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

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

> **Note**
>
> Vous ne pouvez pas connecter un avant-poste à un autre avant-poste ou à une autre zone locale qui s'y trouve. VPC

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

Concepts clés

Ce sont les concepts clés pour AWS Outposts.

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

- Racks Outpost : facteur de format Outpost conforme aux normes de l'industrie en matière de rack 42U. Les racks Outposts incluent des serveurs montables en rack, des commutateurs, un panneau de brassage réseau, une étagère d'alimentation et des panneaux vierges.
- Serveurs Outposts : format Outpost qui est un serveur 1U ou 2U conforme aux normes de l'industrie, qui peut être installé dans un rack à 4 poteaux 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
EC2Instances Amazon	O	Oui

Type de ressource	Racks	Serveurs
ECSClusters Amazon	 O	 Oui
EKSNœuds Amazon	 O	 Non

Base de données et analytique

Type de ressource	Racks	Serveurs
ElastiCache Nœuds Amazon (cluster Redis, cluster Memcached)	 O	 Non
EMRClusters Amazon	 O	 Non
Instances de RDS base de données Amazon	 O	 Non

Réseaux

Type de ressource	Racks	Serveurs
Proxy App Mesh Envoy	 O	 Oui

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

Stockage

Type de ressource	Racks	Serveurs
EBSVolumes Amazon	 O	 Non
Compartiments Amazon S3	 O	 Non

Autres Services AWS

Service	Racks	Serveurs
AWS IoT Greengrass	 O	 Oui

Service	Racks	Serveurs
Amazon SageMaker Edge Manager	 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'EC2instances Amazon et d'options de stockage. Vous choisissez également une durée contractuelle et une option de paiement. Le prix inclut les éléments suivants :

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

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

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

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

Comment AWS Outposts fonctionne

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

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

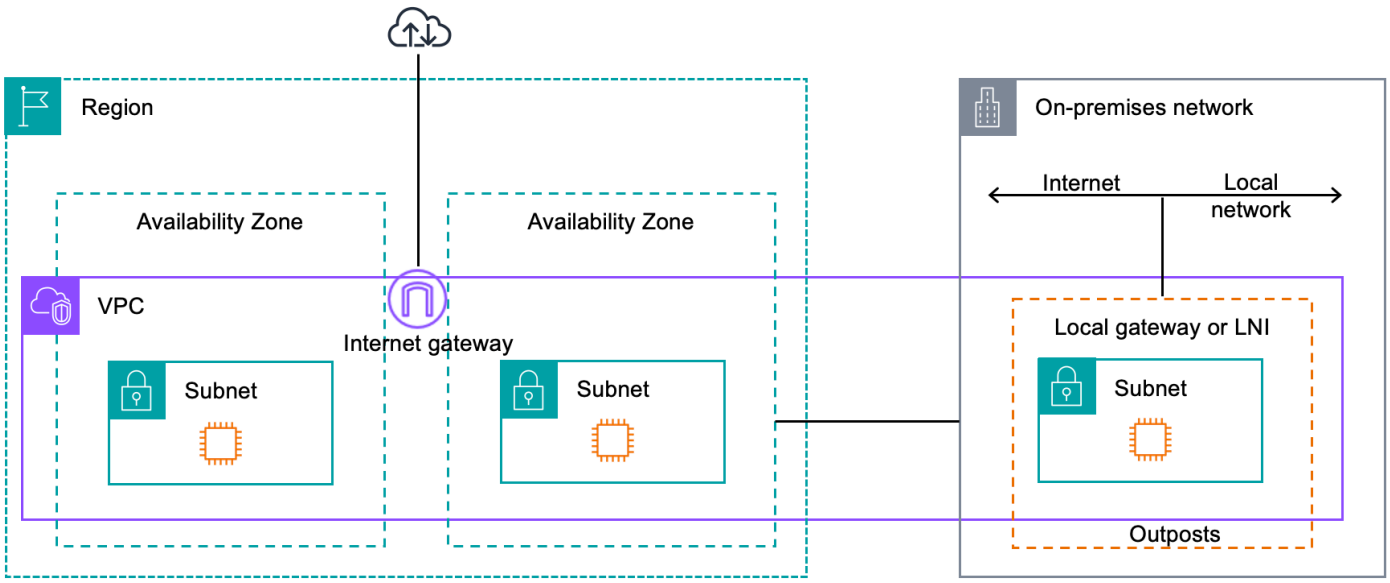
Table des matières

Composants réseau

AWS Outposts étend un Amazon VPC d'une AWS région à un avant-poste avec les VPC composants accessibles dans la région, notamment les passerelles Internet, les passerelles privées virtuelles, les passerelles Amazon VPC Transit 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
- A VPC avec plusieurs sous-réseaux dans la région
- Un Outpost dans le réseau sur site
- Connectivité entre l'Outpost et le réseau local assurée par une passerelle locale (racks) ou une interface de réseau local (serveurs)



VPCset sous-réseaux

Un cloud privé virtuel (VPC) couvre toutes les zones de disponibilité de sa AWS région. Vous pouvez étendre n'importe quel VPC élément de la région à votre avant-poste en ajoutant un sous-réseau d'avant-poste. Pour ajouter un sous-réseau Outpost à unVPC, spécifiez le nom de ressource Amazon (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'EC2instance lorsque vous lancez l'EC2instance 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 plus d'informations sur VPC les quotas, consultez Amazon VPC Quotas dans le guide de VPC l'utilisateur Amazon.

Vous créez des sous-réseaux Outpost à partir de la VPC CIDR plage VPC où 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 VPC route locale. Cela signifie que tout le trafic duVPC, y compris le sous-réseau Outpost avec une destination dans le, VPC CIDR reste acheminé dans le. VPC

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

- VPCCIDRplage : AWS définit cette plage lors de l'installation. Il s'agit de l'itinéraire local qui s'applique à tous les VPC itinéraires, y compris le trafic entre les instances d'Outpost d'une même VPC instance.
- 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 unVPC, EC2 les instances des sous-réseaux Outposts peuvent utiliser le DNS service Amazon Route 53 pour convertir les noms de domaine en adresses IP. Route 53 prend en charge DNS des fonctionnalités telles que l'enregistrement de domaines, le DNS routage et les contrôles de santé pour les instances exécutées dans votre Outpost. Les zones de disponibilité hébergées publiques et privées sont prises en charge pour 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 DNS fonctionnalités fonctionnent.

