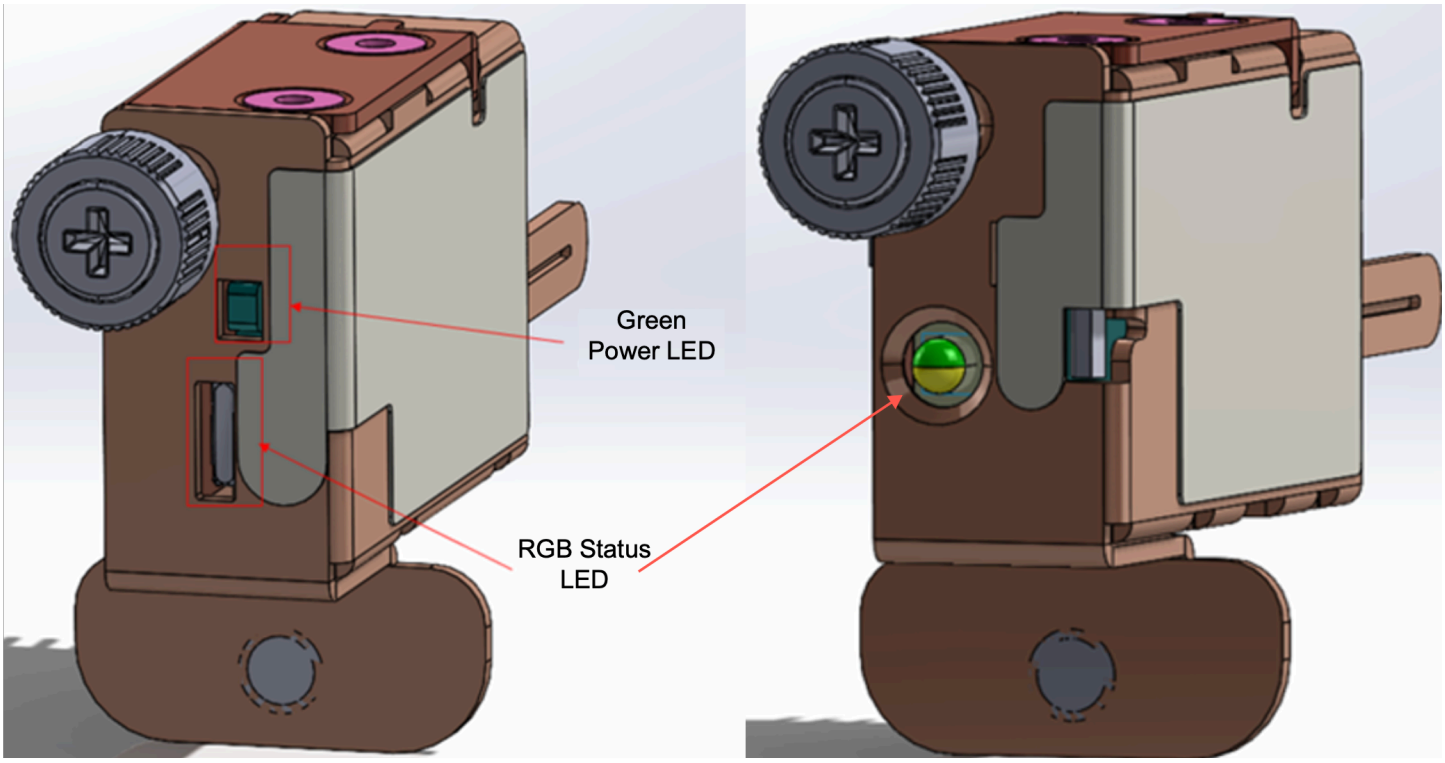
   L’image suivante montre les voyants d’alimentation LED sur un serveur 2U

L’image suivante montre les voyants d’alimentation LED sur un serveur 1U

Vérifiez le voyant d'alimentation de l'Atlas 3.0. NSK

AWS Outposts supporte deux versions de NSK : Atlas 2.0 et Atlas 3.0. Les deux versions NSK sont équipées d'une LED d'état RGB. De plus, l'Atlas 3.0 est doté d'une LED d'alimentation verte. Cette étape concerne uniquement l'Atlas 3.0 NSK.

L'image suivante montre l'emplacement des LED sur les NSK Atlas 2.0 et Atlas 3.0 :



Atlas 3.0 Atlas 2.0

Si vous possédez l'Atlas 2.0 NSK, passez à l'étape suivante, Étape 5 : Connecter le réseau car cette version du NSK possède uniquement le voyant d'état RGB, que vous devez vérifier une fois le serveur Outpost configuré et activé.

Si vous possédez l'Atlas 3.0 NSK, vérifiez le voyant d'alimentation vert :

- Si le voyant vert est allumé, le NSK est correctement connecté à l'hôte et est alimenté. Vous pouvez passer à l'étape suivante.
- Si le voyant vert est éteint, le NSK n'est pas correctement connecté à l'hôte et/ou n'est pas alimenté. Contacter AWS Support.

Étape 5 : Connecter le réseau

Pour configurer le réseau, connectez le serveur à votre appareil réseau situé en amont avec le câble réseau.

Au moment d'établir la connexion au réseau, tenez compte des informations suivantes :

- Le serveur a besoin de connexions pour deux types de trafic : le trafic de la liaison de service et le trafic de la liaison de l'interface de réseau local (LNI). Les instructions qui se trouvent dans la

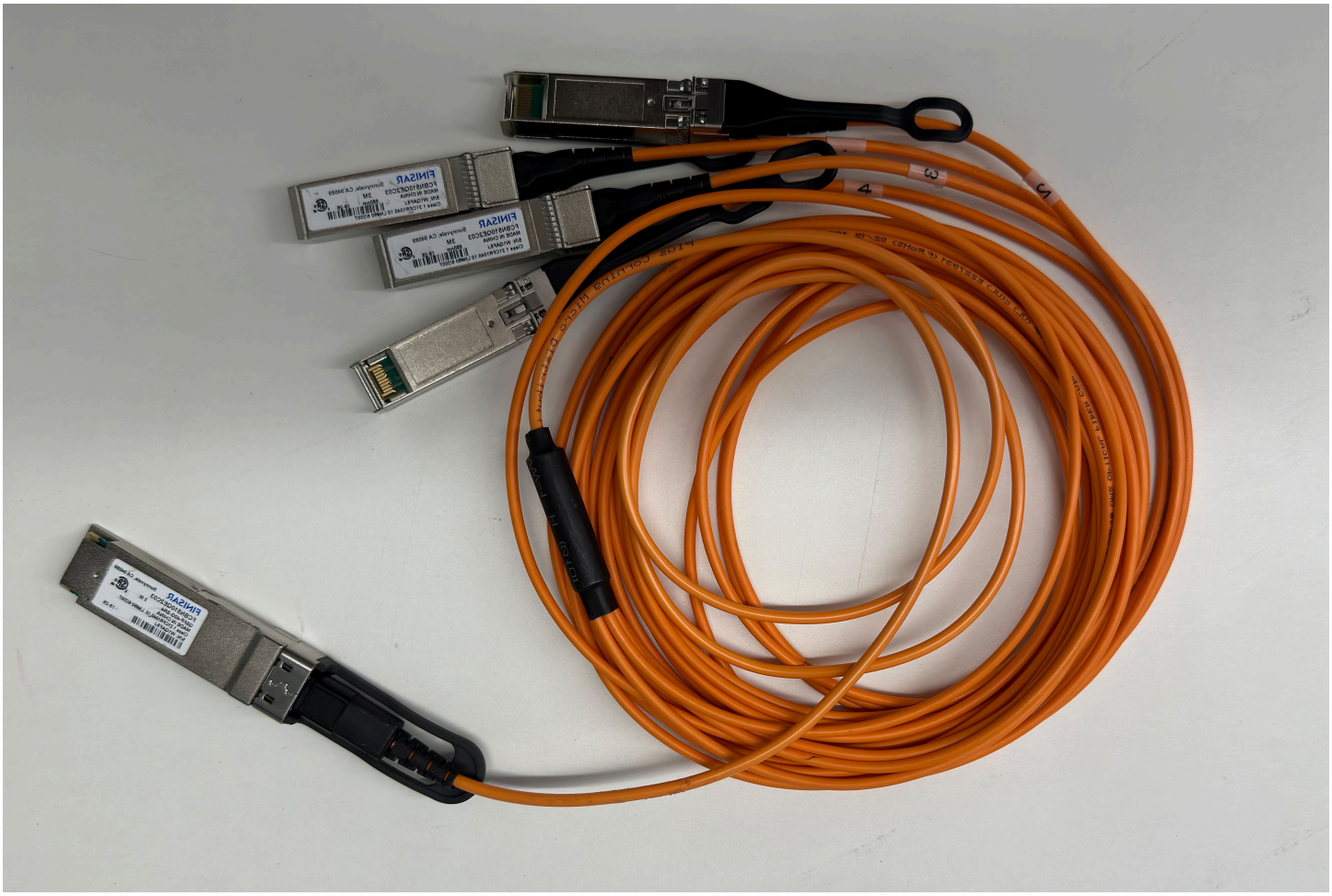
section suivante indiquent quels ports utiliser sur le serveur pour segmenter le trafic. Déterminez avec votre service informatique quel est le port de votre appareil réseau en amont qui doit être utilisé pour transporter chaque type de trafic.

- Vérifiez que le serveur est connecté à votre appareil réseau en amont et qu'une adresse IP lui a été attribuée. Pour plus d'informations, consultez Attribution d'adresse IP de serveur.
- La connexion optique d'un AWS Outposts serveur ne prend en charge que 10 Gbits et ne prend pas en charge la négociation automatique de la vitesse du port. Si le port hôte essaie de négocier la vitesse de port, par exemple entre 10 et 25 Gbits, vous risquez de rencontrer des problèmes. En pareil cas, voici ce que nous vous recommandons :
  - Définissez la vitesse du port du commutateur sur 10 Gbits.
  - Rapprochez-vous du fournisseur de votre commutateur pour trouver le moyen de prendre en charge une configuration statique.

Configuration du réseau QSFP

Avec le câble de dérivation QSFP, vous utilisez des dérivations pour segmenter le trafic.

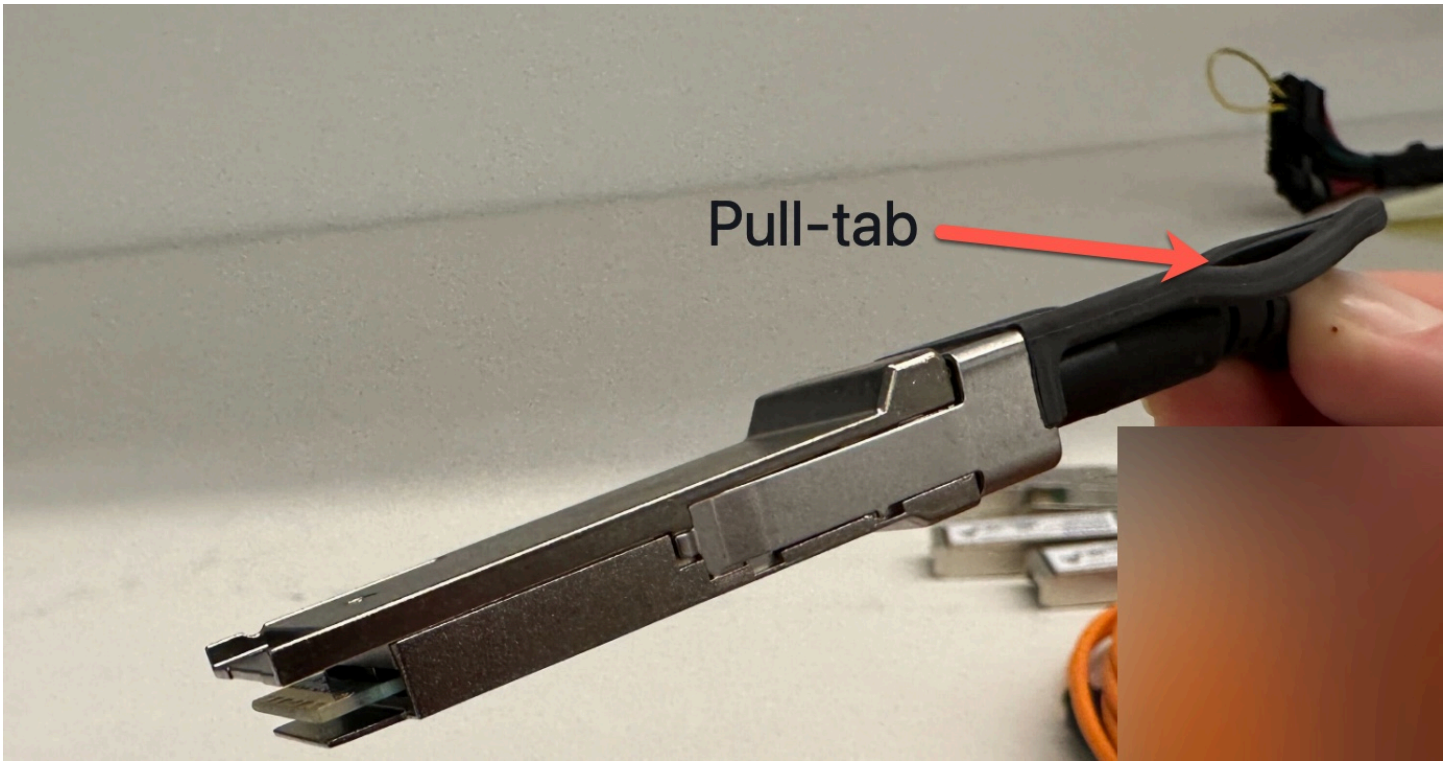
L'image suivante montre le câble de dérivation QSFP :



> **Note**
>
> AWS Outposts les serveurs disposent d'un port RJ45 physique à côté du port QSFP. Cependant, ce port RJ45 n'est activé pour aucun usage par le client. Si vous avez besoin d'une connectivité RJ45 1 GbE, utilisez le câble QSFP inclus pour connecter un SFP+ 10GBASE-X à un convertisseur de média RJ45 1 GbE.

L'une des extrémités du câble QSFP possède un connecteur unique. Connectez celle-ci au serveur.

L'image suivante montre l'extrémité du câble à connecteur unique :



L’autre extrémité du câble QSFP compte 4 câbles de dérivation étiquetés de 1 à 4. Utilisez le câble étiqueté 1 pour le trafic de la liaison LNI et le câble étiqueté 2 pour le trafic de la liaison de service.

