Guia do usuário para servidores

AWS Outposts

AWS Outposts: Guia do usuário para servidores

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 e sub-redes do EC2. As instâncias nas sub-redes do Outpost se comunicam com outras instâncias na região da AWS usando endereços IP privados, tudo na 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.

- Você deve instalar um rack ACE se tiver cinco ou mais racks de computação. Se você tem menos de cinco racks de computação, mas planeja expandir para cinco ou mais racks no futuro, recomendamos que você instale um rack ACE o mais rápido possível.

  Para obter informações adicionais sobre racks ACE, consulte Dimensionando implantações de AWS Outposts rack com racks ACE.
- 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

Tipo de recurso	Racks	Servidores
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

Tipo de recurso	Racks	Servidores
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 AWS Outposts funciona

AWS Outposts foi projetado para operar com uma conexão constante e consistente entre seu Posto Avançado e uma AWS região. 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.

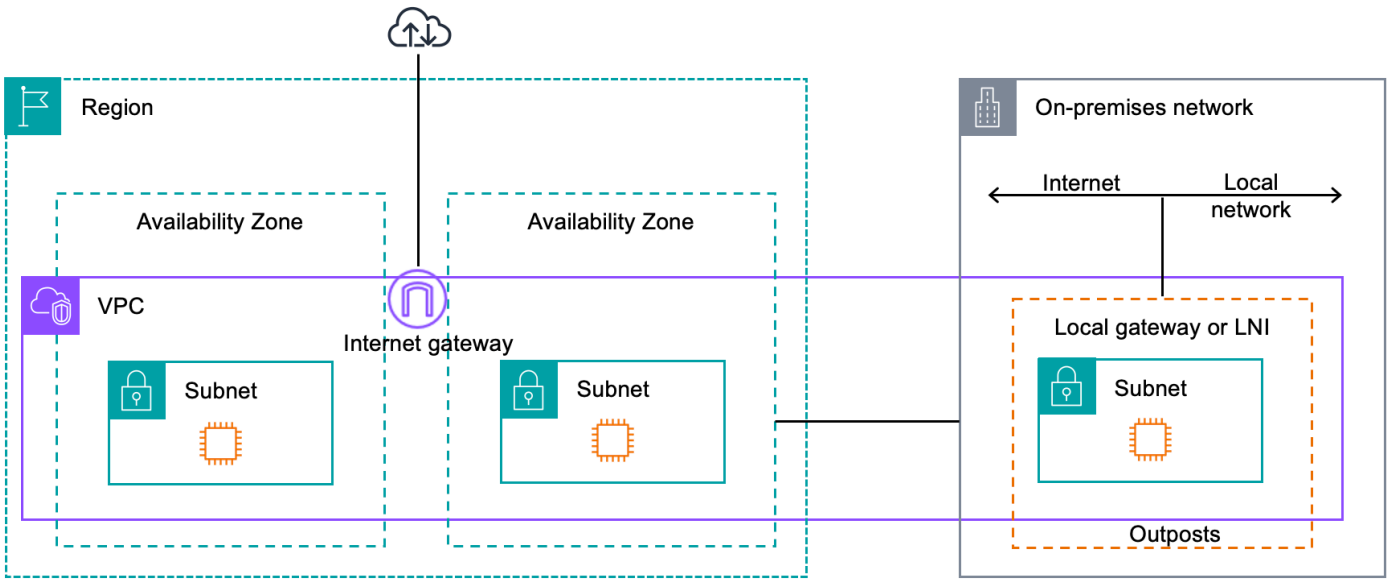
Conteúdo

Componentes da rede

AWS Outposts estende uma Amazon VPC de uma AWS região para um posto avançado com os componentes da VPC que são acessíveis na região, incluindo gateways de internet, gateways privados virtuais, Amazon VPC Transit Gateways e VPC endpoints. 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 local
- 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 pool de AWS capacidade de computação e armazenamento.

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 VPC — AWS define isso 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 regionais — Isso inclui listas de prefixos para Amazon Simple Storage Service (Amazon S3), endpoints de gateway do Amazon DynamoDB, s, gateways privados virtuais AWS Transit Gateway, gateways de 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.

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 AWS região. Portanto, a conectividade do link de serviço do Posto Avançado até a AWS Região deve estar ativa e funcionando para que esses recursos de DNS funcionem.

Você pode encontrar tempos de resolução de DNS mais longos com o Route 53, dependendo da latência do caminho entre seu Outpost e a região. 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 Posto Avançado com a AWS Região escolhida ou a Região de origem do Posto Avançado. 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 Posto Avançado e a AWS Região para o gerenciamento do tráfego do Posto Avançado e do tráfego intra-VPC entre a Região e o Posto Avançado. AWS

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, AWS cria o link de serviço. Para obter mais informações, consulte:

- Conectividade do Outpost com Regiões da AWS
- Roteamento de aplicativos/cargas de trabalho no whitepaper de considerações sobre design e arquitetura AWS Outposts de alta disponibilidade AWS

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 Outpost ou na AWS região. A interface de rede local é destinada apenas a locais on-premises. Para ter mais informações, consulte Interfaces de rede local.

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 servidores AWS Outposts. Consulte a pergunta: em quais países e territórios os servidores Outposts estão disponível?

Esta página aborda os requisitos dos servidores 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 servidores.

> **Note**
>
> As especificações são para servidores em condições operacionais normais. Por exemplo, a acústica pode soar mais alta durante a instalação inicial e, em seguida, operar com a potência sonora nominal após a conclusão da instalação.

- Temperatura: a temperatura ambiente deve estar entre 5 e 35° C (41 e 95° F).

  O servidor será desligado quando a temperatura estiver fora dessa faixa e reiniciará quando a temperatura estiver novamente dentro da faixa.
- Umidade: a umidade relativa deve estar entre 8 e 80% sem condensação.
- Qualidade do ar: o ar deve ser filtrado usando um filtro MERV8 (ou superior).
- Fluxo de ar: a posição do servidor deve garantir uma folga mínima de 15 cm (6 polegadas) entre o servidor e as paredes na frente e atrás do servidor para permitir uma folga suficiente do fluxo de ar.
- Peso: o servidor de 1U pesa 12 kg (26 libras) e o servidor de 2U pesa 16 kg (36 libras). Confirme se o local onde você pretende colocar o servidor pode realmente suportar o peso do servidor.

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

- Compatibilidade com kit de trilhos: o kit de trilhos incluído na embalagem de envio é compatível com um suporte de montagem padrão em forma de L de um rack de 48,3 cm (19 polegadas) compatível com EIA-310-D.

  > **Important**
  >
  > O kit de trilhos não é compatível com um suporte de montagem em forma de U, conforme mostrado na imagem a seguir.

- Posicionamento do rack: recomendamos o uso de racks EIA-310D padrão de 483mm (19 polegadas), com uma profundidade de pelo menos 914 mm (36 polegadas).
  - Os servidores Outposts 2U exigem espaço com as seguintes dimensões: 3,5 polegadas de altura (88,9 mm), 17,5 polegadas de largura (447 mm), 30 polegadas de profundidade (762 mm)
  - Os servidores Outposts 1U exigem espaço com as seguintes dimensões: 1,75 polegadas de altura (44,45 mm), 17,5 polegadas de largura (447 mm), 24 polegadas de profundidade (610 mm)

  > **Note**
  >
  > - A montagem vertical de AWS Outposts servidores não é suportada.
  > - Os servidores Outposts 1U têm a mesma largura dos servidores Outposts 2U, mas metade da altura e menos profundidade

  AWS fornece um kit de trilhos para montagem em rack do servidor. Para ter mais informações, consulte Etapa 3: executar uma tarefa.

  Se você não colocar o servidor em um rack, ainda deverá atender aos outros requisitos listados nesta seção.

- Facilidade de manutenção: os servidores Outposts podem ser reparados no corredor frontal.
- Acústica: avaliada para ser inferior a 78 dBA de potência sonora em temperaturas de 27° C (80° F) e atende à conformidade GR-63 CORE NEBS.
- Suporte sísmico: na medida exigida pela regulamentação ou pelo código, você deverá instalar e manter a ancoragem sísmica e o suporte adequados para o servidor enquanto ele estiver em suas instalações.
- Elevação – A elevação da sala onde o rack está instalado deve estar abaixo de 3.050 metros.

- Limpeza: limpe as superfícies com lenços umedecidos que contenham produtos químicos de limpeza antiestáticos aprovados.

Redes

Cada servidor Outposts inclui não redundantes. As portas têm seus próprios requisitos de velocidade e conector, conforme detalhado abaixo.

Etiqueta de porta	Velocidade	Conector no dispositivo de rede upstream	Tráfego
Porta 3	10 Gbe	SFP+	Tanto o serviço quanto o tráfego de links LNI: o cabo breakout QSFP+ (3 m/10 pés) segmenta o tráfego. Para ter mais informações, consulte Configure a rede QSFP.

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	1024-65535	IP do link de serviço	53	Servidor DNS fornecido pelo DHCP
UDP	443, 1024-65535	IP do link de serviço	443	Pontos finais do Outposts Service Link
TCP	1024-65535	IP do link de serviço	443	Pontos finais de registro de Outposts

Você pode usar uma AWS Direct Connect conexão ou uma conexão pública à Internet para conectar o Posto Avançado à AWS Região. Para conectividade de link de serviço do Outposts, 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.

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 AWS Outposts conectividade com AWS regiões.

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 para a conexão do link de serviço com a região. AWS A utilização máxima para cada servidor do Outpost é de 500 Mbps. Para aumentar a velocidade da conexão, use vários servidores do Outpost. Por exemplo, se você tiver três servidores do AWS Outposts , a velocidade máxima de conexão aumentará para 1,5 Gbps (1.500 Mbps). Para ter mais informações, consulte Tráfego de links de serviço para servidores.

Os requisitos de largura de banda do link de AWS Outposts serviço variam de acordo com as características da carga de trabalho, como tamanho da AMI, elasticidade do aplicativo, necessidades de velocidade de pico e tráfego da Amazon VPC para a região. Observe que os AWS Outposts servidores não armazenam em cache as AMIs. As AMIs são baixadas da região a cada execução da instância.

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

O link de serviço requer resposta DHCP

O link de serviço requer uma resposta DHCP IPv4 para definir as configurações de rede.

Latência máxima do link de serviço

Os links de serviço podem suportar uma latência máxima de rede de 250 ms a partir do servidor e de sua zona de disponibilidade.

Alimentação

Esses são os requisitos de energia para servidores Outposts.

Requisitos

- Suporte de fonte de alimentação
- Consumo de energia
- Cabo de alimentação
- Redundância de energia

Suporte de fonte de alimentação

Os servidores têm potência nominal de até 1600W 90-264 VaC 47/63 Hz de corrente alternada (CA).

Consumo de energia

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

Cabo de alimentação

O servidor vem com um cabo de alimentação IEC C14-C13.

Cabeamento de alimentação do servidor ao rack

Use o cabo de alimentação IEC C14-C13 fornecido para conectar o servidor ao rack.

Cabeamento de alimentação do servidor à tomada

Para conectar o servidor a uma tomada de parede padrão, você deve usar um adaptador para a entrada C14 ou um cabo de alimentação específico do país.

Verifique se você tem o adaptador ou cabo de alimentação correto para sua região para economizar tempo durante a instalação do servidor.

- Nos Estados Unidos, você precisa de um cabo de alimentação IEC C13 para NEMA 5-15P.
- Em partes da Europa, você pode precisar de um cabo de alimentação IEC C13 a CEE 7/7.
- Na Índia, você precisa de um cabo de alimentação IEC C13 a IS1293.

Redundância de energia

Os servidores incluem várias conexões de alimentação e são fornecidos com cabos para permitir a operação redundante de energia. Recomendamos a redundância de energia, mas a redundância não é obrigatória.

Os servidores não incluem um nobreak (fonte de alimentação ininterrupta, UPS).

Atendimento do pedido

Para atender ao pedido, AWS enviaremos o equipamento do servidor Outposts, incluindo suportes de trilhos e cabos de alimentação e de rede necessários, para o endereço que você forneceu. A caixa na qual o servidor é enviado tem as seguintes dimensões:

- Caixa com servidor 2U:
  - Comprimento: 44 polegadas/111,8 cm
  - Altura: 67,3 cm/26,5 polegadas
  - Largura: 43,2 cm/17 polegadas
- Caixa com servidor 1U:
  - Comprimento: 87,6 cm/34,5 polegadas
  - Altura: 61 cm/24 polegadas
  - Largura: 22,9 cm/9 polegadas

Sua equipe ou um fornecedor terceirizado deve instalar o equipamento. Para ter mais informações, consulte Instalação do servidor Outpost.

A instalação é concluída quando você confirma que a capacidade do Amazon EC2 para seu servidor Outposts está disponível em sua conta. 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
- Instalação do servidor Outpost
- Execute uma instância no seu servidor Outpost

Crie um Outpost e solicite capacidade para o Outpost

Para começar a usar AWS Outposts, faça login com a AWS conta que será proprietária do Outpost. Crie um local e um Outpost. Em seguida, faça um pedido para os servidores Outposts de que você precisa.

Pré-requisitos

- Revise as configurações disponíveis para seus servidores 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 .
- Você deve ter um plano AWS Enterprise Support ou um plano AWS Enterprise On-Ramp 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 onde você instalará e executará seus servidores Outposts. Depois de criar o site, AWS Outposts atribui uma ID ao seu site. Você deve especificar esse local ao criar um Outpost.

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 Somente servidores.
7. Insira o nome, a descrição e o endereço operacional do seu local.
8. (Opcional) Para notas do site, insira qualquer outra informação que possa ser útil AWS para conhecer o site.
9. Escolha Criar local.

Etapa 2: Criar um Outpost

Crie um Outpost para cada servidor. Um Outpost só pode ser associado a um único servidor. 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. Selecione Servidores.
4. Digite um nome e uma descrição para o Outpost.
5. Escolha uma zona de disponibilidade para o Outpost.
6. Em ID do local, escolha seu local.
7. Escolha Criar Outpost.

Etapa 3: Fazer o pedido

Faça um pedido dos servidores 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 escolher a opção de pagamento adiantado parcial ou não adiantado, pagará taxas mensais durante o período de três anos.

  O preço inclui entrega 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 Servidores.

4. Para adicionar capacidade, escolha uma configuração.
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. Selecione Next (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

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. Selecione Next (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. Selecione Next (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. Selecione Next (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. Selecione Next (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 agendará uma data de entrega.

Você é responsável por todas as tarefas de instalação, incluindo instalação física e configuração de rede. Você pode contratar um terceiro para realizar essas tarefas para você. Independentemente de você fazer a instalação ou contratar um terceiro, a instalação requer credenciais do IAM no Conta da AWS que contém o Outpost para verificar a identidade do novo dispositivo. Você é responsável por fornecer e gerenciar esse acesso. Para ter mais informações, consulte the section called “Instalação do servidor Outpost”.

A instalação é concluída quando a capacidade do Amazon EC2 para o seu Outpost está disponível em sua Conta da AWS. Depois que a capacidade estiver disponível, você poderá executar instâncias do Amazon EC2 no servidor do Outpost. Para ter mais informações, consulte the section called “Executar uma instância ”.

Instalação do servidor Outpost

Quando você solicita um servidor Outpost, você é responsável pela instalação, seja você mesmo ou contratado por terceiros. A instalação em grupo requer permissões específicas para verificar a identidade do novo dispositivo. Para obter mais informações, consulte Conceder permissões.

Pré-requisito

Você deve ter um fator de forma de servidor Outpost em seu local. Para ter mais informações, consulte Crie um Outpost e solicite capacidade para o Outpost.

> **Note**
>
> Recomendamos que você assista ao vídeo de treinamento de instalação de AWS Outposts servidores antes e durante o processo de instalação. Para acessar o treinamento, você deve entrar ou criar uma conta no AWS Skill Builder.

Tarefas

- Etapa 1: Conceder permissões
- Etapa 2: Inspecionar
- Etapa 3: executar uma tarefa
- Etapa 4: Ligar
- Etapa 5: Conexão à rede
- Etapa 6: Autorizar o servidor
- Referência de comando da Outpost Configuration Tool

Etapa 1: Conceder permissões

Para verificar a identidade do novo dispositivo, você deve ter credenciais do IAM no Conta da AWS que contém o Outpost. A política AWSOutpostsAuthorizeServerPolicy concede as permissões necessárias para instalar um servidor do Outpost. Para ter mais informações, consulte the section called “Gerenciamento de identidade e acesso”.

Considerações

- Se você estiver usando um terceiro que não tem acesso ao seu Conta da AWS, você deve fornecer acesso temporário.
- AWS Outposts suporta o uso de credenciais temporárias. Você pode configurar credenciais temporárias que duram até 36 horas. Certifique-se de dar ao instalador tempo suficiente para executar todas as etapas da instalação do servidor. Para ter mais informações, consulte the section called “Credenciais temporárias”.