Les temps de DNS résolution 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 DNS serveurs installés localement dans votre environnement sur site. Pour utiliser vos propres DNS serveurs, vous devez créer des ensembles d'DHCPoptions pour vos DNS serveurs locaux et les associer auVPC. Vous devez également vous assurer qu'il existe une connectivité IP avec ces DNS serveurs. 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. Les ensembles d'DHCPoptions ayant une VPC portée limitée, les instances des sous-réseaux Outpost et des sous-réseaux de la zone de disponibilité VPC essaieront d'utiliser les DNS serveurs spécifiés pour DNS la résolution de noms.

L'enregistrement des requêtes n'est pas pris en charge pour les DNS requêtes 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. Le lien de service est un ensemble crypté de VPN connexions utilisées chaque fois que l'Outpost communique avec la région d'origine que vous avez choisie. Vous utilisez un virtual LAN (VLAN) pour segmenter le trafic sur le lien de service. La liaison de service VLAN permet la communication entre l'avant-poste et la AWS région à la fois pour la gestion de l'avant-poste et pour le VPC trafic intra-poste entre la AWS région et l'avant-poste.

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 :

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

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 d'expédition est compatible avec le support de montage standard en forme de L d'un rack 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 standards de 19 pouces EIA -310D, 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.
- Acoustique : puissance sonore nominale inférieure à 78 dBA à des températures de 80 °F (27 °C) et conforme à la norme CORE NEBS GR-63.
- 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 service et de LNI liaison — QSFP + un câble de dérivation (10 pieds/3 m) permet de segmenter le trafic.

Pare-feu de la liaison de service

UDPet TCP 443 doivent être répertoriés de manière dynamique 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	DHCPDNSserveur fourni
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 AWS Direct Connect connexion ou une connexion Internet publique pour reconnecter l'avant-poste à la AWS région. Pour la connectivité des liaisons du service Outposts, vous pouvez utiliser NAT ou PAT au niveau de votre pare-feu ou de votre routeur périphérique. L'établissement d'une liaison de service est toujours initié depuis Outpost.

Unité de transmission maximale du lien de service (MTU)

Le réseau doit prendre en charge 1 500 octets MTU entre l'avant-poste et les points de terminaison du lien 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 AMI la taille, l'élasticité de l'application, les besoins en vitesse de rafale et le VPC trafic Amazon vers la région. Notez que les AWS Outposts serveurs ne mettent pas en cacheAMIs. AMIssont 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 APN partenaire.

Le lien de service nécessite une DHCP réponse

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

Latence maximale de la liaison de service

Les liaisons de service peuvent supporter une latence réseau maximale de 175 ms à partir du serveur et de sa zone de disponibilité.

Alimentation

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

Prérequis

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

Soutien en alimentation

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

Consommation énergétique

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

Câble d’alimentation

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

Câblage d’alimentation entre le serveur et le rack

Utilisez le câble d'alimentation IEC C14-C13 fourni pour connecter 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 cordon d'IECalimentation C13 à NEMA 5-15P.
- Dans certaines régions d'Europe, vous pourriez avoir besoin d'un cordon d'alimentation IEC C13 à CEE 7/7.

- En Inde, vous avez besoin d'un câble d'IS1293alimentation IEC C13.

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 coupure ()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 EC2 capacité Amazon 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 EC2 instance Amazon et configurez la connectivité à votre réseau local.

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.

Prérequis

- Passez en revue les configurations disponibles pour vos serveurs Outposts.
- Un site Outpost est l’emplacement physique de votre équipement Outpost. Avant de commander de la capacité, vérifiez que votre site répond aux exigences. Pour 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 un identifiant à votre site. Vous devez spécifier ce site lorsque vous créez un Outpost.

Prérequis

- Déterminez l'adresse d'exploitation.

Pour créer un site

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

Étape 2 : Création d'un Outpost

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

Prérequis

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

Pour créer un Outpost

1. Dans le panneau de navigation, sélectionnez Outposts.

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

Étape 3 : Passer la commande

Passez une commande pour les 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.

Prérequis

- Déterminez le mode de paiement de la commande. Vous pouvez payer la totalité à l'avance, une partie à l'avance ou rien à l'avance. Si vous choisissez l'option de paiement initial partiel ou sans paiement initial, vous devrez payer des frais mensuels pendant toute la durée du paiement.

  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 de 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 JSON fichier.

Console steps

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

Upload JSON file

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

   Example

   Exemple de JSON fichier :

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

4. Passez en revue le contenu du JSON fichier 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. Une fois que vous aurez arrêté ces instances, la tâche AWS Outposts sera exécutée.

Étapes suivantes

Vous pouvez consulter le statut de votre commande à l'aide de la AWS Outposts console. L'état initial de votre commande est Commande reçue. 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 fassiez l'installation ou que vous passiez un contrat avec un tiers, l'installation nécessite des IAM informations d'identification dans le fichier Compte AWS contenant l'Outpost afin de 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 lorsque la EC2 capacité Amazon pour votre Outpost est disponible auprès de votre Compte AWS. Une fois la capacité disponible, vous pouvez lancer des EC2 instances Amazon sur votre serveur Outposts. Pour de plus amples informations, veuillez consulter the section called "Lancer une instance ".

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 EC2 instances Amazon.

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 d'avant-poste à n'importe quel sous-réseau VPC de la AWS région pour l'avant-poste. Lorsque vous le faites, il s'étend VPC également sur l'avant-poste. 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 pour créer un sous-réseau dans la VPC console Amazon. 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. Sélectionnez Create (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 EC2 des instances dans le sous-réseau Outpost que vous avez créé ou dans un sous-réseau Outpost qui a été partagé avec vous. Les groupes de sécurité contrôlent le VPC trafic entrant et sortant pour les instances d'un sous-réseau Outpost, comme ils le font pour les instances

d'un sous-réseau de zone de disponibilité. Pour vous connecter à une EC2 instance d'un sous-réseau Outpost, vous pouvez spécifier une paire de clés lorsque vous lancez l'instance, comme vous le faites pour les instances d'un sous-réseau de zone de disponibilité.

