Guide de l'utilisateur pour les serveurs Outposts

AWS Outposts

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

Table of Contents

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

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

Un avant-poste est un pool de capacités de AWS calcul et de stockage déployé sur le site d'un client. AWS exploite, surveille et gère cette capacité dans le cadre d'une AWS région. Vous pouvez créer des sous-réseaux sur votre Outpost et les spécifier lorsque vous créez des AWS ressources telles que des 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 avant-poste à un autre avant-poste ou à une autre zone locale appartenant au même VPC.

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

Concepts clés

Ce sont les concepts clés pour AWS Outposts.

- Site de l'avant-poste — Les bâtiments physiques gérés par le client où AWS sera installé votre avant-poste. Un site doit répondre aux exigences de votre Outpost en matière de locaux, de mise en réseau et d'alimentation.
- Capacité de l'Outpost : ressources de calcul et de stockage disponibles sur l'Outpost. Vous pouvez consulter et gérer la capacité de votre Outpost depuis la AWS Outposts console. AWS Outposts prend en charge la gestion des capacités en libre-service que vous pouvez définir au niveau des Outposts pour reconfigurer tous les actifs d'un Outposts ou spécifiquement pour chaque actif individuel. Un actif Outpost peut être un serveur unique au sein d'un rack Outposts ou d'un serveur Outposts.

- Équipement de l'avant-poste : matériel physique permettant d'accéder au AWS Outposts service. Le matériel comprend les racks, les serveurs, les commutateurs et le câblage détenus et gérés par. AWS
- Racks Outpost : facteur de format Outpost conforme aux normes de l'industrie en matière de rack 42U. Les racks Outposts incluent des serveurs montables en rack, des commutateurs, un panneau de brassage réseau, une étagère d'alimentation et des panneaux vierges.
- Serveurs Outpost : facteur de format Outpost conforme aux normes de l'industrie en matière de serveur 1U ou 2U, qui peut être installé dans un rack à 4 montants conforme à la norme EIA-310D 19. Les serveurs Outposts fournissent des services de calcul et de mise en réseau locaux aux sites dont l'espace est limité ou les besoins en capacité sont moindres.
- Propriétaire de l'avant-poste : titulaire du compte qui passe la AWS Outposts commande. Après AWS s'être engagé avec le client, le propriétaire peut inclure des points de contact supplémentaires. AWS communiquera avec les contacts pour clarifier les commandes, les rendez-vous d'installation, ainsi que la maintenance et le remplacement du matériel. AWS Support Centre de contact en cas de modification des informations de contact.
- Liaison de service — Route réseau qui permet la communication entre votre avant-poste et AWS la région associée. Chaque Outpost est une extension d'une zone de disponibilité et de sa région associée.
- Passerelle locale (LGW) : routeur virtuel d'interconnexion logique qui permet la communication entre un rack Outposts et votre réseau local.
- Interface réseau locale : interface réseau qui permet la communication entre un serveur Outposts et votre réseau local.

AWS ressources sur Outposts

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

Calcul

Type de ressource	Racks	Serveurs
Instances Amazon EC2	O	Oui

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

Base de données et analytique

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

Réseaux

Type de ressource	Racks	Serveurs
Proxy App Mesh Envoy	 O	 Oui

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

Stockage

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

Autres Services AWS

Service	Racks	Serveurs
AWS IoT Greengrass	 O	 Oui

Tarification

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

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

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

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

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

Comment AWS Outposts fonctionne

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

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

Table des matières

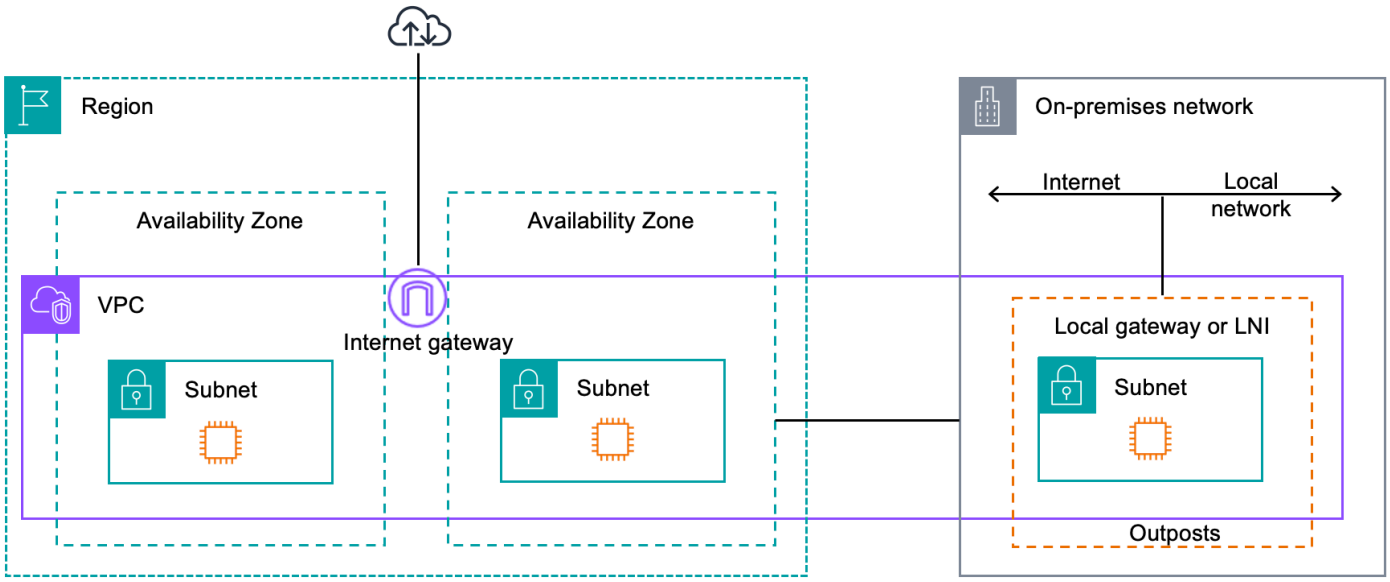
Composants réseau

AWS Outposts étend un Amazon VPC d'une AWS région à un avant-poste avec les composants VPC accessibles dans la région, notamment les passerelles Internet, les passerelles privées virtuelles, les passerelles de transit Amazon VPC et les points de terminaison VPC. Un Outpost est hébergé dans une zone de disponibilité dans la région et est une extension de cette zone de disponibilité que vous pouvez utiliser pour assurer la résilience.

Le diagramme suivant illustre les composants réseau de votre Outpost.

- Un Région AWS et un réseau sur site
- Un VPC constitué de plusieurs sous-réseaux dans la région
- Un Outpost dans le réseau sur site
- La connectivité entre l'avant-poste et le réseau local a fourni :

- Pour les Outposts : une passerelle locale
- Pour les serveurs Outposts : une interface réseau locale (LNI)



VPCs et sous-réseaux

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

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

Chaque Outpost peut en accueillir plusieurs VPCs qui peuvent avoir un ou plusieurs sous-réseaux Outpost. Pour en savoir plus sur les quotas de VPC, consultez Quotas Amazon VPC dans le Guide de l'utilisateur Amazon VPC.

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

Routage

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

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

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

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

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

DNS

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

Les délais de résolution DNS peuvent être plus longs avec Route 53, en fonction de la latence du chemin entre votre avant-poste et la AWS région. Dans ce cas, vous pouvez utiliser les serveurs DNS installés localement dans votre environnement sur site. Pour utiliser vos propres serveurs DNS, vous devez créer des jeux d'options DHCP pour vos serveurs DNS sur site et les associer au VPC. Vous devez également vérifier qu'il existe une connectivité IP avec ces serveurs DNS. Vous devrez peut-être également ajouter des itinéraires à la table de routage de la passerelle locale pour des raisons d'accessibilité, mais cette option n'est possible que pour les racks Outposts dotés d'une passerelle locale. Sachant que les jeux d'options DHCP s'étendent au VPC, les instances situées dans les sous-réseaux Outpost et les sous-réseaux de zone de disponibilité du VPC essaieront d'utiliser les serveurs DNS spécifiés pour la résolution de noms DNS.

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

Liaison de service

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

Votre liaison de service est créée au moment où votre Outpost est provisionné. Si vous disposez d'un facteur de forme de serveur, c'est vous qui créez la connexion. Si vous avez un rack, AWS crée le lien de service. Pour plus d'informations, consultez :

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

Interfaces de réseau local

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

local est réservée aux emplacements sur site. Pour plus d’informations, consultez Interfaces réseau locales pour vos serveurs Outposts.

Exigences du site pour les serveurs Outposts

Un site Outpost est l'emplacement physique où opère votre Outpost. Les sites sont uniquement disponibles dans certains pays et territoires. Pour plus d'informations, consultez la section AWS Outposts serveurs FAQs. 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 aux racks Outposts, consultez la section Exigences du site pour les racks Outposts dans le Guide de l'utilisateur AWS Outposts pour les racks Outposts.

Table des matières

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 des 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. 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 36 pouces (914 mm). AWS fournit un kit de rails pour le montage en rack du serveur.
  - 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)
  - 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

  Si vous ne placez pas le serveur dans un rack, vous devez tout de même satisfaire aux autres exigences du site.
- 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.

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
UDP	443, 1024-65535	Adresse IP de la liaison de service	443	Points de terminaison Outposts Service Link
TCP	1024-65535	Adresse IP de la liaison de service	443	Points de terminaison d'enregistrement des Outposts

Vous pouvez utiliser une 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 le lien de service, consultez la section AWS Outposts connectivité aux AWS régions dans le guide de AWS Outposts l'utilisateur pour les serveurs.

Recommandations concernant la bande passante de la liaison de service

Pour une expérience et une résilience optimales, AWS vous devez utiliser une connectivité redondante d'au moins 500 Mbits/s et une latence aller-retour maximale de 175 ms pour la connexion par liaison de service à la AWS région. L'utilisation maximale de chaque serveur Outposts est de 500 Mbits/s. Pour augmenter la vitesse de connexion, utilisez plusieurs serveurs Outposts. 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 la section Trafic des liaisons de service pour les serveurs dans le guide de AWS Outposts l'utilisateur 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 AMIs. AMIs sont téléchargés 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.

Alimentation

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

Exigences

- Soutien en 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 cordon d'alimentation IEC C13 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 la section Trafic des liaisons de service pour les serveurs dans le guide de AWS Outposts l'utilisateur pour les serveurs.

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

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

Tâches

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

Création d’un Outpost et commande de capacité Outpost

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

Conditions préalables

- 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 de plus amples informations, veuillez consulter Exigences du site pour les serveurs Outposts.
- Vous devez disposer d'un plan AWS Enterprise Support ou d'un plan AWS Enterprise On-Ramp Support.
- Déterminez Compte AWS celui que vous utiliserez pour créer le site Outposts, créer l'Outpost et passer la commande. Surveillez l'e-mail associé à ce compte pour obtenir des informations provenant de AWS.