Etapa 2: Inspecionar

Para concluir uma inspeção do equipamento do Outposts, você deve verificar se há danos na embalagem de remessa, desempacotar a embalagem de remessa e localizar a Chave de Segurança Nitro (NSK). Considere as seguintes informações para inspecionar o servidor:

- O pacote de remessa tem sensores de choque localizados nos dois lados maiores da caixa.
- A aba interna da embalagem de envio contém instruções sobre como desempacotar o servidor e localizar o NSK.
- O NSK é um módulo de criptografia. Para concluir a inspeção, você localiza o NSK. Em uma etapa posterior, você conecta o NSK ao servidor.

Verifique o pacote de envio

Para inspecionar o pacote de envio

- Antes de abrir a embalagem de envio, observe os dois sensores de choque e observe se eles foram ativados. Se os sensores de choque tiverem sido ativados, é possível que a unidade tenha sido danificada. Prossiga com a instalação, observando quaisquer danos adicionais no servidor ou nos acessórios. Se alguma parte do sistema estiver obviamente danificada ou a instalação falhar conforme o esperado, entre em contato com o AWS Support para obter orientação sobre como substituir seu servidor Outposts.

Se a barra no meio do sensor estiver vermelha, o sensor foi ativado.

Desembale o pacote de envio

Para desempacotar o pacote de envio

- Abra a embalagem e verifique se ela contém os seguintes itens:
  - Servidor
  - Chave de segurança Nitro (módulo de criptografia) — embalagem marcada com “NSK” em vermelho. Consulte o procedimento a seguir para localizar o NSK na embalagem de envio para obter mais informações.
  - Kit de instalação de rack (2 trilhos internos, 2 trilhos externos e parafusos)
  - Panfleto de instalação
  - Kit de acessórios
    - Par de cabos de alimentação C13/14 - 10 pés (3 m)
    - Cabo de fuga QSFP -10 pés (3 m)

- Cabo USB, micro-USB para USB-C - 10 pés (3 m)
- Protetor de escova

Localizar o NSK

A NSK está dentro da caixa A que inclui os acessórios para o servidor.

> **Important**
>
> Não use o NSK para destruir dados no servidor durante a instalação.

O NSK é necessário para ativar o servidor. O NSK também é usado para destruir dados no servidor quando você envia o servidor de volta. Nesta etapa de instalação, ignore as instruções no corpo do NSK, pois essas instruções são para destruir dados.

Etapa 3: executar uma tarefa

Para concluir essa etapa, você deve conectar os trilhos internos ao servidor, os trilhos externos ao rack e, em seguida, montar o servidor no rack. Você precisa de uma chave de fenda Phillips para concluir essas etapas.

Alternativas de montagem em rack

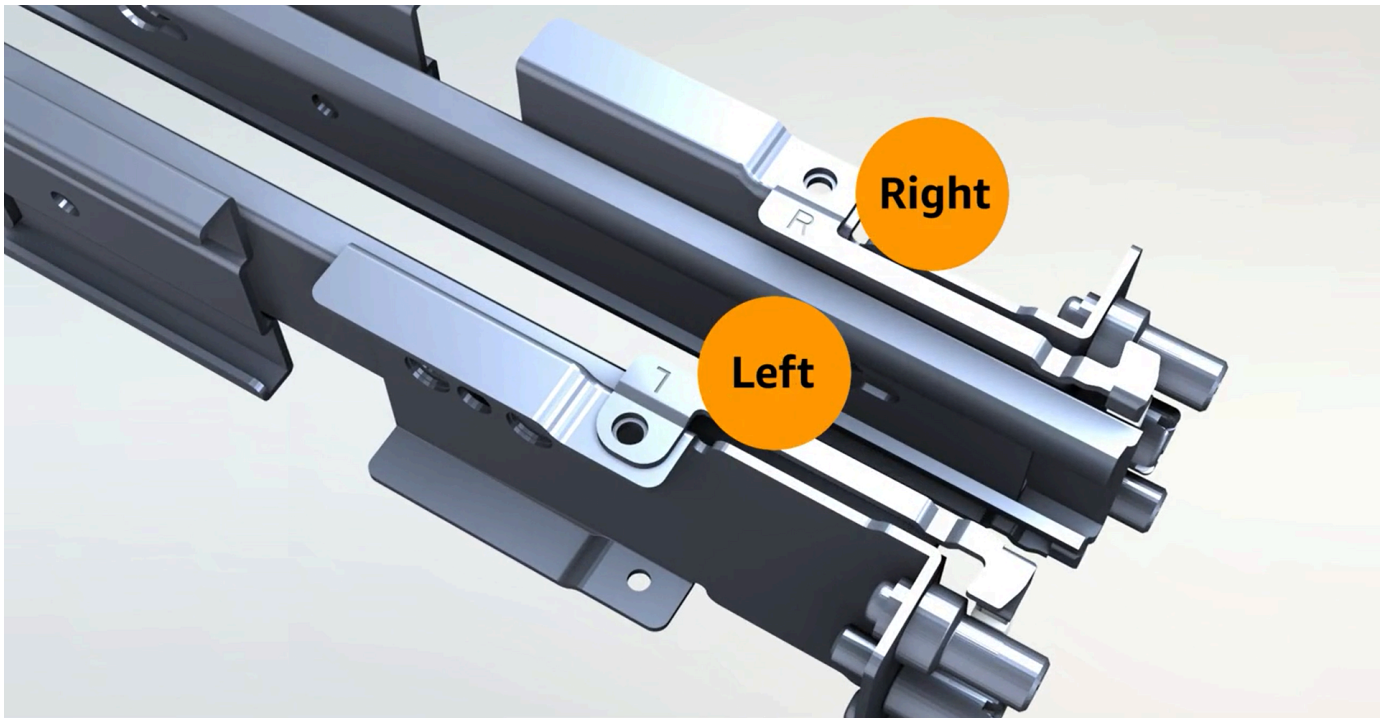
Não é necessário montar o servidor em um rack. Se você não estiver montando o servidor em um rack, considere as seguintes informações:

- Garanta uma folga mínima de 6 polegadas (15 cm) entre o servidor e as paredes na frente e atrás do servidor para permitir que o ar quente circule.
- Coloque o servidor em uma superfície estável, livre de riscos mecânicos, como umidade ou queda de objetos.
- Para usar os cabos de rede incluídos no servidor, você deve colocar o servidor a menos de 10 pés (3 m) do seu dispositivo de rede upstream.
- Siga as orientações locais para reforço e colagem sísmica.

Identifique lados e extremidades

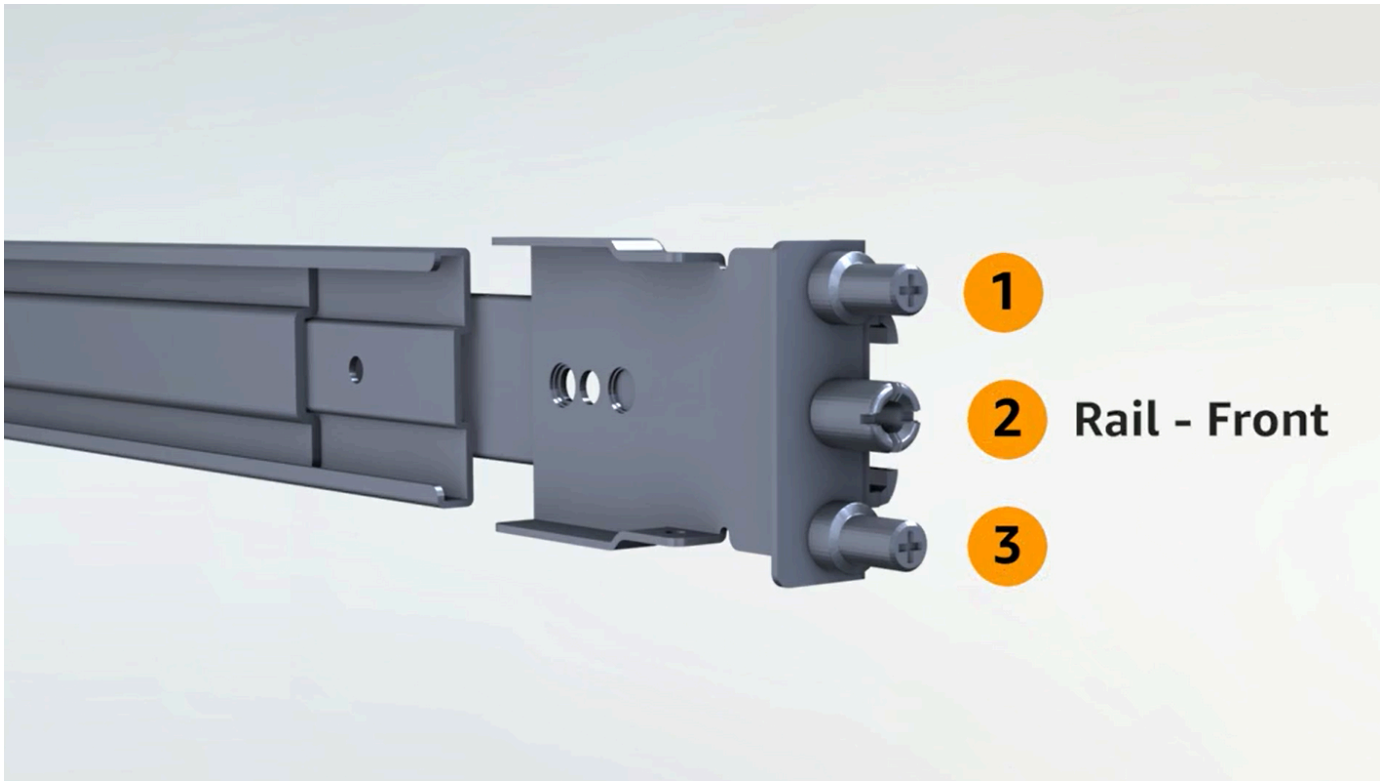
Para identificar a esquerda da direita, da frente para trás

1. Localize e abra a caixa de trilhos de rack que veio com o servidor.
2. Observe as marcações nos trilhos para determinar o que é esquerdo e direito. Essas marcações determinam em qual lado do servidor cada trilho é conectado.

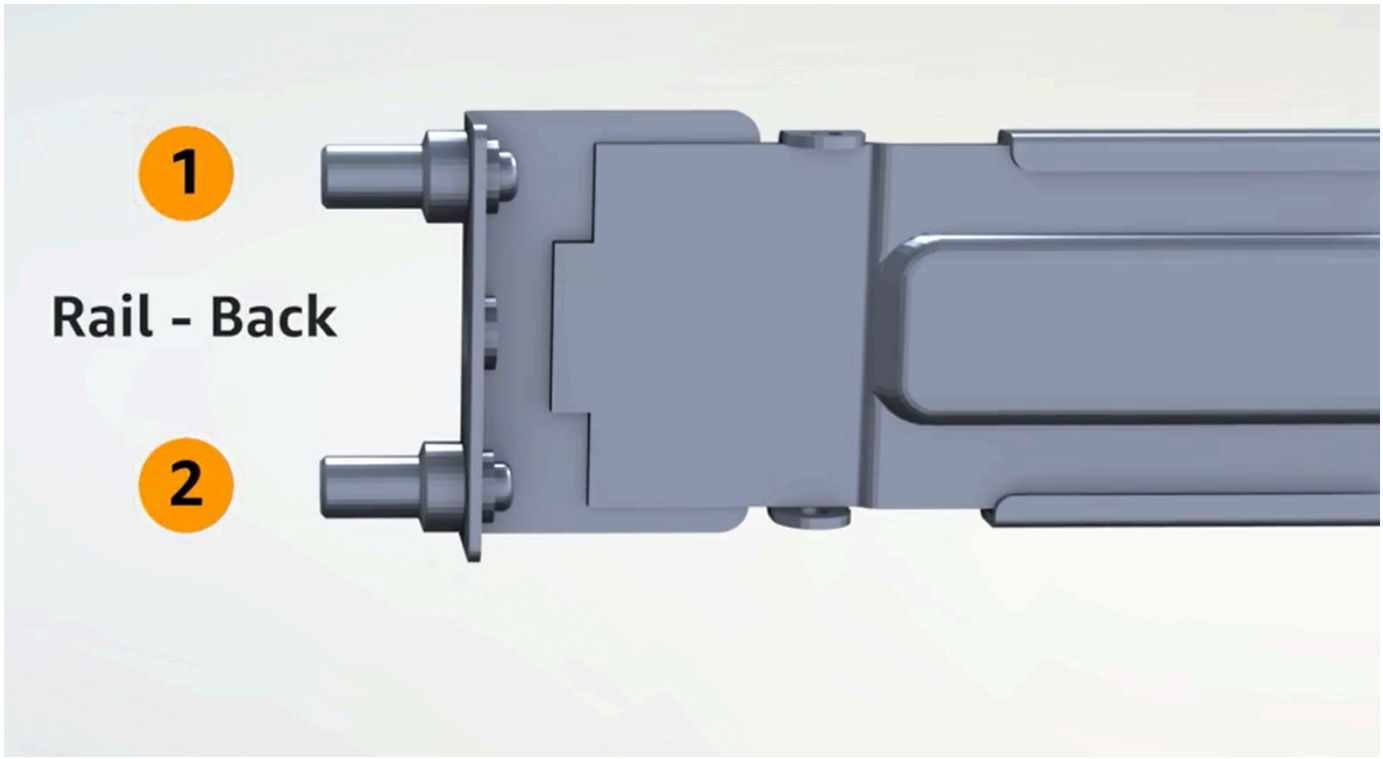


3. Observe os polos em cada extremidade dos trilhos para determinar o que está na frente e o que está atrás.

   O front-end tem três postes.



O back-end tem dois postes.



Anexar rails internos

Para conectar trilhos internos ao servidor

1. Separe o trilho interno do trilho externo para ambos os trilhos. Você deve ter quatro rails.
2. Fixe o trilho interno direito no lado direito do servidor e fixe o trilho com um parafuso. Certifique-se de orientar o trilho corretamente com o servidor. Aponte a parte frontal do trilho em direção à frente do servidor.
3. Fixe o trilho interno esquerdo no lado esquerdo do servidor e fixe o trilho com um parafuso.

Anexar rails externos

Para conectar os trilhos externos ao rack

1. Fique de frente para o rack e use o trilho marcado com R no lado direito do rack. Conecte primeiro a parte traseira do trilho ao rack e, em seguida, estenda o trilho para conectá-lo à frente do rack.

   > **Tip**
   >
   > Preste atenção à orientação dos trilhos. Use os adaptadores de pinos incluídos, se necessário.

2. Repita com o trilho esquerdo no lado esquerdo.

Monte o servidor

Para montar o servidor no rack

- Deslize o servidor nos trilhos externos que você instalou no rack na etapa anterior e fixe o servidor na parte frontal com os dois parafusos fornecidos.

  > **Tip**
  >
  > Use duas pessoas para colocar o servidor no rack.

Etapa 4: Ligar

Para completar a inicialização, conecte o NSK, conecte o servidor a uma fonte de alimentação e verifique se o servidor está ligado. Considere as seguintes informações para ativar o servidor:

- O servidor funciona com uma fonte de alimentação, mas AWS recomenda que você use duas fontes de alimentação para redundância.
- Conecte os cabos de alimentação antes de conectar os cabos de rede.
- Use o par de cabos de alimentação de saída C13 e de entrada C14 para conectar o servidor a uma fonte de alimentação no rack. Se você não estiver usando o cabo de alimentação de entrada C14 para conectar o servidor a uma fonte de alimentação no rack, deverá fornecer adaptadores para as entradas C14 que se conectam a uma fonte de alimentação.

Anexar NSK

Você deve conectar o NSK ao servidor para que ele possa descriptografar dados no servidor durante a operação.

