Melhores práticas para criar uma arquitetura de nuvem híbrida com Serviços da AWS

AWS Recomendações

AWS Recomendações: Melhores práticas para criar uma arquitetura de nuvem híbrida com Serviços da AWS

Table of Contents

Melhores práticas para criar uma arquitetura de nuvem híbrida com Serviços da AWS

Amazon Web Services (colaboradores)

Junho de 2025 (histórico do documento)

Muitas empresas e organizações adotaram a computação em nuvem como um aspecto fundamental de sua estratégia de tecnologia. Eles normalmente migram suas cargas de trabalho para o para aumentar a agilidade, Nuvem AWS a economia de custos, o desempenho, a disponibilidade, a resiliência e a escalabilidade. A maioria dos aplicativos pode ser facilmente migrada, mas alguns devem permanecer no local para aproveitar a baixa latência e o processamento local de dados do ambiente local, para evitar altos custos de transferência de dados ou para fins de conformidade regulatória. Além disso, um subconjunto de aplicativos pode precisar ser rearquitetado ou modernizado antes de poder ser movido para a nuvem. Isso leva muitas organizações a buscarem arquiteturas de nuvem híbrida para integrar suas operações locais e na nuvem para dar suporte a um amplo espectro de casos de uso. Essa abordagem híbrida pode fornecer os benefícios da computação local e baseada em nuvem e pode ser particularmente útil para cenários de computação de ponta.

Ao criar uma nuvem híbrida com AWS, recomendamos que você determine sua estratégia de nuvem híbrida e sua estratégia técnica:

- Uma estratégia de nuvem híbrida fornece diretrizes que regem o consumo de recursos na nuvem e no local para apoiar seus objetivos de negócios. Esta orientação descreve casos de uso comuns para criar uma nuvem híbrida, como apoiar a migração contínua para a nuvem, garantir a continuidade dos negócios durante desastres, estender a infraestrutura de nuvem para o ambiente local para suportar aplicativos de baixa latência ou expandir sua presença internacional em. AWS A definição dessa estratégia ajuda você a identificar e definir seus objetivos de negócios para criar uma nuvem híbrida e fornece diretrizes para o posicionamento da carga de trabalho na nuvem híbrida.
- Uma estratégia técnica para a nuvem híbrida identifica os princípios orientadores da arquitetura da nuvem híbrida e define uma estrutura de implementação. Esta orientação descreve os requisitos comuns para uma arquitetura de nuvem híbrida implantada e gerenciada de forma consistente para ajudá-lo a definir princípios para uma implementação planejada de nuvem híbrida. Esses

requisitos incluem interfaces padronizadas para provisionamento e gerenciamento de recursos em toda a sua infraestrutura de nuvem.

Este guia descreve uma estrutura de operações e gerenciamento para ajudar arquitetos e operadores de soluções a identificar os alicerces, as melhores práticas, a nuvem AWS híbrida e os serviços regionais com AWS os quais implementar uma nuvem híbrida.

Muitas organizações usaram as soluções descritas neste guia para implantar com sucesso ambientes de nuvem híbrida que aproveitam a escala, a agilidade, a inovação e a presença global fornecidas pela. Nuvem AWS(Veja os estudos de caso.) AWS os serviços de nuvem híbrida oferecem uma AWS experiência consistente da nuvem até o local e na borda. Serviços como computação, armazenamento, banco de dados AWS Outposts e outros Zonas locais da AWS locais são selecionados Serviços da AWS perto de grandes centros populacionais e setoriais quando você precisa de baixa latência entre os dispositivos do usuário final ou os data centers e servidores de carga de trabalho locais existentes.

Neste guia:

Visão geral

Este guia classifica AWS as recomendações para a nuvem híbrida em cinco pilares: rede, segurança, resiliência, planejamento de capacidade e gerenciamento de infraestrutura. Ele fornece diretrizes para ajudá-lo a melhorar sua prontidão e desenvolver uma estratégia de migração usando um serviço de ponta AWS híbrido, como AWS Outposts ou Zonas locais da AWS. É altamente recomendável que você trabalhe com sua Conta da AWS equipe ou AWS Partner garanta que um especialista em nuvem AWS híbrida esteja disponível para ajudá-lo a seguir este guia e desenvolver seu processo.

> **Note**
>
> Embora AWS Outposts as Zonas Locais resolvam problemas semelhantes, recomendamos que você analise os casos de uso, bem como os serviços e recursos disponíveis para decidir qual oferta atende melhor às suas necessidades. Para obter mais informações, consulte a postagem do AWS blog Zonas locais da AWS e AWS Outposts escolha da tecnologia certa para sua carga de trabalho de ponta.

Workshops sobre nuvem híbrida

Com a ajuda de um especialista em nuvem AWS híbrida (SME), você pode realizar um workshop sobre nuvem híbrida para avaliar o nível de maturidade da sua empresa em relação aos cinco pilares discutidos neste guia.

O workshop se concentra em áreas internas da sua organização, como redes, segurança, conformidade DevOps, virtualização e unidades de negócios. Ele ajuda você a projetar uma arquitetura de nuvem híbrida que atenda aos requisitos da sua organização e defina os detalhes da implementação, seguindo as etapas na seção Processo de adoção da nuvem híbrida deste guia.

PoCs

Se você tiver requisitos específicos, poderá usar provas de conceito (PoCs) para validar a funcionalidade em Zonas Locais e em AWS Outposts relação a esses requisitos.

AWS usa PoCs para ajudá-lo a testar as cargas de trabalho que você deseja mover para um posto avançado ou zona local, para determinar se as cargas de trabalho funcionarão nas arquiteturas de

teste. Para acessar uma Zona Local para testes, siga as instruções na documentação de Zonas Locais. Para testar sua carga de trabalho AWS Outposts, trabalhar com sua Conta da AWS equipe ou AWS Partner acessar um laboratório de AWS Outposts testes e receber orientação de arquitetos de AWS soluções. Em todos os cenários, o desenvolvimento de uma PoC exige que você gere um documento de teste que contenha:

- Serviços da AWS para usar, como Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Block Store (Amazon EBS), Amazon Virtual Private Cloud (Amazon VPC) e Amazon Elastic Kubernetes Service (Amazon EKS)
- Tamanho e número de instâncias a serem consumidas (por exemplo, `m5.xlarge` ou `c5.2xlarge`)
- Diagrama da arquitetura de teste
- Critérios de sucesso do teste
- Detalhes e objetivos de cada teste a ser executado

Pilares

A próxima seção aborda os pré-requisitos e as limitações do uso das arquiteturas discutidas neste guia. As seções seguintes abordam os detalhes de cada pilar para que o documento de recomendações que você cria durante o workshop de nuvem híbrida possa refletir os detalhes do projeto necessários para a implementação.

- Rede na periferia
- Segurança na borda
- Resiliência na borda
- Planejamento de capacidade na borda
- Gerenciamento de infraestrutura de ponta

Pré-requisitos e limitações

Antes de seguir este guia, trabalhe com sua Conta da AWS equipe ou AWS Partner revise os pré-requisitos e limitações para implementar arquiteturas de borda com Locais AWS Outposts Zones.

Pré-requisitos

AWS Outposts

- Seu data center existente deve atender aos AWS Outposts requisitos de instalações, rede e energia. AWS Outposts foi projetado para operar em um ambiente de data center que tem entradas de alimentação redundantes de 5 a 15 kVA, 145,8 vezes o fluxo de ar em pés cúbicos por minuto (CFM) e uma temperatura ambiente entre 41° F (5° C) e 95° F (35° C), entre outros requisitos.
- Confirme se o AWS Outposts serviço está disponível em seu país consultando o AWS Outposts rack FAQs. Veja a pergunta: Em quais países e territórios o Outposts rack está disponível?
- Se sua organização precisar de quatro ou mais AWS Outposts racks, seu data center deverá atender aos requisitos de rack Aggregation, Core, Edge (ACE).
- Uma Internet ou um AWS Direct Connect link de pelo menos 500 Mbps (1 Gbps é melhor) deve ser fornecido e mantido para se conectar AWS Outposts ao Região da AWS, com conectividade de backup adequada, se seu caso de uso exigir. A latência do tempo de ida e volta AWS Outposts até a região deve ser de 175 milissegundos no máximo.
- Você deve ter um contrato ativo para o AWS Enterprise Support ou um plano de operações AWS unificadas.

Zonas locais da AWS

- Uma zona AWS local deve estar disponível perto de seus data centers ou usuários. Veja os Zonas locais da AWS locais.
- Confirme se você tem conectividade de rede da sua infraestrutura local com a Zona Local:
  - Opção 1: um Direct Connect link do seu data center para o Direct Connect ponto de presença (PoP) mais próximo da zona local. Para obter mais informações, consulte Direct Connect na documentação de Locais Zones.

- Opção 2: Um link de internet, além de um dispositivo de rede privada virtual (VPN) local e o licenciamento necessário para iniciar um dispositivo VPN baseado em software no Amazon EC2 na zona local. Para obter mais informações, consulte Conexão VPN na documentação de Locais Zones.

Para obter mais opções de conectividade, consulte a documentação de Locais Zones.

Limitações

AWS Outposts

- O Amazon Relational Database Service (Amazon RDS) AWS Outposts em implantações Multi-AZ exige pools de endereços IP (CoIP) de propriedade do cliente. Para obter mais informações, consulte Endereços IP de propriedade do cliente para o Amazon RDS em. AWS Outposts
- O Multi-AZ on AWS Outposts está disponível para todas as versões compatíveis do MySQL e do PostgreSQL no Amazon RDS on. AWS Outposts Para ter mais informações, consulte Suporte ao Amazon RDS on AWS Outposts para recursos do Amazon RDS. O Amazon RDS on AWS Outposts oferece suporte aos bancos de dados SQL Server, Amazon RDS para MySQL e Amazon RDS for PostgreSQL.
- AWS Outposts não foi projetado para operar quando está desconectado de um Região da AWS. Para obter mais informações, consulte a seção Pensando em termos de modos de falha no AWS whitepaper Considerações sobre design e arquitetura de AWS Outposts alta disponibilidade.
- O Amazon Simple Storage Service (Amazon S3) AWS Outposts on tem algumas limitações. Eles são discutidos na seção Como o Amazon S3 em Outposts é diferente do Amazon S3? seção do Guia do usuário do Amazon S3 on Outposts.
- Os Application Load Balancers AWS Outposts não oferecem suporte a TLS mútuo (mTLS) ou sessões fixas.
- Os racks ACE não estão totalmente fechados e não incluem portas dianteiras ou traseiras.
- A ferramenta de capacidade da instância é aplicável somente para novos pedidos.

Zonas locais da AWS

- As Zonas Locais não têm um AWS Site-to-Site VPN endpoint. Em vez disso, use uma VPN baseada em software no Amazon EC2.

- As Zonas Locais não oferecem suporte AWS Transit Gateway. Em vez disso, conecte-se à zona local usando uma interface virtual Direct Connect privada (VIF).
- Nem todas as Zonas Locais oferecem suporte a serviços como Amazon RDS, Amazon FSx, Amazon EMR ou ElastiCache Amazon, ou gateways NAT. Para obter mais informações, consulte Zonas locais da AWS features.
- Os Application Load Balancers em Locais Zones não oferecem suporte a mTLS ou sessões fixas.

