Guia do usuário para servidores Outposts

AWS Outposts

AWS Outposts: Guia do usuário para servidores Outposts

Table of Contents

O que AWS Outpostsé

AWS Outposts é um serviço totalmente gerenciado que estende a AWS infraestruturaAPIs, os serviços 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 EC2 instâncias e sub-redes. As instâncias nas sub-redes Outpost se comunicam com outras instâncias na AWS região usando endereços IP privados, tudo dentro da mesma. VPC

> **Note**
>
> Você não pode conectar um Posto Avançado a outro Posto Avançado ou Zona Local que esteja dentro do mesmo. 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 Outposts incluem servidores montáveis em rack, switches, um patch panel de rede, uma prateleira elétrica e painéis vazios.

- Servidores Outposts — Um formato Outpost que é um servidor 1U ou 2U padrão do setor, que pode ser instalado em um rack de 4 postes compatível com -310D 19 padrão. EIA Os servidores Outposts fornecem serviços locais de computação e rede para sites com espaço limitado ou requisitos de capacidade menores.
- Proprietário do Outpost — O proprietário da conta que faz o AWS Outposts pedido. Depois de AWS interagir com o cliente, o proprietário pode incluir pontos de contato adicionais. AWS se comunicará com os contatos para esclarecer pedidos, compromissos de instalação e manutenção e substituição de hardware. AWS Support Centro de contato se as informações de contato mudarem.
- 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 do Outposts e sua rede local.
- Interface de rede local — Uma interface de rede que permite a comunicação entre um servidor Outposts e sua rede local.

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
EC2Instâncias da Amazon	Y (Sim)	Yes (Sim)
ECSClusters da Amazon	Y (Sim)	Yes (Sim)

Tipo de recurso	Racks	Servidores
EKSNodos da Amazon	 Y (Sim)	 Não

Banco de dados e análises

Tipo de recurso	Racks	Servidores
ElastiCache Nós da Amazon (cluster Redis, cluster Memcached)	 Y (Sim)	 Não
EMRClusters da Amazon	 Y (Sim)	 Não
Instâncias de RDS banco de dados da Amazon	 Y (Sim)	 Não

Redes

Tipo de recurso	Racks	Servidores
Proxy Envoy do App Mesh	 Y (Sim)	 Yes (Sim)

Tipo de recurso	Racks	Servidores
Application Load Balancers	 Y (Sim)	 Não
VPCSub-redes da Amazon	 Y (Sim)	 Yes (Sim)
Amazon Route 53	 Y (Sim)	 Não

Armazenamento

Tipo de recurso	Racks	Servidores
EBSVolumes da Amazon	 Y (Sim)	 Não
Buckets do Amazon S3	 Y (Sim)	 Não

Outros Serviços da AWS

Serviço	Racks	Servidores
AWS IoT Greengrass	 Y (Sim)	 Yes (Sim)
Gerenciador Amazon SageMaker Edge	 Y (Sim)	 Yes (Sim)

Definição de preço

O preço é baseado nos detalhes do seu pedido. Ao fazer um pedido, você pode escolher entre uma variedade de configurações do Outpost, cada uma fornecendo uma combinação de tipos de EC2 instância e opções de armazenamento da Amazon. Você também escolhe um termo de contrato e uma opção de pagamento. Os preços incluem o seguinte:

- Racks Outposts — Entrega, instalação, manutenção de serviços de infraestrutura, patches e atualizações de software e remoção de racks.
- Servidores Outposts - Entrega, manutenção de serviços de infraestrutura e patches e atualizações de software. Você é responsável pela instalação e embalagem do servidor para devolução.

Você é cobrado pelos recursos compartilhados e por qualquer transferência de dados da AWS Região para o Posto Avançado. Você também é cobrado pelas transferências de dados realizadas para AWS manter a disponibilidade e a segurança.

Para obter preços com base na localização, configuração e opção de pagamento, consulte:

- Preços dos racks Outposts
- Preços dos servidores Outposts

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 local deve fornecer acesso à rede de área ampla (WAN) de volta à região e à Internet. Ele também deve fornecer LAN ou WAN acessar a rede local em que residem suas cargas de trabalho ou aplicativos locais.

O diagrama a seguir ilustra os dois formatos do Outpost.

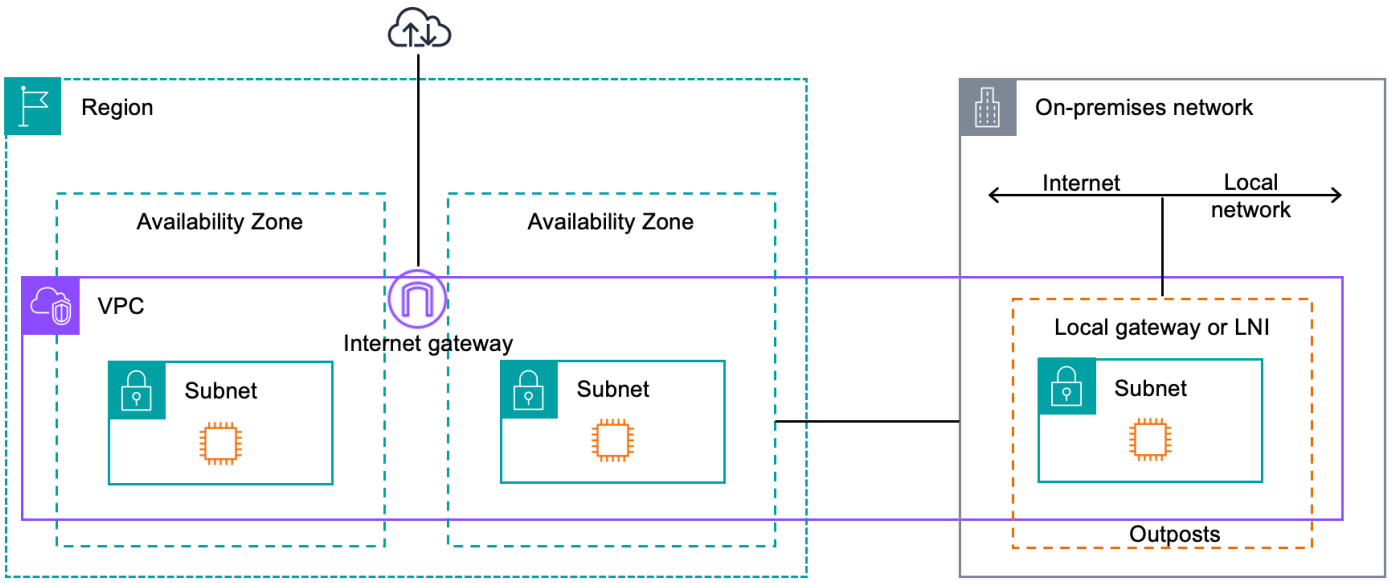
Conteúdo

Componentes da rede

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

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

- Uma Região da AWS e uma rede local
- A 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)



VPCse sub-redes

Uma nuvem privada virtual (VPC) abrange todas as zonas de disponibilidade em sua AWS região. Você pode estender qualquer um VPC na região ao seu Posto Avançado adicionando uma sub-rede do Posto Avançado. Para adicionar uma sub-rede Outpost a umaVPC, especifique o Amazon Resource Name (ARN) do Outpost ao criar a sub-rede.

Os Outposts oferecem suporte a várias sub-redes. Você pode especificar a sub-rede da EC2 instância ao executar a EC2 instância 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 podem ter uma ou mais sub-redes Outpost. Para obter informações sobre VPC cotas, consulte VPCCotas da Amazon no Guia VPC do usuário da Amazon.

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

Roteamento

Por padrão, cada sub-rede 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 Outpost, seja por meio da tabela de rotas principal herdada ou de uma tabela personalizada, herda a rota local. VPC Isso significa que todo o tráfego noVPC, incluindo a sub-rede Outpost com um destino no, VPC CIDR permanece roteado no. VPC

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

- VPCCIDRintervalo — AWS define isso na instalação. Essa é a rota local e se aplica a todo o VPC roteamento, 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 peering. VPC

  Se você tiver uma conexão de emparelhamento com várias VPCs no mesmo Posto Avançado, o tráfego entre elas VPCs permanece no Posto Avançado e não usa o link de serviço de volta para a Região.