Considérations

- Les instances présentes sur les serveurs Outposts incluent les volumes de stockage d'instances, mais pas EBS les volumes. Choisissez une taille d'instance offrant suffisamment de stockage pour répondre aux besoins de votre application. Pour plus d'informations, consultez les sections Volume de stockage d'instance et Création d'une instance sauvegardée par le stockage AMI dans le guide de EC2l'utilisateur Amazon.
- Vous devez utiliser une copie EBS sauvegardée par Amazon AMI avec un seul EBS instantané. AMIsavec plus d'un EBS instantané 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 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'instance dans la EC2 console Amazon. Nous sélectionnons le sous-réseau Outpost pour vous et nous vous indiquons uniquement les types d'instances pris en charge par vos serveurs Outposts.
5. Choisissez un type d'instance compatible avec vos serveurs Outposts.
6. (Facultatif) Vous pouvez ajouter une interface de réseau local maintenant ou après avoir créé l’instance. Pour l’ajouter maintenant, développez Configuration réseau avancée, puis choisissez Ajouter une interface réseau. Choisissez le sous-réseau Outpost. Une interface réseau est alors créée pour l’instance avec l’index d’appareil 1. Si vous avez spécifié 1 comme index 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. Suivez les étapes de l'assistant pour lancer l'instance dans votre sous-réseau Outpost. Pour plus d'informations, consultez Lancer une EC2 instance dans le guide de EC2 l'utilisateur Amazon :

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. Généralement, vous le faites en utilisantDHCP. 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 EC2 instance, consultez Connect to your EC2 instance dans le guide de EC2 l'utilisateur Amazon.

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

```
ping 172.16.0.130
```

Voici un exemple de sortie.

```
Pinging 172.16.0.130

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

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

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

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

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

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

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

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

   ```
   ping 10.0.1.5
   ```

   Voici un exemple de sortie.

   ```
   Pinging 10.0.1.5

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

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

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

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. Le lien de service est un ensemble crypté de VPN connexions utilisées chaque fois que l'Outpost communique avec la région d'origine que vous avez choisie. Vous utilisez un virtual LAN (VLAN) pour segmenter le trafic sur le lien de service. La liaison de service VLAN permet la communication entre l'avant-poste et la AWS région à la fois pour la gestion de l'avant-poste et pour le VPC trafic intra-poste entre la AWS région et l'avant-poste.

The Outpost est en mesure de créer le lien de service VPN vers la AWS région grâce à la connectivité publique de la région. 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 se faire via des itinéraires spécifiques dans le lien VLAN de service ou via un itinéraire par défaut de 0.0.0.0/0. Pour plus d’informations sur les plages publiques pour AWS, consultez Plages d’adresses IP AWS.

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 associéVPCs, y compris le trafic du plan de données client.

Exigences relatives à l'unité de transmission maximale (MTU) de la liaison de service

L'unité de transmission maximale (MTU) d'une connexion réseau est la taille, en octets, du plus grand paquet autorisé pouvant être transmis sur la connexion. Le réseau doit prendre en charge 1 500 octets MTU entre l'avant-poste et les points de terminaison du lien de service dans la région parent. AWS Pour plus d'informations sur le lien de transmission requis MTU entre une instance de l'Outpost et une instance de la AWS région via le lien de service, consultez la section Unité de transmission maximale du réseau (MTU) pour votre EC2 instance Amazon dans le guide de l'EC2utilisateur Amazon.

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 AMI la taille, l'élasticité de l'application, les besoins en vitesse de rafale et le VPC trafic Amazon vers la région. Notez que les AWS Outposts serveurs ne mettent pas en cacheAMIs. AMIssont 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 APN partenaire.

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

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

Si vous utilisez un pare-feu dynamique avec votre connexion Internet pour limiter la connectivité entre l'Internet public et le lien de serviceVLAN, vous pouvez bloquer toutes les connexions entrantes initiées depuis Internet. Cela est dû au fait que le lien VPN de service part uniquement de l'avant-poste vers la région, et non de la région vers l'avant-poste.

Si vous utilisez un pare-feu pour limiter la connectivité depuis le lien de serviceVLAN, 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	DHCPDNSserveur fourni
UDP	443, 1024-65535	Adresse IP de la liaison de service	443	AWS Outposts Points de terminaison Service Link

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

> **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.

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 VPC trafic intra-poste 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 VPC connectivité 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.

Connexions Internet redondantes

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

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

Retourner un serveur Outposts

En AWS Outposts cas de détection d'un défaut sur le serveur, nous vous en informerons, lancerons le processus de remplacement pour vous envoyer un nouveau serveur et vous fournirons l'étiquette d'expédition via la AWS Outposts console. Pour commencer, suivez les étapes ci-dessous.

Tâches

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

Pour renvoyer le serveur parce que le serveur a atteint la fin de la durée du contrat ou pour une autre raison, contactez le AWS Support centre.

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.

Étape 2 : 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.

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

Shipping label for a server that is being replaced

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

Shipping label for a server that is not being replaced

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

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 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 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 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 :

Pays	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	

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

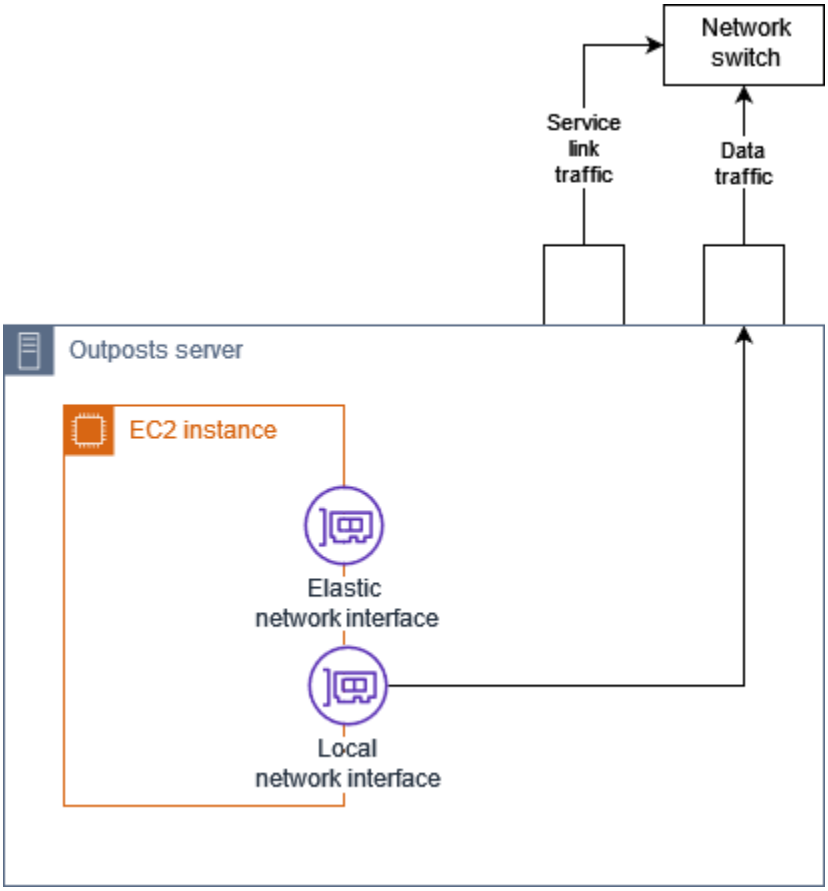
Pays	Contact
États-Unis	Contacte UPS. Vous pouvez renvoyer le serveur des manières suivantes : • Retournez le serveur lors d'un UPS ramassage de routine sur votre site. • Déposez le serveur à un UPSemplacement. • Planifiez une collecte à la date et à l'heure que vous préférez. Saisissez le numéro de suivi indiqué sur l'étiquette d'expédit ion fournie par AWS pour une expédition gratuite.
Tous les autres pays	Contacte DHL. Vous pouvez renvoyer le serveur des manières suivantes : • Déposez le serveur à un DHLemplacement. • Planifiez une collecte à la date et à l'heure que vous préférez. Entrez le numéro de DHL bordereau d'expédition indiqué 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.