Important

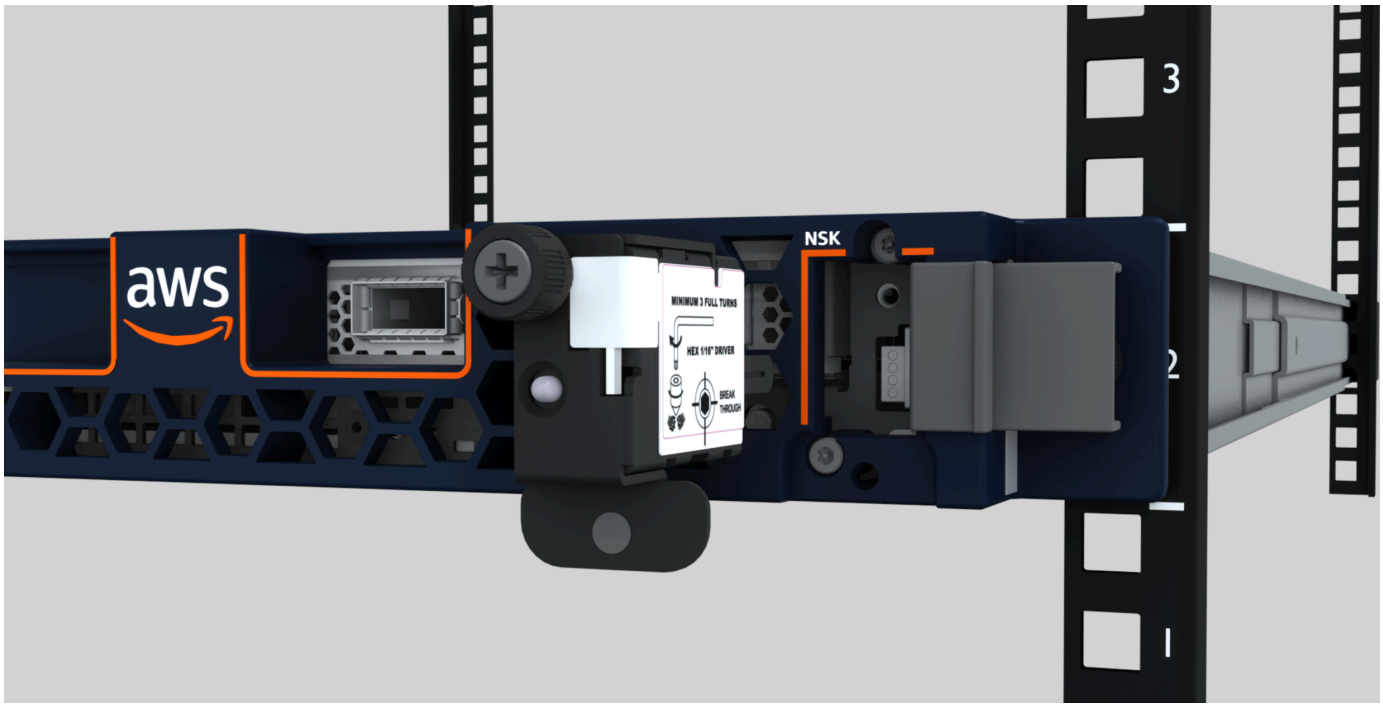
- O lado do NSK tem instruções sobre como destruir o NSK. Não siga essas instruções agora. Siga essas instruções somente ao devolver o servidor para AWS, para destruir criptograficamente os dados no servidor.
- Se você estiver instalando vários servidores ao mesmo tempo, certifique-se de não misturar os NSKs. Você deve conectar o NSK ao servidor com o qual ele foi fornecido. Se você usar um NSK diferente, o servidor não inicializará.

Para anexar o NSK

1. Na parte frontal direita do servidor, abra o compartimento da NSK.

   A imagem a seguir mostra o NSK conectado a um servidor de 2U.

A imagem a seguir mostra o NSK conectado a um servidor de 1U.

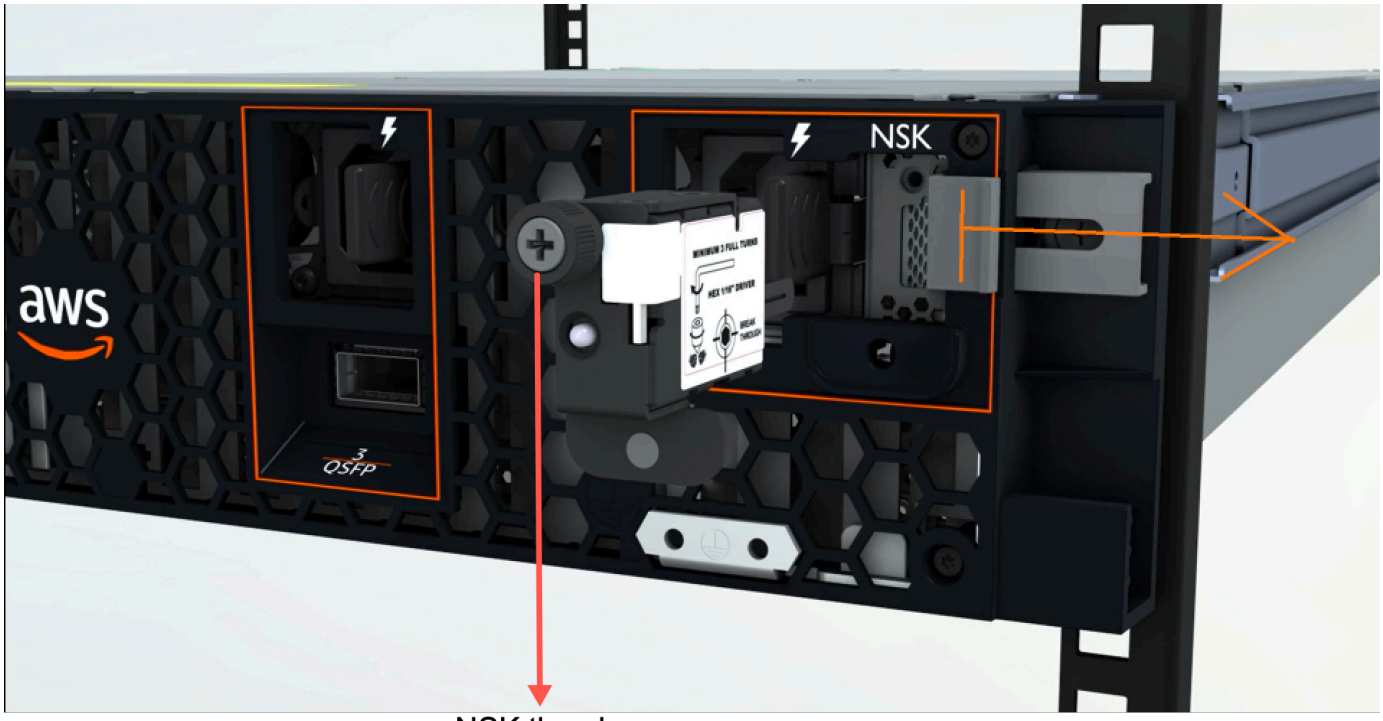


2. Certifique-se de que o número de série (SN) no NSK corresponda ao SN na aba removível do painel do compartimento NSK no servidor.

   A imagem a seguir mostra o número SN no NSK e na aba removível da moldura:

3. Encaixe a NSK no slot.
4. Aperte manualmente usando o parafuso manual ou aperte com uma chave de fenda (0,7 Nm/0,52 lb-ft) até ficar bem ajustado. Não use ferramentas elétricas, pois isso pode causar excesso de torque e danificar o NSK.

   A imagem a seguir mostra a localização do parafuso de aperto.



NSK thumbscrew

A imagem a seguir mostra o tipo de chave de fenda que você pode usar para conectar o NSK ao servidor.

Ativar

Para conectar o servidor à alimentação

1. Localize o par de cabos de alimentação C13/C14 que veio com o servidor.
2. Conecte a extremidade C14 dos dois cabos à sua fonte de alimentação.
3. Conecte a extremidade C13 de ambos os cabos às portas na parte frontal do servidor.

Verifique a potência do servidor

Para verificar se o servidor tem alimentação

1. Verifique se você consegue ouvir o servidor em execução.

   > **Tip**
   >
   > O nível de ruído diminui após o próprio servidor se provisionar.

2. Verifique se as luzes LED de alimentação acima das portas de alimentação estão acesas.

   A imagem a seguir mostra as luzes de alimentação do LED em um servidor de 2U

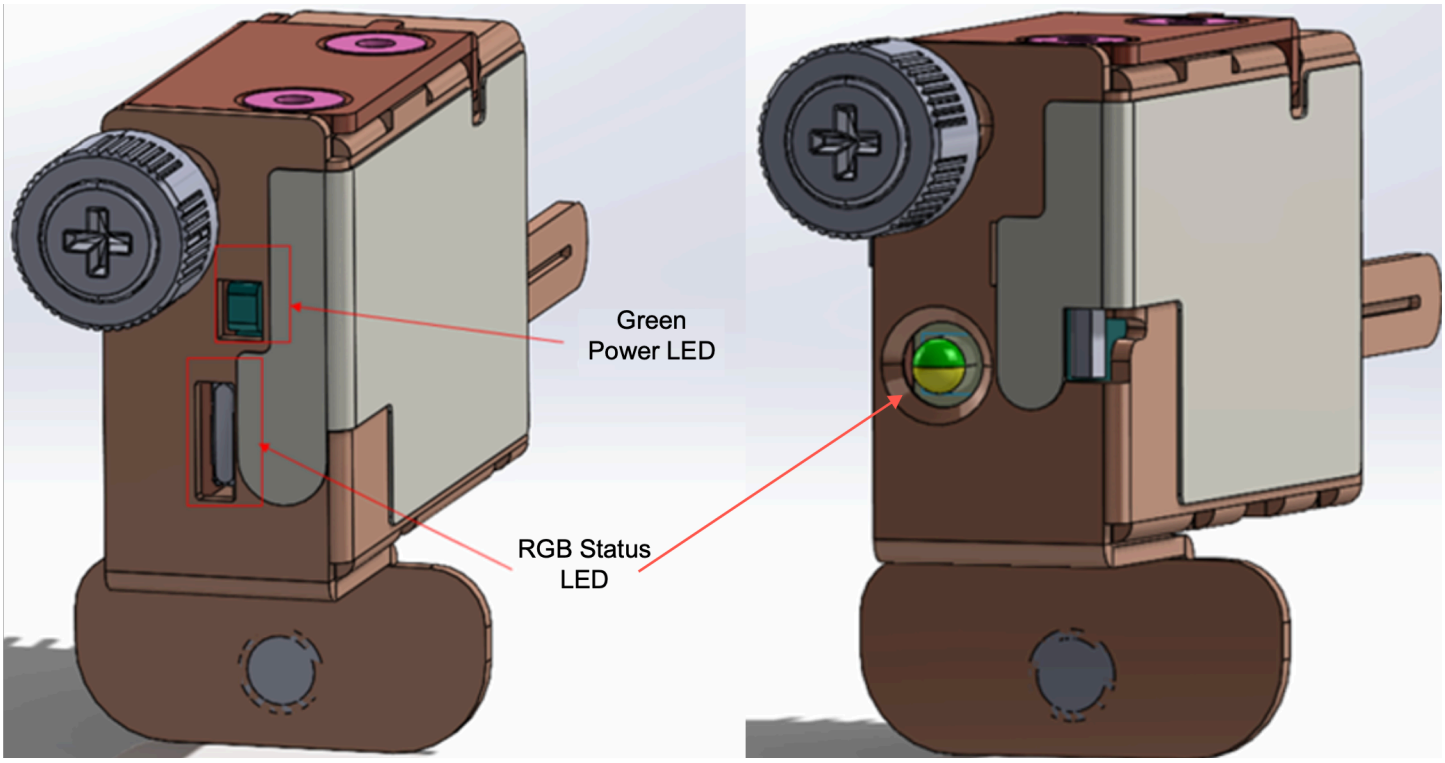
   

   A imagem a seguir mostra as luzes de alimentação do LED em um servidor de 1U

Verifique o LED de alimentação no Atlas 3.0. NSK

AWS Outposts suporta duas versões do NSK: Atlas 2.0 e Atlas 3.0. Ambas as versões do NSK têm um LED de status RGB. Além disso, o Atlas 3.0 tem um LED de alimentação verde. Essa etapa é somente para o Atlas 3.0 NSK.

A imagem a seguir mostra a localização dos LEDs nos NSKs Atlas 2.0 e Atlas 3.0:



Atlas 3.0 Atlas 2.0

Se você tiver o Atlas 2.0 NSK, vá para a próxima etapa, Etapa 5: Conexão à rede pois essa versão do NSK tem apenas o LED de status RGB, que você deve verificar depois que o servidor Outpost for provisionado e ativado.

Se você tiver o Atlas 3.0 NSK, verifique o LED verde de alimentação:

- Se a luz verde estiver acesa, o NSK está conectado corretamente ao host e tem alimentação. Você pode prosseguir para a próxima etapa.
- Se a luz verde estiver apagada, o NSK não está conectado corretamente ao host e/ou não tem alimentação. Contato AWS Support.

Etapa 5: Conexão à rede

Para concluir a configuração da rede, você conecta o servidor ao seu dispositivo de rede upstream com o cabo de rede.

Considere as seguintes informações sobre como se conectar à rede:

- O servidor requer conexões para dois tipos de tráfego: tráfego de link de serviço e tráfego de link de interface de rede local (LNI). As instruções na seção a seguir descrevem quais portas usar no

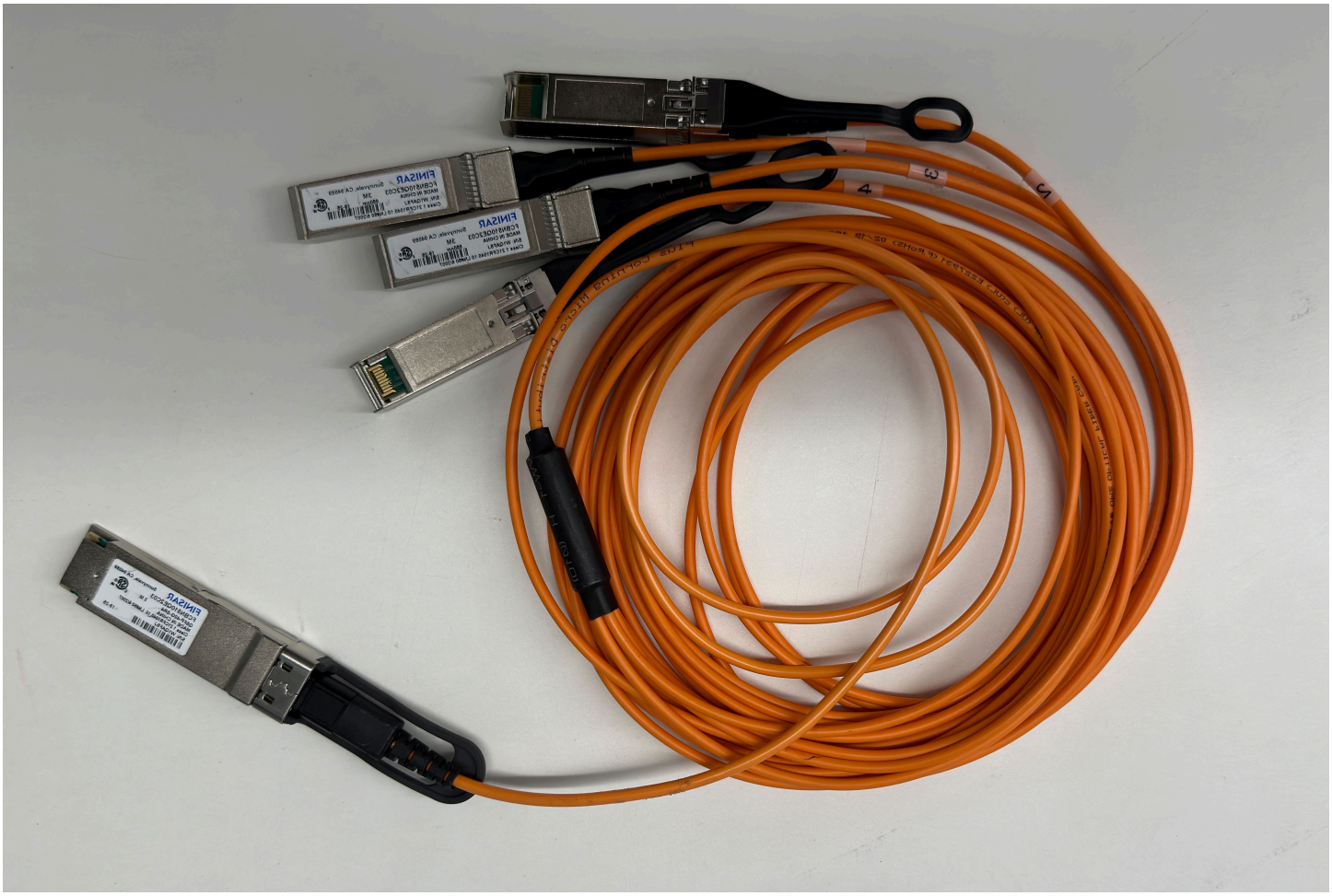
servidor para segmentar o tráfego. Consulte seu grupo de TI para determinar qual porta em seu dispositivo de rede upstream deve transportar cada tipo de tráfego.

- Verifique se o servidor está conectado ao seu dispositivo de rede upstream e se recebeu um endereço IP. Para ter mais informações, consulte Atribuição de endereço IP do servidor.
- A conexão óptica em um AWS Outposts servidor suporta apenas 10 Gbits e não oferece suporte à negociação automática da velocidade da porta. Se a porta do host tentar negociar a velocidade da porta, por exemplo, entre 10 e 25 Gbits, você poderá ter problemas. Nesses casos, recomendamos fazer o seguinte:
  - Defina a velocidade da porta na porta do switch para 10 Gbits.
  - Trabalhe com seu fornecedor de switch para oferecer suporte a uma configuração estática.

Configure a rede QSFP

Com o cabo de breakout QSFP, você usa breakouts para segmentar o tráfego.