Processo de adoção da nuvem híbrida

As seções a seguir discutem arquiteturas e detalhes de design para cada pilar da nuvem AWS híbrida:

- Rede na periferia
- Segurança na borda
- Resiliência na borda
- Planejamento de capacidade na borda
- Gerenciamento de infraestrutura de ponta

Rede na periferia

Ao projetar soluções que usam infraestrutura de AWS borda, como AWS Outposts Zonas Locais, você deve considerar cuidadosamente o design da rede. A rede forma a base da conectividade para alcançar cargas de trabalho implantadas nesses locais periféricos e é fundamental para garantir baixa latência. Esta seção descreve vários aspectos da conectividade de borda híbrida.

Arquitetura da VPC

Uma nuvem privada virtual (VPC) abrange todas as zonas de disponibilidade em sua. Região da AWS Você pode estender facilmente qualquer VPC na região para Outposts ou Zonas Locais AWS usando o console ou AWS CLI o () para adicionar uma sub-rede Outpost AWS Command Line Interface ou Zona Local. Os exemplos a seguir mostram como criar sub-redes em Zonas AWS Outposts Locais usando o: AWS CLI

- AWS Outposts: Para adicionar uma sub-rede Outpost a uma VPC, especifique o Amazon Resource Name (ARN) do Outpost.

```
aws ec2 create-subnet --vpc-id vpc-081ec835f3EXAMPLE \
--cidr-block 10.0.0.0/24 \
--outpost-arn arn:aws:outposts:us-west-2:11111111111:outpost/op-0e32example1 \
--tag-specifications ResourceType=subnet,Tags=[{Key=Name,Value=my-ipv4-only-subnet}]
```

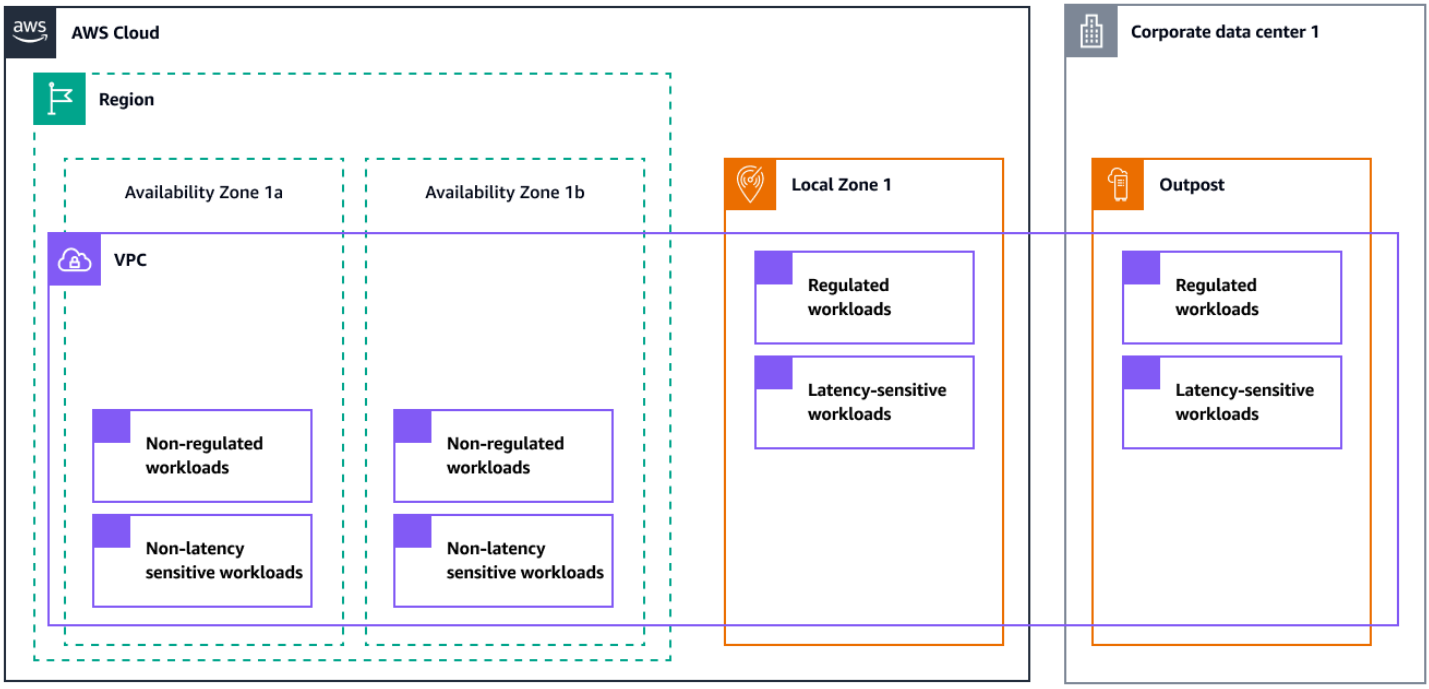
  Para obter mais informações, consulte a documentação do AWS Outposts.

- Zonas locais: para adicionar uma sub-rede de zona local a uma VPC, siga o mesmo procedimento usado com as zonas de disponibilidade, mas especifique a ID da zona local `<local-zone-name>` (no exemplo a seguir).

```
aws ec2 create-subnet --vpc-id vpc-081ec835f3EXAMPLE \
--cidr-block 10.0.1.0/24 \
--availability-zone <local-zone-name> \
--tag-specifications ResourceType=subnet,Tags=[{Key=Name,Value=my-ipv4-only-subnet}]
```

  Para obter mais informações, consulte a documentação de Locais Zones.

O diagrama a seguir mostra uma AWS arquitetura que inclui sub-redes Outpost e Local Zone.

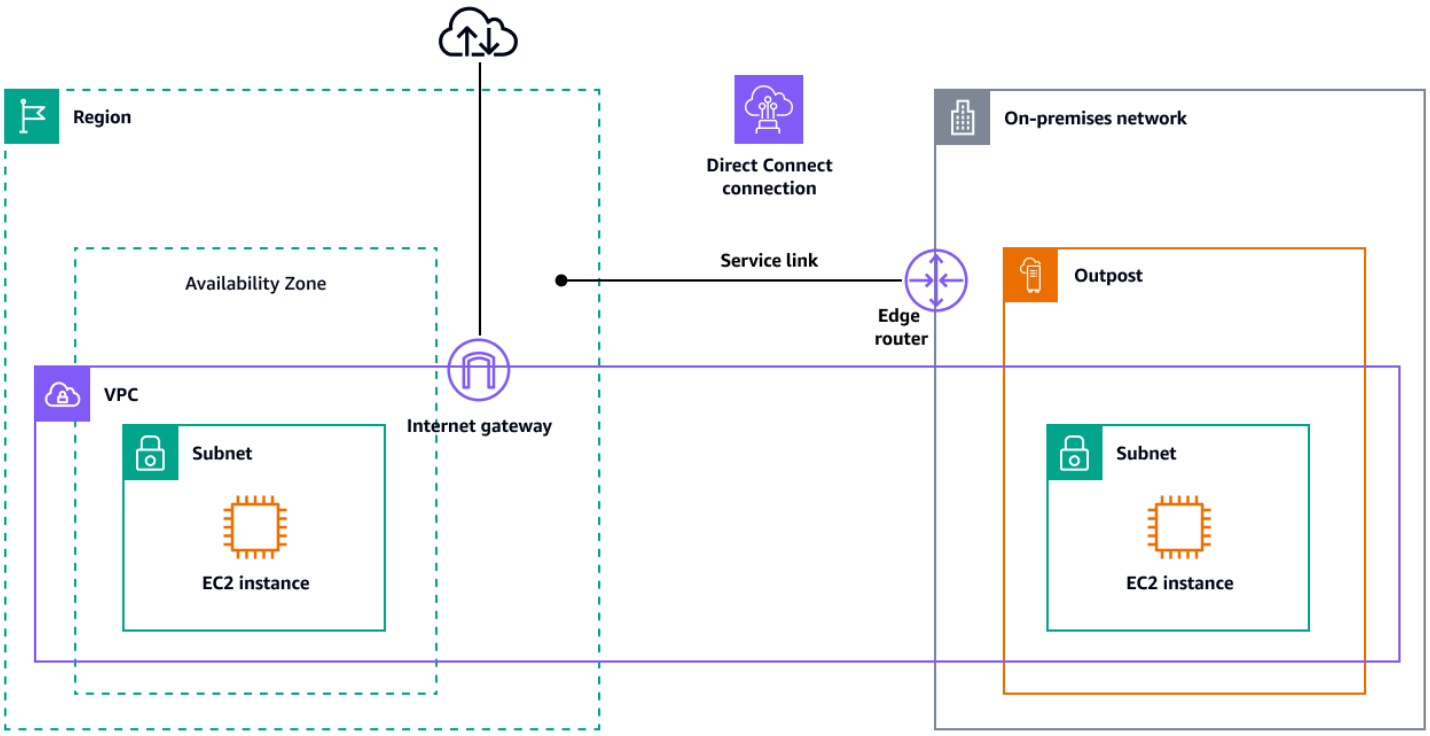


Tráfego da borda para a região

Ao projetar uma arquitetura híbrida usando serviços como Locais Zones e AWS Outposts, considere tanto os fluxos de controle quanto os fluxos de tráfego de dados entre as infraestruturas de borda e. Regiões da AWS Dependendo do tipo de infraestrutura de borda, sua responsabilidade pode variar: algumas infraestruturas exigem que você gerencie a conexão com a região principal, enquanto outras lidam com isso por meio da infraestrutura AWS global. Esta seção explora as implicações da conectividade do plano de controle e do plano de dados para Zonas Locais e. AWS Outposts

AWS Outposts plano de controle

AWS Outposts fornece uma construção de rede chamada link de serviço. O link de serviço é uma conexão obrigatória AWS Outposts entre a região selecionada Região da AWS ou principal (também chamada de região de origem). Ele permite o gerenciamento do Posto Avançado e a troca de tráfego entre o Posto Avançado e. Região da AWS O link do serviço usa um conjunto criptografado de conexões VPN para se comunicar com a região de origem. Você deve fornecer conectividade entre AWS Outposts e por meio de um link de internet ou de uma interface virtual Direct Connect pública (VIF pública) ou por meio de uma interface virtual Direct Connect privada (VIF privada). Região da AWS Para uma experiência e resiliência ideais, AWS recomenda que você use conectividade redundante de pelo menos 500 Mbps (1 Gbps é melhor) para a conexão do link de serviço com o. Região da AWS A conexão mínima de 500 Mbps do link de serviço permite que você inicie instâncias do Amazon EC2, anexe volumes do Amazon EBS e Serviços da AWS acesse métricas como Amazon EKS, Amazon EMR e Amazon. CloudWatch A rede deve suportar uma unidade de transmissão máxima (MTU) de 1.500 bytes entre o Outpost e os endpoints do link de serviço no terminal principal. Região da AWSPara obter mais informações, consulte AWS Outposts conectividade com Regiões da AWS na documentação do Outposts.



Para obter informações sobre a criação de arquiteturas resilientes para links de serviços que usam a Internet pública, consulte a seção Conectividade Anchor no AWS whitepaper Considerações sobre design Direct Connect e arquitetura de AWS Outposts alta disponibilidade.

AWS Outposts plano de dados

O plano de dados entre AWS Outposts e o Região da AWS é suportado pela mesma arquitetura de link de serviço usada pelo plano de controle. A largura de banda do link de serviço do plano de dados entre AWS Outposts e o Região da AWS deve se correlacionar com a quantidade de dados que devem ser trocados: quanto maior a dependência de dados, maior deve ser a largura de banda do link.