DNS

Para interfaces de rede conectadas aVPC, EC2 instâncias em sub-redes Outposts podem usar o Amazon Route 53 DNS Service para resolver nomes de domínio em endereços IP. O Route 53 oferece suporte a DNS recursos, como registro de domínio, DNS roteamento e verificações de saúde para instâncias em execução em 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 em funcionamento para que esses DNS recursos funcionem.

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

redes da Zona de Disponibilidade do VPC tentarão usar os servidores especificados DNS para resolução de nomes. DNS

O registro de consultas não é suportado para DNS consultas originadas de um Posto Avançado.

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 VPN conexões que são usadas sempre que o Outpost se comunica com a região de origem escolhida. Você usa um virtual LAN (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, tanto para o gerenciamento do Posto Avançado quanto para o VPC tráfego interno entre a AWS Região e o Posto Avançado.

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 Outposts incluem uma interface de rede local para fornecer conectividade à sua rede local. 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 EC2 instância em um rack do Outposts ou na AWS região. A interface de rede local é destinada apenas a locais on-premises. Para obter mais informações, consulte Interfaces de rede local para seus servidores Outposts.

Requisitos de site para servidores Outposts

Um local do Outpost é a localização física do seu equipamento Outpost. Os sites estão disponíveis somente em alguns países e territórios. Para obter mais informações, consulte AWS Outposts servidores FAQs. 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 para racks Outposts, consulte Requisitos do site para racks Outposts no Guia do usuário AWS Outposts para racks Outposts.

Conteúdo

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 ferroviário — O kit ferroviário incluído na embalagem de envio é compatível com um suporte de montagem padrão em forma de L de um rack de 19 polegadas compatível com EIA -310-D. 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 19 polegadas, com uma profundidade de pelo menos 36 polegadas (914 mm). AWS fornece um kit de trilhos para montagem em rack do servidor.
  - 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)
  - A montagem vertical de AWS Outposts servidores não é suportada.
  - Os servidores Outposts 1U têm a mesma largura dos servidores Outposts 2U, mas têm metade da altura e menos profundidade

  Se você não colocar o servidor em um rack, ainda deverá atender aos outros requisitos do site.
- 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 80° F (27° C) e atende à conformidade CORE NEBS GR-63.
- 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 tráfego de serviço quanto o tráfego de LNI links — QSFP + o cabo de escape (10 pés/3 m) segmenta o tráfego.

Firewall do link de serviço

UDPe TCP 443 devem estar listados com estado no firewall.

Protocolo	Porta de origem	Endereço de origem	Porta de destino	Endereço de destino
UDP	1024-65535	IP do link de serviço	53	DHCPDNSservidor fornecido
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 máxima de transmissão do link de serviço (MTU)

A rede deve suportar 1500 bytes MTU entre o Outpost e os endpoints do link de serviço na região principal. AWS Para obter mais informações sobre o link do serviço, consulte AWS Outposts conectividade com AWS regiões no guia AWS Outposts do usuário para servidores.

Recomendações de largura de banda do link de serviço

Para uma experiência e resiliência ideais, é AWS necessário que você use conectividade redundante de pelo menos 500 Mbps e uma latência máxima de ida e volta de 175 ms para a conexão do link de serviço com a região. AWS A utilização máxima para cada servidor Outposts é de 500 Mbps. Para aumentar a velocidade da conexão, use vários servidores Outposts. Por exemplo, se você tiver três servidores do AWS Outposts , a velocidade máxima de conexão aumentará para 1,5 Gbps (1.500 Mbps). Para obter mais informações, consulte Tráfego de links de serviço para servidores no guia AWS Outposts do usuário 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 AMI tamanho, elasticidade do aplicativo, necessidades de velocidade de pico e VPC tráfego da Amazon para a região. Observe que os AWS Outposts servidores não armazenam em cacheAMIs. AMIssão baixados da região a cada inicialização 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 AWS de vendas ou APN parceiro.

O link de serviço requer DHCP resposta

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

Latência máxima do link de serviço

Os links de serviço podem suportar uma latência máxima de rede de 175 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

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 IEC alimentação 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 IEC alimentação C13 a 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 IEC C13 para IS1293 alimentar o cabo.

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 uma 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 obter mais informações, consulte Tráfego de links de serviço para servidores no guia AWS Outposts do usuário para servidores.

A instalação é concluída quando você confirma que a EC2 capacidade da Amazon para o seu servidor Outposts está disponível no seu. Conta da AWS

Peça um servidor de Outposts para começar. Após a instalação do seu equipamento Outpost, inicie uma EC2 instância da Amazon e configure a conectividade com sua rede local.

Tarefas

- Crie um Outpost e solicite capacidade para o Outpost
- Inicie uma instância no seu servidor Outposts

Crie um Outpost e solicite capacidade para o Outpost

Para começar a usar AWS Outposts, faça login com sua AWS conta. 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 obter mais informações, consulte Requisitos de site para servidores Outposts.
- Você deve ter um plano AWS Enterprise Support ou um plano AWS Enterprise On-Ramp Support.
- Determine o que Conta da AWS você usará para criar o site 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 em AWS.
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.

> **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 a AWS Support Central.

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 prazo.

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

Etapa 4: modificar a capacidade da instância

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 carregar um JSON arquivo.

Console steps

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

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

Upload JSON file

1. Escolha Carregar uma configuração de capacidade.
2. Escolha Próximo.

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

   Example

   JSONArquivo de exemplo:

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

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

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

Próximas etapas

Você pode ver o status do seu pedido usando o AWS Outposts console. O status inicial do seu pedido é Pedido recebido. Se você tiver alguma dúvida sobre seu pedido, entre em contato com a AWS Support Central.

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. Quer você faça a instalação ou contrate um terceiro, a instalação requer IAM credenciais 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 obter mais informações, consulte o Guia de instalação do servidor.

A instalação será concluída quando a EC2 capacidade da Amazon para seu Outpost estiver disponível em seu Conta da AWS. Depois que a capacidade estiver disponível, você poderá iniciar EC2 instâncias da Amazon em seu servidor Outposts. Para obter mais informações, consulte the section called “Executar uma instância ”.

Inicie uma instância no seu servidor Outposts

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 EC2 instâncias da Amazon.

Pré-requisito

É necessário ter um Outpost instalado em seu local. Para obter 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 do Outpost a qualquer uma VPC na AWS região do Outpost. Quando você faz isso, VPC também abrange o Posto Avançado. Para obter 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 é redirecionado para criar uma sub-rede no console da AmazonVPC. Selecionamos o Outpost para você e a zona de disponibilidade na qual ele está alojado.
4. Selecione um VPC e especifique um intervalo de endereços IP para a sub-rede.
5. Escolha Criar.
6. Depois que a sub-rede for criada, você deverá habilitar a sub-rede para interfaces de rede local. Use o comando modify-subnet-attribute da AWS CLI. 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. O exemplo a seguir usa um valor de 1 para especificar uma interface de rede secundária.

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

Etapa 2: Executar uma instância no Outpost

Você pode iniciar EC2 instâncias na sub-rede Outpost que você criou ou em uma sub-rede Outpost que foi compartilhada com você. Os grupos de segurança controlam o VPC tráfego de entrada e saída para instâncias em uma sub-rede Outpost, assim como fazem para instâncias em uma sub-rede de zona de disponibilidade. Para se conectar a uma EC2 instância em uma sub-rede Outpost, você pode especificar um key pair ao executar a instância, da mesma forma que você 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 EBS volumes. Escolha um tamanho de instância com armazenamento de instâncias suficiente para atender às necessidades do seu aplicativo. Para obter mais informações, consulte Volumes de armazenamento de instâncias e Criar um armazenamento de instâncias respaldado AMI no Guia EC2do usuário da Amazon.
- Você deve usar um EBS suporte da Amazon AMI com apenas um único EBS snapshot. AMIscom mais de um EBS snapshot não são suportados.
- 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 é redirecionado para o assistente de execução da instância no EC2 console da Amazon. 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 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 do dispositivo da interface de rede local para a sub-rede Outpost, essa interface de rede é a interface de rede local da instância. Como alternativa, para adicioná-lo posteriormente, consulteAdicionar uma interface de rede local.