Interfaces réseau locales pour vos serveurs Outposts

Avec les serveurs Outposts, une interface réseau locale est un composant réseau logique qui connecte les EC2 instances Amazon de votre sous-réseau Outposts à votre réseau local.

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 EC2 instances du sous-réseau Outpost pour inclure une interface réseau locale en plus de l'interface elastic network. L'interface réseau locale se connecte au réseau local tandis que l'interface réseau se connecte auVPC. Le schéma suivant montre une EC2 instance sur un serveur Outposts avec une interface réseau élastique 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'DHCPoptions dans a 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 VPC réseau pour accéder aux points de terminaison régionaux publics Services AWS, ou vous pouvez utiliser les points de VPC terminaison d'interface pour accéder Services AWS à l'aide de. 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. A VPC est un réseau virtualisé de couche 3. Les interfaces réseau locales ne prennent pas en charge les composants VPC réseau. 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 de VPC 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

- Support des interfaces réseau locales ARP et DHCP protocoles. 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 VPC l'utilisateur Amazon.
- Chaque EC2 instance 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 EC2 instances, chacune dotée d'une interface réseau locale.

> **Note**
>
> EC2les instances 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 ni l'usurpation d'MACadresse.

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 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 votreVPC. Un groupe de sécurité contrôle le trafic entrant et sortantVPC. L'interface réseau locale n'est pas connectée auVPC. L’interface réseau locale est attachée à votre réseau local. Pour contrôler le trafic entrant et sortant sur l’interface réseau locale, utilisez un pare-feu ou une stratégie similaire, comme vous le feriez avec le reste de votre équipement sur site.

Surveillance

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

MACadresses

AWS fournit des MAC adresses pour les interfaces réseau locales. Les interfaces réseau locales utilisent des adresses administrées localement (LAA) pour leurs MAC adresses. Une interface réseau

locale utilise la même MAC adresse jusqu'à ce que vous la supprimiez. Après avoir supprimé une interface réseau locale, supprimez l'MACadresse de vos configurations locales. AWS peut réutiliser MAC des adresses qui ne sont plus utilisées.

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

Vous pouvez ajouter une interface réseau locale à une EC2 instance Amazon 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 EC2 instance

1. Ouvrez la EC2 console Amazon 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'IPv4adresse 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 EC2 console Amazon pour afficher à la fois l'interface Elastic Network et l'interface réseau locale des 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 depuis le sous-réseauCIDR. Cette adresse n'est pas l'adresse IP de l'interface réseau locale et elle n'est pas utilisable. Cependant, cette adresse est allouée à partir du sous-réseauCIDR, vous devez donc 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 DHCP serveur.

Configuration du système d’exploitation

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

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

- 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 des liaisons de service — Ce trafic permet la communication entre l'avant-poste et la AWS région à la fois pour la gestion de l'avant-poste et pour le VPC trafic intra-régional 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 personnalisé VPN ou relie VPNs l'avant-poste 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 lié à l'interface réseau locale — Ce trafic permet la communication entre VPC vous et votre réseau local LAN 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

QSFP+ câble

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 connectez 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 vers un port VLAN doté d'une passerelle et en tant que 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 être DNS accessible au public pour que l'Outpost découvre son point de terminaison d'enregistrement dans la AWS région. La connexion peut avoir un NAT appareil 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'VPCutilisateur Amazon et les AWS Outposts points de terminaison et quotas dans le Références générales AWS.

Pour enregistrer le serveur, ouvrez les ports réseau suivants :

- TCP443
- UDP443
- UDP53

Vitesse de la liaison montante

Chaque serveur Outposts nécessite une vitesse de liaison montante minimale de 20 Mbits/s vers la région. AWS

Vous aurez peut-être besoin d'une liaison montante plus rapide en fonction de votre lien d'interface réseau local et de l'utilisation du lien de service. Pour plus d’informations, consultez Recommandations en matière de bande passante pour les liaisons de service.

Trafic de liaison d'interface réseau local

Configurez le port de liaison de l'interface réseau local sur votre périphérique réseau en amont en tant que port d'accès standard vers un VLAN port de votre réseau local. Si vous en avez plusieursVLAN, 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 vous attendre à plusieurs MAC adresses. Chaque instance lancée sur le serveur utilisera une MAC adresse. Certains périphériques réseau offrent des fonctionnalités de sécurité des ports qui bloquent un port signalant plusieurs MAC adresses.

