Guia do usuário para os racks

AWS Outposts

AWS Outposts: Guia do usuário para os racks

Table of Contents

O que é AWS Outposts?

AWS Outposts é um serviço totalmente gerenciado que estende a AWS infraestrutura, os serviços, as APIs e as ferramentas até as instalações do cliente. Ao fornecer acesso local à infraestrutura AWS gerenciada, AWS Outposts permite que os clientes criem e executem aplicativos no local usando as mesmas interfaces de programação AWS das regiões, enquanto usam recursos locais de computação e armazenamento para reduzir a latência e as necessidades locais de processamento de dados.

Um posto avançado é um pool de capacidade de AWS computação e armazenamento implantado no local do cliente. AWS opera, monitora e gerencia essa capacidade como parte de uma AWS região. Você pode criar sub-redes em seu Outpost e especificá-las ao criar AWS recursos como instâncias EC2, volumes do EBS, clusters do ECS e instâncias do RDS. As instâncias nas sub-redes Outpost se comunicam com outras instâncias na AWS região usando endereços IP privados, tudo dentro da mesma VPC.

> **Note**
>
> Você não pode conectar um Outpost a outro Outpost ou a outra zona local que esteja dentro da mesma VPC.

Para obter mais informações, consulte a AWS Outposts página do produto .

Principais conceitos

Esses são os conceitos-chave para AWS Outposts.

- Local do Outpost — Os edifícios físicos gerenciados pelo cliente onde AWS instalará seu Outpost. Um local deve atender aos requisitos de instalação, rede e energia do seu Outpost.
- Capacidade do Outpost – Recursos de computação e armazenamento disponíveis no Outpost. Você pode visualizar e gerenciar a capacidade do seu Outpost a partir do console do AWS Outposts .
- Equipamento Outpost — Hardware físico que fornece acesso ao AWS Outposts serviço. O hardware inclui racks, servidores, comutadores e cabeamento de propriedade e gerenciados pela. AWS

- Racks do Outposts – Um fator forma do Outpost que é um rack 42U padrão do setor. Os racks do Outpost incluem servidores montáveis em rack, switches, um painel de patches de rede, uma bandeja de alimentação e painéis vazios.
- Servidores dos Outposts – Um fator forma do Outpost, que é um servidor 1U ou 2U padrão do setor, podendo ser instalado em um rack de 4 posições compatível com EIA-310D 19 padrão. Os servidores do Outpost fornecem serviços locais de computação e de rede para sites com espaço limitado ou requisitos de capacidade menores.
- Link de serviço — Rota de rede que permite a comunicação entre seu Posto Avançado e sua AWS região associada. Cada Outpost é uma extensão de uma zona de disponibilidade e sua região associada.
- Gateway local (LGW) — Um roteador virtual de interconexão lógica que permite a comunicação entre um rack Outpost e sua rede local.
- Interface de rede local – Uma interface de rede que permite a comunicação entre um servidor do Outpost e sua rede on-premises.

AWS recursos em Outposts

Você pode criar os seguintes recursos em seu Outpost para fornecer suporte a workloads de baixa latência que precisam ser executadas perto de dados e aplicativos on-premises:

Computação

Tipo de recurso	Racks	Servidores
Instâncias do Amazon EC2	S	Sim
Clusters do Amazon ECS	S	Sim
Nós do Amazon EKS	S	Não

Banco de dados e análises

Tipo de recurso	Racks	Servidores
ElastiCache Nós da Amazon (cluster Redis, cluster Memcached)	S	Não
Clusters do Amazon EMR	S	Não
Instâncias de banco de dados do Amazon RDS	S	Não

Redes

Tipo de recurso	Racks	Servidores
Proxy Envoy do App Mesh	S	Sim
Application Load Balancers	S	Não
Sub-redes da Amazon VPC	S	Sim
Amazon Route 53	S	Não

Armazenamento

Tipo de recurso	Racks	Servidores
Volumes do Amazon EBS	 S	 Não
Buckets do Amazon S3	 S	 Não

Outros Serviços da AWS

Serviço	Racks	Servidores
AWS IoT Greengrass	 S	 Sim
Gerenciador Amazon SageMaker Edge	 S	 Sim

Definição de preço

Você pode escolher entre uma variedade de configurações do Outpost, cada uma delas fornecendo uma combinação de tipos de instância do EC2 e opções de armazenamento. O preço das configurações de rack inclui instalação, remoção e manutenção. Para servidores, você deve instalar e manter o equipamento.

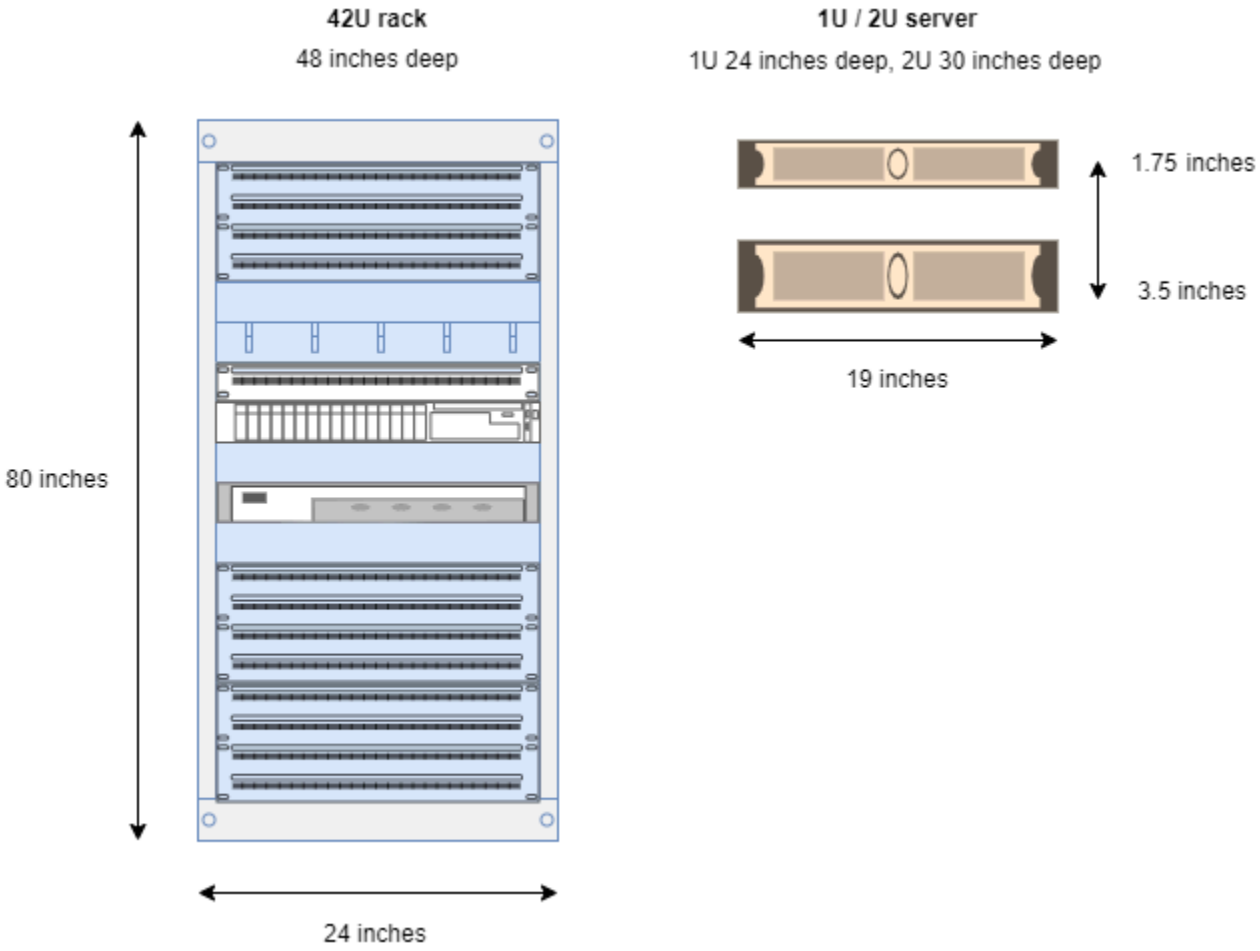
Você compra uma configuração por um período de três anos e pode escolher entre três opções de pagamento: todos os adiantados, adiantamento parcial e sem adiantamento. Se você escolher a opção Parcial ou a opção Nenhum pagamento adiantado, cobranças mensais serão aplicadas. Todas as cobranças adiantadas se aplicam 24 horas após a instalação do Outpost e a capacidade de computação e armazenamento estar disponível para uso. Para obter mais informações, consulte:

- AWS Outposts preços de rack
- AWS Outposts preços de servidores

Como o AWS Outposts funciona

O AWS Outposts foi projetado para operar com uma conexão constante e consistente entre seu Outpost e uma região AWS. Para obter essa conexão com a região e com as workloads locais em seu ambiente on-premises, você deve conectar seu Outpost à sua rede on-premises. Sua rede on-premises deve fornecer acesso à rede de longa distância (WAN) de volta à região e à Internet. Ela também deve fornecer acesso LAN ou WAN à rede local em que residem suas workloads ou aplicativos on-premises.

O diagrama a seguir ilustra os dois formatos do Outpost.



Índice

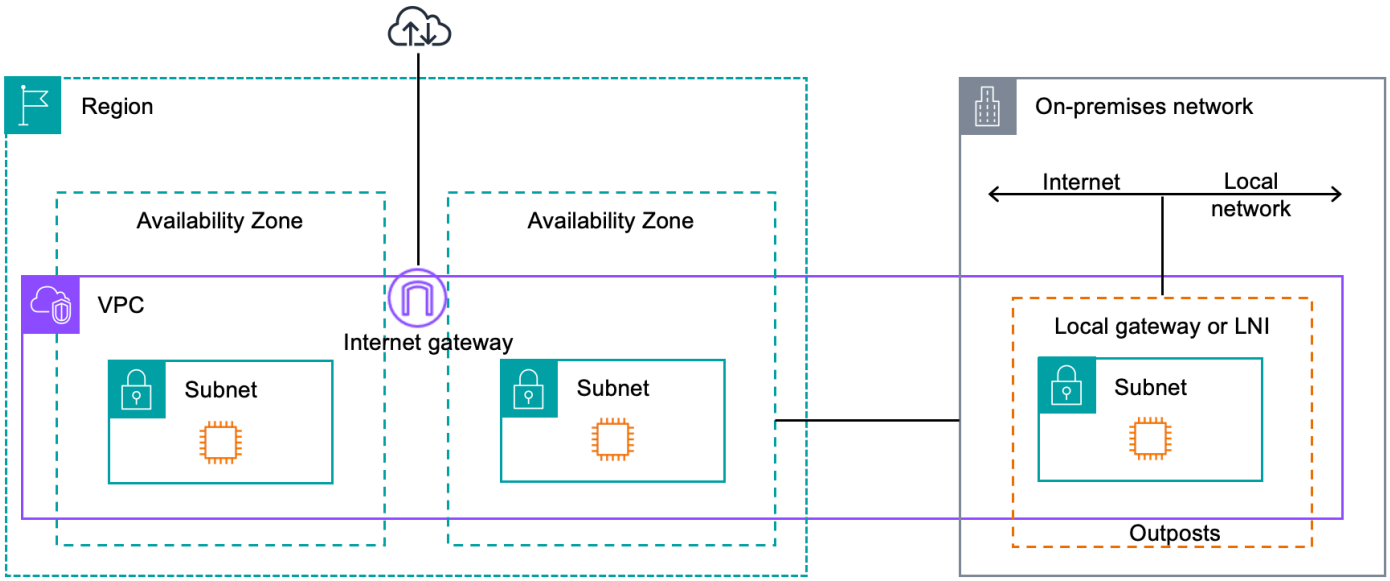
- DNS
- Link de serviço
- Gateways locais
- Interfaces de rede local

Componentes da rede

O AWS Outposts estende um Amazon VPC de uma região da AWS para um Outpost com os componentes da VPC que estão acessíveis na região, incluindo gateways da Internet, gateways privados virtuais, Amazon VPC Transit Gateways e endpoints da VPC. Um Outpost fica hospedado em uma zona de disponibilidade na região e é uma extensão dessa zona de disponibilidade que você pode usar para resiliência.

O diagrama a seguir mostra os componentes de rede do seu Outpost.

- Uma Região da AWS e uma rede on-premises
- Uma VPC com várias sub-redes na região
- Um Outpost na rede on-premises
- Conectividade entre o Outpost e a rede local fornecida por um gateway local (racks) ou uma interface de rede local (servidores)



VPCs e sub-redes

Uma nuvem privada virtual (VPC) abrange todas as zonas de disponibilidade em sua região AWS. É possível estender qualquer VPC na região da ao Outpost adicionando uma sub-rede do Outpost. Para adicionar uma sub-rede do Outpost a uma VPC, especifique o nome do recurso da Amazon (ARN) do Outpost ao criar a sub-rede.

Os Outposts oferecem suporte a várias sub-redes. Você pode especificar a sub-rede de instância do EC2 ao executar a instância do EC2 em seu Outpost. Você não pode especificar o hardware subjacente em que a instância é implantada porque o Outpost é um grupo de capacidade de computação e armazenamento da AWS.

Cada Outpost pode suportar várias VPCs que, por sua vez, podem ter uma ou mais sub-redes do Outpost. Para obter mais informações sobre as cotas da VPC, consulte Amazon VPC Quotas no Manual do usuário da Amazon VPC.

Você cria sub-redes do Outpost a partir do intervalo CIDR da VPC em que você criou o Outpost. Você pode usar os intervalos de endereços do Outpost para recursos, como instâncias do EC2 que residem na sub-rede do Outpost.

Roteamento

Por padrão, cada sub-rede do Outpost herda a tabela de rotas principal de sua VPC. Você pode criar uma tabela de rotas personalizada e associá-la a uma sub-rede.

As tabelas de rotas para sub-redes do Outpost funcionam da mesma forma que as tabelas de rotas para sub-redes da zona de disponibilidade. Você pode especificar endereços IP, gateways da Internet, gateways locais, gateways privados virtuais e conexões de emparelhamento como destinos. Por exemplo, cada sub-rede do Outpost, seja por meio da tabela de rota principal herdada ou de uma tabela personalizada, herda a rota local da VPC. Isso significa que todo o tráfego na VPC, incluindo a sub-rede do Outpost com um destino no CIDR da VPC, permanece roteado na VPC.

As tabelas de rotas de sub-rede do Outpost podem incluir os seguintes destinos:

- Intervalo CIDR da VPC: a AWS define este intervalo na instalação. Essa é a rota local e se aplica a todo o roteamento da VPC, incluindo o tráfego entre instâncias do Outpost na mesma VPC.
- AWS Destinos da região : inclui listas de prefixos para Amazon Simple Storage Service (Amazon S3), endpoints de gateway do Amazon DynamoDB, gateways privados virtuais do AWS Transit Gateway, gateways da internet e emparelhamento de VPC.

Se você tiver uma conexão de emparelhamento com várias VPCs no mesmo Outpost, o tráfego entre as VPCs permanecerá no Outpost e não usará o link de serviço de volta para a região.

- Comunicação intra-VPC entre Outposts com gateway local: você pode estabelecer comunicação entre sub-redes na mesma VPC entre diferentes Outposts com gateways locais usando roteamento Direct VPC. Para obter mais informações, consulte:
  - Roteamento Direct VPC
  - Roteamento para um AWS Outposts gateway local

DNS

Para interfaces de rede conectadas à VPC, as instâncias do EC2 em sub-redes Outposts podem usar o Serviço Amazon Route 53 DNS para resolver nomes de domínio para endereços IP. O Route 53 oferece suporte a recursos de DNS, como registro de domínios, roteamento de DNS e verificações de integridade para instâncias em execução no seu Outpost. Zonas de disponibilidade hospedadas, tanto públicas quanto privadas, são compatíveis para rotear o tráfego para domínios específicos. Os resolvedores do Route 53 estão hospedados na região AWS. Portanto, a conectividade do link de serviço do Outpost até a região AWS deve estar ativa para que esses recursos de DNS funcionem.

Você pode encontrar tempos mais longos de resolução de DNS com Route 53, dependendo da latência do caminho entre o Outpost e a região da AWS. Nesses casos, você pode usar os servidores DNS instalados localmente em seu ambiente local. Para usar seus próprios servidores DNS, você deve criar conjuntos de opções de DHCP para seus servidores DNS on-premises e associá-los à VPC. Você também deve garantir que haja conectividade IP com esses servidores DNS. Talvez você também precise adicionar rotas à tabela de roteamento de gateway local para fins de acessibilidade, mas essa opção é apenas para racks do Outpost com gateway local. Como os conjuntos de opções de DHCP têm um escopo de VPC, as instâncias nas sub-redes do Outpost e nas sub-redes da zona de disponibilidade da VPC tentarão usar os servidores DNS especificados para resolução de nomes DNS.

As consultas em log não são compatíveis para consultas ao DNS originadas de um Outpost.

Link de serviço

O link de serviço é uma conexão do seu Outpost com a região AWS de sua escolha ou com a região de origem do Outpost. O link de serviço é um conjunto criptografado de conexões VPN que

são usadas sempre que o Outpost se comunica com a região de origem escolhida. Você usa uma LAN virtual (VLAN) para segmentar o tráfego no link de serviço. O link de serviço VLAN permite a comunicação entre o Outpost e a região AWS para o gerenciamento do tráfego do Outpost e do tráfego intra-VPC entre a região AWS e o Outpost.

Seu link de serviço é criado quando seu Outpost é provisionado. Se você tiver um formato de servidor, crie a conexão. Se você tiver um rack, a AWS cria o link de serviço. Para obter mais informações, consulte Conectividade do Outpost com as Regiões da AWS.

Gateways locais

Os racks do Outpost incluem um gateway local para fornecer conectividade à sua rede on-premises. Se você tiver um rack do Outpost, poderá incluir um gateway local como destino, onde o destino é sua rede on-premises. Os gateways locais só estão disponíveis para racks do Outpost e só podem ser usados em tabelas de rotas de VPCs e sub-redes associadas a um rack do Outpost. Para obter mais informações, consulte Gateway local.

Interfaces de rede local

Os servidores do Outpost incluem uma interface de rede local para fornecer conectividade à sua rede on-premises. Uma interface de rede local está disponível somente para servidores do Outposts executados em uma sub-rede do Outpost. Você não pode usar uma interface de rede local de uma instância do EC2 em um rack do Outpost ou na região AWS. A interface de rede local é destinada apenas a locais on-premises. Para obter mais informações, consulte Interfaces de rede local no Guia do usuário do AWS Outposts para servidores Outposts.

Requisitos do local para o rack do Outposts

Um local do Outpost é a localização física do seu equipamento Outpost. Os sites estão disponíveis somente em alguns países e territórios. Para obter mais informações, consulte Perguntas frequentes sobre o rack AWS Outposts. Consulte a pergunta: Em quais países e territórios o rack do Outposts está disponível?

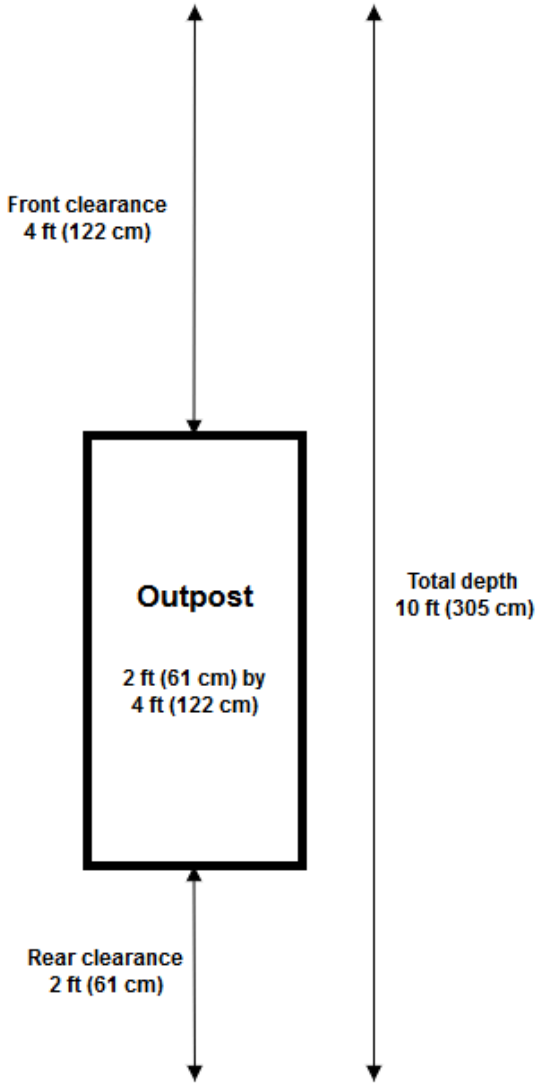
Esta página aborda os requisitos do rack do Outposts. Para obter os requisitos dos servidores do Outposts, consulte Requisitos do local para servidores do Outposts no Guia do usuário do AWS Outposts para servidores do Outposts.

Instalações

Esses são os requisitos da instalação para racks.

- Temperatura e umidade – A temperatura ambiente deve estar entre 5° C e 35° C. A umidade relativa deve estar entre 8 e 80% sem condensação.
- Fluxo de ar – Os racks retiram o ar frio do corredor frontal e expelem o ar quente para o corredor traseiro. A posição do rack deve fornecer pelo menos 145,8 vezes o fluxo de ar em kVA de pés cúbicos por minuto (CFM).
- Plataforma de carregamento – Sua plataforma de carregamento deve acomodar uma caixa de rack com 239 cm de altura por 138 cm de largura por 130 cm de profundidade.
- Suporte de peso – O peso varia de acordo com a configuração. Você pode encontrar o peso de sua configuração especificado no resumo do pedido nas cargas do ponto do rack. O local onde o rack está instalado e o caminho até esse local devem suportar o peso especificado. Isso inclui quaisquer elevadores padrão e de carga ao longo do caminho.
- Espaço livre – O rack tem 203 cm de altura por 61 cm de largura por 122 cm de profundidade. Todas as portas, corredores, curvas, rampas e elevadores devem fornecer espaço livre suficiente. Na posição final de repouso, deve haver uma área de 61 cm de largura por 122 cm de profundidade para o Outpost, com 122 cm de espaço livre frontal e 61 cm de espaço livre traseiro. A área mínima total necessária para o Outpost é de 61 cm de largura por 305 cm de profundidade.

  O diagrama a seguir mostra a área mínima total necessária para o Outpost, incluindo o espaço livre.



- Suporte sísmico — Na medida exigida pela regulamentação ou pelo código, você instalará e manterá a ancoragem sísmica e o suporte adequados para o rack enquanto ele estiver em suas instalações. AWSfornece suportes de piso que fornecem proteção para até 2,0 G de atividade sísmica em todos os racks Outposts.
- Ponto de ligação – Recomendamos que você forneça um cabo/ponto de ligação na posição do rack para que o técnico certificado da AWS possa unir os racks durante a instalação.
- Acesso às instalações – Você não alterará as instalações de uma forma que afete negativamente a capacidade da AWS de acessar, reparar ou remover o Outpost.
- Elevação – A elevação da sala onde o rack está instalado deve estar abaixo de 3.050 metros.

Redes

Esses são os requisitos de rede para racks.

- Forneça uplinks com velocidades de 1 Gbps, 10 Gbps, 40 Gbps ou 100 Gbps.

  Para recomendações de largura de banda para a conexão do link de serviço, consulte Recomendações de largura de banda.
- Forneça fibra monomodo (SMF) com conector Lucent (LC), fibra multimodo (MMF) ou MMF OM4 com LC.
- Forneça um ou dois dispositivos upstream, que podem ser switches ou roteadores. Recomendamos dois dispositivos para oferecer alta disponibilidade.

Lista de verificação de prontidão da rede

Use essa lista de verificação quando estiver reunindo as informações para a configuração do Outpost. Isso inclui a LAN, a WAN e quaisquer dispositivos entre o Outpost e os destinos de tráfego local, além do destino na AWS Region.

Velocidade do uplink, portas e fibra

Velocidade do uplink e portas

Um Outpost tem dois dispositivos de rede que se conectam à sua rede local. O número de uplinks que cada dispositivo pode suportar depende de suas necessidades de largura de banda e do que seu roteador pode suportar. Para ter mais informações, consulte Conectividade física.

A lista a seguir mostra quantas portas de uplink são suportadas para cada dispositivo de rede do Outpost, com base na velocidade do uplink.

1 Gbps

1, 2, 4, 6 ou 8 uplinks

10 Gbps

1, 2, 4, 8, 12 ou 16 uplinks

40 Gbps ou 100 Gbps

1, 2 ou 4 uplinks

Fibra

Há suporte para os seguintes tipos de fibra:

- Fibra monomodo (SMF) com conector Lucent (LC)
- Fibra multimodo (MMF) ou MMF OM4 com LC

Dependendo da velocidade do uplink e do tipo de fibra que você escolher, os padrões ópticos a seguir serão compatíveis.

Velocidade do uplink	Tipo de fibra	Padrão óptico
1 Gbps	SMF	– 1000Base-LX
1 Gbps	MMF	– 1000Base-SX
10 Gbps	SMF	– 10GBASE-IR – 10GBASE-LR
10 Gbps	MMF	– 10GBASE-SR
40 Gbps	SMF	– 40 GBASE-IR4 (LR4L) – 40 GBASE-LR4
Aplicação de breakout de 4 x 10 Gbps	MMF	– 40GBASE-ESR4 – 40 GBASE-SR4
100 Gbps	SMF	– 100G PSM4 ML – 100GBASE-CWDM4 – 100 GBASE-LR4
Aplicação de breakout de 4 x 25 Gbps	MMF	– 100 GBASE-SR4

Agregação de links e VLANs do Outpost

O protocolo de controle de agregação de links (LACP) é necessário entre o Outpost e sua rede. Você deve usar o LAG dinâmico com o LACP.

As VLANs a seguir são necessárias para cada dispositivo de rede do Outpost. Para ter mais informações, consulte LANs virtuais.

Dispositivo de rede do Outpost	VLAN do link de serviço	VLAN do gateway local
Nº 1	Valores válidos: 1 a 4094	Valores válidos: 1 a 4094
Nº 2	Valores válidos: 1 a 4094	Valores válidos: 1 a 4094

Para cada dispositivo de rede do Outpost, você pode escolher se deseja usar as mesmas VLANs ou VLANs diferentes para o link de serviço e o gateway local. No entanto, recomendamos que cada dispositivo de rede do Outpost tenha uma VLAN diferente do outro dispositivo de rede do Outpost. Para obter mais informações, consulte Agregação de links e LANs virtuais.

Também recomendamos conectividade redundante de camada 2. O LACP é usado para agregação de links e não para alta disponibilidade. O LACP entre os dispositivos de rede do Outpost não é suportado.

Conectividade IP do dispositivo de rede do Outpost

Cada um dos dois dispositivos de rede do Outpost requer um CIDR e um endereço IP para o link de serviço e as VLANs do gateway local. Recomendamos alocar uma sub-rede dedicada para cada dispositivo de rede com um CIDR /30 ou /31. Especifique uma sub-rede e um endereço IP da sub-rede para o Outpost usar. Para ter mais informações, consulte Conectividade da camada de rede.

Dispositivo de rede do Outpost	Requisitos do link de serviço	Requisitos do gateway local
Nº 1	– Link de serviço CIDR (/30 ou /31) – Endereço IP do link de serviço	– Gateway local CIDR (/30 ou /31) – Endereço IP do gateway local

Dispositivo de rede do Outpost	Requisitos do link de serviço	Requisitos do gateway local
Nº 2	– Link de serviço CIDR (/30 ou /31) – Endereço IP do link de serviço	– Gateway local CIDR (/30 ou /31) – Endereço IP do gateway local

Unidade de transmissão máxima (MTU) do link de serviço

A rede deve suportar MTU de 1500 bytes entre o Outpost e os endpoints do link de serviço na região principal. AWS Para obter mais informações sobre a função de serviço, consulte Conectividade do AWS Outposts com regiões AWS.

Protocolo do Gateway de Borda do link de serviço

O Outpost estabelece uma sessão de emparelhamento de BGP externo (eBGP) entre cada dispositivo de rede do Outpost e seu dispositivo de rede local para conectividade do link de serviço pela VLAN do link de serviço. Para ter mais informações, consulte Conectividade do link de serviço BGP.

Outpost	Requisitos do link de serviço
Seu Outpost	– Número de sistema autônomo (ASN) do BGP do Outpost. 2 bytes (16 bits) ou 4 bytes (32 bits). Do seu intervalo de ASN privado (64512-65534 ou 4200000000-4294967294). – CIDR de infraestrutura (/26 obrigatório, anunciado como dois /27s contíguos).

Dispositivo de rede local	Requisitos do link de serviço
Nº 1	– Endereço IP do link de serviço do par do BGP – ASN de par do BGP do link de serviço. 2 bytes (16 bits) ou 4 bytes (32 bits).

Dispositivo de rede local	Requisitos do link de serviço
Nº 2	– Endereço IP do link de serviço do par do BGP – ASN de par do BGP do link de serviço. 2 bytes (16 bits) ou 4 bytes (32 bits).

Firewall do link de serviço

O UDP e o TCP 443 devem estar listados com status no firewall.

Protocolo	Porta de origem	Endereço de origem	Porta de destino	Endereço de destino
UDP	443	Link de serviço /26 do Outpost	443	Rotas públicas da região do Outpost
TCP	1025-65535	Link de serviço /26 do Outpost	443	Rotas públicas da região do Outpost

Você pode usar uma conexão AWS Direct Connect ou uma conexão pública à Internet para conectar o Outpost à região AWS. Para conectividade de link de serviço do Outpost, você pode usar NAT ou PAT em seu firewall ou roteador de borda. O estabelecimento do link de serviço é sempre iniciado a partir do Outpost.

Protocolo de Gateway de Borda do gateway local

O Outpost estabelece uma sessão de emparelhamento do eBGP de cada dispositivo de rede do Outpost para um dispositivo de rede local visando À conectividade da sua rede local com o gateway local. Para ter mais informações, consulte Conectividade do BGP do gateway local.

Outpost	Requisitos de BGP do gateway local
Seu Outpost	– Número de sistema autônomo (ASN) do BGP do Outpost. 2 bytes (16 bits) ou 4 bytes (32 bits). Do seu intervalo de ASN privado (64512-65534 ou 4200000000-4294967294).

Outpost	Requisitos de BGP do gateway local
	– CoIP CIDR para anunciar (público ou privado, mínimo de /26).

Dispositivos da rede local	Requisitos de BGP do gateway local
Nº 1	– Endereço IP de par do BGP do gateway local. – ASN de par do BGP de gateway local. 2 bytes (16 bits) ou 4 bytes (32 bits).
Nº 2	– Endereço IP de par do BGP do gateway local. – ASN de par do BGP de gateway local. 2 bytes (16 bits) ou 4 bytes (32 bits).

Alimentação

A bandeja de alimentação do Outposts suporta três configurações de potência: 5 kVA, 10 kVA ou 15 kVA. A configuração da bandeja de alimentação depende do consumo total de potência da capacidade do Outpost. Por exemplo, se seu recurso Outpost tiver um consumo máximo de potência de 9,7 kVA, você deverá fornecer as configurações de potência para 10 kVA: 4 x L6-30P ou IEC309, dois drops para S1 e dois drops para S2 para alimentação monofásica redundante. As três configurações de potência estão descritas na segunda tabela a seguir.

Para ver os requisitos de consumo de potência para diferentes recursos do Outpost, escolha Procurar catálogo no console do AWS Outposts em https://console.aws.amazon.com/outposts/.

Tensão de linha CA	Monofásica de 208 a 277 VCA (50 ou 60 Hz) Trifásica de 346 a 480 VCA (50 a 60 Hz)
Consumo de energia	5 kVA (4 kW), 10 kVA (9 kW) ou 15 kVA (13 kW)
Proteção CA (disjuntores elétricos upstream)	Para entrada 1N (não redundante) e entrada 2N (redundante): 30 A ou 32 A com disjuntor em curva D ou curva K.

	Somente para entrada 2N (redundante): disjuntor em curva C, curva D ou curva K. Não há suporte para curva B ou inferior.
Tipo de entrada CA (tomada)	Monofásica, três plugues L6-30P, P+P+E, 30A ou três plugues IEC60309 P+N+E, IP67, 32A Trifásica, Wye 1 plugue IEC60309, 3P+N+E, IP67, posição do relógio 7, 30A ou 1 plugue IEC60309, 3P+N+E, IP67, posição do relógio 6, 32A Trifásica, Delta 1 plugue CS8365C Hubbell twistlock não NEMA, 3P+E, terra central, 50A **Note** A prática recomendada é conectar um plugue IP67 a uma tomada IP67. Se isso não for possível, o plugue IP67 será conectado a uma tomada IP44. A classific ação do plugue e do soquete combinados se tornará a classificação menor (IP44).
Comprimento do chicote	3 m
Chicote – Entrada de cabeamento de rack	De cima ou abaixo do rack

A bandeja de alimentação tem duas entradas, S1 e S2, que podem ser configuradas conforme a seguir.

	Redundante, monofásic a	Redundante, trifásica	Fase única	Trifásica
5 kVA	2 x L6-30P ou IEC309, um drop para S1 e um drops para S2	2 x AH530P7W ou AH532P6W, um drop para	1 x L6-30P ou IEC309, um drop para S1	1 x AH530P7W ou AH532P6W, um drop para S1

	Redundante, monofásica	Redundante, trifásica	Fase única	Trifásica
10 kVA	2 x L6-30P ou IEC309, dois drops para S1 e dois drops para S2	S1 e um drop para S2	2 x L6-30P ou IEC309, dois drops para S1	
15 kVA	6 x L6-30P ou IEC309, três drops para S1 e três drops para S2		3 x L6-30P ou IEC309, três drops para S1	

Se o chicote de CA que a AWS fornece, conforme descrito anteriormente, precisar ser equipado com um plugue de potência alternativo, considere o seguinte:

- Somente um eletricista certificado fornecido pelo cliente deve modificar o chicote CA para caber em um novo tipo de plugue.
- A instalação deve estar em conformidade com todos os requisitos de segurança nacionais, estaduais e locais aplicáveis e ser inspecionada conforme necessário quanto à segurança elétrica.
- Você, o cliente, deve notificar seu representante da AWS sobre modificações no plugue do chicote de CA. Mediante solicitação, você fornecerá informações sobre as modificações à AWS. Você também incluirá todos os registros de inspeção de segurança emitidos pela autoridade competente. Esse é um requisito para validar a segurança da instalação antes que os funcionários da AWS trabalhem no equipamento.

Atendimento do pedido

Para atender ao pedido, a AWS agendará uma data e hora com você. Você também receberá uma lista de verificação dos itens a serem verificados ou fornecidos antes da instalação.