Os requisitos de largura de banda variam de acordo com as seguintes características:

- O número de AWS Outposts racks e configurações de capacidade
- Características da carga de trabalho, como tamanho da AMI, elasticidade do aplicativo e necessidades de velocidade de pico
- Tráfego de VPC para a região

O tráfego entre as instâncias do EC2 AWS Outposts e as instâncias do EC2 no Região da AWS tem um MTU de 1.300 bytes. Recomendamos que você discuta esses requisitos com um especialista em nuvem AWS híbrida antes de propor uma arquitetura que tenha co-dependências entre a região e. AWS Outposts

Plano de dados de Locais Zones

O plano de dados entre Locais Zones e o Região da AWS é suportado pela infraestrutura AWS global. O plano de dados é estendido por meio de uma VPC de Região da AWS até uma zona local. As Zonas Locais também fornecem uma conexão segura e de alta largura de banda com o Região da AWS e permitem que você se conecte perfeitamente a toda a gama de serviços regionais por meio das mesmas APIs e conjuntos de ferramentas.

A tabela a seguir mostra as opções de conexão e as MTUs associadas.

De	Para	MTU
Amazon EC2 na região	Amazon EC2 em Zonas Locais	1.300 bytes
Direct Connect	Zonas Locais	1.468 bytes
Gateway da Internet	Zonas Locais	1.500 bytes

De	Para	MTU
Amazon EC2 em Zonas Locais	Amazon EC2 em Zonas Locais	9.001 bytes

Locais Zones usam a infraestrutura AWS global com a qual se conectar Regiões da AWS. A infraestrutura é totalmente gerenciada por AWS, então você não precisa configurar essa conectividade. Recomendamos que você discuta seus requisitos e considerações sobre Zonas Locais com um especialista em nuvem AWS híbrida antes de projetar qualquer arquitetura que tenha co-dependências entre a Região e as Zonas Locais.

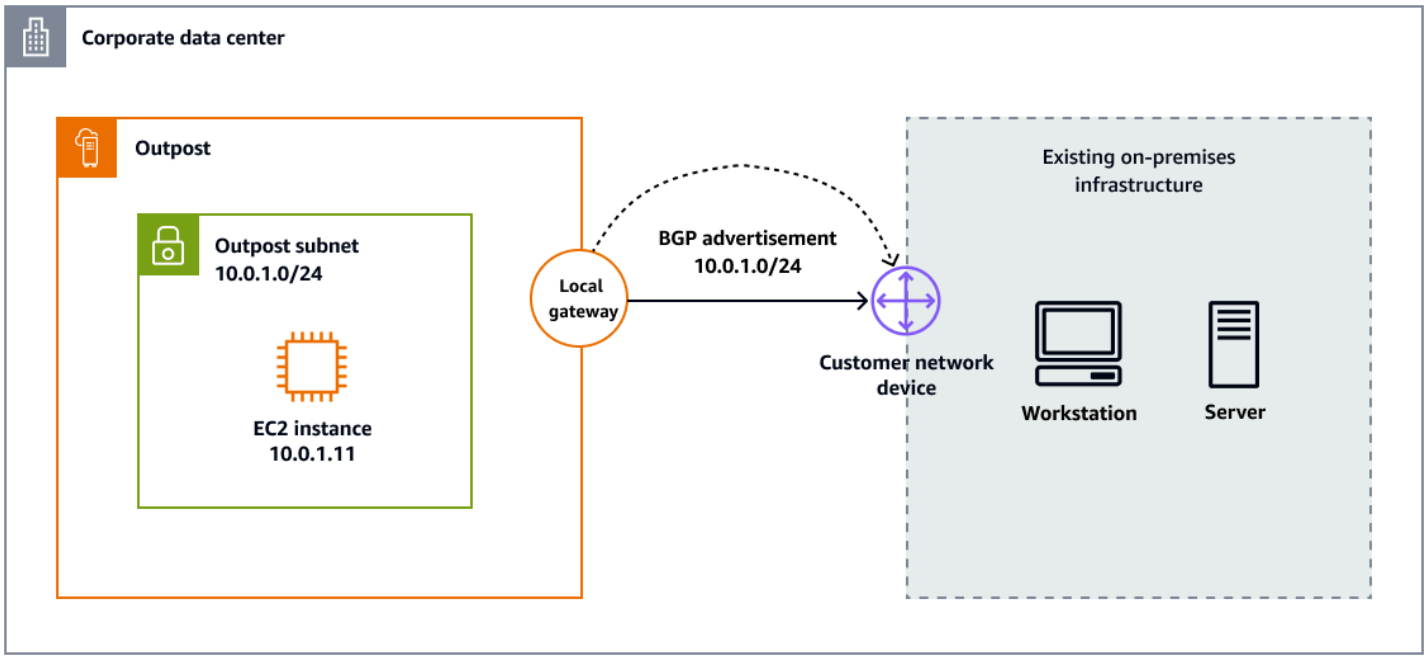
Da borda ao tráfego local

AWS os serviços de nuvem híbrida são projetados para lidar com casos de uso que exigem baixa latência, processamento local de dados ou conformidade com a residência de dados. A arquitetura de rede para acessar esses dados é importante e depende se sua carga de trabalho está sendo executada em AWS Outposts ou em Zonas Locais. A conectividade local também requer um escopo bem definido, conforme discutido nas seções a seguir.

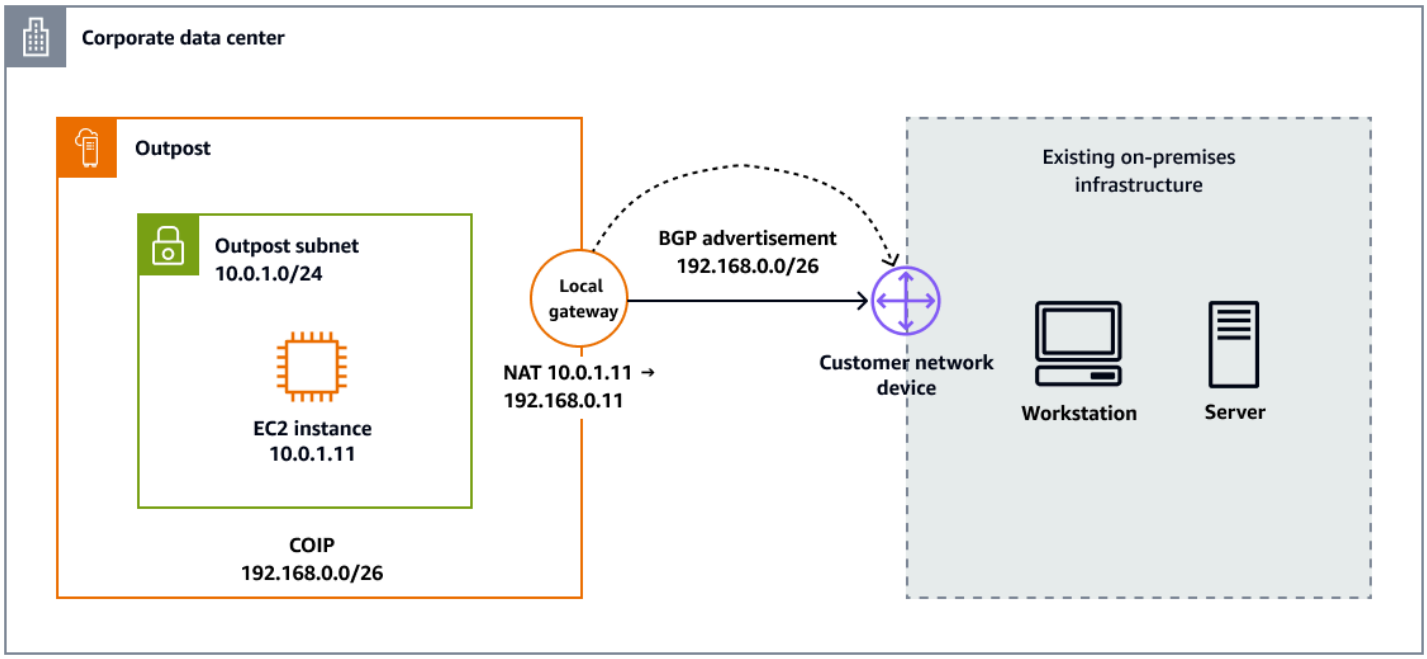
AWS Outposts gateway local

O gateway local (LGW) é um componente central da AWS Outposts arquitetura. O gateway local permite a conectividade entre suas sub-redes Outpost e sua rede on-premises própria. A função principal de um LGW é fornecer conectividade de um Posto Avançado à sua rede local local. Ele também fornece conectividade com a Internet por meio de sua rede local por meio de roteamento direto de VPC ou endereços IP de propriedade do cliente.

- O roteamento direto de VPC usa o endereço IP privado das instâncias em sua VPC para facilitar a comunicação com sua rede local. Esses endereços são anunciados em sua rede local com o Border Gateway Protocol (BGP). O anúncio para o BGP é apenas para os endereços IP privados que pertencem às sub-redes em seu rack Outpost. Esse tipo de roteamento é o modo padrão para AWS Outposts. Nesse modo, o gateway local não executa NAT para instâncias e você não precisa atribuir endereços IP elásticos às suas instâncias do EC2. O diagrama a seguir mostra um gateway AWS Outposts local que usa roteamento direto de VPC.



- Com endereços IP de propriedade do cliente, você pode fornecer um intervalo de endereços, conhecido como pool de endereços IP de propriedade do cliente (CoIP), que suporta intervalos CIDR sobrepostos e outras topologias de rede. Ao escolher um CoIP, você deve criar um pool de endereços, atribuí-lo à tabela de rotas do gateway local e anunciar esses endereços de volta à sua rede por meio do BGP. Os endereços CoIP fornecem conectividade local ou externa aos recursos em sua rede local. Você pode atribuir esses endereços IP aos recursos em seu Outpost, como instâncias do EC2, alocando um novo endereço IP elástico do CoIP e, em seguida, atribuindo-o ao seu recurso. O diagrama a seguir mostra um gateway AWS Outposts local que usa o modo CoIP.



A conectividade local de AWS Outposts uma rede local requer algumas configurações de parâmetros, como ativar o protocolo de roteamento BGP e anunciar prefixos entre os pares do BGP. A MTU que pode ser suportada entre seu Outpost e o gateway local é de 1.500 bytes. Para obter mais informações, entre em contato com um especialista em nuvem AWS híbrida ou revise a AWS Outposts documentação.

Locais Zones e a internet

Os setores que exigem baixa latência ou residência local de dados (exemplos incluem jogos, transmissão ao vivo, serviços financeiros e o governo) podem usar o Local Zones para implantar e fornecer seus aplicativos aos usuários finais pela Internet. Durante a implantação de uma zona local, você deve alocar endereços IP públicos para uso em uma zona local. Ao alocar endereços IP elásticos, você pode especificar o local a partir do qual o endereço IP é anunciado. Esse local é chamado de grupo de borda de rede. Um grupo de borda de rede é uma coleção de Zonas de Disponibilidade, Zonas Locais ou AWS Wavelength Zonas a partir das quais AWS anuncia um endereço IP público. Isso ajuda a garantir latência mínima ou distância física entre a AWS rede e os usuários que acessam os recursos nessas zonas. Para ver todos os grupos de bordas de rede para Zonas Locais, consulte Zonas Locais Disponíveis na documentação de Zonas Locais.

Para expor uma EC2-hosted carga de trabalho da Amazon em uma zona local à Internet, você pode ativar a opção IP Auto-assign público ao iniciar a instância do EC2. Se você usa um Application Load Balancer, pode defini-lo como voltado para a Internet para que os endereços IP públicos atribuídos

à zona local possam ser propagados pela rede de fronteira associada à zona local. Além disso, ao usar endereços IP elásticos, você pode associar um desses recursos a uma instância do EC2 após seu lançamento. Quando você envia tráfego por meio de um gateway de Internet em Zonas Locais, as mesmas especificações de largura de banda da instância usadas pela Região são aplicadas. O tráfego de rede da zona local vai diretamente para a Internet ou para os pontos de presença (PoPs) sem atravessar a região principal da zona local, para permitir o acesso à computação de baixa latência.