Tâches

- Étape 1 : Créer un site
- Étape 2 : 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.

Conditions préalables

- Déterminez l'adresse d'exploitation.

Pour créer un site

1. Connectez-vous à AWS.
2. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.
3. Pour sélectionner le parent Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page.
4. Dans le panneau de navigation, choisissez Sites.
5. Choisissez Créer un site.
6. Pour Type de matériel pris en charge, 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.

Conditions préalables

- 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.

> **Note**
>
> Vous ne pourrez pas modifier l'ancre AZ ou l'emplacement physique de votre avant-poste une fois la commande terminée.

Étape 3 : Passer la commande

Passez une commande pour les serveurs Outposts dont vous avez besoin.

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

Conditions préalables

- 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 de paiement initial partiel ou sans paiement initial, vous paierez des frais mensuels pendant toute la durée.

  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'instances après avoir passé la 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 relative au type d'instance.
7. Pour chaque type d'instance, assurez-vous que la quantité d'instances est spécifiée pour au moins une taille d'instance.
8. Choisissez Suivant.
9. Sur la page Réviser et créer, vérifiez les mises à jour que vous demandez.
10. Choisissez Create. 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. Après avoir 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 Create. 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. Après avoir 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. Si vous avez des questions concernant votre commande, contactez le AWS Support centre.

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 le guide d'installation du serveur.

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

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

Lancez une instance sur votre serveur Outposts

Dès lors que votre Outpost est installé et que la capacité de calcul et de stockage est prête à être utilisée, vous pouvez vous lancer en créant des ressources. 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 de plus amples informations, veuillez consulter Composants réseau.

> **Note**
>
> Si vous lancez une instance dans un sous-réseau Outpost qui a été partagée avec vous par un autre Compte AWS, passez 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, vous devez l'activer pour les interfaces réseau locales. Utilisez la commande modify-subnet-attribute à partir de l' AWS CLI. 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. L'exemple suivant utilise la valeur 1 pour spécifier une interface réseau secondaire.

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

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 avec suffisamment de stockage pour répondre aux besoins de votre application. Pour plus d'informations, consultez les sections Volumes de stockage d'instance et Création d'une AMI sauvegardée par le stockage d'instance dans le guide de l'utilisateur Amazon EC2.
- Vous devez utiliser une AMI basée sur Amazon EBS avec un seul instantané EBS. AMIs avec plusieurs instantanés EBS ne sont pas pris 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 utiliser des blocs de données ou des volumes de démarrage soutenus par un stockage tiers compatible, vous devez approvisionner et configurer ces volumes pour les utiliser avec des instances EC2 sur Outposts. Pour de plus amples informations, veuillez consulter Stockage par blocs tiers.
- 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. Notez que les instances qui apparaissent grisées ne sont pas disponibles.
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 du périphérique d'interface réseau local pour le sous-réseau Outpost, cette interface réseau est l'interface réseau locale de l'instance. Vous pouvez également l'ajouter ultérieurement à la sectionAjout d'une interface réseau locale.
7. (Facultatif) Vous pouvez ajouter un volume de données tiers.
   a. Développez et configurez le stockage. À côté de Volume de stockage externe, choisissez Modifier.
   b. Pour le protocole réseau de stockage, choisissez iSCSI.
   c. Entrez l'IQN de l'initiateur, puis ajoutez l'adresse IP cible, le port et l'IQN de la baie de stockage externe.
8. Suivez les étapes de l'assistant pour lancer l'instance dans votre sous-réseau Outpost. Pour plus d'informations, consultez Lancer une instance EC2 dans le guide de l'utilisateur Amazon EC2 :

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 de plus amples informations, veuillez consulter Ajout d'une interface réseau locale.

Vous devez configurer l'interface de réseau local pour l'instance avec une adresse IP de votre réseau local. 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 EC2, consultez la section Connect to your EC2 User Guide du guide de l'utilisateur Amazon EC2.