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

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 uma interface de rede local.

Você deve configurar a interface de rede local para a instância com um endereço IP da sua rede local. Normalmente, você faz isso usandoDHCP. 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 EC2 instância, consulte Conecte-se à sua EC2 instância no Guia EC2 do usuário da Amazon.

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 EC2 console da Amazon 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 do link de serviço.

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

Conteúdo

Conectividade por meio do link de serviço

Durante o AWS Outposts provisionamento, você AWS cria ou cria uma conexão de link de serviço que conecta seu servidor Outposts à região ou AWS região de origem escolhida. O link de serviço é um conjunto criptografado de VPN conexões que são usadas sempre que o Outpost se comunica com a região de origem escolhida. Você usa um virtual LAN (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, tanto para o gerenciamento do Posto Avançado quanto para o VPC tráfego interno entre a AWS Região e o Posto Avançado.

O Outpost é capaz de criar o link de serviço de VPN volta para a AWS região 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 no link VLAN 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 qualquer associadoVPCs, incluindo tráfego do plano de dados do cliente.

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

A unidade máxima de transmissão (MTU) de uma conexão de rede é o tamanho, em bytes, do maior pacote permitido que pode ser passado pela conexão. A rede deve suportar 1500 bytes MTU entre o Outpost e os endpoints do link de serviço na região principal. AWS Para obter informações sobre a necessidade MTU 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 EC2 instância da Amazon no Guia EC2 do usuário da Amazon.

Recomendações de largura de banda do link de serviço

Para uma experiência e resiliência ideais, é AWS necessário que você use conectividade redundante de pelo menos 500 Mbps e uma latência máxima de ida e volta de 175 ms para a conexão do link de serviço com a região. AWS A utilização máxima para cada servidor Outposts é de 500 Mbps. Para aumentar a velocidade da conexão, use vários servidores Outposts. Por exemplo, se você tiver três AWS Outposts servidores, a velocidade máxima de conexão aumentará para 1,5 Gbps (1.500 Mbps). Para obter 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 AMI tamanho, elasticidade do aplicativo, necessidades de velocidade de pico e VPC tráfego da Amazon para a região. Observe que os AWS Outposts servidores não armazenam em cacheAMIs. AMIssão baixados da região a cada inicialização 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 AWS de vendas ou APN parceiro.

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 Amazônia VPC da AWS Região até o Posto Avançado. 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 Posto Avançado e qualquer associado VPCs

Se você estiver usando um firewall com estado com sua conexão com a Internet para limitar a conectividade da Internet pública ao link do serviçoVLAN, você pode bloquear todas as conexões de entrada que iniciam a partir da Internet. Isso ocorre porque o link de serviço VPN inicia somente do Posto Avançado para a Região, não da Região para o Posto Avançado.

Se você usar um firewall para limitar a conectividade do link de serviçoVLAN, 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	DHCPDNSservidor fornecido
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 Posto Avançado não podem usar o link de serviço para se comunicar com instâncias em outros Postos Avançados. 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 Outposts e sua região mãe AWS . Essa conexão de rede, chamada de link de serviço, é essencial para gerenciar o Posto Avançado, fornecendo VPC tráfego interno entre o Posto Avançado 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 VPC conectividade 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 do AWS Well-Architected e garantindo que seus aplicativos sejam resilientes a falhas ou atividades de manutenção que afetam um único servidor Outposts.

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.

Devolver um servidor Outposts

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 envio por meio do AWS Outposts console. Para começar, conclua as etapas a seguir.

Tarefas

- Etapa 1: Preparar o servidor para devolução
- Etapa 2: Obter a etiqueta de devolução
- Etapa 3: empacotar o servidor
- Etapa 4: devolver o servidor por meio do correio

Para devolver o servidor porque o servidor atingiu o final do prazo do contrato, ou por outro motivo, Contact AWS Support Center.

Etapa 1: Preparar 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 disassociate-resource-sharecomando.

   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 EC2 instâncias da Amazon 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 EC2 do usuário da Amazon.

Etapa 2: Obter a etiqueta de devolução

> **Important**
>
> Você só deve usar a etiqueta de remessa AWS fornecida porque ela contém informações específicas, como a ID do ativo, sobre o servidor que você está devolvendo. 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.

Etapa 3: empacotar o servidor

Para embalar seu servidor, use a caixa e o material de embalagem fornecidos pela AWS.

1. Coloque o servidor em uma das seguintes caixas:
   - A caixa e o material de embalagem em que o servidor veio originalmente.
   - A caixa e o material de embalagem em que o servidor substituto veio.

Como alternativa, entre em contato com a Central AWS Support para solicitar uma caixa.

2. Cole a etiqueta de envio AWS fornecida na parte externa da caixa.

> **Important**
>
> Verifique se a ID do ativo na etiqueta de remessa corresponde à ID do ativo no servidor que você está devolvendo.
> O ID do ativo está localizado na guia removível na parte frontal do servidor. Exemplo: `1203779889` ou `9305589922`

3. Feche a caixa com segurança.

Etapa 4: devolver o servidor por meio do 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	

País	Contato
Hong Kong	
Índia	
Indonésia	
Japão	
Malásia	
Nigéria	
Omã	
Panamá	
Peru	
Filipinas	
Sérvia	
Cingapura	
África do Sul	
Coreia do Sul	
Taiwan	
Tailândia	
Emirados Árabes Unidos	
Vietnã	

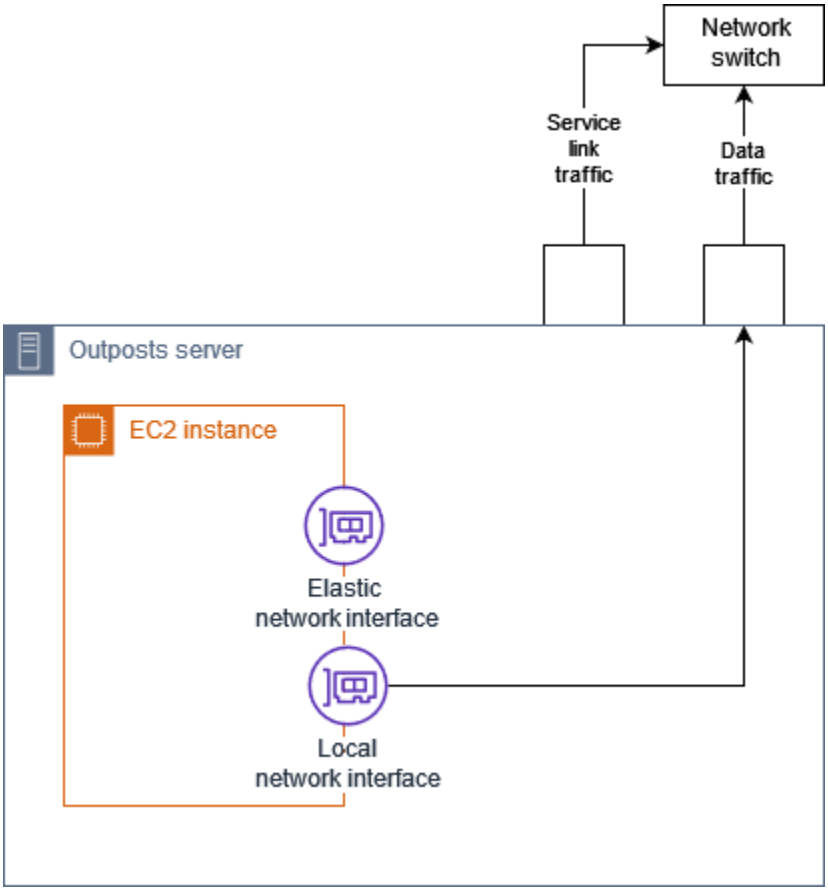
País	Contato
Estados Unidos da América	Contato UPS. Você pode devolver o servidor das seguintes maneiras: • Devolva o servidor durante uma UPS coleta de rotina em seu local. • Entregue o servidor em um UPS local. • Agende uma coleta para a data e hora de sua preferência. Insira o número de rastreamento da etiqueta de envio fornecida pela AWS para obter frete grátis.
Todos os outros países	Contato DHL. Você pode devolver o servidor das seguintes maneiras: • Entregue o servidor em um DHL local. • Agende uma coleta para a data e hora de sua preferência. Insira o número da carta de DHL porte na etiqueta de remessa AWS fornecida para frete grátis. Se você receber o seguinte erro `Courier pickup can't be scheduled for an import shipment`, isso geralment e significa que o país de coleta seleciona do não corresponde ao país de coleta na etiqueta de devolução. Selecione o país de origem da remessa e tente novamente.