As Zonas Locais oferecem as seguintes opções de conectividade pela Internet:

- Acesso público: conecta cargas de trabalho ou dispositivos virtuais à Internet usando endereços IP elásticos por meio de um gateway de internet.
- Acesso externo à Internet: permite que os recursos alcancem endpoints públicos por meio de instâncias de conversão de endereços de rede (NAT) ou dispositivos virtuais com endereços IP elásticos associados, sem exposição direta à Internet.
- Conectividade VPN: estabelece conexões privadas usando a VPN IPsec (Internet Protocol Security) por meio de dispositivos virtuais com endereços IP elásticos associados.

Para obter mais informações, consulte Opções de conectividade para Zonas Locais na documentação de Zonas Locais.

Zonas Locais e Direct Connect

Também há suporte para Locais Zones Direct Connect, o que permite rotear seu tráfego por meio de uma conexão de rede privada. Para obter mais informações, consulte Direct Connect in Local Zones na documentação de Locais Zones.

Zonas Locais e gateways de trânsito

AWS Transit Gateway não oferece suporte a anexos diretos de VPC às sub-redes da zona local. No entanto, você pode se conectar às cargas de trabalho da Zona Local criando anexos do Transit Gateway nas sub-redes principais da Zona de Disponibilidade da mesma VPC. Essa configuração permite a interconectividade entre várias VPCs e suas cargas de trabalho de zona local. Para obter mais informações, consulte Conexão do Transit Gateway entre Zonas Locais na documentação de Zonas Locais.

Zonas locais e emparelhamento de VPC

Você pode estender qualquer VPC de uma região principal para uma zona local criando uma nova sub-rede e atribuindo-a à zona local. O emparelhamento de VPC pode ser estabelecido entre VPCs que são estendidas para Zonas Locais. Quando as VPCs emparelhadas estão na mesma zona local, o tráfego permanece dentro da zona local e não passa pela região principal.

Segurança na borda

No Nuvem AWS, a segurança é a principal prioridade. À medida que as organizações adotam a escalabilidade e a flexibilidade da nuvem, AWS ajuda-as a adotar segurança, identidade e conformidade como fatores-chave de negócios. AWS integra a segurança em sua infraestrutura principal e oferece serviços para ajudá-lo a atender aos seus requisitos exclusivos de segurança na nuvem. Ao expandir o escopo de sua arquitetura para o Nuvem AWS, você se beneficia da integração de infraestruturas como Locais Zones e Outposts no Regiões da AWS. Essa integração permite AWS estender um grupo seleto dos principais serviços de segurança até a borda.

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

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que é executada Serviços da AWS no Nuvem AWS. AWS também fornece serviços que você pode usar com segurança. Third-party auditores testam e verificam regularmente a eficácia da AWS segurança como parte dos programas de AWS conformidade.
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS service (Serviço da AWS) que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade dos dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Proteção de dados

O modelo de responsabilidade AWS compartilhada se aplica à proteção de dados em AWS Outposts Zonas locais da AWS e. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa a Nuvem AWS (segurança da nuvem). Você é responsável por manter o controle sobre o conteúdo hospedado nessa infraestrutura (segurança na nuvem). 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 Identity and Access Management (IAM) ou Centro de Identidade do AWS IAM. Isso concede a cada usuário apenas as permissões necessárias para cumprir suas tarefas.

Criptografia em repouso

Criptografia em volumes do EBS

Com isso AWS Outposts, todos os dados são criptografados em repouso. O material da chave é embalado com uma chave externa, a Nitro Security Key (NSK), que é armazenada em um dispositivo removível. O NSK é necessário para descriptografar os dados em seu rack Outpost. Você pode usar a criptografia do Amazon EBS para volumes do EBS e snapshots. A criptografia do Amazon EBS usa AWS Key Management Service (AWS KMS) e chaves KMS.

No caso de Zonas Locais, todos os volumes do EBS são criptografados por padrão em todas as Zonas Locais, exceto na lista documentada nas Zonas locais da AWS Perguntas Frequentes (consulte a pergunta: Qual é o comportamento padrão de criptografia dos volumes do EBS nas Zonas Locais?), a menos que a criptografia esteja habilitada para a conta.

Criptografia no Amazon S3 em Outposts

Por padrão, todos os dados armazenados no Amazon S3 em Outposts são criptografados usando criptografia do lado do servidor com chaves de criptografia gerenciadas pelo Amazon S3 (). SSE-S3 Opcionalmente, você pode usar a criptografia do lado do servidor com chaves de criptografia fornecidas pelo cliente (). SSE-C Para usar SSE-C, especifique uma chave de criptografia como parte de suas solicitações de API de objetos. Server-side a criptografia criptografa somente os dados do objeto, não os metadados do objeto.

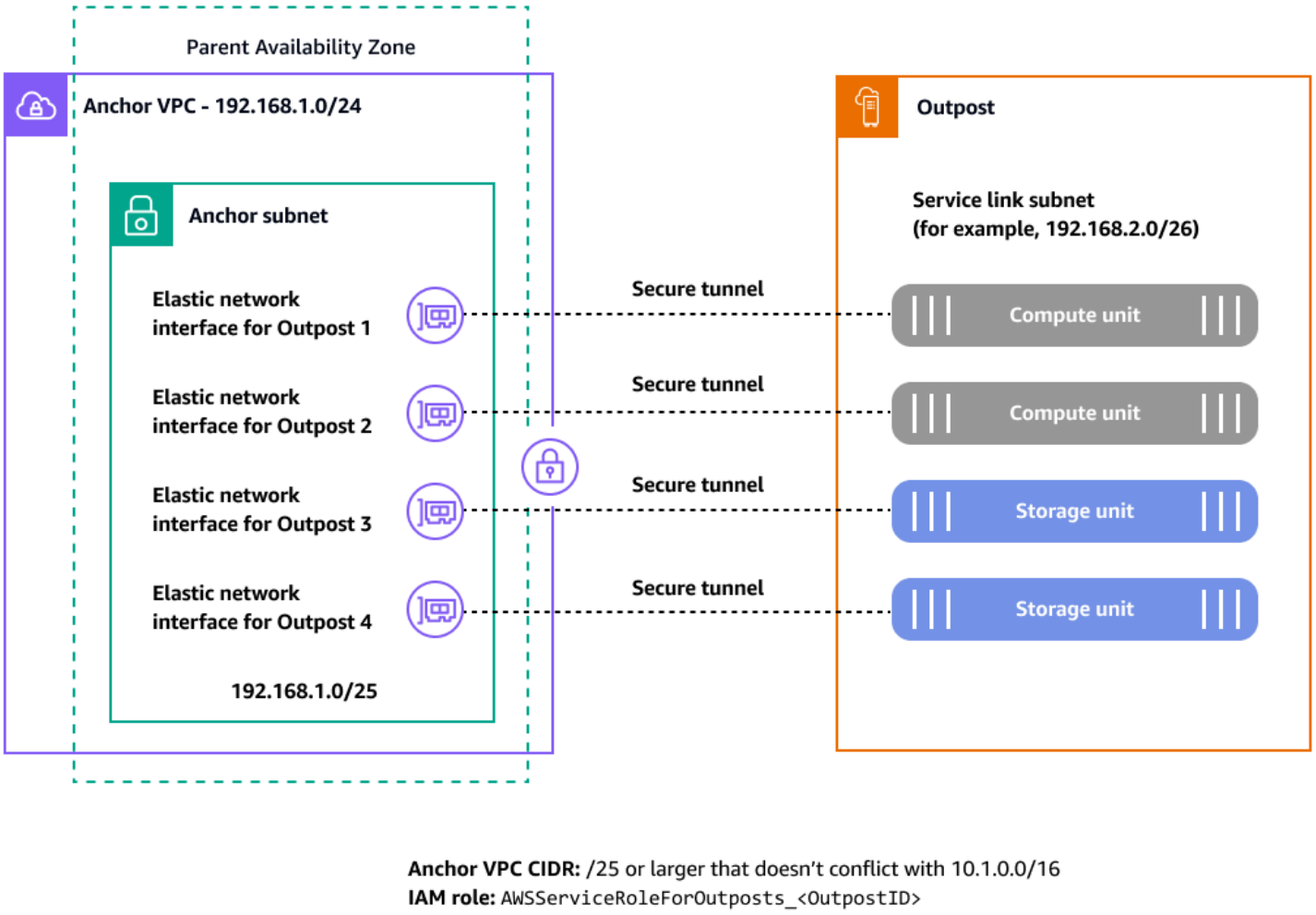
> **Note**
>
> O Amazon S3 on Outposts não oferece suporte à criptografia do lado do servidor com chaves KMS (). SSE-KMS

Criptografia em trânsito

Pois AWS Outposts, o link de serviço é uma conexão necessária entre o servidor do Outposts e a região escolhida Região da AWS (ou de origem) e permite o gerenciamento do Outpost e a troca

de tráfego de e para o. Região da AWS O link de serviço usa uma VPN AWS gerenciada para se comunicar com a região de origem. Cada host interno AWS Outposts cria um conjunto de túneis VPN para dividir o tráfego do plano de controle e o tráfego de VPC. Dependendo da conectividade do link de serviço (internet ou Direct Connect) AWS Outposts, esses túneis exigem que portas de firewall sejam abertas para que o link de serviço crie a sobreposição sobre ele. Para obter informações técnicas detalhadas sobre a segurança AWS Outposts e o link do serviço, consulte Conectividade por meio do link de serviço e Segurança da infraestrutura AWS Outposts na AWS Outposts documentação.

O link AWS Outposts de serviço cria túneis criptografados que estabelecem a conectividade do plano de controle e do plano de dados com o pai Região da AWS, conforme ilustrado no diagrama a seguir.



Cada AWS Outposts host (computação e armazenamento) requer esses túneis criptografados em portas TCP e UDP conhecidas para se comunicar com sua região principal. A tabela a seguir mostra as portas e endereços de origem e destino dos protocolos UDP e TCP.

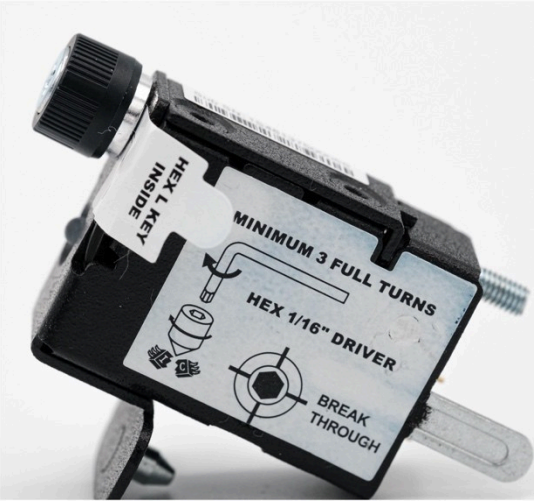
Protocolo	Porta de origem	Endereço de origem	Porta de destino	Endereço de destino
UDP	443	AWS Outposts link de serviço /26	443	AWS Outposts Rotas públicas da região ou VPC CIDR âncora
TCP	1025-65535	AWS Outposts link de serviço /26	443	AWS Outposts Rotas públicas da região ou VPC CIDR âncora

As Zonas Locais também são conectadas à região principal por meio do backbone privado global redundante e de altíssima largura de banda da Amazon. Essa conexão fornece aos aplicativos que estão sendo executados em Zonas Locais acesso rápido, seguro e contínuo a outros Serviços da AWS. Desde que as Zonas Locais façam parte da infraestrutura AWS global, todos os dados que fluem pela rede AWS global são criptografados automaticamente na camada física antes de saírem das instalações AWS protegidas. Se você tiver requisitos específicos para criptografar os dados em trânsito entre seus locais locais e Direct Connect PoPs acessar uma zona local, você pode habilitar a Segurança MAC (MACsec) entre seu roteador ou switch local e o endpoint. Direct Connect Para obter mais informações, consulte a postagem do AWS blog Adicionar segurança MACsec às Direct Connect conexões.