A equipe de instalação da AWS chegará ao seu site na data e hora agendadas. A equipe levará o rack até a posição identificada. Você e seu eletricista são responsáveis por realizar a conexão elétrica e a instalação no rack.

Você deve garantir que as instalações elétricas e quaisquer alterações nessas instalações sejam realizadas por um eletricista certificado de acordo com todas as leis, códigos e práticas recomendadas aplicáveis. Você deve obter aprovação da AWS por escrito antes de fazer qualquer alteração no hardware do Outpost ou nas instalações elétricas. Você concorda em fornecer à AWS a

documentação que comprove a conformidade e a segurança de quaisquer alterações. A AWS não é responsável por quaisquer riscos criados pela instalação elétrica do Outpost, pela fiação elétrica da instalação ou por quaisquer alterações. Você não deve fazer nenhuma outra alteração no hardware do Outposts.

A equipe estabelecerá a conectividade de rede para o rack Outposts por meio do uplink fornecido por você e configurará a capacidade do rack.

A instalação será concluída quando você confirma que a capacidader do Amazon EC2 e do Amazon EBS para seu Outpost está disponível em sua Conta da AWS.

Comece com AWS Outposts

Peça um Outpost para começar. Após a instalação do seu equipamento Outpost, inicie as instâncias do Amazon EC2 e acesse sua on-premises.

Tarefas

- Crie um Outpost e solicite capacidade para o Outpost
- Inicie uma instância em seu rack Outpost

Crie um Outpost e solicite capacidade para o Outpost

Para começar a usar AWS Outposts, você deve criar um Posto Avançado e solicitar a capacidade do Posto Avançado.

Pré-requisitos

- Revise as configurações disponíveis para seus racks de Outposts.
- Um local de Outpost é o local físico onde seu equipamento Outpost opera. Antes de solicitar a capacidade, verifique se seu local atende aos requisitos. Para ter mais informações, consulte Requisitos do local para o rack do Outposts.
- Você deve ter um plano de AWS Enterprise Support.
- Determine quem Conta da AWS será o dono do Posto Avançado. Use essa conta para criar o local dos Outposts, criar o Outpost e fazer o pedido. Monitore o e-mail associado a essa conta para obter informações de AWS.

Tarefas

- Etapa 1: Criar um local
- Etapa 2: Criar um Outpost
- Etapa 3: Fazer o pedido
- Etapa 4: modificar a capacidade da instância
- Próximas etapas

Etapa 1: Criar um local

Crie um local para especificar o endereço operacional. O endereço operacional é o local físico dos racks dos Outposts.

Pré-requisitos

- Determine o endereço operacional.

Como criar um local

1. Faça login para AWS usar o Conta da AWS que será dono do Outpost.
2. Abra o AWS Outposts console em https://console.aws.amazon.com/outposts/.
3. Para selecionar o pai Região da AWS, use o seletor de região no canto superior direito da página.
4. No painel de navegação, selecione Locais.
5. Escolha Criar local.
6. Para Tipo de hardware compatível, escolha Racks e servidores.
7. Insira um nome, descrição e endereço operacional para seu site.
8. Para obter detalhes do local, forneça as informações solicitadas sobre o local.
    - Peso máximo – O peso máximo do rack que este site pode suportar, em libras.
    - Consumo de potência – O consumo de potência disponível na posição de colocação do hardware para o rack, em kVA.
    - Opção de alimentação – A opção de alimentação que você pode fornecer para o hardware.
    - Conector de alimentação – O conector de alimentação que a AWS deve planejar para fornecer conexões ao hardware.
    - Queda da fonte de alimentação – Indique se a fonte de alimentação está acima ou abaixo do rack.
    - Velocidade do uplink – A velocidade do uplink que o rack deve suportar para a conexão com a Region, em Gbps.
    - Número de uplinks – O número de uplinks para cada dispositivo de rede do Outpost que você pretende usar para conectar o rack à sua rede.
    - Tipo de fibra – O tipo de fibra que você usará para conectar o rack à sua rede.

- Padrão óptico – O tipo de padrão óptico que você usará para conectar o rack à sua rede.

9. (Opcional) Para notas do site, insira qualquer outra informação que possa ser útil AWS para conhecer o site.
10. Leia os requisitos do lugar de instalação e selecione Eu li os requisitos do lugar de instalação.
11. Escolha Criar local.

Etapa 2: Criar um Outpost

Crie um Outpost para seus racks. Você poderá especificar esse Outpost ao fazer o pedido.

Pré-requisitos

- Determine a zona de AWS disponibilidade a ser associada ao seu site.

Para criar um Outpost

1. No painel de navegação, escolha Outposts.
2. Escolha Criar Outpost.
3. Escolha Racks.
4. Insira um nome e uma descrição para seu Outpost.
5. Escolha uma zona de disponibilidade para o Outpost.
6. (Opcional) Para configurar a conectividade privada, selecione Usar conectividade privada. Escolha uma VPC e uma sub-rede na mesma Conta da AWS zona de disponibilidade do seu Outpost. Para ter mais informações, consulte the section called “Pré-requisitos”.
7. Em ID do local, escolha seu local.
8. Escolha Criar Outpost.

Etapa 3: Fazer o pedido

Faça um pedido dos racks de Outposts de que você precisa. Depois de enviar o pedido, um representante da AWS Outposts entrará em contato com você.

> **Important**
>
> Você não pode editar um pedido depois de enviá-lo, portanto, revise todos os detalhes cuidadosamente antes do envio. Se você precisar alterar um pedido, entre em contato com seu gerente de AWS conta.

Pré-requisitos

- Determine como você pagará pelo pedido. Você pode pagar com adiantamento integral, com adiantamento parcial ou sem adiantamento. Se você optar por pagar tudo adiantado, pagará taxas mensais durante o período de três anos.

  O preço inclui entrega, instalação e manutenção do serviço de infraestrutura, bem como patches e atualizações de software.
- Determine se o endereço de entrega é diferente do endereço operacional que você especificou para o local.

Para fazer um pedido

1. No painel de navegação, escolha Pedidos.
2. Escolha Fazer pedido.
3. Para Tipo de hardware compatível, escolha Racks.
4. Para adicionar capacidade, escolha uma configuração. Se as configurações disponíveis não atenderem às suas necessidades, você pode entrar em contato AWS para solicitar uma configuração de capacidade personalizada.
5. Escolha Próximo.
6. Escolha Usar um Outpost existente e selecione seu Outpost.
7. Escolha Próximo.
8. Selecione um termo de contrato e uma opção de pagamento.
9. Especifique o endereço de entrega. Você pode especificar um novo endereço ou selecionar o endereço operacional do local. Se você selecionar o endereço operacional, esteja ciente de que qualquer alteração futura no endereço operacional do local não se propagará aos pedidos existentes. Se você precisar alterar o endereço de entrega em um pedido existente, entre em contato com seu gerente de AWS conta.

10. Escolha Próximo.
11. Na página Revisão e pedido, verifique se suas informações estão corretas e edite-as conforme necessário. Você não poderá editar o pedido depois de enviá-lo.
12. Escolha Fazer pedido.

Etapa 4: modificar a capacidade da instância

Um posto avançado fornece um pool de capacidade AWS computacional e de armazenamento em seu local como uma extensão privada de uma zona de disponibilidade em uma AWS região. Como a capacidade computacional e de armazenamento disponível no Outpost é finita e determinada pelo tamanho e número de racks AWS instalados em seu site, você decide quanto Amazon EC2, Amazon EBS e Amazon S3 AWS Outposts em capacidade precisa para executar suas cargas de trabalho iniciais, acomodar o crescimento futuro e fornecer capacidade extra para mitigar falhas no servidor e eventos de manutenção.

A capacidade de cada novo pedido do Outpost é configurada com uma configuração de capacidade padrão. Você pode converter a configuração padrão para criar várias instâncias para atender às suas necessidades comerciais. Para fazer isso, você cria uma tarefa de capacidade, especifica os tamanhos e a quantidade da instância e executa a tarefa de capacidade para implementar as alterações.

> **Note**
>
> - Você pode alterar a quantidade de tamanhos de instância depois de fazer o pedido de seus Outposts.
> - Os tamanhos e quantidades das instâncias são definidos no nível do Outpost.
> - As instâncias são colocadas automaticamente com base nas melhores práticas.

Para modificar a capacidade da instância

1. No painel de navegação AWS Outposts esquerdo do AWS Outposts console, escolha Tarefas de capacidade.
2. Na página Tarefas de capacidade, escolha Criar tarefa de capacidade.
3. Na página de introdução, escolha o pedido.

4. Para modificar a capacidade, você pode usar as etapas no console ou fazer upload de um arquivo JSON.

Console steps

1. Escolha Modificar uma nova configuração de capacidade do Outpost.
2. Escolha Próximo.
3. Na página Configurar capacidade da instância, cada tipo de instância mostra um tamanho de instância com a quantidade máxima pré-selecionada. Para adicionar mais tamanhos de instância, escolha Adicionar tamanho da instância.
4. Especifique a quantidade da instância e anote a capacidade exibida para esse tamanho de instância.
5. Veja a mensagem no final de cada seção do tipo de instância que informa se você está acima ou abaixo da capacidade. Faça ajustes no tamanho da instância ou no nível da quantidade para otimizar sua capacidade total disponível.
6. Você também pode solicitar AWS Outposts a otimização da quantidade de instâncias para um tamanho de instância específico. Para fazer isso:
   a. Escolha o tamanho da instância.
   b. Escolha Balanceamento automático no final da seção relacionada ao tipo de instância.
7. Para cada tipo de instância, certifique-se de que a quantidade da instância seja especificada para pelo menos um tamanho de instância.
8. Escolha Próximo.
9. Na página Revisar e criar, verifique as atualizações que você está solicitando.
10. Escolha Criar. AWS Outposts cria uma tarefa de capacidade.
11. Na página da tarefa de capacidade, monitore o status da tarefa.

> **Note**
>
> AWS Outposts pode solicitar que você interrompa uma ou mais instâncias em execução para permitir a execução da tarefa de capacidade. Depois de parar essas instâncias, AWS Outposts executará a tarefa.

Upload JSON file

1. Escolha Carregar uma configuração de capacidade.
2. Escolha Próximo.
3. Na página Plano de configuração de capacidade de upload, faça upload do arquivo JSON que especifica o tipo, o tamanho e a quantidade da instância.

   Example

   Exemplo de arquivo JSON:

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

4. Examine o conteúdo do arquivo JSON na seção Plano de configuração de capacidade.
5. Escolha Próximo.
6. Na página Revisar e criar, verifique as atualizações que você está solicitando.
7. Escolha Criar. AWS Outposts cria uma tarefa de capacidade.
8. Na página da tarefa de capacidade, monitore o status da tarefa.

> **Note**
>
> AWS Outposts pode solicitar que você interrompa uma ou mais instâncias em execução para permitir a execução da tarefa de capacidade. Depois de parar essas instâncias, AWS Outposts executará a tarefa.

Próximas etapas

Você pode ver o status do seu pedido usando o AWS Outposts console. O status inicial do seu pedido é Pedido recebido. Um AWS representante entrará em contato com você em até três dias úteis. Você receberá um e-mail de confirmação quando o status do seu pedido mudar para Pedido em processamento. Um AWS representante pode entrar em contato com você para obter qualquer informação adicional AWS necessária.

Se você tiver alguma dúvida sobre seu pedido, entre em contato com o AWS Support.

Para atender ao pedido, AWS agendaremos uma data e hora com você.

Você também receberá uma lista de verificação dos itens a serem verificados ou fornecidos antes da instalação. A equipe AWS de instalação chegará ao seu local na data e hora programadas. A equipe rolará o rack até a posição identificada e seu eletricista poderá alimentá-lo. A equipe estabelecerá a conectividade de rede para o rack por meio do uplink fornecido por você e configurará a capacidade do rack. A instalação é concluída quando você confirma que a capacidade do Amazon EC2 e do Amazon EBS para seu Outpost está disponível em sua conta. AWS

Inicie uma instância em seu rack Outpost

Depois que o Outpost for instalado e a capacidade de computação e armazenamento estiver disponível para uso, você poderá começar criando recursos. Execute instâncias do Amazon EC2 e crie volumes do Amazon EBS em seu Outpost usando uma sub-rede do Outpost. É possível também criar snapshots de volumes do Amazon EBS no seu Outpost. Para obter mais informações aplicáveis ao Linux, consulte Snapshots locais do Amazon EBS em AWS Outposts no Guia do usuário do Amazon EC2 para instâncias do Linux. Para obter mais informações aplicáveis ao Windows, consulte Snapshots locais do Amazon EBS AWS Outposts no Guia do usuário do Amazon EC2 para instâncias do Windows .

Pré-requisito

É necessário ter um Outpost instalado em seu local. Para ter mais informações, consulte Crie um Outpost e solicite capacidade para o Outpost.

Tarefas

- Etapa 1: Criar uma VPC
- Etapa 2: criar uma sub-rede e uma tabela de rotas personalizada
- Etapa 3: Configurar a conectividade do gateway local

- Etapa 4: Configurar a rede local
- Etapa 5: iniciar uma instância no Outpost
- Etapa 6: testar a conectividade

Etapa 1: Criar uma VPC

Você pode estender qualquer VPC na AWS região até seu Posto Avançado. Ignore esta etapa se você já tiver uma VPC que possa usar.

Para criar uma VPC para seu Outpost

1. Abra o console do Amazon VPC em https://console.aws.amazon.com/vpc/.
2. Escolha a mesma região do rack Outposts.
3. No painel de navegação, escolha Suas VPCs e, em seguida, escolha Criar VPC.
4. Escolha somente VPC.
5. (Opcional) em Etiqueta de nome, insira um nome para a VPC.
6. Para o bloco CIDR IPv4, escolha a entrada manual IPv4 CIDR e insira o intervalo de endereços IPv4 para a VPC na caixa de texto IPv4 CIDR.

   > **Note**
   >
   > Se você quiser usar o roteamento direto de VPC, especifique um intervalo CIDR que não se sobreponha ao intervalo de IP que você usa na sua rede local.

7. Para bloco CIDR IPv6, escolha Nenhum bloco CIDR IPv6.
8. Em Locação, escolha Padrão.
9. (Opcional) Para adicionar uma tag à sua VPC, escolha Adicionar tag e insira uma chave e um valor.
10. Escolha Criar VPC.

Etapa 2: criar uma sub-rede e uma tabela de rotas personalizada

Você pode criar e adicionar uma sub-rede Outpost a qualquer VPC na AWS região em que o Outpost está hospedado. Quando você faz isso, o VPC inclui o Outpost. Para ter mais informações, consulte Componentes da rede.

> **Note**
>
> Se você estiver iniciando uma instância em uma sub-rede Outpost que foi compartilhada com você por outra pessoa Conta da AWS, vá para. Etapa 5: iniciar uma instância no Outpost

2a: Crie uma sub-rede Outpost

Para criar uma sub-rede Outpost

1. Abra o AWS Outposts console em https://console.aws.amazon.com/outposts/.
2. No painel de navegação, escolha Outposts.
3. Selecione o Outpost e, em seguida, escolha Ações, Criar sub-rede. Você será redirecionado para criar uma sub-rede no console da Amazon VPC. Selecionamos o Outpost para você e a zona de disponibilidade na qual ele está alojado.
4. Selecione uma VPC.
5. Em Configurações de sub-rede, opcionalmente, nomeie sua sub-rede e especifique um intervalo de endereços IP para a sub-rede.
6. Escolha Criar sub-rede.
7. (Opcional) Para facilitar a identificação das sub-redes do Outpost, ative a coluna ID do Outpost na página Sub-redes. Para ativar a coluna, escolha o ícone Preferências, selecione Outpost ID e escolha Confirmar.

2b: Crie uma tabela de rotas personalizada

Siga o procedimento abaixo para criar uma tabela de rotas personalizada com uma rota para o gateway local. Você não pode usar a mesma tabela de rotas das sub-redes da zona de disponibilidade.

Para criar uma tabela de rotas personalizada

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Tabelas de rotas.
3. Escolha Create Route Table (Criar tabela de rotas).
4. (Opcional) Em Name (Nome), insira um nome para a tabela de rotas.
5. Em VPC, escolha sua VPC.

6. (Opcional) Para adicionar uma etiqueta, escolha Add new tag (Adicionar nova etiqueta) e insira a chave e o valor da etiqueta.
7. Escolha Create Route Table (Criar tabela de rotas).

2c: Associe a sub-rede Outpost e a tabela de rotas personalizada

Para destinar rotas de uma tabela a uma sub-rede específica, você deve associar a tabela de rotas à sub-rede. Uma tabela de rotas pode ser associada a várias sub-redes. No entanto, uma sub-rede só pode ser associada a uma tabela de rotas por vez. Por padrão, qualquer sub-rede não associada explicitamente a uma tabela está associada implicitamente à tabela de rotas principal.

Para associar a sub-rede Outpost e a tabela de rotas personalizada

1. Abra o console do Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Tabelas de rotas.
3. Na guia Subnet Associations (Associações da sub-rede) selecione Edit subnet associations (Editar associações da sub-rede).
4. Marque a caixa de seleção para a sub-rede associada à tabela de rotas.
5. SelecioneSave associations (Salvar associações).

Etapa 3: Configurar a conectividade do gateway local

O gateway local (LGW) permite a conectividade entre suas sub-redes Outpost e sua rede local. Para obter mais informações sobre o LGW, consulte Gateway local.

Para fornecer conectividade entre uma instância na sub-rede Outposts e sua rede local, você deve concluir as tarefas a seguir.

3a. Crie uma tabela de rotas de gateway local personalizada

Você pode criar uma tabela de rotas personalizada para seu gateway local (LGW) usando o AWS Outposts console.

Para criar uma tabela de rotas LGW personalizada usando o console

1. Abra o AWS Outposts console em https://console.aws.amazon.com/outposts/.
2. Para alterar o Região da AWS, use o seletor de região no canto superior direito da página.
3. No painel de navegação, selecione Tabela de rotas de gateway local.

4. Escolha Criar tabela de rotas de gateway local.
5. (Opcional) Em Nome, insira um nome para sua tabela de rotas LGW.
6. Para Gateway local, escolha seu gateway local.
7. Em Modo, escolha um modo de comunicação com sua rede on-premises.

   - Escolha Roteamento direto de VPC para usar o endereço IP privado de uma instância.
   - Escolha CoIP para usar o endereço IP de propriedade do cliente.
     - (Opcional) Adicione ou remova grupos de CoIP e blocos CIDR adicionais

       [Adicionar um grupo de CoIP] Escolha Adicionar novo grupo e faça o seguinte:

       - Em Nome, digite um nome para seu grupo de CoIP.
       - Para CIDR, insira um bloco CIDR de endereços IP de propriedade do cliente.
     - [Adicionar blocos CIDR] Escolha Adicionar novo CIDR e insira um intervalo de endereços IP de propriedade do cliente.
     - [Remover um grupo de CoIP ou um bloco CIDR adicional] Escolha Remover à direita de um bloco CIDR ou abaixo do grupo de CoIP.

       Você pode especificar até 10 grupos de CoIP e 100 blocos CIDR.
8. (Opcional) Adicione ou remova uma tag.

   [Adicionar uma tag] Escolha Adicionar nova tag e faça o seguinte:

   - Em Key (Chave), insira o nome da chave.
   - Em Value (Valor), insira o valor da chave.

   [Remover uma tag] Escolha Remover à direita da chave e do valor da tag.
9. Escolha Criar tabela de rotas de gateway local.

3b: Associe a VPC à tabela de rotas LGW personalizada

Você deve associar as VPCs à sua tabela de rotas LGW. Eles não são associados por padrão.

Use o procedimento a seguir para associar uma VPC a uma tabela de rotas LGW.

Você pode marcar o serviço de endpoint para ajudar a identificá-lo ou categorizá-lo de acordo com as necessidades da organização.

AWS Outposts console

Para associar uma VPC à tabela de rotas LGW personalizada

1. Abra o AWS Outposts console em https://console.aws.amazon.com/outposts/.
2. Para alterar o Região da AWS, use o seletor de região no canto superior direito da página.
3. No painel de navegação, selecione Tabelas de rotas de gateway local.
4. Selecione a tabela de rotas e, em seguida, escolha Ações, Associar VPC.
5. Para VPC ID, selecione a VPC a ser associada à tabela de rotas de gateway local.
6. (Opcional) Adicione ou remova uma tag.

   Para adicionar uma tag, escolha Adicionar nova tag e faça o seguinte:

   - Em Chave, insira o nome da chave.
   - Em Valor, insira o valor da chave.

   Para remover uma tag, escolha Remover à direita da chave e do valor da tag.
7. Escolha Associate VPC.

AWS CLI

Para associar uma VPC à tabela de rotas LGW personalizada

Use o table-vpc-association comando create-local-gateway-route-.

Exemplo

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

Saída

```
{
    "LocalGatewayRouteTableVpcAssociation": {
        "LocalGatewayRouteTableVpcAssociationId": "lgw-vpc-assoc-0ee765bcc8EXAMPLE",
        "LocalGatewayRouteTableId": "lgw-rtb-059615ef7dEXAMPLE",
        "LocalGatewayId": "lgw-09b493aa7cEXAMPLE",
```

```
        "VpcId": "vpc-07ef66ac71EXAMPLE",
        "State": "associated"
    }
}
```

3c: Adicione uma entrada de rota na tabela de rotas da sub-rede Outpost

Adicione uma entrada de rota na tabela de rotas de sub-rede do Outpost para ativar o tráfego entre as sub-redes do Outpost e o LGW.

As sub-redes Outpost em uma VPC, associadas às tabelas de rotas LGW do Outpost, podem ter um tipo de destino adicional de um ID de gateway local do Outpost para suas tabelas de rotas. Considere o caso em que você deseja rotear o tráfego com um endereço de destino 172.16.100.0/24 para a rede do cliente por meio do LGW. Para fazer isso, edite a tabela de rotas de sub-rede Outpost e adicione a seguinte rota com a rede de destino e um destino do LGW (). `lgw-xxxx`

Destination (Destino)	Destino
172.16.100.0/24	`lgw-id`

Para adicionar uma entrada de rota com **`lgw-id`** como destino na tabela de rotas da sub-rede Outpost:

1. Abra o console do Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Tabelas de rotas e selecione a tabela de rotas que você criou. 2b: Crie uma tabela de rotas personalizada
3. Escolha Ações e, em seguida, Editar rotas.
4. Para adicionar uma rota, escolha Add route (Adicionar rota).
5. Em Destino, insira o bloco CIDR de destino na rede do cliente.
6. Para Target, escolha Outpost local Gateway ID.
7. Escolha Salvar alterações.

3d: Associe a tabela de rotas LGW personalizada aos grupos LGW VIF

Os grupos VIF são agrupamentos lógicos de interfaces virtuais (VIFs). Associe a tabela de rotas do gateway local ao grupo VIF.

Para associar a tabela de rotas LGW personalizada aos grupos LGW VIF

1. Abra o AWS Outposts console em https://console.aws.amazon.com/outposts/.
2. Para alterar o Região da AWS, use o seletor de região no canto superior direito da página.
3. No painel de navegação, selecione Tabelas de rotas de gateway local.
4. Escolha a tabela de rotas.
5. Escolha a guia Associação de grupo VIF no painel de detalhes e, em seguida, escolha Editar associação de grupo VIF.
6. Para configurações do grupo VIF, selecione Associar grupo VIF e escolha um grupo VIF.
7. Escolha Salvar alterações.

3e: Adicione uma entrada de rota na tabela de rotas LGW

Edite a tabela de rotas do gateway local para adicionar uma rota estática que tenha o Grupo VIF como destino e o intervalo CIDR da sub-rede local (ou 0.0.0.0/0) como destino.

Destination (Destino)	Destino
172.16.100.0/24	`VIF-Group-ID`

Para adicionar uma entrada de rota na tabela de rotas LGW

1. Abra o AWS Outposts console em https://console.aws.amazon.com/outposts/.
2. No painel de navegação, selecione Tabela de rotas de gateway local.
3. Selecione a tabela de rotas do gateway local e, em seguida, escolha Ações, Editar rotas.
4. Escolha Adicionar rota.
5. Em Destino insira o bloco CIDR de destino, um único endereço IP ou o ID de uma lista de prefixos.
6. Em Destino, selecione o ID do gateway local.
7. Escolha Save routes (Salvar rotas).

3f: (Opcional) Atribua um endereço IP de propriedade do cliente à instância

Se você configurou seus Outposts no 3a. Crie uma tabela de rotas de gateway local personalizada para usar um pool de endereços IP (CoIP) de propriedade do cliente, você deve alocar um endereço IP elástico do pool de endereços CoIP e associar o endereço IP elástico à instância. Para obter mais informações sobre o PITR, consulte Endereços IP de propriedade do cliente.

Se você configurou seus Outposts para usar o roteamento direto de VPC (DVR), pule esta etapa.

Amazon VPC console

Para atribuir um endereço CoIP à instância

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Elastic IPs.
3. Escolha Alocar endereço IP elástico.
4. Em Grupo de borda de rede, selecione o local do qual o endereço IP é anunciado.
5. Para Pool de endereços IPv4 públicos, escolha Pool de endereços IPv4 de propriedade do cliente.
6. Para o conjunto de endereços IPv4 pertencente ao cliente, selecione o pool que você configurou.
7. Escolha Allocate.
8. Selecione o endereço IP elástico e escolha Ações, Associar endereço IP elástico.
9. Selecione a instância em Instância e depois Associar.

AWS CLI

Para atribuir um endereço CoIP à instância

1. Use o describe-coip-poolscomando para recuperar informações sobre seus grupos de endereços de propriedade do cliente.

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

A seguir, um exemplo de saída.

```
{
```

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

2. Use o comando allocate-address para alocar um endereço IP elástico. Use a ID do pool retornada na etapa anterior.

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

A seguir, um exemplo de saída.

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

3. Use o comando associate-address para associar o endereço IP elástico à instância do Outpost. Use o ID de alocação retornado da etapa anterior.

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

A seguir, um exemplo de saída.

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

Conjuntos de endereços IP de propriedade do cliente

Se você quiser usar um pool compartilhado de endereços IP de propriedade do cliente, o pool deverá ser compartilhado antes de você iniciar a configuração. Para obter informações sobre como compartilhar um endereço IPv4 de propriedade do cliente, consulte Compartilhando seus AWS recursos no Guia do usuário.AWS RAM

Etapa 4: Configurar a rede local

O Outpost estabelece um emparelhamento BGP externo de cada Dispositivo de Rede Outpost (OND) para um Dispositivo de Rede Local do Cliente (CND) para enviar e receber tráfego da sua rede local para os Outposts. Para obter mais informações, consulte Conectividade BGP do gateway local.

Para enviar e receber tráfego da sua rede local para o Outpost, certifique-se de que:

- Nos dispositivos de rede do cliente, a sessão do BGP na VLAN do gateway local está em um estado ATIVO em relação aos seus dispositivos de rede.
- Para o tráfego que vai do local para os Outposts, verifique se você está recebendo em seu CND os anúncios BGP dos Outposts. Esses anúncios do BGP contêm as rotas que sua rede local deve usar para rotear o tráfego do local para o Outpost. Portanto, garanta que sua rede tenha o roteamento correto entre Outposts e os recursos locais.
- Para o tráfego que vai dos Outposts para a rede local, certifique-se de que seus CNDs estejam enviando os anúncios da rota BGP das sub-redes da rede local para os Outposts (ou 0.0.0.0/0). Como alternativa, você pode anunciar uma rota padrão (por exemplo, 0.0.0.0/0) para Outposts. As sub-redes locais anunciadas pelas CNDs devem ter um intervalo CIDR igual ou incluído no intervalo CIDR em que você configurou. 3e: Adicione uma entrada de rota na tabela de rotas LGW

Exemplo: anúncios BGP no modo Direct VPC

Considere o cenário em que você tem um Outpost, configurado no modo Direct VPC, com dois dispositivos de rede em rack Outposts conectados por uma VLAN de gateway local a dois dispositivos de rede local do cliente. O seguinte foi configurado:

- Uma VPC com um bloco CIDR 10.0.0.0/16.
- Uma sub-rede Outpost na VPC com um bloco CIDR 10.0.3.0/24.
- Uma sub-rede na rede local com um bloco CIDR 172.16.100.0/24
- O Outposts usa o endereço IP privado das instâncias na sub-rede Outpost, por exemplo, 10.0.3.0/24, para se comunicar com sua rede local.

Nesse cenário, a rota anunciada por:

- O gateway local para os dispositivos do seu cliente é 10.0.3.0/24.
- Os dispositivos do seu cliente para o gateway local do Outpost são 172.16.100.0/24.

Como resultado, o gateway local enviará tráfego de saída com a rede de destino 172.16.100.0/24 para os dispositivos do cliente. Certifique-se de que sua rede tenha a configuração de roteamento correta para fornecer tráfego ao host de destino em sua rede.

Para obter os comandos e a configuração específicos necessários para verificar o estado das sessões do BGP e as rotas anunciadas nessas sessões, consulte a documentação do seu fornecedor de rede. Para solucionar problemas, consulte a lista de verificação de solução de problemas de rede em AWS Outposts rack.

Exemplo: anúncios BGP no modo CoIP

Considere o cenário em que você tem um Outpost com dois dispositivos de rede em rack Outposts conectados por uma VLAN de gateway local a dois dispositivos de rede local do cliente. O seguinte foi configurado:

- Uma VPC com um bloco CIDR 10.0.0.0/16.
- Uma sub-rede na VPC com um bloco CIDR 10.0.3.0/24.
- Um grupo de IPs de propriedade do cliente (10.1.0.0/26).
- Uma associação de endereço IP elástico que associa 10.0.3.112 a 10.1.0.2.
- Uma sub-rede na rede local com um bloco CIDR 172.16.100.0/24
- A comunicação entre seu Outpost e a rede on-premises usará os IPs elásticos CoIP para endereçar instâncias no Outpost. O intervalo CIDR da VPC não será usado.

Nesse cenário, a rota anunciada por:

- O gateway local para os dispositivos do seu cliente é 10.1.0.0/26.
- Os dispositivos do seu cliente para o gateway local do Outpost são 172.16.100.0/24.

Como resultado, o gateway local enviará tráfego de saída com a rede de destino 172.16.100.0/24 para os dispositivos do cliente. Certifique-se de que sua rede tenha a configuração de roteamento correta para fornecer tráfego ao host de destino em sua rede.

Para obter os comandos e a configuração específicos necessários para verificar o estado das sessões do BGP e as rotas anunciadas nessas sessões, consulte a documentação do seu fornecedor de rede. Para solucionar problemas, consulte a lista de verificação de solução de problemas de rede em AWS Outposts rack.

Etapa 5: iniciar uma instância no Outpost

Você pode iniciar instâncias do EC2 na sub-rede Outpost que você criou ou em uma sub-rede Outpost que foi compartilhada com você. Os grupos de segurança controlam o tráfego de entrada e de saída de instâncias em uma sub-rede do Outpost, como fazem para instâncias em uma sub-rede de zona de disponibilidade. Para se conectar a uma instância do EC2 em uma sub-rede do Outpost, é possível especificar um par de chaves ao executar a instância, como o faz para instâncias em uma sub-rede de zona de disponibilidade.

Considerações

- Você pode criar grupos de posicionamento para influenciar como o Amazon EC2 deve tentar colocar grupos de instâncias interdependentes no hardware do Outposts. Você pode escolher a estratégia do grupo de colocação que atenda às necessidades de sua carga de trabalho.
- Se o seu Outpost tiver sido configurado para usar um pool de endereços IP de propriedade do cliente (CoIP), você deverá atribuir um endereço IP de propriedade do cliente a todas as instâncias que você iniciar.

Você pode iniciar instâncias na sub-rede do Outpost

1. Abra o AWS Outposts console em https://console.aws.amazon.com/outposts/.
2. No painel de navegação, escolha Outposts.
3. Selecione o Outpost, em seguida, escolha Ações, Visualizar detalhes.
4. Na página de Resumo do Outpost, escolha Executar instância. Você será redirecionado para o assistente de execução de instâncias no console do Amazon EC2. Selecionamos a sub-rede do Outpost para você e mostramos somente os tipos de instância compatíveis com seu rack do Outposts.
5. Escolha um tipo de instância compatível com seu rack Outposts. Observe que as instâncias que aparecem em cinza não estão disponíveis para seu Posto Avançado.
6. (Opcional) Para iniciar as instâncias em um grupo com posicionamento, expanda Detalhes avançados e vá até grupo com posicionamento. É possível selecionar um grupo com posicionamento existente ou criar um novo.

7. Conclua o assistente para executar a instância na sub-rede do Outpost. Para obter mais informações, consulte o seguinte no Guia do usuário do Amazon EC2:

   - Linux — Execute uma instância usando o novo assistente de inicialização de instância
   - Windows — Execute uma instância usando o novo assistente de inicialização de instância

> **Note**
>
> Se você estiver criando um volume Amazon EBS, deverá usar o tipo de volume gp2 ou o assistente falhará.

Etapa 6: testar a conectividade

Você pode testar a conectividade usando os casos de uso apropriados.

Testar a conectividade da sua rede local com o Outpost

Em um computador na sua rede local, execute o `ping` comando no endereço IP privado da instância Outpost.

```
ping 10.0.3.128
```

A seguir, um exemplo de saída.

```
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
```

Teste a conectividade de uma instância do Outpost com sua rede local

Dependendo do seu sistema operacional, use ssh ou rdp para se conectar ao endereço IP privado da sua instância do Outpost. Para obter informações sobre como se conectar a uma instância do Linux, consulte Conectar-se à sua instância do Linux no Guia do usuário do Amazon EC2 para instâncias do Linux. Para obter informações sobre como se conectar a uma instância do Windows, consulte Conectar-se à instância do Windows no Guia do usuário do Amazon EC2 para instâncias do Windows.

Depois que a instância estiver em execução, execute o comando `ping` em um endereço IP de um computador na sua rede local. No exemplo a seguir, o endereço IP é 172.16.0.130.

```
ping 172.16.0.130
```

A seguir, um exemplo de saída.

```
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
```

Teste a conectividade entre a AWS região e o Posto Avançado

Execute uma instância na sub-rede na AWS região. Por exemplo, execute o comando 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
```

Depois que a instância estiver em execução, execute as seguintes operações:

1. Obtenha o endereço IP privado da instância na AWS região. Essas informações estão disponíveis no console do Amazon EC2 na página de detalhes da instância.

2. Dependendo do seu sistema operacional, use ssh ou se conecte rdp ao endereço IP privado da sua instância do Outpost.
3. Execute o ping comando na sua instância do Outpost, especificando o endereço IP da instância na AWS região.

```
ping 10.0.1.5
```

A seguir, um exemplo de saída.