Interfaces de rede local para seus servidores Outposts

Com os servidores Outposts, uma interface de rede local é um componente lógico de rede que conecta as EC2 instâncias da Amazon 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 EC2 instâncias 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 local enquanto a interface de rede se conecta aoVPC. O diagrama a seguir mostra uma EC2 instância 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 DHCP opções em VPC a para configurar uma interface de rede local porque uma interface de rede local é executada em 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 VPC rede para acessar os endpoints regionais públicos ou usar os VPC endpoints de interface para acessar Serviços da AWS usando. Serviços da AWS AWS PrivateLink Para obter 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. A VPC é uma rede virtualizada de três camadas. As interfaces de rede local não oferecem suporte a componentes VPC de rede. 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 Outposts visibilidade dos fluxos da VPC camada três. 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

- Suporte ARP e DHCP protocolos de interfaces de rede local. 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 Cotas de interface de rede no Guia do VPC usuário da Amazon.
- Cada EC2 instância pode ter uma interface de rede local.
- Uma interface de rede local não pode usar a interface de rede primária da instância.

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

> **Note**
>
> EC2instâncias 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 Outposts.
- As interfaces de rede local não oferecem suporte ao modo promíscuo ou à falsificação de MAC endereço.

Performance

A interface de rede local de cada tamanho de instância fornece uma parte da largura de banda física disponível de 10 GbE. A tabela a seguir lista o desempenho da rede 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.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
c6id.32xlarge	10	10

Tipo de instância	Largura de banda da linha de base (Gbps)	Expansão da largura de banda (Gbps)
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 seuVPC. Um grupo de segurança controla o tráfego de entrada e saídaVPC. A interface de rede local não está conectada aoVPC. 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.

Monitorar

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

MACendereços

AWS fornece MAC endereços para interfaces de rede local. As interfaces de rede local usam endereços administrados localmente (LAA) para seus MAC endereços. Uma interface de rede local usa o mesmo MAC endereço até que você exclua a interface. Depois de excluir uma interface de

rede local, remova o MAC endereço das configurações locais. AWS pode reutilizar MAC endereços que não estão mais em uso.

Adicionar uma interface de rede local a uma EC2 instância em uma sub-rede Outposts

Você pode adicionar uma interface de rede local a uma EC2 instância da Amazon em uma sub-rede Outposts durante ou após o lançamento. 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 a. AWS SDK Por exemplo, use os seguintes comandos do AWS CLI: create-network-interfaceattach-network-interfacee.

Use o procedimento a seguir para adicionar a interface de rede local depois de iniciar a instância. Para obter informações sobre como adicioná-la durante a execução da instância, consulte Executar uma instância no Outpost.

Para adicionar uma interface de rede local a uma EC2 instância

1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Rede e segurança, Interfaces de rede.
3. 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 IPv4endereço privado está definido como Atribuição automática.
    d. Selecione qualquer grupo de segurança. Os grupos de segurança não se aplicam à interface de rede local, portanto, o grupo de segurança selecionado não é relevante.
    e. Clique em Criar interface de rede.
4. 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 do dispositivo para a interface de rede local da 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 EC2 console da Amazon 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 IPv4 endereço privado para a interface de rede local a partir da sub-redeCIDR. Esse endereço não é o endereço IP da interface de rede local e não pode ser usado. No entanto, esse endereço é alocado da sub-redeCIDR, portanto, você deve contabilizá-lo no dimensionamento da sub-rede. Você deve definir o endereço IP da interface de rede local no sistema operacional convidado, estaticamente ou por meio do seu DHCP servidor.

Configurar o sistema operacional

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

Conectividade de rede local para servidores Outposts

Use este tópico para entender os requisitos de cabeamento e topologia de rede para hospedar um servidor Outposts. Para obter mais informações, consulte Interfaces de rede local para seus servidores Outposts.

Conteúdo

- Tráfego de links de serviço para servidores
- Tráfego de links da interface de rede local
- Atribuição de endereço IP do servidor
- Registro do servidor

Topologia do servidor na sua rede

Um servidor Outposts 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 rótulos e os tipos de tráfego do servidor Outposts.

Etiqueta de tráfego	Descrição
2	Tráfego do link de serviço — Esse tráfego permite a comunicação entre o Posto Avançado e a AWS Região, tanto para o gerenciamento do Posto Avançado quanto para o VPC tráfego intratráfico entre a AWS Região e o Posto Avançado. O tráfego do link de serviço inclui a conexão do link de serviço do Outpost à região. O link do serviço é personali zado VPN ou VPNs do Posto Avançado para a Região. O Outpost se conecta à zona de disponibilidade na região que você escolheu no momento da compra.
1	Tráfego de links da interface de rede local — Esse tráfego permite a comunicação do seu VPC para o local LAN pela interface da 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 instância

Etiqueta de tráfego	Descrição
	s que se comunicam com a Internet com sua rede on-premises.

Conectividade física do servidor

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

- 10Gbe — tipo de conector + QSFP

QSFP+ cabo

O cabo QSFP + tem um conector que você conecta à porta 3 no servidor Outposts. A outra extremidade do cabo QSFP + tem quatro interfaces SFP + que você conecta ao switch. Duas das interfaces do lado do switch são rotuladas 1 e 2. Ambas as interfaces são necessárias para que um servidor Outposts funcione. Use a 2 interface para tráfego de link de serviço e a 1 interface para tráfego de link de interface de rede local. 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 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 o público DNS disponível para que o Outpost descubra seu terminal de registro na AWS região. A conexão pode ter um NAT dispositivo entre o servidor Outposts 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 VPC do usuário da Amazon e AWS Outposts endpoints e cotas no. Referência geral da AWS

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

- TCP443

- UDP443
- UDP53

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 do link da interface de rede local e da utilização do link de serviço. Para obter mais informações, consulte Recomendações de largura de banda para links de serviço.

Tráfego de links da interface de rede local

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

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

O exemplo a seguir mostra como configurar a VLAN marcação para sua interface de rede local no Amazon Linux 2023. Se você estiver usando outra distribuição Linux, consulte a documentação da sua distribuição Linux sobre como configurar a VLAN marcação.

Exemplo: Para configurar a VLAN marcação para sua interface de rede local 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 VLAN dispositivo. Neste exemplo:

   - O nome da interface de rede local é `ens6`
   - O VLAN id é `59`
   - O nome atribuído ao VLAN dispositivo 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, em que a sub-rede é 192.168.59.0/24. CIDR

```
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 as alterações de VLAN marcação persistentes, 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 da 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 Outposts.

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 Outposts, você pode usar DHCP duas maneiras:

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

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

Para o link da interface de rede local, use 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 Outposts. Alterações no endereço IP podem causar interrupções temporárias no serviço na sub-rede Outpost.

Registro do servidor

Quando os servidores do Outposts estabelecem uma conexão na rede local, eles usam a conexão do link de serviço para se conectar aos endpoints de registro do Outpost e se registrarem. O registro requer públicoDNS. Quando os servidores se registram, eles criam um túnel seguro para o endpoint do link de serviço na região. Os servidores Outposts usam a TCP porta 443 para facilitar a comunicação com a Região pela Internet pública. Os servidores Outposts não oferecem suporte à conectividade privada por meio de. VPC

Compartilhe seus AWS Outposts recursos

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

Nesse modelo, a AWS conta que possui os recursos do Outpost (proprietário) compartilha os recursos com outras AWS contas (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 iniciam nas reservas de capacidade que eles compartilharam.

Os consumidores são responsáveis por gerenciar os recursos que criam nos Outposts e que são compartilhados 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:

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

Conteúdo

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

- Hosts dedicados alocados – Os consumidores com acesso a este recurso podem:
  - Inicie e execute EC2 instâncias em um host dedicado.
- Outposts – Os consumidores com acesso a este recurso podem:
  - Criar e gerenciar sub-redes no Outpost.
  - Use o AWS Outposts API para ver informações sobre o Posto Avançado.
- 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.
  - Inicie e execute EC2 instâncias em sub-redes.

  Use o VPC console da Amazon para compartilhar uma sub-rede Outpost. Para obter mais informações, consulte Compartilhamento de uma sub-rede no Guia do VPC usuário da Amazon.

Pré-requisitos para compartilhar recursos do Outposts

- Para compartilhar um recurso do Outpost com sua organização ou unidade organizacional em AWS Organizations, você deve habilitar o compartilhamento com 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, você deve possuí-lo em sua AWS conta. Você não pode 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 se integra com AWS Resource Access Manager ()AWS RAM. AWS RAM é um serviço que permite que você compartilhe seus AWS recursos com qualquer AWS conta ou por meio de 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 AWS contas individuais, unidades organizacionais ou uma organização inteira em AWS Organizations.

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

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 da `us-east-1a` sua AWS conta pode não ter a mesma localização `us-east-1a` de outra AWS conta.

Para identificar o local do seu recurso do Outpost relacionado a suas contas, use o ID da zona de disponibilidade (ID da AZ). O ID AZ é um identificador exclusivo e consistente para uma zona de disponibilidade em todas as AWS contas. Por exemplo, `use1-az1` é uma ID AZ para a `us-east-1` região e está no mesmo local em todas as AWS contas.

Para visualizar o AZ IDs das zonas de disponibilidade em sua conta

1. Abra o AWS RAM console em https://console.aws.amazon.com/ram.
2. As AZ IDs da região atual são exibidas no painel Sua 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 VPC associações. 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 AWS RAM recurso que permite que você compartilhe seus recursos entre AWS contas. 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 faz parte de uma organização AWS Organizations e o compartilhamento dentro da sua organização está ativado, você pode conceder aos consumidores da sua organização acesso do AWS RAM console ao recurso compartilhado do Outpost. 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.

Você pode compartilhar um recurso do Outpost que você possui usando o AWS Outposts console, o AWS RAM console ou o. AWS CLI

Para compartilhar um Outpost que você possui usando o console AWS Outposts

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, Visualizar detalhes.
4. Na página Resumo do Outpost, escolha Compartilhamentos de recursos.
5. Escolha Criar compartilhamento de recursos.

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

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

Consulte Criar um compartilhamento de atributos 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 create-resource-sharecomando.

Cancelamento do compartilhamento de um recurso compartilhado do Outpost

Quando um Posto Avançado compartilhado não é compartilhado, os consumidores não podem mais ver o Posto Avançado no console. AWS Outposts Eles não podem criar novas sub-redes no Outpost, criar novos EBS volumes no Outpost ou visualizar os detalhes do Outpost e os tipos de instância usando o console ou o. AWS Outposts 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 uma tabela de rotas de gateway local compartilhada não é compartilhada, os consumidores não podem mais criar novas VPC associações com ela. Todas VPC as associações existentes criadas pelos consumidores permanecem associadas à tabela de rotas. Os recursos neles VPCs podem continuar a rotear o tráfego para o gateway local.

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

Para cancelar o compartilhamento de um recurso compartilhado do Outpost que você possui usando o console AWS RAM

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

Para cancelar o compartilhamento de um recurso compartilhado do Outpost que você possui usando o AWS CLI

Use o disassociate-resource-sharecomando.

Identificando um recurso compartilhado do Outpost

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

Para identificar um Posto Avançado compartilhado usando o console AWS Outposts

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, Visualizar detalhes.
4. Na página de resumo do Outpost, veja o ID do proprietário para identificar o ID da AWS conta do proprietário do Outpost.

Para identificar um recurso compartilhado do Outpost 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 ser usados AWS Organizations para visualizar, modificar e excluir recursos que os consumidores criam 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 quaisquer taxas de transferência de dados associadas ao VPN tráfego do link de serviço do Outpost da AWS região.

Não há custos adicionais pelo compartilhamento de tabelas de rotas de gateway local. Para sub-redes compartilhadas, o VPC proprietário é cobrado por recursos em VPC nível de rede, como conexões e, NAT gateways AWS Direct Connect e VPN conexões de link privado.

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

Limitações

As seguintes limitações se aplicam ao trabalho com AWS Outposts compartilhamento:

- As limitações das sub-redes compartilhadas se aplicam ao trabalho com AWS Outposts compartilhamento. Para obter mais informações sobre limites de VPC compartilhamento, consulte Limitações no Guia do usuário da 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 AWS Outposts, consulte os FAQ AWS Outposts servidores em FAQ.

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

Conteúdo

Proteção de dados em AWS Outposts

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

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

Para obter mais informações sobre privacidade de dados, consulte Privacidade de dados FAQ. Para obter informações sobre proteção de dados na Europa, consulte o Modelo de Responsabilidade AWS Compartilhada e GDPR a postagem no blog AWS de segurança.

Criptografia em repouso

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

Criptografia em trânsito

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

Exclusão de dados

Quando você encerra uma EC2 instância, a memória alocada a ela é limpa (definida como zero) pelo hipervisor antes de ser 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. IAMos administradores controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) a usar AWS Outposts os recursos. Você pode usar IAM sem custo adicional.

Conteúdo

Como o AWS Outposts funciona com IAM

Antes de usar IAM para gerenciar o acesso aos AWS Postos Avançados, saiba quais IAM recursos estão disponíveis para uso com os Postos Avançados AWS .

IAMrecursos que você pode usar com AWS Outposts

IAMrecurso	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 nas políticas)	Sim
Credenciais temporárias	Sim

IAMrecurso	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

Compatível com políticas baseadas em identidade: Sim

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

Com políticas IAM baseadas em identidade, você pode especificar ações e recursos permitidos ou negados, bem como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou perfil ao qual ela está anexada. Para saber mais sobre todos os elementos que você pode usar em uma JSON política, consulte a referência IAM JSON de elementos de política no Guia IAM do usuário.

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

Suporte a políticas baseadas em recursos: não

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

Ações políticas para AWS Outposts

Compatível com ações de políticas: Sim

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

O `Action` elemento de uma JSON política 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 AWS API operação associada. Há algumas exceções, como ações somente com permissão que não têm uma operação correspondente. API Algumas operações também 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

Compatível com recursos de políticas: Sim

Os administradores podem usar AWS JSON políticas 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` JSON de política especifica o objeto ou objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou `NotResource`. Como prática recomendada, especifique um recurso usando seu Amazon Resource Name (ARN). Isso pode ser feito para ações que oferecem compatibilidade com um tipo de recurso específico, conhecido como permissões em nível de recurso.

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

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

Algumas API ações AWS do 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 seusARNs, consulte Tipos de recursos definidos AWS Outposts na Referência de Autorização de Serviço. Para saber com quais ações você pode especificar cada recurso, consulte Ações definidas por AWS Outposts. ARN

Chaves de condição de política para AWS Outposts

Compatível com chaves de condição de política específicas de serviço: Sim

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

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

Se você especificar vários elementos `Condition` em uma instrução ou várias chaves em um único `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, você pode conceder permissão a um IAM usuário para acessar um recurso somente se ele estiver marcado com o nome de IAM usuário. Para obter mais informações, consulte elementos de IAM política: variáveis e tags no Guia IAM do usuário.

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 IAM do usuário.

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

ACLsem AWS Outposts

SuportesACLs: Não

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

ABACcom AWS Outposts

Suportes ABAC (tags nas políticas): Sim

O controle de acesso baseado em atributos (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 IAM entidades (usuários ou funções) e a muitos AWS recursos. Marcar entidades e recursos é a primeira etapa doABAC. Em seguida, você cria ABAC políticas para permitir operações quando a tag do diretor corresponde à tag do recurso que ele está tentando acessar.

ABACé útil em ambientes que estão crescendo rapidamente e ajuda em situações em que o gerenciamento de políticas se torna complicado.

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

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

Para obter mais informações sobreABAC, consulte O que éABAC? no Guia do IAM usuário. Para ver um tutorial com etapas de configuraçãoABAC, consulte Usar controle de acesso baseado em atributos (ABAC) no Guia do IAMusuário.

Usando credenciais temporárias com Outposts AWS

Compatível com 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 esse trabalho IAM no Guia do IAM usuário.

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 a troca de funções, consulte Alternando para uma função (console) no Guia IAM do usuário.

Você pode criar manualmente credenciais temporárias usando o AWS CLI ou AWS API. Em seguida, você pode usar essas credenciais temporárias para acessar AWS. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para obter mais informações, consulte Credenciais de segurança temporárias emIAM.

Permissões principais entre serviços para Outposts AWS

Suporta sessões de acesso direto (FAS): Sim

Quando você usa um IAM usuário ou uma função para realizar ações em AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. FASusa 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. FASas solicitações 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 FAS solicitações, consulte Encaminhar sessões de acesso.

Funções de serviço para o Outposts AWS

Compatível com perfis de serviço: não

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

Funções vinculadas a serviços para Outposts AWS

Suporte a perfis vinculados a serviços: sim

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir a função 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 IAM administrador pode visualizar, mas não editar, as permissões das funções vinculadas ao serviço.

Para obter detalhes sobre como criar ou gerenciar funções vinculadas ao serviço do AWS Outposts, consulte. Funções vinculadas a serviços para 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 o AWS Management Console, AWS

Command Line Interface (AWS CLI) ou AWS API. Para conceder permissão aos usuários para realizar ações nos recursos de que precisam, um IAM administrador pode criar IAM políticas. O administrador pode então adicionar as IAM políticas às funções e os usuários podem assumir as funções.

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

Para obter detalhes sobre ações e tipos de recursos definidos pelo AWS Outposts, incluindo o formato do 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 AWS gerenciadas ou políticas AWS gerenciadas para funções de trabalho no Guia IAM do usuário.
- Aplique permissões com privilégios mínimos — Ao definir permissões com IAM políticas, conceda somente as permissões necessárias para realizar 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 IAM como usar para aplicar permissões, consulte Políticas e permissões IAM no Guia IAM do usuário.
- Use condições nas IAM políticas para restringir ainda mais o acesso — Você pode adicionar uma condição às suas políticas para limitar o acesso a ações e recursos. Por exemplo, você pode escrever uma condição de política para especificar que todas as solicitações devem ser enviadas

usandoSSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como AWS CloudFormation. Para obter mais informações, consulte elementos IAM JSON da política: Condição no Guia IAM do usuário.

- Use o IAM Access Analyzer para validar suas IAM políticas e garantir permissões seguras e funcionais — o IAM Access Analyzer valida políticas novas e existentes para que as políticas sigam a linguagem da IAM política (JSON) e as melhores práticas. IAM IAMO Access Analyzer fornece mais de 100 verificações de políticas e recomendações práticas para ajudá-lo a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação da política do IAM Access Analyzer no Guia do IAM Usuário.
- Exigir autenticação multifatorial (MFA) — Se você tiver um cenário que exija IAM usuários ou um usuário root Conta da AWS, ative MFA para obter segurança adicional. Para exigir MFA quando API as operações são chamadas, adicione MFA condições às suas políticas. Para obter mais informações, consulte Configurando o API acesso MFA protegido no Guia do IAMusuário.

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

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"
    }
  ]
}
```