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

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

Exemple : pour configurer le VLAN balisage 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 l'VLANappareil. Dans cet exemple :

   - Le nom de l'interface réseau locale est `ens6`
   - L'VLANidentifiant est `59`
   - Le nom attribué à l'VLANappareil 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 sous-réseau est 192.168.59.0/24. CIDR

```
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 rendre les modifications de VLAN balisage persistantes, consultez les ressources suivantes :

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

Attribution d'adresse IP de serveur

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

Le protocole de contrôle dynamique de l'hôte (DHCP) est un protocole de gestion réseau utilisé pour automatiser le processus de configuration des appareils sur les réseaux IP. Dans le contexte des serveurs Outposts, vous pouvez utiliser DHCP deux méthodes :

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

Pour le lien de service, les serveurs Outposts DHCP se connectent au réseau local. DHCPdoit renvoyer des serveurs de DNS noms et une passerelle par défaut. Les serveurs Outposts ne prennent pas en charge l'attribution statique d'une adresse IP à un lien de service.

Pour le lien d'interface réseau local, utilisez-le DHCP pour configurer les instances à connecter à votre réseau local. Pour de plus amples informations, veuillez consulter the 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'inscription doit être publiqueDNS. 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 TCP port 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

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 configurerVPCs, 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
- Limites

Ressources Outpost partageables

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

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 :
  - Lancez et exécutez EC2 des instances sur un hôte dédié.
- Outposts : les consommateurs ayant accès à cette ressource peuvent :
  - Créer et gérer des sous-réseaux sur l’Outpost.
  - Utilisez le AWS Outposts API pour afficher des informations sur l'avant-poste.
- Sites : les consommateurs ayant accès à cette ressource peuvent :
  - Créer, gérer et contrôler un Outpost sur le site.
- Sous-réseaux : les consommateurs ayant accès à cette ressource peuvent :
  - Afficher des informations sur les sous-réseaux.
  - Lancez et exécutez EC2 des instances dans des sous-réseaux.

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

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 l'AZ IDs des zones de disponibilité de votre compte

1. Ouvrez la AWS RAM console dans https://console.aws.amazon.com/ram.
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 aux tables de routage des passerelles locales partagées peuvent créer et gérer VPC des associations. Pour de plus amples informations, veuillez consulter Ressources Outpost partageables.

Pour partager une ressource Outpost, vous devez l'ajouter à un partage de ressources. Un partage de ressources est une 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 console AWS Outposts , 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 create-resource-sharecommande.

Annulation du partage d'une ressource Outpost

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

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

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 disassociate-resource-sharecommande.

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 qui vous appartiennent et celles qui sont partagées avec vous. `OwnerId` indique l'ID de compte AWS 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 VPN trafic des liaisons de service de leur avant-poste 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 VPC propriétaire est facturé pour les ressources de VPC niveau « and » telles que les VPN connexions, les NAT passerelles AWS Direct Connect et les connexions par lien privé.

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

Limites

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

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

Sécurité dans AWS Outposts

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

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

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

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

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

Table des matières

Protection des données dans AWS Outposts

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

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

Pour plus d'informations sur la confidentialité des données, consultez la section Confidentialité des données FAQ. Pour plus d'informations sur la protection des données en Europe, consultez le modèle de responsabilitéAWS partagée et le billet de GDPR blog sur le blog sur la AWS sécurité.

Chiffrement au repos

Avec AWS Outposts, toutes les données sont cryptées au repos. Le matériau de la clé est enroulé sur une clé externe stockée dans un dispositif amovible, la clé de sécurité Nitro (NSK). NSKII est nécessaire pour déchiffrer les données sur votre serveur rack .

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 mettez fin à une EC2 instance, la mémoire qui lui est allouée est nettoyée (mise à zéro) par l'hyperviseur avant d'être allouée à une nouvelle instance, et chaque bloc de stockage est réinitialisé.

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

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

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

Table des matières

Comment AWS Outposts fonctionne avec IAM

Avant de commencer IAM à gérer l'accès aux AWS Outposts, découvrez quelles IAM fonctionnalités peuvent être utilisées avec AWS Outposts.

IAMfonctionnalités que vous pouvez utiliser avec AWS Outposts

IAMfonctionnalité	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(balises dans les politiques)	Oui
Informations d’identification temporaires	Oui

IAMfonctionnalité	AWS Soutien aux Outposts
Autorisations de principal	Oui
Fonctions du service	Non
Rôles liés à un service	Oui

Politiques basées sur l'identité pour les Outposts AWS

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

Les politiques basées sur l'identité sont JSON des documents de politique d'autorisation que vous pouvez joindre à une identité, telle qu'un IAM utilisateur, un groupe d'utilisateurs ou un rôle. Ces politiques contrôlent quel type d’actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour savoir comment créer une politique basée sur l'identité, consultez la section Création de IAM politiques dans le Guide de l'IAMutilisateur.

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

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

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

Politiques basées sur les ressources au sein d'Outposts AWS

Prend en charge les politiques basées sur les ressources : non

Les politiques basées sur les ressources sont des documents JSON de stratégie que vous attachez à une ressource. Les politiques de confiance dans les IAM rôles et les politiques relatives aux compartiments Amazon S3 sont des exemples de politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l’accès à une ressource spécifique. Pour la ressource dans

laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

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

Actions politiques pour les AWS Outposts

Prend en charge les actions de politique : oui

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

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

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

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