L’image suivante montre l’extrémité du câble avec les 4 câbles de dérivation :

Pour connecter le serveur au réseau avec le câble de dérivation QSFP

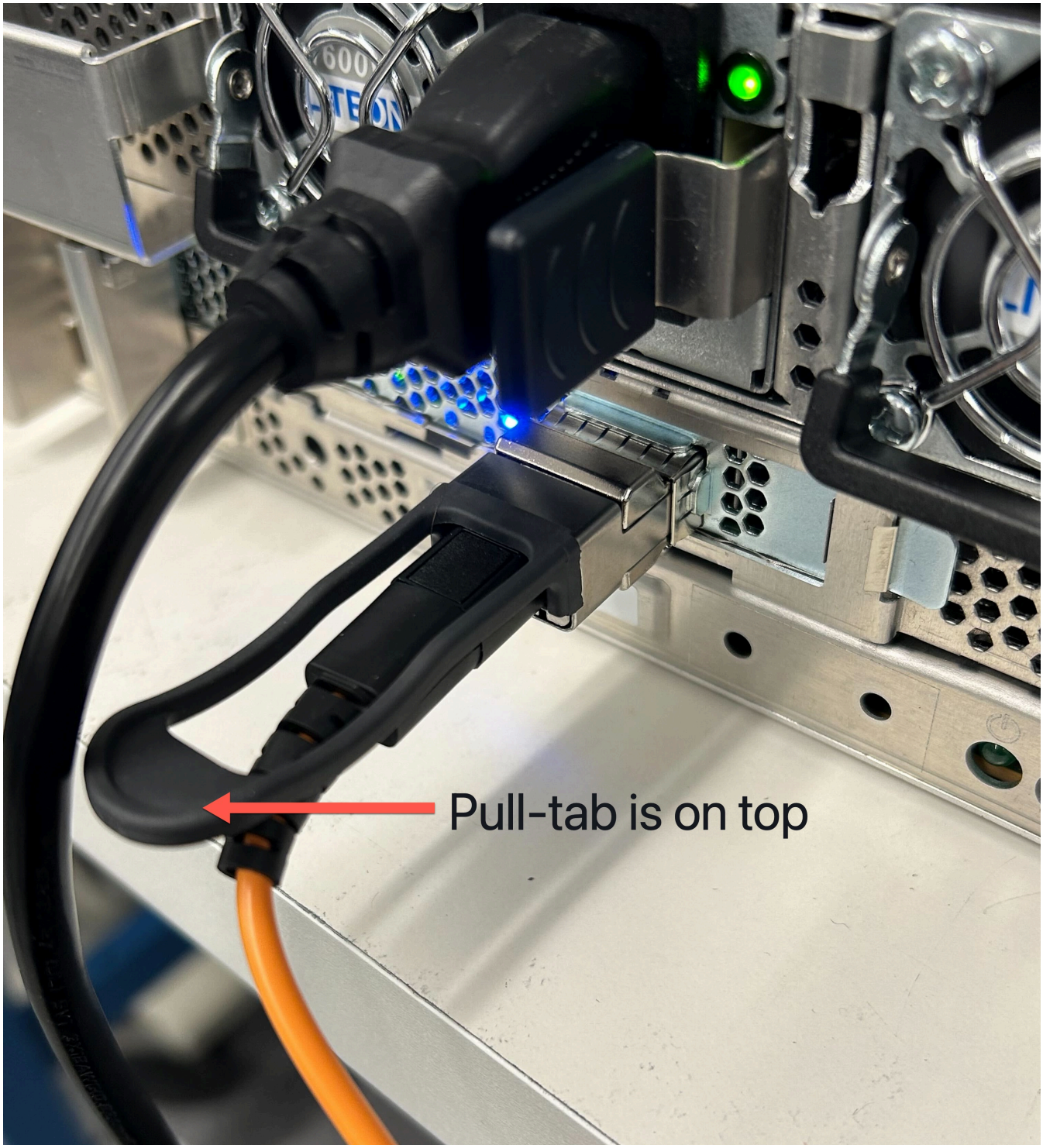
1. Localisez le câble de dérivation QSFP fourni avec le serveur.
2. Connectez l'extrémité unique du câble de dérivation QSFP au port QSFP du serveur.
    1. Localisez le port QSFP.

        L'image suivante montre l'emplacement du port QSFP sur le serveur 2U.

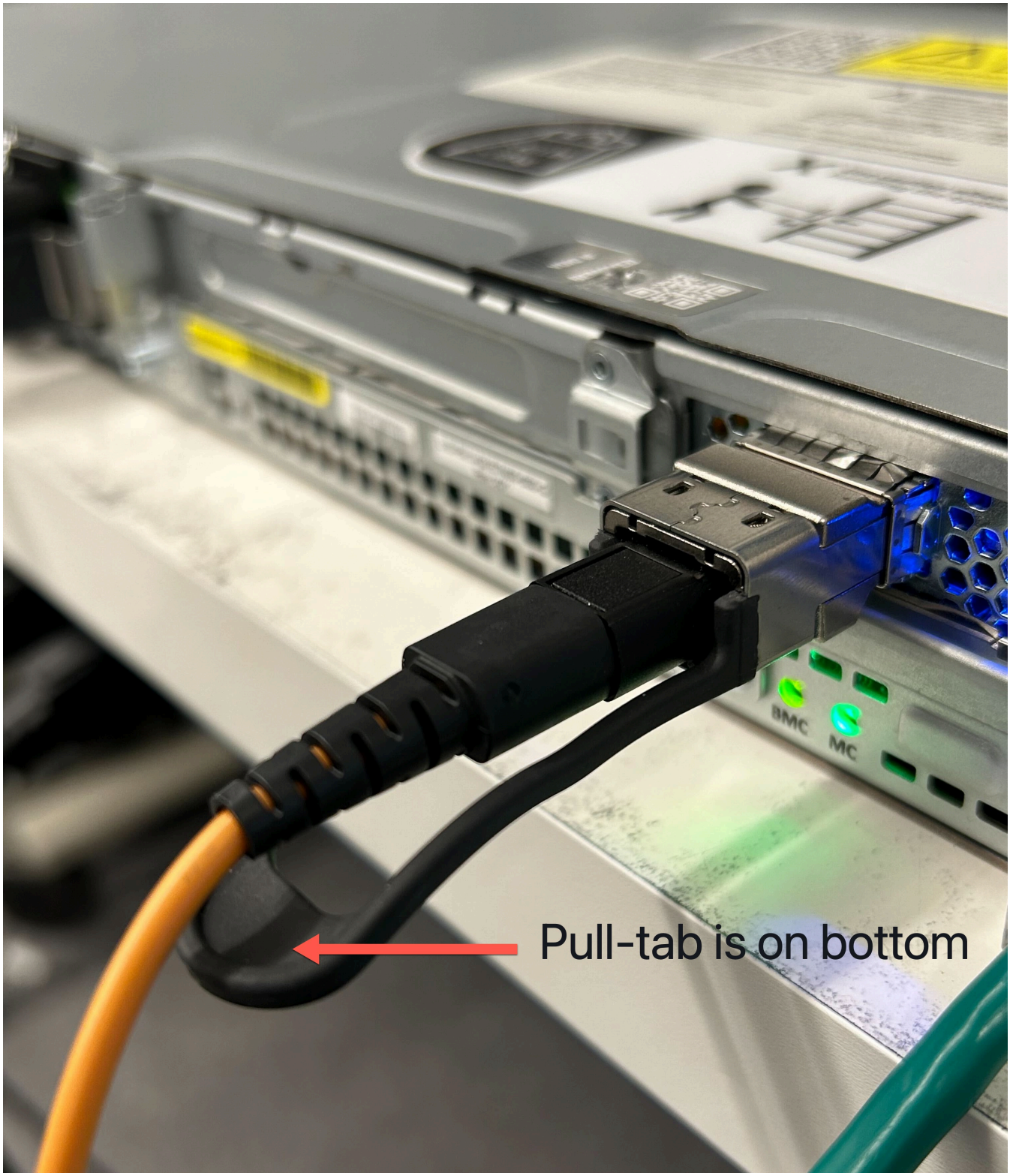
L'image suivante montre l'emplacement du port QSFP sur le serveur 1U.

2. Branchez le câble QSFP en veillant à ce que la languette soit bien orientée.

   Pour le serveur 2U, branchez le câble QSFP avec la languette en dessus comme sur l'image suivante.



Pour le serveur 1U, branchez le câble QSFP avec la languette en dessous comme sur l'image suivante.



3. Vous devez entendre ou sentir un clic lorsque vous branchez les câbles. Cela indique que les câbles sont bien branchés.

3. Connectez les dérivations 1 et 2 du câble QSFP à l'appareil réseau en amont.

> **Important**
>
> Les deux câbles suivants sont nécessaires au fonctionnement d'un serveur Outpost.
>
> - Utilisez le câble étiqueté 1 pour le trafic de la liaison LNI.
> - Utilisez le câble étiqueté 2 pour le trafic de la liaison de service.

Étape 6 : Autoriser le serveur

Pour autoriser le serveur, vous devez connecter votre ordinateur portable au serveur avec un câble USB, puis utiliser un protocole série basé sur des commandes pour tester la connexion et autoriser le serveur. Outre les informations d'identification IAM, vous avez besoin d'un câble USB, d'un ordinateur portable et d'un logiciel de terminal série, tel que PuTTY ou screen, pour effectuer ces étapes.

Si vous êtes équipé d'un téléphone ou d'une tablette Android disposant d'un connecteur USB-C ou micro-USB compatible USB On-The-Go (OTG), vous pouvez également utiliser l'application Outposts Server Activator pour vous faire guider tout au long le processus d'autorisation du serveur. Vous pouvez télécharger l'application depuis Google Play

Au moment d'autoriser le serveur, tenez compte des informations suivantes :

- Pour autoriser le serveur, vous ou la partie qui l'installe avez besoin d'informations d'identification IAM dans le fichier Compte AWS qui contient l'Outpost. Pour plus d'informations, consultez the section called "Étape 1 : Accorder des autorisations".
- Vous n'avez pas besoin de vous authentifier avec les informations d'identification IAM pour tester votre connexion.
- Pensez à tester la connexion avant d'utiliser la commande d'exportation pour définir les informations d'identification IAM en tant que variables d'environnement.
- Pour protéger votre compte, l'outil de configuration d'Outpost n'enregistre jamais vos informations d'identification IAM.
- Pour connecter votre ordinateur portable au serveur, branchez toujours le câble USB sur l'ordinateur portable avant de le brancher sur le serveur.

Tâches

- Connexion de l'ordinateur portable au serveur

- Création d'une connexion série au serveur
- Test de la connexion
- Autorisation du serveur
- Vérifiez les LED NSK

Connexion de l'ordinateur portable au serveur

Connectez le câble USB d'abord à votre ordinateur portable, puis au serveur. Le serveur comporte un circuit intégré USB qui crée un port série virtuel dont vous pouvez vous servir sur l'ordinateur portable. Vous pouvez utiliser ce port série virtuel pour vous connecter au serveur à l'aide d'un logiciel d'émulation de terminal série. Vous ne pouvez utiliser ce port série virtuel que pour exécuter les commandes de l'outil de configuration d'Outpost.

Pour connecter l'ordinateur portable au serveur

Branchez le câble USB d'abord sur votre ordinateur portable, puis sur le serveur.

> **Note**
>
> Le circuit intégré USB a besoin de pilotes pour créer le port série virtuel. Si les pilotes nécessaires ne sont pas déjà présents, votre système d'exploitation devrait les installer automatiquement. Pour télécharger et installer les pilotes, consultez les guides d'installation sur le site FTDI.

Création d'une connexion série au serveur

Vous trouverez dans cette section des instructions pour utiliser des programmes de terminal série très répandus, mais vous n'êtes pas tenu de les utiliser. Utilisez le programme de terminal série de votre choix avec une vitesse de connexion de `115200` bauds.

Exemples

- Connexion série Windows
- Connexion série Mac

Connexion série Windows

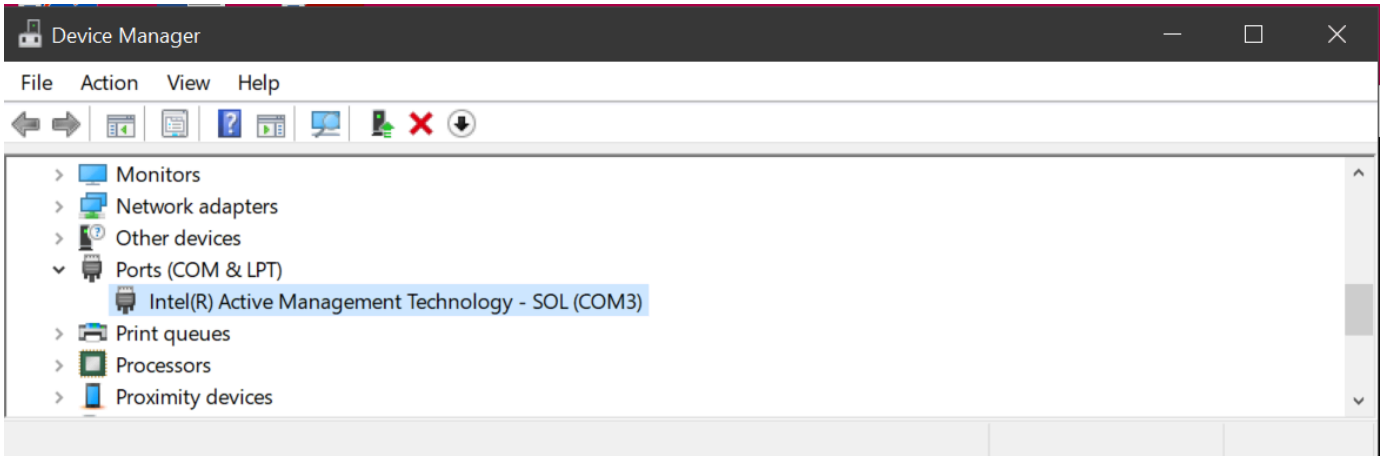
Les instructions suivantes s'appliquent à PuTTY sous Windows. PuTTY est gratuit, mais vous devrez peut-être le télécharger.

Téléchargement de PuTTY

Téléchargez et installez PuTTY à partir de la page de téléchargement PuTTY.