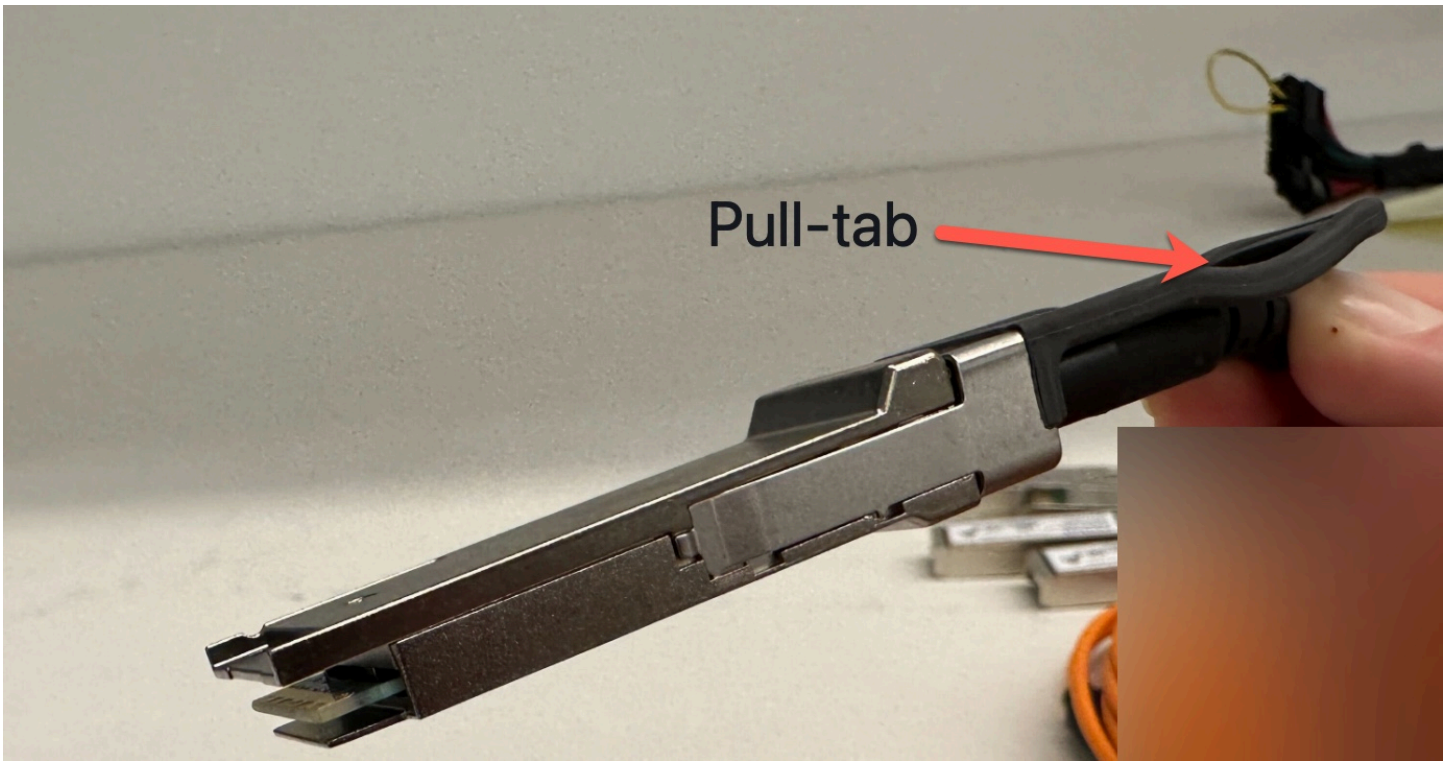
A imagem a seguir mostra o cabo de saída do QSFP:



> **Note**
>
> AWS Outposts os servidores têm uma porta RJ45 física ao lado da porta QSFP. No entanto, essa porta RJ45 não está habilitada para uso de nenhum cliente. Se você precisar de conectividade RJ45 de 1 GbE, use o cabo QSFP incluído para conectar um 10GBASE-X SFP + a um conversor de mídia RJ45 de 1 GbE.

Uma extremidade do cabo QSFP tem um único conector. Conecte essa extremidade ao servidor.

A imagem a seguir mostra a extremidade do cabo com o conector único:



A outra extremidade do cabo QSFP tem 4 cabos de separação rotulados de 1 a 4. Use o cabo rotulado 1 para o tráfego do link LNI e o cabo rotulado 2 para o tráfego do link de serviço.

A imagem a seguir mostra a extremidade do cabo com os 4 cabos de saída:

Para conectar o servidor à rede com o cabo breakout QSFP

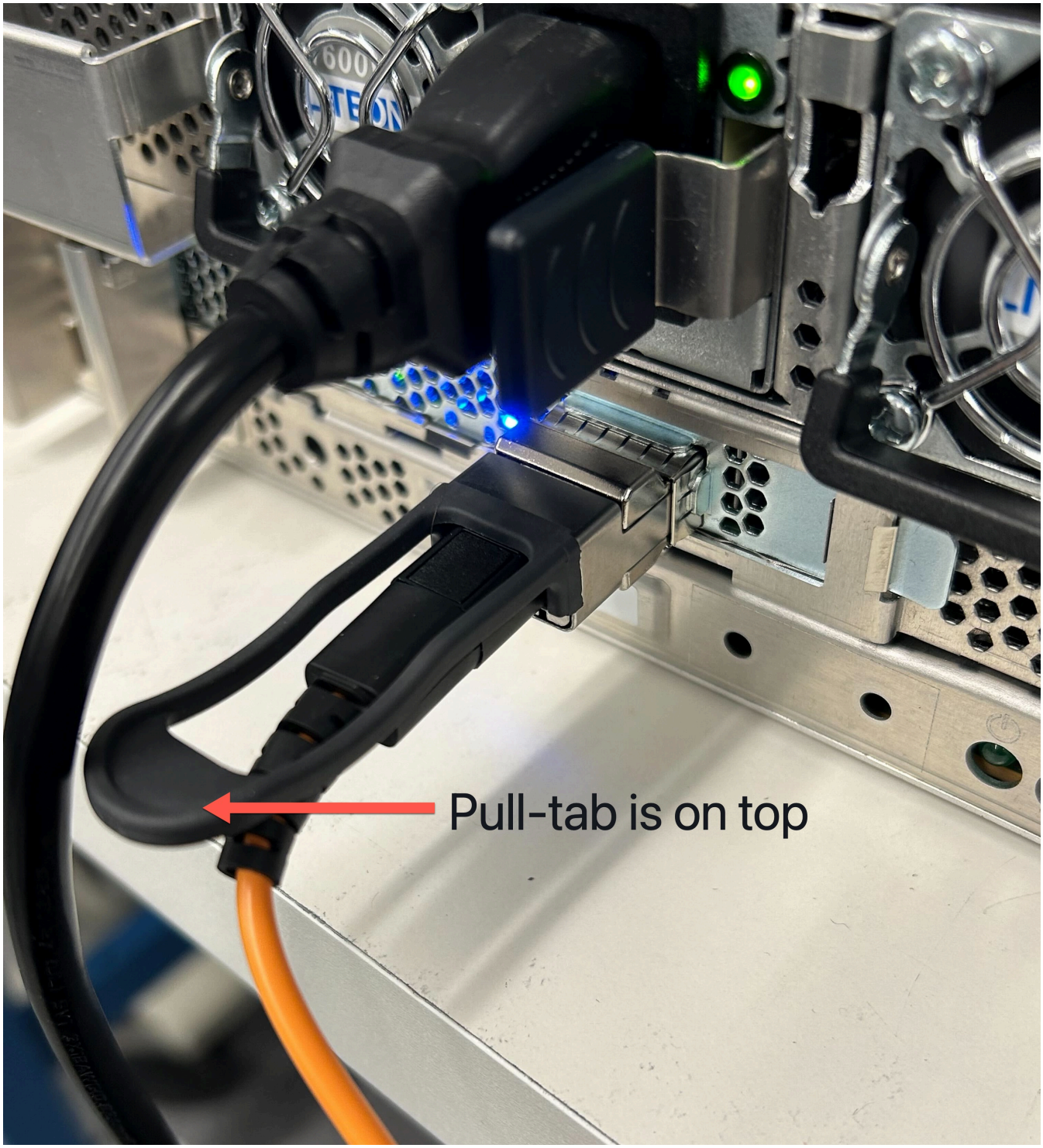
1. Localize o cabo de saída QSFP que veio com o servidor.
2. Conecte a extremidade única do cabo de saída QSFP à porta QSFP no servidor.
    1. Localize a porta QSFP.

        A imagem a seguir mostra a localização da porta QSFP no servidor 2U.

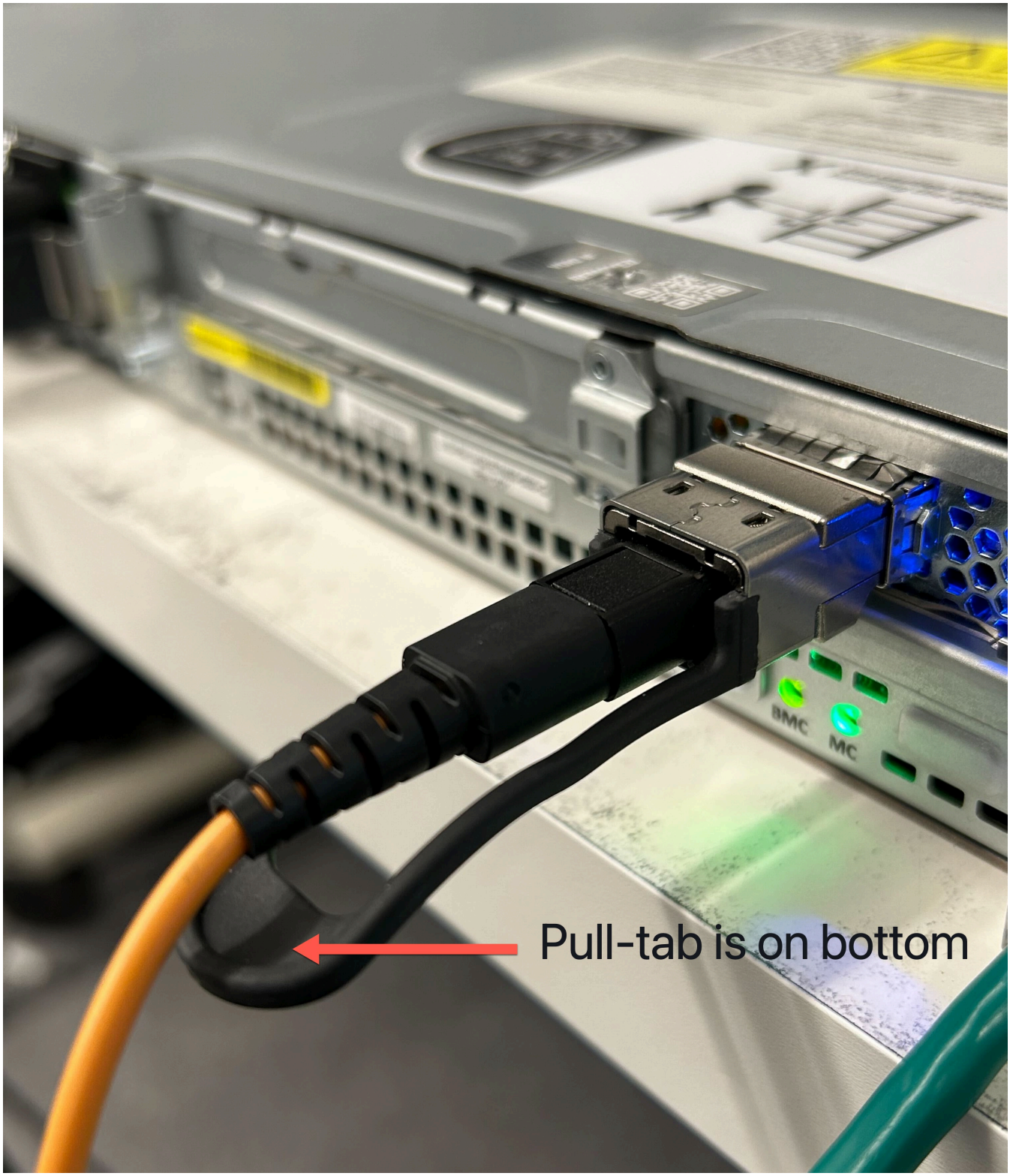
A imagem a seguir mostra a localização da porta QSFP no servidor 1U.

2. Conecte o QSFP com a aba na orientação correta.

   Para o servidor 2U, conecte o QSFP com a guia na parte superior, conforme mostra a imagem a seguir.



Para o servidor 1U, conecte o QSFP com a guia na parte inferior, conforme mostra a imagem a seguir.



3. Certifique-se de sentir ou ouvir um clique ao conectar os cabos. Isso indica que você conectou os cabos corretamente.

3. Conecte os breakouts 1 e 2 do cabo QSFP ao dispositivo de rede upstream.

> **Important**
>
> Os dois cabos a seguir são necessários para que um servidor Outpost funcione.
>
> - Use o cabo identificado como 1 para o tráfego do link LNI.
> - Use o cabo rotulado 2 para o tráfego do link de serviço.

Etapa 6: Autorizar o servidor

Para autorizar o servidor, você deve conectar seu laptop ao servidor com um cabo USB e, em seguida, usar um protocolo serial baseado em comandos para testar a conexão e autorizar o servidor. Além das credenciais do IAM, você precisa de um cabo USB, um laptop e um software de terminal serial, como PuTTY screen ou, para concluir essas etapas.

Como alternativa, se você tiver um telefone ou tablet Android com um conector USB-C ou micro-USB com suporte para USB On The Go (OTG), você pode usar o aplicativo Outposts Server Activator para orientá-lo no processo de autorização do servidor. Você pode baixar o aplicativo no Google Play

Considere as seguintes informações sobre como autorizar o servidor:

- Para autorizar o servidor, você ou a parte que está instalando o servidor precisam de credenciais do IAM no Conta da AWS que contém o Outpost. Para ter mais informações, consulte the section called “Etapa 1: Conceder permissões”.
- Você não precisa se autenticar com as credenciais do IAM para testar sua conexão.
- Considere testar a conexão antes de usar o comando export para definir as credenciais do IAM como variáveis de ambiente.
- Para proteger sua conta, o Outpost Configuration Tool nunca salva suas credenciais do IAM.
- Para conectar seu laptop ao servidor, sempre conecte primeiro o cabo USB ao laptop e depois ao servidor.

Tarefas

- Conecte seu laptop ao servidor
- Crie uma conexão serial com o servidor
- Teste a conexão.

- Autorizar o servidor
- Verifique os LEDs NSK

Conecte seu laptop ao servidor

Conecte o cabo USB ao seu laptop primeiro e depois ao servidor. O servidor inclui um chip USB que cria uma porta serial virtual disponível para você no laptop. Você pode usar essa porta serial virtual para se conectar ao servidor com o software de emulação de terminal serial. Você só pode usar essa porta serial virtual para executar comandos do Outpost Configuration Tool.

Para conectar o laptop ao servidor

Conecte primeiro o cabo USB ao laptop e depois ao servidor.

> **Note**
>
> O chip USB requer drivers para criar a porta serial virtual. Seu sistema operacional deve instalar automaticamente os drivers necessários, caso eles ainda não estejam presentes. Para baixar e instalar os drivers, consulte os Guias de instalação do FTDI.

Crie uma conexão serial com o servidor

Esta seção contém instruções para usar programas populares de terminal serial, mas você não precisa usá-los. Use o programa de terminal serial de sua preferência com uma velocidade de conexão de `115200` baud.

Exemplos

- Conexão serial do Windows
- Conexão serial do Mac

Conexão serial do Windows

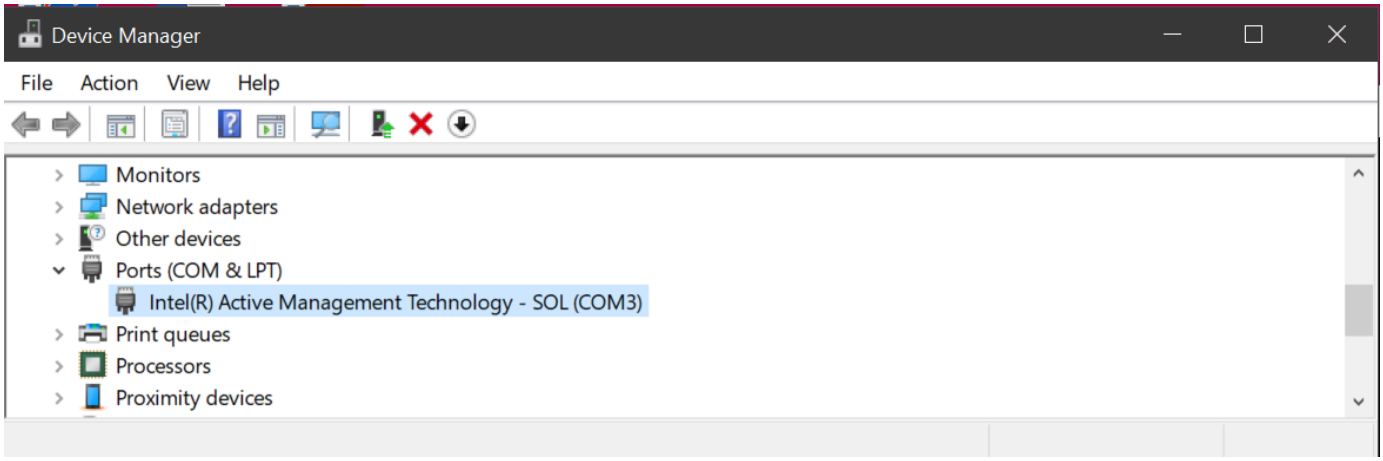
As instruções a seguir são para PuTTY no Windows. O PuTTY é gratuito, mas talvez você precise baixá-lo.