Exclusão de dados

Quando você interrompe ou encerra uma instância do EC2 AWS Outposts, a memória alocada para ela é limpa (definida como zero) pelo hipervisor antes de ser alocada para uma nova instância, e cada bloco de armazenamento é redefinido. A exclusão de dados do hardware do Outpost envolve o uso de hardware especializado. O NSK é um pequeno dispositivo, ilustrado na fotografia a seguir, que se conecta à frente de cada unidade de computação ou armazenamento em um Posto Avançado. Ele foi projetado para fornecer um mecanismo para evitar que seus dados sejam expostos do seu data center ou site de colocation. Os dados no dispositivo Outpost são protegidos embalando o material de chaveamento usado para criptografar o dispositivo e armazenando

o material embalado no NSK. Ao retornar um host do Outpost, você destrói o NSK girando um pequeno parafuso no chip que esmaga o NSK e destrói fisicamente o chip. Destruir o NSK destrói os dados criptograficamente em seu Posto Avançado.



Gerenciamento de identidade e acesso

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) a usar AWS Outposts os recursos. Se você tiver um Conta da AWS, poderá usar o IAM sem custo adicional.

A tabela a seguir lista os recursos do IAM com os quais você pode usar AWS Outposts.

Recurso do IAM	AWS Outposts apoio
Identity-based políticas	Sim
Resource-based políticas	Sim*
Ações de políticas	Sim
Recursos de políticas	Sim
Chaves de condição de política (específicas do serviço)	Sim
Listas de controle de acesso (ACLs)	Não

Recurso do IAM	AWS Outposts apoio
Attribute-based controle de acesso (ABAC) (tags nas políticas)	Sim
Credenciais temporárias	Sim
Permissões de entidade principal	Sim
Perfis de serviço	Não
Service-linked funções	Sim

* Além das políticas baseadas em identidade do IAM, o Amazon S3 on Outposts oferece suporte a políticas de bucket e de ponto de acesso. Essas são políticas baseadas em recursos anexadas ao recurso Amazon S3 on Outposts.

Para obter mais informações sobre como esses recursos são suportados no AWS Outposts, consulte o guia AWS Outposts do usuário.

Segurança da infraestrutura

A proteção da infraestrutura é elemento essencial de um programa de segurança da informação. Ele garante que os sistemas e serviços de carga de trabalho estejam protegidos contra acesso não intencional e não autorizado e possíveis vulnerabilidades. Por exemplo, você define limites de confiança (por exemplo, limites de rede e conta), configuração e manutenção da segurança do sistema (por exemplo, fortalecimento, minimização e aplicação de patches), autenticação e autorizações do sistema operacional (por exemplo, usuários, chaves e níveis de acesso) e outros pontos apropriados de aplicação de políticas (por exemplo, firewalls de aplicativos web ou gateways de API).

AWS fornece várias abordagens para a proteção da infraestrutura, conforme discutido nas seções a seguir.

Proteção de redes

Seus usuários podem fazer parte de sua força de trabalho ou de seus clientes e podem estar localizados em qualquer lugar. Por esse motivo, você não pode confiar em todos que têm acesso

à sua rede. Ao seguir o princípio de aplicar segurança em todas as camadas, você emprega uma abordagem de confiança zero. No modelo de segurança de confiança zero, os componentes ou microsserviços do aplicativo são considerados discretos, e nenhum componente ou microsserviço confia em nenhum outro componente ou microsserviço. Para obter segurança de confiança zero, siga estas recomendações:

- Crie camadas de rede. As redes em camadas ajudam a agrupar logicamente componentes de rede semelhantes. Eles também reduzem o escopo potencial de impacto do acesso não autorizado à rede.
- Controle as camadas de tráfego. Aplique vários controles com uma abordagem de defesa aprofundada para tráfego de entrada e saída. Isso inclui o uso de grupos de segurança (firewalls de inspeção de estado), ACLs de rede, sub-redes e tabelas de rotas.
- Implemente inspeção e proteção. Inspecione e filtre seu tráfego em cada camada. Você pode inspecionar suas configurações de VPC em busca de possíveis acessos não intencionais usando o Network Access Analyzer. Você pode especificar seus requisitos de acesso à rede e identificar possíveis caminhos de rede que não os atendam.

Protegendo os recursos computacionais

Os recursos computacionais incluem instâncias do EC2, contêineres, AWS Lambda funções, serviços de banco de dados, dispositivos de IoT e muito mais. Cada tipo de recurso computacional exige uma abordagem diferente de segurança. No entanto, esses recursos compartilham estratégias comuns que você precisa considerar: defesa em profundidade, gerenciamento de vulnerabilidades, redução na superfície de ataque, automação da configuração e operação e execução de ações à distância.

Aqui estão as orientações gerais para proteger seus recursos computacionais para os principais serviços:

- Crie e mantenha um programa de gerenciamento de vulnerabilidades. Examine e corrija regularmente recursos como instâncias do EC2, contêineres do Amazon Elastic Container Service (Amazon ECS) e cargas de trabalho do Amazon Elastic Kubernetes Service (Amazon EKS).
- Automatize a proteção computacional. Automatize seus mecanismos de proteção computacional, incluindo gerenciamento de vulnerabilidades, redução na superfície de ataque e gerenciamento de recursos. Essa automação libera tempo que você pode usar para proteger outros aspectos da sua carga de trabalho e ajuda a reduzir o risco de erro humano.

- Reduza a superfície de ataque. Reduza sua exposição ao acesso não intencional fortalecendo seus sistemas operacionais e minimizando os componentes, bibliotecas e serviços consumíveis externos que você usa.

Além disso, para cada um AWS service (Serviço da AWS) que você usa, verifique as recomendações de segurança específicas na documentação do serviço.

Acesso à Internet

AWS Outposts Tanto as Zonas Locais quanto as Zonas Locais fornecem padrões de arquitetura que dão às suas cargas de trabalho acesso de e para a Internet. Ao usar esses padrões, considere o consumo de internet da região uma opção viável somente se você o usar para corrigir, atualizar, acessar repositórios Git externos e cenários semelhantes. AWS Para esse padrão arquitetônico, os conceitos de inspeção de entrada centralizada e saída centralizada da Internet se aplicam. Esses padrões de acesso usam AWS Transit Gateway gateways NAT, firewalls de rede e outros componentes que residem Regiões da AWS, mas estão conectados às AWS Outposts Zonas Locais por meio do caminho de dados entre a Região e a borda.

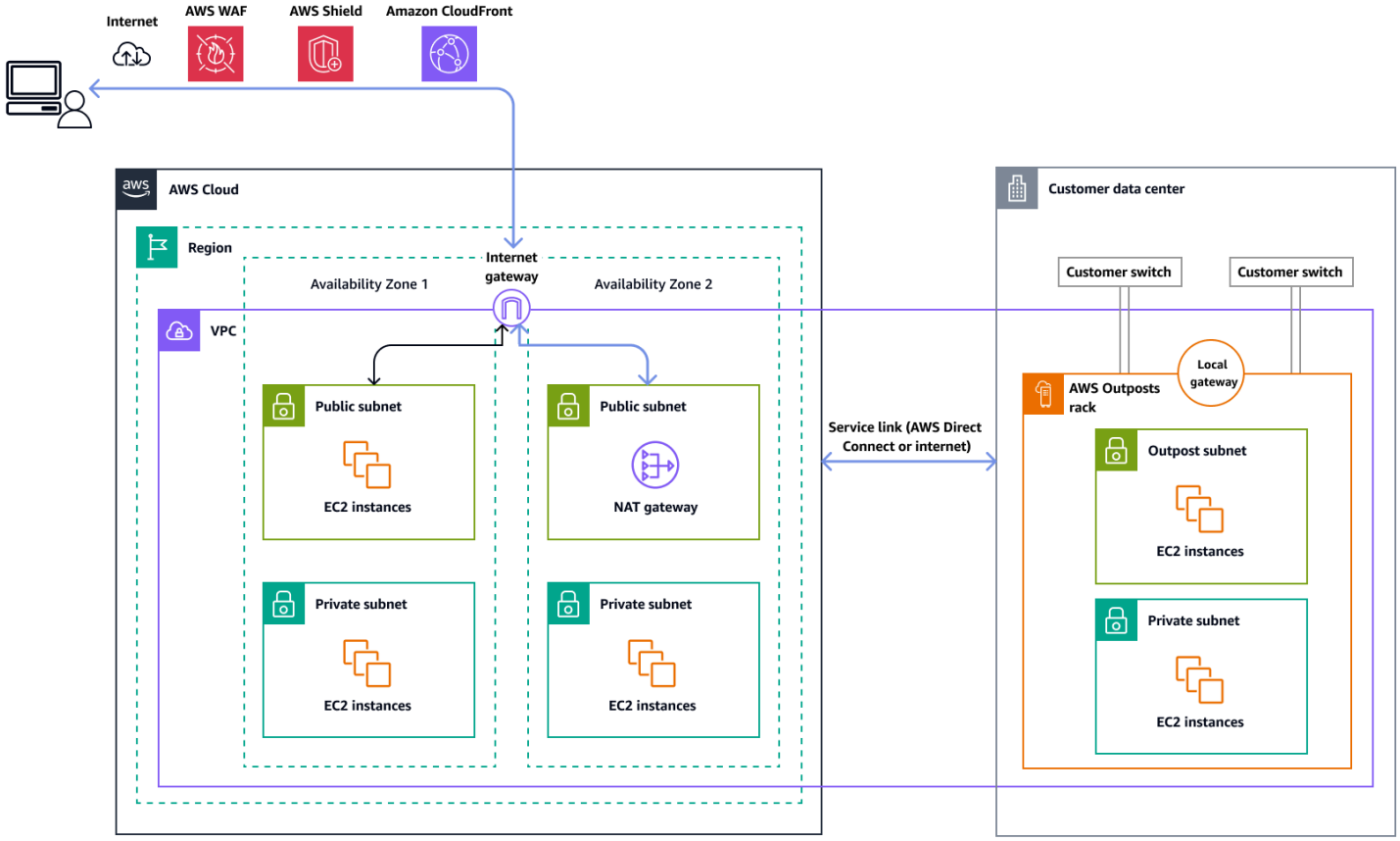
Local Zones adota uma construção de rede chamada grupo de borda de rede, que é usada em Regiões da AWS. AWS anuncia endereços IP públicos desses grupos exclusivos. Um grupo de bordas de rede consiste em Zonas de Disponibilidade, Zonas Locais ou Zonas de Wavelength. Você pode alocar explicitamente um pool de endereços IP públicos para uso em um grupo de borda de rede. Você pode usar um grupo de borda de rede para estender o gateway da Internet às Zonas Locais, permitindo que endereços IP elásticos sejam atendidos pelo grupo. Essa opção exige que você implante outros componentes para complementar os principais serviços disponíveis em Locais Zones. Esses componentes podem vir de ISVs e ajudá-lo a criar camadas de inspeção em sua zona local, conforme descrito na postagem do AWS blog Arquiteturas de inspeção híbridas com. Zonas locais da AWS

Em AWS Outposts, se você quiser usar o gateway local (LGW) para acessar a Internet a partir da sua rede, deverá modificar a tabela de rotas personalizada associada à AWS Outposts sub-rede. A tabela de rotas deve ter uma entrada de rota padrão (0.0.0). 0/0) que usa o LGW como o próximo salto. Você é responsável por implementar os controles de segurança restantes em sua rede local, incluindo defesas perimetrais, como firewalls e sistemas de prevenção de intrusões ou sistemas de detecção de intrusões (). IPS/IDS Isso se alinha ao modelo de responsabilidade compartilhada, que divide as tarefas de segurança entre você e o provedor de nuvem.