Pour créer un terminal série sous Windows à l'aide de PuTTY

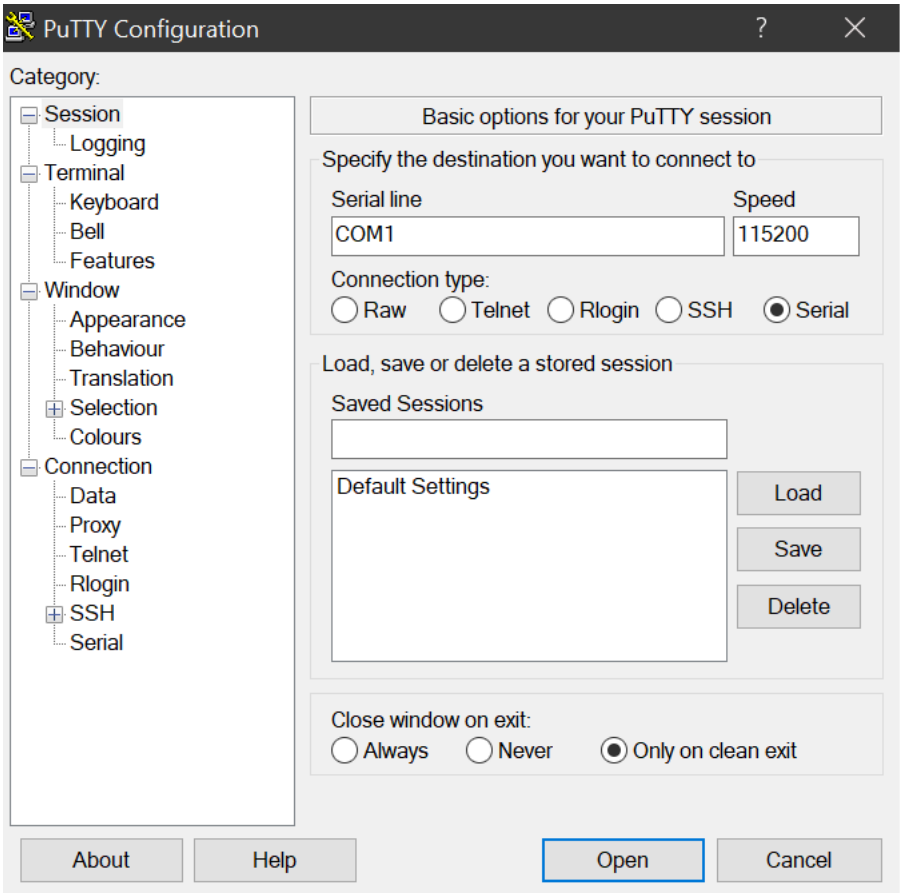
1. Branchez d'abord le câble USB sur votre ordinateur portable Windows, puis sur le serveur.
2. Sur le Bureau, cliquez avec le bouton droit sur Démarrer, puis choisissez Gestionnaire de périphériques.
3. Dans le Gestionnaire de périphériques, ouvrez Ports (COM et LPT) pour identifier le port COM de la connexion série USB. Vous voyez un nœud nommé Port série USB (COM **#**). La valeur du port COM dépend de votre matériel.



4. Dans PuTTY, dans Session, choisissez Serial pour Connection type, puis saisissez les informations suivantes :

   - Sous Serial line, saisissez le port COM# du Gestionnaire de périphériques.
   - Sous Speed, saisissez `115200`

   L'image suivante montre un exemple sur la page PuTTY Configuration :



5. Choisissez Ouvrir.

   Une fenêtre de console vide s'affiche. Après 1 à 2 minutes, vous voyez l'un des éléments suivants s'afficher :

   - `Please wait for the system to stabilize. This can take up to 900 seconds, so far x seconds have elapsed on this boot.`
   - L'invite `Outpost>`.

Connexion série Mac

Les instructions suivantes s'appliquent à screen sous macOS. L'outil screen est inclus dans le système d'exploitation.

Pour créer un terminal série sous macOS à l'aide de screen

1. Branchez d'abord le câble USB sur votre ordinateur portable Mac, puis sur le serveur.
2. Dans Terminal, listez `/dev` avec un filtre `*usb*` pour la sortie afin d'identifier le port série virtuel.

```
ls -ltr /dev/*usb*
```

Le périphérique série apparaît sous le nom `tty`. Par exemple, examinons l'exemple de sortie suivant résultant de la commande list précédente :

```
ls -ltr /dev/*usb*
crw-rw-rw-  1 root  wheel   21,   3 Feb  8 15:48 /dev/cu.usbserial-EXAMPLE1
crw-rw-rw-  1 root  wheel   21,   2 Feb  9 08:56 /dev/tty.usbserial-EXAMPLE1
```

3. Dans Terminal, utilisez screen avec le périphérique série et le débit en bauds de la connexion série pour configurer la connexion série. Dans la commande suivante, remplacez *EXAMPLE1* par la valeur de votre ordinateur portable.

```
screen /dev/tty.usbserial-EXAMPLE1 115200
```

Une fenêtre de console vide s'affiche. Après 1 à 2 minutes, vous voyez l'un des éléments suivants s'afficher :

- `Please wait for the system to stabilize. This can take up to 900 seconds, so far x seconds have elapsed on this boot.`
- L'invite `Outpost>`.

Test de la connexion

Cette section explique comment utiliser l'outil de configuration d'Outpost pour tester la connexion. Vous n'avez pas besoin d'informations d'identification IAM pour tester la connexion. Votre connexion doit pouvoir résoudre le DNS pour accéder à la Région AWS.

1. Tester les liaisons et recueillir les informations sur la connexion
2. Tester le résolveur DNS
3. Testez l'accès au Région AWS

Pour tester les liaisons

1. Branchez le câble USB d'abord sur votre ordinateur portable, puis sur le serveur.

2. Utilisez un programme de terminal série, tel que PuTTY ou screen, pour vous connecter au serveur. Pour plus d'informations, consultez the section called "Création d'une connexion série au serveur".
3. Appuyez sur Enter pour accéder à l'invite de commande de l'outil de configuration d'Outpost.

```
Outpost>
```

> **Note**
>
> Si, après la mise sous tension, un voyant rouge reste allumé à l'intérieur du châssis du serveur sur le côté gauche et que vous ne parvenez pas à vous connecter à l'outil de configuration d'Outpost, vous avez peut-être besoin de mettre le serveur hors tension et d'attendre qu'il se décharge avant de continuer. Pour décharger le serveur, déconnectez tous les câbles réseau et d'alimentation, attendez cinq minutes, puis rebranchez et reconnectez le réseau.

4. Utilisez describe-links pour renvoyer les informations sur les liaisons réseau du serveur. Les serveurs Outpost doivent disposer d'une liaison de service et d'une liaison d'interface de réseau local (LNI).

```
Outpost>describe-links
---
service_link_connected: True
local_link_connected: False
links:
-
  name: local_link
  connected: False
  mac: 00:00:00:00:00:00
-
  name: service_link
  connected: True
  mac: 0A:DC:FE:D7:8E:1F
checksum: 0x46FDC542
```

Si vous obtenez `connected: False` pour l'une ou l'autre des liaisons, résolvez les problèmes liés à la connexion réseau au niveau du matériel.

5. Utilisez describe-ip pour renvoyer le statut d'affectation d'adresse IP et la configuration de la liaison de service.

```
Outpost>describe-ip
---
links:
-
  name: service_link
  configured: True
  ip: 192.168.0.0
  netmask: 255.255.0.0
  gateway: 192.168.1.1
  dns: [ "192.168.1.1" ]
  ntp: [ ]
checksum: 0x8411B47C
```

Il est possible que la valeur NTP soit manquante, car NTP est facultatif dans un jeu d'options DHCP. Il ne devrait pas vous manquer d'autres valeurs.

Pour tester le DNS

1. Branchez le câble USB d'abord sur votre ordinateur portable, puis sur le serveur.
2. Utilisez un programme de terminal série, tel que PuTTY ou screen, pour vous connecter au serveur. Pour plus d'informations, consultez the section called "Création d'une connexion série au serveur".
3. Appuyez sur Enter pour accéder à l'invite de commande de l'outil de configuration d'Outpost.

```
Outpost>
```

> **Note**
>
> Si, après la mise sous tension, un voyant rouge reste allumé à l'intérieur du châssis du serveur sur le côté gauche et que vous ne parvenez pas à vous connecter à l'outil de configuration d'Outpost, vous avez peut-être besoin de mettre le serveur hors tension et d'attendre qu'il se décharge avant de continuer. Pour décharger le serveur, déconnectez tous les câbles réseau et d'alimentation, attendez cinq minutes, puis rebranchez et reconnectez le réseau.

4. Utilisez export pour entrer la région parente du serveur Outpost comme valeur de AWS_DEFAULT_REGION.

   AWS_DEFAULT_REGION=*Région*

   ```
   Outpost>export AWS_DEFAULT_REGION=us-west-2

   result: OK
   checksum: 0xB2A945RE
   ```

   - N'insérez pas d'espace avant ou après le signe égal (=).
   - Aucune valeur d'environnement n'est enregistrée. Vous devez effectuer une exportation Région AWS chaque fois que vous exécutez l'outil de configuration Outpost.
   - Si vous confiez l'installation du serveur à un tiers, vous devez lui fournir la région parente.

5. Utilisez describe-resolve pour déterminer si le serveur Outpost peut accéder à un résolveur DNS et résoudre l'adresse IP du point de terminaison de configuration d'Outpost de la région. Nécessite au moins une liaison avec une configuration IP.

   ```
   Outpost>describe-resolve
   ---
   dns_responding: True
   dns_resolving: True
   dns: [ "198.xx.xxx.xx", "198.xx.xxx.xx" ]
   query: outposts.us-west-2.amazonaws.com
   records: [ "18.xxx.xx.xxx", "44.xxx.xxx.xxx", "44.xxx.xxx.xxx" ]
   checksum: 0xB6A961CE
   ```

Pour tester l'accès à Régions AWS

1. Branchez le câble USB d'abord sur votre ordinateur portable, puis sur le serveur.
2. Utilisez un programme de terminal série, tel que PuTTY ou screen, pour vous connecter au serveur. Pour plus d'informations, consultez the section called "Création d'une connexion série au serveur".
3. Appuyez sur Enter pour accéder à l'invite de commande de l'outil de configuration d'Outpost.

   ```
   Outpost>
   ```

> **Note**
>
> Si, après la mise sous tension, un voyant rouge reste allumé à l'intérieur du châssis du serveur sur le côté gauche et que vous ne parvenez pas à vous connecter à l'outil de configuration d'Outpost, vous avez peut-être besoin de mettre le serveur hors tension et d'attendre qu'il se décharge avant de continuer. Pour décharger le serveur, déconnectez tous les câbles réseau et d'alimentation, attendez cinq minutes, puis rebranchez et reconnectez le réseau.

4. Utilisez export pour entrer la région parente du serveur Outpost comme valeur de `AWS_DEFAULT_REGION`.

   `AWS_DEFAULT_REGION=`*`Région`*

   ```
   Outpost>export AWS_DEFAULT_REGION=us-west-2

   result: OK
   checksum: 0xB2A945RE
   ```

   - N'insérez pas d'espace avant ou après le signe égal (=).
   - Aucune valeur d'environnement n'est enregistrée. Vous devez effectuer une exportation Région AWS chaque fois que vous exécutez l'outil de configuration Outpost.
   - Si vous confiez l'installation du serveur à un tiers, vous devez lui fournir la région parente.

5. Utilisez describe-reachability pour déterminer si le serveur Outpost peut accéder au point de terminaison de configuration d'Outpost de la région. Nécessite une configuration DNS fonctionnelle, ce que vous pouvez déterminer à l'aide de describe-resolve.

   ```
   Outpost>describe-reachability
   ---
   is_reachable: True
   src_ip: 10.0.0.0
   dst_ip: 54.xx.x.xx
   dst_port: xxx
   checksum: 0xCB506615
   ```

   - `is_reachable` indique le résultat du test
   - `src_ip` est l'adresse IP du serveur

- `dst_ip` est l'adresse IP du point de terminaison de configuration d'Outpost de la région
- `dst_port` est le port du serveur utilisé pour se connecter à `dst_ip`

Autorisation du serveur

Cette section explique comment utiliser l'outil de configuration d'Outpost et les informations d'identification IAM du compte AWS qui contient l'Outpost pour autoriser le serveur.

Pour autoriser le serveur

1. Branchez le câble USB d'abord sur votre ordinateur portable, puis sur le serveur.
2. Utilisez un programme de terminal série, tel que PuTTY ou screen, pour vous connecter au serveur. Pour plus d'informations, consultez the section called "Création d'une connexion série au serveur".
3. Appuyez sur Enter pour accéder à l'invite de commande de l'outil de configuration d'Outpost.

   ```
   Outpost>
   ```

   > **Note**
   >
   > Si, après la mise sous tension, un voyant rouge reste allumé à l'intérieur du châssis du serveur sur le côté gauche et que vous ne parvenez pas à vous connecter à l'outil de configuration d'Outpost, vous avez peut-être besoin de mettre le serveur hors tension et d'attendre qu'il se décharge avant de continuer. Pour décharger le serveur, déconnectez tous les câbles réseau et d'alimentation, attendez cinq minutes, puis rebranchez et reconnectez le réseau.

4. Utilisez export pour saisir vos informations d'identification IAM dans l'outil de configuration d'Outpost. Si vous confiez l'installation du serveur à un tiers, vous devez lui fournir les informations d'identification IAM.

   Pour l'authentification, vous devez exporter les quatre variables suivantes. Exportez une variable à la fois. N'insérez pas d'espace avant ou après le signe égal (=).

   - `AWS_ACCESS_KEY_ID=`*`access-key-id`*
   - `AWS_SECRET_ACCESS_KEY=`*`secret-access-key`*
   - `AWS_SESSION_TOKEN=`*`session-token`*

- Utilisez la AWS CLI `GetSessionToken` commande pour obtenir le`AWS_SESSION_TOKEN`. Pour plus d'informations, consultez get-session-tokenle manuel de référence des AWS CLI commandes.

  > **Note**
  >
  > Vous devez avoir le rôle AWSOutpostsAuthorizeServerPolicyattaché à votre rôle IAM pour obtenir le`AWS_SESSION_TOKEN`.

- Pour l'installer AWS CLI, consultez la section Installation ou mise à jour de la dernière version de l'interface de ligne de commande AWS dans le guide de AWS CLI l'utilisateur de la version 2.

- `AWS_DEFAULT_REGION=`*`Région`*

  Utilisez la région parente du serveur Outpost comme valeur de `AWS_DEFAULT_REGION`. Si vous confiez l'installation du serveur à un tiers, vous devez lui fournir la région parente.

La sortie présentée dans les exemples suivants montre que les exportations ont bien abouti.

```
Outpost>export AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE

result: OK
checksum: example-checksum
```

```
Outpost>export AWS_SECRET_ACCESS_KEY=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY

result: OK
checksum: example-checksum
```

```
Outpost>export AWS_SESSION_TOKEN=MIICiTCCAfICCQD6m7oRw0uXOjANBgk
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
```

```
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=

result: OK
checksum: example-checksum
```

```
Outpost>export AWS_DEFAULT_REGION=us-west-2

result: OK
checksum: example-checksum
```

5. Utilisez start-connection pour créer une connexion sécurisée à la région.

   La sortie présentée dans l'exemple suivant montre que la connexion a bien démarré.

```
Outpost>start-connection

is_started: True
asset_id: example-asset-id
connection_id: example-connection-id
timestamp: 2021-10-01T23:30:26Z
checksum: example-checksum
```

6. Attendez environ 5 minutes.
7. Utilisez get-connection pour vérifier si la connexion à la région a bien été établie.

   La sortie présentée dans l'exemple suivant indique une connexion réussie.

```
Outpost>get-connection


---
keys_exchanged: True
connection_established: True
exchange_active: False
primary_peer: xx.xx.xx.xx:xxx
primary_status: success
primary_connection_id: a1b2c3d4567890abcdefEXAMPLE11111
primary_handshake_age: 1111111111
primary_server_public_key: AKIAIOSFODNN7EXAMPLE
```

```
primary_client_public_key: AKIAI44QH8DHBEXAMPLE
primary_server_endpoint: xx.xx.xx.xx:xxx
secondary_peer: xx.xxx.xx.xxx:xxx
secondary_status: success
secondary_connection_id: a1b2c3d4567890abcdefEXAMPLE22222
secondary_handshake_age: 1111111111
secondary_server_public_key: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
secondary_client_public_key: je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY
secondary_server_endpoint: xx.xxx.xx.xxx:xxx
timestamp: 2023-02-22T22:19:28Z
checksum: 0x83FA0123
```

Dès lors que la valeur de `keys_exchanged` et de `connection_established` passe à `True`, le serveur Outpost est automatiquement provisionné et mis à jour avec le logiciel et la configuration les plus récents.