Baixar PuTTY

Faça download e instale o PuTTY pela página de download do PuTTY.

Para criar um terminal serial no Windows usando o PuTTY

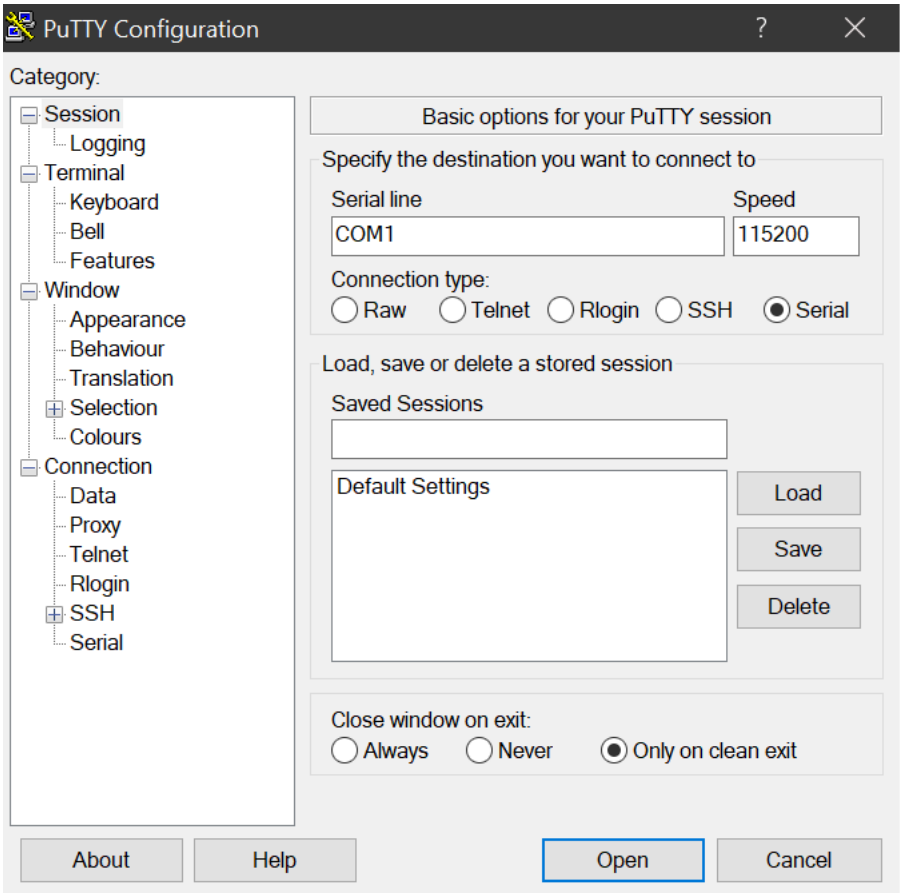
1. Conecte primeiro o cabo USB ao laptop Windows e depois ao servidor.
2. Na área de trabalho, clique com o botão direito do mouse em Iniciar e escolha Gerenciador de dispositivos.
3. No Gerenciador de dispositivos, expanda Portas (COM e LPT) para determinar a porta COM para a conexão serial USB. Você verá um nó chamado Porta serial USB (COM **#**). O valor da porta COM depende do seu hardware.



4. No PuTTY, em Sessão, escolha Serial para o Tipo de conexão e, em seguida, insira as seguintes informações:

   - Em Linha serial, insira a porta COM # no Gerenciador de dispositivos.
   - Em Velocidade, insira: `115200`

   A imagem a seguir mostra um exemplo na página Configuração do PuTTY:



5. Escolha Open (Abrir).

   Uma janela de console vazia é exibida. Pode levar de 1 a 2 minutos para que uma das seguintes opções apareça:

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

Conexão serial do Mac

As instruções a seguir são para screen macOS. Você pode encontrar screen incluído no sistema operacional.

Para criar um terminal serial no macOS usando screen

1. Conecte primeiro o cabo USB ao laptop Mac e depois ao servidor.
2. No Terminal, liste `/dev` com um filtro `*usb*` de saída para encontrar a porta serial virtual.

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

O dispositivo serial aparece como `tty`. Por exemplo, considere a seguinte exemplo de saída do comando list anterior:

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

3. No Terminal, use screen com o dispositivo serial e uma taxa de transmissão da conexão serial para configurar a conexão serial. No comando a seguir, substitua *EXAMPLE1* pelo valor do seu laptop.

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

Uma janela de console vazia é exibida. Pode levar de 1 a 2 minutos para que uma das seguintes opções apareça:

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

Teste a conexão.

Esta seção descreve como usar a Outpost Configuration Tool para testar a conexão. Você não precisa de credenciais do IAM para testar a conexão. Sua conexão precisa ser capaz de resolver o DNS para acessar a Região da AWS.

1. Teste os links e reúna informações sobre a conexão
2. Teste para resolvedor de DNS
3. Teste para acesso ao Região da AWS

Para testar os links

1. Conecte primeiro o cabo USB ao laptop e depois ao servidor.

2. Use um programa de terminal serial, como PuTTY ou screen, para se conectar ao servidor. Para ter mais informações, consulte the section called “Crie uma conexão serial com o servidor”.
3. Pressione Enter para acessar o prompt de comando da Outpost Configuration Tool.

```
Outpost>
```

> **Note**
>
> Se você vir uma luz vermelha persistente dentro do chassi do servidor no lado esquerdo depois de ligar e não conseguir se conectar à Outpost Configuration Tool, talvez seja necessário desligar e drenar o servidor para continuar. Para drenar o servidor, desconecte todos os cabos de rede e alimentação, aguarde cinco minutos, depois ligue e conecte a rede novamente.

4. Use describe-links para retornar informações sobre os links de rede no servidor. Os servidores Outpost devem ter um link de serviço e um link de interface de rede local (LNI).

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

Se você acessar `connected: False` qualquer um dos links, solucione o problema da conexão de rede no hardware.

5. Use describe-ip para retornar o status de atribuição de IP e a configuração do link de serviço.

```
Outpost>describe-ip
---
links:
```

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

O valor do NTP pode estar ausente, pois o NTP é opcional em um conjunto de opções DHCP. Não deve haver nenhum outro valor ausente.

Para testar o DNS

1. Conecte primeiro o cabo USB ao laptop e depois ao servidor.
2. Use um programa de terminal serial, como PuTTY ou screen, para se conectar ao servidor. Para ter mais informações, consulte the section called “Crie uma conexão serial com o servidor”.
3. Pressione Enter para acessar o prompt de comando da Outpost Configuration Tool.

```
Outpost>
```

> **Note**
>
> Se você vir uma luz vermelha persistente dentro do chassi do servidor no lado esquerdo depois de ligar e não conseguir se conectar à Outpost Configuration Tool, talvez seja necessário desligar e drenar o servidor para continuar. Para drenar o servidor, desconecte todos os cabos de rede e alimentação, aguarde cinco minutos, depois ligue e conecte a rede novamente.

4. Use export para inserir a região principal do servidor do Outpost como o valor para `AWS_DEFAULT_REGION`.

   `AWS_DEFAULT_REGION=Region`

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

result: OK
```

```
checksum: 0xB2A945RE
```

- Não inclua um espaço antes ou depois do sinal de igual (=).
- Nenhum valor do ambiente é salvo. Você deve exportar Região da AWS sempre que executar o Outpost Configuration Tool.
- Se você estiver usando um terceiro para instalar o servidor, deverá fornecer ao terceiro a região principal.

5. Use describe-resolve para determinar se o servidor Outpost pode acessar um resolvedor de DNS e resolver o endereço IP do endpoint de configuração do Outpost na região. Requer pelo menos um link com uma configuração IP.

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

Para testar o acesso ao Regiões da AWS

1. Conecte primeiro o cabo USB ao laptop e depois ao servidor.
2. Use um programa de terminal serial, como PuTTY ou screen, para se conectar ao servidor. Para ter mais informações, consulte the section called “Crie uma conexão serial com o servidor”.
3. Pressione Enter para acessar o prompt de comando da Outpost Configuration Tool.

```
Outpost>
```

> **Note**
>
> Se você vir uma luz vermelha persistente dentro do chassi do servidor no lado esquerdo depois de ligar e não conseguir se conectar à Outpost Configuration Tool, talvez seja necessário desligar e drenar o servidor para continuar. Para drenar o servidor, desconecte todos os cabos de rede e alimentação, aguarde cinco minutos, depois ligue e conecte a rede novamente.

4. Use export para inserir a região principal do servidor do Outpost como o valor para `AWS_DEFAULT_REGION`.

   `AWS_DEFAULT_REGION=`*`Region`*

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

   result: OK
   checksum: 0xB2A945RE
   ```

   - Não inclua um espaço antes ou depois do sinal de igual (=).
   - Nenhum valor do ambiente é salvo. Você deve exportar Região da AWS sempre que executar o Outpost Configuration Tool.
   - Se você estiver usando um terceiro para instalar o servidor, deverá fornecer ao terceiro a região principal.

5. Use describe-reachability para determinar se o servidor Outpost pode alcançar o endpoint de configuração do Outpost na região. Requer uma configuração de DNS funcional, que você pode determinar usando describe-resolve.

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

   - `is_reachable` indica o resultado do teste
   - `src_ip` é o endereço IP do servidor
   - `dst_ip` é o endereço IP do endpoint de configuração do Outpost na região
   - `dst_port` é a porta que o servidor usou para se conectar `dst_ip`

Autorizar o servidor

Esta seção descreve como usar o Outpost Configuration Tool e as credenciais do IAM da AWS conta que contém o Outpost para autorizar o servidor.

Para autorizar o servidor

1. Conecte primeiro o cabo USB ao laptop e depois ao servidor.
2. Use um programa de terminal serial, como PuTTY ou screen, para se conectar ao servidor. Para ter mais informações, consulte the section called “Crie uma conexão serial com o servidor”.
3. Pressione Enter para acessar o prompt de comando da Outpost Configuration Tool.

   ```
   Outpost>
   ```

   > **Note**
   >
   > Se você vir uma luz vermelha persistente dentro do chassi do servidor no lado esquerdo depois de ligar e não conseguir se conectar à Outpost Configuration Tool, talvez seja necessário desligar e drenar o servidor para continuar. Para drenar o servidor, desconecte todos os cabos de rede e alimentação, aguarde cinco minutos, depois ligue e conecte a rede novamente.

4. Use export para inserir suas credenciais do IAM na Outpost Configuration Tool. Se você estiver usando um terceiro para instalar o servidor, deverá fornecer a ele as credenciais do IAM.

   Para autenticar, você deve exportar as quatro variáveis a seguir. Exporte uma variável por vez. Não inclua um espaço antes ou depois do sinal de igual (=).

   - `AWS_ACCESS_KEY_ID=`*`access-key-id`*
   - `AWS_SECRET_ACCESS_KEY=`*`secret-access-key`*
   - `AWS_SESSION_TOKEN=`*`session-token`*
     - Use o AWS CLI `GetSessionToken` comando para obter `AWS_SESSION_TOKEN` o. Para obter mais informações, consulte get-session-token na AWS CLI Referência de comando.

       > **Note**
       >
       > Você deve ter o AWSOutpostsAuthorizeServerPolicyanexo à sua função do IAM para obter `AWS_SESSION_TOKEN` o.

     - Para instalar o AWS CLI, consulte Instalando ou atualizando a versão mais recente da AWS CLI no Guia do AWS CLI usuário da versão 2.
   - `AWS_DEFAULT_REGION=`*`Region`*

Use a região principal do servidor Outpost como valor para `AWS_DEFAULT_REGION`. Se você estiver usando um terceiro para instalar o servidor, deverá fornecer a esse terceiro a região principal.

Os exemplos a seguir mostram exportações bem-sucedidas.

```
Outpost>export AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE

result: OK
checksum: example-checksum
```

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

result: OK
checksum: example-checksum
```

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

result: OK
checksum: example-checksum
```

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

result: OK
checksum: example-checksum
```

5. Use start-connection para criar uma conexão segura com a região.

   O exemplo a seguir mostra uma conexão iniciada com sucesso.

```
Outpost>start-connection

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

6. Aguarde cerca de 5 minutos.
7. Use get-connection para verificar se a conexão com a região foi estabelecida.

   A saída do exemplo a seguir mostra uma conexão bem-sucedida.

```
Outpost>get-connection


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

Depois `keys_exchanged` de fazer `connection_established` alteraçõesTrue, o servidor Outpost é automaticamente provisionado e atualizado com o software e a configuração mais recentes.

> **Note**
>
> Observe o seguinte sobre o processo de provisionamento:
>
> - Após a conclusão da ativação, pode levar até 10 horas até que seu servidor Outpost esteja utilizável.
> - Você deve manter a alimentação e a rede do servidor Outpost conectadas e estáveis durante esse processo.
> - É normal que o link do serviço flutue durante esse processo.
> - Se `exchange_active` estiver `True`, a conexão ainda está sendo estabelecida. Tente novamente em cinco minutos.
> - Se `keys_exchanged` ou `connection_established` for `False`, e se `exchange_active` for `True`, a conexão ainda está sendo estabelecida. Tente novamente em cinco minutos.
> - Se `keys_exchanged` ou `connection_established` for `False` depois de uma hora, entre em contato com a Central do AWS Support.
> - Se a mensagem for `primary_status: No such asset id found.` exibida, confirme o seguinte:
>   - Você especificou a região correta.
>   - Você está usando a mesma conta usada para solicitar o servidor Outpost.
>
>   Se a região estiver correta e você estiver usando a mesma conta usada para solicitar o servidor Outpost, entre em contato com a AWS Support Central de contatos.
> - O atributo `LifeCycleStatus` do Outpost passará de `Provisioning` para`Active`. Em seguida, você receberá um e-mail informando que seu servidor Outpost está provisionado e ativado.
> - Você não precisa reautorizar o servidor Outposts após a ativação do servidor Outposts.

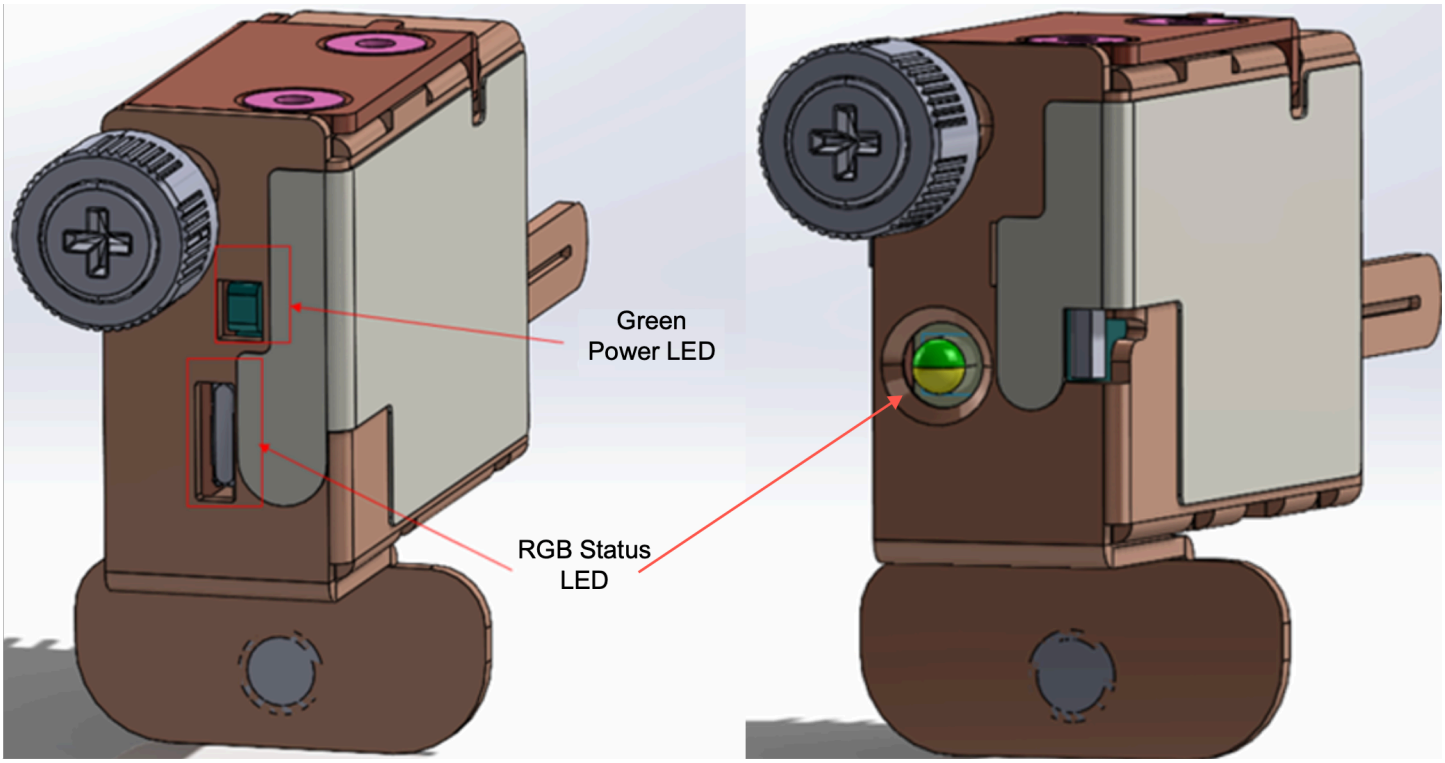
8. Depois de fazer uma conexão bem-sucedida, você pode desconectar seu laptop do servidor.

Verifique os LEDs NSK

Depois que o processo de provisionamento for concluído, verifique os LEDs NSK.

AWS Outposts suporta duas versões do NSK: Atlas 2.0 e Atlas 3.0. Ambas as versões do NSK têm um LED de status RGB. Além disso, o Atlas 3.0 tem um LED de alimentação verde.

A imagem a seguir mostra a localização dos LEDs no Atlas 2.0 e no Atlas 3.0:



Atlas 3.0 Atlas 2.0

Para verificar o status e os LEDs de alimentação no NSK

1. Verifique a cor do LED de status RGB. Se a cor for verde, o NSK está saudável. Se a cor não for verde, entre em contato AWS Support.
2. Se você tiver um Atlas 3.0 NSK, verifique o LED verde de alimentação. Se a luz verde estiver acesa, o NSK está conectado corretamente ao host e tem alimentação. Se a luz verde não estiver acesa, entre em contato AWS Support.

Referência de comando da Outpost Configuration Tool

A Outpost Configuration Tool fornece os seguintes comandos.

Comandos

Export

Export

Use export para definir as credenciais do IAM como variáveis de ambiente.

Sintaxe

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

export usa a declaração de atribuição de variáveis.

Deve usar o seguinte formato: *variable*=*value*

Para autenticar, você deve exportar as quatro variáveis a seguir. Exporte uma variável por vez. Não inclua um espaço antes ou depois do sinal de igual (=).

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

  Use a região principal do servidor Outpost como valor para AWS_DEFAULT_REGION.

Example : importações de credenciais bem-sucedidas