```
outposts
```

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

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

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

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

Ressources politiques pour les AWS Outposts

Prend en charge les ressources de politique : oui

Les administrateurs peuvent utiliser AWS JSON des politiques 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 `Resource` JSON de stratégie indique le ou les objets auxquels s'applique l'action. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de spécifier une ressource en utilisant son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

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

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

Certaines API actions AWS d'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 caractéristiquesARNs, consultez la section Types de ressources définis par AWS Outposts dans la référence d'autorisation de service. Pour savoir avec quelles actions vous pouvez spécifier pour chaque ressource, consultez la ARN section 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 AWS JSON des politiques pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

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

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

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez autoriser un IAM utilisateur à accéder à une ressource uniquement si celle-ci est étiquetée avec son nom IAM d'utilisateur. Pour plus d'informations, consultez IAMla section Éléments de politique : variables et balises dans le Guide de IAM l'utilisateur.

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

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

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

ACLsdans AWS Outposts

Supports ACLs : Non

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLssont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format du document JSON de stratégie.

ABACavec AWS Outposts

Supports ABAC (balises dans les politiques) : Oui

Le contrôle d'accès basé sur les attributs (ABAC) est une stratégie d'autorisation qui définit les autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises à IAM des entités (utilisateurs ou rôles) et à de nombreuses AWS ressources. Le balisage des entités et des ressources est la première étape deABAC. Vous concevez ensuite des ABAC politiques pour autoriser les opérations lorsque le tag du principal correspond à celui de la ressource à laquelle il essaie d'accéder.

ABACest utile dans les environnements qui se développent rapidement et aide dans les situations où la gestion des politiques devient fastidieuse.

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

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

Pour plus d'informationsABAC, voir Qu'est-ce que c'est ABAC ? dans le guide de IAM l'utilisateur. Pour consulter un didacticiel présentant les étapes de configurationABAC, voir Utiliser le contrôle d'accès basé sur les attributs (ABAC) dans le guide de l'IAMutilisateur.

Utiliser des informations d'identification temporaires avec AWS Outposts

Prend en charge les informations d'identification temporaires : oui

Certains Services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui Services AWS fonctionnent

avec des informations d'identification temporaires, consultez Services AWS la section relative à l'utilisation IAM dans le Guide de IAM l'utilisateur.

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

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

Autorisations principales interservices pour les Outposts AWS

Prend en charge les sessions d'accès transféré (FAS) : Oui

Lorsque vous utilisez un IAM utilisateur ou un rôle pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FASutilise les autorisations du principal appelant an Service AWS, combinées à la demande Service AWS pour adresser des demandes aux services en aval. FASles demandes ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur les politiques relatives FAS aux demandes, consultez la section Transférer les sessions d'accès.

Fonctions du service pour AWS Outposts

Supporte les rôles de service : Non

Un rôle de service est un IAMrôle qu'un service assume pour effectuer des actions en votre nom. Un IAM administrateur peut créer, modifier et supprimer un rôle de service de l'intérieurIAM. Pour plus d'informations, consultez la section Création d'un rôle auquel déléguer des autorisations Service AWS dans le Guide de IAM l'utilisateur.

Rôles liés à un service pour les Outposts AWS

Prend en charge les rôles liés aux services : Oui

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

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

AWS Exemples de politiques relatives aux Outposts

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

Pour savoir comment créer une politique IAM basée sur l'identité à l'aide de ces exemples de documents de JSON stratégie, consultez la section Création de IAM politiques dans le guide de l'IAMutilisateur.

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 les politiques AWS gérées ou les politiques AWS gérées pour les fonctions professionnelles dans le Guide de IAM l'utilisateur.
- Appliquer les autorisations du moindre privilège : lorsque vous définissez des autorisations à IAM l'aide de politiques, accordez uniquement les autorisations nécessaires à l'exécution d'une 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 IAM pour appliquer des autorisations, consultez la section Politiques et autorisations IAM dans le guide de IAM l'utilisateur.
- Utilisez des conditions dans IAM les politiques pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques pour limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez rédiger une condition de politique pour spécifier que toutes les demandes doivent être envoyées en utilisantSSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, voir Éléments IAM JSON de politique : Condition dans le guide de IAM l'utilisateur.
- Utilisez IAM Access Analyzer pour valider vos IAM politiques afin de garantir des autorisations sécurisées et fonctionnelles. IAM Access Analyzer valide les politiques nouvelles et existantes afin qu'elles soient conformes au langage des IAM politiques (JSON) et IAM aux meilleures pratiques. IAMAccess Analyzer fournit plus de 100 vérifications des politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez la section Validation des politiques d'IAMAccess Analyzer dans le guide de IAM l'utilisateur.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des IAM utilisateurs ou un utilisateur root Compte AWS, activez-le MFA pour une sécurité supplémentaire. Pour exiger le MFA moment où les API opérations sont appelées, ajoutez MFA des conditions à vos politiques. Pour plus d'informations, consultez la section Configuration de l'APIaccès MFA protégé dans le Guide de l'IAMutilisateur.

Pour plus d'informations sur les meilleures pratiques en matière de sécuritéIAM, consultez la section Bonnes pratiques en matière de sécurité IAM dans le Guide de IAM l'utilisateur.

Exemple : Utilisation d’autorisations au niveau des ressources

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

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

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

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

Rôles liés à un service pour AWS Outposts

AWS Outposts utilise AWS Identity and Access Management (IAM) des rôles liés à un service. 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 incluent la politique de confiance et la politique d'autorisations, et cette politique d'autorisations ne peut être attachée à aucune autre IAM entité.

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

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

- `outposts.amazonaws.com`

Le AWSServiceRoleForOutposts _***OutpostID***un rôle lié à un service inclut les politiques suivantes :

- AWSOutpostsServiceRolePolicy
- AWSOutpostsPrivateConnectivityPolicy_***OutpostID***

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

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

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

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

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

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

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

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

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

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

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

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

Vous devez configurer les autorisations pour autoriser une IAM entité (telle qu'un utilisateur, un groupe ou un rôle) à créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez la section Autorisations relatives aux rôles liés à un service dans le Guide de l'IAMutilisateur.

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 AWSServiceRoleForOutposts _*OutpostID* rôle lié au service. 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. Vous pouvez toutefois modifier la description du rôle à l'aide deIAM. Pour plus d'informations, voir Mettre à jour un rôle lié à un service dans le Guide de l'IAMutilisateur.

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 avant-poste avant de pouvoir supprimer le _ AWSServiceRoleForOutposts*`OutpostID`* rôle lié au service.

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

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

Contactez le Support aux AWS entreprises pour supprimer votre Outpost.

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

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

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

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

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

AWS politique gérée : AWSOutpostsServiceRolePolicy

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 : AWSOutpostsPrivateConnectivityPolicy

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 : AWSOutpostsAuthorizeServerPolicy

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.

```
{
  "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.

Modification	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 les API appels AWS publiés pour accéder aux AWS Outposts via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Sécurité de la couche de transport (TLS). Nous avons besoin de la TLS version 1.2 et recommandons la TLS version 1.3.

- Des suites de chiffrement parfaitement confidentielles (PFS) telles que (Ephemeral Diffie-Hellman) ou DHE ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

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

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

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

Lorsque vous créez un avant-poste, vous sélectionnez une zone de disponibilité AWS dans une région. Cette zone de disponibilité prend en charge les opérations du plan de contrôle, telles que la réponse aux API appels, la surveillance de l'avant-poste et la mise à jour de l'avant-poste. 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.

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

Validation de conformité pour AWS Outposts

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

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

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

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

> **Note**
>
> Tous ne Services AWS sont pas HIPAA éligibles. Pour plus d'informations, consultez la référence des services HIPAA éligibles.

- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.

- AWS Guides de conformité destinés aux clients — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation Services AWS et reprennent les directives relatives aux contrôles de sécurité dans de nombreux cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).
- Évaluation des ressources à l'aide des règles du guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub— Cela Service AWS fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez Référence des contrôles Security Hub.
- Amazon GuardDuty — Cela Service AWS détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité PCIDSS, par exemple en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.
- AWS Audit Manager— Cela vous Service AWS permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

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 à l'APIaction pour AWS Outposts. Ils contiennent également des informations relatives aux appels à l'APIaction lancés par les services d'un Outpost, tels qu'Amazon EC2 et AmazonEBS. Pour de plus amples informations, veuillez consulter Enregistrez les API appels en utilisant CloudTrail.