> **Note**
>
> Notez les points suivants concernant le processus de provisionnement :
>
> - Une fois l'activation terminée, un délai d'attente de 10 heures peut être nécessaire avant de pouvoir utiliser le serveur Outpost.
> - L'alimentation et le réseau du serveur Outpost doivent rester connectés et stables pendant ce processus.
> - Il est normal que la liaison de service fluctue au cours de ce processus.
> - Si `exchange_active` a la valeur `True`, la connexion n'est pas encore établie. Réessayez dans les 5 minutes.
> - Si `keys_exchanged` ou `connection_established` ont la valeur `False`, et si `exchange_active` a la valeur `True`, la connexion n'est toujours pas établie. Réessayez dans les 5 minutes.
> - Si `keys_exchanged` ou `connection_established` ont la valeur `False` même après 1 heure, contactez le centre AWS Support.
> - Si le message `primary_status: No such asset id found.` apparaît, confirmez les points suivants :
>   - Vous avez indiqué la bonne région.
>   - Vous utilisez le même compte que celui utilisé pour commander le serveur Outpost.

Si la région est correcte et que vous utilisez le même compte que celui utilisé pour commander le serveur Outpost, contactez le AWS Support centre d'appels.

- La valeur de l'attribut `LifeCycleStatus` de l'Outpost passe de `Provisioning` à `Active`. Vous recevez ensuite un e-mail vous informant que votre serveur Outpost est provisionné et activé.
- Vous n'avez pas besoin de réautoriser le serveur Outposts une fois qu'il est activé.

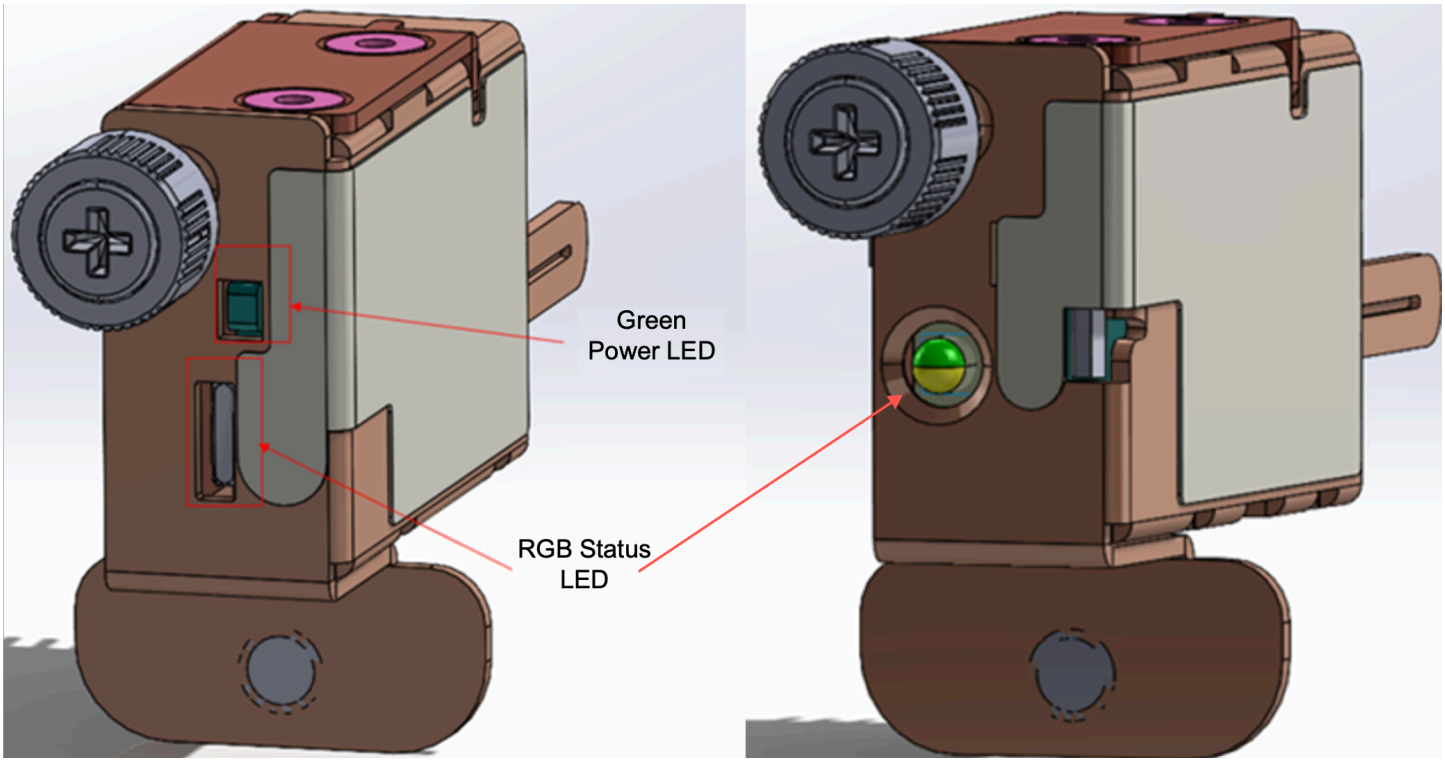
8. Après avoir établi la connexion, vous pouvez déconnecter votre ordinateur portable du serveur.

Vérifiez les LED NSK

Une fois le processus de provisionnement terminé, vérifiez les voyants NSK.

AWS Outposts supporte deux versions de NSK : Atlas 2.0 et Atlas 3.0. Les deux versions NSK sont équipées d'une LED d'état RGB. De plus, l'Atlas 3.0 est doté d'une LED d'alimentation verte.

L'image suivante montre l'emplacement des LED sur les modèles Atlas 2.0 et Atlas 3.0 :



Atlas 3.0 Atlas 2.0

Pour vérifier les voyants d'état et d'alimentation du NSK

1. Vérifiez la couleur du voyant d'état RGB. Si la couleur est verte, le NSK est sain. Si la couleur n'est pas verte, contactez AWS Support.
2. Si vous possédez un Atlas 3.0 NSK, vérifiez le voyant d'alimentation vert. Si le voyant vert est allumé, le NSK est correctement connecté à l'hôte et est alimenté. Si le voyant vert n'est pas allumé, contactez AWS Support.

Informations de référence sur les commandes de l'outil de configuration d'Outpost

L'outil de configuration d'Outpost propose les commandes suivantes.

Commandes

Export

export

Utilisez export pour définir les informations d'identification IAM en tant que variables d'environnement.

Syntaxe

```
Outpost>export variable=value
```

export accepte la déclaration d'affectation de variable.

Elle doit se présenter sous la forme suivante : *variable*=*value*

Pour l'authentification, vous devez exporter les quatre variables suivantes. Exportez une variable à la fois. N'insérez pas d'espace avant ou après le signe égal (=).

- AWS_ACCESS_KEY_ID=*access-key-id*
- AWS_SECRET_ACCESS_KEY=*secret-access-key*
- AWS_SESSION_TOKEN=*session-token*
- AWS_DEFAULT_REGION=*Région*

  Utilisez la région parente du serveur Outpost comme valeur de AWS_DEFAULT_REGION.

Example : informations d'identification correctement importées

```
Outpost>export AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE

result: OK
checksum: example-checksum
```

```
Outpost>export AWS_SECRET_ACCESS_KEY=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY

result: OK
checksum: example-checksum
```

```
Outpost>export AWS_SESSION_TOKEN=MIICiTCCAfICCQD6m7oRw0uXOjANBgk
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=

result: OK
```

```
checksum: example-checksum
```

```
Outpost>export AWS_DEFAULT_REGION=us-west-2

result: OK
checksum: example-checksum
```

Echo

echo

Utilisez echo pour afficher la valeur que vous avez définie pour une variable à l'aide de la commande export.

Syntaxe

```
Outpost>echo $variable-name
```

La valeur de *variable-name* peut être l'une des suivantes :

- AWS_ACCESS_KEY_ID
- AWS_SECRET_ACCESS_KEY
- AWS_SESSION_TOKEN
- AWS_DEFAULT_REGION

Example : réussite

```
Outpost>export AWS_DEFAULT_REGION=us-west-2

result: OK
checksum: example-checksum

---

Outpost>echo $AWS_DEFAULT_REGION

variable name: AWS_DEFAULT_REGION
variable value: us-west-2
checksum: example-checksum
```

Example : échec car la valeur de la variable n'a pas été définie avec la commande export

```
Outpost> echo $AWS_ACCESS_KEY_ID

error_type: execution_error
error_attributes:
  AWS_ACCESS_KEY_ID: no value set
error_message: No value set for AWS_ACCESS_KEY_ID using export.
checksum: example-checksum
```

Example : échec car le nom de la variable n'est pas valide

```
Oupost>echo $foo

error_type: invalid_argument
error_attributes:
  foo: invalid variable name
error_message: Variables can only be AWS credentials.
checksum: example-checksum
```

Example : échec en raison d'un problème de syntaxe

```
Outpost>echo AWS_SECRET_ACCESS_KEY

error_type: invalid_argument
error_attributes:
  AWS_SECRET_ACCESS_KEY: not a variable
error_message: Expecting $ before variable name.
checksum: example-checksum
```

Description des liaisons

describe-links

Utilisez describe-links pour renvoyer les informations sur les liaisons réseau du serveur. Les serveurs Outpost doivent disposer d'une liaison de service et d'une liaison d'interface de réseau local (LNI).

Syntaxe

```
Outpost>describe-links
```

describe-links n'accepte pas d'arguments.

Description d'adresse IP

describe-ip

Utilisez describe-ip pour renvoyer le statut d'affectation d'adresse IP et la configuration de chaque liaison connectée.

Syntaxe

```
Outpost>describe-ip
```

describe-ip n'accepte pas d'arguments.

Description de la résolution

describe-resolve

Utilisez describe-resolve pour déterminer si le serveur Outpost peut accéder à un résolveur DNS et résoudre l'adresse IP du point de terminaison de configuration d'Outpost de la région. Nécessite au moins une liaison avec une configuration IP.

Syntaxe

```
Outpost>describe-resolve
```

describe-resolve n'accepte pas d'arguments.

Description de l'accessibilité

describe-reachability

Utilisez describe-reachability pour déterminer si le serveur Outpost peut accéder au point de terminaison de configuration d'Outpost de la région. Nécessite une configuration DNS fonctionnelle, ce que vous pouvez déterminer à l'aide de describe-resolve.

Syntaxe

```
Outpost>describe-reachability
```

describe-reachability n'accepte pas d'arguments.

Démarrage de la connexion

start-connection

Utilisez start-connection pour initier une connexion avec le service Outpost de la région. Cette commande tire les informations d'identification Signature Version 4 (SigV4) des variables d'environnement que vous avez chargées avec export. La connexion s'exécute de manière asynchrone et renvoie immédiatement. Pour vérifier le statut de la connexion, utilisez get-connection.

Syntaxe

```
Outpost>start-connection [0|1]
```

start-connection utilise un index de connexion facultatif pour initier une autre connexion. Seules les valeurs `0` et 1 sont valides.

Example : connexion démarrée

```
Outpost>start-connection

is_started: True
asset_id: example-asset-id
connection_id: example-connecdtion-id
timestamp: 2021-10-01T23:30:26Z
checksum: example-checksum
```

Obtention d'une connexion

get-connection

Utilisez get-connection pour renvoyer le statut de la connexion.

Syntaxe

```
Outpost>get-connection [0|1]
```

get-connection utilise un index de connexion facultatif pour renvoyer le statut d'une autre connexion. Seules les valeurs `0` et 1 sont valides.

Example : connexion réussie

```
Outpost>get-connection


---
keys_exchanged: True
connection_established: True
exchange_active: False
primary_peer: xx.xx.xx.xx:xxx
primary_status: success
primary_connection_id: a1b2c3d4567890abcdefEXAMPLE11111
primary_handshake_age: 1111111111
primary_server_public_key: AKIAIOSFODNN7EXAMPLE
primary_client_public_key: AKIAI44QH8DHBEXAMPLE
primary_server_endpoint: xx.xx.xx.xx:xxx
secondary_peer: xx.xxx.xx.xxx:xxx
secondary_status: success
secondary_connection_id: a1b2c3d4567890abcdefEXAMPLE22222
secondary_handshake_age: 1111111111
secondary_server_public_key: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
secondary_client_public_key: je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY
secondary_server_endpoint: xx.xxx.xx.xxx:xxx
timestamp: 2023-02-22T22:19:28Z
checksum: 0x83FA0123
```

Remarque :

- Si `exchange_active` a la valeur `True`, la connexion n'est pas encore établie. Réessayez dans les 5 minutes.
- Si `keys_exchanged` ou `connection_established` ont la valeur `False`, et si `exchange_active` a la valeur `True`, la connexion n'est toujours pas établie. Réessayez dans les 5 minutes.

Si le problème persiste après 1 heure, contactez le centre AWS Support.

Lancez une instance sur votre serveur Outpost

Dès lors que votre Outpost est installé et que la capacité de calcul et de stockage est prête à être utilisée, vous pouvez vous lancer en créant des ressources. Par exemple, vous pouvez lancer des instances Amazon EC2.

Prérequis

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

Tâches

- Étape 1 : Créer un sous-réseau
- Étape 2 : Lancer une instance sur l'Outpost
- Étape 3 : Configurer la connectivité
- Étape 4 : Tester la connexion

Étape 1 : Créer un sous-réseau

Vous pouvez ajouter des sous-réseaux Outpost à n'importe quel VPC de la AWS région pour l'Outpost. Dans ce cas, le VPC englobe également l'Outpost. Pour plus d'informations, consultez Composants du réseau.

> **Note**
>
> Si vous lancez une instance dans un sous-réseau Outpost qui a été partagée avec vous par un autre Compte AWS, passez directement à. Étape 2 : Lancer une instance sur l'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 et spécifiez une plage d'adresses IP pour le sous-réseau.