```
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
```

Exemplos de conectividade de endereço IP de propriedade do cliente

Teste a conectividade da sua rede local com o Outpost

Em um computador na sua rede local, execute o `ping` comando no endereço IP de propriedade do cliente da instância Outpost.

```
ping 172.16.0.128
```

A seguir, um exemplo de saída.

```
Pinging 172.16.0.128

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

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

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

Teste a conectividade de uma instância do Outpost com sua rede local

Dependendo do seu sistema operacional, use ssh ou rdp para se conectar ao endereço IP privado da sua instância do Outpost. Para obter informações sobre como se conectar a uma instância do Linux, consulte Conectar-se à sua instância do Linux no Guia do usuário do Amazon EC2 para instâncias do Linux. Para obter informações sobre como se conectar a uma instância do Windows, consulte Conectar-se à instância do Windows no Guia do usuário do Amazon EC2 para instâncias do Windows.

Depois que a instância do Outpost estiver em execução, execute o `ping` comando em um endereço IP de um computador na sua rede local.

```
ping 172.16.0.130
```

A seguir, um exemplo de saída.

```
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
```

Teste a conectividade entre a AWS região e o Posto Avançado

Execute uma instância na sub-rede na AWS região. Por exemplo, execute o comando 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
```

Depois que a instância estiver em execução, execute as seguintes operações:

1. Obtenha o endereço IP privado AWS da instância da região, por exemplo, 10.0.0.5. Essas informações estão disponíveis no console do Amazon EC2 na página de detalhes da instância.
2. Dependendo do seu sistema operacional, use ssh ou rdp para se conectar ao endereço IP privado da sua instância do Outpost.
3. Execute o `ping` comando da sua instância Outpost para o endereço IP AWS da instância da Região.

   ```
   ping 10.0.0.5
   ```

   A seguir, um exemplo de saída.

   ```
   Pinging 10.0.0.5

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

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

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

Conectividade do AWS Outposts com regiões AWS

O AWS Outposts suporta conectividade de rede de longa distância (WAN) por meio da conexão de link de serviço.

Conteúdo

Conectividade por meio de links de serviço

O link de serviço é uma conexão necessária entre seus Postos Avançados e a AWS Região escolhida (ou Região de origem) e permite o gerenciamento dos Postos Avançados e a troca de tráfego de e para a Região. AWS O link de serviço utiliza um conjunto criptografado de conexões VPN para se comunicar com a região de origem.

Para configurar a conectividade do link de serviço, você ou AWS deve configurar a conectividade física, da LAN virtual (VLAN) e da camada de rede do link de serviço com seus dispositivos de rede local durante o provisionamento do Outpost. Para obter mais informações, consulte Conectividade de rede local para racks e Requisitos de site para rack Outposts.

Para a conectividade de rede de área ampla (WAN) com a AWS região, AWS Outposts pode estabelecer conexões VPN de link de serviço por meio da conectividade pública da AWS região. Isso exige que os Outposts tenham acesso aos intervalos de IP públicos da região, que podem ser por meio da Internet pública ou de interfaces virtuais AWS Direct Connect públicas. Para os intervalos de endereços IP atuais, consulte Intervalos de endereços IP da AWS no guia do usuário da Amazon VPC. Essa conectividade pode ser habilitada configurando rotas específicas ou padrão (0.0.0.0/0) no caminho da camada de rede do link de serviço. Para obter mais informações, consulte Conectividade BGP do link de serviço e anúncio de sub-rede da infraestrutura de link de serviço e intervalo de IP.

Como alternativa, você pode selecionar a opção de conectividade privada para seu Outpost. Para obter mais informações, consulte Conectividade privada do link de serviço usando VPC.

Depois que a conexão do link de serviço é estabelecida, seu Outpost se torna operacional e é gerenciado porAWS. O link de serviço é usado para o seguinte tráfego:

- Tráfego de VPC do cliente entre o Outpost e quaisquer VPCs associadas.
- Os Outposts gerenciam o tráfego, como gerenciamento de recursos, monitoramento de recursos e atualizações de firmware e software.

Requisitos da unidade de transmissão máxima (MTU) do link de serviço

A unidade de transmissão máxima (MTU) de uma conexão de rede é o tamanho, em bytes, do maior pacote permissível que pode ser passado pela conexão. A rede deve suportar MTU de 1500 bytes entre o Outpost e os endpoints do link de serviço na região principal. AWS Para obter informações sobre a MTU necessária entre uma instância no Outpost e uma instância na AWS região por meio do link de serviço, consulte Unidade máxima de transmissão de rede (MTU) para sua instância do Amazon EC2 no Guia do usuário do Amazon EC2 para instâncias Linux.

Recomendações de largura de banda do link de serviço

Para uma experiência e resiliência ideais, AWS recomenda que você use conectividade redundante de pelo menos 500 Mbps (1 Gbps é melhor) para a conexão do link de serviço com a região AWS. Você pode usar o AWS Direct Connect ou uma conexão com a Internet para o link de serviço. A conexão mínima de link de serviço de 500 Mbps permite que você inicie instâncias do Amazon EC2, anexe volumes do Amazon EBS e AWS acesse serviços, como Amazon EKS, Amazon EMR e métricas. CloudWatch

Os requisitos de largura de banda do link de serviço do Outposts variam de acordo com as seguintes características:

- Número de racks do AWS Outposts e configurações de capacidade
- As características da workload, como tamanho da AMI, elasticidade do aplicativo, necessidades de velocidade de pico e tráfego da Amazon VPC para a região

Para receber uma recomendação personalizada sobre a largura de banda do link de serviço exigida para suas necessidades, entre em contato com seu representante de vendas da AWS ou com seu parceiro do APN.

Firewalls e o link de serviço

Esta seção discute as configurações de firewall e a conexão do link de serviço.

No diagrama a seguir, a configuração estende a Amazon VPC da região AWS até o Outpost. Uma interface virtual pública do AWS Direct Connect é a conexão do link de serviço. O tráfego a seguir passa pelo link de serviço e pela conexão do AWS Direct Connect:

- Tráfego de gerenciamento para o Outpost por meio do link de serviço
- Tráfego entre o Outpost e quaisquer VPCs associadas

Se você estiver usando um firewall com estado com sua conexão com a Internet para limitar a conectividade da Internet pública à VLAN do link de serviço, poderá bloquear todas as conexões de entrada iniciadas pela Internet. Isso ocorre porque a VPN do link de serviço é iniciada somente do Outpost para a região, e não da região para o Outpost.

Se você usar um firewall para limitar a conectividade da VLAN do link de serviço, poderá bloquear todas as conexões de entrada. Você deve permitir conexões de saída da região AWS de volta ao Outpost, conforme a tabela a seguir. Se o firewall estiver com estado, as conexões de saída do Outpost que são permitidas, o que significa que foram iniciadas a partir do Outpost, devem ser permitidas de volta na entrada.

Protocolo	Porta de origem	Endereço de origem	Porta de destino	Endereço de destino
UDP	443	Link de serviço /26 do AWS Outposts	443	Rotas públicas da região do AWS Outposts
TCP	1025-65535	Link de serviço /26 do AWS Outposts	443	Rotas públicas da região do AWS Outposts

Note

As instâncias em um Outpost não podem usar o link de serviço para se comunicar com instâncias em outros Outposts. Aproveite o roteamento por meio do gateway local ou da interface de rede local para se comunicar entre Outposts.

Os racks do AWS Outposts também são projetados com potência redundante e equipamentos de rede, incluindo componentes de gateway local. Para ter mais informações, consulte Resiliência no AWS Outposts.

Conectividade privada do link de serviço usando VPC

Você pode selecionar a opção de conectividade privada ao criar seu Outpost. Ao fazer isso, uma conexão VPN de link de serviço é estabelecida após a instalação do Outpost usando uma VPC e uma sub-rede especificadas por você. Isso permite conectividade privada por meio da VPC e minimiza a exposição pública à Internet.

Pré-requisitos

Os seguintes pré-requisitos são necessários antes que você possa configurar a conectividade privada para seu Outpost:

- Configure as permissões para que uma entidade do IAM (usuário ou função) permita que o usuário ou a função crie ou edite a função vinculada ao serviço para conectividade privada. A entidade do IAM precisa de permissão para acessar as seguintes ações:
  - `iam:CreateServiceLinkedRole` no `arn:aws:iam::*:role/aws-service-role/outposts.amazonaws.com/AWSServiceRoleForOutposts*`
  - `iam:PutRolePolicy` no `arn:aws:iam::*:role/aws-service-role/outposts.amazonaws.com/AWSServiceRoleForOutposts*`
  - `ec2:DescribeVpcs`
  - `ec2:DescribeSubnets`

  Para obter mais informações, consulte Usar perfis vinculados a serviço do AWS Outposts e Gerenciamento de identidade e acesso (IAM) para AWS Outposts.
- Na mesma conta da AWS e na mesma zona de disponibilidade do seu Outpost, crie uma VPC com o único objetivo de estabelecer conectividade privada do Outpost com uma sub-rede /25 ou maior que não entre em conflito com 10.1.0.0/16. Por exemplo, você pode usar 10.2.0.0/16.
- Crie uma conexão do AWS Direct Connect, uma interface virtual privada e um gateway privado virtual para permitir que seu Outpost local acesse a VPC. Se a conexão do AWS Direct Connect estiver em uma conta da AWS diferente da sua VPC, consulte Associação de um gateway privado virtual entre contas no Guia do usuário do AWS Direct Connect.

- Anuncie o CIDR da sub-rede na rede on-premises. Você pode usar o AWS Direct Connect para fazer isso. Para obter mais informações, consulte interfaces virtuais do AWS Direct Connect e Trabalho com gateways do AWS Direct Connect no Guia do usuário do AWS Direct Connect.

Você pode selecionar a opção de conectividade privada ao criar seu Outpost no console do AWS Outposts. Para obter instruções, consulte Crie um Outpost e solicite capacidade para o Outpost.

> **Note**
>
> Para selecionar a opção de conectividade privada quando seu Outpost estiver no status PENDENTE, escolha Outposts no console e selecione seu Outpost. Escolha Ações, Adicionar conectividade privada e siga as etapas.

Depois de selecionar a opção de conectividade privada para seu Outpost, o AWS Outposts cria automaticamente uma função vinculada ao serviço na sua conta que permite concluir as seguintes tarefas em seu nome:

- Cria interfaces de rede na sub-rede e na VPC que você especifica, além de criar um grupo de segurança para as interfaces de rede.
- Concede permissão ao serviço do AWS Outposts para conectar as interfaces de rede a uma instância de endpoint do link de serviço na conta.
- Anexa as interfaces de rede às instâncias do endpoint do link de serviço a partir da conta.

Para obter mais informações sobre a função vinculada ao serviço, consulte Usar perfis vinculados a serviço do AWS Outposts.

> **Important**
>
> Depois que seu Outpost for instalado, confirme a conectividade com os IPs privados em sua sub-rede.

Conexões redundantes à Internet

Ao criar conectividade a partir do seu Outpost para a AWS Region, recomendamos que você crie várias conexões para maiores disponibilidade e resiliência. Para obter mais informações, consulte Recomendações de resiliência do AWS Direct Connect.

Se você precisar de conectividade com a Internet pública, poderá usar conexões de Internet redundantes e diversos provedores de Internet, assim como faria com suas workloads on-premises existentes.

Outposts e sites

Gerencie Outposts e sites para. AWS Outposts

Você pode marcar os Outposts e sites para ajudar a identificá-los ou categorizá-los de acordo com as necessidades da organização. Para obter mais informações sobre marcação, consulte AWS Recursos de marcação no Referência geral da AWS Guia.

Tópicos

- Gerenciar Outposts
- Gerenciar sites do Outpost

Gerenciar Outposts

AWS Outposts inclui hardware e recursos virtuais conhecidos como Outposts. Use esta seção para criar e gerenciar Outposts, incluindo alterar o nome e adicionar ou visualizar detalhes ou tags.

Para criar um Outpost

1. Abra o AWS Outposts console em https://console.aws.amazon.com/outposts/.
2. Para alterar o Região da AWS, use o seletor de região no canto superior direito da página.
3. No painel de navegação, escolha Outposts.
4. Escolha Criar Outpost.
5. Escolha um tipo de hardware para este Outpost.
6. Insira um nome e uma descrição para seu Outpost.
7. Escolha uma zona de disponibilidade para seu Outpost.
8. (Opcional) Escolha a Opção de conectividade privada. Para VPC e sub-rede, selecione uma VPC e uma sub-rede na mesma AWS conta e zona de disponibilidade do seu Outpost.

   > **Note**
   >
   > Se precisar desfazer a conectividade privada do seu Outpost, entre em contato com o Enterprise Support da AWS .

9. No ID do site, siga um destes procedimentos:

- Para selecionar um site existente, escolha o site.
- Para criar um novo site, escolha Criar site, clique em Avançar e insira as informações sobre seu site na nova janela.

  Depois de criar o site, retorne a essa janela para selecionar o site. Talvez seja necessário atualizar a lista de sites para ver o novo site. Para atualizar seus dados, escolha o ícone de atualização ().

  Para ter mais informações, consulte the section called “Sites”.

10. Escolha Criar Outpost.

> **Tip**
>
> Para adicionar capacidade ao seu novo Outpost, você deve fazer um pedido.

Use as etapas a seguir para editar o nome e a descrição de um Outpost.

Para editar o nome e a descrição do Outpost

1. Abra o AWS Outposts console em https://console.aws.amazon.com/outposts/.
2. Para alterar o Região da AWS, use o seletor de região no canto superior direito da página.
3. No painel de navegação, escolha Outposts.
4. Selecione o Outpost e escolha Ações, Editar Outpost.
5. Modifique o nome e a descrição.

   Em Nome, insira o nome.

   Em Descrição, insira a descrição.
6. Escolha Salvar alterações.

Siga as etapas abaixo para exibir os detalhes de um Outpost.

Como exibir os detalhes do Outpost

1. Abra o AWS Outposts console em https://console.aws.amazon.com/outposts/.
2. Para alterar o Região da AWS, use o seletor de região no canto superior direito da página.
3. No painel de navegação, escolha Outposts.
4. Selecione o Outpost, em seguida, escolha Ações, Visualizar detalhes.

Você também pode usar o AWS CLI para ver os detalhes do Outpost.

Para ver os detalhes do Outpost com o AWS CLI

- Use o comando get-outpost AWS CLI .

Realize as etapas a seguir para gerenciar as tags em um Outpost.

Para gerenciar as tags Outpost

1. Abra o AWS Outposts console em https://console.aws.amazon.com/outposts/.
2. Para alterar o Região da AWS, use o seletor de região no canto superior direito da página.
3. No painel de navegação, escolha Outposts.
4. Selecione o Outpost e escolha Ações, Gerenciar tags.
5. Adicione ou remova uma tag.

   Para adicionar uma tag, escolha Adicionar nova tag e faça o seguinte:

   - Em Chave, insira o nome da chave.
   - Em Valor, insira o valor da chave.

   Para remover uma tag, escolha Remover à direita da chave e do valor da tag.
6. Escolha Salvar alterações.

Gerenciar sites do Outpost

Os edifícios físicos gerenciados pelo cliente onde AWS instalará seu Posto Avançado. Um local deve atender aos requisitos de instalação, rede e energia do seu Outpost. Para ter mais informações, consulte Requisitos.

Para criar um site do Outpost

1. Abra o AWS Outposts console em https://console.aws.amazon.com/outposts/.
2. Para alterar o Região da AWS, use o seletor de região no canto superior direito da página.
3. No painel de navegação, selecione Sites.
4. Escolha Criar local.
5. Escolha um tipo de hardware compatível para o site.
6. Insira um nome, descrição e endereço operacional para seu site. Se você optar por oferecer suporte a racks no local, insira as seguintes informações:
   - Peso máximo: especifique o peso máximo do rack que este site pode suportar.
   - Consumo de energia: especifique em kVA o consumo de energia disponível na posição de posicionamento do hardware do rack.
   - Opção de alimentação: especifique a opção de alimentação que você pode fornecer para o hardware.
   - Conector de alimentação — especifique o conector de alimentação que AWS deve ser planejado para fornecer conexões ao hardware.
   - Queda de alimentação: especifique se a alimentação vem acima ou abaixo do rack.
   - Velocidade do uplink: especifique a velocidade do uplink que o rack deve suportar para a conexão com a região.
   - Número de uplinks: especifique o número de uplinks para cada dispositivo de rede do Outpost que você pretende usar para conectar o rack à sua rede.
   - Tipo de fibra: especifique o tipo de fibra que você usará para conectar o Outpost à sua rede.
   - Padrão óptico: especifique o tipo de padrão óptico que você usará para conectar o Outpost à sua rede.
   - Notas: especifique notas sobre um site.
7. Leia os requisitos da instalação e selecione Eu li os requisitos da instalação.
8. Escolha Criar local.

Use as etapas a seguir para editar um site do Outpost.

Para editar um site

1. Abra o AWS Outposts console em https://console.aws.amazon.com/outposts/.

2. Para alterar o Região da AWS, use o seletor de região no canto superior direito da página.
3. No painel de navegação, selecione Sites.
4. Selecione o site e, em seguida, selecione Ações, Editar site.
5. É possível modificar o nome, a descrição, o endereço operacional e os detalhes do site.

   Se você alterar o endereço operacional, saiba que as alterações não se propagarão para os pedidos existentes.
6. Escolha Salvar alterações.

Siga os passos a seguir para visualizar os detalhes de um site do Outpost.

Como visualizar os detalhes do site

1. Abra o AWS Outposts console em https://console.aws.amazon.com/outposts/.
2. Para alterar o Região da AWS, use o seletor de região no canto superior direito da página.
3. No painel de navegação, selecione Sites.
4. Selecione o site, e escolha Ações, Visualizar detalhes.

Realize as etapas a seguir para gerenciar as tags em um site do Outpost.

Para gerenciar as tags do site

1. Abra o AWS Outposts console em https://console.aws.amazon.com/outposts/.
2. Para alterar o Região da AWS, use o seletor de região no canto superior direito da página.
3. No painel de navegação, selecione Sites.
4. Selecione o site e escolha Ações, Gerenciar tags.
5. Adicione ou remova uma tag.

   Para adicionar uma tag, escolha Adicionar nova tag e faça o seguinte:

   - Em Chave, insira o nome da chave.
   - Em Valor, insira o valor da chave.

   Para remover uma tag, escolha Remover à direita da chave e do valor da tag.
6. Escolha Salvar alterações.

Gateway local

O gateway local é um componente central da arquitetura Outposts. O gateway local permite a conectividade entre suas sub-redes Outpost e sua rede on-premises própria. Se a infraestrutura on-premise fornecer acesso à Internet, as workloads executadas no Outposts também poderão aproveitar o gateway local para se comunicar com serviços regionais ou workloads regionais. Essa conectividade pode ser obtida usando uma conexão pública (internet) ou usando o Direct Connect. Para ter mais informações, consulte Conectividade do AWS Outposts com regiões AWS.

Conteúdo

Noções básicas de gateway local

Cada Outpost suporta um único gateway local. Um gateway local tem os seguintes componentes:

- Tabelas de rotas: você usa para criar tabelas de rotas de gateway local. Para ter mais informações, consulte the section called “Tabelas de rotas do gateway local”.
- Grupos de CoIP: (opcional) você pode usar intervalos de endereços IP de sua propriedade para facilitar a comunicação entre a rede on-premises e as instâncias em sua VPC. Para ter mais informações, consulte the section called “Endereços IP de propriedade do cliente”.
- Interfaces virtuais (VIFs) — AWS cria uma VIF para cada LAG e adiciona as duas VIFs a um grupo de VIFs. A tabela de rotas de gateway local deve ter uma rota padrão para as duas VIFs para conectividade de rede local. Para ter mais informações, consulte Conectividade de rede local.
- Associações de grupos VIF — AWS adiciona os VIFs criados a um grupo VIF. Os grupos VIF são agrupamentos lógicos de VIFs. Para ter mais informações, consulte the section called “associações de grupos VIF”.
- Associações de VPC: você usa para criar associações de VPC com suas VPCs e a tabela de rotas de gateway local. As tabelas de rotas da VPC associadas às sub-redes que residem em um Outpost podem usar o gateway local como destino da rota. Para ter mais informações, consulte the section called “associações de VPC”.

Ao AWS provisionar seu rack Outpost, criamos alguns componentes e você é responsável por criar outros.

AWS responsabilidades

- Fornece o hardware.
- Cria o gateway local.
- Cria as interfaces virtuais (VIFs) e um grupo VIF.

Suas responsabilidades

- Criar a tabela de rotas de gateway local.
- Associar um gateway com uma tabela de rotas.
- Associar um grupo VIF à tabela de rotas de gateway local.

Roteamento

As instâncias em sua sub-rede Outpost podem usar uma das seguintes opções para comunicação com sua rede on-premises por meio do gateway local:

- Endereços IP privados: o gateway local usa os endereços IP privados das instâncias em sua sub-rede Outpost para facilitar a comunicação com sua rede on-premises. Esse é o padrão.
- Endereços IP de propriedade do cliente: o gateway local realiza a conversão de endereços de rede (NAT) para os endereços IP de propriedade do cliente que você atribui às instâncias na sub-rede Outpost. Essa opção suporta intervalos CIDR sobrepostos e outras topologias de rede.

Para ter mais informações, consulte the section called “Tabelas de rotas do gateway local”.

Conectividade por meio do gateway local

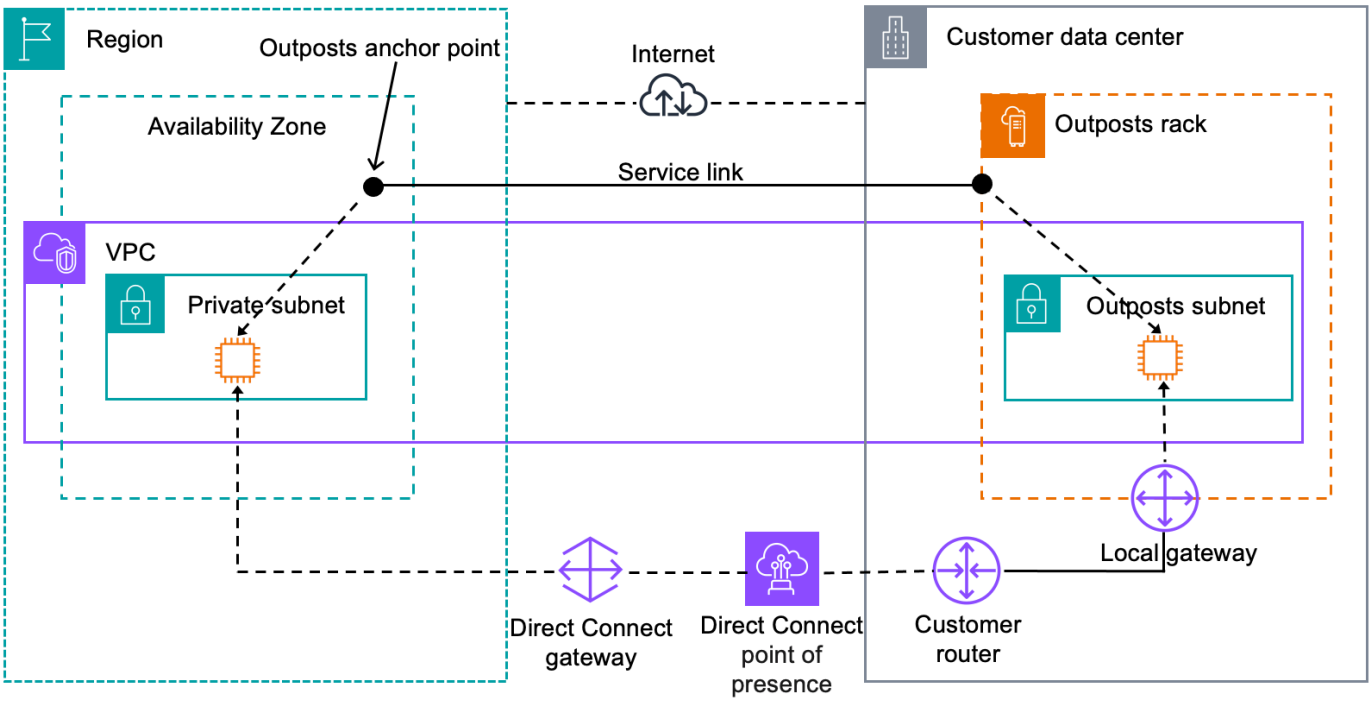
A função principal de um gateway local é fornecer conectividade de um Outpost à sua rede on-premises local. Ele também fornece conectividade com a Internet por meio de sua rede on-premises própria. Veja exemplos em the section called “Roteamento Direct VPC” e the section called “Endereços IP de propriedade do cliente”.

O gateway local também pode fornecer um caminho de plano de dados de volta para a AWS região. O caminho do plano de dados para o gateway local vai do Outpost, passando pelo gateway local e

até o segmento de LAN do gateway local privado. Depois, seguiria um caminho privado de volta aos endpoints de serviço AWS na região. Observe que o caminho do ambiente de gerenciamento sempre usa a conectividade do link de serviço, independentemente do caminho do plano de dados usado.

Você pode conectar sua infraestrutura local de Outposts Serviços da AWS à região de forma privada. AWS Direct Connect Para obter mais informações sobre conteúdo privado, consulte conectividade privada AWS Outposts.

A imagem a seguir mostra a conectividade por meio do gateway local:



Tabelas de rotas do gateway local

As tabelas de rotas de sub-rede do Outpost em um rack podem incluir uma rota para sua rede on-premises própria. O gateway local roteia esse tráfego para roteamento de baixa latência para a rede on-premises.

Por padrão, o Outposts usa o endereço IP privado das instâncias no Outpost para se comunicar com sua rede on-premises. Isso é conhecido como roteamento Direct VPC para AWS Outposts (ou roteamento Direct VPC). No entanto, você pode fornecer um intervalo de endereços, conhecido como grupo de endereços IP pertencente ao cliente (CoIP), e fazer com que as instâncias da sua rede usem esses endereços para se comunicar com sua rede on-premises. O roteamento Direct

VPC e o CoIP são opções mutuamente exclusivas e o roteamento funciona de forma diferente com base na sua escolha.

Conteúdo

Roteamento Direct VPC

O roteamento Direct VPC usa o endereço IP privado das instâncias em sua VPC para facilitar a comunicação com sua rede on-premises. Esses endereços são anunciados em sua rede on-premises com BGP. O anúncio para o BGP é apenas para os endereços IP privados que pertencem às sub-redes em seu rack Outpost. Esse tipo de roteamento é o modo padrão para Outposts. Nesse modo, o gateway local não executa NAT para instâncias e você não precisa atribuir endereços IP elásticos às suas instâncias do EC2. Você tem a opção de usar seu próprio espaço de endereço em vez do modo de roteamento Direct VPC. Para ter mais informações, consulte Endereços IP de propriedade do cliente.

O roteamento Direct VPC é compatível somente com interfaces de rede da instância. Com interfaces de rede AWS criadas em seu nome (conhecidas como interfaces de rede gerenciadas pelo solicitante), seus endereços IP privados não podem ser acessados pela sua rede local. Por exemplo, endpoints VPC não são acessíveis diretamente de sua rede on-premises.

Os exemplos a seguir ilustram o roteamento Direct VPC.

Exemplos

Exemplo: conectividade com a Internet por meio da VPC

As instâncias em uma sub-rede Outpost podem acessar a Internet por meio do gateway da Internet conectado à VPC.

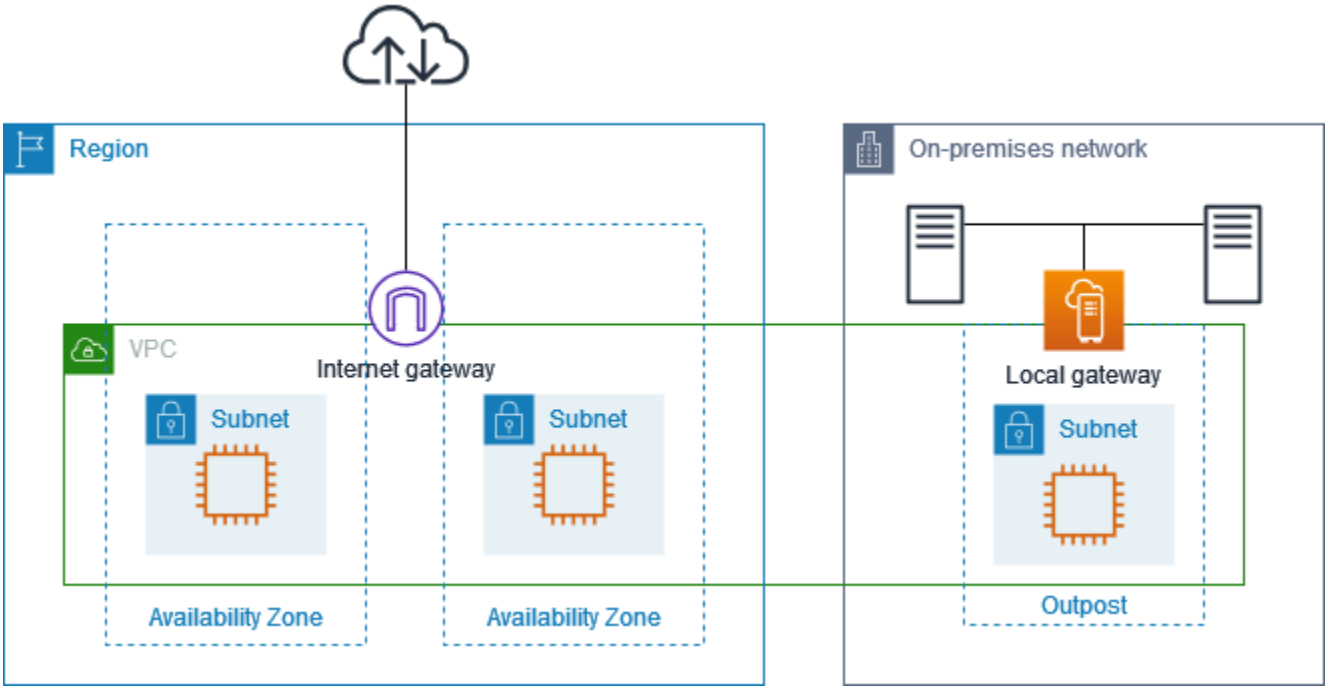
Considere a configuração a seguir:

- A VPC principal abrange duas zonas de disponibilidade e tem uma sub-rede em cada zona.

- O Outpost tem uma sub-rede.
- Cada sub-rede tem uma instância do EC2.
- O gateway local usa anúncio do BGP para anunciar os endereços IP privados da sub-rede Outpost na rede on-premises.

> **Note**
>
> O anúncio do BGP é suportado somente para sub-redes em um Outpost que tenha uma rota com o gateway local como destino. Quaisquer outras sub-redes não são anunciadas pelo BGP.

No diagrama a seguir, o tráfego da instância na sub-rede Outpost pode usar o gateway da Internet para que a VPC acesse a Internet.



Para obter conectividade com a Internet por meio da região principal, a tabela de rotas da sub-rede Outpost deve ter as seguintes rotas.

Destino	Destino	Comentários
CIDR DA VPC	Local	Fornece conectividade entre as sub-redes na VPC.

Destino	Destino	Comentários
0.0.0.0	*internet-gateway-id*	Envia tráfego destinado à Internet para o gateway da Internet.
CIDR de rede on-premises	*local-gateway-id*	Envia tráfego destinado à rede on-premises para o gateway local.

Exemplo: conectividade com a Internet por meio da rede on-premises

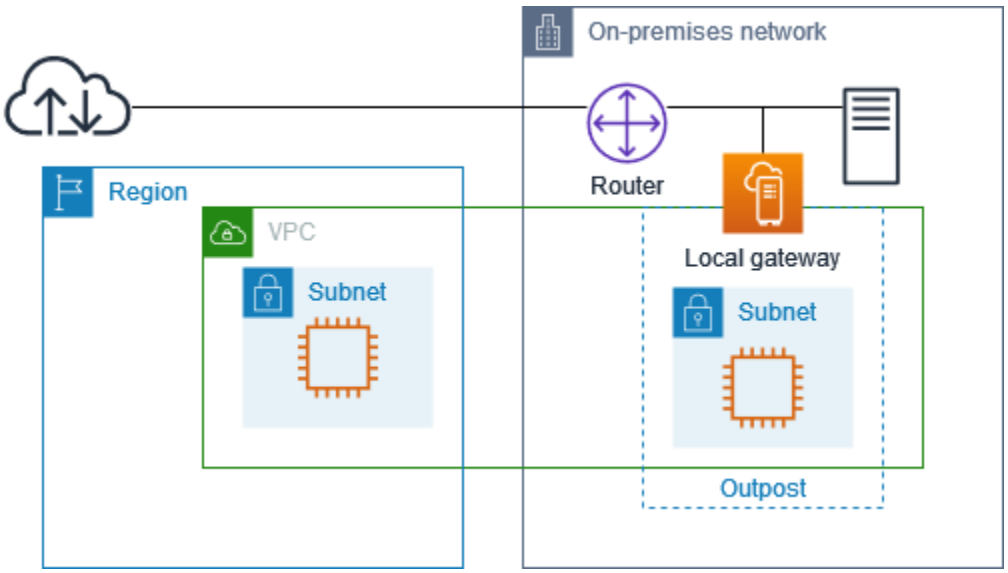
As instâncias em uma sub-rede Outpost podem acessar a Internet por meio da rede on-premises. As instâncias na sub-rede Outpost não precisam de um endereço IP público ou um endereço IP elástico.

Considere a configuração a seguir:

- A sub-rede Outpost tem uma instância do EC2.
- O roteador na rede on-premises executa a conversão de endereços de rede (NAT).
- O gateway local usa anúncio do BGP para anunciar os endereços IP privados da sub-rede Outpost na rede on-premises.

> **Note**
>
> O anúncio do BGP é suportado somente para sub-redes em um Outpost que tenha uma rota com o gateway local como destino. Quaisquer outras sub-redes não são anunciadas pelo BGP.

No diagrama a seguir, o tráfego da instância na sub-rede Outpost pode usar o gateway local para acessar a Internet ou a rede on-premises. O tráfego da rede on-premises usa o gateway local para acessar a instância na sub-rede Outpost.



Para obter conectividade com a Internet por meio da rede on-premises, a tabela de rotas da sub-rede Outpost deve ter as seguintes rotas.

Destino	Destino	Comentários
CIDR DA VPC	Local	Fornece conectividade entre as sub-redes na VPC.
0.0.0.0/0	*local-gateway-id*	Envia tráfego destinado à Internet para o gateway local.

Fornece acesso de saída à Internet

O tráfego iniciado da instância na sub-rede Outpost com um destino da Internet usa a rota de 0.0.0.0/0 para rotear o tráfego para o gateway local. O gateway local envia o tráfego para o roteador. O roteador usa NAT para traduzir o endereço IP privado em um endereço IP público no roteador e envia o tráfego para o destino.