Funções vinculadas a serviços para AWS Outposts

AWS Outposts usa AWS Identity and Access Management (IAM) funções vinculadas ao serviço. Uma função vinculada ao serviço é um tipo de função de serviço vinculada diretamente a. AWS Outposts AWS Outposts define funções vinculadas ao serviço e inclui todas as permissões necessárias 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, e essa política de permissões não pode ser anexada a nenhuma outra IAM entidade.

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.

Permissões de função vinculadas ao serviço para AWS Outposts

AWS Outposts usa a função vinculada ao serviço chamada _ AWSServiceRoleForOutposts***OutpostID***— Permite que Outposts acessem AWS 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.

O AWSServiceRoleForOutposts *_OutpostID* a função vinculada ao serviço confia nos seguintes serviços para assumir a função:

- `outposts.amazonaws.com`

O AWSServiceRoleForOutposts _*OutpostID*a função vinculada ao serviço inclui as seguintes políticas:

- AWSOutpostsServiceRolePolicy
- AWSOutpostsPrivateConnectivityPolicy_*OutpostID*

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`

O AWSOutpostsPrivateConnectivityPolicy _*OutpostID*a política AWS Outposts permite concluir 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 permitir que uma IAM entidade (como usuário, grupo ou função) crie, edite ou exclua uma função vinculada ao serviço. Para obter mais informações, consulte Permissões de funções vinculadas ao serviço no Guia do IAMusuário.

Crie uma função vinculada ao serviço para AWS Outposts

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

Edite uma função vinculada ao serviço para AWS Outposts

AWS Outposts não permite que você edite o AWSServiceRoleForOutposts _*OutpostID* função vinculada ao serviço. Depois que você criar um perfil vinculado ao serviço, não poderá alterar o nome do perfil, pois várias entidades podem fazer referência ao perfil. No entanto, você pode editar a descrição da função usandoIAM. Para obter mais informações, consulte Atualizar uma função vinculada ao serviço no Guia do IAMusuário.

Excluir uma função vinculada ao serviço para 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.

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.

Você deve excluir seu Outpost antes de excluir o _ AWSServiceRoleForOutposts*OutpostID* função vinculada ao serviço.

Antes de começar, certifique-se de que seu Outpost não esteja sendo compartilhado usando AWS Resource Access Manager (AWS RAM). Para obter 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.

Para excluir manualmente a função vinculada ao serviço usando IAM

Para obter mais informações, consulte Excluir uma função vinculada ao serviço no Guia do IAMusuário.

Regiões suportadas para funções vinculadas a AWS Outposts serviços

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 os racks do FAQs Outposts e os servidores do Outposts.

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 API operações são disponibilizadas para os serviços existentes.

Para obter mais informações, consulte as políticas AWS gerenciadas no Guia IAM do usuário.

AWS política gerenciada: AWSOutpostsServiceRolePolicy

Essa política está vinculada a uma função vinculada ao serviço que permite que AWS Outposts realizem ações em seu nome. Para obter mais informações, consulte Funções vinculadas a serviço.

AWS política gerenciada: AWSOutpostsPrivateConnectivityPolicy

Essa política está vinculada a uma função vinculada ao serviço que permite que AWS Outposts realizem ações em seu nome. Para obter mais informações, consulte Funções vinculadas a serviço.

AWS política gerenciada: AWSOutpostsAuthorizeServerPolicy

Use essa política para conceder as permissões necessárias para autorizar o hardware do servidor Outposts em sua rede local.

Esta política inclui as seguintes permissões:

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

AWS Outposts: atualizações das políticas gerenciadas AWS

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

Alteração	Descrição	Data
AWSOutpostsAuthorizeServerPolicy— Nova política	AWS O Outposts adicionou uma política que concede permissões para autorizar o hardware do servidor Outposts em sua rede local.	4 de janeiro de 2023
AWS Outposts começaram a monitorar as mudanças	AWS Outposts começou a monitorar as mudanças em	03 de dezembro de 2019

Alteração	Descrição	Data
	suas políticas AWS gerenciadas.	

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 API chamadas AWS publicadas para acessar AWS Outposts pela rede. Os clientes devem oferecer suporte para:

- Segurança da camada de transporte (TLS). Exigimos TLS 1,2 e recomendamos TLS 1,3.
- Suítes de criptografia com sigilo direto perfeito (), como (Ephemeral PFS Diffie-Hellman) ou DHE (Elliptic Curve Ephemeral Diffie-Hellman). ECDHE A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando uma ID de chave de acesso e uma chave de acesso secreta associada a um IAM principal. Ou você pode 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 EC2 instâncias e EBS volumes em execução no seu Outpost, consulte Segurança da infraestrutura na Amazon EC2.