5. Choisissez Créer.
6. Une fois le sous-réseau créé, activez-le pour les interfaces de réseau local.

Étape 2 : Lancer une instance sur l'Outpost

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

Considérations

- Les instances sur les serveurs Outposts comportent des volumes de stockage d'instances, mais pas de volumes EBS. Choisissez une taille d'instance offrant suffisamment de stockage pour répondre aux besoins de votre application. Pour plus d'informations, consultez Volumes de stockage d'instances dans le Guide de l'utilisateur Amazon EC2.
- Vous devez spécifier une AMI constituée d'un seul instantané. Les AMI comportant plusieurs instantanés ne sont pas prises en charge.
- Les données stockées sur les volumes de stockage d'instances subsistent après un redémarrage d'instance, mais pas après une résiliation d'instance. Pour conserver les données à long terme sur vos volumes de stockage d'instances au-delà de la durée de vie de l'instance, veillez à sauvegarder les données sur un système de stockage persistant, tel qu'un compartiment Amazon S3 ou un dispositif de stockage de votre réseau sur site.
- Pour connecter une instance de sous-réseau Outpost à votre réseau sur site, vous devez ajouter une interface de réseau local, comme décrit dans la procédure suivante.

Pour lancer des instances dans votre sous-réseau Outpost

1. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.
2. Dans le panneau de navigation, choisissez Outposts.
3. Sélectionnez l'Outpost, puis choisissez Actions, Afficher les détails.
4. Sur la page Récapitulatif de l'Outpost, choisissez Lancer une instance. Vous êtes redirigé vers l'assistant de lancement d'instances dans la console Amazon EC2. Nous sélectionnons le sous-

réseau Outpost pour vous et nous vous indiquons uniquement les types d'instances pris en charge par vos serveurs Outposts.

5. Choisissez un type d'instance compatible avec vos serveurs Outposts.
6. (Facultatif) Vous pouvez ajouter une interface de réseau local maintenant ou après avoir créé l'instance. Pour l'ajouter maintenant, développez Configuration réseau avancée, puis choisissez Ajouter une interface réseau. Choisissez le sous-réseau Outpost. Une interface réseau est alors créée pour l'instance avec l'index d'appareil 1. Si vous avez spécifié 1 comme index d'appareil LNI pour le sous-réseau Outpost, cette interface réseau devient l'interface de réseau local de l'instance.
7. Suivez les étapes de l'assistant pour lancer l'instance dans votre sous-réseau Outpost. Pour plus d'informations, consultez les rubriques suivantes dans le Guide de l'utilisateur Amazon EC2 :

   - Linux — Lancez une instance à l'aide du nouvel assistant de lancement d'instance
   - Windows — Lancez une instance à l'aide du nouvel assistant de lancement d'instance

Étape 3 : Configurer la connectivité

Si vous n'avez pas ajouté d'interface de réseau local à votre instance au cours de son lancement, vous devez le faire maintenant. Pour plus d'informations, consultez Ajout d'une interface LNI après le lancement.

Vous devez configurer l'interface de réseau local pour l'instance avec une adresse IP de votre réseau local. Dans ce cas, le protocole DHCP est généralement utilisé. Pour plus d'informations, consultez la documentation correspondant au système d'exploitation s'exécutant sur l'instance. Recherchez des informations sur la configuration d'interfaces réseau supplémentaires et d'adresses IP secondaires.

Étape 4 : Tester la connexion

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 de l'interface réseau locale de l'instance Outpost.

```
ping 10.0.3.128
```

Voici un exemple de sortie.

```
Pinging 10.0.3.128

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

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

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

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

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

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

```
ping 172.16.0.130
```

Voici un exemple de sortie.

```
Pinging 172.16.0.130

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

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

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

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

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

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

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

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

   ```
   ping 10.0.1.5
   ```

   Voici un exemple de sortie.

   ```
   Pinging 10.0.1.5

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

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

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

Connectivité AWS Outposts avec les régions AWS

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

> **Note**
>
> Vous ne pouvez pas utiliser de connectivité privée pour votre connexion de liaison de service qui relie votre serveur Outpost à votre région AWS (ou région d'origine AWS Outposts).

Table des matières

Connectivité via les liaisons de service

Pendant le provisionnement d'AWS Outposts, vous ou AWS créez une connexion de liaison de service qui relie votre Outpost à la région AWS de votre choix (ou région d'origine AWS Outposts). 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. Le VLAN de la liaison de service permet la communication entre l'Outpost et la région AWS, tant pour la gestion de l'Outpost que pour le trafic intra-VPC entre la région AWS et l'Outpost.

L'Outpost est en mesure de créer le VPN de la liaison de service vers la région AWS via une connectivité régionale publique. Pour cela, l'Outpost a besoin d'une connectivité avec les plages d'adresses IP publiques de la région AWS en passant soit par l'Internet public, soit par une interface virtuelle publique AWS Direct Connect. Cette connectivité peut emprunter des routes spécifiques dans le réseau VLAN de la liaison de service ou bien la route par défaut 0.0.0.0/0. Pour plus d'informations sur les plages publiques pour AWS, consultez Plages d'adresses IP AWS.

Une fois la liaison de service établie, l'Outpost est en service et géré par AWS. La liaison de service est utilisée pour le trafic suivant :

- Trafic de gestion vers l'Outpost via la liaison de service, y compris le trafic du plan de contrôle interne, la surveillance des ressources internes et les mises à jour de microprogramme et de logiciel.
- Trafic entre l'Outpost et les VPC associés, y compris le trafic du plan de données du client.

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

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

Recommandations concernant la bande passante de la liaison de service

Pour une expérience et une résilience optimales, AWS vous recommande d'utiliser une connectivité redondante d'au moins 500 Mbits/s pour la connexion de la liaison de service vers la région AWS. L'utilisation maximale pour chaque serveur Outpost est de 500 Mbits/s. Pour accroître la vitesse de connexion, utilisez plusieurs serveurs Outpost. Par exemple, avec trois serveurs AWS Outposts, la vitesse de connexion maximale passe à 1,5 Gbit/s (1 500 Mbits/s). Pour plus d'informations, consultez Trafic de liaison de service pour les serveurs.

Les besoins en bande passante de votre liaison de service AWS Outposts varient en fonction des 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. Notez que les serveurs AWS Outposts ne mettent pas les AMI en cache. Les AMI sont téléchargées depuis la région à chaque lancement d'instance.

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

Pare-feu et liaison de service

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

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

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

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

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

Protocole	Port source	Adresse source	Port de destination	Adresse de destination
UDP	1024-65535	Adresse IP de la liaison de service	53	Serveur DNS fourni par DHCP
UDP	443, 1024-65535	Adresse IP de la liaison de service	443	Points de terminaison de la liaison de service AWS Outposts
TCP	1024-65535	Adresse IP de la liaison de service	443	Points de terminaison d'enregistrement AWS Outposts

> **Note**
>
> Les instances contenues dans un Outpost ne peuvent pas utiliser la liaison de service pour communiquer avec les instances d'un autre Outpost. Pour permettre la communication entre les Outposts, optez pour un routage via la passerelle locale ou l'interface de réseau local.

Mises à jour et liaison de service

AWSmaintient une connexion réseau sécurisée entre votre serveur Outpost et sa AWS région mère. Cette connexion réseau, appelée liaison de service, est essentielle à la gestion de l'avant-poste en fournissant du trafic intra-VPC entre l'avant-poste et la région. AWS AWS Les meilleures pratiques de Well-Architected recommandent de déployer des applications sur deux Outposts associés à différentes zones de disponibilité avec une conception active-active. Pour plus d'informations, consultez la section Considérations relatives à la conception et à l'architecture de AWS Outposts haute disponibilité.

Le lien de service est régulièrement mis à jour pour maintenir la qualité et les performances opérationnelles. Au cours de la maintenance, vous pouvez observer de brèves périodes de latence et de perte de paquets sur ce réseau, ce qui a un impact sur les charges de travail qui dépendent de la connectivité VPC aux ressources hébergées dans la région. Toutefois, le trafic passant par les interfaces réseau locales (LNI) ne sera pas affecté. Vous pouvez éviter tout impact sur votre application en suivant les meilleures pratiques de AWSWell-Architected et en veillant à ce que vos applications résistent aux défaillances ou aux activités de maintenance affectant un seul serveur Outpost.

Connexions Internet redondantes

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

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

Outposts et sites

Gérez les Outposts et les sites pour. AWS Outposts

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

Rubriques

- Gestion des Outposts
- Gestion des sites Outpost

Gestion des Outposts

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

Pour créer un Outpost

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

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

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

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

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

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

10. Choisissez Créer un Outpost.

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

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

Pour modifier le nom et la description de l'Outpost

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

   Dans Nom, saisissez le nom.

Dans Description, saisissez la description.

6. Sélectionnez Enregistrer les modifications.

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

Pour afficher les détails de l’Outpost

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

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

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

- Utilisez la commande get-outpost AWS CLI .

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

Pour gérer les balises de l’Outpost

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

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

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

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

6. Sélectionnez Enregistrer les modifications.

Gestion des sites Outpost

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

Pour créer un site Outpost

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

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

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

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

Effectuez les étapes suivantes pour modifier un site Outpost.

Pour modifier un site

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

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

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

Pour afficher les détails du site

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

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

Pour gérer les balises du site

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

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

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

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

Renvoyer un AWS Outposts serveur

Si un défaut est AWS Outposts détecté sur le serveur, nous vous en informerons, lancerons le processus de remplacement pour vous envoyer un nouveau serveur et vous fournirons l'étiquette d'expédition via la AWS Outposts console.

Si vous souhaitez renvoyer le serveur parce qu'il arrive à la fin de la durée du contrat ou pour toute autre raison, contactez le AWS Supportcentre.

Rubriques

Les étapes suivantes expliquent comment renvoyer un serveur àAWS.

1. Préparer le serveur pour le retour

Pour préparer le serveur au retour, annulez le partage des ressources, sauvegardez les données, supprimez les interfaces réseau locales et mettez fin aux instances actives.

1. Si les ressources de l'avant-poste sont partagées, vous devez annuler le partage de ces ressources.

   Vous pouvez annuler le partage d'une ressource Outpost partagée de l'une des manières suivantes :

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

   Pour consulter la liste des ressources d'Outpost qui peuvent être partagées, consultez la section Ressources d'Outpost partageables.
2. Créez des sauvegardes des données stockées dans le stockage d'instance des instances Amazon EC2 exécutées sur le AWS Outposts serveur.

3. Supprimez les interfaces réseau locales associées aux instances qui s'exécutaient sur le serveur.
4. Mettez fin aux instances actives associées aux sous-réseaux de votre Outpost. Pour mettre fin aux instances, suivez les instructions de la section Résilier votre instance dans le Guide de l'utilisateur Amazon EC2 pour les instances Linux.

2. Obtenez l'étiquette d'expédition de retour

> **Important**
>
> Vous ne devez utiliser que l'étiquette d'expédition AWS fournie. Ne créez pas votre propre étiquette d'expédition.

Obtenez votre étiquette d'expédition en fonction du motif de votre retour.

Shipping label for a server that is being replaced

1. Ouvrez la console AWS Outposts à l'adresse https://console.aws.amazon.com/outposts/.
2. Dans le volet de navigation, sélectionnez Commandes.
3. Sous Résumé de la commande de remplacement, choisissez Imprimer l'étiquette de retour et choisissez l'ID de configuration du serveur que vous souhaitez renvoyer.

Shipping label for a server that is not being replaced

1. AWS SupportCentre de contact.
2. Demandez une étiquette d'expédition pour le serveur que vous souhaitez renvoyer.

3. Emballez le serveur

Pour emballer votre serveur, utilisez la boîte et le matériel d'emballage dans lesquels le serveur a été initialement fourni. Vous pouvez également utiliser la boîte dans laquelle le serveur de remplacement arrive. Vous pouvez également contacter AWS Supportle centre pour demander une boîte. Après avoir emballé le serveur, apposez l'étiquette d'expédition AWS fournie.

4. Renvoyez le serveur par le service de messagerie

Vous devez renvoyer le serveur par le service de messagerie désigné pour votre pays. Vous pouvez livrer le serveur au transporteur ou planifier le jour et l'heure que vous préférez pour que le coursier vienne chercher le serveur. L'étiquette d'expédition AWS fournie contient l'adresse correcte pour renvoyer le serveur.

Le tableau suivant indique les personnes à contacter pour le pays d'où vous expédiez :

Pays	Contact
Argentine	AWS SupportCentre de contact. Dans votre demande, incluez les informations suivantes : • Le numéro de suivi figurant sur l'étiquette d'expédition AWS fournie • La date et l'heure auxquelles vous préférez que le coursier vienne chercher le serveur • Le nom d'un contact • Un numéro de téléphone • Une adresse e-mail
Bahreïn	
Brésil	
Brunei	
Canada	
Chili	
Colombie	
Hong Kong	
Inde	
Indonésie	
Japon	
Malaisie	
Nigeria	
Oman	
Panama	

Pays	Contact
Pérou	
Philippines	
Serbie	
Singapour	
Afrique du Sud	
Corée du Sud	
Taïwan	
Thaïlande	
Emirats arabes unis	
Vietnam	
États-Unis	Contactez UPS. Vous pouvez renvoyer le serveur de différentes manières : • Retournez le serveur lors d'un ramassage UPS de routine sur votre site. • Déposez le serveur dans une agence UPS. • Planifiez un ramassage à la date et à l'heure que vous préférez. Entrez le numéro de suivi indiqué sur l'étiquette d'expédition AWS fournie pour une livraison gratuite.

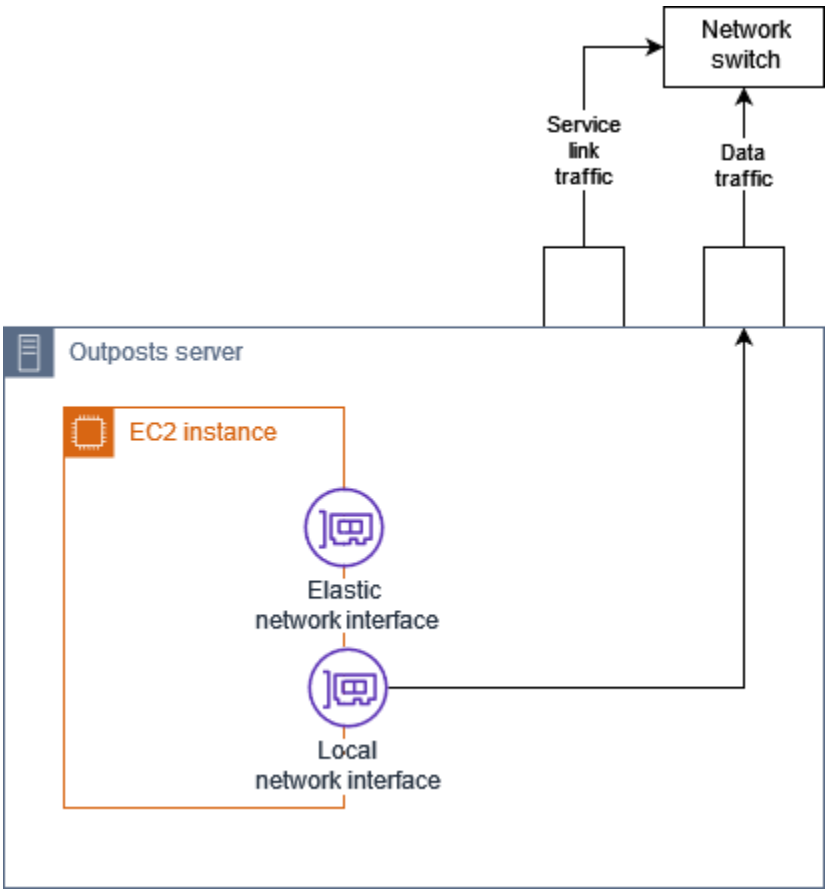
Pays	Contact
Tous les autres pays	Contactez DHL. Vous pouvez renvoyer le serveur de différentes manières : • Déposez le serveur dans une agence DHL. • Planifiez un ramassage à la date et à l'heure que vous préférez. Entrez le numéro de bordereau DHL figurant sur l'étiquette d'expédition AWS fournie pour une livraison gratuite. Si l'erreur suivante s'affiche`Courier pickup cannot be scheduled for an import shipment`, cela signifie généralement que le pays de collecte que vous avez sélectionné ne correspond pas au pays de collecte indiqué sur l'étiquette d'expédition de retour. Sélectionnez le pays d'origine de l'envoi et réessayez.

Interfaces réseau locales

Dans le cas des AWS Outposts serveurs, une interface réseau locale (LNI) est un composant réseau logique qui connecte les instances Amazon EC2 de votre sous-réseau Outposts à votre réseau sur site.

Une interface réseau locale fonctionne directement sur votre réseau local. Avec ce type de connectivité locale, vous n'avez pas besoin de routeurs ou de passerelles pour communiquer avec votre équipement sur site. Les interfaces réseau locales sont nommées de la même manière que les interfaces réseau ou les interfaces réseau Elastic. Nous distinguons les deux interfaces en utilisant toujours le terme locale lorsque nous faisons référence aux interfaces réseau locales.

Après avoir activé les interfaces réseau locales sur un sous-réseau Outpost, vous pouvez configurer les instances EC2 du sous-réseau Outpost pour inclure une interface réseau locale en plus de l'interface réseau Elastic. L'interface réseau locale se connecte au réseau sur site tandis que l'interface réseau se connecte au VPC. Le diagramme suivant présente une instance EC2 sur un serveur Outposts avec une interface réseau Elastic et une interface réseau locale.



Vous devez configurer le système d'exploitation pour permettre à l'interface réseau locale de communiquer sur votre réseau local, comme vous le feriez pour tout autre équipement sur site. Vous ne pouvez pas utiliser les ensembles d'options DHCP dans un VPC pour configurer une interface réseau locale, car une interface réseau locale s'exécute sur votre réseau local.

L'interface réseau Elastic fonctionne exactement comme pour les instances d'un sous-réseau de zone de disponibilité. Par exemple, vous pouvez utiliser la connexion réseau VPC pour accéder aux points de terminaison régionaux publics Services AWS, ou vous pouvez utiliser les points de terminaison VPC d'interface pour accéder à l'aide de. Services AWS AWS PrivateLink Pour de plus amples informations, veuillez consulter Connectivité AWS Outposts avec les régions AWS.

Table des matières

Notions fondamentales concernant l'interface réseau locale

Les interfaces réseau locales permettent d'accéder à un réseau physique de couche 2. Un VPC est un réseau virtualisé de couche 3. Les interfaces réseau locales ne prennent pas en charge les composants réseau VPC. Ces composants incluent les groupes de sécurité, les listes de contrôle d'accès réseau, les routeurs ou tables de routage virtualisés et les journaux de flux. L'interface réseau locale ne fournit pas au serveur Outpost de visibilité sur les flux VPC de couche 3. Le système d'exploitation hôte de l'instance dispose d'une visibilité complète sur les trames provenant du réseau physique. Vous pouvez appliquer une logique de pare-feu standard aux informations contenues dans ces trames. Cependant, cette communication s'effectue à l'intérieur de l'instance mais en dehors du champ d'application des constructions virtualisées.

Considérations

- Les interfaces réseau locales prennent en charge les protocoles ARP et DHCP. Elles ne prennent pas en charge les messages de diffusion L2 généraux.
- Les quotas pour les interfaces réseau locales proviennent de votre quota pour les interfaces réseau. Pour plus d'informations, consultez Interfaces réseau dans le Guide de l'utilisateur Amazon VPC.

- Chaque instance EC2 peut avoir une interface réseau locale.
- Une interface réseau locale ne peut pas utiliser l'interface réseau principale (eth0) de l'instance.
- Les serveurs Outposts peuvent héberger plusieurs instances EC2, chacune dotée d'une interface réseau locale.

> **Note**
>
> Les instances EC2 d'un même serveur peuvent communiquer directement sans envoyer de données en dehors du serveur Outposts. Cette communication inclut le trafic via une interface réseau locale ou des interfaces réseau Elastic.

- Les interfaces réseau locales ne sont disponibles que pour les instances exécutées dans un sous-réseau Outposts sur un serveur Outpost.
- Les interfaces réseau locales ne prennent pas en charge le mode promiscuité ou l'usurpation d'adresse MAC.

Performance

Le LNI de chaque taille d'instance fournit une partie de la bande passante LNI physique 10 GbE disponible. Le tableau suivant répertorie les performances du réseau LNI pour chaque type d'instance :

Type d'instance	Bande passante de référence (Gbit/s)	Bande passante de rafale (Gbit/s)
c6id.large	0,15625	2,5
c6id.large	0,15625	2,5
c6id.xlarge	0,3125	2,5
c6id.2xlarge	0,625	2,5
c6id.4xlarge	1,25	2,5
c6id.8xlarge	2,5	2,5
c6id.12xlarge	3,75	3,75

Type d'instance	Bande passante de référence (Gbit/s)	Bande passante de rafale (Gbit/s)
c6id.16xlarge	5	5
c6id.24xlarge	7,5	7,5
c6id.32xlarge	10	10
c6gd.medium	0,15625	4
c6gd.large	0,3125	4
c6gd.xlarge	0,625	4
c6gd.2xlarge	1,25	4
c6gd.4xlarge	2,5	4
c6gd.8xlarge	4.8	4.8
c6gd.12xlarge	7,5	7,5
c6gd.16xlarge	10	10

Groupes de sécurité

De par sa conception, l'interface réseau locale n'utilise pas de groupes de sécurité dans votre VPC. Un groupe de sécurité contrôle le trafic VPC entrant et sortant. L'interface réseau locale n'est pas attachée au VPC. L'interface réseau locale est attachée à votre réseau local. Pour contrôler le trafic entrant et sortant sur l'interface réseau locale, utilisez un pare-feu ou une stratégie similaire, comme vous le feriez avec le reste de votre équipement sur site.

Surveillance

CloudWatch des métriques sont produites pour chaque interface réseau locale, tout comme elles le sont pour les interfaces réseau élastiques. Pour plus d'informations relatives aux instances Linux, consultez Surveiller les performances réseau de votre instance EC2 dans le Guide de l'utilisateur Amazon EC2 pour les instances Linux. Pour les instances Windows, consultez Surveiller

les performances réseau de votre instance EC2 dans le Guide de l'utilisateur Amazon EC2 pour les instances Windows.

Adresses MAC

AWS fournit des adresses MAC pour les interfaces réseau locales. Les interfaces réseau locales utilisent des adresses administrées localement (LAA) pour leurs adresses MAC. Une interface réseau locale utilise la même adresse MAC tant que vous ne supprimez pas l'interface. Après avoir supprimé une interface réseau locale, supprimez l'adresse MAC de vos configurations locales. AWS peut réutiliser les adresses MAC qui ne sont plus utilisées.

Activer les sous-réseaux sur les serveurs Outposts pour les interfaces réseau locales

Utilisez la modify-subnet-attributecommande du AWS CLI pour activer un sous-réseau Outpost pour les interfaces réseau locales. Vous devez spécifier la position de l'interface réseau sur l'index de périphérique. Toutes les instances lancées dans un sous-réseau Outpost activé utilisent la position de ce périphérique pour les interfaces réseau locales. Par exemple, une valeur 1 indique que l'interface réseau secondaire (eth1) d'une instance du sous-réseau Outpost est l'interface réseau locale.

Pour activer un sous-réseau Outpost pour les interfaces réseau locales

À l'invite de commande, utilisez la commande suivante pour spécifier la position du périphérique pour l'interface réseau locale.