Acesso à Internet através dos pais Região da AWS

Nessa opção, as cargas de trabalho no Outpost acessam a Internet por meio do link de serviço e do gateway de Internet no principal. Região da AWS O tráfego de saída para a Internet pode ser roteado por meio do gateway NAT que é instanciado em sua VPC. Para obter segurança adicional para seu tráfego de entrada e saída, você pode usar serviços AWS de segurança como AWS WAF, AWS Shield, e Amazon CloudFront no. Região da AWS

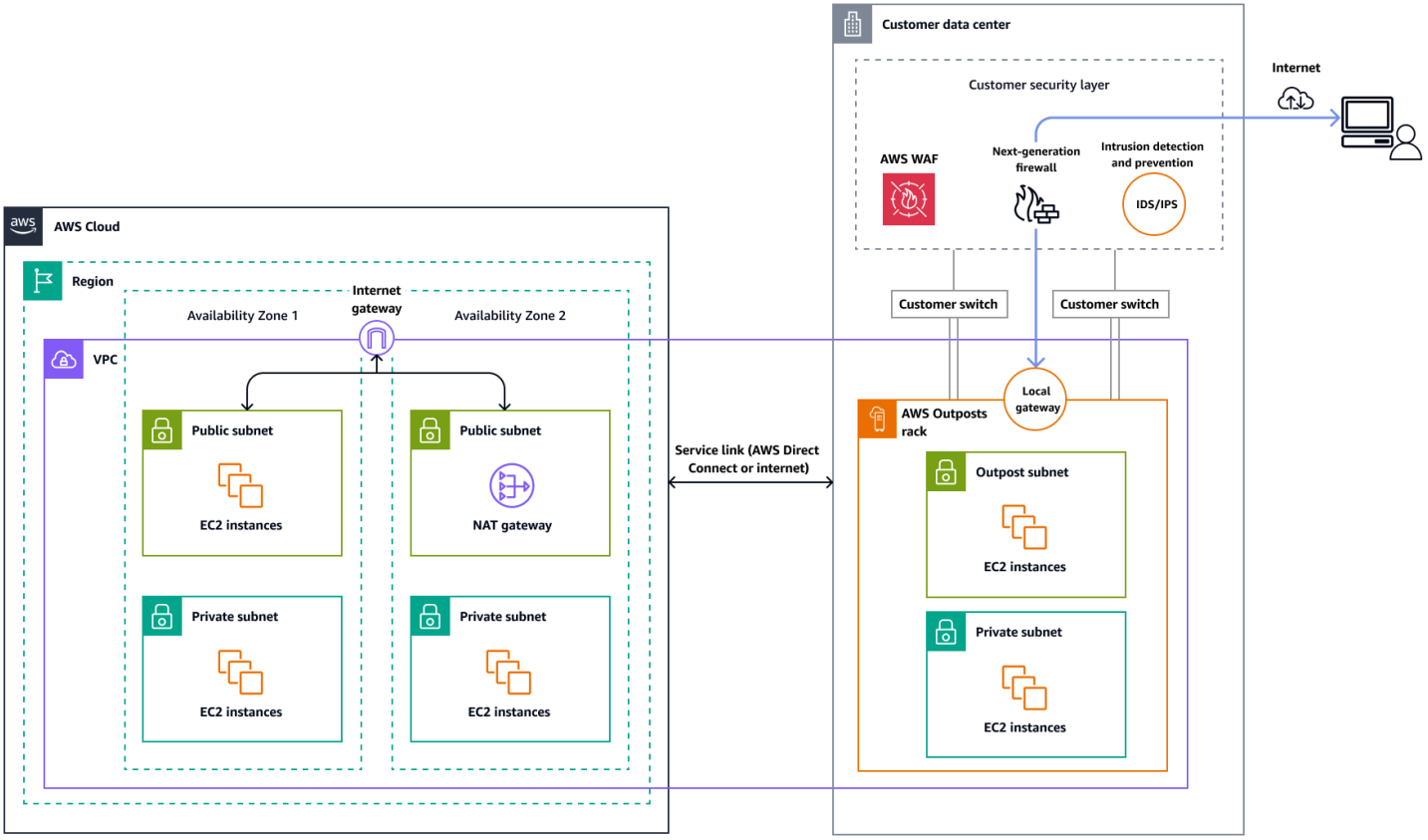
O diagrama a seguir mostra o tráfego entre a carga de trabalho na AWS Outposts instância e a Internet passando pela principal Região da AWS.



Acesso à internet por meio da rede do data center local

Nessa opção, as cargas de trabalho no Outpost acessam a internet por meio de seu data center local. O tráfego da carga de trabalho que acessa a Internet atravessa seu ponto de presença na Internet local e sai localmente. Nesse caso, a infraestrutura de segurança de rede do seu data center local é responsável por proteger o tráfego da AWS Outposts carga de trabalho.

A imagem a seguir mostra o tráfego entre uma carga de trabalho na AWS Outposts sub-rede e a Internet passando por um data center.



Governança da infraestrutura

Independentemente de suas cargas de trabalho serem implantadas em uma Região da AWS zona local ou em um posto avançado, você pode usá-las AWS Control Tower para governança da infraestrutura. AWS Control Tower oferece uma maneira simples de configurar e administrar um ambiente com AWS várias contas, seguindo as melhores práticas prescritivas. AWS Control Tower orquestra os recursos de vários outros Serviços da AWS, inclusive AWS Organizations AWS Service Catalog, e do IAM Identity Center (veja todos os serviços integrados) para criar uma landing zone em menos de uma hora. Os recursos são configurados e gerenciados em seu nome.

AWS Control Tower fornece governança unificada em todos os AWS ambientes, incluindo Regiões, Zonas Locais (extensões de baixa latência) e Outposts (infraestrutura local). Isso ajuda a garantir segurança e conformidade consistentes em toda a sua arquitetura de nuvem híbrida. Para obter mais informações, consulte a documentação do AWS Control Tower.

Você pode configurar AWS Control Tower recursos, como grades de proteção, para atender aos requisitos de residência de dados em governos e setores regulamentados, como instituições de

serviços financeiros (FSIs). Para entender como implantar grades de proteção para residência de dados na borda, veja o seguinte:

- Melhores práticas para gerenciar a residência de dados Zonas locais da AWS usando controles de landing zone (postagem AWS no blog)
- Arquitetura para residência de dados com grades de proteção em AWS Outposts rack e landing zone (postagem no blog)AWS
- Residência de dados com o Hybrid Cloud Services Lens (documentação da AWS Well-Architected estrutura)

Compartilhando recursos do Outposts

Como um Posto Avançado é uma infraestrutura finita que reside em seu data center ou em um espaço de co-localização, para uma governança centralizada AWS Outposts, você precisa controlar centralmente com quais contas AWS Outposts os recursos são compartilhados.

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 outros Contas da AWS que estão na mesma organização em. AWS Organizations Como proprietário do Outpost, você pode criar e gerenciar recursos do Outpost a partir de um local central e compartilhar os recursos entre vários membros da sua Contas da AWS AWS organização. Isso permite que outros consumidores usem sites do Outposts, configurem VPCs e iniciem e executem instâncias no Outpost compartilhado.

Os recursos compartilháveis AWS Outposts são:

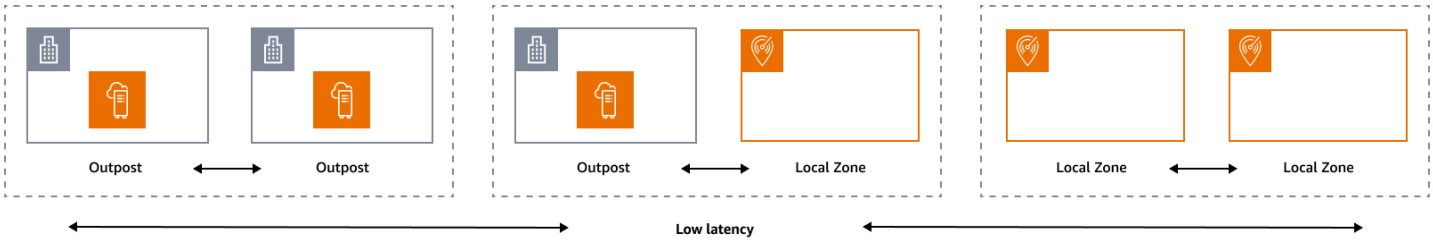
- Hosts dedicados alocados
- Reservas de capacidade
- Customer-owned Pools de endereços IP (CoIP)
- Tabelas de rotas de gateway local
- Outposts
- Amazon S3 on Outposts
- Sites
- Sub-redes

Para seguir as melhores práticas para compartilhar recursos do Outposts em um ambiente com várias contas, consulte as seguintes AWS postagens no blog:

- Compartilhamento AWS Outposts em um AWS ambiente com várias contas: Parte 1
- Compartilhamento AWS Outposts em um AWS ambiente com várias contas: Parte 2

Resiliência na borda

O pilar de confiabilidade engloba a capacidade de uma carga de trabalho realizar a função pretendida de forma correta e consistente quando se espera que isso aconteça. Isso inclui a capacidade de operar e testar a carga de trabalho durante seu ciclo de vida. Nesse sentido, ao projetar uma arquitetura resiliente na borda, você deve primeiro considerar quais infraestruturas você usará para implantar essa arquitetura. Há três combinações possíveis de implementar usando Zonas locais da AWS e AWS Outposts: posto avançado para posto avançado, posto avançado para zona local e zona local para zona local, conforme ilustrado no diagrama a seguir. Embora existam outras possibilidades para arquiteturas resilientes, como combinar serviços de AWS ponta com a infraestrutura local tradicional Regiões da AWS, ou, este guia se concentra nessas três combinações que se aplicam ao design de serviços de nuvem híbrida



Considerações sobre infraestrutura

Em AWS, um dos princípios fundamentais do design de serviços é evitar pontos únicos de falha na infraestrutura física subjacente. Por causa desse princípio, o AWS software e os sistemas usam várias zonas de disponibilidade e são resilientes às falhas de uma única zona. Na borda, AWS oferece infraestruturas baseadas em Locais Zones e Outposts. Portanto, um fator crítico para garantir a resiliência no design da infraestrutura é definir onde os recursos de um aplicativo são implantados.

Zonas Locais

As Zonas Locais agem de forma semelhante às Zonas de Disponibilidade dentro delas Região da AWS, pois podem ser selecionadas como um local de posicionamento para AWS recursos zonais,

como sub-redes e instâncias EC2. No entanto, eles não estão localizados em um Região da AWS, mas perto de grandes centros populacionais, industriais e de TI onde não Região da AWS existem atualmente. Apesar disso, eles ainda mantêm conexões seguras e de alta largura de banda entre as cargas de trabalho locais na zona local e as cargas de trabalho que estão sendo executadas na. Região da AWS Portanto, você deve usar as Zonas Locais para implantar cargas de trabalho mais próximas de seus usuários para requisitos de baixa latência.