VPCOs registros de fluxo 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 às operações do plano de controle, como responder a API chamadas, monitorar o Posto Avançado e atualizar o Posto Avançado. 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.

Os servidores Outposts incluem volumes de armazenamento de instâncias, mas não oferecem suporte aos volumes da AmazonEBS. 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 HIPAA segurança e conformidade na Amazon Web Services — Este whitepaper descreve como as empresas podem usar AWS para criar HIPAA aplicativos qualificados.

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

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

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

CloudWatch métricas

Use CloudWatch a Amazon para recuperar estatísticas sobre pontos de dados para seu servidor de rack 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 obter mais informações, consulte CloudWatch .

CloudTrail troncos

Use AWS CloudTrail para capturar informações detalhadas sobre as chamadas feitas para AWS APIs o. 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 API ações do AWS Outposts. Eles também contêm informações para chamadas para API ações de serviços em um Posto Avançado, como Amazon EC2 e AmazonEBS. Para obter mais informações, consulte Registre API chamadas usando CloudTrail.

Logs de fluxo da VPC

Use registros VPC de fluxo para capturar informações detalhadas sobre o tráfego que entra e sai do seu Posto Avançado e dentro do seu Posto Avançado. Para obter mais informações, consulte Logs de VPC fluxo no Guia VPC do usuário da Amazon.

Espelhamento de tráfego

Use o Espelhamento de Tráfego para copiar e encaminhar o tráfego de rede do seu servidor de rack out-of-band para dispositivos de segurança e monitoramento. Você pode usar o tráfego espelhado para inspeção de conteúdo, monitoramento de ameaças ou solução de problemas. Para obter mais informações, consulte o Amazon VPC Traffic Mirroring Guide.

AWS Health Dashboard

AWS Health Dashboard Exibe informações e notificações que são iniciadas por mudanças na integridade dos AWS recursos. 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 AWS Health serviço, não AWS Health Dashboard requer configuração e pode ser visualizada por qualquer usuário autenticado em sua conta. Para obter mais informações, consulte Conceitos básicos do AWS Health Dashboard.

CloudWatch

AWS Outposts publica 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 alterações recentes na configuração da rede local no firewall e nas NAT regras ou problemas de conexão com a Internet. Em caso de `ConnectedStatus` problemas, recomendamos verificar a conectividade com a AWS Região de dentro da sua rede local e entrar em contato com o AWS Support 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

Metrics

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 (RDSAmazon) 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 inclui a `AvailableReservedInstances` contagem.

Para determinar o número de instâncias que você pode reservar, subtraia a `AvailableReservedInstances` contagem da `AvailableInstanceType_Count` contagem.

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

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 que estão disponíveis para execução na capacidade computacional reservada usando reservas de capacidade.

Essa métrica não inclui as Instâncias EC2 Reservadas da Amazon.

Essa métrica não inclui o número de instâncias que você pode reservar. Para determinar quantas instâncias você pode reservar, subtraia a `AvailableReservedInstances` contagem da `AvailableInstanceType_Count` contagem.

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

Unidade: Contagem

Resolução máxima: 5 minutos

Dimensões: `InstanceType` e `OutpostId`

`UsedReservedInstances`

O número de instâncias em execução na capacidade computacional reservada usando reservas de capacidade. Essa métrica não inclui as Instâncias EC2 Reservadas da Amazon.

Unidade: Contagem

Resolução máxima: 5 minutos

Dimensões: `InstanceType` e `OutpostId`

`TotalReservedInstances`

O número total de instâncias, em execução e disponíveis para execução, fornecido pela capacidade computacional reservada usando reservas de capacidade. Essa métrica não inclui as Instâncias EC2 Reservadas da Amazon.

Unidade: Contagem

Resolução máxima: 5 minutos

Dimensões: `InstanceType` e `OutpostId`

Dimensões da métrica

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 EBS volume.
`VirtualInterfaceId`	A ID do gateway local ou do link de serviço Virtual Interface (VIF).

Dimensão	Descrição
`VirtualInterfaceGroupId`	A ID do grupo de interface virtual para a interface virtual do gateway local (VIF).

Você pode visualizar as CloudWatch métricas do seu servidor de Outposts 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 no campo 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 o 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 AWS Outposts API chamadas usando AWS CloudTrail

AWS Outposts é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço. CloudTrail captura API chamadas AWS Outposts como eventos. As chamadas capturadas incluem chamadas do AWS Outposts console e chamadas de código para as AWS Outposts API operações. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita AWS Outposts, o endereço IP do qual a solicitação foi feita, quando foi feita e detalhes adicionais.

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 de usuário raiz ou credenciais de usuário.
- Se a solicitação foi feita em nome de um usuário do IAM Identity Center.
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro AWS service (Serviço da AWS).

CloudTrail está ativo em sua AWS conta quando você cria a conta e você tem acesso automático ao histórico de CloudTrail eventos. O histórico de CloudTrail eventos fornece um registro visível, pesquisável, baixável e imutável dos últimos 90 dias de eventos de gerenciamento registrados em um. Região da AWS Para obter mais informações, consulte Trabalhando com o histórico de CloudTrail eventos no Guia AWS CloudTrail do usuário. Não há CloudTrail cobrança pela visualização do histórico de eventos.

Para um registro contínuo dos eventos dos Conta da AWS últimos 90 dias, crie uma trilha ou um armazenamento de dados de eventos do CloudTrailLake.

CloudTrail trilhas

Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Todas as trilhas criadas usando o AWS Management Console são multirregionais. Só é possível criar uma trilha de região única ou de várias regiões usando a AWS CLI. É recomendável criar uma trilha multirregional porque você captura todas as atividades Regiões da AWS em sua conta. Se você criar uma trilha de região única, poderá visualizar somente os eventos registrados na Região da AWS da trilha. Para obter mais informações sobre trilhas, consulte Criar uma trilha para a Conta da AWS e Criar uma trilha para uma organização no Guia do usuário do AWS CloudTrail .

Você pode entregar uma cópia dos seus eventos de gerenciamento contínuos para o bucket do Amazon S3 sem nenhum custo CloudTrail criando uma trilha. No entanto, há cobranças de armazenamento do Amazon S3. Para obter mais informações sobre CloudTrail preços, consulte AWS CloudTrail Preços. Para receber informações sobre a definição de preço do Amazon S3, consulte Definição de preço do Amazon S3.

CloudTrail Armazenamentos de dados de eventos em Lake

CloudTrail O Lake permite que você execute consultas SQL baseadas em seus eventos. CloudTrail O Lake converte eventos existentes em JSON formato baseado em linhas para o formato ORCApache. ORCé um formato de armazenamento colunar otimizado para recuperação rápida de dados. Os eventos são agregados em armazenamentos de dados de eventos, que são coleções imutáveis de eventos baseados nos critérios selecionados com a aplicação de seletores de eventos avançados. Os seletores que você aplica a um armazenamento de dados de eventos controlam quais eventos persistem e estão disponíveis para você consultar. Para obter mais informações sobre o CloudTrail Lake, consulte Trabalhando com o AWS CloudTrail Lake no Guia AWS CloudTrail do Usuário.

CloudTrail Os armazenamentos e consultas de dados de eventos em Lake incorrem em custos. Ao criar um armazenamento de dados de eventos, você escolhe a opção de preço que deseja usar para ele. A opção de preço determina o custo para a ingestão e para o armazenamento de eventos, e o período de retenção padrão e máximo para o armazenamento de dados de eventos. Para obter mais informações sobre CloudTrail preços, consulte AWS CloudTrail Preços.

AWS Outposts eventos de gerenciamento em CloudTrail

Os eventos de gerenciamento fornecem informações sobre as operações de gerenciamento que são realizadas nos recursos do seu Conta da AWS. Elas também são conhecidas como operações de plano de controle. Por padrão, CloudTrail registra eventos de gerenciamento.