```
aws ec2 modify-subnet-attribute \
    --subnet-id subnet-1a2b3c4d \
    --enable-lni-at-device-index 1
```

Utilisation des interfaces réseau locales

Reportez-vous à cette section pour savoir comment utiliser les interfaces réseau locales.

Tâches

- Ajout d'une interface réseau locale
- Affichage de l'interface réseau locale

- Configuration du système d'exploitation

Ajout d'une interface réseau locale

Vous pouvez ajouter une interface réseau locale (LNI) à une instance Amazon EC2 sur un sous-réseau Outposts pendant ou après le lancement. Pour ce faire, ajoutez une interface réseau secondaire à l'instance, en utilisant l'index de périphérique que vous avez spécifié lors de l'activation du sous-réseau Outpost pour les interfaces réseau locales.

Considération

Lorsque vous spécifiez l'interface réseau secondaire à l'aide de la console, l'interface réseau est créée à l'aide de l'index de périphérique 1. S'il ne s'agit pas de l'index de périphérique que vous avez spécifié lorsque vous avez activé le sous-réseau Outpost pour les interfaces réseau locales, vous pouvez spécifier l'index de périphérique correct en utilisant le AWS CLI ou un AWS SDK à la place. Par exemple, utilisez les commandes suivantes à partir de AWS CLI : create-network-interfaceet attach-network-interface.

Pour ajouter une interface réseau locale lors du lancement de l'instance

1. Dans l'assistant de lancement d'instance, choisissez Modifier en regard de Paramètres réseau.
2. Développez Configuration réseau avancée.
3. Choisissez Ajouter une interface réseau. Cela crée une interface réseau à l'aide de l'index de périphérique 1. Si vous avez spécifié 1 comme index de périphérique LNI pour le sous-réseau Outpost, cette interface réseau sera l'interface réseau locale de l'instance.
4. Choisissez le sous-réseau Outpost et mettez à jour la configuration de l'interface réseau selon les besoins.
5. Exécutez l'assistant pour lancer l'instance.

Pour ajouter une interface réseau locale après le lancement de l'instance

1. Dans le panneau de navigation, choisissez Réseau et sécurité; Interfaces réseau.
2. Créez l'interface réseau.
   a. Sélectionnez Create network interface (Créer une interface réseau).
   b. Sélectionnez le même sous-réseau Outpost que l'instance.

c. Vérifiez que l'option Adresse IPv4 privée est définie sur Attribution automatique.

d. Sélectionnez un groupe de sécurité. Les groupes de sécurité ne s'appliquant pas aux LNI, le groupe de sécurité que vous sélectionnez n'est pas pertinent.

e. Sélectionnez Create network interface (Créer une interface réseau).

3. Attachez l'interface réseau à l'instance.

a. Cochez la case correspondant à l'interface réseau nouvellement créée.

b. Sélectionnez Actions, puis Attach (Attacher).

c. Choisissez l'instance.

d. Choisissez Attacher. L'interface réseau est attachée au niveau de l'index de périphérique 1. Si vous avez spécifié 1 comme index de périphérique LNI pour le sous-réseau Outpost, cette interface réseau est l'interface réseau locale de l'instance.

Affichage de l'interface réseau locale

Lorsque l'instance est en cours d'exécution, vous pouvez utiliser la console Amazon EC2 pour afficher à la fois l'interface réseau Elastic et l'interface réseau locale pour les instances de votre sous-réseau Outpost. Sélectionnez l'instance, puis choisissez l'onglet Mise en réseau.

La console affiche une adresse IPv4 privée pour l'interface réseau locale à partir du CIDR du sous-réseau. Cette adresse n'est pas l'adresse IP de l'interface réseau locale et n'est pas utilisable. Cependant, cette adresse étant allouée à partir du CIDR du sous-réseau, vous devez en tenir compte dans le dimensionnement de votre sous-réseau. Vous devez définir l'adresse IP de l'interface réseau locale dans le système d'exploitation « invité », soit de manière statique, soit via votre serveur DHCP.

Configuration du système d'exploitation

Une fois les interfaces réseau locales activées, les instances Amazon EC2 disposeront de deux interfaces réseau, dont l'une est une interface réseau locale. Assurez-vous de configurer le système d'exploitation des instances Amazon EC2 que vous lancez pour prendre en charge une configuration réseau multi-résidents.

Connectivité réseau locale pour les serveurs

Reportez-vous à cette rubrique pour comprendre les exigences en matière de topologie et de câblage réseau pour héberger un serveur Outpost. Pour de plus amples informations, veuillez consulter Interfaces réseau locales.

Table des matières

Topologie du serveur sur votre réseau

Un serveur Outpost nécessite deux connexions distinctes à votre équipement réseau. Chaque connexion utilise un câble différent et achemine un type de trafic différent. Les divers câbles sont destinés à l'isolation des classes de trafic uniquement, et non à la redondance. Il n'est pas nécessaire que les deux câbles soient connectés à un réseau commun.

Le tableau suivant décrit les types et les étiquettes de trafic du serveur Outpost.

Étiquette de trafic	Description
2	Trafic de liaison de service — Ce trafic 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 AWS région et l'avant-poste. Le trafic de liaison de service inclut la connexion de la liaison de service entre l'Outpost et la région. La liaison de service correspond à un ou plusieurs VPN personnal isés entre l'Outpost et la région. L'Outpost se connecte à la zone de disponibilité de la région que vous avez choisie au moment de l'achat.

Étiquette de trafic	Description
1	Trafic de liaison d'interface réseau locale (LNI) : ce trafic permet la communication entre votre VPC et votre réseau local via l'interfa ce réseau locale. Le trafic de liaison local inclut les instances exécutées sur l'Outpost qui communiquent avec votre réseau sur site. Le trafic de liaison local peut également inclure des instances qui communiquent avec Internet via votre réseau sur site.

Connectivité physique du serveur

Chaque serveur Outpost est doté de ports physiques non redondants de liaison montante. Chaque port a ses propres exigences en matière de vitesse et de connecteurs, comme indiqué ci-dessous.

- 10 GbE : type de connecteur QSFP+

Câble QSFP+

Le câble QSFP+ possède un connecteur que vous pouvez relier au port 3 du serveur Outpost. L'autre extrémité du câble QSFP+ possède quatre interfaces SFP+ que vous pouvez connecter à votre commutateur. Deux des interfaces côté commutateur sont étiquetées 1 et 2. Les deux interfaces sont nécessaires au fonctionnement d'un serveur Outpost. Utilisez l'interface 2 pour le trafic de liaison de service et l'interface 1 pour le trafic de liaison LNI. Les autres interfaces ne sont pas utilisées.

Trafic de liaison de service pour les serveurs

Configurez le port de liaison de service de votre commutateur en tant que port d'accès non balisé à un VLAN avec une passerelle et une route vers les points de terminaison régionaux suivants :

- Points de terminaison de liaison de service
- Point de terminaison d'enregistrement Outposts

La connexion par lien de service doit disposer d'un DNS public pour que l'Outpost découvre son point de terminaison d'enregistrement dans la AWS région. La connexion peut avoir un périphérique NAT

entre le serveur Outpost et le point de terminaison d'enregistrement. Pour plus d'informations sur les plages d'adresses publiques pour AWS, consultez les plages d'adresses AWS IP dans le guide de l'utilisateur Amazon VPC et les AWS Outposts points de terminaison et quotas dans le. Références générales AWS

Pour enregistrer le serveur, ouvrez les ports réseau suivants :

- TCP 443
- UDP 443
- UDP 53

Vitesse de la liaison montante

Chaque serveur Outposts a besoin d'une vitesse de liaison montante minimale de 20 Mbits/s vers la région AWS .

Vous aurez peut-être besoin d'une liaison montante plus rapide en fonction de votre utilisation de la liaison LNI et de la liaison de service. Pour plus d'informations, consultez Recommandations en matière de bande passante pour les liaisons de service.

Trafic de liaison d'interface réseau locale (LNI)

Configurez le port de liaison LNI de votre périphérique réseau en amont en tant que port d'accès standard à un VLAN sur votre réseau local. Si vous disposez de plusieurs VLAN, configurez tous les ports du périphérique réseau en amont en tant que ports de jonction. Configurez le port de votre périphérique réseau en amont pour qu'il puisse accepter plusieurs adresses MAC. Chaque instance lancée sur le serveur utilisera une adresse MAC. Certains périphériques réseau proposent des fonctionnalités de sécurité des ports qui désactivent un port signalant plusieurs adresses MAC.

> **Note**
>
> AWS Outposts les serveurs ne balisent pas le trafic VLAN. Si vous configurez votre LNI en tant que jonction, vous devez vous assurer que votre système d'exploitation balise le trafic VLAN.

L'exemple suivant montre comment configurer le balisage VLAN pour votre LNI sur Amazon Linux 2023. Si vous utilisez une autre distribution Linux, consultez la documentation correspondante pour la configuration du balisage VLAN.

Exemple : pour configurer le balisage VLAN pour votre LNI sur Amazon Linux 2023 et Amazon Linux 2

1. Assurez-vous que le module 8021q est chargé dans le noyau. Sinon, chargez-le à l'aide de la commande `modprobe`.