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
```

AWS Outposts connectivité aux AWS régions

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

> **Note**
>
> Vous ne pouvez pas utiliser la connectivité privée pour votre connexion par lien de service qui connecte votre serveur Outposts à votre AWS région ou à votre région d' AWS Outposts origine.

Table des matières

Connectivité via un lien de service

Pendant le AWS Outposts provisionnement, vous créez ou AWS créez une connexion par lien de service qui connecte votre serveur Outposts à la région que vous AWS avez choisie ou à la région d'origine. La liaison de service est un jeu chiffré des connexions VPN qui sont utilisées chaque fois que l'Outpost communique avec la région d'origine choisie. Vous pouvez utiliser un réseau local virtuel (VLAN) pour segmenter le trafic sur la liaison de service. La liaison de service VLAN permet la communication entre l'avant-poste et la AWS région pour la gestion de l'avant-poste et le trafic intra-VPC entre la région et l'avant-poste. AWS

L'Outpost est en mesure de créer le VPN de la liaison de service vers la région AWS via une connectivité régionale publique. Pour ce faire, l'Outpost a besoin d'être connecté aux plages d'adresses IP publiques de la AWS région, soit via l'Internet public, soit via une interface virtuelle AWS Direct Connect publique. 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 les plages d'adresses AWS IP dans le guide de l'utilisateur Amazon VPC.

Une fois le lien de service établi, l'avant-poste 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'avant-poste et tout ce qui y est associé VPCs, y compris le trafic du plan de données 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.

Notez ce qui suit :

- Le réseau doit prendre en charge une MTU de 1 500 octets entre l'avant-poste et les points de terminaison des liaisons de service dans la région parent. AWS
- Le trafic qui passe d'une instance d'Outposts à une instance de la région a une MTU de 1 300 octets, ce qui est inférieur à la MTU requise de 1 500 octets en raison des surcharges de paquets.

Recommandations concernant la bande passante de la liaison de service

Pour une expérience et une résilience optimales, AWS vous devez utiliser une connectivité redondante d'au moins 500 Mbits/s et une latence aller-retour maximale de 175 ms pour la connexion par liaison de service à la AWS région. L'utilisation maximale de chaque serveur Outposts est de 500 Mbits/s. Pour augmenter la vitesse de connexion, utilisez plusieurs serveurs Outposts. Par exemple, si vous avez trois AWS Outposts serveurs, la vitesse de connexion maximale passe à 1,5 Gbit/s (1 500 Mbits/s). Pour plus d'informations, consultez la section Trafic des liaisons 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 AMIs. AMIs sont téléchargés depuis la Région à chaque lancement d'instance.

Nous vous recommandons vivement de consulter votre représentant AWS commercial ou votre partenaire APN pour évaluer les options de région d'origine disponibles dans votre zone géographique et obtenir une recommandation personnalisée concernant les exigences de bande passante et de latence des liaisons de service pour vos charges de travail.

Connexions Internet redondantes

Lorsque vous établissez une connectivité entre votre avant-poste et la AWS région, nous vous recommandons de créer plusieurs connexions pour une disponibilité et une résilience accrues. Pour plus d'informations, consultez Recommandations relatives à la résilience 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.

Mises à jour et liaison de service

AWS maintient une connexion réseau sécurisée entre votre serveur Outposts et sa région parente AWS . 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 AWS Well-Architected et en veillant à ce que vos applications résistent aux défaillances ou aux activités de maintenance affectant un seul serveur Outposts.

Pare-feu et liaison de service

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

Dans le schéma suivant, la configuration étend le VPC Amazon de la AWS région à l'avant-poste. Une interface virtuelle Direct Connect publique est la connexion du lien de service. Le trafic suivant transite par la liaison de service et la connexion Direct Connect :

- Trafic de gestion à destination de l'Outpost via la liaison de service
- Trafic entre l'avant-poste et tout ce qui y est associé VPCs

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

Si vous utilisez un pare-feu dynamique compatible UDP et TCP pour limiter la connectivité concernant le VLAN de liaison de service, vous pouvez refuser toutes les connexions entrantes. Si le pare-feu agit de manière dynamique, les connexions sortantes autorisées depuis le lien du service Outposts devraient automatiquement autoriser le trafic de réponse à revenir sans configuration de règles explicite. Seules les connexions sortantes initiées à partir du lien du service Outpost doivent être configurées comme autorisées.

Protocole	Port source	Adresse source	Port de destination	Adresse de destination
UDP	1024-65535	Adresse IP de la liaison de service	53	serveur DNS
UDP	443, 1024-65535	Adresse IP de la liaison de service	443	AWS Outposts Points de terminaison Service Link
TCP	1024-65535	Adresse IP de la liaison de service	443	AWS Outposts Points de terminaison d'enregistrement

Si vous utilisez un pare-feu non statique pour limiter la connectivité concernant le VLAN de liaison de service, vous devez autoriser les connexions sortantes initiées depuis le lien de service Outposts vers les réseaux publics de la région. AWS Outposts Vous devez également autoriser explicitement le trafic de réponse entrant depuis les réseaux publics de la région des Outposts vers le VLAN de liaison de service. La connectivité est toujours initiée depuis le lien de service Outposts, mais le trafic de réponse doit être autorisé à revenir dans le VLAN de liaison de service.

Protocole	Port source	Adresse source	Port de destination	Adresse de destination
UDP	1024-65535	Adresse IP de la liaison de service	53	Serveur DNS
UDP	443, 1024-65535	Adresse IP de la liaison de service	443	AWS Outposts Points de terminaison Service Link
TCP	1025-65535	Adresse IP de la liaison de service	443	AWS Outposts Points de terminaison Service Link
UDP	53	Serveur DNS	1025-65535	Adresse IP de la liaison de service
UDP	443	AWS Outposts Points de terminaison Service Link	443, 1024-65535	Adresse IP de la liaison de service
TCP	443	AWS Outposts Points de terminaison Service Link	1025-65535	Adresse IP de la liaison de service

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

Dépannage du réseau du serveur Outposts

Utilisez cette liste de contrôle pour résoudre les problèmes liés à une liaison de service dont le statut est `DOWN`.

Évaluation initiale

Vérifiez l'état du lien de service via CloudWatch les métriques Amazon :

1. Surveillez la ConnectedStatusmétrique dans l'espace de AWS Outposts noms.
2. Si la valeur moyenne est inférieure à 1, cela confirme que le lien de service est perturbé.
3. Si le lien de service est perturbé, suivez les étapes décrites dans les sections suivantes pour résoudre et rétablir la connexion.

Étape 1. Vérifiez la connectivité physique

1. Vérifiez que vous utilisez le câble de dérivation QSFP fourni. Si le problème persiste, testez avec un autre câble de dérivation QSFP, le cas échéant.
2. Vérifiez que le câble de dérivation QSFP du serveur Outposts est bien branché.
3. Vérifiez que le câble 1 (LNI) est bien inséré dans le commutateur.
4. Vérifiez que le câble 2 (liaison de service) est bien inséré dans le commutateur.
5. Effectuez une vérification générale du bon fonctionnement du commutateur, par exemple en vérifiant les voyants des liaisons.

Étape 2. Testez la connexion du serveur Outposts à AWS

Créez une connexion série avec le serveur Outposts et effectuez les tests suivants :

1. Testez les liens.

a. En cas de succès, passez au test suivant.

b. En cas d'échec,Vérifier la configuration du réseau.

2. Testez la résolution DNS.

a. En cas de succès, passez au test suivant.

b. En cas d'échec,Vérifiez les règles du pare-feu.

3. Testez l'accès à la AWS région.

a. En cas de succès, rétablissez la connexion.

b. En cas d'échec,Vérifiez le MTU.

Vérifier la configuration du réseau

Assurez-vous que votre commutateur répond aux spécifications suivantes :

- Configuration de base — Le port de liaison de service doit être un port d'accès non balisé à un VLAN doté d'une passerelle et d'une route vers les points de terminaison AWS.
- Vitesse de liaison — La vitesse de liaison du port du commutateur doit être réglée sur 10 Go et la négociation automatique doit être désactivée.

Vérifiez le MTU

Le réseau doit prendre en charge une MTU de 1 500 octets entre l'avant-poste et les points de terminaison des liaisons de service dans la région parent. AWS Pour plus d'informations sur le lien de service, consultez la section AWS Outposts Connectivité aux AWS régions.

Vérifiez les règles du pare-feu

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

Protocole	Port source	Adresse source	Port de destination	Adresse de destination
UDP	1024-65535	Adresse IP de la liaison de service	53	serveur DNS
UDP	443, 1024-65535	Adresse IP de la liaison de service	443	AWS Outposts Points de terminaison Service Link
TCP	1024-65535	Adresse IP de la liaison de service	443	AWS Outposts Points de terminaison d'enregistrement

Étape 3. Rétablissez la connectivité

Si les vérifications précédentes réussissent mais que le lien de service ConnectedStatusest maintenu `DOWN` (moins de 1 entrée CloudWatch), suivez les étapes décrites dans Autoriser le serveur Outposts à l'aide de l'outil de configuration Outpost pour rétablir la connexion.

> **Note**
>
> Si le lien de service reste inactif, créez un dossier au AWS Support Centre.

Retourner un serveur Outposts

> **Note**
>
> Si vous avez reçu un serveur endommagé lors de l'expédition, reportez-vous à l'étape 2 : Inspecter l'équipement du serveur Outposts dans le guide d'installation du AWS Outposts serveur.
> Pour renvoyer un serveur en cours d'utilisation que vous souhaitez remplacer ou un serveur dont l'abonnement a pris fin, consultez cette section.

En AWS Outposts cas de détection d'un défaut sur un serveur, nous vous en informerons, lancerons le processus de remplacement pour vous envoyer un nouveau serveur et vous fournirons l'étiquette de retour via la AWS Outposts console. Aucuns frais d'expédition ne vous seront facturés lorsque vous renverrez un serveur Outposts. Toutefois, si vous retournez un serveur endommagé, des frais peuvent vous être facturés.

Pour commencer, suivez les étapes ci-dessous.

Tâches

Étape 1 : préparer le serveur pour le retour

Pour préparer le serveur pour le renvoi, 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’Outpost sont partagées, vous devez annuler le partage de ces ressources.

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

   - Utilisez la AWS RAM console. Pour plus d’informations, consultez Mise à jour d’un partage de ressources dans le Guide de l’utilisateur AWS RAM .

- Utilisez le AWS CLI pour exécuter la disassociate-resource-sharecommande.

Pour consulter la liste des ressources Outpost qui peuvent être partagées, consultez Ressources Outpost partageables.

2. Créez des sauvegardes des données stockées dans le stockage d'instance des EC2 instances Amazon exécutées sur le AWS Outposts serveur.
3. Supprimez les interfaces réseau locales associées aux instances qui s'exécutaient sur le serveur.
4. Résiliez les instances actives associées aux sous-réseaux sur votre Outpost. Pour mettre fin aux instances, suivez les instructions de la section Résiliation de votre instance dans le guide de EC2 l'utilisateur Amazon.
5. Détruisez la clé de sécurité Nitro (NSK) pour détruire cryptographiquement vos données sur le serveur. Pour détruire le NSK, suivez les instructions de la section Déchiqueter cryptographiquement les données du serveur.

Étape 2 : Imprimez l'étiquette de retour

> **Important**
>
> Vous ne devez utiliser que l'étiquette de retour AWS fournie car elle contient des informations spécifiques, telles que l'identifiant de l'actif, sur le serveur que vous renvoyez. Ne créez pas votre propre étiquette de retour.

Pour obtenir votre étiquette de retour :

1. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.
2. Dans le panneau de navigation, choisissez Commandes.
3. Choisissez la commande pour le serveur que vous souhaitez renvoyer.
4. Sur la page des détails de la commande, dans la section État de la commande, choisissez Imprimer l'étiquette de retour.

> **Note**
>
> Le retour de vos serveurs Outposts avant la fin de l'abonnement en cours n'annulera pas les frais impayés associés à cet Outpost.

Étape 3 : emballer le serveur

Pour emballer votre serveur, utilisez la boîte et le matériel d'emballage fournis par AWS.

1. Placez le serveur dans l'une des boîtes suivantes :

   - La boîte et le matériel d'emballage dans lesquels le serveur est arrivé à l'origine.
   - La boîte et le matériel d'emballage dans lesquels le serveur de remplacement est arrivé.

   Vous pouvez également contacter le Centre AWS Support pour demander une boîte.
2. Apposez l'étiquette de retour AWS fournie à l'extérieur de la boîte.

   > **Important**
   >
   > Vérifiez que l'ID d'actif sur l'étiquette de retour correspond à l'ID d'actif sur le serveur que vous retournez.
   > L'identifiant de l'actif se trouve sur l'onglet déroulant situé à l'avant du serveur. Exemple : `1203779889` ou `9305589922`
3. Fermez bien la boîte.

Étape 4 : Retourner 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 service de messagerie ou planifier le jour et l'heure que vous préférez pour que le coursier vienne chercher le serveur. L'étiquette de retour AWS fournie contient l'adresse correcte pour renvoyer le serveur.

Le tableau suivant indique les personnes à contacter pour le pays depuis lequel a lieu l'expédition :

Pays	Contact
Argentine	Centre AWS Support de contact. Dans la demande, fournissez les informations suivantes : • Le numéro de suivi figurant sur l'étiquette de retour AWS fournie • La date et l'heure auxquelles vous préférez que le coursier vienne chercher le serveur • Un nom de contact • Un numéro de téléphone • Une adresse e-mail
Bahreïn	
Brésil	
Brunei	
Canada	
Chili	
Colombie	
Hong Kong	
Inde	
Indonésie	
Japon	
Malaisie	
Nigeria	
Oman	
Panama	
Pérou	
Philippines	
Serbie	
Singapour	
Afrique du Sud	

Pays	Contact
Corée du Sud	
Taïwan	
Thaïlande	
Emirats arabes unis	
Vietnam	
Mexique	AWS contacte DB Schenker et demande qu'on vienne le chercher chez vous. DB Schenker vous contacte ensuite pour fixer la date et l'heure du ramassage.
États-Unis	Contactez UPS. Vous pouvez renvoyer le serveur des manières suivantes : • Renvoyez le serveur lors d'une collecte UPS de routine sur votre site. • Déposez le serveur chez UPS. • Planifiez une collecte à la date et à l'heure que vous préférez. Entrez le numéro de suivi figurant sur l'étiquette de retour AWS fournie pour la livraison gratuite.

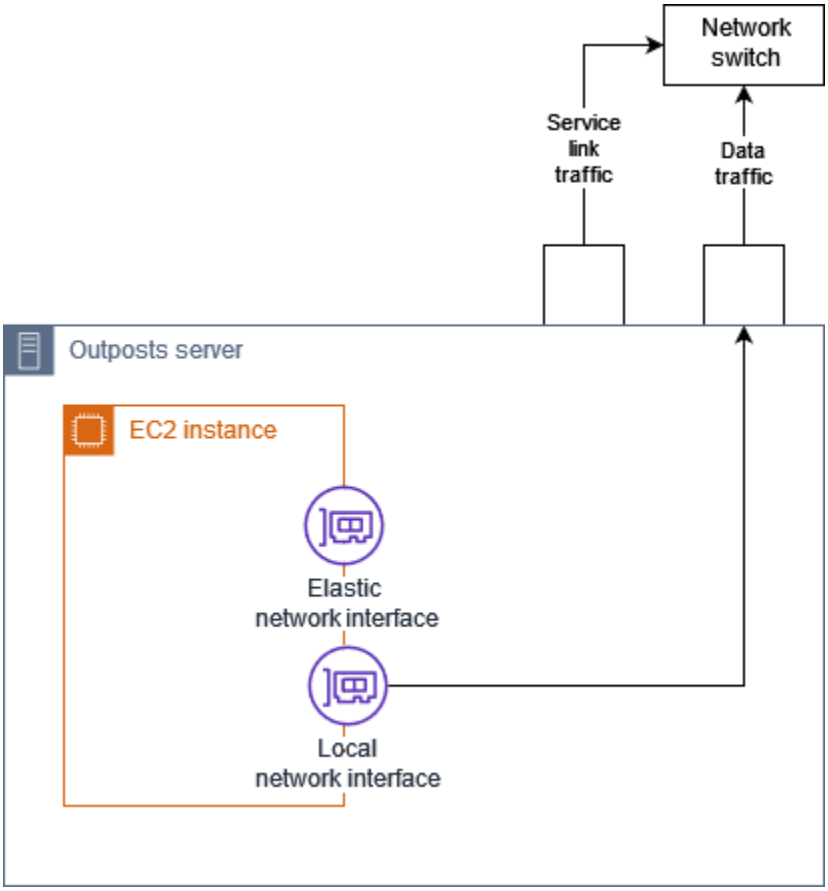
Pays	Contact
Tous les autres pays	Contactez DHL. Vous pouvez renvoyer le serveur des manières suivantes : • Déposez le serveur chez DHL. • Planifiez une collecte à la date et à l'heure que vous préférez. Entrez le numéro de bordereau DHL figurant sur l'étiquette de retour AWS fournie pour une livraison gratuite. Si l'erreur suivante s'affiche : `Courier pickup can't 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 de renvoi. Sélectionnez le pays à partir duquel le renvoi est réalisé et réessayez.

Interfaces réseau locales pour vos serveurs Outposts

Avec les serveurs Outposts, une interface réseau locale 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 AWS Outposts connectivité aux AWS régions.

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 Outposts 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 la section Quotas d'interface 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 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 Outposts.
- Les interfaces réseau locales ne prennent pas en charge le mode promiscuité ou l'usurpation d'adresse MAC.

Performance

L'interface réseau locale de chaque taille d'instance fournit une partie de la bande passante physique disponible de 10 GbE. Le tableau suivant répertorie les performances du réseau 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.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
c6id.16xlarge	5	5
c6id.24xlarge	7,5	7,5

Type d’instance	Bande passante de référence (Gbit/s)	Bande passante de rafale (Gbit/s)
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.

Contrôle

CloudWatch des métriques sont produites pour chaque interface réseau locale, tout comme elles le sont pour les interfaces réseau élastiques. Pour plus d'informations, consultez la section Surveiller les performances du réseau pour les paramètres ENA sur votre instance EC2 dans le guide de l'utilisateur Amazon EC2.

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.

Ajouter une interface réseau locale à une instance EC2 dans un sous-réseau Outposts

Vous pouvez ajouter une interface réseau locale 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.

Utilisez la procédure suivante pour ajouter l'interface réseau locale après le lancement de l'instance. Pour plus d'informations sur son ajout lors du lancement d'une instance, consultez Lancer une instance sur l'Outpost.

Pour ajouter une interface réseau locale à une instance EC2

1. Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Réseau et sécurité; Interfaces réseau.
3. 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' IPv4 adresse privée est définie sur Attribuer automatiquement.
    d. Sélectionnez un groupe de sécurité. Les groupes de sécurité ne s'appliquant pas à l'interface réseau locale, le groupe de sécurité que vous sélectionnez n'est pas pertinent.
    e. Sélectionnez Create network interface (Créer une interface réseau).

4. 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 pour l'interface réseau locale du 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 IPv4 adresse privée pour l'interface réseau locale à partir du sous-réseau CIDR. Cette adresse n'est pas l'adresse IP de l'interface réseau locale et elle 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 au sein du système d'exploitation client, 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 Outposts

Utilisez cette rubrique pour comprendre les exigences en matière de câblage réseau et de topologie pour héberger un serveur Outposts. Pour de plus amples informations, veuillez consulter Interfaces réseau locales pour vos serveurs Outposts.

Table des matières

- Connectivité physique du serveur
- Trafic de liaison de service pour les serveurs
- Trafic de liaison d'interface réseau local
- Attribution d’adresse IP de serveur
- Enregistrement du serveur

Topologie du serveur sur votre réseau

Un serveur Outposts 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 de trafic et les libellés du serveur Outposts.

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. Le lien de service est un VPN personnalisé ou VPNs relie l'Outpost à la région. L’Outpost se connecte à la zone de disponibilité de la région que vous avez choisie au moment de l’achat.
1	Trafic de liaison d'interface réseau local : ce trafic permet la communication entre votre VPC et votre réseau local via l'interface 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

Étiquette de trafic	Description
	des instances qui communiquent avec Internet via votre réseau sur site.

Connectivité physique du serveur

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.

- 10 GbE : type de connecteur QSFP+

Câble QSFP+

Le câble QSFP+ possède un connecteur que vous pouvez connecter au port 3 du serveur Outposts. 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 Outposts. Utilisez l'2interface pour le trafic de liaison de service et l'1interface pour le trafic de liaison d'interface réseau local. 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 Outposts 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

Trafic de liaison d'interface réseau local

Configurez le port de liaison d'interface réseau local sur 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 interface réseau locale 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 interface réseau locale 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 interface réseau locale 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 d'ec2-net-utils dans AL2 le guide de l'utilisateur Amazon Linux 2.
- 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 pour le lien de service du AWS Outposts serveur et les interfaces réseau locales sur les instances. Pour le lien de service, vous pouvez attribuer des adresses IP manuellement ou utiliser le protocole DHCP (Dynamic Host Control Protocol). Pour configurer la connexion Service Link, voir Configurer et tester la connexion dans le guide d'installation AWS Outposts du serveur.

Pour configurer le lien d'interface réseau local, consultezthe section called "Configuration du système d'exploitation".

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

Enregistrement du serveur

Lorsque les serveurs Outposts établissent une connexion sur le réseau local, ils utilisent la connexion Service Link pour se connecter aux points 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 Outposts utilisent le port TCP 443 pour faciliter la communication avec la région via l'Internet public. Les serveurs Outposts ne prennent pas en charge la connectivité privée via VPC.