Acesso de saída à rede on-premises

O tráfego iniciado da instância na sub-rede Outpost com um destino da rede on-premises usa a rota de 0.0.0.0/0 para rotear o tráfego para o gateway local. O gateway local envia o tráfego para o destino na rede on-premises.

Acesso de entrada da rede on-premises

O tráfego da rede on-premises com um destino da instância na sub-rede Outpost usa o endereço IP privado da instância. Quando o tráfego chega ao gateway local, o gateway local envia o tráfego para o destino na VPC.

Endereços IP de propriedade do cliente

Por padrão, o gateway local usa o endereço IP privado das instâncias na sua VPC para facilitar a comunicação com a sua rede on-premises. No entanto, você pode fornecer um intervalo de endereços, conhecido como grupo de endereços IP (CoIP) de propriedade do cliente, que suporta intervalos CIDR sobrepostos e outras topologias de rede.

Se você escolher o CoIP, deverá criar um grupo de endereços, atribuí-lo à tabela de rotas de gateway local e anunciar esses endereços de volta à rede do cliente por meio do BGP. Todos os endereços IP de propriedade do cliente associados à tabela de rotas de gateway local são exibidos na tabela de rotas como rotas propagadas.

Os endereços IP de propriedade do cliente fornecem conectividade local ou externa aos recursos na sua rede on-premises. Você pode atribuir esses endereços IP aos recursos em seu Outpost, como instâncias do EC2, alocando um novo endereço IP elástico do grupo IP de propriedade do cliente e, em seguida, atribuindo-o ao seu recurso. Para ter mais informações, consulte the section called “3f: (Opcional) Atribua um endereço IP de propriedade do cliente à instância”.

Os requisitos a seguir se aplicam ao grupo de endereços IP pertencentes ao cliente:

- Você deve ser capaz de rotear o endereço na sua rede
- O bloco CIDR deve ter no mínimo /26

Quando você aloca um endereço IP elástico do seu grupo de endereços IP pertencentes ao cliente, você continua a possuir os endereços IP em seu grupo de endereços IP pertencentes ao cliente. Você é responsável por anunciá-los conforme necessário em suas redes internas ou WAN.

Opcionalmente, você pode compartilhar seu pool de propriedade do cliente com vários Contas da AWS em sua organização usando. AWS Resource Access Manager Depois de compartilhar o grupo, os participantes podem alocar um endereço IP elástico do grupo de endereços IP pertencentes ao cliente e, em seguida, atribuí-lo a uma instância do EC2 no Outpost. Para obter mais informações, consulte Compartilhar seus recursos da AWS no Guia do usuário do AWS RAM .

Exemplos

- Exemplo: conectividade com a Internet por meio da VPC

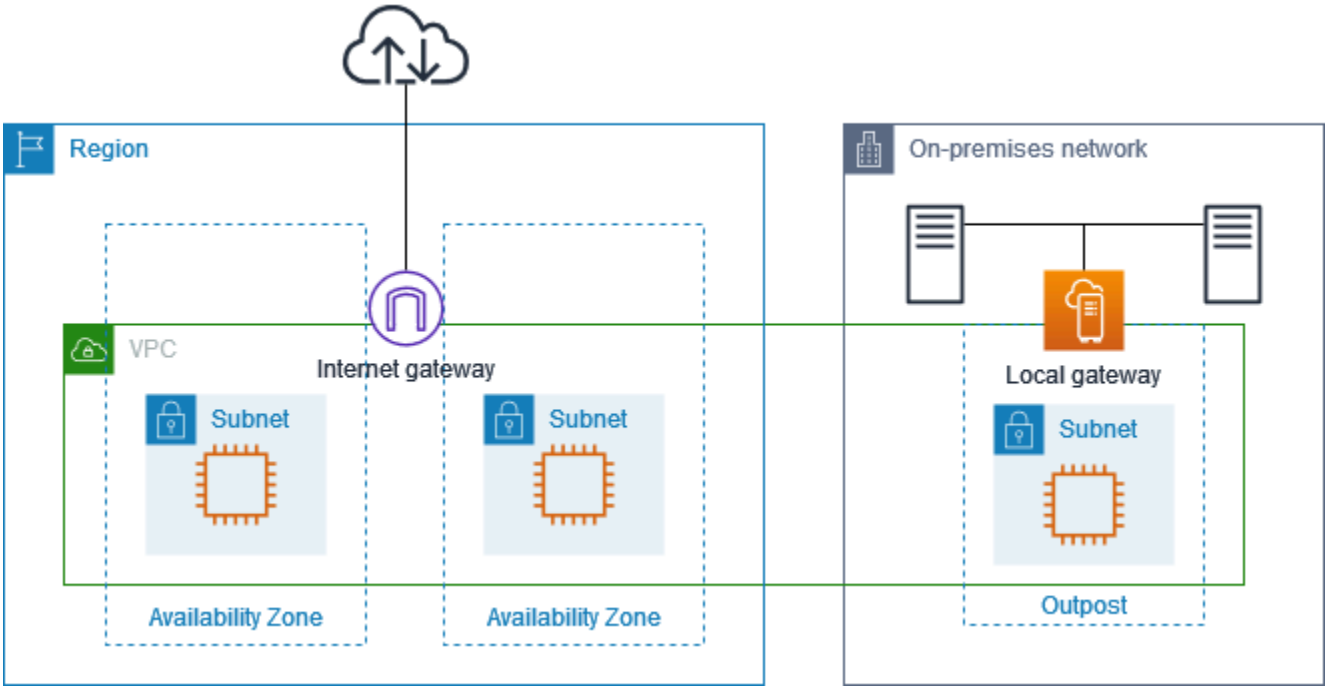
- Exemplo: conectividade com a Internet por meio da rede on-premises

Exemplo: conectividade com a Internet por meio da VPC

As instâncias em uma sub-rede Outpost podem acessar a Internet por meio do gateway da Internet conectado à VPC.

Considere a configuração a seguir:

- A VPC principal abrange duas zonas de disponibilidade e tem uma sub-rede em cada zona.
- O Outpost tem uma sub-rede.
- Cada sub-rede tem uma instância do EC2.
- Há um grupo de endereços IP pertencentes ao cliente.
- A instância na sub-rede Outpost tem um endereço IP elástico do grupo de endereços IP pertencentes ao cliente.
- O gateway local usa o anúncio do BGP para anunciar o grupo de endereços IP pertencentes ao cliente na rede on-premises.



Para obter conectividade com a Internet por meio da região, a tabela de rotas da sub-rede Outpost deve ter as seguintes rotas.

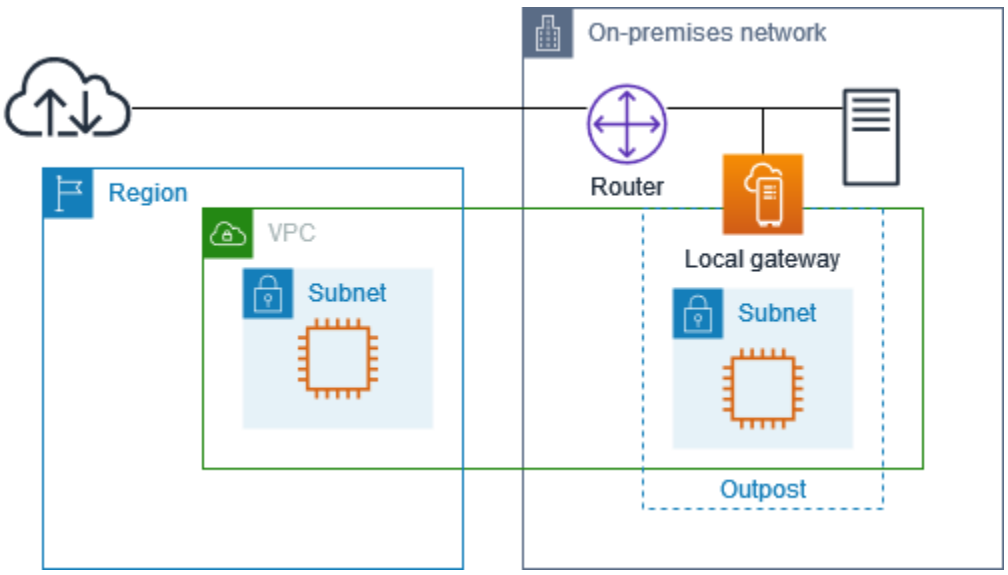
Destino	Destino	Comentários
CIDR DA VPC	Local	Fornece conectividade entre as sub-redes na VPC.
0.0.0.0	*internet-gateway-id*	Envia tráfego destinado à Internet pública para o gateway da Internet.
CIDR de rede on-premises	*local-gateway-id*	Envia tráfego destinado à rede on-premises para o gateway local.

Exemplo: conectividade com a Internet por meio da rede on-premises

As instâncias em uma sub-rede Outpost podem acessar a Internet por meio da rede on-premises.

Considere a configuração a seguir:

- A sub-rede Outpost tem uma instância do EC2.
- Há um grupo de endereços IP pertencentes ao cliente.
- O gateway local usa o anúncio do BGP para anunciar o grupo de endereços IP pertencentes ao cliente na rede on-premises.
- Uma associação de endereço IP elástico que mapeia 10.0.3.112 para 10.1.0.2.
- O roteador na rede on-premises do cliente executa o NAT.



Para obter conectividade com a Internet por meio do gateway local, a tabela de rotas da sub-rede Outpost deve ter as seguintes rotas.

Destino	Destino	Comentários
CIDR DA VPC	Local	Fornece conectividade entre as sub-redes na VPC.
0.0.0.0/0	*local-gateway-id*	Envia tráfego destinado à Internet para o gateway local.

Fornece acesso de saída à Internet

O tráfego iniciado da instância do EC2 na sub-rede Outpost com um destino da Internet usa a rota de 0.0.0.0/0 para rotear o tráfego para o gateway local. O gateway local mapeia o endereço IP privado da instância para o endereço IP do cliente e, em seguida, envia o tráfego para o roteador. O roteador usa NAT para traduzir o endereço IP privado de propriedade do cliente em um endereço IP público no roteador e envia o tráfego para o destino.

Acesso de saída à rede on-premises

O tráfego iniciado da instância do EC2 na sub-rede Outpost com um destino da rede on-premises usa a rota de 0.0.0.0/0 para rotear o tráfego para o gateway local. O gateway local converte o endereço IP da instância do EC2 para o endereço IP de propriedade do cliente (endereço IP elástico) e, em seguida, envia o tráfego para o destino.

Acesso de entrada da rede on-premises

O tráfego da rede on-premises com um destino da instância na sub-rede Outpost usa o endereço IP propriedade do cliente (endereço IP elástico) da instância. Quando o tráfego chega ao gateway local, o gateway local mapeia o endereço IP de propriedade do cliente (endereço IP elástico) para o endereço IP da instância e, em seguida, envia o tráfego para o destino na VPC. Além disso, a tabela de rotas de gateway local avalia todas as rotas que tenham como alvo interfaces de rede elásticas. Se o endereço de destino corresponder ao CIDR de destino de qualquer rota estática, o tráfego será enviado para essa interface de rede elástica. Quando o tráfego segue uma rota estática para uma interface de rede elástica, o endereço de destino é preservado e não é traduzido para o endereço IP privado da interface de rede.

Trabalhe com tabelas de rotas de gateway local

Como parte da instalação do rack, AWS cria o gateway local, configura VIFs e um grupo de VIFs. Crie a tabela de rotas de gateway local. Uma tabela de rotas de gateway local deve ter uma associação com o grupo VIF e uma VPC. Você cria e gerencia a associação do grupo VIF e da VPC. Considere as seguintes informações sobre as tabelas de rotas de gateway local:

- Os grupos VIF e as tabelas de rotas do gateway local devem ter um one-to-one relacionamento.
- O gateway local pertence à AWS conta associada ao Outpost e somente o proprietário pode modificar a tabela de rotas do gateway local.
- Você pode compartilhar a tabela de rotas do gateway local com outras AWS contas ou unidades organizacionais usando AWS Resource Access Manager. Para obter mais informações, consulte Trabalhar com recursos compartilhados AWS Outposts.
- As tabelas de rotas de gateway local têm um modo que determina se você deve usar o endereço IP privado das instâncias para se comunicar com sua rede on-premises (roteamento direto de VPC) ou com um grupo de endereços IP pertencentes ao cliente (CoIP). O roteamento Direct VPC e o CoIP são opções mutuamente exclusivas e o roteamento funciona de forma diferente com base na sua escolha. Para ter mais informações, consulte ???.
- O modo de roteamento direto de VPC não suporta intervalos CIDR sobrepostos.

Tarefas

- Exibir detalhes da tabela de rotas de gateway local
- Crie tabelas de rotas de gateway local personalizadas
- Gerenciar rotas da tabela de rotas de gateway local
- Gerenciar tags da tabela de rotas de gateway local
- Alternar os modos da tabela de rotas de gateway local ou excluir uma tabela de rotas de gateway local
- Gerenciar grupos de CoIP
- associações de grupos VIF
- associações de VPC

Exibir detalhes da tabela de rotas de gateway local

Você pode visualizar os detalhes das tabelas de rotas de gateway local usando o console ou a AWS CLI.

AWS Outposts console

Para visualizar os detalhes da tabela de rotas de gateway local

1. Abra o AWS Outposts console em https://console.aws.amazon.com/outposts/.
2. Para alterar o Região da AWS, use o seletor de região no canto superior direito da página.
3. No painel de navegação, selecione Tabela de rotas de gateway local.
4. Selecione o a tabela de rotas de gateway local e escolha Ações, Visualizar detalhes.

AWS CLI

Para visualizar os detalhes da tabela de rotas de gateway local

Use o AWS CLI comando describe-local-gateway-route-tables.

Exemplo

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

Saída

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

> **Note**
>
> Se a tabela de rotas de gateway local padrão que você está visualizando estiver usando o modo CoIP, a tabela de rotas de gateway local será configurada com uma rota padrão para cada uma das VIFs e uma rota propagada para cada endereço IP de propriedade do cliente associado no grupo de CoIP.

Crie tabelas de rotas de gateway local personalizadas

Você pode criar uma tabela de rotas personalizada para sua VPC usando o console da AWS Outposts .

Para criar uma tabela de rotas personalizada usando o console

1. Abra o AWS Outposts console em https://console.aws.amazon.com/outposts/.
2. Para alterar o Região da AWS, use o seletor de região no canto superior direito da página.
3. No painel de navegação, selecione Tabela de rotas de gateway local.
4. Escolha Criar tabela de rotas de gateway local.
5. (Opcional) Em Nome, insira um nome para a tabela de rotas do gateway.
6. Para Gateway local, escolha seu gateway local.
7. (Opcional) Escolha Associar o grupo VIF e escolha seu grupo VIF.
8. Em Modo, escolha um modo de comunicação com sua rede on-premises.
   - Escolha Roteamento direto de VPC para usar o endereço IP privado de uma instância.
   - Escolha CoIP para usar o endereço IP de propriedade do cliente.
     - (Opcional) Adicione ou remova grupos de CoIP e blocos CIDR adicionais

       [Adicionar um grupo de CoIP] Escolha Adicionar novo grupo e faça o seguinte:
       - Em Nome, digite um nome para seu grupo de CoIP.
       - Para CIDR, insira um bloco CIDR de endereços IP de propriedade do cliente.
     - [Adicionar blocos CIDR] Escolha Adicionar novo CIDR e insira um intervalo de endereços IP de propriedade do cliente.
     - [Remover um grupo de CoIP ou um bloco CIDR adicional] Escolha Remover à direita de um bloco CIDR ou abaixo do grupo de CoIP.

Você pode especificar até 10 grupos de CoIP e 100 blocos CIDR.

9. (Opcional) Adicione ou remova uma tag.

   [Adicionar uma tag] Escolha Adicionar nova tag e faça o seguinte:

   - Em Key (Chave), insira o nome da chave.
   - Em Value (Valor), insira o valor da chave.

   [Remover uma tag] Escolha Remover à direita da chave e do valor da tag.

10. Escolha Criar tabela de rotas de gateway local.

Gerenciar rotas da tabela de rotas de gateway local

Você pode criar e modificar tabelas de rotas de gateway local e rotas de entrada para interfaces de rede elásticas em seu Outpost. Você também pode modificar uma rota de entrada de gateway local existente para alterar a interface de rede elástica de destino.

Uma rota está no status ativo somente quando sua interface de rede elástica de destino está conectada a uma instância em execução. Se a instância for interrompida ou a interface for desconectada, a rota passará do status ativo para o de buraco negro.

Os seguintes requisitos e limitações se aplicam a um gateway local:

- A interface de rede elástica de destino deve pertencer a uma sub-rede em seu Outpost e deve estar conectada a uma instância nesse Outpost. Uma rota de gateway local não pode ter como alvo uma instância do Amazon EC2 em um Outpost diferente ou na Região da AWS principal.
- A sub-rede deve pertencer a uma VPC associada à tabela de rotas de gateway local.
- Você não deve exceder mais de 100 rotas de interface de rede elástica na mesma tabela de rotas.
- AWS prioriza a rota mais específica e, se as rotas corresponderem, priorizamos as rotas estáticas sobre as rotas propagadas.
- Os endpoints da VPC de interface não são compatíveis.
- O anúncio do BGP é suportado somente para sub-redes em um Outpost que tenham uma rota na tabela de rotas com o gateway local como destino. Se as sub-redes não tiverem uma rota na tabela de rotas que tenha como alvo o gateway local, essas sub-redes não serão anunciadas com o BGP.

- Somente os ENIs que estão conectados às instâncias do Outpost podem se comunicar por meio do gateway local desse Outpost. Os ENIs que pertencem à sub-rede do Outpost, mas que estão conectados a uma instância na região, não podem se comunicar por meio do gateway local desse Outpost.
- As interfaces gerenciadas, como endpoints ou interfaces VPCE, não podem ser acessadas on-premise por meio do gateway local. Elas só podem ser acessadas a partir de instâncias que estão dentro do Outpost.

As seguintes considerações NAT se aplicam.

- O gateway local não executa NAT no tráfego que corresponde a uma rota de interface de rede elástica. Em vez disso, o endereço IP de destino é preservado.
- Desative a verificação de origem/destino da interface de rede elástica de destino. Para obter mais informações, consulte Conceitos básicos de interface de rede no Manual do usuário do Amazon EC2 para instâncias do Linux.
- Configure o sistema operacional para permitir que o tráfego do CIDR de destino seja aceito na interface de rede.

AWS Outposts console

Para editar uma rota da tabela de rotas de gateway local

1. Abra o AWS Outposts console em https://console.aws.amazon.com/outposts/.
2. Para alterar o Região da AWS, use o seletor de região no canto superior direito da página.
3. No painel de navegação, selecione Tabela de rotas de gateway local.
4. Selecione a tabela de rotas de gateway local e, em seguida, escolha Ações, Editar rotas.
5. Para adicionar uma rota, escolha Add route (Adicionar rota). Em Destino insira o bloco CIDR de destino, um único endereço IP ou o ID de uma lista de prefixos.
6. Para modificar uma rota existente, em Destination (Destino), substitua o bloco CIDR de destino ou o endereço IP único. Em Target (alvo), escolha um alvo.
7. Escolha Save routes (Salvar rotas).

AWS CLI

Para criar uma rota da tabela de rotas de gateway local

- Use o create-local-gateway-route AWS CLI comando.

Exemplo

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

Saída

```
{
    "Route": {
        "DestinationCidrBlock": "192.0.2.0/24",
        "NetworkInterfaceId": "eni-03e612f0a1EXAMPLE",
        "Type": "static",
        "State": "active",
        "LocalGatewayRouteTableId": "lgw-rtb-059615ef7dEXAMPLE",
        "LocalGatewayRouteTableArn": "arn:aws:ec2:us-west-2:111122223333:local-
gateway-route-table/lgw-rtb-059615ef7dEXAMPLE",
        "OwnerId": "111122223333"
    }
}
```

Para modificar uma rota da tabela de rotas de gateway local

Você pode modificar a interface de rede elástica direcionada por uma rota existente. Para usar a operação de modificação, a tabela de rotas já deve ter uma rota com o bloco CIDR de destino especificado.

- Use o modify-local-gateway-route AWS CLI comando.

Exemplo

```
aws ec2 modify-local-gateway-route \
    --local-gateway-route-table-id lgw-rtb-059615ef7dEXAMPLE \
```

```
    --network-interface-id eni-12a345b6c7EXAMPLE \
    --destination-cidr-block 192.0.2.0/24
```

Saída

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

Gerenciar tags da tabela de rotas de gateway local

Você pode marcar suas tabelas de rotas de gateway local para ajudar a identificá-las ou categorizá-las de acordo com as necessidades da organização.

Para gerenciar as tags da tabela de rotas de gateway local

1. Abra o AWS Outposts console em https://console.aws.amazon.com/outposts/.
2. Para alterar o Região da AWS, use o seletor de região no canto superior direito da página.
3. No painel de navegação, selecione Tabelas de rotas de gateway local.
4. Selecione a tabela de rotas de gateway local e, em seguida, escolha Ações, Gerenciar tags.
5. Adicione ou remova uma tag.

   Para adicionar uma tag, escolha Adicionar nova tag e faça o seguinte:

   - Em Chave, insira o nome da chave.
   - Em Valor, insira o valor da chave.

   Para remover uma tag, escolha Remover à direita da chave e do valor da tag.
6. Escolha Salvar alterações.

Alternar os modos da tabela de rotas de gateway local ou excluir uma tabela de rotas de gateway local

Você deve excluir e recriar a tabela de rotas de gateway local para alternar os modos. A exclusão da tabela de rotas de gateway local causa interrupção do tráfego de rede.

Para alternar entre modos ou excluir uma tabela de rotas de gateway local

1. Abra o AWS Outposts console em https://console.aws.amazon.com/outposts/.
2. Para alterar o Região da AWS, use o seletor de região no canto superior direito da página.
3. No painel de navegação, selecione Tabelas de rotas de gateway local.
4. Selecione a tabela de rotas de gateway local e escolha Ações, Excluir tabela de rotas de gateway local.
5. Na caixa de diálogo de confirmação, insira **`delete`** e selecione Excluir.
6. (Opcional) Crie uma tabela de rotas de gateway local com um novo modo.
    a. Escolha Criar tabela de rotas de gateway local.
    b. Configure a tabela de rotas de gateway local usando o novo modo. Para obter mais informações, consulte Criar uma tabela de rotas de gateway local personalizada.

Gerenciar grupos de CoIP

Você pode fornecer intervalos de endereço IP para facilitar a comunicação entre sua rede e instâncias on-premises na sua VPC. Para obter mais informações, consulte Customer-owned IP addresses (Endereços IP pertencentes ao cliente).

Os grupos de IP de propriedade do cliente estão disponíveis para tabelas de rotas de gateway local no modo CoIP. Para alternar entre os modos da tabela de rotas de gateway local, consulte Mudar os modos da tabela de rotas de gateway local.

Use o procedimento a seguir para criar um grupo de CoIP.

Para criar um grupo de CoIP

1. Abra o AWS Outposts console em https://console.aws.amazon.com/outposts/.
2. Para alterar o Região da AWS, use o seletor de região no canto superior direito da página.
3. No painel de navegação, selecione Tabelas de rotas de gateway local.

4. Escolha a tabela de rotas.
5. Escolha a guia Grupos de CoIP no painel de detalhes e, em seguida, escolha Criar grupo de CoIP.
6. (Opcional) Em Nome, insira um nome para seu grupo de CoIP.
7. Escolha Adicionar novo CIDR e insira um intervalo de endereços IP de propriedade do cliente.
8. (Opcional) Adicione ou remova blocos CIDR

   [Adicionar bloco CIDR] Escolha Adicionar novo CIDR e insira um intervalo de endereços IP de propriedade do cliente.

   [Remover bloco CIDR] Escolha Remover à direita de um bloco CIDR.
9. Selecione Criar grupo de CoIP.

Use o procedimento a seguir para editar um grupo de CoIP.

Para editar um grupo de CoIP

1. Abra o AWS Outposts console em https://console.aws.amazon.com/outposts/.
2. Para alterar o Região da AWS, use o seletor de região no canto superior direito da página.
3. No painel de navegação, selecione Tabelas de rotas de gateway local.
4. Escolha a tabela de rotas.
5. Escolha a guia Grupos de CoIP no painel de detalhes e, em seguida, escolha um grupo de CoIP.
6. Escolha Ações, Editar grupo de CoIP.
7. Escolha Adicionar novo CIDR e insira um intervalo de endereços IP de propriedade do cliente.
8. (Opcional) Adicione ou remova blocos CIDR

   [Adicionar bloco CIDR] Escolha Adicionar novo CIDR e insira um intervalo de endereços IP de propriedade do cliente.

   [Remover bloco CIDR] Escolha Remover à direita de um bloco CIDR.
9. Escolha Salvar alterações.

Use o procedimento a seguir para gerenciar tags ou adicionar uma tag de nome a um grupo de CoIP.

Para gerenciar tags em um grupo de CoIP

1. Abra o AWS Outposts console em https://console.aws.amazon.com/outposts/.
2. Para alterar o Região da AWS, use o seletor de região no canto superior direito da página.
3. No painel de navegação, selecione Tabelas de rotas de gateway local.
4. Escolha a tabela de rotas.
5. Escolha a guia Grupos de CoIP no painel de detalhes e, em seguida, escolha um grupo de CoIP.
6. Escolha Ações, Gerenciar tags.
7. Adicione ou remova uma tag.

   Para adicionar uma tag, escolha Adicionar nova tag e faça o seguinte:

   - Em Chave, insira o nome da chave.
   - Em Valor, insira o valor da chave.

   Para remover uma tag, escolha Remover à direita da chave e do valor da tag.
8. Escolha Salvar alterações.

Use o procedimento a seguir para excluir um grupo de CoIP.

Para excluir um grupo de CoIP

1. Abra o AWS Outposts console em https://console.aws.amazon.com/outposts/.
2. Para alterar o Região da AWS, use o seletor de região no canto superior direito da página.
3. No painel de navegação, selecione Tabelas de rotas de gateway local.
4. Escolha a tabela de rotas.
5. Escolha a guia Grupos de CoIP no painel de detalhes e, em seguida, escolha um grupo de CoIP.
6. Escolha Ações, Excluir grupo de CoIP.
7. Na caixa de diálogo de confirmação, insira **`delete`** e selecione Excluir.

associações de grupos VIF

Os grupos VIF são agrupamentos lógicos de interfaces virtuais (VIFs). Você pode alterar a tabela de rotas de gateway local à qual o grupo VIF está associado. Ao desassociar um grupo VIF de uma

tabela de rotas de gateway local, você exclui todas as rotas da tabela de rotas e interrompe o tráfego da rede.

Para alterar a associação de um grupo VIF

1. Abra o AWS Outposts console em https://console.aws.amazon.com/outposts/.
2. Para alterar o Região da AWS, use o seletor de região no canto superior direito da página.
3. No painel de navegação, selecione Tabelas de rotas de gateway local.
4. Escolha a tabela de rotas.
5. Escolha a guia Associação de grupo VIF no painel de detalhes e, em seguida, escolha Editar associação de grupo VIF.
6. Para configurações de grupo VIF, execute uma das seguintes ações:
   - Para associar o grupo VIF à tabela de rotas de gateway local, selecione Associar grupo VIF e escolha um grupo VIF.
   - Para dissociar o grupo VIF da tabela de rotas de gateway local, desmarque Associar grupo VIF.

   > **Important**
   >
   > A desassociação de um grupo VIF da tabela de rotas de gateway local exclui automaticamente todas as rotas e interrompe o tráfego da rede.
7. Escolha Salvar alterações.

associações de VPC

Você deve associar as VPCs à tabela de rotas de gateway local. Eles não são associados por padrão.

Crie uma associação de VPC

Siga o procedimento abaixo para associar a VPC à tabela de rotas de gateway local.

Você pode marcar o serviço de endpoint para ajudar a identificá-lo ou categorizá-lo de acordo com as necessidades da organização.

AWS Outposts console

Para associar uma VPC

1. Abra o AWS Outposts console em https://console.aws.amazon.com/outposts/.
2. Para alterar o Região da AWS, use o seletor de região no canto superior direito da página.
3. No painel de navegação, selecione Tabelas de rotas de gateway local.
4. Selecione a tabela de rotas e, em seguida, escolha Ações, Associar VPC.
5. Para VPC ID, selecione a VPC a ser associada à tabela de rotas de gateway local.
6. (Opcional) Adicione ou remova uma tag.

   Para adicionar uma tag, escolha Adicionar nova tag e faça o seguinte:

   - Em Chave, insira o nome da chave.
   - Em Valor, insira o valor da chave.

   Para remover uma tag, escolha Remover à direita da chave e do valor da tag.
7. Escolha Associate VPC.

AWS CLI

Para associar uma VPC

Use o table-vpc-association comando create-local-gateway-route-.

Exemplo

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

Saída

```
{
    "LocalGatewayRouteTableVpcAssociation": {
        "LocalGatewayRouteTableVpcAssociationId": "lgw-vpc-assoc-0ee765bcc8EXAMPLE",
        "LocalGatewayRouteTableId": "lgw-rtb-059615ef7dEXAMPLE",
        "LocalGatewayId": "lgw-09b493aa7cEXAMPLE",
```

```
        "VpcId": "vpc-07ef66ac71EXAMPLE",
        "State": "associated"
    }
}
```

Excluir uma associação VPC

Siga o procedimento abaixo para desassociar a VPC à tabela de rotas de gateway local.

AWS Outposts console

Para desassociar uma VPC

1. Abra o AWS Outposts console em https://console.aws.amazon.com/outposts/.
2. Para alterar o Região da AWS, use o seletor de região no canto superior direito da página.
3. No painel de navegação, selecione Tabelas de rotas de gateway local.
4. Selecione a tabela de rotas e escolha Ações, Visualizar detalhes.
5. Em associações de VPC, selecione a VPC a ser dissociada e escolha Dissociar.
6. Escolha Desassociar.

AWS CLI

Para desassociar uma VPC

Use o table-vpc-association comando delete-local-gateway-route-.

Exemplo

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

Saída

```
{
    "LocalGatewayRouteTableVpcAssociation": {
        "LocalGatewayRouteTableVpcAssociationId": "lgw-vpc-assoc-0ee765bcc8EXAMPLE",
        "LocalGatewayRouteTableId": "lgw-rtb-059615ef7dEXAMPLE",
        "LocalGatewayId": "lgw-09b493aa7cEXAMPLE",
```

```
        "VpcId": "vpc-07ef66ac71EXAMPLE",
        "State": "associated"
    }
}
```

Conectividade da rede local para racks

Você precisa dos seguintes componentes para conectar seu rack Outpost à sua rede on-premises:

- Conectividade física do painel de patches do Outpost com os dispositivos de rede local do cliente.
- Protocolo de Controle de Agregação de Links (LACP) para estabelecer duas conexões de grupo de agregação de links (LAG) com seus dispositivos de rede Outpost e com seus dispositivos de rede local.
- Conectividade de LAN virtual (VLAN) entre o Outpost e os dispositivos de rede local do seu cliente.
- point-to-point Conectividade de camada 3 para cada VLAN.
- Protocolo de Gateway da Borda (BGP) para o anúncio da rota entre o Outpost e seu link de serviço on-premises.
- BGP para o anúncio da rota entre o Outpost e seu dispositivo de rede on-premises local para conectividade com o gateway local.

Conteúdo

Conectividade física

Um rack Outpost tem dois dispositivos físicos de rede que se conectam à sua rede local.

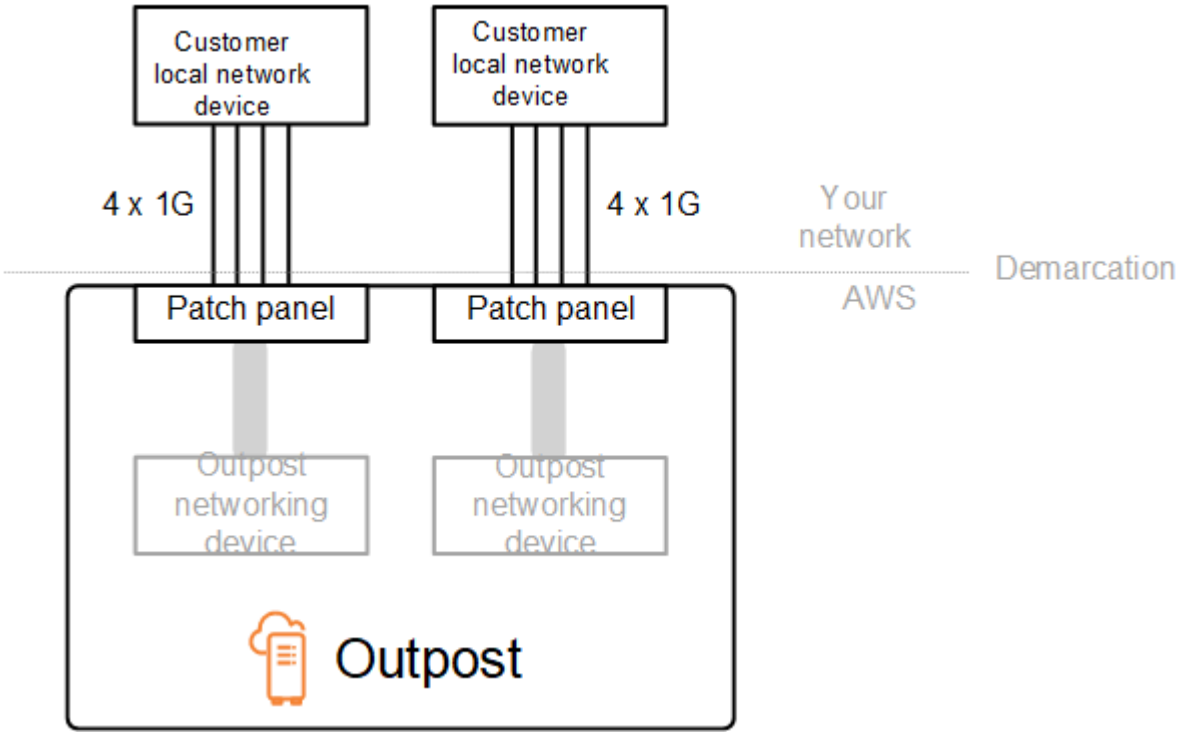
Um Outpost requer no mínimo dois links físicos entre esses dispositivos de rede Outpost e seus dispositivos de rede local. Um Outpost suporta as seguintes velocidades e quantidades de uplink para cada dispositivo de rede Outpost.