```
Outpost>export AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE
```

```
result: OK
checksum: example-checksum
```

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

result: OK
checksum: example-checksum
```

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

result: OK
checksum: example-checksum
```

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

result: OK
checksum: example-checksum
```

Echo

echo

Use echo para exibir o valor que você definiu para uma variável usando o export comando.

Sintaxe

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

O *variable-name* pode ser um dos seguintes:

- AWS_ACCESS_KEY_ID
- AWS_SECRET_ACCESS_KEY
- AWS_SESSION_TOKEN
- AWS_DEFAULT_REGION

Example : bem-sucedido

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

result: OK
checksum: example-checksum

---

Outpost>echo $AWS_DEFAULT_REGION

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

Example : falha porque o valor da variável não foi definido com o comando export

```
Outpost> echo $AWS_ACCESS_KEY_ID

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

Example : falha porque o nome da variável não é válido

```
Oupost>echo $foo

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

Example : falha devido a um problema de sintaxe

```
Outpost>echo AWS_SECRET_ACCESS_KEY

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

Descrever links

describe-links

Use describe-links para retornar informações sobre os links de rede no servidor. Os servidores Outpost devem ter um link de serviço e um link de interface de rede local (LNI).

Sintaxe

```
Outpost>describe-links
```

describe-links não usa argumentos.

Descreva o IP

describe-ip

Use describe-ip para retornar o status de atribuição de IP e a configuração de cada link conectado.

Sintaxe

```
Outpost>describe-ip
```

describe-ip não usa argumentos.

Descrever a resolução

describe-resolve

Use describe-resolve para determinar se o servidor Outpost pode acessar um resolvedor de DNS e resolver o endereço IP do endpoint de configuração do Outpost na região. Requer pelo menos um link com uma configuração IP.

Sintaxe

```
Outpost>describe-resolve
```

describe-resolve não usa argumentos.

Descrever a acessibilidade

describe-reachability

Use describe-reachability para determinar se o servidor Outpost pode alcançar o endpoint de configuração do Outpost na região. Requer uma configuração de DNS funcional, que você pode determinar usando describe-resolve.

Sintaxe

```
Outpost>describe-reachability
```

describe-reachability não usa argumentos.

Iniciar conexão

conexão inicial

Use start-connection para iniciar uma conexão com o serviço Outpost na região. Esse comando obtém as credenciais do Signature Version 4 (SigV4) das variáveis de ambiente que você carregou com export. A conexão é executada de forma assíncrona e retorna imediatamente. Para verificar o status da conexão, use get-connection.

Sintaxe

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

start-connection usa um índice de conexão opcional para iniciar outra conexão. Os únicos valores válidos são `0` e 1.

Example : conexão iniciada

```
Outpost>start-connection

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

Obter conexão

get-connection

Use get-connection para retornar o status da conexão.

Sintaxe

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

get-connectionusa um índice de conexão opcional para retornar o status de outra conexão. Os únicos valores válidos são `0` e 1.

Example : conexão bem-sucedida

```
Outpost>get-connection


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

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

Nota:

- Se `exchange_active` estiver `True`, a conexão ainda está sendo estabelecida. Tente novamente em cinco minutos.
- Se `keys_exchanged` ou `connection_established` for `False`, e se `exchange_active` for `True`, a conexão ainda está sendo estabelecida. Tente novamente em cinco minutos.

Se o problema persistir após 1 hora, entre em contato com a AWS Support Central.

Execute uma instância no seu servidor Outpost

Depois que o Outpost for instalado e a capacidade de computação e armazenamento estiver disponível para uso, você poderá começar criando recursos. Por exemplo, você pode iniciar instâncias do Amazon EC2.

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 sub-rede
- Etapa 2: Executar uma instância no Outpost
- Etapa 3: Configurar a conectividade
- Etapa 4: Testar a conectividade

Etapa 1: Criar uma sub-rede

Você pode adicionar sub-redes Outpost a qualquer VPC na região para o AWS Outpost. Quando você faz isso, o VPC também abrange 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 2: Executar uma instância no Outpost

Criar uma 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 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 e especifique um intervalo de endereços IP para a sub-rede.
5. Escolha Create.
6. Depois que a sub-rede for criada, habilite a sub-rede para interfaces de rede local.

Etapa 2: Executar 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

- As instâncias nos servidores Outposts incluem volumes de armazenamento de instâncias, mas não volumes do EBS. Escolha um tamanho de instância com armazenamento de instância

suficiente para atender às necessidades do seu aplicativo. Para obter mais informações, consulte Volumes de armazenamento de instâncias, no Guia do Usuário do Amazon EC2.

- Especifique uma AMI com apenas um único snapshot. Não há suporte para AMIs com mais de um snapshot.
- Os dados nos volumes de armazenamento de instâncias persistem após a reinicialização da instância, mas não persistem após o encerramento da instância. Para reter os dados de longo prazo nos volumes de armazenamento de instâncias além da vida útil da instância, faça backup deles em um armazenamento persistente, como um bucket do Amazon S3 ou um dispositivo de armazenamento em rede on-premises.
- Para conectar uma instância em uma sub-rede Outpost à sua rede on-premises, você deve adicionar uma interface de rede local, conforme descrito no procedimento a seguir.

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 Outpost para você e mostramos somente os tipos de instância compatíveis com seus servidores Outposts.
5. Escolha um tipo de instância que seja compatível com seus servidores Outposts.
6. (Opcional) Você pode adicionar uma interface de rede local agora ou depois de criar a instância. Para adicioná-lo agora, expanda Configuração avançada de rede e escolha Adicionar interface de rede. Escolha a sub-rede Outpost. Isso cria uma interface de rede para a instância usando o índice de dispositivo 1. Se você especificou 1 como o índice de dispositivos LNI para a sub-rede Outpost, essa interface de rede será a interface de rede local da instância.
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

Etapa 3: Configurar a conectividade

Se você não adicionou uma interface de rede local à sua instância durante a execução da instância, faça isso agora. Para obter mais informações, consulte Adicionar um LNI após o lançamento.

Você deve configurar a interface de rede local para a instância com um endereço IP da sua rede local. Normalmente, você faz isso usando DHCP. Para obter mais informações, consulte a documentação do sistema sendo executado na instância. Procure informações sobre como configurar interfaces de rede adicionais e endereços IP secundários.

Etapa 4: 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 da interface de rede local da instância do Outpost.

```
ping 10.0.3.128
```

O seguinte é 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 Linux, consulte Conecte-se à sua instância Linux no Guia do usuário do Amazon EC2. Para obter

informações sobre como se conectar a uma instância do Windows, consulte Conecte-se à sua instância do Windows no Guia do usuário do Amazon EC2.

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
```

O seguinte é 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
```

O seguinte é 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
```

AWS Outposts conectividade com AWS regiões

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

> **Note**
>
> Você não pode usar conectividade privada para sua conexão de link de serviço que conecta seu servidor Outpost à sua AWS região ou região de AWS Outposts origem.

Conteúdo

Conectividade por meio de links de serviço

Durante o AWS Outposts provisionamento, você AWS cria ou cria uma conexão de link de serviço que conecta seu Posto Avançado à AWS região ou AWS Outposts região de origem escolhida. 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 Posto Avançado e a AWS Região para o gerenciamento do tráfego do Posto Avançado e do tráfego intra-VPC entre a Região e o Posto Avançado. AWS

O Outpost é capaz de criar a VPN do link de serviço de volta para a região AWS por meio da conectividade pública da região. Para fazer isso, o Outpost precisa de conectividade com os intervalos de IP públicos da AWS região, seja por meio da Internet pública ou da interface virtual AWS Direct Connect pública. Essa conectividade pode ser por meio de rotas específicas na VLAN do link de serviço ou por meio de uma rota padrão de 0.0.0.0/0. Para obter mais informações sobre os intervalos públicos para a AWS, consulte AWS Intervalos de endereço IP.

Depois que o link de serviço é estabelecido, o Outpost está em serviço e é gerenciado por AWS. O link de serviço é usado para o seguinte tráfego:

- Tráfego de gerenciamento para o Outpost por meio do link de serviço, incluindo tráfego interno do plano de controle e monitoramento interno de recursos, além de atualizações de firmware e software.
- Tráfego entre o Outpost e quaisquer VPCs associadas, incluindo tráfego do plano de dados do cliente.

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.

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 para a conexão do link de serviço com a região. AWS A utilização máxima para cada servidor do Outpost é de 500 Mbps. Para aumentar a velocidade da conexão, use vários servidores do Outpost. Por exemplo, se você tiver três servidores do AWS Outposts , a velocidade máxima de conexão aumentará para 1,5 Gbps (1.500 Mbps). Para ter mais informações, consulte Tráfego de links de serviço para servidores.

Os requisitos de largura de banda do link de AWS Outposts serviço variam de acordo com as características da carga de trabalho, como tamanho da AMI, elasticidade do aplicativo, necessidades de velocidade de pico e tráfego da Amazon VPC para a região. Observe que os AWS Outposts servidores não armazenam em cache as AMIs. As AMIs são baixadas da região a cada execução da instância.

Para receber uma recomendação personalizada sobre a largura de banda do link de serviço necessária para suas necessidades, entre em contato com seu representante de AWS vendas ou parceiro da 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 AWS região até o Outpost. Uma interface virtual AWS Direct Connect pública 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 AWS região de volta ao Posto Avançado, 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	1024-65535	IP do link de serviço	53	Servidor DNS fornecido pelo DHCP
UDP	443, 1024-65535	IP do link de serviço	443	AWS Outposts Endpoints do Service Link
TCP	1024-65535	IP do link de serviço	443	AWS Outposts Pontos finais de registro

> **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.

Atualizações e o link de serviço

AWS mantém uma conexão de rede segura entre seu servidor Outpost e sua AWS região mãe. Essa conexão de rede, chamada de link de serviço, é essencial para gerenciar o Outpost, fornecendo tráfego intra-VPC entre o Outpost e a Região. AWS AWS As melhores práticas da Well-Architected recomendam a implantação de aplicativos em dois Outposts vinculados a diferentes zonas de disponibilidade com um design ativo-ativo. Para obter mais informações, consulte Considerações sobre design e arquitetura de AWS Outposts alta disponibilidade.

O link de serviço é atualizado regularmente para manter a qualidade e o desempenho operacionais. Durante a manutenção, você pode observar breves períodos de latência e perda de pacotes nessa rede, resultando em impacto nas cargas de trabalho que dependem da conectividade da VPC com recursos hospedados na região. No entanto, o tráfego que atravessa as Interfaces de Rede Local (LNI) não será afetado. Você pode evitar o impacto em seu aplicativo seguindo as melhores práticas da AWS Well-Architected e garantindo que seus aplicativos sejam resilientes a falhas ou atividades de manutenção que afetam um único servidor Outpost.

Conexões redundantes à Internet

Ao criar conectividade do seu Posto Avançado com a AWS Região, recomendamos que você crie várias conexões para maior 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.

Devolver um AWS Outposts servidor

Se AWS Outposts detectar um defeito no servidor, informaremos você, iniciaremos o processo de substituição para enviar um novo servidor e forneceremos a etiqueta de remessa por meio do AWS Outposts console.

Se você quiser devolver o servidor porque ele atingiu o final do prazo do contrato ou por qualquer outro motivo, entre em contato com a AWS Support Central .

Tópicos

As etapas a seguir explicam como devolver um servidor para AWS.

1. Prepare o servidor para devolução

Para preparar o servidor para devolução, cancele o compartilhamento de recursos, faça backup de dados, exclua interfaces de rede local e encerre instâncias ativas.

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 AWS RAM console. Para obter mais informações, consulte Atualização de um compartilhamento de recursos no Guia do usuário do AWS RAM .
   - Use o 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. Crie backups dos dados armazenados no armazenamento de instâncias do Amazon EC2 em execução no AWS Outposts servidor.

3. Exclua as interfaces de rede local associadas às instâncias que estavam sendo executadas no servidor.
4. 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.

2. Obtenha a etiqueta de devolução

> **Important**
>
> Você só deve usar a etiqueta de envio que AWS fornece. Não crie sua própria etiqueta de envio.

Obtenha sua etiqueta de envio com base no motivo da devolução.

Shipping label for a server that is being replaced

1. Abra o AWS Outposts console em https://console.aws.amazon.com/outposts/.
2. No painel de navegação, escolha Pedidos.
3. Em Resumo do pedido de substituição, escolha Imprimir etiqueta de devolução e escolha a ID de configuração do servidor que você planeja devolver.

Shipping label for a server that is not being replaced

1. Entre em contato com a Central AWS Support.
2. Solicite uma etiqueta de envio para o servidor que você pretende devolver.

3. Embale o servidor

Para embalar seu servidor, use a caixa e o material de embalagem em que o servidor veio originalmente. Também é possível usar a caixa na qual o servidor de substituição é entregue. Como alternativa, entre em contato com a Central AWS Support para solicitar uma caixa. Depois de embalar o servidor, afixe a etiqueta de remessa AWS fornecida.

4. Devolva o servidor pelo correio

Você deve devolver o servidor por meio da transportadora designada para o seu país. Você pode entregar o servidor à transportadora ou agendar o dia e a hora de sua preferência para que a transportadora retire o servidor. A etiqueta de remessa AWS fornecida contém o endereço correto para devolver ao servidor.

A tabela a seguir mostra quem contatar no país de onde você está enviando:

País	Contato
Argentina	Entre em contato com a Central AWS Support. Na solicitação, forneça as seguintes informaçõ es: • O número de rastreamento que está na etiqueta AWS de envio fornecida • A data e a hora de sua preferência para a retirada do servidor pela transportadora • Um nome de contato • Um número de telefone • Um endereço de e-mail
Bahrein	
Brasil	
Brunei	
Canadá	
Chile	
Colômbia	
Hong Kong	
Índia	
Indonésia	
Japão	
Malásia	
Nigéria	
Omã	
Panamá	

País	Contato
Peru	
Filipinas	
Sérvia	
Cingapura	
África do Sul	
Coreia do Sul	
Taiwan	
Tailândia	
Emirados Árabes Unidos	
Vietnã	
Estados Unidos da América	Entre em contato com a UPS. Você pode devolver o servidor das seguintes maneiras: • Devolva o servidor durante uma coleta rotineira da UPS em seu local. • Entregue o servidor em um local da UPS. • Agende uma coleta para a data e hora de sua preferência. Insira o número de rastreamento da etiqueta AWS de envio fornecida para frete grátis.