```
modinfo 8021q
modprobe --first-time 8021q
```

2. Créez le périphérique VLAN. Dans cet exemple :

   - Le nom de l'interface réseau locale est `ens6`
   - L'identifiant du VLAN est `59`
   - Le nom attribué au périphérique VLAN est `ens6.59`

```
ip link add link ens6 name ens6.59 type vlan id 59
```

3. Facultatif. Exécutez cette étape si vous souhaitez attribuer manuellement l'adresse IP. Dans cet exemple, nous attribuons l'adresse IP 192.168.59.205, où le CIDR du sous-réseau est 192.168.59.0/24.

```
ip addr add 192.168.59.205/24 brd 192.168.59.255 dev ens6.59
```

4. Activez le lien.

```
ip link set dev ens6.59 up
```

Pour configurer vos interfaces réseau au niveau du système d'exploitation et faire en sorte que les modifications de balisage VLAN soient permanentes, consultez les ressources suivantes :

- Si vous utilisez Amazon Linux 2, consultez Configurer votre interface réseau à l'aide de ec2-net-utils pour Amazon Linux dans le Guide de l'utilisateur Amazon EC2 pour les instances Linux.
- Si vous utilisez Amazon Linux 2023, consultez Service de mise en réseau dans le Guide de l'utilisateur Amazon Linux 2023.

Attribution d'adresse IP de serveur

Il n'est pas nécessaire d'attribuer des adresses IP publiques aux serveurs Outpost.

Le protocole DHCP (Dynamic Host Control Protocol) est un protocole de gestion réseau utilisé pour automatiser le processus de configuration des périphériques sur les réseaux IP. Dans le contexte des serveurs Outpost, vous pouvez utiliser le protocole DHCP de deux manières :

- Cartes réseau sur le serveur
- Interfaces réseau locales sur les instances

Pour la liaison de service, les serveurs Outpost utilisent le protocole DHCP pour se connecter au réseau local. Le protocole DHCP doit renvoyer des serveurs de noms DNS et une passerelle par défaut. Les serveurs Outpost ne prennent pas en charge l'attribution d'adresses IP statiques aux liaisons de service.

Pour la liaison LNI, utilisez le protocole DHCP pour configurer les instances à connecter à votre réseau local. Pour plus d'informations, veuillez consulter the section called “Configuration du système d'exploitation”.

> **Note**
>
> Assurez-vous d'utiliser une adresse IP stable pour le serveur Outpost. Les modifications d'adresse IP peuvent entraîner des interruptions de service temporaires sur le sous-réseau Outpost.

Enregistrement du serveur

Lorsque les serveurs Outpost établissent une connexion sur le réseau local, ils utilisent la connexion de la liaison de service pour se connecter aux points de terminaison d'enregistrement Outpost et s'enregistrer. L'enregistrement nécessite un DNS public. Lorsque les serveurs s'enregistrent, ils créent un tunnel sécurisé vers le point de terminaison de leur liaison de service dans la région. Les serveurs Outpost utilisent le port TCP 443 pour faciliter la communication avec la région via l'Internet public. Actuellement, AWS Outposts les serveurs ne prennent pas en charge la connectivité privée via VPC. Pour de plus amples informations, veuillez consulter the section called “Étape 6 : Autoriser le serveur”.

Utilisation de AWS Outposts ressources partagées

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

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

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

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

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

Table des matières

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

Ressources Outpost partageables

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

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

- Hôtes dédiés alloués — Les consommateurs ayant accès à cette ressource peuvent :
  - Lancez et exécutez des instances EC2 sur un hôte dédié.
- Outposts — Les consommateurs ayant accès à cette ressource peuvent :
  - Créez et gérez des sous-réseaux sur l'Outpost.
  - Utilisez l'AWS OutpostsAPI pour consulter les informations relatives à l'Outpost.
- Sites — Les consommateurs ayant accès à cette ressource peuvent :
  - Créez, gérez et contrôlez un avant-poste sur le site.
- Sous-réseaux — Les consommateurs ayant accès à cette ressource peuvent :
  - Afficher les informations relatives aux sous-réseaux.
  - Lancez et exécutez des instances EC2 dans des sous-réseaux.

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

Conditions préalables au partage des ressources des Outposts

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

Services connexes

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

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

Partage sur plusieurs zones de disponibilité

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

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

Pour afficher les ID de zone de disponibilité pour votre compte

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

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

Partage d'une ressource Outpost

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

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

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

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

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

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

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

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

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

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

Utilisez la commande create-resource-share.

Annulation du partage d'une ressource Outpost

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

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

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

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

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

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

Utilisez la commande disassociate-resource-share.

Identifier une ressource Outpost partagée

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

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

1. Ouvrez la console AWS Outposts à l'adresse https://console.aws.amazon.com/outposts/.
2. Dans le volet de navigation, choisissez Outposts.
3. Sélectionnez l'avant-poste, puis choisissez Actions, Afficher les détails.
4. Sur la page récapitulative de l'Outpost, consultez l'ID du propriétaire pour identifier le numéro de AWS compte du propriétaire de l'Outpost.

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

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

Autorisations relatives aux ressources Shared Outpost

Autorisations accordées aux propriétaires

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

Autorisations accordées aux consommateurs

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

Facturation et mesures

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

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

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

Limites

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

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

Sécurité dans AWS Outposts

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

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

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

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

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

Table des matières

Protection des données dans AWS Outposts

Le modèle de responsabilité AWS partagée de s'applique à la protection des données dans AWS Outposts. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Ce contenu inclut la configuration de la sécurité et les tâches de gestion pour le Services AWS produit que vous utilisez.

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

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

Chiffrement au repos

Avec AWS Outposts, toutes les données sont cryptées au repos. Les éléments de clé sont encapsulés dans une clé externe stockée dans un dispositif amovible : la clé de sécurité Nitro (NSK). La clé NSK est nécessaire pour déchiffrer les données sur votre rack Outpost.

Chiffrement en transit

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

Suppression de données

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

La destruction par chiffrement de la clé de sécurité Nitro déchiquette les données sur votre Outpost. Pour plus d’informations, consultez Déchiquetage par chiffrement des données d'un serveur.

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

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

Table des matières

Comment AWS Outposts fonctionne avec IAM

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

Fonctionnalités IAM que vous pouvez utiliser avec Outposts AWS

Fonction IAM	AWS Soutien aux Outposts
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique (spécifiques au service)	Oui
ACL	Non
ABAC (étiquettes dans les politiques)	Oui
Informations d'identification temporaires	Oui

Fonction 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 Groupes d'utilisateurs IAM ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, veuillez consulter Création de politiques IAM dans le Guide de l'utilisateur IAM.

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

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

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

Politiques basées sur les ressources au sein d'Outposts AWS

Prend en charge les politiques basées sur les ressources	Non

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

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

Actions politiques pour les AWS Outposts

Prend en charge les actions de politique	Oui

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

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

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

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

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

```
outposts
```

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

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

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

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

Ressources politiques pour les AWS Outposts

Prend en charge les ressources de politique	Oui

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

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

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

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

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

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

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

Clés de conditions politiques pour les AWS Outposts

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

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

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

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

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource

uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour plus d'informations, consultez Éléments d'une politique IAM : variables et identifications dans le Guide de l'utilisateur IAM.

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

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

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

ACL dans les Outposts AWS

Prend en charge les listes ACL	Non

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

ABAC avec Outposts AWS

Prend en charge ABAC (étiquettes dans les politiques)	Oui

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

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

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

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

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

Utiliser des informations d'identification temporaires avec AWS Outposts

Prend en charge les informations d'identification temporaires	Oui

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

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

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

Autorisations principales interservices pour les Outposts AWS

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

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

Fonctions du service pour AWS Outposts

Prend en charge les fonctions de service	Non

Une fonction du service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

Rôles liés à un service pour les Outposts AWS

Prend en charge les rôles liés à un service.	Oui

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

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

AWS Exemples de politiques relatives aux Outposts

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

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

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

Table des matières

Bonnes pratiques en matière de politiques

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

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour de plus amples informations, consultez Politiques gérées AWS ou Politiques gérées AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Accorder les autorisations de moindre privilège - Lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une

seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation de IAM pour appliquer des autorisations, consultez Politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.

- Utiliser des conditions dans les politiques IAM pour restreindre davantage l'accès - Vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez IAM Access Analyzer pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles - IAM Access Analyzer valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour de plus amples informations, consultez Validation de politique IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour de plus amples informations, consultez Configuration de l'accès aux API protégé par MFA dans le Guide de l'utilisateur IAM.

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

Exemple : Utilisation d'autorisations au niveau des ressources

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

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```
      "Action": "outposts:GetOutpost",
      "Resource": "arn:aws:outposts:region:12345678012:outpost/op-1234567890abcdef0"
    }
  ]
}
```

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

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

Utilisation des rôles liés aux services pour AWS Outposts

AWS Outposts utilise des AWS Identity and Access Management rôles liés à un service (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à. AWS Outposts Les rôles liés au service sont prédéfinis par AWS Outposts et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom.

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

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

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

Autorisations des rôles liés à un service pour AWS Outposts

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

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

- `outposts.amazonaws.com`

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

- AWSOutpostsServiceRolePolicy
- AWSOutpostsPrivateConnectivityPolicy_ ***OutPostID***

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Si vous n'avez plus besoin d'utiliser une fonctionnalité ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous évitez d'avoir

une entité inutilisée non surveillée ou non gérée activement. Cependant, vous devez nettoyer les ressources de votre rôle lié à un service avant de pouvoir les supprimer manuellement.

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

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

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

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

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

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

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

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

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

AWS politiques gérées pour AWS Outposts

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

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

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

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

AWS politique gérée : AWSOutpostsServiceRolePolicy

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

AWS politique gérée : AWSOutpostsPrivateConnectivityPolicy

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

AWS politique gérée : AWSOutpostsAuthorizeServerPolicy

Utilisez cette politique pour accorder les autorisations nécessaires pour autoriser le matériel serveur Outpost dans votre réseau sur site. Pour plus d'informations, consultez Accorder des autorisations.

Cette politique inclut les autorisations suivantes.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "outposts:StartConnection",
        "outposts:GetConnection"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS Outposts mises à jour des politiques AWS gérées

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

Modification	Description	Date
AWSOutpostsAuthorizeServerPolicy – Nouvelle politique	AWS Outposts a ajouté une politique qui accorde des autorisations pour autoriser le matériel du serveur Outpost sur votre réseau local.	4 janvier 2023
AWS Outposts a commencé à suivre les modifications	AWS Outposts a commencé à suivre les modifications apportées AWS à ses politique s gérées.	3 décembre 2019

Sécurité de l'infrastructure dans AWS Outposts

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

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

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

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

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

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

Résilience dans AWS Outposts

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

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

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

Si les serveurs Outposts intègrent des volumes de stockage d'instances, ils ne prennent toutefois pas en charge les volumes Amazon EBS. Les données stockées sur les volumes de stockage d'instances subsistent après un redémarrage d'instance, mais pas après une résiliation d'instance. Pour conserver les données à long terme sur vos volumes de stockage d'instances au-delà de la durée de vie de l'instance, veillez à sauvegarder les données sur un système de stockage persistant, tel qu'un compartiment Amazon S3 ou un dispositif de stockage de votre réseau sur site.

Validation de conformité pour AWS Outposts

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

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

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

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

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

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

Surveillance de votre Outpost

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

CloudWatch métriques

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

CloudTrail journaux

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

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

Journaux de flux VPC

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

Mise en miroir du trafic

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

AWS Health Dashboard

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

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

CloudWatch métriques pour AWS Outposts

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

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

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

Table des matières

Métriques Outpost

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

`ConnectedStatus`

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

Unité : nombre

Résolution maximale : 1 minute

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

Dimensions : `OutpostId`

`CapacityExceptions`

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

Unité : nombre

Résolution maximale : 5 minutes

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

Dimensions : `InstanceType` et `OutpostId`

`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 p`NN.NN` (percentiles).