Gestion des capacités pour AWS Outposts

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

Rubriques

Afficher la AWS Outposts capacité

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

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

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

Modifier la capacité de l' AWS Outposts instance

La capacité de chaque nouvelle commande Outpost est configurée avec une configuration de capacité par défaut. Vous pouvez convertir la configuration par défaut pour créer différentes instances répondant aux besoins de votre entreprise. Pour ce faire, vous devez créer une tâche de capacité, choisir un Outposts ou un actif unique, spécifier les tailles et le nombre d'instances, puis exécuter la tâche de capacité pour mettre en œuvre les modifications.

Considérations

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

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

- Vous ne pouvez modifier la configuration de capacité de vos Outposts existante que pour utiliser des tailles d'instance Amazon EC2 valides issues de familles d'instances prises en charge par votre modèle d'actif respectif.
- Si vous avez des instances en cours d'exécution sur votre avant-poste et que vous ne souhaitez pas les arrêter pour exécuter une tâche de capacité, sélectionnez leur ID d'instance respectif dans la section Instances à conserver telles quelles — facultatif et assurez-vous de conserver la quantité nécessaire de cette taille d'instance dans votre configuration de capacité mise à jour. Cela permettra de conserver les instances utilisées pour prendre en charge les charges de travail de production pendant l'exécution d'une tâche de capacité.
- Lorsque vous configurez un actif avec plusieurs tailles d'instance au sein d'une même famille d'instances, utilisez Auto-balance pour vous assurer que vous n'essayez pas de surprovisionner ou de sous-approvisionner votre droplet. Le surprovisionnement n'est pas pris en charge et entraînera une défaillance de la tâche de capacité.
- Plusieurs tâches de capacité peuvent être exécutées en parallèle tant qu'elles s'appliquent à des ensembles d'actifs qui s'excluent mutuellementIDs. Par exemple, vous pouvez créer plusieurs tâches de capacité au niveau des actifs pour différents actifs IDs en même temps. Toutefois, si une tâche de niveau Outpost est en cours d'exécution, vous ne pouvez pas créer une autre tâche au niveau de l'Outpost ou de l'actif en même temps. De même, si une tâche au niveau de l'actif est en cours d'exécution, vous ne pouvez pas créer une tâche au niveau Outpost ou une tâche au niveau de l'actif sur le même AssetID en même temps.

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

1. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.
2. Dans le volet de navigation de gauche, sélectionnez Capacity tasks.
3. Sur la page Tâches de capacité, choisissez Créer une tâche de capacité.
4. Sur la page de démarrage, choisissez la commande, l'Outpost ou l'actif à configurer.
5. Pour modifier la capacité, spécifiez une option pour Méthode de modification : e steps dans la console ou téléchargez un fichier JSON.
   - Modifiez le plan de configuration de la capacité pour suivre les étapes de la console
   - Téléchargez un plan de configuration de capacité pour télécharger un fichier JSON

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

Console steps

1. Choisissez la vue Instance ou la vue Rack.
2. Choisissez Modifier la configuration de la capacité d'un avant-poste ou Modifier sur un seul actif.
3. Choisissez un avant-poste ou un actif s'il est différent de la sélection actuelle.
4. Choisissez d'exécuter cette tâche de capacité immédiatement ou régulièrement pendant 48 heures.
5. Choisissez Suivant.
6. Sur la page Configurer la capacité de l'instance, chaque type d'instance indique une taille d'instance avec la quantité maximale présélectionnée. Pour ajouter d'autres tailles d'instance, choisissez Ajouter une taille d'instance.
7. Spécifiez la quantité d'instance et notez la capacité affichée pour cette taille d'instance.
8. Consultez le message à la fin de chaque section sur le type d'instance qui vous indique si votre capacité est dépassée ou insuffisante. Effectuez des ajustements au niveau de la taille ou de la quantité de l'instance pour optimiser votre capacité totale disponible.
9. Vous pouvez également demander AWS Outposts à optimiser la quantité d'instances pour une taille d'instance spécifique. Pour ce faire :
    a. Choisissez la taille de l'instance.
    b. Choisissez Auto-balance à la fin de la section sur le type d'instance correspondante.
10. Pour chaque type d'instance, assurez-vous que la quantité d'instances est spécifiée pour au moins une taille d'instance.
11. Choisissez éventuellement les instances à conserver telles quelles.
12. Choisissez Suivant.
13. Sur la page Réviser et créer, vérifiez les mises à jour que vous demandez.
14. Choisissez Créer. AWS Outposts crée une tâche de capacité.

15. Sur la page de la tâche de capacité, surveillez l'état de la tâche.

Upload a JSON file

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

   Example

   Exemple de fichier JSON :

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

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

Résolution des problèmes liés aux tâches de capacité

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

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

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

Pour résoudre ce problème :

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

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

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

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

Utilisation de la console

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

Utilisation de l'interface de ligne de commande

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

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

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

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

Pour résoudre ce problème :

1. Notez la AWS région que vous avez utilisée dans la demande `StartCapacityTask` d'API.
2. Utilisez l'action `ListOutposts`API pour obtenir la liste des Outposts que vous possédez dans la AWS région.
3. Vérifiez si l'identifiant de l'Outpost est répertorié.

4. Entrez l'ID Outpost correct dans la `StartCapacityTask` demande.
5. Si vous ne trouvez pas l'identifiant de l'avant-poste, utilisez à nouveau l'action de l'`ListOutpostsAPI` pour vérifier si l'avant-poste existe dans une autre AWS région.

CapacityTask Casquette active- *XXXX* déjà trouvée pour Outpost op- *XXXX*

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

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

Utilisation de la console

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

Utilisation de l’interface de ligne de commande

1. Utilisez la ListCapacityTaskscommande pour rechercher les tâches relatives à la capacité de fonctionnement de l'avant-poste.
2. Attendez que toutes les tâches de capacité en cours soient terminées ou annulez-les si vous le souhaitez.
3. Lorsqu'aucune tâche de capacité n'est en cours pour la demande OutpostId, réessayez de créer la tâche de capacité.

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

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

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

Utilisation de la console

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

Utilisation de l’interface de ligne de commande

1. Utilisez la ListCapacityTaskscommande pour rechercher les tâches de capacité d'exécution pour OutpostID et AssetID.
2. Assurez-vous qu'aucune tâche de capacité au niveau de l'Outpost n'est en cours d'exécution pour le OutpostId, et qu'aucune tâche de capacité au niveau des actifs n'est en cours d'exécution pour le. AssetId
3. Si des tâches de capacité sont en cours d'exécution, attendez qu'elles se terminent ou annulez-les si vous le souhaitez.
4. Réessayez votre demande pour créer la tâche de capacité.

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

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

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

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

Utilisation de la console

1. Connectez-vous à AWS.
2. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.
3. Choisissez Rack view pour l'Outpost.
4. Vérifiez que la demande AssetId est associée à l'avant-poste et qu'elle n'est pas marquée comme hôte isolé.

    a. Si l'actif est isolé, cela peut être dû au fait qu'une tâche de capacité est en cours d'exécution sur celui-ci. Vous pouvez accéder au panneau des tâches de capacité et vérifier si des tâches au niveau de l'avant-poste ou des actifs sont en cours d'exécution pour le et. OutpostId AssetId Si tel est le cas, attendez que la tâche soit terminée et que la ressource soit de nouveau disponible.

    b. S'il n'existe aucune tâche de capacité d'exécution pour un actif isolé, celui-ci peut être dégradé.
5. Après avoir vérifié que l'actif existe et est dans un état valide, réessayez votre demande pour créer la tâche de capacité.

Utilisation de l’interface de ligne de commande

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

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

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

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

Partagez vos AWS Outposts ressources

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

Dans ce modèle, le AWS compte propriétaire des ressources Outpost (propriétaire) partage les ressources avec d'autres AWS comptes (consommateurs) de la même organisation. Les consommateurs peuvent créer des ressources sur des Outposts partagés avec eux comme ils le feraient sur des Outposts créés dans leur propre compte. Le propriétaire est responsable de la gestion de l'Outpost et des ressources qu'il y crée. Les propriétaires peuvent modifier ou révoquer l'accès partagé à tout moment. À l'exception des instances qui consomment des réserves de capacité, les propriétaires peuvent également afficher, modifier et supprimer des ressources que les consommateurs créent sur des Outposts partagés. Les propriétaires ne peuvent pas modifier les instances que les consommateurs lancent dans Capacity Reservations qu'ils ont partagées.

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

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

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

Table des matières

- Partage sur plusieurs zones de disponibilité
- Partage d’une ressource Outpost
- Annulation du partage d’une ressource Outpost
- Identification d’une ressource Outpost partagée
- Autorisations relatives aux ressources Outpost partagées
- Facturation et mesures
- Limitations

Ressources Outpost partageables

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

Pour les ressources du serveur Outposts, consultez la section Utilisation de ressources partagées AWS Outposts.

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

- Hôtes dédiés alloués : les consommateurs ayant accès à cette ressource peuvent :
  - Lancer et exécuter des instances EC2 sur un hôte dédié.
- Outposts : les consommateurs ayant accès à cette ressource peuvent :
  - Créer et gérer des sous-réseaux sur l’Outpost.
  - Utilisez l' AWS Outposts API pour consulter les informations relatives à l'Outpost.
- Sites : les consommateurs ayant accès à cette ressource peuvent :
  - Créer, gérer et contrôler un Outpost sur le site.
- Sous-réseaux : les consommateurs ayant accès à cette ressource peuvent :
  - Afficher des informations sur les sous-réseaux.
  - Lancer et exécuter des instances EC2 dans des sous-réseaux.

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

Conditions préalables requises pour le partage de ressources Outposts

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

Services connexes

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

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

Partage sur plusieurs zones de disponibilité

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

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

Pour consulter les IDs zones de disponibilité de votre compte

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

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

Partage d'une ressource Outpost

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

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

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

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

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

1. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.
2. Dans le panneau de navigation, choisissez Outposts.
3. Sélectionnez l'Outpost, puis choisissez Actions, Afficher les détails.
4. Sur la page Récapitulatif de l'Outpost, choisissez Partages de ressources.
5. Choisissez Créer une ressource.

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

Pour partager 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

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

- Affichez l'Outpost dans la AWS Outposts console.
- Créez de nouveaux sous-réseaux sur l'Outpost.
- Créez de nouveaux volumes Amazon EBS sur l'Outpost.
- Consultez les détails de l'Outpost et les types d'instances à l'aide de la AWS Outposts console ou du AWS CLI.

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

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

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

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

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

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

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

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

Utilisez la commande disassociate-resource-share.

Identification d’une ressource Outpost partagée

Les propriétaires et les consommateurs peuvent identifier les Outposts partagés à l'aide de la AWS Outposts console et. AWS CLI Ils peuvent identifier les tables de routage de passerelle locale partagées à l’aide de l’ AWS CLI.

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

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

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

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

Autorisations relatives aux ressources Outpost partagées

Autorisations accordées aux propriétaires

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

Autorisations accordées aux consommateurs

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

Facturation et mesures

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

Le partage de tables de routage de passerelle locale n'entraîne pas de frais supplémentaires. Pour les sous-réseaux partagés, le propriétaire du VPC est facturé pour les ressources de niveau VPC Direct Connect telles que les connexions VPN, les passerelles NAT et les connexions de liaison privée.

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

Limitations

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

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

Avec les serveurs Outposts, vous pouvez exploiter les données existantes que vous stockez sur des baies de stockage tierces. Vous pouvez spécifier des volumes de données par blocs externes et des volumes de démarrage par blocs externes pour vos instances EC2 sur Outposts. Grâce à cette intégration, vous pouvez utiliser des données par blocs et des volumes de démarrage externes soutenus par des fournisseurs tiers tels que Dell PowerStore, HPE Alletra Storage MP B10000, des baies de stockage d'entreprise NetApp sur site et des systèmes de stockage Pure Storage. FlashArray

Considérations

- Disponible sur les racks Outposts et les serveurs Outposts 2U. Non disponible sur les serveurs Outposts 1U.
- Disponible dans toutes les AWS régions où les serveurs Outposts 2U sont pris en charge.
- Disponible sans frais supplémentaires.
- Vous êtes responsable de la configuration et de day-to-day la gestion de la baie de stockage. Vous créez et gérez également les volumes de blocs externes sur la baie de stockage. Si vous rencontrez des problèmes liés au matériel, au logiciel ou à la connectivité de la baie de stockage, contactez le fournisseur de stockage tiers.

> **Note**
>
> Le volume de blocs stocké sur votre baie de stockage externe contient le système d'exploitation qui sera démarré dans une instance EC2 sur Outposts. Le lancement d'une AMI soutenue par des baies de stockage externes n'est pas pris en charge. Pour lancer une AMI, le stockage d'instance sur le serveur Outposts est utilisé.

Volumes de données par blocs externes

Après avoir approvisionné et configuré des volumes de données par blocs soutenus par un système de stockage tiers compatible, vous pouvez associer les volumes à vos instances EC2 lorsque vous les lancez. Si vous configurez les volumes pour l'attachement multiple sur la baie de stockage, vous pouvez associer un volume à plusieurs instances EC2.

Étapes clés

- Vous êtes responsable de l'établissement de la connectivité entre les sous-réseaux Outpost et le réseau local par le biais de l'interface réseau locale.
- Vous utilisez l'interface de gestion de la baie de stockage externe pour créer le volume. Vous allez ensuite configurer le mappage des initiateurs en créant un nouveau groupe d'initiateurs et en ajoutant le nom qualifié iSCSI (IQN) de l'instance EC2 cible à ce groupe. Cela associe le volume de données de bloc externe à l'instance EC2.
- Vous ajoutez le volume de données externe lorsque vous lancez l'instance. Vous aurez besoin de l'IQN de l'initiateur, de l'adresse IP cible, du port et de l'IQN de la baie de stockage externe. Pour plus d'informations, consultez Lancer une instance sur l'Outpost.

Pour plus d'informations, consultez Simplifier l'utilisation du stockage par blocs tiers avec AWS Outposts.

Volumes de démarrage par blocs externes

Le démarrage d'une instance EC2 sur Outposts à partir de baies de stockage externes fournit une solution centralisée, rentable et efficace pour les charges de travail sur site qui dépendent d'un stockage tiers. Vous pouvez choisir entre les options suivantes :

Démarrage du SAN iSCSI

Permet un démarrage direct à partir de la baie de stockage externe. Utilise une AMI auxiliaire iPXE AWS fournie afin que les instances puissent démarrer depuis un emplacement réseau. Lorsque iPXE est associé à iSCSI, l'instance EC2 traite la cible iSCSI distante (la baie de stockage) comme un disque local. Toutes les opérations de lecture et d'écriture du système d'exploitation sont effectuées sur la baie de stockage externe.

iSCSI ou NVMe-over-TCP LocalBoot

Lance les instances EC2 à l'aide d'une copie du volume de démarrage extrait de la baie de stockage, sans modifier l'image source d'origine. Nous lançons une instance d'assistance à l'aide d'une LocalBoot AMI. Cette instance d'assistance copie le volume de démarrage de la baie de stockage vers le magasin d'instance de l'instance EC2 et agit en tant qu'initiateur ou hôte iSCSI. NVMe-over-TCP Enfin, l'instance EC2 redémarre à l'aide du volume de stockage d'instance local.

Le stockage d'instance étant un stockage temporaire, le volume de démarrage est supprimé lorsque l'instance EC2 est arrêtée. Par conséquent, cette option convient aux volumes de démarrage en lecture seule, tels que ceux utilisés dans l'infrastructure de bureau virtuel (VDI).

Vous ne pouvez pas démarrer des instances Windows EC2 à l'aide NVMe-over-TCP LocalBoot de. Ceci n'est pris en charge qu'avec les instances Linux EC2.

Pour plus d'informations, consultez la section Déploiement de volumes de démarrage externes à utiliser avec AWS Outposts.

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 Gestion des identités et des accès AWS (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches.

Pour plus d'informations sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée d'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).

Chiffrement en transit

AWS chiffre les données en transit entre votre avant-poste et sa région. AWS Pour de plus amples informations, veuillez consulter Connectivité via un lien de service.

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

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

Table des matières

Comment AWS Outposts fonctionne avec IAM

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

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

Fonctionnalité IAM	AWS Soutien aux Outposts
Rôles du service	Non
Rôles liés à un service	Oui

Politiques basées sur l'identité pour les Outposts AWS

Prend en charge les politiques basées sur l'identité : oui

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

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

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

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

Actions politiques pour les AWS Outposts

Prend en charge les actions de politique : oui

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

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Intégration d'actions dans une politique afin d'accorder l'autorisation d'exécuter les opérations associées.

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

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