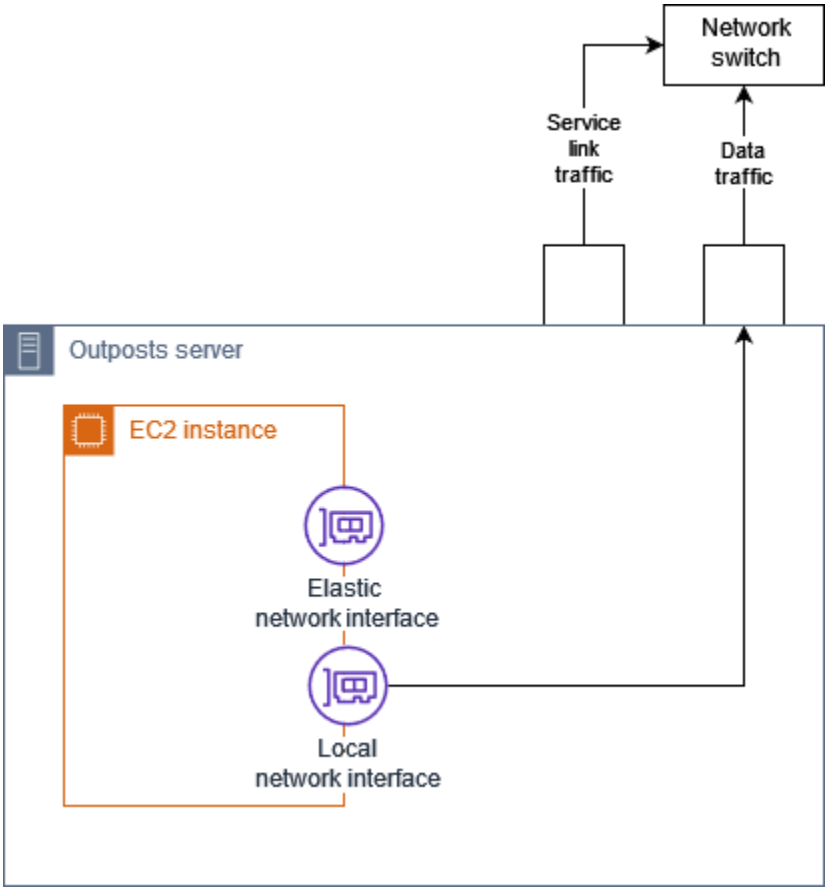
País	Contato
Todos os outros países	Entre em contato com a DHL. Você pode devolver o servidor das seguintes maneiras: • Entregue o servidor em um local da DHL. • Agende uma coleta para a data e hora de sua preferência. Insira o número da DHL Waybill na etiqueta de remessa AWS fornecida para frete grátis. Se você receber o seguinte erro `Courier pickup cannot be scheduled for an import shipment`, isso geralmente significa que o país de coleta selecionado não corresponde ao país de coleta na etiqueta de devolução. Selecione o país de origem da remessa e tente novamente.

Interfaces de rede local

Com AWS Outposts servidores, uma interface de rede local (LNI) é um componente lógico de rede que conecta as instâncias do Amazon EC2 em sua sub-rede Outposts à sua rede local.

Uma interface de rede local é executada diretamente na sua rede local. Com esse tipo de conectividade local, você não precisa de roteadores ou gateways para se comunicar com seu equipamento on-premises. As interfaces de rede local são nomeadas de forma semelhante às interfaces de rede ou interfaces de rede elásticas. Distinguimos entre as duas interfaces sempre usando local quando nos referimos às interfaces de rede locais.

Depois de habilitar as interfaces de rede local em uma sub-rede Outpost, você pode configurar as instâncias do EC2 na sub-rede Outpost para incluir uma interface de rede local além da interface de rede elástica. A interface de rede local se conecta à rede on-premises, enquanto a interface de rede se conecta à VPC. O diagrama a seguir mostra uma instância do EC2 em um servidor Outposts com uma interface de rede elástica e uma interface de rede local.



Você deve configurar o sistema operacional para permitir que a interface de rede local se comunique na sua rede local, assim como faria com qualquer outro equipamento on-premises. Você não pode usar conjuntos de opções DHCP em uma VPC para configurar uma interface de rede local porque uma interface de rede local está sendo executada na sua rede local.

A interface de rede elástica funciona exatamente da mesma forma que funciona para instâncias em uma sub-rede de zona de disponibilidade. Por exemplo, você pode usar a conexão de rede VPC para acessar os endpoints regionais públicos ou usar os endpoints VPC de interface para Serviços da AWS acessar usando. Serviços da AWS AWS PrivateLink Para ter mais informações, consulte AWS Outposts conectividade com AWS regiões.

Conteúdo

Conceitos básicos da interface de rede local

As interfaces de rede local fornecem acesso a uma rede física de camada dois. Uma VPC é uma rede virtualizada de camada três. As interfaces de rede local não oferecem suporte a componentes de rede VPC. Esses componentes incluem grupos de segurança, listas de controle de acesso à rede, roteadores ou tabelas de rotas virtualizados e logs de fluxo. A interface de rede local não fornece ao servidor Outpost visibilidade dos fluxos da camada três da VPC. O sistema operacional host da instância tem visibilidade total dos quadros da rede física. Você pode aplicar a lógica de firewall padrão às informações dentro desses quadros. No entanto, essa comunicação acontece dentro da instância, mas fora do alcance das construções virtualizadas.

Considerações

- As interfaces de rede local oferecem suporte aos protocolos ARP e DHCP. Eles não suportam mensagens gerais de transmissão L2.
- As cotas para interfaces de rede local saem da sua cota para interfaces de rede. Para obter mais informações, consulte Interfaces de rede no Guia do usuário da Amazon VPC.
- Cada instância do EC2 pode ter uma interface de rede local.
- Uma interface de rede local não pode usar a interface de rede primária (eth0) da instância.

- Os servidores Outposts podem hospedar várias instâncias do EC2, cada uma com uma interface de rede local.

> **Note**
>
> As instâncias do EC2 dentro do mesmo servidor podem se comunicar diretamente sem enviar dados para fora do servidor Outposts. Essa comunicação inclui tráfego em uma interface de rede local ou interfaces de rede elástica.

- As interfaces de rede local estão disponíveis somente para instâncias executadas em uma sub-rede Outposts em um servidor Outpost.
- As interfaces de rede local não oferecem suporte ao modo promíscuo ou falsificação de endereços MAC.

Performance

O LNI de cada tamanho de instância fornece uma parte da largura de banda física disponível do LNI de 10 GbE. A tabela a seguir lista o desempenho da rede LNI para cada tipo de instância:

Tipo de instância	Largura de banda da linha de base (Gbps)	Expansão da largura de banda (Gbps)
c6id.large	0,15625	2,5
c6id.large	0,15625	2,5
c6id.xlarge	0,3125	2,5
c6id.2xlarge	0,625	2,5
c6id.4xlarge	1,25	2,5
c6id.8xlarge	2,5	2,5
c6id.12xlarge	3,75	3,75
c6id.16xlarge	5	5
c6id.24xlarge	7,5	7,5

Tipo de instância	Largura de banda da linha de base (Gbps)	Expansão da largura de banda (Gbps)
c6id.32xlarge	10	10
c6gd.medium	0,15625	4
c6gd.large	0,3125	4
c6gd.xlarge	0,625	4
c6gd.2xlarge	1,25	4
c6gd.4xlarge	2,5	4
c6gd.8xlarge	4.8	4.8
c6gd.12xlarge	7,5	7,5
c6gd.16xlarge	10	10

Grupos de segurança

Por padrão, a interface de rede local não usa grupos de segurança em sua VPC. Um grupo de segurança controla o tráfego VPC de entrada e saída. A interface de rede local não é conectada à VPC. A interface de rede local é conectada à sua rede local. Para controlar o tráfego de entrada e saída na interface de rede local, use um firewall ou uma estratégia similar, assim como você faria com o restante do seu equipamento on-premises.

Monitoramento

CloudWatch as métricas são produzidas para cada interface de rede local, assim como são para interfaces de rede elásticas. Para obter mais informações sobre instâncias Linux, consulte Monitore o desempenho da rede para sua instância do EC2 no Guia do usuário do Amazon EC2. Para instâncias do Windows, consulte Monitorar o desempenho da rede para sua instância do EC2 no Guia do usuário do Amazon EC2.

Endereços MAC

AWS fornece endereços MAC para interfaces de rede local. As interfaces de rede local usam endereços administrados localmente (LAA) para seus endereços MAC. Uma interface de rede local usa o mesmo endereço MAC até que você exclua a interface. Depois de excluir uma interface de rede local, remova o endereço MAC das configurações locais. AWS pode reutilizar endereços MAC que não estão mais em uso.

Habilite sub-redes em servidores Outposts para interfaces de rede local

Use o comando modify-subnet-attribute do AWS CLI para habilitar uma sub-rede Outpost para interfaces de rede locais. Você deve especificar a posição da interface de rede no índice do dispositivo. Todas as instâncias executadas em uma sub-rede Outpost habilitada usam essa posição do dispositivo para interfaces de rede local. Por exemplo, um valor de 1 indica que a interface de rede secundária (eth1) de uma instância na sub-rede Outpost é a interface de rede local.

Para habilitar uma sub-rede Outpost para interfaces de rede local

Em um prompt de comando, use o comando a seguir para especificar a posição do dispositivo para a interface de rede local.

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

Trabalhar com interfaces de rede local

Use esta seção para entender como trabalhar com interfaces de rede local.

Tarefas

- Adicionar uma interface de rede local
- Visualizar a interface de rede local
- Configurar o sistema operacional

Adicionar uma interface de rede local

Você pode adicionar uma interface de rede local (LNI) a uma instância do Amazon EC2 em uma sub-rede do Outposts durante ou após a execução. Você faz isso adicionando uma interface de rede secundária à instância, usando o índice de dispositivos que você especificou ao habilitar a sub-rede do Outpost para interfaces de rede local.

Consideração

Quando você especifica a interface de rede secundária usando o console, a interface de rede é criada usando o índice de dispositivos 1. Se esse não for o índice de dispositivos que você especificou ao habilitar a sub-rede Outpost para interfaces de rede local, você pode especificar o índice de dispositivo correto usando o AWS CLI ou um AWS SDK em vez disso. Por exemplo, use os seguintes comandos do AWS CLI: create-network-interface e attach-network-interface.

Para adicionar um LNI durante a execução da instância

1. No assistente de inicialização de instâncias, escolha Editar ao lado de Configurações de rede.
2. Expanda Configuração de rede avançada.
3. Escolha Add network interface (Adicionar interface de rede). Isso cria uma interface de rede usando o índice de dispositivo 1. Se você especificou 1 como o índice de dispositivos LNI para a sub-rede Outpost, essa interface de rede será a interface de rede local da instância.
4. Escolha a sub-rede Outpost e atualize a configuração da interface de rede conforme necessário.
5. Conclua o assistente e execute a instância.

Para adicionar um LNI após a execução da instância

1. No painel de navegação, escolha Rede e segurança, Interfaces de rede.
2. Criar a interface de rede
    a. Clique em Criar interface de rede.
    b. Selecione a mesma sub-rede Outpost da instância.
    c. Verifique se o endereço IPv4 privado está definido como Atribuição automática.
    d. Selecione qualquer grupo de segurança. Os grupos de segurança não se aplicam aos LNIs, portanto, o grupo de segurança selecionado não é relevante.
    e. Clique em Criar interface de rede.

3. Anexar uma interface de rede a uma instância

    a. Marque a caixa de seleção para a interface de rede recém-criada.

    b. Clique em Actions (Ações) e em Attach (Associar).

    c. Escolha a instância.

    d. Escolha Anexar. A interface de rede está conectada no índice de dispositivo 1. Se você especificou 1 como o índice de dispositivos LNI para a sub-rede Outpost, essa interface de rede é a interface de rede local da instância.

Visualizar a interface de rede local

Enquanto a instância estiver em execução, você pode usar o console do Amazon EC2 para visualizar a interface de rede elástica e a interface de rede local das instâncias em sua sub-rede Outpost. Selecione a instância e escolha a guia Redes.

O console exibe um endereço IPv4 privado para o LNI a partir do CIDR da sub-rede. Esse endereço não é o endereço IP do LNI e não pode ser usado. No entanto, esse endereço é alocado do CIDR da sub-rede, portanto, você deve contabilizá-lo no dimensionamento da sub-rede. Você deve definir o endereço IP do LNI no sistema operacional convidado, estaticamente ou por meio do servidor DHCP.

Configurar o sistema operacional

Depois de habilitar as interfaces de rede local, as instâncias do Amazon EC2 terão duas interfaces de rede, uma das quais é uma interface de rede local. Certifique-se de configurar o sistema operacional das instâncias do Amazon EC2 que você executa para suportar uma configuração de rede com várias hospedagens.

Conectividade da rede local para servidores

Use este tópico para entender os requisitos de cabeamento e topologia de rede para hospedar um servidor Outpost. Para ter mais informações, consulte Interfaces de rede local.

Conteúdo

- Tráfego de links de interface de rede local (LNI)
- Atribuição de endereço IP do servidor
- Registro do servidor

Topologia do servidor na sua rede

Um servidor Outpost requer duas conexões distintas com seu equipamento de rede. Cada conexão usa um cabo diferente e transporta um tipo diferente de tráfego. Os vários cabos são apenas para isolamento de classe de tráfego, e não para redundância. Os dois cabos não precisam se conectar a uma rede comum.

A tabela a seguir descreve os tipos e etiquetas de tráfego do servidor Outpost.

Etiqueta de tráfego	Descrição
2	Tráfego do link de serviço — Esse tráfego permite a comunicação entre o Posto Avançado e a AWS Região para o gerenciam ento do Posto Avançado e do tráfego intra-VPC entre a Região e o AWS Posto Avançado. O tráfego do link de serviço inclui a conexão do link de serviço do Outpost à região. O link do serviço é uma VPN ou VPNs personalizadas, desde o Outpost até a região. O Outpost se conecta à zona de disponibilidade na região que você escolheu no momento da compra.
1	Tráfego de link da interface de rede local (LNI): esse tráfego permite a comunicação da VPC com a LAN local pela interface de rede local. O tráfego de links locais inclui instâncias em execução no Outpost que se comunicam com sua rede on-premises. O tráfego de links locais pode incluir instâncias que se comunicam com a Internet com sua rede on-premises.

Conectividade física do servidor

Cada servidor Outpost inclui portas de uplink físicas não redundantes. As portas têm seus próprios requisitos de velocidade e conector, conforme detalhado abaixo:

- 10 Gbe: tipo de conector QSFP+

Cabo QSFP+

O cabo QSFP+ tem um conector que se acopla à porta 3 no servidor Outpost. A outra extremidade do cabo QSFP+ tem quatro interfaces SFP+ que você conecta ao seu switch. Duas das interfaces do lado do switch são rotuladas 1 e 2. Os dois cabos a seguir são necessários para que um servidor do Outpost funcione. Use a interface 2 para tráfego de link de serviço e a interface 1 para tráfego de link LNI. As interfaces restantes não são usadas.

Tráfego de links de serviço para servidores

Configure a porta do link de serviço em seu switch como uma porta de acesso não marcada para uma VLAN com um gateway e uma rota para os seguintes endpoints da região:

- Endpoints do link de serviço
- Endpoint de registro do Outposts

A conexão do link de serviço deve ter um DNS público disponível para que o Outpost descubra seu endpoint de registro na região. AWS A conexão pode ter um dispositivo NAT entre o servidor Outpost e o endpoint de registro. Para obter mais informações sobre os intervalos de endereços públicos para AWS, consulte intervalos de endereços AWS IP no Guia do usuário da Amazon VPC e AWS Outposts endpoints e cotas no. Referência geral da AWS

Para registrar o servidor, abra as seguintes portas de rede:

- TCP 443
- UDP 443
- UDP 53

Velocidade do uplink

Cada servidor Outposts requer uma velocidade mínima de uplink de 20 Mbps para a região AWS .

Você pode precisar de um uplink mais rápido, dependendo da utilização do link LNI e do link de serviço. Para obter mais informações, consulte Recomendações de largura de banda para links de serviço.

Tráfego de links de interface de rede local (LNI)

Configure a porta de link LNI em seu dispositivo de rede upstream como uma porta de acesso padrão a uma VLAN em sua rede local. Se você tiver mais de uma VLAN, configure todas as portas no dispositivo de rede upstream como portas de tronco. Configure a porta em seu dispositivo de rede upstream para esperar vários endereços MAC. Cada instância executada no servidor usará um endereço MAC. Alguns dispositivos de rede oferecem recursos de segurança de porta que desligarão uma porta que relata vários endereços MAC.

> **Note**
>
> AWS Outposts os servidores não marcam o tráfego da VLAN. Se você configurar seu LNI como tronco, deverá garantir que seu sistema operacional identifique o tráfego de VLAN.

O exemplo a seguir mostra como configurar a marcação de VLAN para seu LNI no Amazon Linux 2023. Se estiver usando outra distribuição do Linux, consulte a documentação da sua distribuição do Linux sobre como configurar marcação de VLAN.