Dimensions : `InstanceFamily` et `OutpostId`

`InstanceFamilyCapacityUtilization`

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

Unité : pourcentage

Résolution maximale : 5 minutes

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

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

`InstanceTypeCapacityAvailability`

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

Unité : pourcentage

Résolution maximale : 5 minutes

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

Dimensions : `InstanceType` et `OutpostId`

`InstanceTypeCapacityUtilization`

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

Unité : pourcentage

Résolution maximale : 5 minutes

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

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

`UsedInstanceType_Count`

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

Unité : nombre

Résolution maximale : 5 minutes

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

`AvailableInstanceType_Count`

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

Unité : nombre

Résolution maximale : 5 minutes

Dimensions : `InstanceType` et `OutpostId`

`AvailableReservedInstances`

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

Unité : nombre

Résolution maximale : 5 minutes

Dimensions : `InstanceType` et `OutpostId`

`UsedReservedInstances`

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

Unité : nombre

Résolution maximale : 5 minutes

Dimensions : `InstanceType` et `OutpostId`

`TotalReservedInstances`

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

Unité : nombre

Résolution maximale : 5 minutes

Dimensions : `InstanceType` et `OutpostId`

Dimensions des métriques Outpost

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

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

Afficher CloudWatch les statistiques de votre avant-poste

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

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

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

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

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

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

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

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

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

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

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

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

AWS Outpostsinformations dans CloudTrail

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

télécharger les événements récents dans votre compte AWS. Pour plus d'informations, consultez la section Affichage des événements avec l'historique des CloudTrail événements.

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

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

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

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

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

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

Présentation des entrées des fichiers journaux AWS Outposts

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent

une ou plusieurs entrées de journal. Un événement représente une demande unique d’une source quelconque. Il inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

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


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAIOSFODNN7EXAMPLE:jdoe",
        "arn": "arn:aws:sts::111122223333:assumed-role/example/jdoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAIOSFODNN7EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/example",
                "accountId": "111122223333",
                "userName": "example"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2020-08-14T16:28:16Z"
            }
        }
    },
    "eventTime": "2020-08-14T16:32:23Z",
    "eventSource": "outposts.amazonaws.com",
    "eventName": "SetSiteAddress",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "XXX.XXX.XXX.XXX",
    "userAgent": "userAgent",
    "requestParameters": {
        "SiteId": "os-123ab4c56789de01f",
        "Address": "***"
    },
    "responseElements": {
        "Address": "***",
        "SiteId": "os-123ab4c56789de01f"
```

```
    },
    "requestID": "1abcd23e-f4gh-567j-klm8-9np01q234r56",
    "eventID": "1234a56b-c78d-9e0f-g1h2-34jk56m7n890",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

Maintenance d'un Outpost

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

> **Warning**
>
> Si le lecteur de disque sous-jacent rencontre une défaillance ou si l'instance s', 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 ou un dispositif de stockage de votre réseau sur site.

Table des matières

Maintenance matérielle

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

AWS résilie les instances affectées à la date prévue de leur retrait. Les données stockées sur des volumes de stockage d'instances ne sont pas conservées à l'issue de la résiliation d'instances. Il est donc important de prendre des mesures avant la date de retrait des instances. Dans un premier temps, transférez vos données à long terme des volumes de stockage de chaque instance concernée vers un stockage persistant, tel qu'un compartiment Amazon S3 ou un dispositif de stockage de votre réseau.

Un serveur de remplacement sera expédié sur le site de l'Outpost. Ensuite, procédez comme suit :

- Retirez les câbles réseau et d'alimentation du serveur irréparable puis, si nécessaire, ôtez ce dernier du rack.
- Installez le serveur de remplacement au même emplacement. Suivez les instructions d'installation décrites dans Installation d'un serveur Outpost.
- Retournez le serveur irréparable à AWS en utilisant l'emballage du serveur de remplacement.
- Servez-vous de l'étiquette de retour prépayée disponible dans la console et qui est jointe aux détails de configuration de la commande ou à la commande du serveur de remplacement.
- Retournez le serveur à AWS. Pour plus d'informations, consultez Retour d'un serveur AWS Outposts.

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.

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

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

Événements liés à l'alimentation

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

- Déplacez vos services et applications en dehors de l'équipement Outposts de manière contrôlée, en procédant à des changements d'équilibrage de charge extérieurs au rack ou basés sur DNS.

- Arrêtez les conteneurs, les instances et les bases de données de manière incrémentielle et ordonnée et restaurez-les dans l'ordre inverse.
- Testez des solutions permettant de déplacer ou d'arrêter les services de manière contrôlée.
- Sauvegardez les données et les configurations critiques et stockez-les en dehors des Outposts.
- Limitez les coupures de courant au minimum.
- Évitez de changer plusieurs fois les alimentations (off-on-off-on) pendant la maintenance.
- Prévoyez du temps supplémentaire dans la fenêtre de maintenance pour faire face aux imprévus.
- Gérez les attentes de vos utilisateurs et de vos clients en leur communiquant une fenêtre de maintenance plus grande que le temps dont vous auriez normalement besoin.

Événements liés à la connectivité réseau

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

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

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

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

  Capturez un trace-route entre :

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

Ressources

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

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

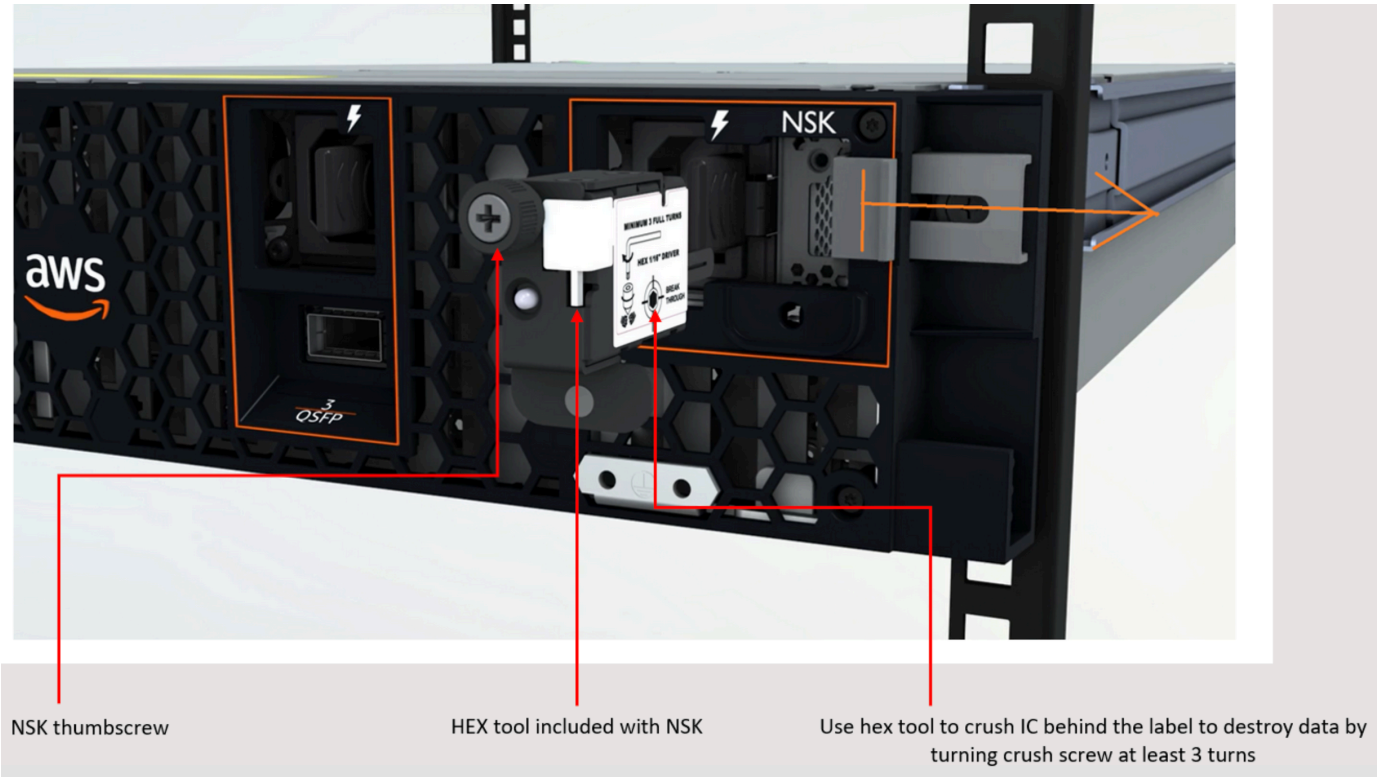
- Si vous avez des questions ou si vous souhaitez obtenir des informations supplémentaires, consultez Création d'un dossier de support dans le Guide de l'utilisateur AWS Support.

Déchiquetage par chiffrement des données d'un serveur

La clé de sécurité Nitro (NSK) est nécessaire pour déchiffrer les données du serveur. Lorsque vous retournez le serveur à AWS, soit pour le remplacer, soit parce que vous renoncez au service, vous pouvez détruire la clé NSK pour déchiqueter par chiffrement les données du serveur.

Pour déchiqueter par chiffrement les données du serveur

1. Retirez la clé NSK du serveur avant de le retourner à AWS.
2. Vérifiez que vous disposez de la clé NSK adéquate qui a été fournie avec le serveur.
3. Retirez le petit outil à tête hexagonale ou la clé Allen qui se trouve sous l'autocollant.
4. À l'aide de l'outil à tête hexagonale, faites tourner la petite vis située sous l'autocollant de trois tours complets. Cela a pour effet de détruire la clé NSK et de déchiqueter par chiffrement toutes les données présentes sur le serveur.



AWS Outposts end-of-term options

À la fin de votre contrat AWS Outposts, trois options s'offrent à vous :

- Renouvelez votre abonnement et conservez votre Outpost existant.
- Mettez fin à votre abonnement et renvoyez vos serveurs Outpost.
- Passez à un month-to-month abonnement et conservez votre serveur Outpost existant.

Si vous n'indiquez pas que vous souhaitez renouveler votre abonnement ou renvoyer votre serveur Outpost, vous serez converti en month-to-month abonnement.

Rubriques

Renouvellement de votre abonnement

Pour renouveler votre abonnement et conserver votre serveur Outpost existant :

Effectuez les étapes suivantes au moins 30 jours avant la fin du contrat de votre Outpost :

1. Connectez-vous à la console du Centre AWS Support.
2. Choisissez Create case (Créer une demande).
3. Choisissez Compte et facturation.
4. Pour Service, choisissez Facturation.
5. Pour Catégorie, choisissez Autres questions de facturation.
6. Pour Gravité, choisissez Question importante.
7. Choisissez Next step: Additional information (Étape suivante : informations supplémentaires).
8. Dans la page Informations supplémentaires, pour Objet, entrez votre demande de renouvellement, telle que **`Renew my Outpost subscription`**.
9. Pour Description, entrez l'une des options de paiement suivantes :

    - Sans frais initiaux

- Frais initiaux partiels
- Tous les frais initiaux

Pour connaître les tarifs, consultez les Tarification des serveurs AWS Outposts. Vous pouvez également demander un devis.

10. Choisissez Next step: Solve now or contact us (Étape suivante : résolvez maintenant ou contactez-nous).
11. Sur la page Contact us (Contactez-nous), choisissez votre langue préférée.
12. Choisissez votre méthode de contact préférée.
13. Vérifiez les détails de votre cas et choisissez Submit (Envoyer). Votre numéro d'ID de dossier et votre résumé apparaissent.

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

Mettez fin à votre abonnement et renvoyez le serveur

> **Important**
>
> AWS ne peut pas commencer le processus de retour tant que vous n'avez pas effectué la procédure suivante. Nous ne pouvons pas arrêter le processus de retour une fois que vous avez ouvert un cas de support pour mettre fin à votre abonnement.

Pour mettre fin à votre abonnement :

Effectuez les étapes suivantes au moins 30 jours avant la fin du contrat de votre Outpost :

1. Connectez-vous à la console du Centre AWS Support.
2. Choisissez Create case (Créer une demande).
3. Choisissez Compte et facturation.
4. Pour Service, choisissez Facturation.
5. Pour Catégorie, choisissez Autres questions de facturation.
6. Pour Gravité, choisissez Question importante.

7. Choisissez Next step: Additional information (Étape suivante : informations supplémentaires).
8. Dans la page Informations supplémentaires, pour Objet, entrez une demande claire, telle que **`End my Outpost subscription`**.
9. Dans Description, entrez la date à laquelle vous souhaitez mettre fin à votre abonnement.
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. Si nécessaire, sauvegardez toutes les instances et les données d'instance présentes sur votre serveur.
14. Mettez fin aux instances lancées sur votre serveur.
15. Vérifiez les détails de votre cas et choisissez Submit (Envoyer). Votre numéro d'ID de dossier et votre résumé apparaissent.
16. NE METTEZ PAS le serveur hors tension ni ne le déconnectez du réseau avant d'avoir reçu l'instruction de le faire dans le dossier d'assistance.

Pour renvoyer votre serveur AWS Outposts, suivez les procédures décrites dans la section Renvoyer un serveur AWS Outposts.

Convertir en month-to-month abonnement

Pour passer à un month-to-month abonnement et conserver votre serveur Outpost existant, aucune action n'est nécessaire. Si vous avez des questions, ouvrez un cas de support pour la facturation.

Votre Outpost sera renouvelé sur une base mensuelle au taux de l'option de paiement Aucuns frais initiaux correspondant à votre configuration AWS Outposts. Votre nouvel abonnement mensuel débutera le lendemain de la fin de votre abonnement actuel.

Quotas pour AWS Outposts

VotreCompte AWS dispose de quotas par défaut, anciennement appelés limites, pour chaque dispose de quotas par défaut, anciennement appelés limitesService AWS. Sauf indication contraire, chaque quota est spécifique à la région. Vous pouvez demander des augmentations pour certains quotas, et pas pour tous les quotas.

Pour afficher les quotas pourAWS Outposts, ouvrez la boîte de dialogue Service Quotas Console (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.

Les quotas de votre Compte AWS concernant AWS Outposts sont les suivants :

Ressource	Par défaut	Ajustable	Commentaires
Sites d'avant-poste	100	Oui	Un site Outpost est le bâtiment physique géré par le client dans lequel vous alimentez et connectez votre équipement Outpost au réseau. Vous pouvez avoir 100 sites Outposts dans chaque région de votreAWS compte.
Outposts par site	10	Oui	AWS Outpostsinclut des ressource s matérielles et virtuelles, appelées Outposts. Ce quota limite les ressources virtuelles de votre Outpost. Vous pouvez avoir 10 Outposts dans chaque site d'avant-poste.

AWS Outpostset les quotas pour les autres services

AWS Outpostsdépend des ressources d'autres services et ces services peuvent avoir leurs propres quotas par défaut. Par exemple, votre quota pour les interfaces réseau locales provient du quota Amazon VPC pour les interfaces réseau.

Historique du document

Le tableau suivant décrit les modifications importantes apportées au Guide de l'utilisateur AWS Outposts .

Modification	Description	Date
Gestion des capacités	Vous pouvez modifier la configuration de capacité par défaut pour votre nouvelle commande d'Outposts.	16 avril 2024
nd-of-term Options E pour AWS Outposts serveurs	À la fin de votre AWS Outposts période, vous pouvez renouveler, résilier ou convertir votre abonnement.	1er août 2023
Guide de AWS Outposts l'utilisateur créé pour les serveurs Outposts	AWS Outposts Le guide de l'utilisateur a été divisé en guides distincts pour le rack et les serveurs.	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
Présentation des serveurs Outpost	Ajout de serveurs Outposts, un nouveau AWS Outposts format.	30 novembre 2021

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.