AWS O Outposts registra todas as operações do plano de controle AWS do Outposts como eventos de gerenciamento. Para obter uma lista das operações do plano de controle do AWS Outposts nas quais o AWS Outposts se registra, CloudTrail consulte a Referência do Outposts.AWS API

AWS Outposts exemplos de eventos

O exemplo a seguir mostra um CloudTrail evento que demonstra a `SetSiteAddress` operação.

```
{
```

```
    "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 servidor de Outposts

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 servidor de Outposts 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 local.

Conteúdo

Atualizar detalhes de contato

Se o proprietário do Outpost mudar, entre em contato com a AWS Support Central com o nome e as informações de contato do novo proprietário.

Manutenção de hardware

Se AWS detectar um problema irreparável com o hardware durante o processo de provisionamento do servidor ou ao hospedar instâncias da Amazon em EC2 execução no seu servidor de Outposts, 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 instâncias no Guia EC2 do usuário da Amazon.

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 na instalação do servidor Outposts.
- 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 de energia e de 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 aplicações dos equipamentos da Outposts de forma controlada, usando mudanças de balanceamento de carga DNS baseadas ou fora da prateleira.
- Pare contêineres, instâncias e bancos de dados de forma incremental ordenada e use a ordem inversa ao restaurá-los.
- Planos de teste para movimentação ou parada controlada de serviços.
- Faça backup de dados e de configurações essenciais e armazene-os fora dos Outposts.
- Mantenha os tempos de inatividade de energia no mínimo.
- Evite a troca repetida das fontes de alimentação (off-on-off-on) durante a manutenção.
- Reserve mais tempo no intervalo de manutenção para lidar com o inesperado.
- Gerencie as expectativas de seus usuários e clientes comunicando um prazo de manutenção mais amplo do que você normalmente precisaria.
- Depois que a energia for restaurada, crie um caso no AWS Support Centro para solicitar a verificação de que AWS Outposts os serviços relacionados estão em execução.

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.

EC2As instâncias, LNI redes e volumes de armazenamento de instâncias da Amazon no servidor Outposts continuarão operando normalmente e poderão ser acessados localmente por meio da rede local e. LNI Da mesma forma, recursos AWS de serviços, como os nós de ECS trabalho da Amazon, continuam sendo executados localmente. No entanto, API a disponibilidade será reduzida. Por exemplo, executar, iniciar, parar e finalizar APIs podem não funcionar. As métricas e os registros da instância continuarão sendo armazenados em cache localmente por algumas horas e serão enviados

para a AWS região quando a conectividade retornar. No entanto, a desconexão por mais de algumas horas pode resultar na perda de métricas e registros.

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 AWSSupport etupIPMonitoring-S From. VPC Essa ferramenta é um AWS Systems Manager documento (SSMdocumento) que cria uma instância do Amazon EC2 Monitor em uma sub-rede especificada por você e monitora os endereços IP de destino. O documento executa testes de diagnóstico de pingMTR, TCP trace-route e trace-path 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

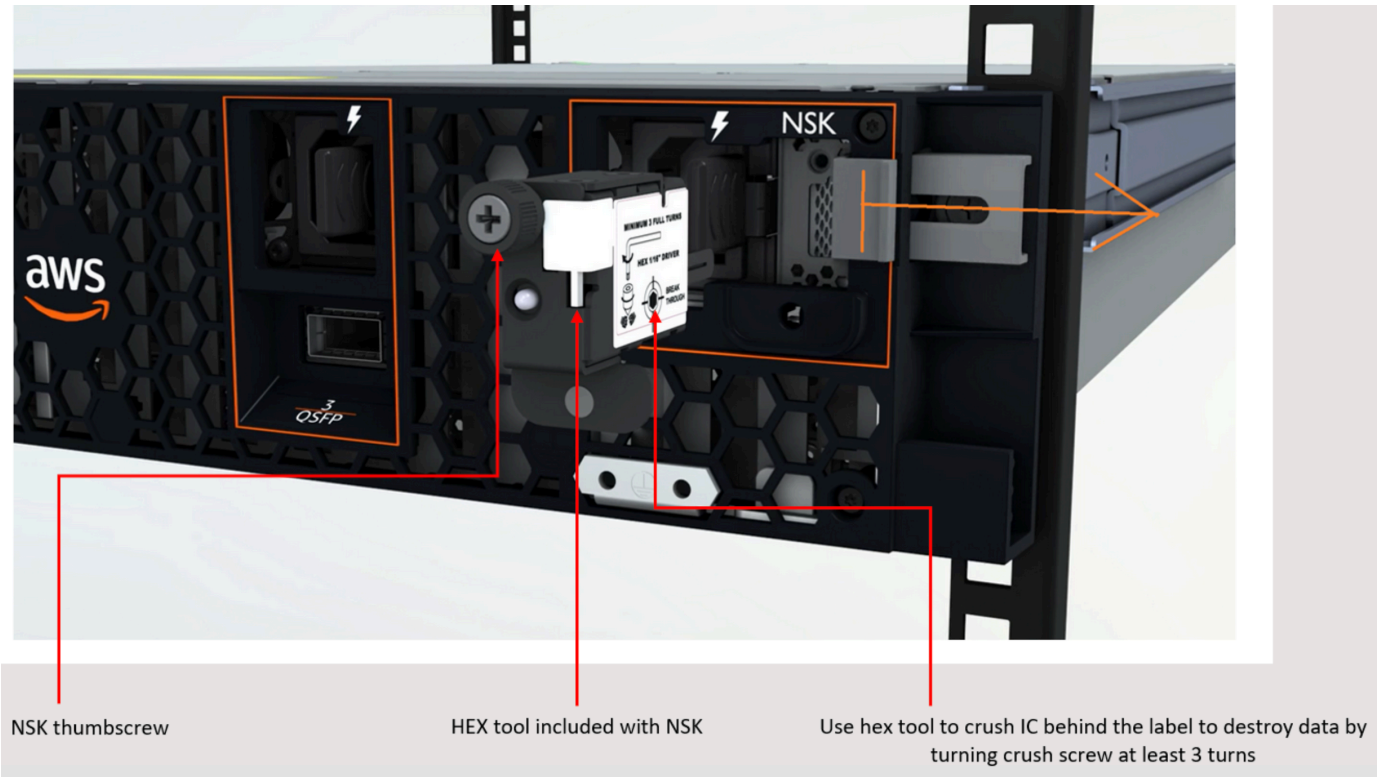
- O AWS blog Implantando um CloudWatch painel automatizado da Amazon para AWS Outposts uso AWS CDK descreve as etapas envolvidas na implantação de um painel automatizado.
- Se você tiver dúvidas ou precisar de mais informações, consulte Criação de um caso de suporte no AWS Guia do usuário de suporte.

Destrua criptograficamente os dados do servidor

A chave de segurança Nitro (NSK) é necessária para descriptografar dados no servidor. Quando você retorna o servidor para AWS, seja porque está substituindo o servidor ou descontinuando o serviço, você pode destruí-lo 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. Certifique-se de que você tenha o correto NSK que foi enviado 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 NSK e destrói criptograficamente todos os dados no servidor.



Opções de servidor Outposts end-of-term

Ao final do seu AWS Outposts mandato, você deve escolher entre as seguintes opções:

- Renove sua assinatura e mantenha seus servidores Outposts existentes.
- Encerre sua assinatura e devolva seus servidores Outposts.
- Converta para uma month-to-month assinatura e mantenha seus servidores Outposts existentes.

Renove sua assinatura

Você deve concluir as etapas a seguir pelo menos 30 dias antes do término da assinatura atual dos seus servidores Outposts.

Para renovar sua assinatura e manter seus servidores Outposts existentes

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 Outposts, você será convertido em month-to-month uma 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

Você deve concluir as etapas a seguir pelo menos 30 dias antes do término da assinatura atual dos seus servidores Outposts. AWS não pode iniciar o processo de devolução até que você faça isso.

> **Important**
>
> AWS não é possível interromper o processo de devolução depois de abrir um caso de suporte para encerrar sua assinatura.

Para encerrar sua assinatura

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. NOTDesligue ou desconecte o servidor da rede até que seja instruído a fazer isso 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 seus servidores Outposts existentes, 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 começa 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.

A tabela a seguir descreve as atualizações da documentação dos servidores de 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
Apresentando os servidores Outposts	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.