Velocidade do uplink	Número de uplinks
1 Gbps	1, 2, 4, 6, ou 8
10 Gbps	1, 2, 4, 8, 12, ou 16
40 Gbps ou 100 Gbps	1, 2, ou 4

A velocidade e a quantidade do uplink são simétricas em cada dispositivo de rede Outpost. Se você usar 100 Gbps como velocidade de uplink, deverá configurar o link com correção de erro de encaminhamento (FEC CL91).

Os racks Outpost podem suportar fibra monomodo (SMF) com conector Lucent (LC), fibra multimodo (MMF) ou MMF OM4 com LC. A AWS fornece a ótica compatível com a fibra que você fornece na posição do rack.

No diagrama a seguir, a demarcação física é o painel de patch de fibra em cada Outpost. Você fornece os cabos de fibra necessários para conectar o Outpost ao painel de patch.



Agregação de links

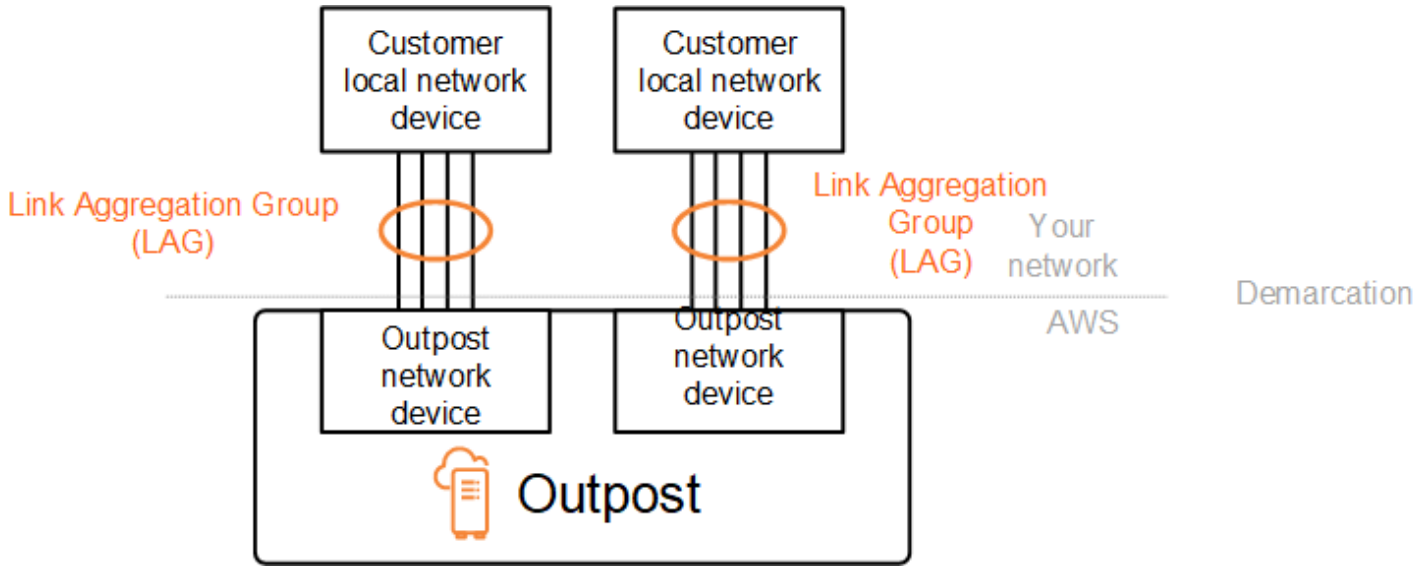
O AWS Outposts usa o Protocolo de Controle de Agregação de Links (LACP) para estabelecer duas conexões de grupo de agregação de links (LAG), uma de cada dispositivo de rede Outpost para cada dispositivo de rede local. Os links de cada dispositivo de rede Outpost são agregados em um LAG Ethernet para representar uma única conexão de rede. Esses LAGs usam LACP com temporizadores rápidos padrão. Você não pode configurar LAGs para usar temporizadores lentos.

Para habilitar uma instalação do Outpost em seu site, você deve configurar seu lado das conexões LAG em seus dispositivos de rede.

De uma perspectiva lógica, ignore os painéis de patch do Outpost como ponto de demarcação e use os dispositivos de rede do Outpost.

Para implantações com vários racks, um Outpost deve ter quatro LAGs entre a camada de agregação dos dispositivos de rede Outpost e seus dispositivos de rede local.

O diagrama a seguir mostra quatro conexões físicas entre cada dispositivo de rede Outpost e seu dispositivo de rede local conectado. Usamos LAGs Ethernet para agregar os links físicos que conectam os dispositivos de rede Outpost e os dispositivos de rede local do cliente.



LANs virtuais

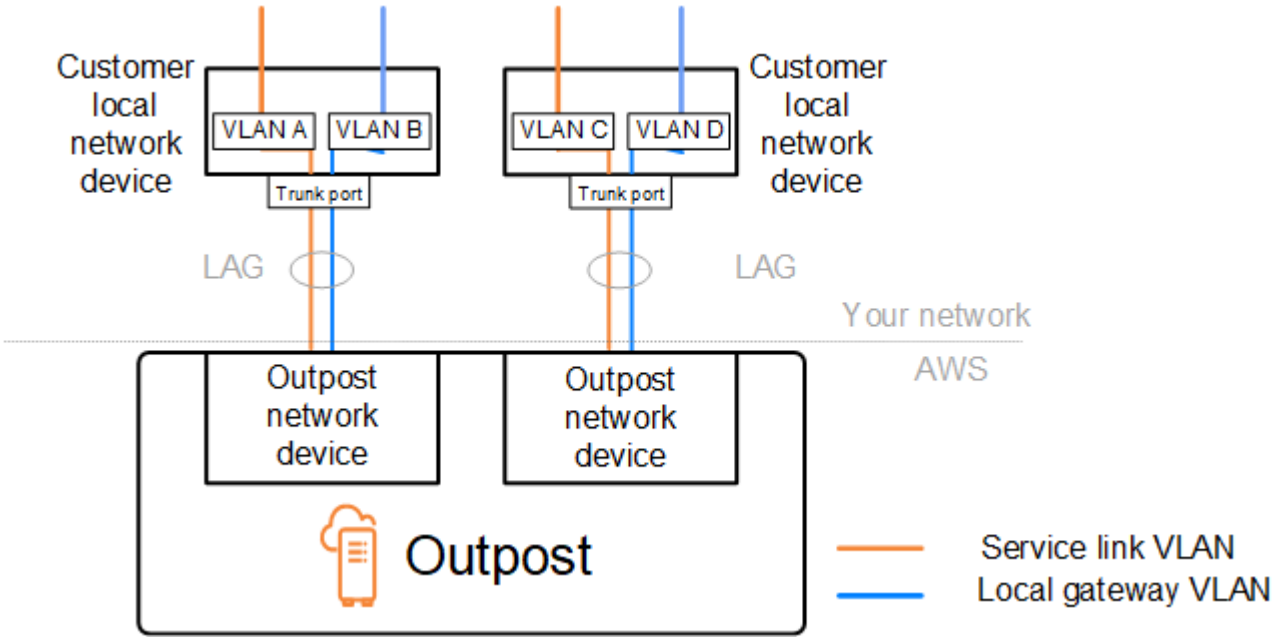
Cada LAG entre um dispositivo de rede Outpost e um dispositivo de rede local deve ser configurado como um tronco Ethernet IEEE 802.1q. Isso permite o uso de várias VLANs para segmentação de rede entre caminhos de dados.

Cada Outpost tem as seguintes VLANs para se comunicar com seus dispositivos de rede local:

- VLAN de link de serviço — Permite a comunicação entre seu Outpost e seus dispositivos de rede local para estabelecer um caminho de link de serviço para a conectividade do link de serviço. Para obter mais informações, consulte AWS Outpostsconectividade com AWS regiões.
- VLAN de gateway local — Permite a comunicação entre seu Outpost e seus dispositivos de rede local para estabelecer um caminho de gateway local para conectar suas sub-redes Outpost e sua rede local. O gateway local Outpost aproveita essa VLAN para fornecer às suas instâncias a conectividade com sua rede local, o que pode incluir acesso à Internet por meio de sua rede. Para obter mais informações, consulte Gateway local.

Você pode configurar a VLAN do link de serviço e a VLAN do gateway local somente entre o Outpost e os dispositivos de rede local do seu cliente.

Um Outpost foi projetado para separar o link de serviço e os caminhos de dados do gateway local em duas redes isoladas. Isso permite que você escolha quais de suas redes podem se comunicar com os serviços em execução no Outpost. Ele também permite que você transforme o link de serviço em uma rede isolada da rede de gateway local usando várias tabela de rotas no dispositivo de rede local do cliente, comumente conhecido como instâncias de roteamento e encaminhamento virtuais (VRF). A linha de demarcação existe na porta dos dispositivos de rede Outpost. A AWS gerencia qualquer infraestrutura no lado da conexão do AWS, e você gerencia qualquer infraestrutura no seu lado da linha.



Para integrar seu Outpost à sua rede on-premises durante a instalação e a operação contínua, você deve alocar as VLANs usadas entre os dispositivos de rede Outpost e os dispositivos de rede local do cliente. Você precisa fornecer essas informações para AWS antes da instalação. Para ter mais informações, consulte the section called “Lista de verificação de prontidão da rede”.

Conectividade da camada de rede

Para estabelecer a conectividade da camada de rede, cada dispositivo de rede Outpost é configurado com interfaces virtuais (VIFs) que incluem o endereço IP de cada VLAN. Por meio desses VIFs, os dispositivos de AWS Outposts rede podem configurar sessões de conectividade IP e BGP com seu equipamento de rede local.

Recomendamos o seguinte:

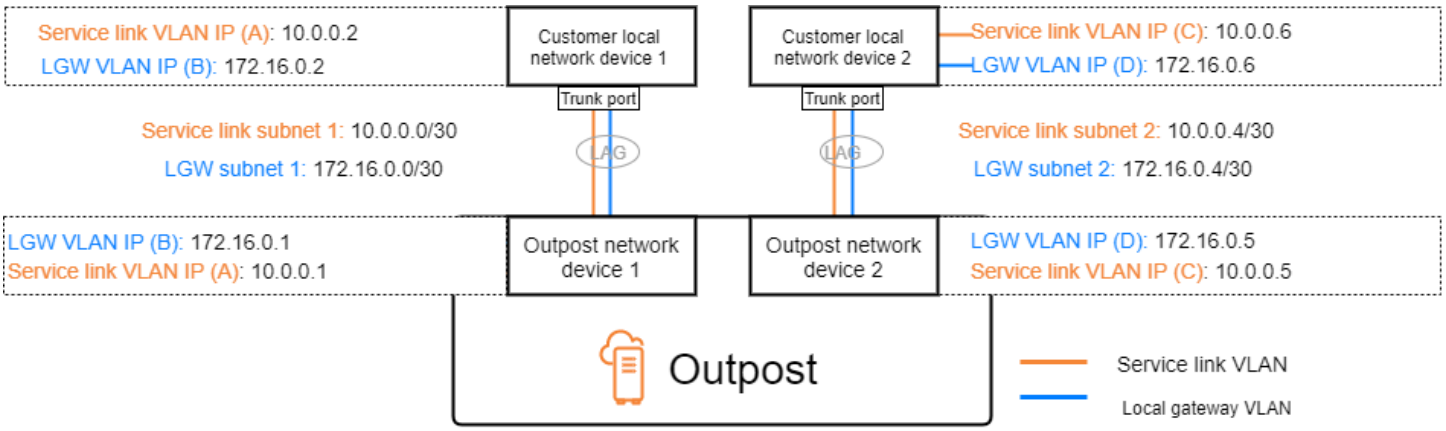
- Use uma sub-rede dedicada, com um CIDR /30 ou /31, para representar essa conectividade lógica. point-to-point
- Não conecte as VLANs entre seus dispositivos de rede local.

Para a conectividade da camada de rede, você deve estabelecer dois caminhos:

- Caminho do link de serviço - Para estabelecer esse caminho, especifique uma sub-rede de VLAN com um intervalo de /30 ou /31 e um endereço IP para cada VLAN de link de serviço no dispositivo de rede. AWS Outposts As interfaces virtuais de link de serviço (VIFs) são usadas nesse caminho para estabelecer conectividade IP e sessões de BGP entre seu Outpost e seus dispositivos de rede local para conectividade de link de serviço. Para obter mais informações, consulte AWS Outpostsconectividade com AWS regiões.
- Caminho do gateway local - Para estabelecer esse caminho, especifique uma sub-rede de VLAN com um intervalo de /30 ou /31 e um endereço IP para a VLAN do gateway local no dispositivo de rede. AWS Outposts Os VIFs de gateway local são usados nesse caminho para estabelecer conectividade IP e sessões BGP entre seu Outpost e seus dispositivos de rede local para sua conectividade de recursos locais.

O diagrama a seguir mostra as conexões de cada dispositivo de rede Outpost com o dispositivo de rede local do cliente para o caminho do link de serviço e o caminho do gateway local. Há quatro VLANs para este exemplo:

- A VLAN A é para o caminho do link de serviço que conecta o dispositivo de rede Outpost 1 ao dispositivo de rede local 1 do cliente.
- A VLAN B é para o caminho do gateway local que conecta o dispositivo de rede Outpost 1 ao dispositivo de rede local 1 do cliente.
- A VLAN C é para o caminho do link de serviço que conecta o dispositivo de rede Outpost 2 ao dispositivo de rede local 2 do cliente.
- A VLAN D é para o caminho do gateway local que conecta o dispositivo de rede Outpost 2 ao dispositivo de rede local 2 do cliente.



A tabela a seguir mostra exemplos de valores para as sub-redes que conectam o dispositivo de rede Outpost 1 ao dispositivo de rede local 1 do cliente.

VLAN	Sub-rede	Dispositivo do cliente: 1 IP	AWS OND 1 IP
A	10.0.0.0/30	10.0.0.2	10.0.0.1
B	172.16.0.0/30	172.16.0.2	172.16.0.1

A tabela a seguir mostra exemplos de valores para as sub-redes que conectam o dispositivo de rede Outpost 2 ao dispositivo de rede local 2 do cliente.

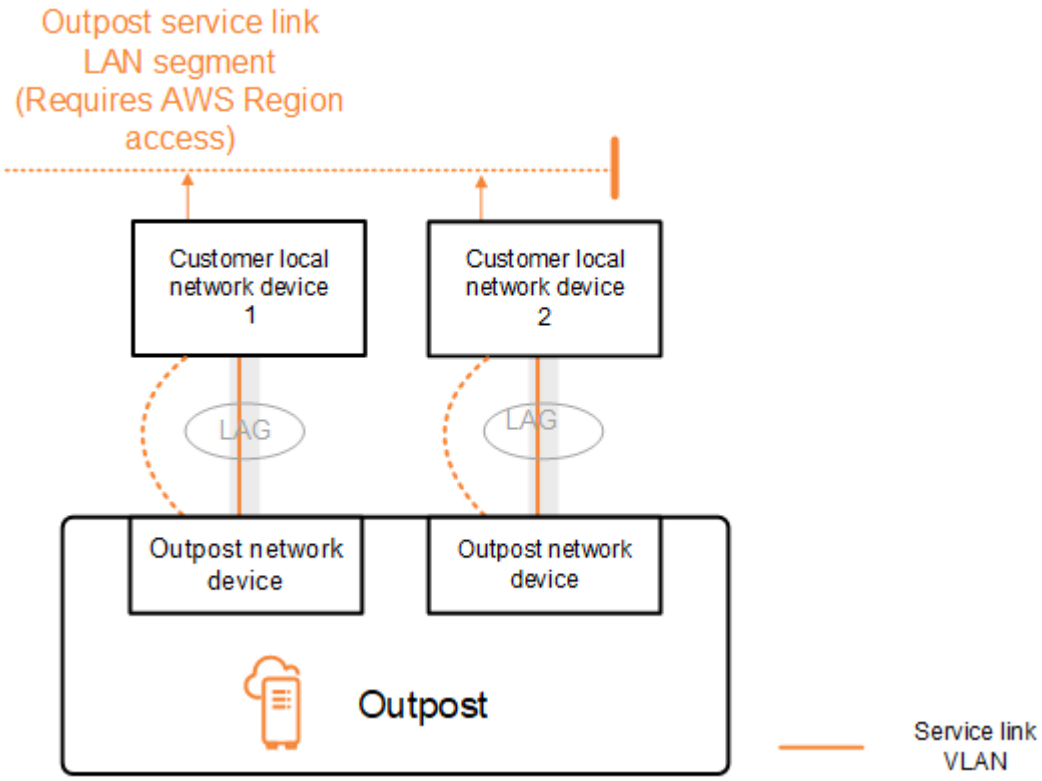
VLAN	Sub-rede	Dispositivo do cliente: 2 IP	AWS OND 2 IP
C	10.0.0.4/30	10.0.0.6	10.0.0.5
D	172.16.0.4/30	172.16.0.6	172.16.0.5

Conectividade do link de serviço BGP

O Outpost estabelece uma sessão de emparelhamento de BGP externo entre cada dispositivo de rede do Outpost e o dispositivo de rede local do cliente para conectividade do link de serviço pela VLAN do link de serviço. A sessão de emparelhamento BGP é estabelecida entre os endereços IP /30 ou /31 fornecidos para a VLAN. point-to-point Cada sessão de emparelhamento do BGP usa um Número de Sistema Autônomo (ASN) privado no dispositivo de rede Outpost e um ASN que você escolhe para os dispositivos de rede local do cliente. A AWS fornece os atributos como parte do processo de instalação.

Considere o cenário em que você tem um Outpost com dois dispositivos de rede Outpost conectados por uma VLAN de link de serviço a dois dispositivos de rede local do cliente. Você configura a seguinte infraestrutura e os atributos BGP ASN do dispositivo de rede local do cliente para cada link de serviço:

- O link de serviço BGP ASN. 2 bytes (16 bits) ou 4 bytes (32 bits). Os valores válidos são 64512-65535 ou 4200000000-4294967294.
- A infraestrutura CIDR. Deve ser um CIDR /26 por rack.
- O endereço IP do par BGP do link de serviço do dispositivo de rede local 1 do cliente.
- O ASN do par BGP do link de serviço do dispositivo de rede local 1 do cliente. Os valores válidos são 1-4294967294.
- O endereço IP do par BGP do link de serviço do dispositivo de rede local 2 do cliente.
- O ASN do par BGP do link de serviço do dispositivo de rede local 2 do cliente. Os valores válidos são 1-4294967294. Para obter mais informações, consulte RFC4893.



O Outpost estabelece uma sessão externa de emparelhamento BGP pela VLAN do link de serviço usando o seguinte processo:

1. Cada dispositivo de rede Outpost usa o ASN para estabelecer uma sessão de emparelhamento BGP com seu dispositivo de rede local conectado.
2. Os dispositivos de rede Outpost anunciam o intervalo CIDR /26 como dois intervalos CIDR /27 para suportar falhas de links e dispositivos. Cada OND anuncia seu próprio prefixo /27 com um comprimento de AS-path de 1, mais os prefixos /27 de todos os outros ONDs com um comprimento de AS-path de 4 como backup.
3. A sub-rede é usada para conectividade do Outpost à região da AWS.

Recomendamos que você configure o equipamento de rede do cliente para receber anúncios BGP do Outposts sem alterar os atributos do BGP. A rede do cliente deve preferir rotas de Outposts com um comprimento de caminho AS de 1 em vez de rotas com um comprimento de caminho AS de 4.

A rede do cliente deve anunciar prefixos BGP iguais com os mesmos atributos para todos os ONDs. Por padrão, a carga da rede Outpost equilibra o tráfego de saída entre todos os uplinks. As políticas de roteamento são usadas no lado do Outpost para afastar o tráfego de um OND se a manutenção for necessária. Essa mudança de tráfego exige prefixos BGP iguais do lado do cliente em todos os

ONDs. Se for necessária manutenção na rede do cliente, recomendamos que você use o acréscimo de caminho AS para mudar temporariamente a matriz de tráfego de uplinks específicos.

Infraestrutura de link de serviço, anúncio de sub-rede e faixa de IP

Você fornece um intervalo CIDR /26 durante o processo de pré-instalação da sub-rede da infraestrutura do link de serviço. A infraestrutura do Outpost usa essa faixa para estabelecer conectividade com a região por meio do link de serviço. A sub-rede do link de serviço é a fonte Outpost, que inicia a conectividade.

Os dispositivos de rede Outpost anunciam o intervalo CIDR /26 como dois blocos CIDR /27 para suportar falhas de links e dispositivos.

Você deve fornecer um link de serviço BGP ASN e um CIDR de sub-rede de infraestrutura (/26) para o Outpost. Para cada dispositivo de rede Outpost, forneça o endereço IP de emparelhamento BGP na VLAN do dispositivo de rede local e o BGP ASN do dispositivo de rede local.

Se você tiver uma implantação de vários racks, deverá ter uma sub-rede /26 por rack.

Conectividade do BGP do gateway local

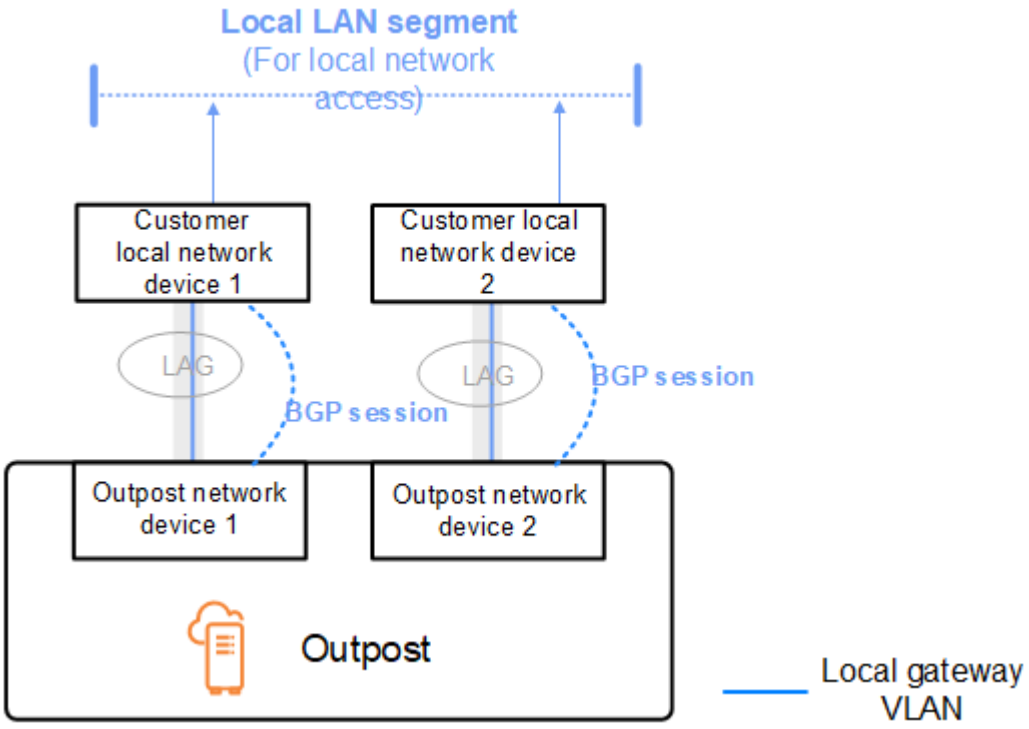
O Outpost estabelece uma sessão de emparelhamento do BGP externo de cada dispositivo de rede do Outpost para um dispositivo de rede local para conectividade com o gateway local. Ele usa um número de sistema autônomo (ASN) privado que você atribui para estabelecer as sessões BGP externas. Cada dispositivo de rede Outpost tem um único BGP externo emparelhando para um dispositivo de rede local usando sua VLAN de gateway local.

O Outpost estabelece uma sessão de emparelhamento de BGP pela VLAN do gateway local entre cada dispositivo de rede do Outpost e seu dispositivo de rede local do cliente conectado. A sessão de emparelhamento é estabelecida entre os IPs /30 ou /31 que você forneceu ao configurar a conectividade de rede e usa a point-to-point conectividade entre os dispositivos de rede Outpost e os dispositivos de rede local do cliente. Para ter mais informações, consulte the section called “Conectividade da camada de rede”.

Cada sessão de emparelhamento do BGP usa um Número de Sistema Autônomo (ASN) privado no dispositivo de rede Outpost e um ASN que você escolhe para os dispositivos de rede local do cliente. A AWS fornece os atributos como parte do processo de pré-instalação.

Considere o cenário em que você tem um Outpost com dois dispositivos de rede Outpost conectados por uma VLAN de link de serviço a dois dispositivos de rede local do cliente. Você configura os seguintes atributos BGP ASN do gateway local e do dispositivo de rede local do cliente para cada link de serviço:

- A AWS fornece o gateway local BGP ASN. 2 bytes (16 bits) ou 4 bytes (32 bits). Os valores válidos são 64512-65535 ou 4200000000-4294967294.
- (Opcional) Você fornece o CIDR de propriedade do cliente que é anunciado (público ou privado, no mínimo /26).
- Você fornece o endereço IP do par BGP do gateway do dispositivo de rede local do cliente 1.
- Você fornece o ASN do par BGP do gateway do dispositivo de rede local do cliente 1. Os valores válidos são 1-4294967294. Para obter mais informações, consulte RFC4893.
- Você fornece o endereço IP do par BGP do gateway do dispositivo de rede local do cliente 2.
- Você fornece o ASN do par BGP do gateway do dispositivo de rede local do cliente 2. Os valores válidos são 1-4294967294. Para obter mais informações, consulte RFC4893.



Recomendamos que você configure o equipamento de rede do cliente para receber anúncios BGP dos Outposts sem alterar os atributos do BGP e habilite o balanceamento de vários caminhos/carga do BGP para obter fluxos de tráfego de entrada ideais. O acréscimo de caminho AS é usado para

prefixos de gateway local para afastar o tráfego dos ONDs se a manutenção for necessária. A rede do cliente deve preferir rotas de Outposts com um comprimento de caminho AS de 1 em vez de rotas com um comprimento de caminho AS de 4.

A rede do cliente deve anunciar prefixos BGP iguais com os mesmos atributos para todos os ONDs. Por padrão, a carga da rede Outpost equilibra o tráfego de saída entre todos os uplinks. As políticas de roteamento são usadas no lado do Outpost para afastar o tráfego de um OND se a manutenção for necessária. Essa mudança de tráfego exige prefixos BGP iguais do lado do cliente em todos os ONDs. Se for necessária manutenção na rede do cliente, recomendamos que você use o acréscimo de caminho AS para mudar temporariamente a matriz de tráfego de uplinks específicos.

Anúncio de sub-rede IP de propriedade do cliente do gateway local

Por padrão, o gateway local usa o endereço IP privado das instâncias na sua VPC para facilitar a comunicação com a sua rede on-premises. No entanto, você pode fornecer um grupo de endereços IP pertencentes ao cliente (CoIP).

Se você escolher CoIP, a AWS cria o grupo a partir das informações fornecidas durante o processo de instalação. Você pode criar endereços IP elásticos a partir desse grupo e, em seguida, atribuir os endereços aos recursos em seu Outpost, como instâncias do EC2.

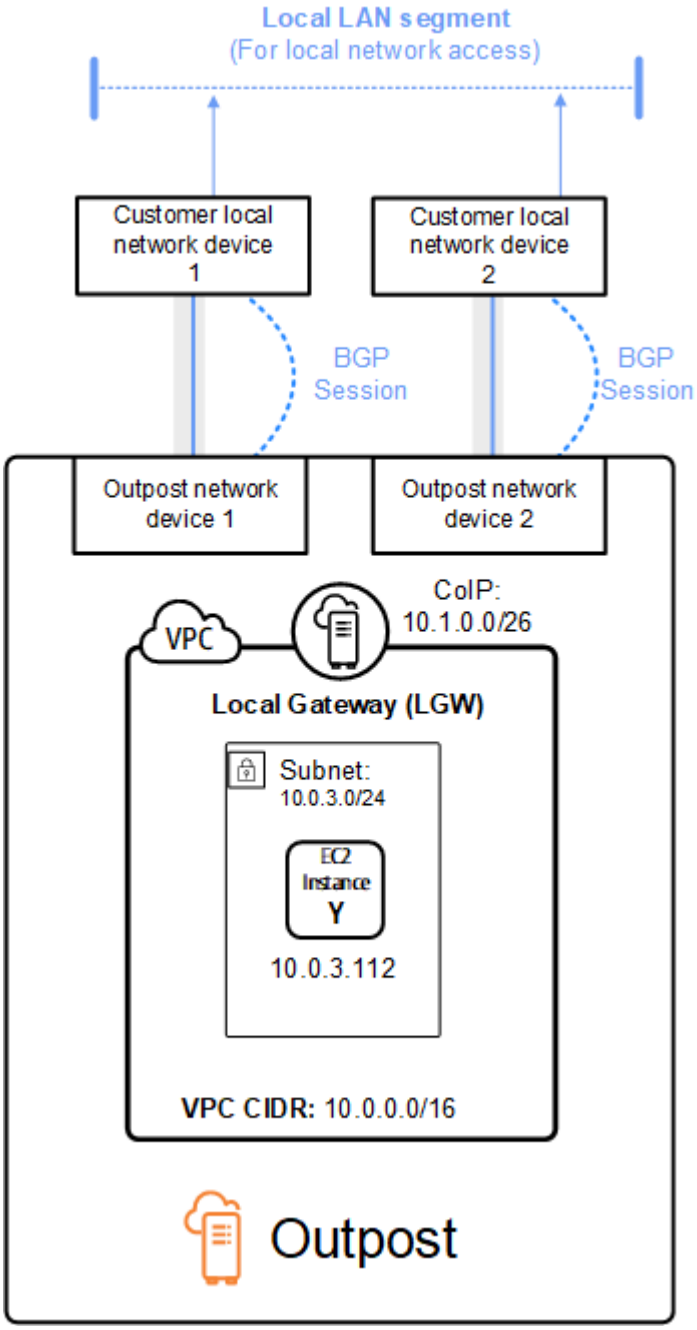
O gateway local converte o endereço IP elástico em um endereço no grupo de propriedade do cliente. O gateway local anuncia o endereço traduzido em sua rede on-premises e em qualquer outra rede que se comunique com o Outpost. Os endereços são anunciados em ambas as sessões BGP do gateway local para os dispositivos de rede local.

> **Tip**
>
> Se você não estiver usando CoIP, o BGP anuncia os endereços IP privados de qualquer sub-rede em seu Outpost que tenha uma rota na tabela de rotas que tem como alvo o gateway local.

Considere o cenário em que você tem um Outpost com dois dispositivos de rede Outpost conectados por uma VLAN de link de serviço a dois dispositivos de rede local do cliente. O seguinte foi configurado:

- Uma VPC com um bloco CIDR 10.0.0.0/16.

- Uma sub-rede na VPC com um bloco CIDR 10.0.3.0/24.
- Uma instância do EC2 na sub-rede com um endereço IP privado 10.0.3.112.
- Um grupo de IPs de propriedade do cliente (10.1.0.0/26).
- Uma associação de endereço IP elástico que associa 10.0.3.112 a 10.1.0.2.
- Um gateway local que usa o BGP para anunciar 10.1.0.0/26 na rede on-premises por meio dos dispositivos locais.
- A comunicação entre seu Outpost e a rede on-premises usará os IPs elásticos CoIP para endereçar instâncias no Outpost. O intervalo CIDR da VPC não será usado.


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

Trabalhar com recursos do AWS Outposts compartilhados

Com o compartilhamento do Outpost, os proprietários do Outpost podem compartilhar seus Outposts e recursos do Outpost, incluindo locais e sub-redes do Outpost, com outras contas AWS da mesma organização da AWS. Como proprietário do Outpost, você pode criar e gerenciar recursos do Outpost de forma centralizada, além de compartilhar os recursos em várias contas da AWS na sua organização da AWS. Isso permite que outros consumidores usem sites do Outposts, configurem VPCs e iniciem e executem instâncias no Outpost compartilhado.

Nesse modelo, a conta AWS que tem os recursos do Outpost (Proprietário) compartilha os recursos com outras contas AWS (consumidores) na mesma organização. Os consumidores podem criar recursos nos Outposts que são compartilhados com eles da mesma maneira que elaborariam recursos nos Outposts criados nas próprias contas. O proprietário é responsável pelo gerenciamento do Outpost e pelos recursos que ele cria nele. Os proprietários podem alterar ou revogar o acesso compartilhado a qualquer momento. Com exceção das instâncias que consomem Reservas de capacidade, os proprietários também podem visualizar, modificar e excluir recursos criados pelos consumidores em Outposts compartilhados. Os proprietários não podem modificar as instâncias que os consumidores executam nas Reservas de Capacidade que compartilharam.

Os consumidores são responsáveis por gerenciar os recursos que criam nos Outposts e que são compartilhadas com eles, incluindo quaisquer recursos que consumam reservas de capacidade. Os consumidores não podem visualizar nem modificar recursos de propriedade de outros consumidores ou do proprietário do Outpost. Também não é possível modificar os Outposts que são compartilhados com eles.

O proprietário de um Outpost pode compartilhar recursos do Outpost com:

- Contas da AWS específicas dentro da organização no AWS Organizations.
- Uma unidade organizacional dentro da sua organização no AWS Organizations.
- Toda a organização no AWS Organizations.

Índice

- Compartilhamento de um recurso do Outpost
- Cancelamento do compartilhamento de um recurso compartilhado do Outpost
- Identificando um recurso compartilhado do Outpost
- Permissões de recursos do Outpost compartilhadas
- Faturamento e medição
- Limitações

Recursos compartilháveis do Outpost

O proprietário de um Outpost pode compartilhar os recursos do Outpost listados nesta seção com os consumidores.

Esses são os recursos disponíveis para os de rack Outpost. Para recursos de servidor, consulte Trabalho com recursos compartilhados do AWS Outposts no Guia do usuário do AWS Outposts para servidores do Outposts.

- Hosts dedicados alocados – Os consumidores com acesso a este recurso podem:
  - Inicie e execute instâncias do EC2 em um Host dedicado.
- Reservas de capacidade – Os consumidores com acesso a este recurso podem:
  - Identificar as reservas de capacidade compartilhadas com eles.
  - Executar e gerenciar instâncias que consomem reservas de capacidade.
- Pools de endereços IP pertencentes ao cliente (CoIP) – Os consumidores com acesso a este recurso podem:
  - Aloque e associe os endereços IP de propriedade do cliente às instâncias.
- Tabelas de rotas de gateway local – Os consumidores com acesso a este recurso podem:
  - Crie e gerencie associações de VPC com um gateway local.
  - Visualizar as configurações das tabelas de rotas de gateway local e das interfaces virtuais.
- Outposts – Os consumidores com acesso a este recurso podem:
  - Criar e gerenciar sub-redes no Outpost.
  - Criar e gerenciar volumes do EBS no Outpost.
  - Usar a API do AWS Outposts para exibir informações sobre o Outpost.
- S3 em Outposts: os consumidores com acesso a esse recurso podem:
  - Criar e gerenciar buckets, pontos de acesso e endpoints do S3 no Outpost.