Exemplo: para configurar a marcação de VLAN para seu LNI no Amazon Linux 2023 e no Amazon Linux 2

1. Certifique-se de que o módulo 8021q esteja carregado no kernel. Caso contrário, carregue-o usando o comando `modprobe`.

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

2. Crie o dispositivo VLAN. Neste exemplo:

   - O nome da interface do LNI é `ens6`
   - O id da VLAN é `59`
   - O nome atribuído ao dispositivo VLAN é `ens6.59`

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

3. Opcional. Conclua esta etapa se quiser atribuir manualmente o IP. Neste exemplo, estamos atribuindo o IP 192.168.59.205, onde o CIDR da sub-rede é 192.168.59.0/24.

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

4. Ative o link.

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

Para configurar suas interfaces de rede no nível do sistema operacional e tornar persistentes as alterações na marcação da VLAN, consulte os seguintes recursos:

- Se você estiver usando o Amazon Linux 2, consulte Configurar sua interface de rede usando ec2-net-utils para Amazon Linux no Guia do usuário do Amazon EC2.
- Se você estiver usando o Amazon Linux 2023, consulte Serviço de rede no Guia do usuário do Amazon Linux 2023.

Atribuição de endereço IP do servidor

Você não precisa de atribuições de endereços IP públicos para servidores Outpost.

O protocolo de controle dinâmico de host (DHCP) é um protocolo de gerenciamento de rede usado para automatizar o processo de configuração de dispositivos em redes IP. No contexto dos servidores Outpost, você pode usar o DHCP de duas maneiras:

- Placas de rede no servidor
- Interfaces de rede local em instâncias

Para o link de serviço, os servidores Outpost usam DHCP para se conectar à rede local. O DHCP deve retornar servidores de nomes DNS e um gateway padrão. Os servidores Outpost não suportam a atribuição de IP estático do link de serviço.

Para o link LNI, use o DHCP para configurar instâncias a serem conectadas à sua rede local. Para obter mais informações, consulte, the section called “Configurar o sistema operacional”.

> **Note**
>
> Certifique-se de usar um endereço IP estável para o servidor Outpost. Alterações no endereço IP podem causar interrupções temporárias no serviço na sub-rede Outpost.

Registro do servidor

Quando os servidores Outpost estabelecem uma conexão na rede local, eles usam a conexão de link de serviço para se conectar aos endpoints de registro do Outpost e se registrarem. O registro requer DNS público. Quando os servidores se registram, eles criam um túnel seguro para o endpoint do link de serviço na região. Os servidores Outpost usam a porta TCP 443 para facilitar a comunicação com a região pela Internet pública. Atualmente, AWS Outposts os servidores não oferecem suporte à conectividade privada por meio de VPC. Para ter mais informações, consulte the section called “Etapa 6: Autorizar o servidor”.

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 servidores de Outpost. Para recursos de rack, consulte Trabalho com recursos compartilhados do AWS Outposts no Guia do usuário AWS Outposts para racks do Outposts.

- Hosts dedicados alocados – Os consumidores com acesso a este recurso podem:
  - Inicie e execute instâncias do EC2 em um Host dedicado.
- Outposts – Os consumidores com acesso a este recurso podem:
  - Criar e gerenciar sub-redes no Outpost.
  - Usar a API do AWS Outposts para exibir informações sobre o 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 do AWS 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 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 Manual do usuário do AWS 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 .

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 ter mais informações sobre a privacidade de dados, consulte as Perguntas frequentes sobre privacidade de dados. Para ter mais informações sobre a proteção de dados na Europa, consulte a AWS postagem do blog Shared Responsibility Model and GDPR no AWS Blog de segurança da.

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 de rack do Outpost.

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.

Exclusão de dados

Quando você 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. Para obter mais informações, consulte Destrua criptograficamente os dados do servidor.

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

Atributo do IAM	AWS Suporte para Outposts
Políticas baseadas em identidade	Sim
Políticas baseadas em recursos	Não
Ações das políticas	Sim
atributos de políticas	Sim
Chaves de condição de política (específicas do serviço)	Sim
ACLs	Não
ABAC (tags em políticas)	Sim
Credenciais temporárias	Sim

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

Políticas baseadas em identidade para Outposts AWS

Suporta 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 IAM, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e funções podem realizar, em quais recursos e em quais condições. Saiba como criar uma política baseada em identidade consultando Criando 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, assim 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 recursos	Não

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de função do IAM e as políticas do bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, 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 deve especificar uma entidade principal em uma política baseada em recursos. 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 atributo. Adicionar uma entidade principal entre contas à política baseada em atributo 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 atributo conceder acesso a uma entidade principal na mesma conta, nenhuma política baseada em identidade adicional 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 atributos 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 `Resource` de política 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 atributo específico, conhecido como permissões em nível de atributo.

Para ações não compatíveis com permissões no nível de recurso, como operações de listagem, use um 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

Suporta chaves de condição de política específicas de serviço	Sim

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

O elemento `Condition` (ou bloco `Condition`) permite especificar condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. Você pode criar expressões condicionais que usem operadores de condição, como “igual a” ou “menor que”, para corresponder a condição da política aos valores na solicitação.

Se você especificar vários elementos `Condition` em uma instrução ou várias chaves em um único `Condition` elemento, 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 antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um atributo 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 funções da conta) têm permissões para acessar um recurso. As ACLs são semelhantes as políticas baseadas em recursos, 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 atributos 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 estiver 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 a tag no elemento de condição de uma política usando as chaves de condição `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* ou `aws:TagKeys`.

Se um serviço oferecer suporte às três chaves de condição para todo 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 funções, 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 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 IAMhttps://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html 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 Criando um Perfil 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 perfis vinculados 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 de 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 visualizar, mas não pode editar as permissões para funções vinculadas a 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 permissões de usuários para executar ações nos recursos 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

Melhores práticas de política

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 seus 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 AWS Políticas Gerenciadas para Funções 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 atributos 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.
- Utilize 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 gravar 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 Condição de Elementos de Política JSON do IAM no Guia do Usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM para garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam

o idioma de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de 100 verificações de política e ações recomendadas para ajudar você a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação de Política 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 MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte Configurando 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 suportados por funções vinculadas a serviços, consulte Serviços da AWS Suportados pelo IAM e procure os serviços que apresentarem 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 uma função vinculada a 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 uma função vinculada a serviço. Quando você configura a conectividade privada para seu Outpost no AWS Management Console, AWS Outposts cria a função vinculada ao serviço para você.

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 do perfil usando o IAM. Para obter mais informações, consulte Editar uma função vinculada a 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 recursos de sua função vinculada ao serviço antes de excluí-la 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 a função vinculada a 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 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 da 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 mais informações, consulte Políticas gerenciadas pela AWS no Manual 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 política gerenciada: AWSOutpostsAuthorizeServerPolicy

Use esta política para conceder permissões necessárias para autorizar o hardware do servidor do Outpost em sua rede on-premises. Para obter mais informações, consulte Conceder permissões.

Esta política inclui as seguintes permissões:

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

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
AWSOutpostsAuthorizeServerPolicy – Nova política	AWS Outposts adicionou uma política que concede permissões para autorizar o hardware do servidor Outpost em sua rede local.	4 de janeiro de 2023
AWS Outposts começou a rastrear alterações	AWS Outposts começou a rastrear as mudanças em suas políticas AWS gerenciadas.	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 devem ser compatíveis com:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com Perfect Forward Secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, suporta 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.

Resiliência em AWS Outposts

Para alta disponibilidade, você pode e solicitar servidores adicionais 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 alocar 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.

As instâncias nos servidores do Outposts incluem volumes de armazenamento de instâncias, mas não volumes do EBS. Os dados nos volumes de armazenamento de instâncias persistem após a reinicialização da instância, mas não persistem após o encerramento da instância. Para reter os dados de longo prazo nos volumes de armazenamento de instâncias além da vida útil da instância, faça backup deles em um armazenamento persistente, como um bucket do Amazon S3 ou um dispositivo de armazenamento em rede on-premises.

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 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 atributos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços com suporte e controles aceitos, consulte a Referência de controles do Security Hub.
- Amazon GuardDuty — Isso AWS service (Serviço da AWS) detecta possíveis ameaças às suas cargas de trabalho Contas da AWS, contêineres e dados monitorando seu ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de conformidade, como o PCI DSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.
- 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.

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 que`1`, 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`

`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`

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

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

AWS encerra as instâncias afetadas na data de desativação da instância. Os dados nos volumes de armazenamento de instâncias não persistem após o encerramento da instância. Portanto, é importante que você execute uma ação antes da data de desativação da instância. Primeiro, transfira seus dados de longo prazo dos volumes de armazenamento de instâncias de cada instância afetada para o armazenamento persistente, como um bucket do Amazon S3 ou um dispositivo de armazenamento de rede em sua rede.

Um servidor substituto será enviado para o local do Outpost. Então, faça o seguinte:

- Remova os cabos de rede e alimentação do servidor irreparável e, se necessário, remova-o do rack.
- Instale o servidor substituto no mesmo local. Siga as instruções de instalação em Instalação do servidor do Outpost.
- Empacote o servidor irreparável AWS na mesma embalagem em que o servidor substituto chegou.
- Use a etiqueta de devolução pré-paga que está disponível no console anexada aos detalhes de configuração do pedido ou ao pedido do servidor de substituição.
- Retorne o servidor para AWS o. Para obter mais informações, consulte Devolver um servidor do AWS Outposts.

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.

Melhores práticas para eventos AWS Outposts de energia e rede

Conforme declarado nos Termos de AWS Serviço para AWS Outposts clientes, a instalação onde o equipamento Outposts está localizado deve atender aos requisitos mínimos de energia e rede para apoiar a instalação, manutenção e uso do equipamento Outposts. Um servidor de Outposts pode operar corretamente somente quando a energia e a conectividade de rede são ininterruptas.

Eventos de energia

Com quedas de energia completas, há um risco inerente de que um AWS Outposts recurso 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 (liga/desliga) 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 seu Posto Avançado e a AWS Região ou Região de origem do Posto Avançado 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.

Se o link do serviço estiver inativo devido a um problema de energia no local ou à perda de conectividade de rede, AWS Health Dashboard ele 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 do AWS 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 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:

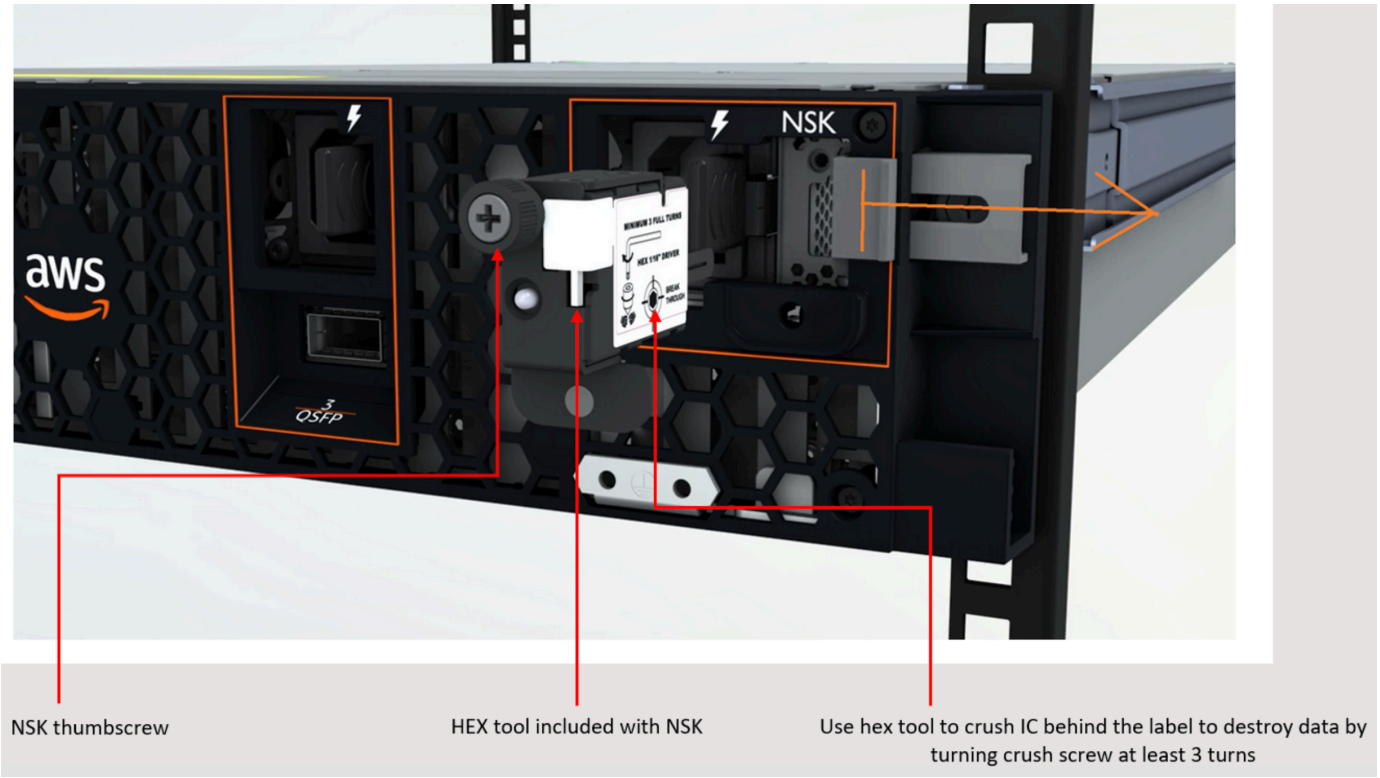
- O AWS blog Monitoring best practices for AWS Outposts aborda as melhores práticas de observabilidade e gerenciamento de eventos específicas para Outposts.
- O AWS blog Ferramenta de depuração para conectividade de rede da Amazon VPC explica a ferramenta -SetupIP VPC. AWSSupport MonitoringFrom Essa 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 AWS região principal e configurada para monitorar uma ou mais de suas instâncias Outpost usando seus IPs privados. Isso fornecerá gráficos de perda de pacotes e latência entre e a região principal. AWS Outposts AWS
- 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 AWS Guia do usuário de suporte.

Destrua criptograficamente os dados do servidor

A chave de segurança Nitro (NSK) é necessária para descriptografar dados no servidor. Quando você retorna o servidor AWS, seja porque está substituindo o servidor ou descontinuando o serviço, você pode destruir o NSK para destruir criptograficamente os dados no servidor.

Para destruir criptograficamente os dados no servidor

1. Remova o NSK do servidor antes de enviar o servidor de volta para AWS.
2. Verifique se você tem o NSK correto que foi fornecido com o servidor.
3. Remova a pequena ferramenta hexagonal/chave Allen de baixo do adesivo.
4. Use a ferramenta hexagonal para girar o pequeno parafuso sob o adesivo três voltas completas. Essa ação destrói o NSK e destrói criptograficamente todos os dados no servidor.


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

AWS Outposts end-of-term opções

No final do seu AWS Outposts mandato, você tem três opções:

- Renove sua assinatura e mantenha seu Outpost existente.
- Encerre sua assinatura e devolva seu servidor Outpost.
- Converta para uma month-to-month assinatura e mantenha seu servidor Outpost existente.

Tópicos

Renove sua assinatura

Para renovar sua assinatura e manter seu servidor 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 saber os preços, consulte os preços dos servidores AWS Outposts. 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.

AWS O Customer Support iniciará o processo de renovação da assinatura. Sua nova assinatura começará no dia seguinte ao término da assinatura atual.

Se você não indicar que deseja renovar sua assinatura ou devolver seu servidor Outpost, você será convertido em uma month-to-month assinatura automaticamente. Seu Outpost será renovado mensalmente de acordo com a taxa da opção de pagamento sem adiantamento que corresponde à sua AWS Outposts configuração. Sua nova assinatura mensal começará no dia seguinte ao término da assinatura atual.

Encerre sua assinatura e devolva o servidor

> **Important**
>
> AWS não pode iniciar o processo de devolução até que você tenha concluído o procedimento 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 deseja encerrar sua assinatura.
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. Se necessário, faça backup de todas as instâncias e dados de instância presentes no seu servidor.
14. Encerre as instâncias lançadas em seu servidor.
15. Revise os detalhes do seu caso e escolha Enviar. O número do ID do caso e o resumo são exibidos.
16. NÃO desligue ou desconecte o servidor da rede até que seja instruído a fazê-lo no caso de suporte.

Para devolver seu AWS Outposts servidor, siga os procedimentos em Devolver um AWS Outposts servidor.

Converter em uma month-to-month assinatura

Para converter para uma month-to-month assinatura e manter seu servidor 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 AWS Outposts configuração. 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 Solicitando 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	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	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
nd-of-term Opções E para AWS Outposts servidores	Ao final do AWS Outposts período, você pode renovar, encerrar ou converter sua assinatura.	1º de agosto de 2023
Guia AWS Outposts do usuário criado para servidores Outposts	AWS Outposts O Guia do Usuário foi dividido em guias separados para rack e servidores.	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
Introdução aos servidores do Outpost	Foram adicionados os servidores Outposts, um novo AWS Outposts formato.	30 de novembro de 2021

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.