```
outposts
```

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

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

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

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

Ressources politiques pour les AWS Outposts

Prend en charge les ressources de politique : oui

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

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

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

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

```
"Resource": [
```

```
    "resource1",
    "resource2"
]
```

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

Clés de conditions politiques pour les AWS Outposts

Prend en charge les clés de condition de politique spécifiques au service : oui

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

L'élément `Condition` indique à quel moment les instructions s'exécutent en fonction de critères définis. 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. 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, consultez la section Clés de condition pour AWS Outposts la référence d'autorisation de service. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez la section Actions définies par AWS Outposts.

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

ABAC avec Outposts AWS

Prise en charge d'ABAC (balises dans les politiques) : Oui

Le contrôle d'accès par attributs (ABAC) est une stratégie d'autorisation qui définit les autorisations en fonction des attributs appelés balises. Vous pouvez associer des balises aux entités et aux AWS ressources IAM, puis concevoir des politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de la ressource.

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

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

Pour plus d'informations sur ABAC, consultez Définition d'autorisations avec l'autorisation ABAC dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez Utilisation du contrôle d'accès par attributs (ABAC) dans le Guide de l'utilisateur IAM.

Utiliser des informations d'identification temporaires avec AWS Outposts

Prend en charge les informations d'identification temporaires : oui

Les informations d'identification temporaires fournissent un accès à court terme aux AWS ressources et sont automatiquement créées lorsque vous utilisez la fédération ou que vous changez de rôle. 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 et Services AWS compatibles avec IAM dans le Guide de l'utilisateur IAM.

Autorisations principales interservices pour les Outposts AWS

Prend en charge les sessions d'accès direct (FAS) : oui

Les sessions d'accès direct (FAS) utilisent les autorisations du principal appelant et Service AWS, combinées Service AWS à la demande d'envoi de demandes aux services en aval. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez la section Sessions de transmission d'accès.

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 au service apparaissent dans votre

Compte AWS fichier et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

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

AWS Exemples de politiques relatives aux Outposts

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier les ressources d' AWS Outposts. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM.

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

Pour plus de détails sur les actions et les types de ressources définis par AWS Outposts, y compris le format ARNs de chaque type de ressource, voir Actions, ressources et clés de condition AWS Outposts dans la référence d'autorisation de service.

Table des matières

Bonnes pratiques en matière de politiques

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

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

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

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

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

Exemple : Utilisation d'autorisations au niveau des ressources

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

JSON