- Sites – Os consumidores com acesso a este recurso podem:
  - Criar, gerenciar e controlar um Outpost no site.
- Sub-redes: os consumidores com acesso a esse recurso podem:
  - Exibir informações sobre sub-redes.
  - Iniciar e executar instâncias do EC2 em sub-redes.

  Usar o console do Amazon VPC para compartilhar uma sub-rede do Outpost. Para obter mais informações, consulte Compartilhar uma sub-rede no Guia do usuário do Amazon VPC.

Pré-requisitos para compartilhar recursos do Outposts

- Para compartilhar um recurso do Outpost com a sua organização ou com uma unidade organizacional no AWS Organizations, é necessário habilitar o compartilhamento com o AWS Organizations. Para obter mais informações, consulte Habilitar o compartilhamento com o AWS Organizations no Guia do usuário doAWS RAM.
- Para compartilhar um recurso do Outpost, é necessário ser o proprietário dele em sua conta AWS. Não é possível compartilhar um recurso do Outpost que tenha sido compartilhado com você.
- Para compartilhar um recurso do Outpost, você deve compartilhá-lo com uma conta que esteja dentro da sua organização.

Serviços relacionados

O compartilhamento de recursos do Outpost integra-se ao AWS Resource Access Manager (AWS RAM). O AWS RAM é um serviço que permite compartilhar seus recursos do AWS com qualquer conta da AWS ou por meio do AWS Organizations. Com o AWS RAM, você compartilha recursos que possui criando um compartilhamento de recursos. Um compartilhamento de recursos especifica os recursos a serem compartilhados, e os consumidores com os quais compartilhá-los. Os consumidores podem ser contas individuais da AWS, unidades organizacionais ou toda uma organização doAWS Organizations.

Para obter mais informações sobre o AWS RAM, consulte o Guia do usuário do AWS RAM.

Compartilhamento entre zonas de disponibilidade

Para garantir a distribuição de recursos entre as zonas de disponibilidade de uma região, mapeamos as zonas de disponibilidade de forma independente para os nomes de cada conta. Isso pode resultar em diferenças na nomenclatura de zonas de disponibilidade entre contas. Por exemplo, a zona de disponibilidade `us-east-1a` de sua conta da AWS pode não ter o mesmo local que a `us-east-1a` de outra conta da AWS.

Para identificar o local do seu recurso do Outpost relacionado a suas contas, use o ID da zona de disponibilidade (ID da AZ). O AZ ID é um identificador exclusivo e consistente de uma zona de disponibilidade em todas as contas da AWS. Por exemplo, `use1-az1` é um ID de AZ da região `us-east-1` e é o mesmo local em cada conta da AWS.

Para visualizar os IDs de AZs das zonas de disponibilidade em sua conta

1. Abra o console do AWS RAM em https://console.aws.amazon.com/ram.
2. Os IDs de AZs da região atual são exibidos no painel Your AZ ID (Seu ID de AZ) no lado direito da tela.

> **Note**
>
> As tabelas de rotas de gateway local estão na mesma zona de disponibilidade (AZ) do Outpost, portanto, você não precisa especificar uma ID da AZ para as tabelas de rotas.

Compartilhamento de um recurso do Outpost

Quando um proprietário compartilha um Outpost com um consumidor, o consumidor pode criar recursos no Outpost da mesma forma que criaria recursos nos Outposts em sua própria conta. Consumidores com acesso a tabelas de rotas de gateway local compartilhadas podem criar e gerenciar associações da VPC. Para obter mais informações, consulte Recursos compartilháveis do Outpost.

Para compartilhar um recurso do Outpost, é necessário adicioná-lo a um compartilhamento de recursos. Um compartilhamento de recursos é um recurso do AWS RAM que permite que você compartilhe seus recursos entre contas da AWS. Um compartilhamento de recursos especifica os recursos a serem compartilhados, e os consumidores com os quais compartilhá-los. Ao compartilhar

um recurso do Outpost usando o console do AWS Outposts, você o adiciona a um compartilhamento de recursos existente. Para adicionar o recurso do Outpost a um novo compartilhamento de recursos, você deve primeiro criar o compartilhamento de recursos usando o console do AWS RAM.

Se você fizer parte de uma organização no AWS Organizations e o compartilhamento estiver habilitado na organização, será possível conceder aos consumidores da organização o acesso a partir do console do AWS RAM para o recurso do Outpost compartilhado. Caso contrário, os consumidores receberão um convite para participar do compartilhamento de recursos e terão acesso ao recurso do Outpost compartilhado após aceitar o convite.

É possível compartilhar um recurso do Outpost de sua propriedade usando o console do AWS Outposts, o console do AWS RAM ou o AWS CLI.

Compartilhar um Outpost de sua propriedade usando o console do AWS Outposts

1. Abra o console do AWS Outposts em https://console.aws.amazon.com/outposts/.
2. No painel de navegação, escolha Outposts.
3. Selecione o Outpost e, em seguida, escolha Ações, Visualizar detalhes.
4. Na página Resumo do Outpost, escolha Compartilhamentos de recursos.
5. Escolha Criar compartilhamento de recursos.

Você será redirecionado para o console do AWS RAM para concluir o compartilhamento do Outpost conforme o procedimento a seguir. Para compartilhar uma tabela de rotas de gateway local de sua propriedade, siga o mesmo também.

Para compartilhar um Outpost ou uma tabela de rotas de gateway local de sua propriedade usando o console do AWS RAM

Consulte Criar um compartilhamento de recursos no Guia do usuárioAWS RAM.

Para compartilhar uma tabela de rotas de Outpost ou gateway local que você possui usando o AWS CLI

Use o comando create-resource-share.

Cancelamento do compartilhamento de um recurso compartilhado do Outpost

Quando o compartilhamento de um Outpost é cancelado, os consumidores não podem mais ver o Outpost no console do AWS Outposts. Eles não podem criar novas sub-redes no Outpost, criar novos volumes do EBS no Outpost nem visualizar os detalhes do Outpost e os tipos de instância usando o console do AWS Outposts ou a AWS CLI. As sub-redes, os volumes ou as instâncias existentes criados pelos consumidores não são excluídos. Qualquer sub-rede existente criada pelos consumidores no Outpost ainda pode ser usada para executar novas instâncias.

Quando o compartilhamento de uma tabela de rotas de gateway local é cancelado, os consumidores não podem mais criar novas associações da VPC a ela. Todas as associações da VPC existentes criadas pelos consumidores permanecem associadas à tabela de rotas. Os recursos nessas VPCs podem continuar direcionando o tráfego para o gateway local.

Para cancelar o compartilhamento de um recurso do Outpost compartilhado, é necessário removê-lo do compartilhamento de recursos. É possível fazer isso usando o console do AWS RAM ou a AWS CLI.

Para cancelar o compartilhamento de um recurso compartilhado do Outpost de sua propriedade usando o console do AWS RAM

Consulte Atualização de um compartilhamento de recursos no Guia do usuário do AWS RAM.

Para cancelar o compartilhamento de um recurso compartilhado do Outpost de sua propriedade usando o AWS CLI

Use o comando disassociate-resource-share.

Identificando um recurso compartilhado do Outpost

Os proprietários e consumidores podem identificar Outposts compartilhados usando o console do AWS Outposts e AWS CLI. Eles podem identificar tabelas de rotas de gateway local usando a AWS CLI.

Como identificar um Outpost compartilhado usando o console do AWS Outposts

1. Abra o console do AWS Outposts em https://console.aws.amazon.com/outposts/.

2. No painel de navegação, escolha Outposts.
3. Selecione o Outpost e, em seguida, escolha Ações, Visualizar detalhes.
4. Na página Resumo do Outpost, veja a ID do proprietário para identificar a ID da conta da AWS do proprietário do Outpost.

Identificar um recurso do Outpost compartilhado usando o AWS CLI

Use os comandos list-outposts e describe-local-gateway-route-tables. Esses comandos retornam os recursos do Outpost de sua propriedade e recursos do Outpost compartilhados com você. O `OwnerId` mostra o ID da conta da AWS do proprietário do recurso do Outpost.

Permissões de recursos do Outpost compartilhadas

Permissões para proprietários

Os proprietários são responsáveis por gerenciar o Outpost e pelos recursos que eles criam nele. Os proprietários podem alterar ou revogar o acesso compartilhado a qualquer momento. Eles podem usar o AWS Organizations para visualizar, modificar e excluir recursos criados pelos consumidores em Outposts compartilhados.

Permissões para consumidores

Os consumidores podem criar recursos nos Outposts que são compartilhados com eles da mesma maneira que elaborariam recursos nos Outposts criados nas próprias contas. Os consumidores são responsáveis por gerenciar os recursos que executam em Outposts compartilhados com eles. Os consumidores não podem visualizar ou modificar recursos de propriedade de outros consumidores ou do proprietário do Outpost, e não podem modificar os Outposts que são compartilhados com eles.

Faturamento e medição

Os proprietários são cobrados por Outposts e pelos recursos do Outpost que compartilham. Eles também são cobrados por eventuais taxas de transferência de dados associadas ao tráfego da VPN do link de serviço do Outpost da AWS Region.

Não há custos adicionais pelo compartilhamento de tabelas de rotas de gateway local. Para sub-redes compartilhadas, o proprietário da VPC é cobrado pelos recursos no nível da VPC, como conexões VPN e de AWS Direct Connect, gateways NAT e conexões de link privado.

Os consumidores são cobrados pelos recursos de aplicativos que criam em Outposts compartilhados, como balanceadores de carga e bancos de dados do Amazon RDS. Os consumidores também são cobrados pelas transferências de dados cobráveis da Região AWS.

Limitações

As limitações a seguir se aplicam ao compartilhamento de AWS Outposts:

- As limitações das sub-redes compartilhadas se aplicam ao trabalho com compartilhamento do AWS Outposts. Para obter mais informações sobre os limites de compartilhamento de VPC, consulte Limitações no Guia do usuário do Amazon Virtual Private Cloud.
- As cotas de serviços são aplicadas por conta individual.

Segurança em AWS Outposts

A segurança AWS é a maior prioridade. Como AWS cliente, você se beneficia de uma arquitetura de data center e rede criada para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isso como a segurança da nuvem e a segurança na nuvem:

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços na AWS nuvem. AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados testam e verificam regularmente a eficácia de nossa segurança como parte dos Programas de Conformidade Programas de AWS de . Para saber mais sobre os programas de conformidade aplicáveis AWS Outposts, consulte AWS Serviços no escopo do programa de conformidade AWS .
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Para obter mais informações sobre segurança e conformidade para AWS Outposts, consulte as perguntas frequentes sobre de AWS Outposts rack.

Esta documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar AWS Outposts. Ela mostra como atender aos objetivos de segurança e conformidade. Você também aprenderá a usar outros AWS serviços que ajudam a monitorar e proteger seus recursos.

Conteúdo

Proteção de dados em AWS Outposts

O modelo de responsabilidade AWS compartilhada modelo se aplica à proteção de dados em AWS Outposts. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Esse conteúdo inclui as tarefas de configuração e gerenciamento de segurança do Serviços da AWS que você usa.

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho.

Para obter mais informações sobre a privacidade de dados, consulte as Perguntas frequentes sobre privacidade de dados. Para mais informações sobre a proteção de dados na Europa, consulte o artigo AWS Shared Responsibility Model and GDPR no Blog de segurança da AWS .

Criptografia inativa

Com isso AWS Outposts, todos os dados são criptografados em repouso. O material de chaves é embalado em uma chave externa armazenada em um dispositivo removível, a Chave de Segurança Nitro (NSK). A NSK é necessário para descriptografar os dados em seus servidores.

Você pode usar a criptografia do Amazon EBS para volumes do EBS e snapshots. A criptografia do Amazon EBS usa AWS Key Management Service (AWS KMS) e chaves KMS. Para obter mais informações, consulte Criptografia do Amazon EBS no Guia do usuário do Amazon EC2.

Criptografia em trânsito

AWS criptografa dados em trânsito entre seu Posto Avançado e sua região. AWS Para ter mais informações, consulte Conectividade por meio de links de serviço.

Você pode usar um protocolo de criptografia, como o Transport Layer Security (TLS), para criptografar dados sigilosos em trânsito pelo gateway local para sua rede local.

Exclusão de dados

Quando você interrompe ou encerra uma instância EC2, a memória alocada para ela é apagada (definida como zero) pelo hipervisor antes que ela seja alocada para uma nova instância, e cada bloco de armazenamento é redefinido.

Destruir a Chave de Segurança Nitro destrói criptograficamente os dados em seu Outpost.

Gerenciamento de identidade e acesso (IAM) para AWS Outposts

AWS Identity and Access Management (IAM) é um AWS serviço que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) a usar AWS Outposts os recursos. Você pode usar o IAM sem custo adicional.

Conteúdo

Como o AWS Outposts funciona com o IAM

Antes de usar o IAM para gerenciar o acesso aos AWS Outposts, saiba quais recursos do IAM estão disponíveis para uso com o AWS Outposts.

Recursos do IAM que você pode usar com AWS Outposts

Recurso do IAM	AWS Suporte para Outposts
Políticas baseadas em identidade	Sim
Políticas baseadas em recurso	Não
Ações de políticas	Sim
Recursos de políticas	Sim
Chaves de condição de política (específicas do serviço)	Sim
ACLs	Não
ABAC (tags em políticas)	Sim

Recurso do IAM	AWS Suporte para Outposts
Credenciais temporárias	Sim
Permissões de entidade principal	Sim
Perfis de serviço	Não
Funções vinculadas ao serviço	Sim

Políticas baseadas em identidade para Outposts AWS

É compatível com políticas baseadas em identidade	Sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criar políticas do IAM no Guia do usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou recursos permitidos ou negados, bem como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou função à qual ela está anexada. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elementos da política JSON do IAM no Guia do Usuário do IAM.

Exemplos de políticas baseadas em identidade para Outposts AWS

Para ver exemplos de políticas baseadas em identidade do AWS Outposts, consulte. AWS Exemplos de políticas de Outposts

Políticas baseadas em recursos em Outposts AWS

Oferece suporte a políticas baseadas em recurso	Não

Políticas baseadas em recurso são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recurso as políticas de confiança de função do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recurso, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações uma entidade principal especificada pode executar nesse recurso e em que condições. Você precisa especificar uma entidade principal em uma política baseada em recurso. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Para permitir o acesso entre contas, você pode especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em recurso. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando o principal e o recurso são diferentes Contas da AWS, um administrador do IAM na conta confiável também deve conceder permissão à entidade principal (usuário ou função) para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso conceder acesso a uma entidade principal na mesma conta, nenhuma outra política baseada em identidade será necessária. Para obter mais informações, consulte Como os perfis do IAM diferem de políticas baseadas em recursos no Guia do usuário do IAM.

Ações políticas para AWS Outposts

Oferece suporte a ações de políticas	Sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Action` de uma política JSON descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da operação de AWS API associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Há também algumas operações que exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista de ações do AWS Outposts, consulte Ações definidas por AWS Outposts na Referência de Autorização de Serviço.

As ações políticas em AWS Outposts usam o seguinte prefixo antes da ação:

```
outposts
```

Para especificar várias ações em uma única instrução, separe-as com vírgulas.

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

Você também pode especificar várias ações usando caracteres-curinga (*). Por exemplo, para especificar todas as ações que começam com a palavra `List`, inclua a seguinte ação:

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

Recursos políticos para AWS Outposts

Oferece suporte a recursos de políticas	Sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento de política `Resource` JSON especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou um elemento `NotResource`. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Isso pode ser feito para ações que oferecem suporte a um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem suporte a permissões em nível de recurso, como operações de listagem, use um caractere curinga (*) para indicar que a instrução se aplica a todos os recursos.

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

Algumas ações da API AWS Outposts oferecem suporte a vários recursos. Para especificar vários recursos em uma única instrução, separe os ARNs com vírgulas.

```
"Resource": [
```

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

Para ver uma lista dos tipos de recursos do AWS Outposts e seus ARNs, consulte Tipos de recursos definidos AWS Outposts na Referência de Autorização de Serviço. Para saber com quais ações é possível especificar o ARN de cada atributo, consulte Ações definidas pelo AWS Outposts.

Chaves de condição de política para AWS Outposts

Compatível com chaves de condição de política específicas do serviço	Sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Condition` (ou bloco de `Condition`) permite que você especifique condições nas quais uma instrução está em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usam atendentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos `Condition` em uma instrução ou várias chaves em um único elemento `Condition`, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, AWS avalia a condição usando uma `OR` operação lógica. Todas as condições devem ser atendidas para que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar as condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um recurso somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte Elementos de política do IAM: variáveis e tags no Guia do usuário do IAM.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia do usuário do IAM.

Para ver uma lista das chaves de condição do AWS Outposts, consulte Chaves de condição AWS Outposts na Referência de Autorização de Serviço. Para saber com quais ações e recursos você pode usar uma chave de condição, consulte Ações definidas por AWS Outposts.

Para ver exemplos de políticas baseadas em identidade do AWS Outposts, consulte. AWS Exemplos de políticas de Outposts

ACLs em Outposts AWS

Oferece suporte a ACLs	Não

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes às políticas baseadas em recurso, embora não usem o formato de documento de política JSON.

ABAC com Outposts AWS

Oferece suporte a ABAC (tags em políticas)	Sim

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define permissões com base em atributos. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a entidades do IAM (usuários ou funções) e a vários AWS recursos. A marcação de entidades e recursos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso que ela está tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações em que o gerenciamento de políticas se torna um problema.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* ou `aws:TagKeys` chaves de condição.

Se um serviço oferecer suporte às três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço oferecer suporte às três chaves de condição somente para alguns tipos de recursos, o valor será Parcial.

Para obter mais informações sobre o ABAC, consulte O que é ABAC? no Guia do usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Usar controle de acesso baseado em atributos (ABAC) no Guia do usuário do IAM.

Usando credenciais temporárias com Outposts AWS

Oferece suporte a credenciais temporárias	Sim

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS “Trabalhe com o IAM” no Guia do usuário do IAM.

Você está usando credenciais temporárias se fizer login AWS Management Console usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa AWS usando o link de login único (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre como alternar perfis, consulte Alternar para uma função (console) no Guia do usuário do IAM.

Você pode criar manualmente credenciais temporárias usando a AWS API AWS CLI ou. Em seguida, você pode usar essas credenciais temporárias para acessar AWS. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para obter mais informações, consulte Credenciais de segurança temporárias no IAM.

Permissões principais entre serviços para Outposts AWS

Suporte para o recurso Encaminhamento de sessões de acesso (FAS)	Sim

Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.

Funções de serviço para o Outposts AWS

Oferece suporte a perfis de serviço	Não

O perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar uma função para delegar permissões a um AWS service (Serviço da AWS) no Guia do usuário do IAM.

Funções vinculadas a serviços para Outposts AWS

Oferece suporte a funções vinculadas ao serviço	Sim

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode assumir o perfil para executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode exibir, mas não pode editar as permissões para perfis vinculados ao serviço.

Para obter detalhes sobre como criar ou gerenciar funções vinculadas ao serviço do AWS Outposts, consulte. Usar perfis vinculados a serviço do AWS Outposts

AWS Exemplos de políticas de Outposts

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos do AWS Outposts. Eles também não podem realizar tarefas usando a AWS API AWS Management Console, AWS Command Line Interface (AWS CLI) ou. Para conceder aos usuários permissões para executar ações nos recursos de que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis, e os usuários podem assumir os perfis.

Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documento de política JSON, consulte Criação de políticas do IAM no Guia do Usuário do IAM.

Para obter detalhes sobre ações e tipos de recursos definidos pelo AWS Outposts, incluindo o formato dos ARNs para cada um dos tipos de recursos, consulte Ações, recursos e chaves de condição AWS Outposts na Referência de Autorização de Serviço.

Conteúdo

Práticas recomendadas de políticas

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos do AWS Outposts em sua conta. Essas ações podem incorrer em custos para a Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para obter mais informações, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para perfis de trabalho no Guia do usuário do IAM.
- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso: você pode adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, você pode escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como AWS CloudFormation. Para obter mais informações, consulte Elementos de política JSON do IAM: Condition no Guia do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access

Analyzer oferece mais de cem verificações de política e recomendações acionáveis para ajudar você a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação de políticas do IAM Access Analyzer no Guia do usuário do IAM.

- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS a MFA para obter segurança adicional. Para exigir a MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte Configuração de acesso à API protegido por MFA no Guia do usuário do IAM.

Para obter mais informações sobre as práticas recomendadas do IAM, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

Exemplo: Concessão de permissões em nível de recurso

O exemplo a seguir usa permissões em nível de recurso para conceder permissão para obter informações sobre o Outpost especificado.

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

O exemplo a seguir usa permissões em nível de recurso para conceder permissão para obter informações sobre o site especificado.

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

```
}
```

Usar perfis vinculados a serviço do AWS Outposts

AWS Outposts usa funções vinculadas ao serviço AWS Identity and Access Management (IAM). Uma função vinculada ao serviço é um tipo exclusivo de função do IAM vinculada diretamente a. AWS Outposts As funções vinculadas ao serviço são predefinidas AWS Outposts e incluem todas as permissões que o serviço exige para chamar outros AWS serviços em seu nome.

Uma função vinculada ao serviço torna sua configuração AWS Outposts mais eficiente, pois você não precisa adicionar manualmente as permissões necessárias. AWS Outposts define as permissões de suas funções vinculadas ao serviço e, a menos que seja definido de outra forma, só AWS Outposts pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões, que não pode ser anexada a nenhuma outra entidade do IAM.

Você pode excluir um perfil vinculado ao serviço somente depois de excluir os atributos relacionados. Isso protege seus AWS Outposts recursos porque você não pode remover inadvertidamente a permissão para acessar os recursos.

Para obter informações sobre outros serviços compatíveis com funções vinculadas a serviços, consulte Serviços da AWS compatíveis com o IAM e procure os serviços que contenham Sim na coluna Função vinculada a serviço. Escolha Sim com um link para visualizar a documentação da função vinculada a esse serviço.

Permissões de função vinculada ao serviço AWS Outposts

AWS Outposts usa a função vinculada ao serviço chamada AWSServiceRoleForOutposts_ ***OutpostID*** — Permite que Outposts AWS acessem recursos para conectividade privada em seu nome. Essa função vinculada ao serviço permite a configuração de conectividade privada, cria interfaces de rede e anexa-as às instâncias de endpoint do link de serviço.

A função vinculada ao serviço AWSServiceRoleForOutposts _ *OutPostID* confia nos seguintes serviços para assumir a função:

- `outposts.amazonaws.com`

A função vinculada ao serviço AWSServiceRoleForOutposts_ ***OutPostID*** inclui as seguintes políticas:

- AWSOutpostsServiceRolePolicy

- AWSOutpostsPrivateConnectivityPolicy_ ID do Posto ***Avançado***

A AWSOutpostsServiceRolePolicypolítica é uma política de função vinculada a serviços para permitir o acesso aos AWS recursos gerenciados pelo. AWS Outposts

Essa política permite AWS Outposts concluir as seguintes ações nos recursos especificados:

- Ação: `ec2:DescribeNetworkInterfaces` em `all AWS resources`
- Ação: `ec2:DescribeSecurityGroups` em `all AWS resources`
- Ação: `ec2:CreateSecurityGroup` em `all AWS resources`
- Ação: `ec2:CreateNetworkInterface` em `all AWS resources`

A política AWSOutpostsPrivateConnectivityPolicy_ ***OutPostID*** permite concluir AWS Outposts as seguintes ações nos recursos especificados:

- Ação: `ec2:AuthorizeSecurityGroupIngress` em `all AWS resources that match the following Condition:`

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

- Ação: `ec2:AuthorizeSecurityGroupEgress` em `all AWS resources that match the following Condition:`

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

- Ação: `ec2:CreateNetworkInterfacePermission` em `all AWS resources that match the following Condition:`

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

- Ação: `ec2:CreateTags` em `all AWS resources that match the following Condition:`

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

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua um perfil vinculado ao serviço. Para obter mais informações, consulte Permissões de Função Vinculadas ao Serviço no Guia do Usuário do IAM.

Crie uma função vinculada ao serviço para o AWS Outposts

Não é necessário criar manualmente um perfil vinculado ao serviço. Quando você configura a conectividade privada para seu Outpost no AWS Management Console, AWS Outposts cria a função vinculada ao serviço para você.

Para ter mais informações, consulte Conectividade privada do link de serviço usando VPC.

Editar uma função vinculada ao serviço para o AWS Outposts

AWS Outposts não permite que você edite a função vinculada ao AWSServiceRoleForOutposts serviço _ *`OutpostID.`* Depois que criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ele. No entanto, será possível editar a descrição da função usando o IAM. Para obter mais informações, consulte Editar um perfil vinculado ao serviço no Guia do usuário do IAM.

Excluir uma função vinculada ao serviço para o AWS Outposts

Se você não precisar mais usar um recurso ou um serviço que requer uma função vinculada ao serviço, é recomendável excluí-la. Dessa forma, você evita ter uma entidade não utilizada que não seja monitorada ou mantida ativamente. No entanto, você deve limpar os atributos de seu perfil vinculado ao serviço antes de excluí-lo manualmente.

> **Note**
>
> Se o AWS Outposts serviço estiver usando a função quando você tentar excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

> **Warning**
>
> Você deve excluir seu Outpost antes de excluir a função vinculada ao serviço AWSServiceRoleForOutposts _ *`OutpostID`*. O procedimento a seguir exclui seu Outpost.

Antes de começar, certifique-se de que seu Outpost não esteja sendo compartilhado usando AWS Resource Access Manager (AWS RAM). Para ter mais informações, consulte Cancelamento do compartilhamento de um recurso compartilhado do Outpost.

Para excluir AWS Outposts recursos usados pelo AWSServiceRoleForOutposts _ ***OutPostID***

- Entre em contato com o AWS Enterprise Support para excluir seu Outpost.

Como excluir manualmente o perfil vinculado ao serviço usando o IAM

Use o console do IAM AWS CLI, o ou a AWS API para excluir a função vinculada ao AWSServiceRoleForOutposts serviço _ ***outPostID.*** Para obter mais informações, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

Regiões suportadas por funções vinculadas ao serviço do AWS Outposts

AWS Outposts suporta o uso de funções vinculadas ao serviço em todas as regiões em que o serviço está disponível. Para obter mais informações, consulte AWS Outposts Endpoints e cotas.

AWS políticas gerenciadas para AWS Outposts

Uma política AWS gerenciada é uma política autônoma criada e administrada por AWS. AWS as políticas gerenciadas são projetadas para fornecer permissões para muitos casos de uso comuns, para que você possa começar a atribuir permissões a usuários, grupos e funções.

Lembre-se de que as políticas AWS gerenciadas podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque elas estão disponíveis para uso de todos os AWS clientes. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente específicas para seus casos de uso.

Você não pode alterar as permissões definidas nas políticas AWS gerenciadas. Se AWS atualizar as permissões definidas em uma política AWS gerenciada, a atualização afetará todas as identidades principais (usuários, grupos e funções) às quais a política está anexada. AWS é mais provável que atualize uma política AWS gerenciada quando uma nova AWS service (Serviço da AWS) é lançada ou novas operações de API são disponibilizadas para serviços existentes.

Para obter mais informações, consulte AWS Políticas gerenciadas pela no Guia do usuário do IAM.

AWS política gerenciada: AWSOutpostsServiceRolePolicy

Essa política está vinculada a uma função vinculada ao serviço que permite AWS Outposts realizar ações em seu nome. Para ter mais informações, consulte Usar perfis vinculados a serviço.

AWS política gerenciada: AWSOutpostsPrivateConnectivityPolicy

Essa política está vinculada a uma função vinculada ao serviço que permite AWS Outposts realizar ações em seu nome. Para ter mais informações, consulte Usar perfis vinculados a serviço.

AWS Outposts atualizações nas políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas AWS Outposts desde que esse serviço começou a rastrear essas alterações.

Alteração	Descrição	Data
AWS Outposts começou a rastrear alterações	AWS Outposts começou a rastrear as mudanças em suas políticas AWS gerenciad as.	03 de dezembro de 2019

Segurança da infraestrutura em AWS Outposts

Como um serviço gerenciado, o AWS Outposts é protegido pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura, consulte AWS Cloud Security. Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte Proteção de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar AWS Outposts pela rede. Os clientes precisam oferecer suporte para:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com sigilo de encaminhamento perfeito (perfect forward secrecy, ou PFS) como DHE (Ephemeral Diffie-Hellman, ou Efêmero Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman, ou Curva elíptica efêmera Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas utilizando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou é possível usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Para obter mais informações sobre a segurança da infraestrutura fornecida para as instâncias do EC2 e os volumes do EBS em execução no seu Outpost, consulte Segurança da infraestrutura no Amazon EC2.

Os registros de fluxo de VPC funcionam da mesma forma que em uma AWS região. Isso significa que eles podem ser publicados na CloudWatch Logs, no Amazon S3 ou na Amazon GuardDuty para análise. Os dados precisam ser enviados de volta à Região para publicação nesses serviços, para que não sejam visíveis de CloudWatch ou de outros serviços quando o Posto Avançado estiver em um estado desconectado.

Monitoramento de adulteração em equipamentos AWS Outposts

Certifique-se de que ninguém modifique, altere, faça engenharia reversa ou adultere o equipamento. AWS Outposts AWS Outposts o equipamento pode ser equipado com monitoramento de adulteração para garantir a conformidade com os Termos AWS de Serviço.

Resiliência em AWS Outposts

AWS Outposts foi projetado para ser altamente disponível. Os racks do Outpost são projetados com potência redundante e equipamentos de rede. Para obter resiliência adicional, recomendamos que você forneça fontes de alimentação duplas e conectividade da rede redundante para seu Outpost.

Para alta disponibilidade, você pode provisionar capacidade adicional integrada e sempre ativa no rack do Outposts. As configurações de capacidade do Outpost foram projetadas para operar em ambientes de produção e oferecer suporte a instâncias N+1 para cada família de instâncias quando você provisiona a capacidade para isso. A AWS recomenda que você aloque capacidade adicional suficiente para suas aplicações essenciais à missão a fim de permitir recuperação e failover se houver um problema de host subjacente. Você pode usar as métricas de disponibilidade de CloudWatch capacidade da Amazon e definir alarmes para monitorar a integridade de seus aplicativos, criar CloudWatch ações para configurar opções de recuperação automática e monitorar a utilização da capacidade de seus Outposts ao longo do tempo.

Ao criar um Posto Avançado, você seleciona uma Zona de Disponibilidade de uma AWS Região. Essa zona de disponibilidade oferece suporte a operações do plano de controle, como responder

a chamadas de API, além de monitorar e atualizar o Outpost. Para se beneficiar da resiliência fornecida pelas zonas de disponibilidade, você pode implantar aplicativos em vários Outposts, cada um deles conectado a uma zona de disponibilidade diferente. Isso permite que você crie resiliência adicional de aplicativos e evite a dependência de uma zona de disponibilidade única. Para obter mais informações sobre regiões e zonas de disponibilidade, consulte AWS Infraestrutura global.

Você pode usar um grupo de posicionamento com uma estratégia de disseminação para garantir que as instâncias sejam posicionadas em racks distintos do Outposts. Isso pode ajudar a reduzir falhas correlacionadas. Para ter mais informações, consulte Grupos de posicionamento em Outposts.

Você pode executar instâncias no Outposts usando o Amazon EC2 Auto Scaling e criar um Application Load Balancer para distribuir o tráfego entre as instâncias. Para obter mais informações, consulte Configurar um Application Load Balancer no AWS Outposts.

Validação de conformidade para AWS Outposts

Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas de conformidade específicos, consulte Serviços da AWS Escopo por Programa de Conformidade Serviços da AWS e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de AWS conformidade Programas AWS de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Baixar relatórios em AWS Artifact .

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- Guias de início rápido sobre segurança e conformidade — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos AWS focados em segurança e conformidade.
- Arquitetura para segurança e conformidade com a HIPAA na Amazon Web Services — Este whitepaper descreve como as empresas podem usar AWS para criar aplicativos qualificados para a HIPAA.

> **Note**
>
> Nem todos Serviços da AWS são elegíveis para a HIPAA. Para obter mais informações, consulte a Referência dos serviços qualificados pela HIPAA.

- AWS Recursos de https://aws.amazon.com/compliance/resources/ de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- AWS Guias de conformidade do cliente — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- Avaliação de recursos com regras no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- AWS Security Hub— Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os recursos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.
- AWS Audit Manager— Isso AWS service (Serviço da AWS) ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

Acesso à Internet para AWS Outposts cargas de trabalho

Esta seção explica como AWS Outposts as cargas de trabalho podem acessar a Internet das seguintes formas:

- Por meio da AWS região mãe
- Por meio da rede do seu data center local

Acesso à Internet através da AWS região principal

Nessa opção, as cargas de trabalho nos Outposts acessam a Internet por meio do link de serviço e, em seguida, pelo gateway de Internet (IGW) na região principal. AWS O tráfego de saída para a Internet pode ser feito por meio do gateway NAT instanciado em sua VPC. Para obter segurança adicional para seu tráfego de entrada e saída, você pode usar serviços AWS de segurança como AWS WAF, AWS Shield, e Amazon CloudFront na AWS região.

Para a configuração da tabela de rotas na sub-rede Outposts, consulte Tabelas de rotas do gateway local.

Considerações

- Use essa opção quando:
  - Você precisa de flexibilidade para proteger o tráfego da Internet com vários AWS serviços na AWS região.
  - Você não tem um ponto de presença na Internet em seu data center ou instalação de co-localização.
- Nessa opção, o tráfego deve atravessar a AWS região principal, o que introduz latência.
- Semelhante às cobranças de transferência de dados nas AWS regiões, a transferência de dados da Zona de Disponibilidade principal para o Posto Avançado incorre em cobranças. Para saber mais sobre transferência de dados, consulte Amazon EC2 On-Demand Pricing.
- A utilização da largura de banda do link de serviço aumentará.

A imagem a seguir mostra o tráfego entre a carga de trabalho na instância Outposts e a Internet passando pela AWS região principal.

Acesso à Internet por meio da rede do seu data center local

Nessa opção, as cargas de trabalho que residem nos Outposts acessam a Internet por meio de seu data center local. O tráfego da carga de trabalho que acessa a Internet atravessa seu ponto de presença na Internet local e sai localmente. A camada de segurança da rede do seu data center local é responsável por proteger o tráfego da carga de trabalho do Outposts.

Para a configuração da tabela de rotas na sub-rede Outposts, consulte Tabelas de rotas do gateway local.