Outposts

AWS Outposts é um serviço totalmente gerenciado que estende a AWS infraestrutura Serviços da AWS, as APIs e as ferramentas ao seu data center. A mesma infraestrutura de hardware usada no Nuvem AWS é instalada em seu data center. Outposts são então conectados ao mais próximo. Região da AWS Você pode usar o Outposts para suportar suas cargas de trabalho com baixa latência ou requisitos locais de processamento de dados.

Zonas de disponibilidade para pais

Cada zona local ou posto avançado tem uma região principal (também chamada de região de origem). A região principal é onde o plano de controle da infraestrutura de AWS ponta (posto avançado ou zona local) está ancorado. No caso de Zonas Locais, a Região principal é um componente arquitetônico fundamental de uma Zona Local e não pode ser modificada pelos clientes. AWS Outposts estende o Nuvem AWS para seu ambiente local, portanto, você deve selecionar uma região e uma zona de disponibilidade específicas durante o processo de pedido. Essa seleção ancora o plano de controle da implantação do Outposts na AWS infraestrutura escolhida.

Quando você desenvolve arquiteturas de alta disponibilidade na borda, a região principal dessas infraestruturas, como Outposts ou Locais Zones, deve ser a mesma, para que uma VPC possa ser estendida entre elas. Essa VPC estendida é a base para a criação dessas arquiteturas de alta disponibilidade. Ao definir uma arquitetura altamente resiliente, é por isso que você deve validar a região principal e a zona de disponibilidade da região em que o serviço será (ou está) ancorado. Conforme ilustrado no diagrama a seguir, se você quiser implantar uma solução de alta disponibilidade entre dois Postos Avançados, deverá escolher duas Zonas de Disponibilidade diferentes para ancorar os Postos Avançados. Isso permite uma Multi-AZ arquitetura do ponto de vista do plano de controle. Se você quiser implantar uma solução altamente disponível que inclua uma ou mais Zonas Locais, você deve primeiro validar a Zona de Disponibilidade principal na qual a infraestrutura está ancorada. Para isso, use o seguinte AWS CLI comando:

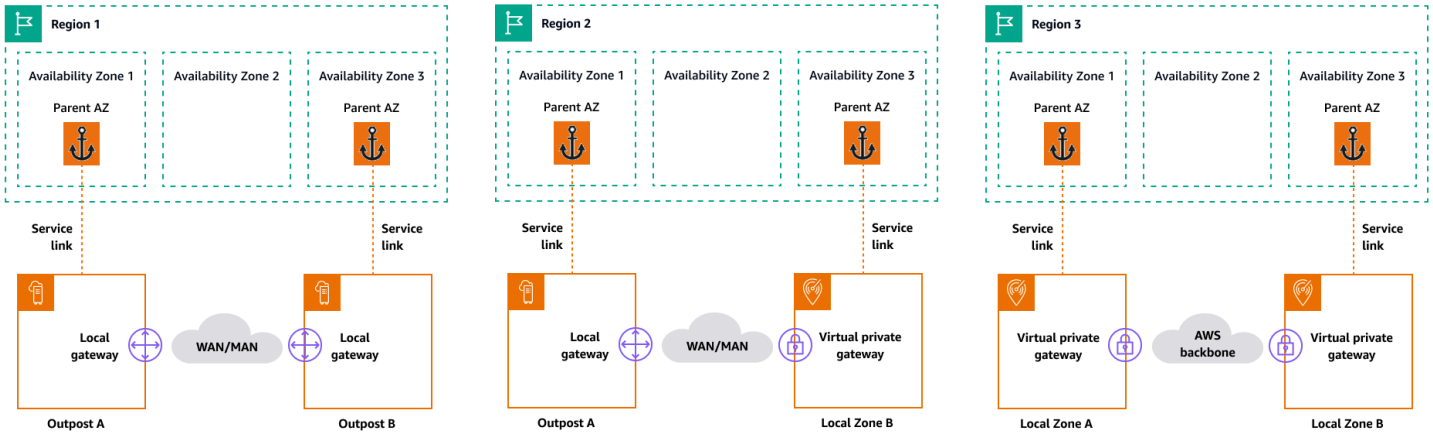
```
aws ec2 describe-availability-zones --zone-ids use1-mia1-az1
```

Saída do comando anterior:


```
{     "AvailabilityZones": [
          {
              "State": "available",
              "OptInStatus": "opted-in",
              "Messages": [],
              "RegionName": "us-east-1",
              "ZoneName": "us-east-1-mia-1a",
              "ZoneId": "use1-mia1-az1",
              "GroupName": "us-east-1-mia-1",
              "NetworkBorderGroup": "us-east-1-mia-1",
              "ZoneType": "local-zone",
              "ParentZoneName": "us-east-1d",
              "ParentZoneId": "use1-az2"
          }
      ]
 }
```


Neste exemplo, a Zona Local de Miami (`us-east-1d-mia-1a1`) está ancorada na Zona de `us-east-1d-az2` Disponibilidade. Portanto, se você precisar criar uma arquitetura resiliente na borda, deverá garantir que a infraestrutura secundária (Outposts ou Zonas Locais) esteja ancorada em uma Zona de Disponibilidade diferente de. **`us-east-1d-az2`** Por exemplo, `us-east-1d-az1` seria válido.

O diagrama a seguir fornece exemplos de infraestruturas de ponta altamente disponíveis.



Considerações sobre redes

Esta seção discute as considerações iniciais sobre redes na borda, principalmente para conexões para acessar a infraestrutura de borda. Ele analisa arquiteturas válidas que fornecem uma rede resiliente para o link de serviço.

Rede de resiliência para Zonas Locais

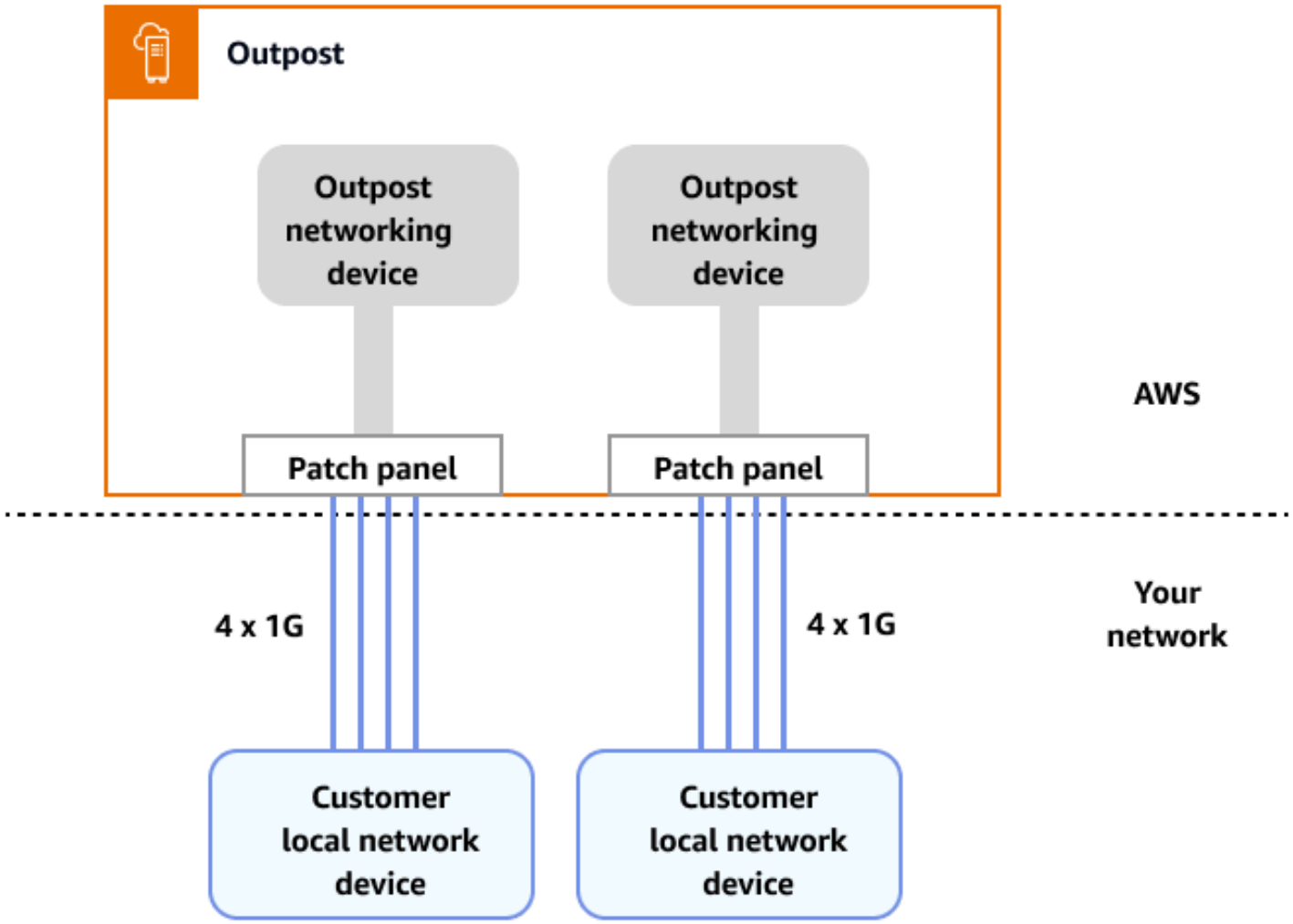
As Zonas Locais são conectadas à região principal com vários links redundantes, seguros e de alta velocidade que permitem que você consuma qualquer serviço regional, como Amazon S3 e Amazon RDS, sem problemas. Você é responsável por fornecer conectividade do seu ambiente local ou dos usuários à Zona Local. Independentemente da arquitetura de conectividade escolhida (por exemplo, VPN ou Direct Connect), a latência que deve ser alcançada por meio dos links de rede deve ser equivalente para evitar qualquer impacto no desempenho do aplicativo no caso de uma falha no link principal. Se você estiver usando Direct Connect, as arquiteturas de resiliência aplicáveis são as mesmas para acessar um Região da AWS, conforme documentado nas recomendações de Direct Connect resiliência. No entanto, existem cenários que se aplicam principalmente às Zonas Locais internacionais. No país em que a Zona Local está habilitada, ter apenas um único Direct Connect PoP impossibilita a criação das arquiteturas recomendadas para Direct Connect resiliência. Se você tiver acesso a apenas um único Direct Connect local ou precisar de resiliência além de uma única conexão, poderá criar um dispositivo VPN no Amazon EC2 Direct Connect e, conforme ilustrado e discutido na postagem AWS do blog, habilitar a conectividade altamente disponível do local para o. Zonas locais da AWS

Rede de resiliência para Outposts

Em contraste com as Zonas Locais, os Outposts têm conectividade redundante para acessar cargas de trabalho implantadas nos Outposts a partir de sua rede local. Essa redundância é obtida por meio de dois dispositivos de rede Outposts (ONDs). Cada OND requer pelo menos duas conexões de fibra de 1 Gbps, 10 Gbps, 40 Gbps ou 100 Gbps para sua rede local. Essas conexões devem ser configuradas como um grupo de agregação de links (LAG) para permitir a adição escalável de mais links.