```
{
    "Version":"2012-10-17",
```

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "outposts:GetOutpost",
            "Resource": "arn:aws:outposts:us-east-1:111122223333: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.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "outposts:GetSite",
            "Resource": "arn:aws:outposts:us-east-1:111122223333:site/
os-0abcdef1234567890"
        }
    ]
}
```

Rôles liés à un service pour AWS Outposts

AWS Outposts utilise des Gestion des identités et des accès AWS rôles liés à un service (IAM). Un rôle lié à un service est un type de rôle de service directement lié à. AWS Outposts AWS Outposts définit les rôles liés aux services et inclut toutes les autorisations nécessaires pour appeler d'autres AWS services en votre nom.

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

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

Autorisations de rôle liées à un service pour AWS Outposts

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

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

- `outposts.amazonaws.com`

Politiques relatives aux rôles liés aux services

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

- AWSOutpostsServiceRolePolicy
- AWSOutpostsPrivateConnectivityPolicy_*OutpostID*

AWSOutpostsServiceRolePolicy

La `AWSOutpostsServiceRolePolicy` politique permet d'accéder aux AWS ressources gérées par AWS Outposts.

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

- Action : `ec2:DescribeNetworkInterfaces` sur toutes les AWS ressources
- Action : `ec2:DescribeSecurityGroups` sur toutes les AWS ressources
- Action : `ec2:CreateSecurityGroup` sur toutes les AWS ressources
- Action : `ec2:CreateNetworkInterface` sur toutes les AWS ressources

AWSOutpostsPrivateConnectivityPolicy_OutpostID

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

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

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

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

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

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

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

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

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

Créez un rôle lié à un service pour AWS Outposts

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

Modifier un rôle lié à un service pour AWS Outposts

AWS Outposts ne vous permet pas de modifier le rôle *`OutpostID`* lié au service AWSService RoleForOutposts _. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence au rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, voir Mettre à jour un rôle lié à un service dans le Guide de l'utilisateur IAM.

Supprimer un rôle lié à un service pour AWS Outposts

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

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

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

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

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

Contactez le Support aux AWS entreprises pour supprimer votre Outpost.

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

Pour plus d'informations, consultez la section Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

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

AWS Outposts prend en charge l'utilisation de rôles liés au service dans toutes les régions où le service est disponible. Pour plus d'informations, consultez le FAQs pour les serveurs 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 politique Service AWS est lancée ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

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

AWS politique gérée : AWSOutposts ServiceRolePolicy

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

AWS politique gérée : AWSOutposts AuthorizeServerPolicy

Utilisez cette politique pour accorder les autorisations requises pour autoriser le matériel du serveur Outposts sur votre réseau local.

Cette politique inclut les autorisations suivantes.