Considerações

- Use essa opção quando:
  - Suas cargas de trabalho exigem acesso de baixa latência aos serviços da Internet.
  - Você prefere evitar cobranças de transferência de dados para fora (DTO).
  - Você deseja preservar a largura de banda do link de serviço para controlar o tráfego do plano.
- Sua camada de segurança é responsável por proteger o tráfego da carga de trabalho do Outposts.
- Se você optar pelo Direct VPC Routing (DVR), deverá garantir que os CIDRs do Outposts não entrem em conflito com os CIDRs locais.
- Se a rota padrão (0/0) for propagada pelo gateway local (LGW), talvez as instâncias não consigam chegar aos endpoints do serviço. Como alternativa, você pode escolher VPC endpoints para alcançar o serviço desejado.

A imagem a seguir mostra o tráfego entre a carga de trabalho na instância Outposts e a Internet passando pelo seu data center local.

Monitore seu Outpost

O AWS Outposts se integra aos seguintes serviços que oferecem recursos de monitoramento e de logs:

CloudWatch métricas

Use CloudWatch a Amazon para recuperar estatísticas sobre pontos de dados para seus Outposts como um conjunto ordenado de dados de séries temporais, conhecido como métricas. Você pode usar essas métricas para verificar se o sistema está executando conforme o esperado. Para ter mais informações, consulte CloudWatch métricas para AWS Outposts.

CloudTrail troncos

Use o AWS CloudTrail para capturar informações detalhadas sobre as chamadas feitas para APIs do AWS. Você pode armazenar essas chamadas como arquivos de log no Amazon S3. Você pode usar esses CloudTrail registros para determinar informações como qual chamada foi feita, o endereço IP de origem de onde veio a chamada, quem fez a chamada e quando a chamada foi feita.

Os CloudTrail registros contêm informações sobre as chamadas para ações de API paraAWS Outposts. Eles também contêm informações para chamadas para ações de API de serviços em um Outpost, como Amazon EC2 e Amazon EBS. Para ter mais informações, consulte AWS Outpostsinformações em CloudTrail.

Logs de fluxo da VPC

Você pode usar os logs de fluxo da VPC para capturar informações detalhadas sobre o tráfego de entrada e saída do seu Outpost e no seu Outpost. Para obter mais informações, consulte Logs de fluxo da VPC no Guia do usuário do Amazon Virtual Private Cloud.

Traffic Mirroring (Espelhamento de tráfego)

Use o espelhamento de tráfego para copiar e encaminhar o tráfego de rede do Outpost para dispositivos out-of-band de segurança e monitoramento no Outpost. Você pode usar o tráfego espelhado para inspeção de conteúdo, monitoramento de ameaças ou solução de problemas. Para obter mais informações, consulte o Guia de espelhamento de tráfego para a Amazon Virtual Private Cloud.

AWS Health Dashboard

O AWS Health Dashboard exibe informações e também fornece notificações que são invocadas por alterações no funcionamento dos recursos da AWS. As informações são apresentadas de duas formas: em um painel que mostra eventos recentes e futuros organizados por categoria e em um log de eventos completo que mostra todos os eventos dos últimos 90 dias. Por exemplo, um problema de conectividade no link de serviço iniciaria um evento que apareceria no painel e no log de eventos e permaneceria no log de eventos por 90 dias. Uma parte do serviço AWS Health, AWS Health Dashboard não requer configuração e pode ser visualizado por qualquer usuário autenticado na sua conta. Para obter mais informações, consulte Conceitos básicos do AWS Health Dashboard.

CloudWatch métricas para AWS Outposts

AWS Outpostspublica pontos de dados na Amazon CloudWatch para seus Outposts. CloudWatch permite que você recupere estatísticas sobre esses pontos de dados como um conjunto ordenado de dados de séries temporais, conhecido como métricas. Considere uma métrica como uma variável a ser monitorada, e os pontos de dados como os valores dessa variável ao longo do tempo. Por exemplo, você pode monitorar a capacidade da instância disponível para seu Outpost durante um tempo especificado. Cada ponto de dados tem um time stamp associado e uma unidade de medida opcional.

Você pode usar métricas para verificar se o sistema está executando conforme o esperado. Por exemplo, você pode criar um CloudWatch alarme para monitorar a `ConnectedStatus` métrica. Se a métrica média for menor que1, CloudWatch pode iniciar uma ação, como enviar uma notificação para um endereço de e-mail. Em seguida, você pode investigar possíveis problemas de rede on-premises ou de uplink que possam afetar as operações do seu Outpost. Os problemas comuns incluem mudanças recentes na configuração da rede on-premises nas regras de firewall e NAT ou problemas de conexão com a Internet. Em caso de problemas de `ConnectedStatus`, recomendamos verificar a conectividade com a região AWS de dentro da sua rede on-premises e entrar em contato com o suporte da AWS se o problema persistir.

Para obter mais informações sobre a criação de um CloudWatch alarme, consulte Usando CloudWatch alarmes da Amazon no Guia do CloudWatch usuário da Amazon. Para obter mais informações sobre CloudWatch, consulte o Guia CloudWatch do usuário da Amazon.

Conteúdo

- Dimensões de métrica do Outpost
- Veja CloudWatch as métricas do seu posto avançado

Métricas do Outpost

O namespace `AWS/Outposts` inclui as métricas a seguir.

`ConnectedStatus`

O status da conexão do link de serviço de um Outpost. Se a estatística média for menor que `1`, a conexão ficará prejudicada.

Unidade: Contagem

Resolução máxima: 1 minuto

Estatísticas: a estatística mais útil é `Average`.

Dimensões: `OutpostId`

`CapacityExceptions`

O número de erros de capacidade insuficiente para execução de instância.

Unidade: Contagem

Resolução máxima: 5 minutos

Estatísticas: as estatísticas mais úteis são `Maximum` e `Minimum`.

Dimensões: `InstanceType` e `OutpostId`

`IfTrafficIn`

A taxa de bits dos dados que as Outposts Virtual Interfaces (VIFs) recebem dos dispositivos de rede local conectados.

Unidade: bits por segundo

Resolução máxima: 5 minutos

Estatísticas: as estatísticas mais úteis são `Max` e `Min`.

Dimensões para VIFs de gateway local (lgw-vif):, e `OutpostsId` `VirtualInterfaceGroupId` `VirtualInterfaceId`

Dimensões dos VIFs do link de serviço (sl-vif): e `OutpostsId` `VirtualInterfaceId`

`IfTrafficOut`

A taxa de bits dos dados que as Outposts Virtual Interfaces (VIFs) transferem para os dispositivos de rede local conectados.

Unidade: bits por segundo

Resolução máxima: 5 minutos

Estatísticas: as estatísticas mais úteis são `Max` e `Min`.

Dimensões para VIFs de gateway local (lgw-vif):, e `OutpostsId` `VirtualInterfaceGroupId` `VirtualInterfaceId`

Dimensões dos VIFs do link de serviço (sl-vif): e `OutpostsId` `VirtualInterfaceId`

`InstanceFamilyCapacityAvailability`

A porcentagem da capacidade da instância disponível. Essa métrica não inclui a capacidade de nenhum host dedicado configurado no Outpost.

Unidade: percentual

Resolução máxima: 5 minutos

Estatística: as estatísticas mais úteis são `Average` e `pNN.NN` (percentis).

Dimensões: `InstanceFamily` e `OutpostId`

`InstanceFamilyCapacityUtilization`

A porcentagem da capacidade da instância em uso. Essa métrica não inclui a capacidade de nenhum host dedicado configurado no Outpost.

Unidade: percentual

Resolução máxima: 5 minutos

Estatística: as estatísticas mais úteis são `Average` e `pNN.NN` (percentis).

Dimensões: `Account`, `InstanceFamily` e `OutpostId`

`InstanceTypeCapacityAvailability`

A porcentagem da capacidade da instância disponível. Essa métrica não inclui a capacidade de nenhum host dedicado configurado no Outpost.

Unidade: percentual

Resolução máxima: 5 minutos

Estatística: as estatísticas mais úteis são `Average` e `pNN.NN` (percentis).

Dimensões: `InstanceType` e `OutpostId`

`InstanceTypeCapacityUtilization`

A porcentagem da capacidade da instância em uso. Essa métrica não inclui a capacidade de nenhum host dedicado configurado no Outpost.

Unidade: percentual

Resolução máxima: 5 minutos

Estatística: as estatísticas mais úteis são `Average` e `pNN.NN` (percentis).

Dimensões: `Account`, `InstanceType` e `OutpostId`

`UsedInstanceType_Count`

O número de tipos de instância atualmente em uso, incluindo qualquer tipo de instância usado por serviços gerenciados, como Amazon Relational Database Service (Amazon RDS) ou Application Load Balancer. Essa métrica não inclui a capacidade de nenhum host dedicado configurado no Outpost.

Unidade: Contagem

Resolução máxima: 5 minutos

Dimensões: `Account`, `InstanceType` e `OutpostId`

`AvailableInstanceType_Count`

O número de tipos de instâncias disponíveis. Essa métrica não inclui a capacidade de nenhum host dedicado configurado no Outpost.

Unidade: Contagem

Resolução máxima: 5 minutos

Dimensões: `InstanceType` e `OutpostId`

`AvailableReservedInstances`

O número de instâncias disponíveis no Outpost para reservas de capacidade sob demanda (ODCR). Essa métrica não mede instâncias reservadas do Amazon EC2.

Unidade: Contagem

Resolução máxima: 5 minutos

Dimensões: `InstanceType` e `OutpostId`

`UsedReservedInstances`

O número de instâncias disponíveis no Outpost para reservas de capacidade sob demanda (ODCR). Essa métrica não mede instâncias reservadas do Amazon EC2.

Unidade: Contagem

Resolução máxima: 5 minutos

Dimensões: `InstanceType` e `OutpostId`

`TotalReservedInstances`

O número de instâncias disponíveis no Outpost para reservas de capacidade sob demanda (ODCR). Essa métrica não mede instâncias reservadas do Amazon EC2.

Unidade: Contagem

Resolução máxima: 5 minutos

Dimensões: `InstanceType` e `OutpostId`

`EBSVolumeTypeCapacityUtilization`

A porcentagem da capacidade do tipo de volume do EBS em uso.

Unidade: percentual

Resolução máxima: 5 minutos

Estatística: as estatísticas mais úteis são `Average` e `pNN.NN` (percentis).

Dimensões: `VolumeType` e `OutpostId`

`EBSVolumeTypeCapacityAvailability`

A porcentagem da capacidade disponível do tipo de volume do EBS.

Unidade: percentual

Resolução máxima: 5 minutos

Estatística: as estatísticas mais úteis são `Average` e `pNN.NN` (percentis).

Dimensões: `VolumeType` e `OutpostId`

`EBSVolumeTypeCapacityUtilizationGB`

O número de gigabytes em uso para o tipo de volume do EBS.

Unidade: Gigabyte

Resolução máxima: 5 minutos

Estatística: as estatísticas mais úteis são `Average` e `pNN.NN` (percentis).

Dimensões: `VolumeType` e `OutpostId`

`EBSVolumeTypeCapacityAvailabilityGB`

O número de gigabytes de capacidade disponível para o tipo de volume do EBS.

Unidade: Gigabyte

Resolução máxima: 5 minutos

Estatística: as estatísticas mais úteis são `Average` e `pNN.NN` (percentis).

Dimensões: `VolumeType` e `OutpostId`

Dimensões de métrica do Outpost

Para filtrar as métricas do seu Outpost, use as dimensões a seguir.

Dimensão	Descrição
`Account`	A conta ou serviço usando a capacidade.
`InstanceFamily`	A família da instância.
`InstanceType`	O tipo de instância.
`OutpostId`	O ID do Outpost.
`VolumeType`	O tipo de volume do EBS.
`VirtualInterfaceId`	A ID do gateway local ou da interface virtual (VIF) do link de serviço.
`VirtualInterfaceGroupId`	A ID do grupo de interface virtual para a interface virtual (VIF) do gateway local.

Veja CloudWatch as métricas do seu posto avançado

Você pode ver as CloudWatch métricas dos seus balanceadores de carga usando o CloudWatch console.

Para visualizar métricas usando o CloudWatch console

1. Abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, selecione Métricas.
3. Selecione o namespace Outposts.
4. (Opcional) Para visualizar uma métrica em todas as dimensões, digite o nome na caixa de pesquisa.

Para visualizar métricas usando o AWS CLI

Use o comando list-metrics para listar as métricas disponíveis.

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

Para obter as estatísticas de uma métrica usando a AWS CLI

Use o get-metric-statisticscomando a seguir para obter estatísticas para a métrica e a dimensão especificadas. CloudWatch trata cada combinação exclusiva de dimensões como uma métrica separada. Você não consegue recuperar estatísticas usando combinações de dimensões que não tenham sido especialmente publicadas. Você deve especificar as mesmas dimensões usadas ao criar as métricas.

```
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
```

Registre em log as chamadas à API do AWS Outposts usando o AWS CloudTrail.

AWS Outpostsé integrado comAWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço emAWS Outposts. CloudTrail captura todas as chamadas de API AWS Outposts como eventos. As chamadas capturadas incluem as aquelas do AWS Outposts console e chamadas de código para AWS Outposts operações API. Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos em um bucket do S3, incluindo eventos paraAWS Outposts. Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feitaAWS Outposts, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Para obter mais informações sobre CloudTrail, consulte o Guia AWS CloudTrail do usuário.

AWS Outpostsinformações em CloudTrail

CloudTrail é ativado em sua AWS conta quando você cria a conta. Quando a atividade ocorre emAWS Outposts, essa atividade é registrada em um CloudTrail evento junto com outros eventos AWS de serviço no histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes em sua conta AWS. Para obter mais informações, consulte Visualização de eventos com histórico de CloudTrail eventos.

Para um registro contínuo de eventos em sua AWS conta, inclusive eventos para AWS Outposts, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do S3 no local principalRegião da AWS. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas

as Regiões da AWS. A trilha registra eventos de todas as regiões na partição da AWS e fornece os arquivos de log ao bucket do S3 que você especificar. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para obter mais informações, consulte:

- Visão geral da criação de uma trilha
- CloudTrail Serviços e integrações compatíveis
- Configurando notificações do Amazon SNS para CloudTrail
- Recebendo arquivos de CloudTrail log de várias regiões e Recebendo arquivos de CloudTrail log de várias contas

Todas as AWS Outposts ações são registradas por CloudTrail. Elas são documentadas na Referência da API do AWS Outposts. Por exemplo, chamadas para as `ListSites` ações `CreateOutpostGetOutpostInstanceTypes`, e geram entradas nos arquivos de CloudTrail log.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar se a solicitação foi feita:

- Com credenciais raiz ou do usuário.
- Com credenciais de segurança temporárias para uma função ou um usuário federado.
- Por outro AWS service (Serviço da AWS).

Para obter mais informações, consulte Elemento userIdentity do CloudTrail .

Noções básicas sobre entradas de arquivos de log do AWS Outposts

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do S3 que você especificar. CloudTrail os arquivos de log contêm uma ou mais entradas de log. Um evento representa uma solicitação única de qualquer fonte. Ele inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros da solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, eles não aparecem em nenhuma ordem específica.

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a `CreateOutpost` ação.

```
{
```

```
    "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"
}
```

Manutenção do Outpost

Em modelo de responsabilidade compartilhada, AWS é responsável pelo hardware e software que executam os serviços AWS. Isso se aplica aAWS Outposts, assim como a uma região AWS. Por exemplo, AWS gerencia patches de segurança, atualiza o firmware e faz a manutenção do equipamento Outpost. AWStambém monitora o desempenho, a integridade e as métricas do seu Outpost e determina se alguma manutenção é necessária.

> **Warning**
>
> Os dados sobre volumes de armazenamento de instâncias são perdidos se o drive de disco subjacente falhar ou se a instância parar, hibernar ou terminar. Para evitar a perda de dados, recomendamos que você faça backup de seus dados de longo prazo em volumes de armazenamento de instâncias em armazenamento persistente, como um bucket do Amazon S3, um volume do Amazon EBS ou um dispositivo de armazenamento de rede em sua rede on-premises.

Conteúdo

Manutenção de hardware

Se AWS detectar um problema irreparável com o hardware que hospeda instâncias do Amazon EC2 em execução em seu Outpost, notificaremos o proprietário do Outpost e o proprietário das instâncias de que as instâncias afetadas estão programadas para serem desativadas. Para obter mais informações, consulte Desativação de instância, no Guia do usuário do Amazon EC2.

O proprietário do Outpost e o proprietário da instância podem trabalhar juntos para resolver o problema. O proprietário da instância pode parar e iniciar uma instância afetada para migrá-la para

a capacidade disponível. Os proprietários de instâncias podem interromper e iniciar as instâncias afetadas em um horário que seja conveniente para eles. Caso contrário, AWS interrompe e inicia as instâncias afetadas na data de desativação da instância. Se não houver capacidade adicional no Outpost, a instância permanecerá no estado parado. O proprietário do Outpost pode tentar liberar a capacidade usada ou solicitar capacidade adicional para o Outpost, para que a migração possa ser concluída.

Se for necessária manutenção de hardware, AWS entraremos em contato com o gerente do local do Outpost para confirmar a data e a hora da visita da equipe de AWS instalação. As visitas podem ser agendadas em até dois dias úteis a partir do momento em que o gerente do local fala com a equipe do AWS.

Quando a equipe de instalação do AWS chegar ao local, ela substituirá os hosts, switches ou elementos de rack insalubres e colocará o novo recurso on-line. Eles não realizarão nenhum diagnóstico ou reparo de hardware no local. Se substituírem um host, removerão e destruirão a chave de segurança física compatível com o NIST, destruindo efetivamente todos os dados que possam permanecer no hardware. Isso garante que nenhum dado saia do seu local. Se eles substituírem um dispositivo de rede Outpost, as informações de configuração da rede poderão estar presentes no dispositivo quando ele for removido do local. Essas informações podem incluir endereços IP e ASNs usados para estabelecer interfaces virtuais para configurar o caminho para sua rede local ou de volta para a região.

Atualizações de firmware

A atualização do firmware do Outpost normalmente não afeta as instâncias do seu Outpost. No caso raro de precisarmos reinicializar o equipamento Outpost para instalar uma atualização, você receberá um aviso de desativação de instância para todas as instâncias em execução com esse recurso.

Manutenção de equipamentos de rede

A manutenção dos dispositivos de rede Outpost (OND) é realizada sem afetar as operações e o tráfego regulares do Outpost. Se a manutenção for necessária, o tráfego será desviado do OND. Você pode notar mudanças temporárias nos anúncios do BGP, como a prependência AS-Path, e as alterações correspondentes nos padrões de tráfego nos uplinks do Outpost. Com as atualizações do firmware do OND, você pode notar uma oscilação do BGP.

Recomendamos que você configure o equipamento de rede do cliente para receber anúncios BGP dos Outposts sem alterar os atributos do BGP e habilite o balanceamento de vários caminhos/carga do BGP para obter fluxos de tráfego de entrada ideais. O acréscimo de caminho AS é usado para prefixos de gateway local para afastar o tráfego dos ONDs se a manutenção for necessária. A rede do cliente deve preferir rotas de Outposts com um comprimento de caminho AS de 1 em vez de rotas com um comprimento de caminho AS de 4.

A rede do cliente deve anunciar prefixos BGP iguais com os mesmos atributos para todos os ONDs. Por padrão, a carga da rede Outpost equilibra o tráfego de saída entre todos os uplinks. As políticas de roteamento são usadas no lado do Outpost para afastar o tráfego de um OND se a manutenção for necessária. Essa mudança de tráfego exige prefixos BGP iguais do lado do cliente em todos os ONDs. Se for necessária manutenção na rede do cliente, recomendamos que você use o acréscimo de caminho AS para mudar temporariamente a matriz de tráfego de uplinks específicos.

Melhores práticas para eventos AWS Outposts de energia e de rede

Conforme declarado nos AWSTermos de Serviço para AWS Outposts clientes, a instalação onde os equipamentos Outposts estão localizados deve atender aos requisitos mínimos de energia e de rede para apoiar a instalação, a manutenção e o uso dos equipamentos Outposts. Um rack de Outposts pode operar corretamente somente quando a energia e a conectividade com a rede são ininterruptas.

Eventos de energia

Com quedas de energia completas, há um risco inerente de que um recurso do AWS Outposts não retorne ao serviço automaticamente. Além de implantar soluções redundantes de energia e energia de backup, recomendamos que você faça o seguinte com antecedência para mitigar o impacto de alguns dos piores cenários:

- Retire seus serviços e aplicativos dos equipamentos Outposts de forma controlada, usando mudanças de balanceamento de carga baseadas em DNS ou fora do rack.
- Pare contêineres, instâncias e bancos de dados de forma incremental ordenada e use a ordem inversa ao restaurá-los.
- Planos de teste para movimentação ou parada controlada de serviços.
- Faça backup de dados e de configurações essenciais e armazene-os fora dos Outposts.
- Mantenha os tempos de inatividade de energia no mínimo.

- Evite a troca repetida das fontes de alimentação (off-on-off-on) durante a manutenção.
- Reserve mais tempo no intervalo de manutenção para lidar com o inesperado.
- Gerencie as expectativas de seus usuários e clientes comunicando um prazo de manutenção mais amplo do que você normalmente precisaria.

Eventos de conectividade de rede

A conexão do link de serviço entre o Outpost e a região AWS ou região de origem dos outposts normalmente se recupera automaticamente de interrupções ou problemas de rede que possam ocorrer em seus dispositivos de rede corporativa upstream ou na rede de qualquer provedor de conectividade terceirizado após a conclusão da manutenção da rede. Durante o período em que a conexão do link de serviço está inativa, suas operações de Outposts são limitadas às atividades da rede local. Para obter mais informações, consulte a pergunta O que acontece quando a conexão de rede da minha instalação cai? na página de perguntas frequentes do AWS Outposts rack.

Se o link do serviço estiver inativo devido a um problema de energia no local ou à perda de conectividade de rede, o AWS Health Dashboard enviará uma notificação para a conta proprietária dos Outposts. Nem você nem AWS pode suprimir a notificação de uma interrupção do link de serviço, mesmo que a interrupção seja esperada. Para obter mais informações, consulte Como iniciar o AWS Health Dashboard no Guia do usuário doAWS Health.

No caso de uma manutenção de serviço planejada que afetará a conectividade da rede, siga as seguintes etapas proativas para limitar o impacto de possíveis cenários problemáticos:

- Se seu rack de Outposts se conectar à região AWS principal por meio da Internet ou do Direct Connect público, antes de uma manutenção planejada, capture uma rota de rastreamento. Ter um caminho de rede funcional (pre-network-maintenance) e um caminho de rede problemático (post-network-maintenance) para identificar as diferenças ajudaria na solução de problemas. Se você encaminhar um problema pós-manutenção para AWS ou para o seu ISP, poderá incluir essas informações.

  Capture uma rota de rastreamento entre:

  - Os endereços IP públicos no local dos Outposts e o endereço IP retornado pelo `outposts.`*`region`*`.amazonaws.com`. Substitua *`região`* pelo nome da região AWS principal.
  - Qualquer instância na região principal com conectividade pública à Internet e endereços IP públicos no local dos Outposts.

- Se você estiver no controle da manutenção da rede, limite a duração do tempo de inatividade do link de serviço. Inclua uma etapa em seu processo de manutenção que verifique se a rede foi recuperada.
- Se você não estiver no controle da manutenção da rede, monitore o tempo de inatividade do link de serviço em relação ao intervalo de manutenção anunciado e encaminhe antecipadamente para a parte responsável pela manutenção planejada da rede se o link de serviço não estiver funcionando novamente no final do intervalo de manutenção anunciado.

Recursos

Aqui estão alguns recursos relacionados ao monitoramento que podem garantir que os Outposts estejam operando normalmente após um evento planejado ou não planejado de energia ou de rede:

- O AWS blog Monitoramento das melhores práticas para AWS Outposts aborda as melhores práticas de observabilidade e gerenciamento de eventos específicas para Outposts.
- O AWS blog Ferramenta de depuração para conectividade de rede da Amazon VPC explica a ferramenta -SetupIP VPC. AWSSupport MonitoringFrom Essa ferramenta é um documento AWS Systems Manager (documento SSM) que cria uma instância de monitoramento do Amazon EC2 em uma sub-rede especificada por você e monitora os endereços IP de destino. O documento executa testes de diagnóstico de ping, MTR, rota de rastreamento e caminho de rastreamento de TCP e armazena os resultados no Amazon CloudWatch Logs, que podem ser visualizados em um CloudWatch painel (por exemplo, latência, perda de pacotes). Para o monitoramento de Outposts, a instância de monitor deve estar em uma sub-rede da região AWS principal e configurada para monitorar uma ou mais de suas instâncias de Outpost usando seus IPs privados. Isso fornecerá gráficos de perda de pacotes e latência entre e a região AWS Outposts e a região AWS principal.
- O AWS blog Implantando um CloudWatch painel automatizado da Amazon para AWS Outposts uso AWS CDK descreve as etapas envolvidas na implantação de um painel automatizado.
- Se você tiver dúvidas ou precisar de mais informações, consulte Criação de um caso de suporte no AWSGuia do usuário de suporte.

Otimizar o Amazon EC2 para AWS Outposts

Em contraste com a Região da AWS, a capacidade do Amazon Elastic Compute Cloud (Amazon EC2) em um Outpost é finita. Você está limitado pelo volume total de capacidade computacional

que solicitou. Este tópico oferece as melhores práticas e estratégias de otimização para ajudá-lo a aproveitar ao máximo sua capacidade do Amazon EC2 em AWS Outposts.

Conteúdo

Hosts dedicados em Outposts

Um host dedicado do Amazon EC2 é um servidor físico com capacidade de instância do EC2 totalmente dedicado para seu uso. Seu Outpost já fornece hardware dedicado, mas os hosts dedicados permitem que você use licenças de software existentes com restrições de licença por soquete, por núcleo ou por VM em um único host. Para obter mais informações, consulte Hosts dedicadosAWS Outposts no Guia do usuário do Amazon EC2 para instâncias Linux. Para Windows, consulte Host dedicado no AWS Outposts no Guia do usuário do Amazon EC2 para instâncias Windows.

Além do licenciamento, os proprietários dos Outposts podem usar hosts dedicados para otimizar os servidores em suas implantações do Outpost de duas maneiras:

- Alterar o layout da capacidade de um servidor
- Posicionamento da instância de controle no nível do hardware

Alterar o layout da capacidade de um servidor

Os hosts dedicados oferecem a capacidade de alterar o layout dos servidores em sua implantação do Outpost sem entrar em contato com AWS Support. Ao comprar capacidade para seu Outpost, você especifica um layout de capacidade do EC2 que cada servidor fornece. Cada servidor oferece suporte a uma única família de tipos de instância. Um layout pode oferecer um único tipo de instância ou vários tipos de instâncias. Os hosts dedicados permitem que você altere o que você escolher para esse layout inicial. Se você alocar um host para oferecer suporte a um único tipo de instância para toda a capacidade, só poderá executar um único tipo de instância a partir desse host. A ilustração a seguir apresenta um servidor m5.24xlarge com um layout homogêneo:

Você pode alocar a mesma capacidade para vários tipos de instância. Ao alocar um host para oferecer suporte a vários tipos de instância, você obtém um layout heterogêneo que não exige um layout de capacidade explícito. A ilustração a seguir apresenta um servidor m5.24xlarge com um layout heterogêneo em capacidade total:

Para obter mais informações, consulte Alocar hosts dedicados no Guia do usuário do Amazon EC2 para instâncias Linux ou Alocar hosts dedicados Guia do usuário do Amazon EC2 para instâncias Windows.

Posicionamento da instância de controle no nível do hardware

Você pode usar hosts dedicados para controlar o posicionamento da instância no nível do hardware. Use o posicionamento automático para hosts dedicados para gerenciar se as instâncias que você iniciar serão iniciadas em um host específico ou em qualquer host disponível que tenha configurações correspondentes. Use a afinidade de host para estabelecer um relacionamento entre uma instância e um host dedicado. Se você tiver um rack de Outpost, poderá usar esses atributos de hosts dedicados para minimizar o impacto de falhas de hardware correlacionadas. Para obter mais informações sobre recuperação de instâncias, consulte Entender o posicionamento automático e a afinidade no Guia do usuário do Amazon EC2 para instâncias Linux ou Entender o posicionamento automático e a afinidade no Guia do usuário do Amazon EC2 para instâncias Windows..

Você pode compartilhar hosts dedicados usando AWS Resource Access Manager. O compartilhamento de hosts dedicados permite que você distribua hosts em uma implantação do Outpost em Contas da AWS. Para ter mais informações, consulte Trabalhar com recursos compartilhados.

Configurar a recuperação de instâncias

As instâncias em seu Outpost que entrarem em um estado de não integridade devido a uma falha de hardware devem ser migradas para um host íntegro. Você pode configurar a recuperação automática para que essa migração seja feita automaticamente com base nas verificações de status da instância. Para obter mais informações, consulte Recuperar sua instância Linux ou Recuperar sua instância Windodws.

Grupos de posicionamento em Outposts

O AWS Outposts suporta grupos de posicionamento. Use grupos de posicionamento para influenciar como o Amazon EC2 deve tentar posicionar grupos de instâncias interdependentes que você

executa no hardware subjacente. Você pode usar estratégias diferentes (cluster, partição ou distribuição) para atender às necessidades de diferentes cargas de trabalho. Se você tiver um Outpost de rack único, poderá usar a estratégia de distribuição para posicionar instâncias em hosts em vez de em racks.

Grupos com posicionamento distribuído

Use um grupo com posicionamento distribuído para distribuir uma única instância em hardware distinto. Executar instâncias em um grupo com posicionamento distribuído reduz o risco de falhas simultâneas que podem ocorrer quando as instâncias compartilham os mesmos equipamentos. Grupos de posicionamento podem distribuir instâncias em racks ou hosts. Você pode usar grupos de posicionamento de distribuição em host somente com AWS Outposts.

Grupos de posicionamento de distribuição em rack

Seu grupo com posicionamento distribuído em racks pode armazenar o mesmo número de instâncias quanto de racks que você tiver em sua implantação do Outpost. A ilustração a seguir mostra uma implantação do Outpost de três racks executando três instâncias em um grupo com posicionamento em nível de distribuição em racks.

Grupos de posicionamento em nível de distribuição em hosts

Seu grupo com posicionamento em nível de distribuição em host pode conter o mesmo número de instâncias que o número de hosts que você tiver em sua implantação do Outpost. A ilustração a seguir mostra uma implantação de Outpost de rack único executando três instâncias em um grupo com posicionamento em nível de distribuição em hosts.

Grupos de posicionamento de partição

Use um grupo com posicionamento em partições para distribuir várias instâncias em racks com partições. Cada partição pode conter várias instâncias. Você pode usar a distribuição automática para distribuir instâncias entre partições ou implantar instâncias em partições de destino. A ilustração a seguir mostra um grupo com posicionamento em partições com distribuição automática.

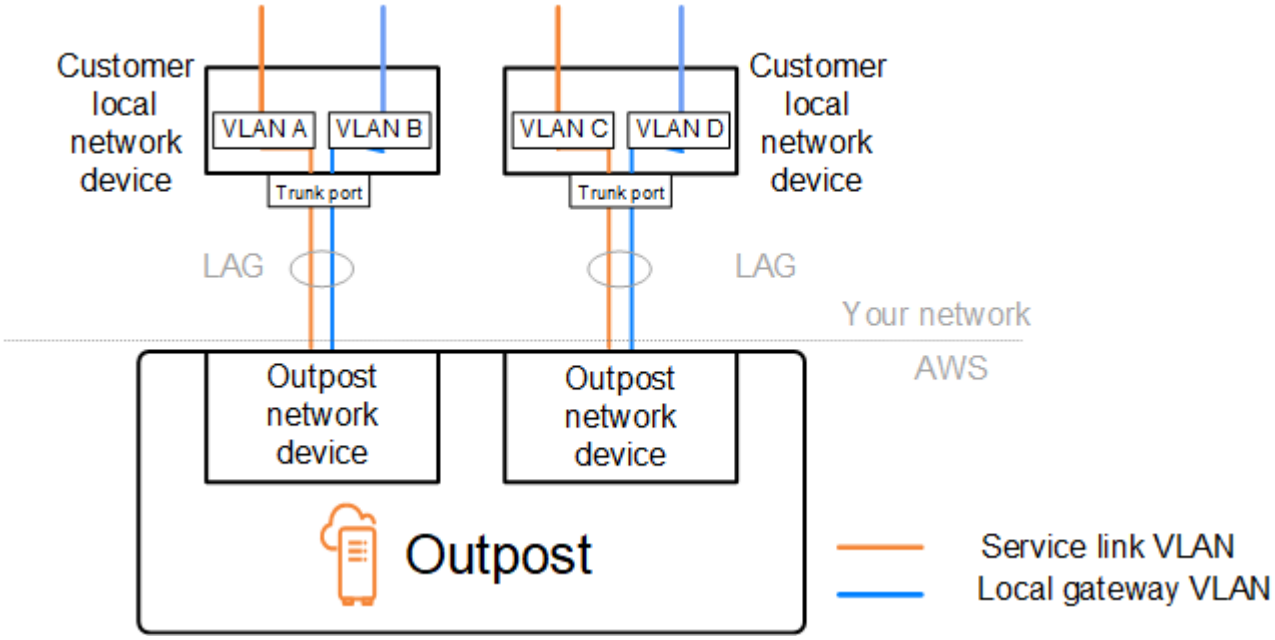
Você também pode implantar instâncias em partições de destino. A ilustração a seguir mostra um grupo com posicionamento em partições com distribuição direcionada.

Para obter mais informações sobre como trabalhar com grupos de posicionamento, consulte Grupos de posicionamento e Grupos de posicionamento em AWS Outposts no Guia do usuário do Amazon EC2 para instâncias Linux. Para Windows, consulte Grupos de posicionamento e Grupos de posicionamento em AWS Outposts no Guia do usuário do Amazon EC2 para instâncias do Windows.

Para obter mais informações sobre a alta disponibilidade do AWS Outposts, consulte Considerações sobre design e arquitetura de alta disponibilidade do AWS Outposts.

Lista de verificação de solução de problemas de rede em rack do AWS Outposts

Use essa lista de verificação para ajudar a solucionar problemas de um link de serviço que tem o status de `DOWN`.



Conectividade com dispositivos de rede Outpost

Verifique o status do emparelhamento BGP nos dispositivos de rede local do cliente que estão conectados aos dispositivos de rede Outpost. Se o status de emparelhamento do BGP for `DOWN`, siga estas etapas:

1. Faça o ping do endereço IP do peer remoto nos dispositivos de rede Outpost a partir dos dispositivos do cliente. Você pode encontrar o endereço IP do peer na configuração do BGP do

seu dispositivo. Você também pode consultar o Lista de verificação de prontidão da rede fornecido no momento da instalação.