Journaux de flux VPC

Utilisez les journaux de VPC flux pour recueillir des informations détaillées sur le trafic à destination et en provenance de votre avant-poste et à l'intérieur de votre avant-poste. Pour plus d'informations, consultez VPCFlow Logs dans le guide de VPC l'utilisateur Amazon.

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.

AWS Health Dashboard

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

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

CloudWatch

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

Vous pouvez utiliser les métriques pour vérifier que le système fonctionne comme prévu. Par exemple, vous pouvez créer une CloudWatch alarme pour surveiller la `ConnectedStatus` métrique. Si la métrique moyenne est inférieure à1, CloudWatch vous pouvez lancer une action, telle que l'envoi d'une notification à une adresse e-mail. Vous pouvez ensuite étudier les éventuels problèmes de réseau sur site ou par liaison montante susceptibles d'avoir un impact sur les opérations de votre Outpost. Les problèmes courants incluent les récentes modifications apportées à la configuration réseau sur site du pare-feu et des NAT règles, 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 à ce sujet CloudWatch, consultez le guide de CloudWatch l'utilisateur Amazon.

Table des matières

Métriques

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

`ConnectedStatus`

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

Unité : nombre

Résolution maximale : 1 minute

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

Dimensions : `OutpostId`

`CapacityExceptions`

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

Unité : nombre

Résolution maximale : 5 minutes

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

Dimensions : `InstanceType` et `OutpostId`

`InstanceFamilyCapacityAvailability`

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

Unité : pourcentage

Résolution maximale : 5 minutes

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

Dimensions : `InstanceFamily` et `OutpostId`

`InstanceFamilyCapacityUtilization`

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

Unité : pourcentage

Résolution maximale : 5 minutes

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

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

`InstanceTypeCapacityAvailability`

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

Unité : pourcentage

Résolution maximale : 5 minutes

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

Dimensions : `InstanceType` et `OutpostId`

`InstanceTypeCapacityUtilization`

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

Unité : pourcentage

Résolution maximale : 5 minutes

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

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

`UsedInstanceType_Count`

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

Unité : nombre

Résolution maximale : 5 minutes

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

`AvailableInstanceType_Count`

Nombre de types d'instances disponibles. Cette métrique inclut le `AvailableReservedInstances` nombre.

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

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

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

Unité : nombre

Résolution maximale : 5 minutes

Dimensions : `InstanceType` et `OutpostId`

`AvailableReservedInstances`

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

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

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

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

Unité : nombre

Résolution maximale : 5 minutes

Dimensions : `InstanceType` et `OutpostId`

`UsedReservedInstances`

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

Unité : nombre

Résolution maximale : 5 minutes

Dimensions : `InstanceType` et `OutpostId`

`TotalReservedInstances`

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

Unité : nombre

Résolution maximale : 5 minutes

Dimensions : `InstanceType` et `OutpostId`

Dimensions métriques

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

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

Dimension	Description
`VirtualInterfaceGroupId`	ID du groupe d'interfaces virtuelles pour l'interface virtuelle de la passerelle locale (VIF).

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 AWS Outposts API appels en utilisant 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 API les appels 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 AWS Outposts API opérations. 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 de IAM l'Identity Center.
- 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 CloudTrailLake.

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 pouvez créer un parcours à région unique ou multirégionale à l'aide du. 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 parcours à région unique, vous ne pouvez voir que les événements enregistrés dans le parcours. Région AWS Pour plus d'informations sur les sentiers, consultez les sections Création d'un sentier pour votre organisation Compte AWS et Création d'un sentier pour une organisation dans le guide de AWS CloudTrail 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 SQL des requêtes basées sur vos événements. CloudTrail Lake convertit les événements existants au JSON format basé sur les lignes au ORC format Apache. ORCest un format de stockage en colonnes optimisé pour une extraction 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 des AWS

Outposts auxquelles Outposts se connecte, CloudTrail consultez le Guide de référence des AWS Outposts.AWS API

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**
>
> Si le lecteur de disque sous-jacent rencontre une défaillance ou si l'instance s', les données stockées sur les volumes de stockage d'instances sont perdues. Pour éviter toute perte de données, nous vous recommandons de sauvegarder 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'EC2instances Amazon exécutées sur votre serveur Outposts, nous informerons le propriétaire de l'Outpost et le propriétaire des instances que les instances

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

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 hors des équipements des Outposts de manière contrôlée, en utilisant des modifications d'équilibrage de charge DNS basées ou non sur le rack.
- 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 AWS Outposts 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.

EC2Les instances Amazon, le LNI réseau et les volumes de stockage d'instances sur le serveur Outposts continueront de fonctionner normalement et seront accessibles localement via le réseau local et. LNI De même, les ressources de AWS service telles que les ECS nœuds de travail Amazon

continuent de s'exécuter localement. Cependant, API la disponibilité 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 quelques heures et seront transmis à la AWS région lorsque la connectivité sera rétablie. Une déconnexion au-delà de quelques heures peut toutefois entraîner la perte de métriques 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 AWS Health Dashboard envoie une notification au compte propriétaire des Outposts. Ni vous ni ne AWS pouvez supprimer la notification d'une interruption de liaison de service, même si l'interruption est prévue. Pour plus d’informations, consultez Premiers pas avec le AWS Health Dashboard dans le Guide de l’utilisateur AWS Health .