JSON

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

```
      "Action": [
        "outposts:StartConnection",
        "outposts:GetConnection"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS Outposts met à jour les politiques gérées AWS

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

Modifier	Description	Date
AWSOutpostsAuthorizeServerPolicy : nouvelle politique	AWS Outposts a ajouté une politique qui accorde des autorisations pour autoriser le matériel du serveur Outposts sur votre réseau local.	4 janvier 2023
AWS Outposts ont commencé à suivre les changements	AWS Outposts a commencé à suivre les modifications apportées à ses politiques AWS gérées.	3 décembre 2019

Sécurité de l'infrastructure dans AWS Outposts

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

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

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

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

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 métriques de disponibilité des CloudWatch capacités d'Amazon et définir des alarmes pour surveiller l'état de vos applications, créer des CloudWatch actions pour configurer les options de restauration automatique et surveiller l'utilisation de la capacité de vos Outposts au fil du temps.

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

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. Pour plus d'informations sur votre responsabilité en matière de conformité lors de l'utilisation Services AWS, consultez AWS la documentation de sécurité.

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

CloudWatch métriques

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

CloudTrail journaux

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

Les CloudTrail journaux contiennent des informations sur les appels aux actions d'API pour AWS Outposts. Ils contiennent également des informations relatives aux appels aux actions d'API depuis des services d'un Outpost, tels qu'Amazon EC2 et Amazon EBS. Pour de plus amples informations, veuillez consulter Enregistrez les appels d'API à l'aide de CloudTrail.

Journaux de flux VPC

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

Mise en miroir du trafic

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

Tableau de bord AWS Health

Tableau de bord Health Affiche les informations et les notifications déclenchées par des modifications de l'état de santé des AWS ressources. Les informations sont présentées de deux manières : sur un tableau de bord qui montre les événements récents et à venir organisés

par catégorie, et dans un journal des événements complet qui contient tous les événements des 90 derniers jours. Par exemple, un problème de connectivité sur la liaison de service déclencherait un événement qui apparaîtrait sur le tableau de bord et dans le journal des événements, puis resterait dans ce dernier pendant 90 jours. Une partie du AWS Health service ne Tableau de bord Health nécessite aucune configuration et peut être consultée par tout utilisateur authentifié dans votre compte. Pour plus d'informations, consultez Démarrer avec le Tableau de bord AWS Health.

CloudWatch

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

Vous pouvez utiliser les métriques pour vérifier que le système fonctionne comme prévu. Par exemple, vous pouvez créer une CloudWatch alarme pour surveiller la `ConnectedStatus` métrique. Si la métrique moyenne est inférieure à1, CloudWatch vous pouvez lancer une action, telle que l'envoi d'une notification à une adresse e-mail. Vous pouvez ensuite étudier les éventuels problèmes de réseau sur site ou par liaison montante susceptibles d'avoir un impact sur les opérations de votre Outpost. Parmi les problèmes courants, citons les modifications récentes de la configuration réseau sur site apportées aux règles de pare-feu et NAT, ou les problèmes de connexion Internet. En cas de `ConnectedStatus` problème, nous vous recommandons de vérifier la connectivité à la AWS région depuis votre réseau local et de contacter le AWS Support si le problème persiste.

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

Table des matières

Métriques

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

Table des matières

Métriques des instances

Les métriques suivantes sont disponibles pour les instances Amazon EC2.

Métrique	Dimension	Description
`InstanceFamilyCapacityAvailability`	`InstanceFamily` et `OutpostId`	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).
`InstanceFamilyCapacityUtilization`	`Account`, `InstanceFamily` et `OutpostId`	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

Métrique	Dimension	Description
		Résolution maximale : 5 minutes Statistics : les statistiques les plus utiles sont `Average` et `pNN.NN` (percentiles).
`InstanceTypeCapacityAvailability`	`InstanceType` et `OutpostId`	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).
`InstanceTypeCapacityUtilization`	`Account`, `InstanceType` et `OutpostId`	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).

Métrique	Dimension	Description
`UsedInstanceType_Count`	`Account`, `InstanceType` et `OutpostId`	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

Métrique	Dimension	Description
`AvailableInstanceType_Count`	`InstanceType` et `OutpostId`	Nombre de types d'instances disponibles. Cette métrique inclut le `AvailableReservedInstances` nombre. Pour déterminer le nombre d'instances que vous pouvez réserver, soustrayez le `AvailableReservedInstances` nombre du `AvailableInstanceType_Count` nombre. `Number of instances that you can reserve = AvailableInstanceType_Count - AvailableReservedInstances` Cette métrique n'inclut pas de capacité pour les hôtes dédiés configurés sur l'Outpost. Unité : nombre Résolution maximale : 5 minutes

Métrique	Dimension	Description
`AvailableReservedInstances`	`InstanceType` et `OutpostId`	Le nombre d'instances disponibles pour le lancement dans la capacité de calcul réservée à l'aide des réservations de capacité. Cette métrique n'inclut pas les instances réservées Amazon EC2. Cette métrique n'inclut pas le nombre d'instances que vous pouvez réserver. Pour déterminer le nombre d'instances que vous pouvez réserver, soustrayez le `AvailableReservedInstances` nombre du `AvailableInstanceType_Count` nombre. `Number of instances that you can reserve = AvailableInstanceType_Count - AvailableReservedInstances` Unité : nombre Résolution maximale : 5 minutes

Métrique	Dimension	Description
`UsedReservedInstances`	`InstanceType` et `OutpostId`	Le nombre d'instances qui s'exécutent dans la capacité de calcul réservée à l'aide des réservations de capacité. Cette métrique n'inclut pas les instances réservées Amazon EC2. Unité : nombre Résolution maximale : 5 minutes
`TotalReservedInstances`	`InstanceType` et `OutpostId`	Le nombre total d'instances, en cours d'exécution et disponibles pour le lancement, fourni par la capacité de calcul réservée à l'aide des réservations de capacité. Cette métrique n'inclut pas les instances réservées Amazon EC2. Unité : nombre Résolution maximale : 5 minutes

Métriques des Outposts

Les statistiques suivantes sont disponibles pour vos Outposts.

Métrique	Dimension	Description
`ConnectedStatus`	`OutpostId`	État de la connexion de la liaison de service d'un

Métrique	Dimension	Description
		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`.
`CapacityExceptions`	`InstanceType` et `OutpostId`	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 des métriques

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

Dimension	Description
`Account`	Compte ou service qui utilise la capacité.
`InstanceFamily`	Famille de l'instance.
`InstanceType`	Type d'instance.

Dimension	Description
`OutpostId`	L'ID de l'Outpost.

Vous pouvez consulter les CloudWatch statistiques de votre serveur Outposts à l'aide de la CloudWatch console.

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

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

Pour consulter les statistiques à l'aide du AWS CLI

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

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

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

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

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

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

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

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

- Si la demande a été effectuée avec des informations d'identification d'utilisateur root ou d'utilisateur root.
- Si la demande a été faite au nom d'un utilisateur du centre d'identité IAM.
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la requête a été effectuée par un autre Service AWS.

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

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

CloudTrail sentiers

Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Tous les sentiers créés à l'aide du AWS Management Console sont multirégionaux. Vous ne pouvez créer un journal de suivi en une ou plusieurs régions à l'aide de l' AWS CLI. Il est recommandé de créer un parcours multirégional, car vous capturez l'activité dans l'ensemble Régions AWS

de votre compte. Si vous créez un journal de suivi pour une seule région, il convient de n'afficher que les événements enregistrés dans le journal de suivi pour une seule région Région AWS. Pour plus d'informations sur les journaux de suivi, consultez Créez un journal de suivi dans vos Compte AWS et Création d'un journal de suivi pour une organisation dans le AWS CloudTrail Guide de l'utilisateur.

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

CloudTrail Stockages de données sur les événements du lac

CloudTrail Lake vous permet d'exécuter des requêtes SQL sur vos événements. CloudTrail Lake convertit les événements existants au format JSON basé sur les lignes au format Apache ORC. ORC est un format de stockage en colonnes qui est optimisé pour une récupération rapide des données. Les événements sont agrégés dans des magasins de données d'événement. Ceux-ci constituent des collections immuables d'événements basées sur des critères que vous sélectionnez en appliquant des sélecteurs d'événements avancés. Les sélecteurs que vous appliquez à un magasin de données d'événement contrôlent les événements qui persistent et que vous pouvez interroger. Pour plus d'informations sur CloudTrail Lake, consultez la section Travailler avec AWS CloudTrail Lake dans le guide de AWS CloudTrail l'utilisateur.

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

AWS Outposts événements de gestion dans CloudTrail

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

AWS Outposts enregistre toutes les opérations du plan de contrôle des AWS Outposts en tant qu'événements de gestion. Pour une liste des opérations du plan de contrôle AWS Outposts

auxquelles Outposts se connecte, CloudTrail consultez le Guide de référence de l'API AWSAWS Outposts.

AWS Outposts exemples d'événements

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


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

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

Maintenance du serveur Outposts

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

> **Warning**
>
> Les données sur les volumes de stockage de l'instance sont perdues en cas de défaillance de l'unité de disque sous-jacente ou en cas de cessation de l'instance. Pour éviter toute perte de données, nous vous recommandons de sauvegarder vos données à long terme sur les volumes de stockage d'instance sur un stockage persistant, tel qu'un compartiment Amazon S3 ou un périphérique de stockage réseau de votre réseau sur site.

Table des matières

Mettre à jour les coordonnées

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

Maintenance matérielle

Si un problème matériel irréparable est AWS détecté pendant le processus de mise en service du serveur ou lors de l'hébergement d'instances Amazon EC2 exécutées sur votre serveur Outposts, nous informerons le propriétaire des instances que le retrait des instances concernées est prévu. Pour plus d’informations, consultez Retrait d’instances dans le Guide de l’utilisateur Amazon EC2.

AWS met fin aux instances concernées à la date de mise hors service de l'instance. 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 de la section Installation du serveur Outposts.
- Emballez le serveur irréparable AWS dans le même emballage que celui dans lequel le serveur de remplacement est arrivé.
- 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.
- Renvoyez 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

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

Événements liés à l’alimentation

En cas de panne de courant complète, il existe un risque inhérent qu'une AWS Outposts ressource ne soit pas remise en service automatiquement. Outre le déploiement de solutions d’alimentation redondante et d’alimentation de secours, nous vous recommandons de prendre les mesures suivantes pour vous préparer aux pires scénarios :

- Déplacez vos services et applications en dehors de l’équipement Outposts de manière contrôlée, en procédant à des changements d’équilibrage de charge extérieurs au rack ou basés sur DNS.
- Arrêtez les conteneurs, les instances et les bases de données de manière incrémentielle et ordonnée et restaurez-les dans l’ordre inverse.
- Testez des solutions permettant de déplacer ou d’arrêter les services de manière contrôlée.
- Sauvegardez les données et les configurations critiques et stockez-les en dehors des Outposts.
- Limitez les coupures de courant au minimum.
- Évitez de changer plusieurs fois les alimentations (off-on-off-on) pendant la maintenance.
- Prévoyez du temps supplémentaire dans la fenêtre de maintenance pour faire face aux imprévus.
- Gérez les attentes de vos utilisateurs et de vos clients en leur communiquant une fenêtre de maintenance plus grande que le temps dont vous auriez normalement besoin.
- Une fois l'alimentation rétablie, créez un dossier au AWS Support centre pour demander à vérifier que les services associés sont en cours d'exécution AWS Outposts et que les services associés sont en cours d'exécution.

Événements liés à la connectivité réseau