2. Se o ping não for bem-sucedido, verifique a conexão física e verifique se o status da conectividade é UP.
   a. Confirme o status do LACP dos dispositivos de rede local do cliente.
   b. Verifique o status da interface no dispositivo. Se o status forUP, passe para a etapa 3.
   c. Verifique os dispositivos de rede local do cliente e confirme se o módulo óptico está funcionando.
   d. Substitua as fibras defeituosas e certifique-se de que as luzes (Tx/Rx) estejam dentro da faixa aceitável.
3. Se o ping for bem-sucedido, verifique os dispositivos de rede local do cliente e certifique-se de que as seguintes configurações de BGP estejam corretas.
   a. Confirme se o Número do Sistema Autônomo local (ASN do cliente) está configurado corretamente.
   b. Confirme se o Número do Sistema Autônomo remoto (Outpost ASN) está configurado corretamente.
   c. Confirme se o IP da interface e os endereços IP do peer remoto estão configurados corretamente.
   d. Confirme se as rotas anunciadas e recebidas estão corretas.
4. Se sua sessão do BGP estiver oscilando entre os estados ativo e de conexão, verifique se a porta TCP 179 e outras portas efêmeras relevantes não estão bloqueadas nos dispositivos de rede local do cliente.
5. Se precisar solucionar mais problemas, verifique o seguinte nos dispositivos de rede local do cliente:
   a. Registros de depuração BGP e TCP
   b. Registros do BGP
   c. Captura de pacotes
6. Se o problema persistir, realize capturas de pacotes MTR/traceroute/do roteador conectado ao Outpost para os endereços IP do peer do dispositivo de rede do Outpost. Compartilhe os resultados do teste com o Suporte do AWS, usando seu plano de suporte corporativo.

Se o status de emparelhamento do BGP estiver UP entre os dispositivos de rede local do cliente e os dispositivos de rede do Outpost, mas o link de serviço ainda estiverDOWN, você poderá solucionar

mais problemas verificando os seguintes dispositivos nos dispositivos da rede local do cliente. Use uma das seguintes listas de verificação, dependendo de como a conectividade do link de serviço é provisionada.

- Roteadores Edge conectados com AWS Direct Connect — Interface virtual pública em uso para conectividade de link de serviço. Para ter mais informações, consulte conectividade de interface virtual pública de AWS Direct Connect com a região AWS.
- Roteadores Edge conectados com AWS Direct Connect — Interface virtual privada em uso para conectividade de link de serviço. Para ter mais informações, consulte conectividade de interface virtual privada do AWS Direct Connect com a região AWS.
- Roteadores Edge conectados a provedores de serviços de Internet (ISPs) — Internet pública em uso para conectividade de link de serviço. Para ter mais informações, consulte Conectividade de internet pública do ISP com a região AWS.

conectividade de interface virtual pública de AWS Direct Connect com a região AWS

Use a lista de verificação a seguir para solucionar problemas de roteadores de borda conectados a AWS Direct Connect quando uma interface virtual pública está em uso para conectividade de link de serviço.

1. Confirme se os dispositivos conectados diretamente aos dispositivos de rede do Outpost estão recebendo os intervalos de endereços IP do link de serviço por meio do BGP.
   a. Confirme as rotas que estão sendo recebidas pelo BGP do seu dispositivo.
   b. Verifique a tabela de rotas da instância de roteamento e encaminhamento virtual (VRF) do link de serviço. Ela deve mostrar que está usando o intervalo de endereços IP.
2. Para garantir a conectividade da região, verifique a tabela de rotas do link de serviço VRF. Ela deve incluir os intervalos de endereços IP públicos de AWS ou a rota padrão.
3. Se você não estiver recebendo os intervalos de endereços IP AWS públicos no link de serviço VRF, verifique os itens a seguir.
   a. Verifique o status do link AWS Direct Connect no roteador de borda ou noAWS Management Console.
   b. Se o link físico estiver`UP`, verifique o status de emparelhamento do BGP no roteador de borda.
   c. Se o status de emparelhamento BGP for`DOWN`, faça ping no endereço IP AWS do peer e verifique a configuração do BGP no roteador de borda. Para obter mais informações, consulte

Solução de problemas AWS Direct Connect no AWS Direct Connect Guia do usuário e O status do BGP da minha interface virtual está inativo no console do AWS. O que devo fazer?

d. Se o BGP estiver estabelecido e você não estiver vendo a rota padrão ou os intervalos de endereços IP AWS públicos no VRF, entre em contato com o Suporte do AWS usando seu plano de suporte Enterprise.

4. Se você tiver um firewall on-premises, verifique os itens abaixo.

   a. Confirme se as portas necessárias para a conectividade do link de serviço são permitidas nos firewalls da rede. Use o traceroute na porta 443 ou qualquer outra ferramenta de solução de problemas de rede para confirmar a conectividade por meio dos firewalls e dos dispositivos de rede. As portas a seguir devem ser configuradas nas políticas de firewall para a conectividade do link de serviço.

      - Protocolo TCP — Porta de origem: TCP 1025-65535, Porta de destino: 443.
      - Protocolo UDP — Porta de origem: TCP 1025-65535, Porta de destino: 443.

   b. Se o firewall estiver stateful, certifique-se de que as regras de saída permitam que o serviço do Outpost vincule o intervalo de endereços IP aos intervalos de endereços IP AWS públicos. Para ter mais informações, consulte Conectividade do AWS Outposts com regiões AWS.

   c. Se o firewall não estiver stateful, certifique-se de permitir também o fluxo de entrada (dos intervalos de endereços IP AWS públicos até o intervalo de endereços IP do link de serviço).

   d. Se você tiver configurado um roteador virtual nos firewalls, certifique-se de que o roteamento apropriado esteja configurado para o tráfego entre o Outpost e a Região AWS.

5. Se você tiver configurado o NAT na rede on-premises para converter os intervalos de endereços IP do link de serviço do Outpost para seus próprios endereços IP públicos, verifique os itens a seguir.

   a. Confirme se o dispositivo NAT não está sobrecarregado e tem portas livres para alocar para novas sessões.

   b. Confirme se o dispositivo NAT está configurado corretamente para realizar a conversão do endereço.

6. Se o problema persistir, realize capturas de pacotes MTR/traceroute/do roteador de borda para os endereços IP dos peers. AWS Direct Connect Compartilhe os resultados do teste com o Suporte do AWS, usando seu plano de suporte corporativo.

conectividade de interface virtual privada do AWS Direct Connect com a região AWS

Use a lista de verificação a seguir para solucionar problemas de roteadores de borda conectados a AWS Direct Connect quando uma interface virtual privada está em uso para conectividade de link de serviço.

1. Se a conectividade entre o rack do Outpost e a região AWS estiver usando o recurso de conectividade privada com AWS Outposts, verifique os itens a seguir.
   a. Faça ping no endereço IP AWS de emparelhamento remoto do roteador de borda e confirme o status de emparelhamento do BGP.
   b. Certifique-se de que o emparelhamento do BGP pela interface virtual privada do AWS Direct Connect entre seu endpoint de link de serviço (VPC) e o Outpost configurado on-premises esteja UP. Para obter mais informações, consulte Solução de problemas AWS Direct Connect no AWS Direct Connect Guia do usuário, Status do BGP da minha interface virtual está inativo no console AWS. O que devo fazer?, e Como posso solucionar problemas de conexão BGP pelo Direct Connect? .
   c. A interface virtual privada do AWS Direct Connect é uma conexão privada com o roteador de borda no local AWS Direct Connect escolhido e usa o BGP para trocar rotas. Sua faixa de CIDR de nuvem privada virtual (VPC) é anunciada por meio dessa sessão BGP para seu roteador de borda. Da mesma forma, o intervalo de endereços IP do link do serviço do Outpost é anunciado para a região por meio do BGP a partir do seu roteador de borda.
   d. Confirme se as ACLs de rede associadas ao endpoint privado do link de serviço em sua VPC permitem o tráfego relevante. Para ter mais informações, consulte Lista de verificação de prontidão da rede.
   e. Se você tiver um firewall on-premises, certifique-se de que o firewall tenha regras de saída que permitam os intervalos de endereços IP do link de serviço e os endpoints do serviço Outpost (os endereços IP da interface de rede) localizados na VPC ou no CIDR da VPC. Certifique-se de que as portas TCP 1025-65535 e UDP 443 não estejam bloqueadas. Para obter mais informações, consulte Introdução da conectividade privada do AWS Outposts.
   f. Se o firewall não estiver stateful, certifique-se de que o firewall tenha regras e políticas para permitir o tráfego de entrada para o Outpost a partir dos endpoints do serviço do Outpost na VPC.

2. Se você tiver mais de 100 redes em sua rede on-premises, poderá anunciar uma rota padrão na sessão do BGP para sua interface virtual privada do AWS. Se você não quiser anunciar uma rota padrão, resuma as rotas para que o número de rotas anunciadas seja menor que 100.
3. Se o problema persistir, realize capturas de pacotes MTR/traceroute/do roteador de borda para os endereços IP dos peers. AWS Direct Connect Compartilhe os resultados do teste com o Suporte do AWS, usando seu plano de suporte corporativo.

Conectividade de internet pública do ISP com a região AWS

Use a lista de verificação a seguir para solucionar problemas de roteadores de borda conectados por meio de um ISP ao usar a Internet pública para conectividade de link de serviço.

- Confirme se o link da Internet está ativo.
- Confirme se os servidores públicos estão acessíveis a partir de seus dispositivos periféricos conectados por meio de um ISP.

Se a Internet ou os servidores públicos não estiverem acessíveis por meio dos links do ISP, conclua as etapas a seguir.

1. Verifique se o status de emparelhamento BGP com os roteadores ISP está estabelecido.
   a. Confirme se o BGP não está oscilando.
   b. Confirme se o BGP está recebendo e anunciando as rotas necessárias do ISP.
2. No caso de configuração de rota estática, verifique se a rota padrão está configurada corretamente no dispositivo de borda.
3. Confirme se você pode acessar a Internet usando outra conexão ISP.
4. Se o problema persistir, execute capturas de pacotes MTR/traceroute/em seu roteador de borda. Compartilhe os resultados com a equipe de suporte técnico do seu ISP para solucionar problemas adicionais.

Se a Internet e os servidores públicos estiverem acessíveis por meio dos links do ISP, conclua as etapas a seguir.

1. Confirme se alguma de suas instâncias do EC2 ou balanceadores de carga acessíveis ao público na região de origem do Outpost pode ser acessada a partir do seu dispositivo de borda. Você

pode usar ping ou telnet para confirmar a conectividade e, em seguida, usar traceroute para confirmar o caminho da rede.

2. Se você usa VRFs para separar o tráfego em sua rede, confirme se o link de serviço VRF tem rotas ou políticas que direcionam o tráfego de e para o ISP (Internet) e o VRF. Veja os seguintes pontos de verificação.
   a. Roteadores Edge conectados ao ISP. Verifique a tabela de rotas ISP VRF do roteador de borda para confirmar se o intervalo de endereços IP do link de serviço está presente.
   b. Dispositivos de rede local do cliente conectados ao Outpost. Verifique as configurações dos VRFs e assegure-se de que o roteamento e as políticas necessárias para a conectividade entre o VRF do link de serviço e o ISP VRF estejam configurados corretamente. Normalmente, uma rota padrão é enviada do ISP VRF para o link de serviço VRF para tráfego para a Internet.
   c. Se você configurou o roteamento com base na origem nos roteadores conectados ao seu Outpost, confirme se a configuração está correta.
3. Certifique-se de que os firewalls on-premises estejam configurados para permitir conectividade de saída (portas TCP 1025-65535 e UDP 443) dos intervalos de endereços IP do link do serviço Outpost aos intervalos de endereços IP AWS públicos. Se os firewalls não estiverem stateful, certifique-se de que a conectividade de entrada com o Outpost também esteja configurada.
4. Certifique-se de que o NAT esteja configurado na rede on-premises para converter os intervalos de endereços IP do link de serviço do Outpost em endereços IP públicos. Além disso, confirme os itens abaixo.
   a. O dispositivo NAT não está sobrecarregado e tem portas livres para alocar para novas sessões.
   b. O dispositivo NAT está configurado corretamente para realizar a conversão do endereço.

Se o problema persistir, execute capturas de pacotes MTR/traceroute/.

- Se os resultados mostrarem que os pacotes estão sendo descartados ou bloqueados na rede on-premises, consulte sua equipe de rede ou equipe técnica para obter orientação adicional.
- Se os resultados mostrarem que os pacotes estão caindo ou bloqueados na rede do ISP, entre em contato com a equipe de suporte técnico do ISP.
- Se os resultados não mostrarem nenhum problema, colete os resultados de todos os testes (como MTR, telnet, traceroute, capturas de pacotes e logs de BGP) e entre em contato com o Suporte do AWS usando seu plano de suporte Enterprise.

Outposts está por trás de dois dispositivos de firewall

Se você colocou seu Outpost atrás de um par de firewalls sincronizados de alta disponibilidade ou dois firewalls independentes, o roteamento assimétrico do link de serviço pode ocorrer. Isso significa que o tráfego de entrada pode passar pelo firewall-1, enquanto o tráfego de saída passa pelo firewall-2. Use a lista de verificação a seguir para identificar o possível roteamento assimétrico do link de serviço, especialmente se ele estava funcionando corretamente antes.

- Verifique se houve alguma alteração recente ou manutenção contínua na configuração de roteamento da sua rede corporativa que possa ter levado ao roteamento assimétrico do link de serviço por meio dos firewalls.
  - Use gráficos de tráfego de firewall para verificar se há alterações nos padrões de tráfego que se alinham com o início do problema do link de serviço.
  - Verifique se há uma falha parcial no firewall ou um cenário de par de firewalls com cérebro dividido que possa ter feito com que seus firewalls não sincronizassem mais suas tabelas de conexão entre si.
  - Verifique se há links inativos ou alterações recentes no roteamento (alterações na métrica OSPF/ISIS/EIGRP, alterações no mapa de rotas do BGP) em sua rede corporativa que estejam alinhadas com o início do problema do link de serviço.
- Se você estiver usando conectividade pública à Internet para o link de serviço para a região de origem, a manutenção do provedor de serviços pode ter dado origem ao roteamento assimétrico do link de serviço por meio dos firewalls.
  - Verifique os gráficos de tráfego em busca de links para seus ISPs para ver se há alterações nos padrões de tráfego que estejam alinhados com o início do problema do link de serviço.
- Se você estiver usando AWS Direct Connect conectividade para o link de serviço, é possível que uma manutenção AWS planejada tenha acionado o roteamento assimétrico do link de serviço.
  - Verifique se há notificações de manutenção planejada em seu (s) AWS Direct Connect serviço (s).
  - Observe que, se você tiver AWS Direct Connect serviços redundantes, poderá testar proativamente o roteamento do link de serviço Outposts em cada caminho de rede provável sob condições de manutenção. Isso permite testar se uma interrupção em um de seus AWS Direct Connect serviços pode levar ao roteamento assimétrico do link de serviço. A resiliência da AWS Direct Connect parte da conectividade de end-to-end rede pode ser testada pelo AWS Direct Connect Resiliency with Resiliency Toolkit. Para obter mais informações, consulte Testando AWS Direct Connect resiliência com o kit de ferramentas de resiliência — Teste de failover.

Depois de examinar a lista de verificação anterior e identificar o roteamento assimétrico do link de serviço como uma possível causa raiz, há várias ações adicionais que você pode tomar:

- Restaure o roteamento simétrico revertendo quaisquer alterações na rede corporativa ou aguardando a conclusão da manutenção planejada do provedor.
- Faça login em um ou em ambos os firewalls e limpe todas as informações do estado do fluxo de todos os fluxos da linha de comando (se suportado pelo fornecedor do firewall).
- Filtre temporariamente os anúncios do BGP por meio de um dos firewalls ou feche as interfaces em um firewall para forçar o roteamento simétrico pelo outro firewall.
- Reinicialize cada firewall alternadamente para eliminar a possível corrupção no rastreamento do estado de fluxo do tráfego do link de serviço na memória do firewall.
- Entre em contato com seu fornecedor de firewall para verificar ou relaxar o rastreamento do estado do fluxo UDP para conexões UDP originadas na porta 443 e destinadas à porta 443.

AWS Outposts end-of-term opções

Ao final do seu período AWS Outposts, você tem três opções:

- Renove sua assinatura e mantenha seu Outpost existente.
- Encerre sua assinatura e prepare seus racks de Outpost para devolução.
- Converta para uma month-to-month assinatura e mantenha seu Outpost existente.

Se você não indicar que deseja renovar sua assinatura ou devolver seu Outpost, você será convertido em uma month-to-month assinatura.

Tópicos

Renove sua assinatura

Renove sua assinatura e mantenha seu Outpost existente:

Conclua as etapas a seguir pelo menos 30 dias antes do término do período do seu Outpost:

1. Faça login no console do AWS Support Center.
2. Escolha Criar caso.
3. Escolha Conta e faturamento.
4. Em Serviço, escolha Cobrança.
5. Em Categoria, escolha Outras perguntas sobre faturamento.
6. Em Gravidade, escolha Pergunta importante.
7. Selecione Próxima etapa: informações adicionais.
8. Na página Informações adicionais, em Assunto, insira sua solicitação de renovação, como **`Renew my Outpost subscription`**.
9. Em Descrição, insira uma das seguintes opções de pagamento:

    - Sem taxas iniciais

- Adiantado parcial
- Adiantado integral

Para obter a definição de preço, consulte AWS Outposts preço do rack. Você também pode solicitar uma cotação de preço.

10. Escolha Próxima etapa: solucione ou entre em contato conosco.
11. Na página Entre em contato conosco, escolha seu idioma preferencial.
12. Escolha seu método de contato preferido.
13. Revise os detalhes do seu caso e escolha Enviar. O número do ID do caso e o resumo são exibidos.

O Suporte ao cliente da AWS iniciará o processo de renovação da assinatura. Sua nova assinatura começará no dia seguinte ao término da assinatura atual.

Encerre sua assinatura e prepare os racks para devolução

> **Important**
>
> AWSnão pode iniciar o processo de devolução até que você tenha concluído os procedimentos a seguir. Não podemos interromper o processo de devolução depois que você abrir um caso de suporte para encerrar sua assinatura.

Para encerrar sua assinatura:

Conclua as etapas a seguir pelo menos 30 dias antes do término do período do seu Outpost:

1. Faça login no console do AWS Support Center.
2. Escolha Criar caso.
3. Escolha Conta e faturamento.
4. Em Serviço, escolha Cobrança.
5. Em Categoria, escolha Outras perguntas sobre faturamento.
6. Em Gravidade, escolha Pergunta importante.
7. Selecione Próxima etapa: informações adicionais.

8. Na página Informações adicionais, em Assunto, insira uma solicitação clara, como **`End my Outpost subscription`**.
9. Em Descrição, insira a data em que você prefere que o Outpost seja recuperado.
10. Escolha Próxima etapa: solucione ou entre em contato conosco.
11. Na página Entre em contato conosco, escolha seu idioma preferencial.
12. Escolha seu método de contato preferido.
13. Revise os detalhes do seu caso e escolha Enviar. O número do ID do caso e o resumo são exibidos.

AWSO Suporte ao cliente entrará em contato com você para coordenar a recuperação.

Para preparar seus racks de AWS Outposts para devolução:

> **Important**
>
> Não desligue o rack do Outpost até que AWS esteja no local para a recuperação programada.

1. Se os recursos do Outpost estiverem compartilhados, você deverá cancelar o compartilhamento desses recursos.

   É possível cancelar o compartilhamento de um recurso do Outpost por uma das seguintes maneiras:

   - Use o console do AWS RAM. Para obter mais informações, consulte Atualização de um compartilhamento de recursos no Guia do usuário do AWS RAM.
   - Use a AWS CLI para executar o comando disassociate-resource-share.

   Para ver a lista de recursos do Outpost que podem ser compartilhados, consulte Recursos compartilháveis do Outpost.
2. Encerre as instâncias ativas associadas às sub-redes em seu Outpost. Para encerrar as instâncias, siga as instruções em Encerrar sua instância no Guia do usuário do Amazon EC2 para instâncias do Linux.
3. Verifique as instâncias instance-capacity-availability do Amazon EC2 em sua AWS conta.

a. Abra o console do AWS Outposts em https://console.aws.amazon.com/outposts/.

b. Escolha Outposts.

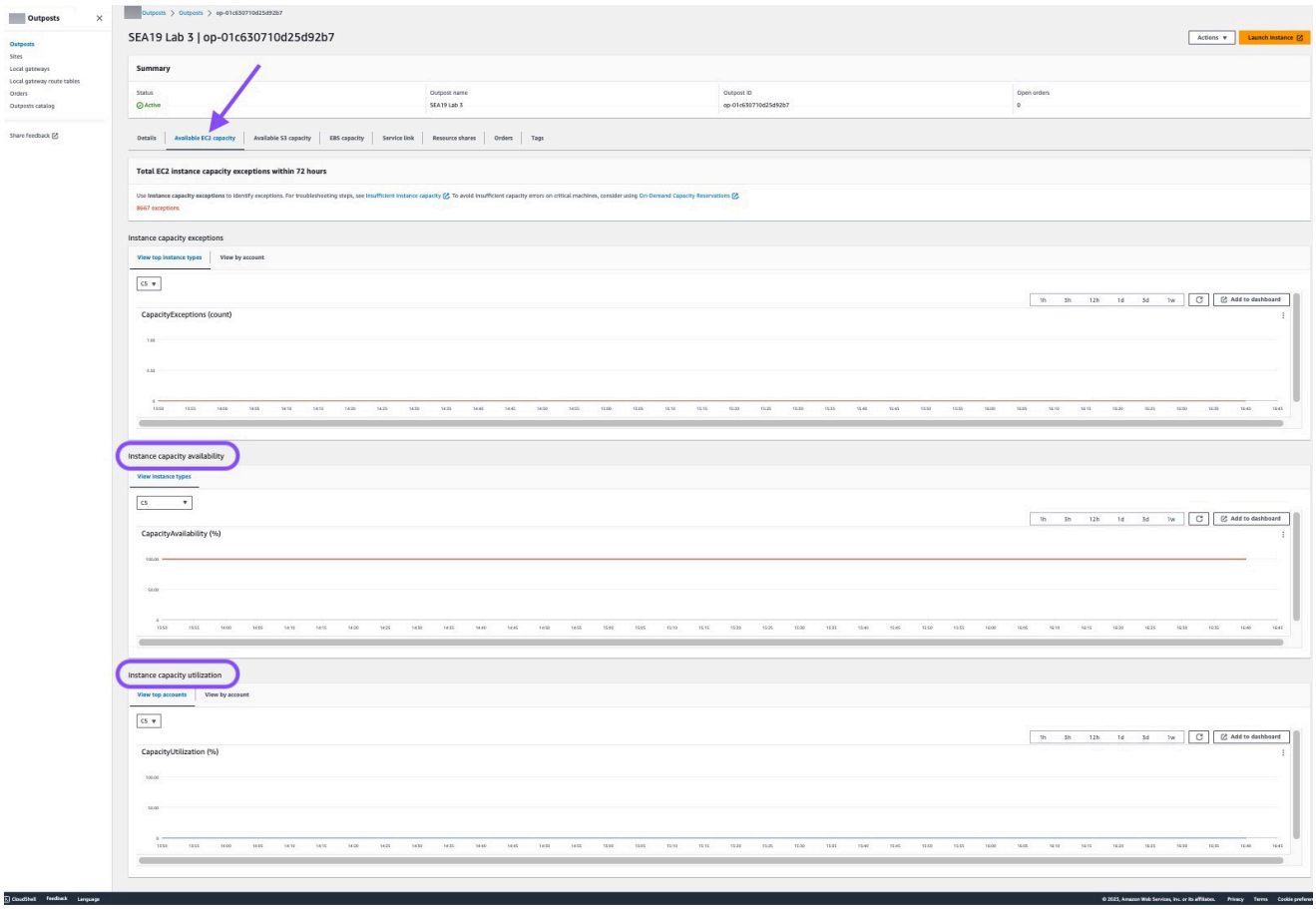
c. Escolha o Outpost específico que você está retornando.

d. Na página do Outpost, escolha a guia Capacidade disponível do EC2.

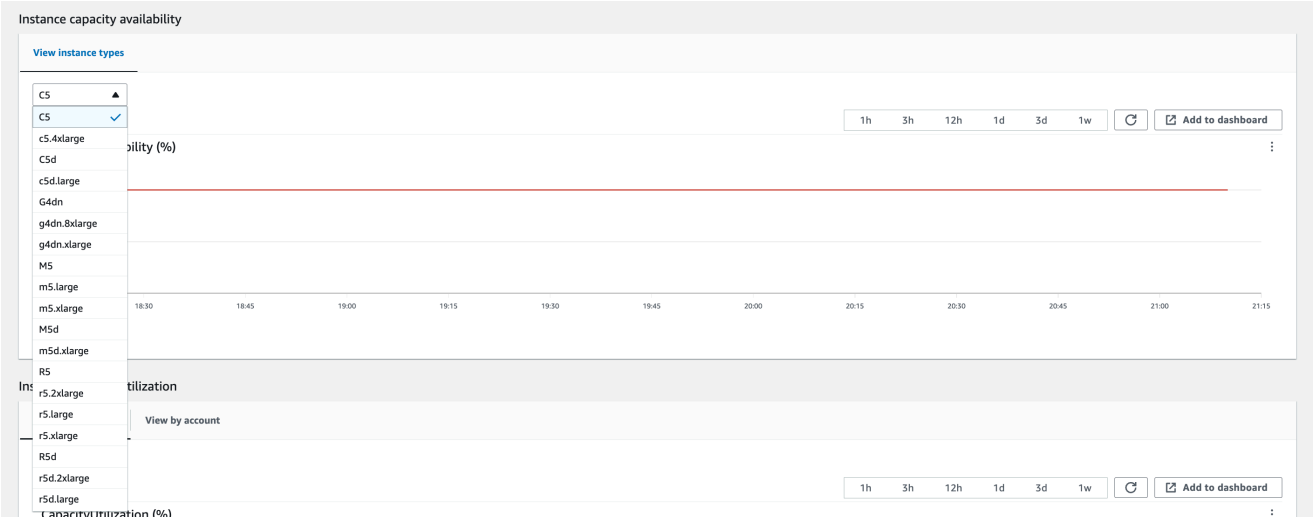
e. Certifique-se de que a disponibilidade da capacidade da instância seja de 100% para cada família de instâncias.

f. Certifique-se de que a utilização da capacidade da instância seja de 0% para cada família de instâncias.

A imagem a seguir mostra os gráficos de disponibilidade da capacidade da instância e de utilização da capacidade da instância na guia Capacidade disponível do EC2.



A imagem a seguir mostra a lista de tipos de instância.



4. Crie backups de suas instâncias e volumes de servidores do Amazon EC2. Para criar os backups, siga as instruções em Backup e recuperação para Amazon EC2 com volumes do EBS no AWS Guia de orientação prescritiva.
5. Exclua os volumes do Amazon EBS associados ao seu Outpost.
   a. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
   b. No painel de navegação, escolha Volumes.
   c. Escolha Ações e Excluir volume.
   d. Na caixa de diálogo de confirmação, escolha Excluir.
6. Se você tiver o Amazon S3 on Outposts, exclua todos os snapshots locais dos Outposts.
   a. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
   b. No painel de navegação, selecione Snapshots.
   c. Selecione os snapshots com um ARN do Outpost.
   d. Escolha Ações e Excluir snapshots.
   e. Na caixa de diálogo de confirmação, escolha Excluir.
7. Exclua todos os buckets do Amazon S3 associados ao seu Outpost. Para excluir os buckets, siga as instruções apresentadas em Excluir o Amazon S3 on Outposts no Guia do usuário do Amazon Simple Storage Service.
8. Exclua todas as associações de VPC e CIDRs de grupo de endereços IP (CoIPs) de propriedade do cliente associados ao seu Outpost.

Uma equipe de recuperação de AWS desligará o rack. Depois de desligada, você pode destruir a chave de segurança AWS Nitro ou a equipe de recuperação do AWS pode fazer isso em seu nome.

Converter em uma month-to-month assinatura

Para converter em uma month-to-month assinatura e manter seu Outpost existente, nenhuma ação é necessária. Se tiver dúvidas, abra um caso de suporte de faturamento.

Seu Outpost será renovado mensalmente de acordo com a taxa da opção de pagamento sem adiantamento que corresponde à sua configuração do AWS Outposts. Sua nova assinatura mensal começará no dia seguinte ao término da assinatura atual.

Cotas para AWS Outposts

Sua Conta da AWS tem cotas padrão, anteriormente chamadas de limites, para cada AWS service (Serviço da AWS). A menos que especificado de outra forma, cada cota é específica da região. Você pode solicitar aumentos para algumas cotas, mas não para todas as cotas.

Para visualizar todas as cotas do AWS Outposts, abra o console do Service Quotas. No painel de navegação, selecione Serviços da AWS e AWS Outposts.

Para solicitar o aumento da cota, consulte Requesting a Quota Increase (Solicitar um aumento de cota) no Guia do usuário do Service Quotas.

A Conta da AWS tem as seguintes cotas relacionadas ao AWS Outposts.

Recurso	Padrão	Ajustável	Comentários
Sites do Outposts	100	Yes (Sim)	Um site do Outposts é a locação física gerenciada pelo cliente onde você alimenta e conecta seu equipamento do Outpost à rede. Você pode ter 100 sites do Outposts em cada região da sua conta da AWS.
Outposts por site	10	Yes (Sim)	O AWS Outposts inclui hardware e recursos virtuais, conhecidos como Outposts. Essa cota limita seus recursos virtuais do Outpost. Você pode ter 10 Outposts em cada site Outpost.

AWS Outposts e as cotas para outros serviços

O AWS Outposts depende dos recursos de outros serviços e esses serviços podem ter suas próprias cotas padrão. Por exemplo, sua cota para interfaces de rede local é extraída da cota do Amazon VPC para interfaces de rede.

Histórico do documento

A tabela a seguir descreve as alterações importantes feitas no Guia do usuário do AWS Outposts .

Alteração	Descrição	Data
Gerenciamento de capacidade	Você pode modificar a configuração de capacidade padrão para seu novo pedido de Outposts.	16 de abril de 2024
AWS Outposts O rack suporta métricas de taxa de transferência da interface de link de serviço	Agora você pode monitorar o uso da taxa de transferência entre as interfaces virtuais (VIFs) do Outpost rack Service Link e seus dispositivos de rede local, `IfTrafficIn` aproveitando as métricas. `IfTrafficOut` Amazon CloudWatch	17 de novembro de 2023
Comunicação intra-VPC com gateway local AWS Outposts	Você pode estabelecer comunicação entre sub-redes que estão na mesma VPC entre diferentes Outposts usando os gateways locais do Outpost e sua rede on-premises.	30 de agosto de 2023
nd-of-term Opções E para AWS Outposts racks	Ao final do AWS Outposts período, você pode renovar, encerrar ou converter sua assinatura.	1º de agosto de 2023
O Amazon Route 53 on Outposts está disponível em racks. AWS Outposts	O Amazon Route 53 inclui um Resolvedor que armazena em cache todas as consultas	20 de julho de 2023

	ao DNS oriundas do AWS Outposts. É possível também configurar conectividade híbrida entre um Outpost e um resolver de DNS on-premis es quando você implanta endpoints de entrada e de saída.	
Rotas de entrada do gateway local	Você pode criar e modificar rotas de entrada de gateway local para interfaces de rede elásticas em seu Outpost.	15 de setembro de 2022
Apresentando o roteament o direto de VPC para AWS Outposts	Usa o endereço IP privado das instâncias na sua VPC para facilitar a comunicação com a sua rede on-premises.	14 de setembro de 2022
Guia AWS Outposts do usuário criado para Outposts rack	AWS Outposts O Guia do Usuário foi dividido em guias separados para rack e servidores.	14 de setembro de 2022
Criar e gerenciar tabelas de rotas de gateway local	Crie e modifique tabelas de rotas de gateway local e grupos de CoIP. Gerencie associações de grupos VIF.	14 de setembro de 2022
Grupos de colocação em AWS Outposts	Grupos de posicionamento que usam uma estratégia de distribuição podem distribuir instâncias entre os hosts.	30 de junho de 2022
Anfitriões dedicados em AWS Outposts	Agora você pode usar hosts dedicados no Outposts.	31 de maio de 2022

Sites compartilhados do Outpost	Crie e gerencie sites do Outpost e compartilhe-os com outras AWS contas em sua organização.	18 de outubro de 2021
Nova CloudWatch dimensão	Uma nova CloudWatch dimensão para métricas no AWS Outposts namespace.	13 de outubro de 2021
Compartilhar buckets do S3	Compartilhe e gerencie buckets do S3 em seu Outpost.	5 de agosto de 2021
Suporte para alguns grupos de posicionamento	Você pode usar estratégi as de colocação de cluster, partição ou disseminação da mesma forma que faria em uma região.	28 de julho de 2021
CloudWatch Métricas adicionai s	CloudWatch Métricas adicionai s estão disponíveis para instâncias reservadas.	24 de maio de 2021
Lista de verificação de solução de problemas de rede	Uma lista de verificação de solução de problemas de rede está disponível.	22 de fevereiro de 2021
CloudWatch Métricas adicionai s	CloudWatch Métricas adicionai s para volumes do EBS estão disponíveis.	2 de fevereiro de 2021
Atualizações de pedidos do console	O processo de pedidos do console foi atualizado.	14 de janeiro de 2021
Conectividade privada	Você pode selecionar a opção de conectividade privada ao criar seu Outpost no console do AWS Outposts .	21 de dezembro de 2020

Lista de verificação de prontidão da rede	Use essa lista de verificação quando estiver reunindo as informações para a configura ção do Outpost.	28 de outubro de 2020
AWS Outposts Recursos compartilhados	Com o compartilhamento do Outpost, os proprietários do Outpost podem compartilhar seus recursos do Outposts e do Outpost, incluindo tabelas de rotas de gateway locais, com outras AWS contas da mesma organização. AWS	15 de outubro de 2020
CloudWatch Métricas adicionai s	CloudWatch Métricas adicionai s para contagens de tipos de instâncias estão disponíveis.	21 de setembro de 2020
CloudWatch Métrica adicional	Uma CloudWatch métrica adicional para o status de conexão do link de serviço está disponível.	11 de setembro de 2020
Suporte para compartilhar endereços IPv4 pertencentes ao cliente	Use AWS Resource Access Manager para compartilhar endereços IPv4 de proprieda de do cliente.	20 de abril de 2020
CloudWatch Métricas adicionai s	CloudWatch Métricas adicionai s para volumes do EBS estão disponíveis.	4 de abril de 2020
Lançamento inicial	Esta é a versão inicial do AWS Outposts.	3 de dezembro de 2019

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.