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

- Si 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, l'outil de débogage pour la connectivité réseau d'Amazon, VPC explique l'outil AWSSupport-S etupIPMonitoring FromVPC. Cet outil est un AWS Systems Manager document (SSMdocument) qui crée une instance Amazon EC2 Monitor dans un sous-réseau que vous avez spécifié et qui surveille les adresses IP cibles. Le document exécute des tests de diagnostic pingMTR, 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

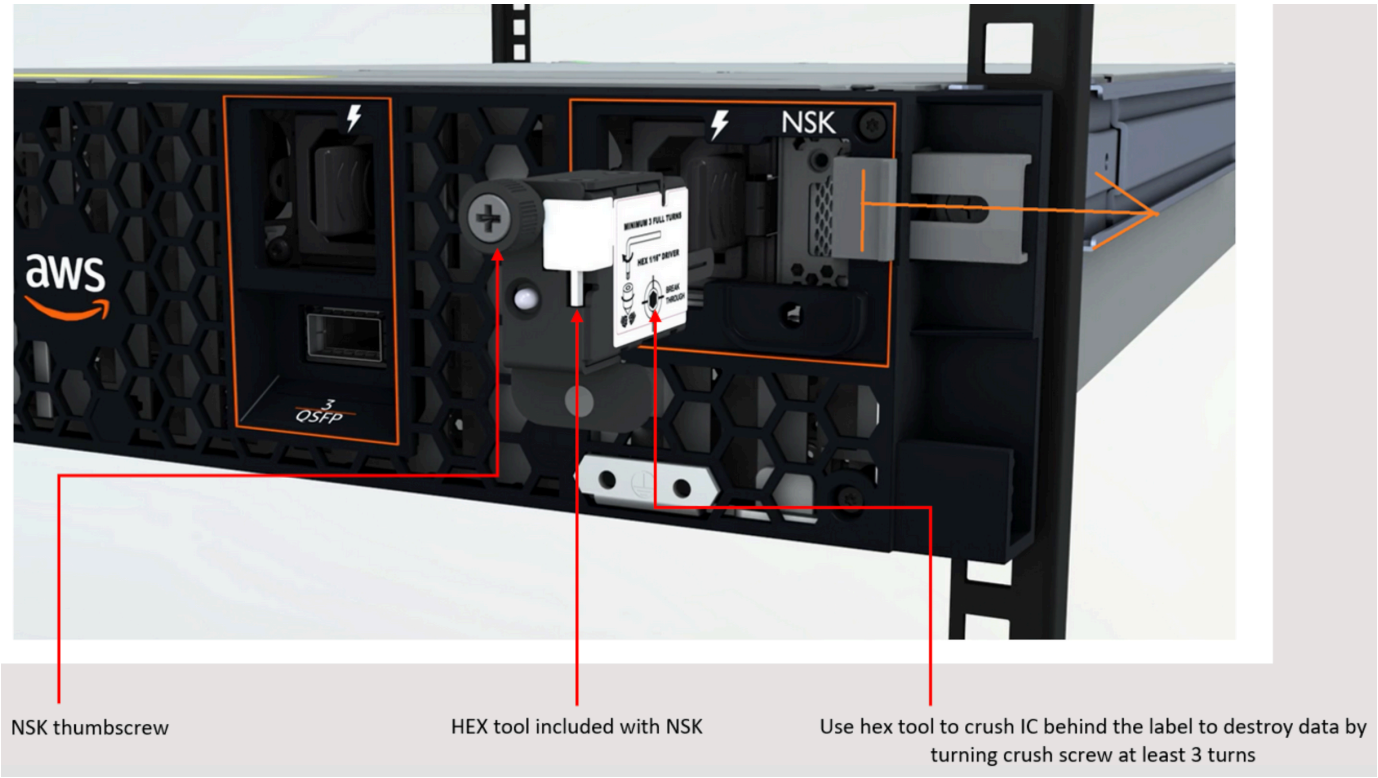
- Le AWS blog Déploiement d'un CloudWatch tableau de bord Amazon automatisé AWS Outposts à utiliser AWS CDK décrit les étapes du déploiement d'un tableau de bord automatisé.
- Si vous avez des questions ou si vous souhaitez obtenir des informations supplémentaires, consultez Création d’un dossier de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

Déchiquetage par chiffrement des données d’un serveur

La clé de sécurité Nitro (NSK) est requise pour déchiffrer les données sur le serveur. Lorsque vous replacez le serveur AWS, soit parce que vous le remplacez, soit parce que vous interrompez le service, vous pouvez le détruire NSK pour déchiqueter 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 bonne NSK information livrée 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. Cette action détruit NSK et détruit cryptographiquement toutes les données du 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.
- Mettez fin à votre abonnement et restituez 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 30 jours avant la fin de l'abonnement en cours pour vos serveurs Outposts.

Pour renouveler votre abonnement et conserver vos serveurs Outposts existants

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

   - Sans frais initiaux
   - Frais initiaux partiels
   - Tous les frais initiaux

   Pour connaître les tarifs, consultez les Tarification des serveurs AWS Outposts. Vous pouvez également demander un devis.
10. Choisissez Next step: Solve now or contact us (Étape suivante : résolvez maintenant ou contactez-nous).

11. Sur la page Contact us (Contactez-nous), choisissez votre langue préférée.
12. Choisissez votre méthode de contact préférée.
13. Vérifiez les détails de votre cas et choisissez Submit (Envoyer). Votre numéro d'ID de dossier et votre résumé apparaissent.

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

Si vous n'indiquez pas que vous souhaitez renouveler votre abonnement ou 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.

Mettez fin à votre abonnement et renvoyez le serveur

Vous devez effectuer les étapes suivantes au moins 30 jours 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.

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

Pour mettre fin à votre abonnement

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

8. Dans la page Informations supplémentaires, pour Objet, entrez une demande claire, telle que **`End my Outpost subscription`**.
9. Dans Description, entrez la date à laquelle vous souhaitez mettre fin à votre abonnement.
10. Choisissez Next step: Solve now or contact us (Étape suivante : résolvez maintenant ou contactez-nous).
11. Sur la page Contact us (Contactez-nous), choisissez votre langue préférée.
12. Choisissez votre méthode de contact préférée.
13. Si nécessaire, sauvegardez toutes les instances et les données d'instance présentes sur votre serveur.
14. Mettez fin aux instances lancées sur votre serveur.
15. Vérifiez les détails de votre cas et choisissez Submit (Envoyer). Votre numéro d'ID de dossier et votre résumé apparaissent.
16. NOTÉteignez ou déconnectez le serveur du réseau jusqu'à ce que le dossier d'assistance vous le demande.

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

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

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

Pour afficher les quotas pourAWS Outposts, ouvrez la boîte de dialogue Service Quotas Console (Console Service Quotas. Dans le volet de navigation, choisissez Services AWS, puis sélectionnez AWS Outposts.

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

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

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

AWS Outpostset les quotas pour les autres services

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

Modification	Description	Date
Gestion des capacités	Vous pouvez modifier la configuration de capacité par défaut pour votre nouvelle commande d'Outposts.	16 avril 2024
nd-of-term Options E pour 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
Hôtes dédiés sur AWS Outposts	Vous pouvez désormais utiliser des hôtes dédiés sur Outposts.	31 mai 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.