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

Les instances Amazon EC2, le réseau LNI et les volumes de stockage d'instances sur le serveur Outposts continueront de fonctionner normalement et seront accessibles localement via le réseau local et le LNI. De même, les ressources de AWS service telles que les nœuds de travail Amazon ECS continuent de s'exécuter localement. Cependant, la disponibilité des API sera dégradée. Par exemple, les commandes run, start, stop et terminate APIs risquent de ne pas fonctionner. Les

statistiques et les journaux des instances continueront d'être mis en cache localement pendant 7 jours au maximum et seront transmis à la AWS région lorsque la connectivité sera rétablie. Une déconnexion au-delà de 7 jours peut entraîner la perte de statistiques et de journaux.

Si la liaison de service est interrompue en raison d'un problème d'alimentation sur site ou d'une perte de connectivité réseau, le service Tableau de bord Health envoie une notification au compte propriétaire des Outposts. Ni vous ni ne AWS pouvez supprimer la notification d'une interruption de liaison de service, même si l'interruption est prévue. Pour plus d'informations, consultez Premiers pas avec le Tableau de bord Health 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 vous êtes responsable de la maintenance réseau, limitez la durée du temps d'arrêt de la liaison de service. Prévoyez une étape supplémentaire dans votre processus de maintenance pour vérifier que le réseau a été rétabli.
- Si vous n'êtes pas responsable de la maintenance réseau, surveillez le temps d'arrêt de la liaison de service par rapport à la fenêtre de maintenance annoncée et faites rapidement remonter l'information à la personne en charge de la maintenance réseau planifiée si la liaison de service n'est pas rétablie à la fin de la fenêtre de maintenance annoncée.

Ressources

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

- Le AWS blog Monitoring best practices for AWS Outposts couvre les meilleures pratiques en matière d'observabilité et de gestion des événements spécifiques aux Outposts.
- Le AWS blog sur l'outil de débogage pour la connectivité réseau d'Amazon VPC explique AWSSupport-SetupIPMonitoringFromVPCcet outil. Cet outil est un 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 des Outposts, l'instance de surveillance doit se trouver dans un sous-réseau de la AWS région parent et être configurée pour surveiller

une ou plusieurs de vos instances Outpost à l'aide de ses adresses IP privées. Cela fournira des graphiques de perte de paquets et de latence entre AWS Outposts et la région parent. AWS

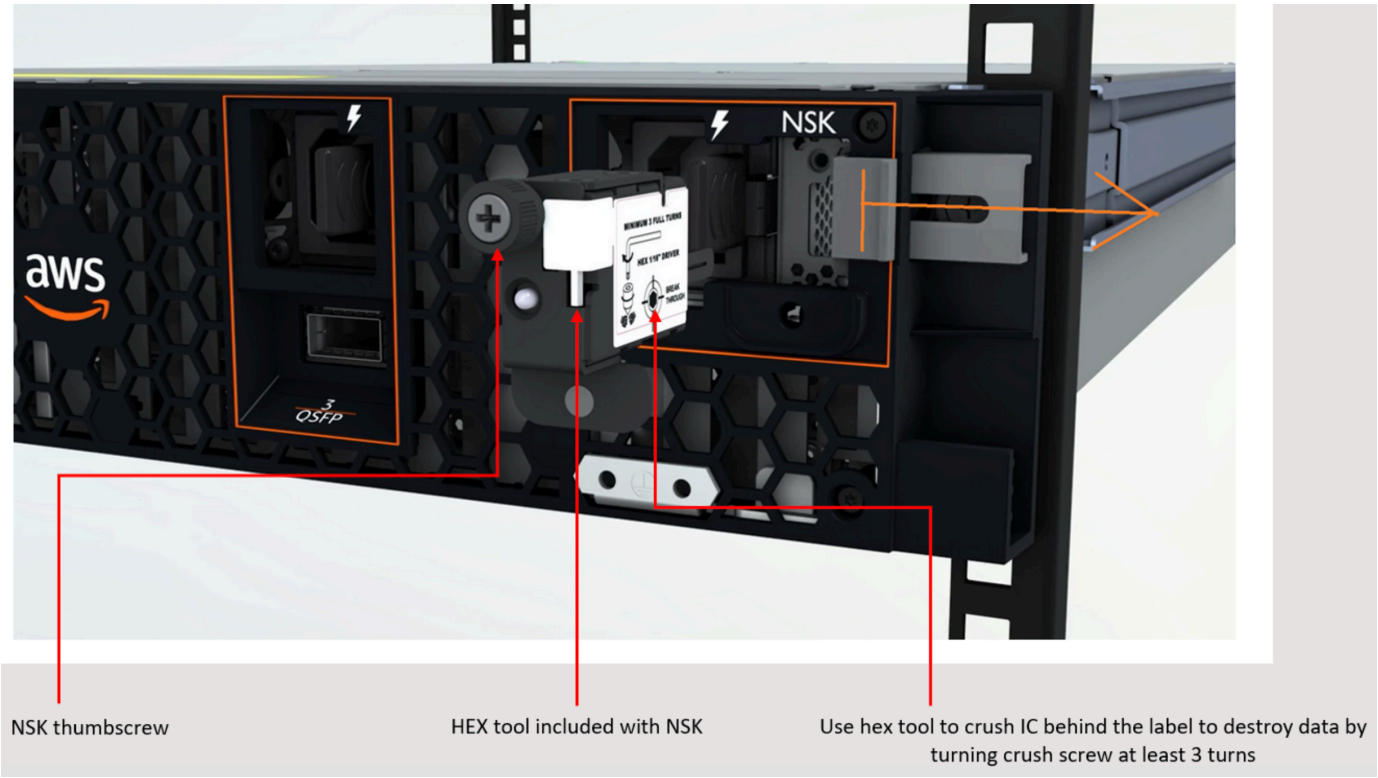
- Le AWS blog Déploiement d'un CloudWatch tableau de bord Amazon automatisé AWS Outposts à utiliser AWS CDK décrit les étapes du déploiement d'un tableau de bord automatisé.
- Si vous avez des questions ou si vous souhaitez obtenir des informations supplémentaires, consultez Création d'un dossier de support dans le Guide de l'utilisateur AWS Support.

Déchiquetage par chiffrement des données d'un serveur

La clé de sécurité Nitro (NSK) est nécessaire pour déchiffrer les données du serveur. Lorsque vous replacez le serveur AWS, soit parce que vous le remplacez, soit parce que vous interrompez le service, vous pouvez détruire le NSK pour détruire cryptographiquement les données sur le serveur.

Pour déchiqueter par chiffrement les données du serveur

1. Retirez le NSK du serveur avant de le renvoyer 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.


NSK
aws
QSFP
NSK thumbscrew
HEX tool included with NSK
Use hex tool to crush IC behind the label to destroy data by turning crush screw at least 3 turns

Options du serveur Outposts end-of-term

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

- Renouvelez votre abonnement et conservez vos serveurs Outposts existants.
- Renvoyez vos serveurs Outposts.
- Passez à un month-to-month abonnement et conservez vos serveurs Outposts existants.

Renouvellement de votre abonnement

Vous devez effectuer les étapes suivantes au moins 5 jours ouvrables avant la fin de l'abonnement en cours pour vos serveurs Outposts. Le fait de ne pas effectuer ces étapes au moins 5 jours ouvrables avant la fin de l'abonnement en cours peut entraîner des frais imprévus.

Pour renouveler votre abonnement et conserver vos serveurs Outposts existants

1. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.
2. Dans le panneau de navigation, sélectionnez Outposts.
3. Choisissez Actions.
4. Choisissez Renew Outpost.
5. Choisissez la durée de l'abonnement et l'option de paiement.

   Pour connaître les tarifs, consultez les Tarification des serveurs AWS Outposts. Vous pouvez également demander un devis.
6. Choisissez Soumettre un ticket d'assistance.

> **Note**
>
> Si vous renouvelez votre abonnement avant la fin de l'abonnement en cours pour vos serveurs Outposts, les frais initiaux vous seront immédiatement facturés.

Votre nouvel abonnement débutera le lendemain de la fin de votre abonnement actuel.

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

renouvelé sur une base mensuelle au taux de l'option de paiement No Upfront correspondant à votre AWS Outposts configuration. Votre nouvel abonnement mensuel débutera le lendemain de la fin de votre abonnement actuel.

Serveurs Return Outposts

Pour renvoyer un serveur parce qu'il a atteint la fin de la durée du contrat, vous devez d'abord terminer le processus de mise hors service au moins 5 jours ouvrables avant la fin de l'abonnement en cours pour vos serveurs Outposts. AWS vous ne pouvez pas démarrer le processus de retour tant que vous ne l'avez pas fait. Le fait de ne pas terminer le processus de mise hors service au moins 5 jours ouvrables avant la fin de l'abonnement en cours peut entraîner des retards dans la mise hors service et des frais imprévus.

Une fois le processus de mise hors service terminé, vous devez préparer le serveur pour le retour, obtenir l'étiquette d'expédition, emballer et renvoyer le serveur à AWS.

Aucuns frais d'expédition ne vous seront facturés lorsque vous renverrez un serveur Outposts. Toutefois, si vous retournez un serveur endommagé, des frais peuvent vous être facturés.

Tâches

- Étape 1 : préparer le serveur pour le retour
- Étape 2 : mise hors service du serveur
- Étape 3 : Obtenir l'étiquette de retour
- Étape 4 : emballer le serveur
- Étape 5 : Retourner le serveur par le service de messagerie

Étape 1 : préparer le serveur pour le retour

Pour préparer le serveur pour le renvoi, 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’Outpost sont partagées, vous devez annuler le partage de ces ressources.

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

   - Utilisez la AWS RAM console. Pour plus d’informations, consultez Mise à jour d’un partage de ressources dans le Guide de l’utilisateur AWS RAM .

- Utilisez le AWS CLI pour exécuter la disassociate-resource-sharecommande.

Pour consulter la liste des ressources Outpost qui peuvent être partagées, consultez Ressources Outpost partageables.

2. Créez des sauvegardes des données stockées dans le stockage d'instance des EC2 instances Amazon exécutées sur le AWS Outposts serveur.
3. Supprimez les interfaces réseau locales associées aux instances qui s'exécutaient sur le serveur.
4. Résiliez les instances actives associées aux sous-réseaux sur votre Outpost. Pour mettre fin aux instances, suivez les instructions de la section Résiliation de votre instance dans le guide de EC2 l'utilisateur Amazon.
5. Détruisez la clé de sécurité Nitro (NSK) pour détruire cryptographiquement vos données sur le serveur. Pour détruire le NSK, suivez les instructions de la section Déchiqueter cryptographiquement les données du serveur.

Étape 2 : mise hors service du serveur

Effectuez les étapes suivantes au moins 5 jours ouvrables avant la fin de l'abonnement en cours pour vos serveurs Outposts.

> **Important**
>
> AWS vous ne pouvez pas arrêter le processus de retour une fois que vous avez soumis votre demande de mise hors service.

1. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.
2. Dans le panneau de navigation, sélectionnez Outposts.
3. Choisissez Actions.
4. Choisissez Decommission Outpost et suivez le flux de travail pour supprimer des ressources.
5. Choisissez Submit request (Soumettre une demande).

> **Note**
>
> Le retour de vos serveurs Outposts avant la fin de l'abonnement en cours n'annulera pas les frais impayés associés à cet Outpost.

Étape 3 : Obtenir l'étiquette de retour

> **Important**
>
> Vous ne devez utiliser que l'étiquette d'expédition AWS fournie, car elle contient des informations spécifiques, telles que l'identifiant de l'actif, concernant le serveur que vous renvoyez. Ne créez pas votre propre étiquette d'expédition.

Pour obtenir votre étiquette d'expédition :

1. Ouvrez la AWS Outposts console à l'adresse https://console.aws.amazon.com/outposts/.
2. Dans le panneau de navigation, choisissez Commandes.
3. Choisissez la commande pour le serveur que vous souhaitez renvoyer.
4. Sur la page des détails de la commande, dans la section État de la commande, choisissez Imprimer l'étiquette de retour.

> **Note**
>
> Le retour de vos serveurs Outposts avant la fin de l'abonnement en cours n'annulera pas les frais impayés associés à cet Outpost.

Étape 4 : emballer le serveur

Pour emballer votre serveur, utilisez la boîte et le matériel d'emballage fournis par AWS.

1. Placez le serveur dans l'une des boîtes suivantes :
   - La boîte et le matériel d'emballage dans lesquels le serveur est arrivé à l'origine.
   - La boîte et le matériel d'emballage dans lesquels le serveur de remplacement est arrivé.

Vous pouvez également contacter le Centre AWS Support pour demander une boîte.

2. Apposez l'étiquette d'expédition AWS fournie à l'extérieur de la boîte.

> **Important**
>
> Vérifiez que l'identifiant de l'article sur l'étiquette d'expédition correspond à l'identifiant de l'actif sur le serveur que vous retournez.
> L'identifiant de l'actif se trouve sur l'onglet déroulant situé à l'avant du serveur. Exemple : `1203779889` ou `9305589922`

3. Fermez bien la boîte.

Étape 5 : Retourner 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 service de messagerie 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 depuis lequel a lieu l'expédition :

Country	Contact
Argentine	Centre AWS Support de contact. Dans la demande, fournissez 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 • Un nom de contact • Un numéro de téléphone • Une adresse e-mail
Bahreïn	
Brésil	
Brunei	
Canada	
Chili	
Colombie	
Hong Kong	

Country	Contact
Inde	
Indonésie	
Japon	
Malaisie	
Nigeria	
Oman	
Panama	
Pérou	
Philippines	
Serbie	
Singapour	
Afrique du Sud	
Corée du Sud	
Taïwan	
Thaïlande	
Emirats arabes unis	
Vietnam	

Country	Contact
États-Unis	Contactez UPS. Vous pouvez renvoyer le serveur des manières suivantes : • Renvoyez le serveur lors d'une collecte UPS de routine sur votre site. • Déposez le serveur chez UPS. • Planifiez une collecte à la date et à l'heure que vous préférez. Saisissez le numéro de suivi indiqué sur l'étiquette d'expédit ion fournie par AWS pour une expédition gratuite.
Tous les autres pays	Contactez DHL. Vous pouvez renvoyer le serveur des manières suivantes : • Déposez le serveur chez DHL. • Planifiez une collecte 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 can't be scheduled for an import shipment`, cela signifie généralem ent que le pays de collecte que vous avez sélectionné ne correspond pas au pays de collecte indiqué sur l'étiquette de renvoi. Sélectionnez le pays à partir duquel le renvoi est réalisé et réessayez.

Convertir en month-to-month abonnement

Pour passer à un month-to-month abonnement et conserver vos serveurs Outposts existants, 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 No Upfront correspondant à votre AWS Outposts configuration. Votre nouvel abonnement mensuel commence le lendemain de la fin de votre abonnement actuel.

Quotas pour AWS Outposts

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

Pour consulter les quotas pour AWS Outposts, ouvrez la console Service Quotas. Dans le volet de navigation, choisissez Services AWS, puis sélectionnez AWS Outposts.

Pour demander une augmentation de quota, consultez Demande d'augmentation de quota dans le Guide de l'utilisateur Service Quotas.

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

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

AWS Outposts et les quotas pour les autres services

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

Modification	Description	Date
AWS Outposts prend en charge les volumes de blocs externes provenant des baies de stockage Dell et HPE	Vous pouvez utiliser des blocs de données externes et des volumes de démarrage fournis par des fournisseurs tiers tels que Dell PowerStore et HPE Alletra Storage MP B10000.	30 septembre 2025
Renouveler votre abonnement et préparer le retour des serveurs	Pour renouveler un abonnement ou renvoyer un serveur, vous devez terminer le processus au moins 10 jours ouvrables avant la fin de l'abonnement en cours.	16 juillet 2025
Résolution des problèmes liés à la connexion Service Link	Si la connexion entre votre serveur Outposts et votre AWS région est interrompue, suivez ces étapes pour résoudre le problème.	5 mai 2025
Mises à jour de la stabilité statique	En cas d'interruption de votre réseau, les métriques et les journaux de l'instance seront mis en cache localement pendant 7 jours au maximum. Auparavant, les Outposts pouvaient mettre en cache les journaux pendant quelques heures seulement.	1er mai 2025
Gestion des capacités au niveau des actifs	Vous pouvez modifier la configuration de la capacité au niveau de l'actif.	31 mars 2025

Volumes de blocs externes soutenus par un système de stockage tiers	Vous pouvez désormais associer des volumes de données par blocs soutenus par des systèmes de stockage par blocs tiers compatibles pendant le processus de lancement de l'instance sur Outpost.	1er décembre 2024
Gestion des capacités	Vous pouvez modifier la configuration de capacité par défaut pour votre nouvelle commande d'Outposts.	16 avril 2024
End-of-term options pour les 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
Présentation des serveurs Outposts	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.