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

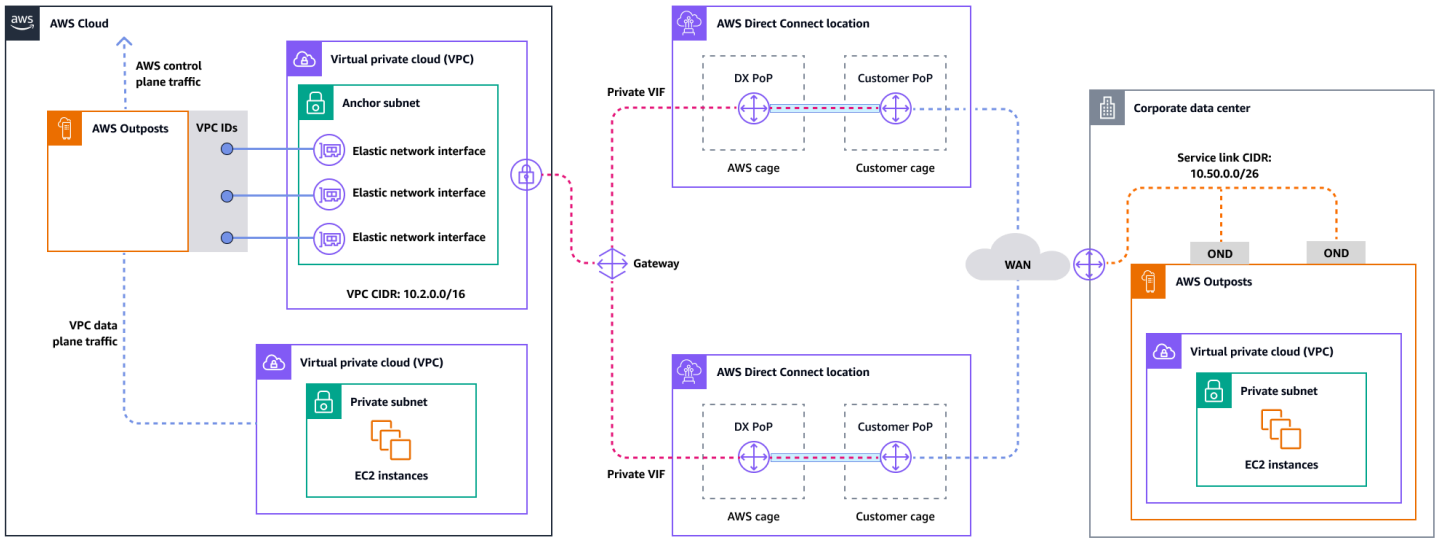
Velocidade do uplink	Número de uplinks
40 ou 100 Gbps	1, 2, ou 4



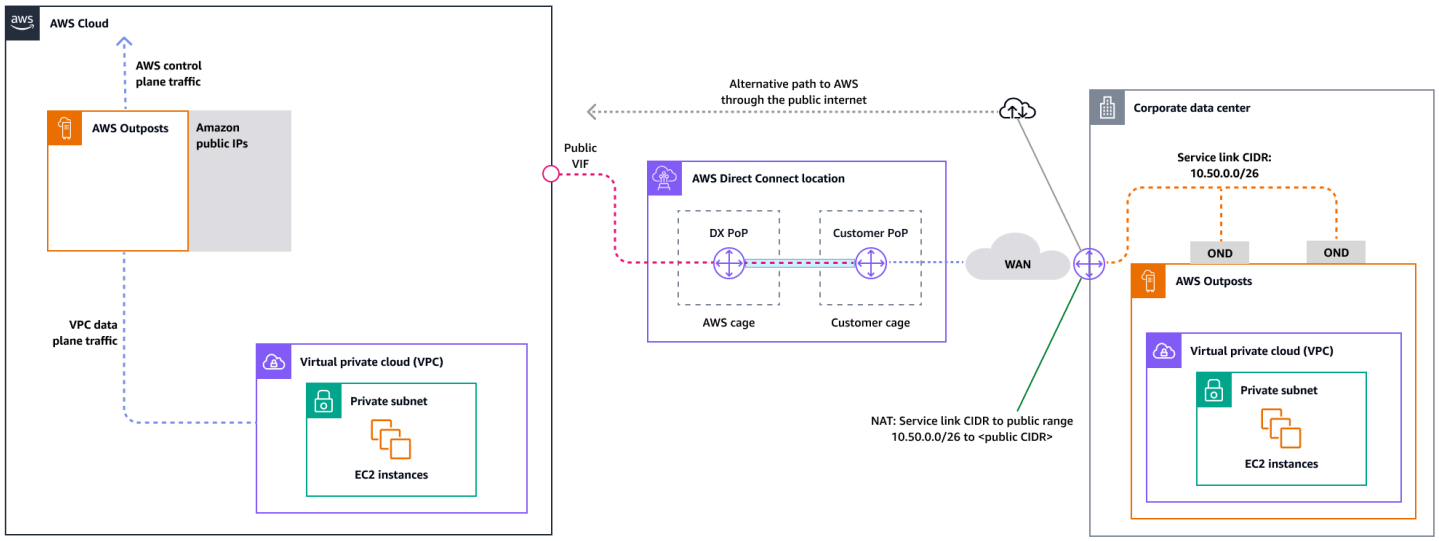
Para obter mais informações sobre essa conectividade, consulte Conectividade de rede local para Outposts Racks na documentação. AWS Outposts

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

O diagrama a seguir ilustra essa arquitetura para uma conexão privada altamente disponível.



O diagrama a seguir ilustra essa arquitetura para uma conexão pública altamente disponível.



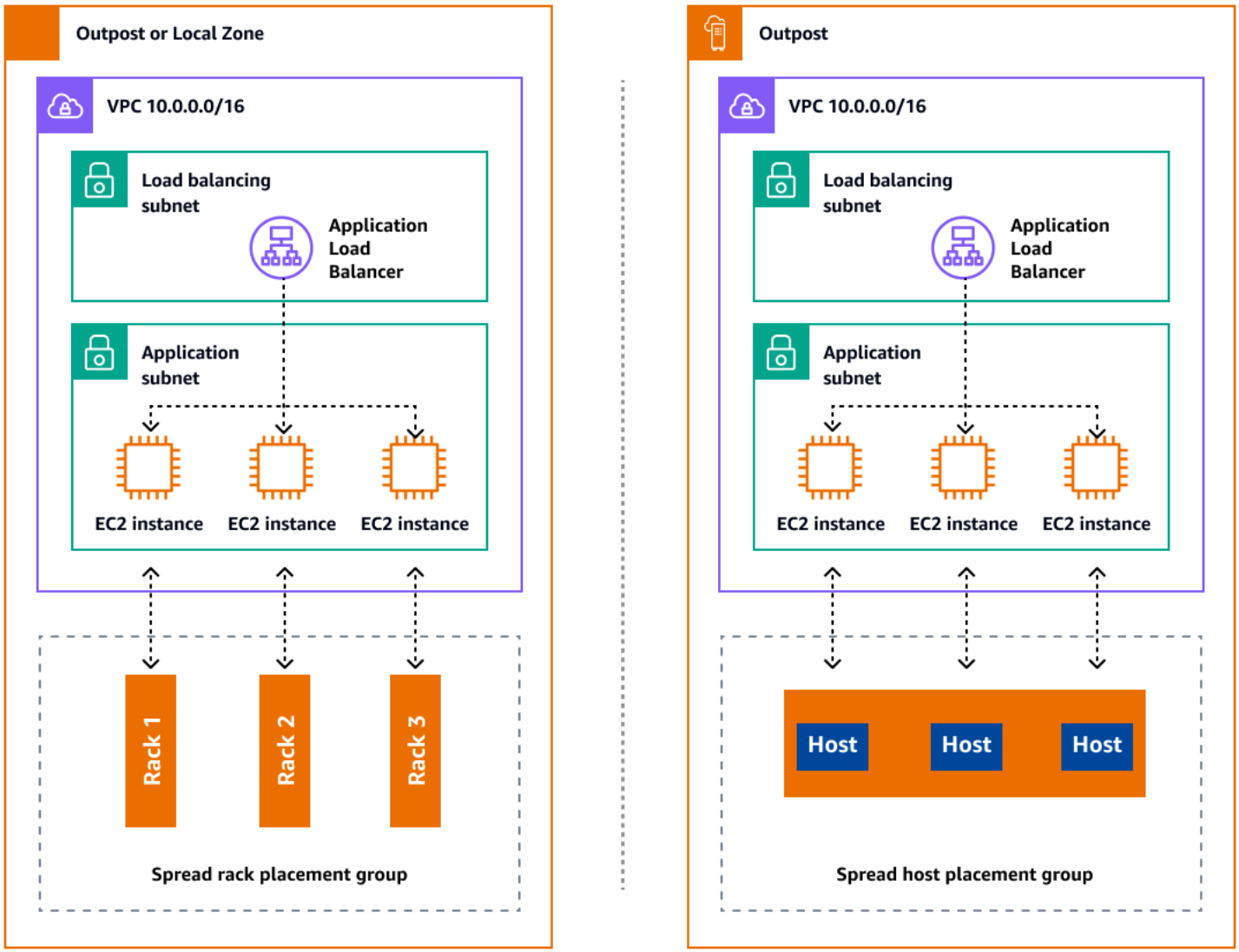
Dimensionando as implantações de rack do Outposts com racks ACE

O rack Aggregation, Core, Edge (ACE) serve como um ponto de agregação crítico para implantações de AWS Outposts vários racks e é recomendado principalmente para instalações que excedam três racks ou para planejar futuras expansões. Cada rack ACE possui quatro roteadores que suportam conexões de 10 Gbps, 40 Gbps e 100 Gbps (100 Gbps é o ideal). Cada rack pode se conectar a até quatro dispositivos upstream do cliente para obter redundância máxima. Os racks ACE consomem até 10 kVA de energia e pesam até 705 libras. Os principais benefícios incluem requisitos reduzidos de rede física, menos uplinks de cabeamento de fibra e menos interfaces virtuais de VLAN. AWS monitora esses racks por meio de dados de telemetria por meio de túneis VPN e trabalha em estreita colaboração com os clientes durante a instalação para garantir a

disponibilidade adequada de energia, a configuração da rede e o posicionamento ideal. A arquitetura de rack ACE fornece valor crescente à medida que as implantações se expandem e simplifica efetivamente a conectividade, ao mesmo tempo em que reduz a complexidade e os requisitos de portas físicas em instalações maiores. Para obter mais informações, consulte a postagem do AWS blog Dimensionando implantações de AWS Outposts rack com ACE Rack.

Distribuindo instâncias em Outposts e Zonas Locais

Outposts e Locais Zones têm um número finito de servidores computacionais. Se seu aplicativo implantar várias instâncias relacionadas, essas instâncias poderão ser implantadas no mesmo servidor ou em servidores no mesmo rack, a menos que estejam configuradas de forma diferente. Além das opções padrão, você pode distribuir instâncias entre servidores para reduzir o risco de executar instâncias relacionadas na mesma infraestrutura. Você também pode distribuir instâncias em vários racks usando grupos de posicionamento de partições. Isso é chamado de modelo de distribuição de spread rack. Use a distribuição automática para distribuir instâncias entre as partições do grupo ou implante instâncias em partições de destino selecionadas. Ao implantar instâncias nas partições de destino, você pode implantar recursos selecionados no mesmo rack enquanto distribui outros recursos entre os racks. Outposts também fornece outra opção chamada spread host, que permite distribuir sua carga de trabalho no nível do host. O diagrama a seguir mostra as opções de distribuição do spread rack e do spread host.



Amazon RDS em Multi-AZ AWS Outposts

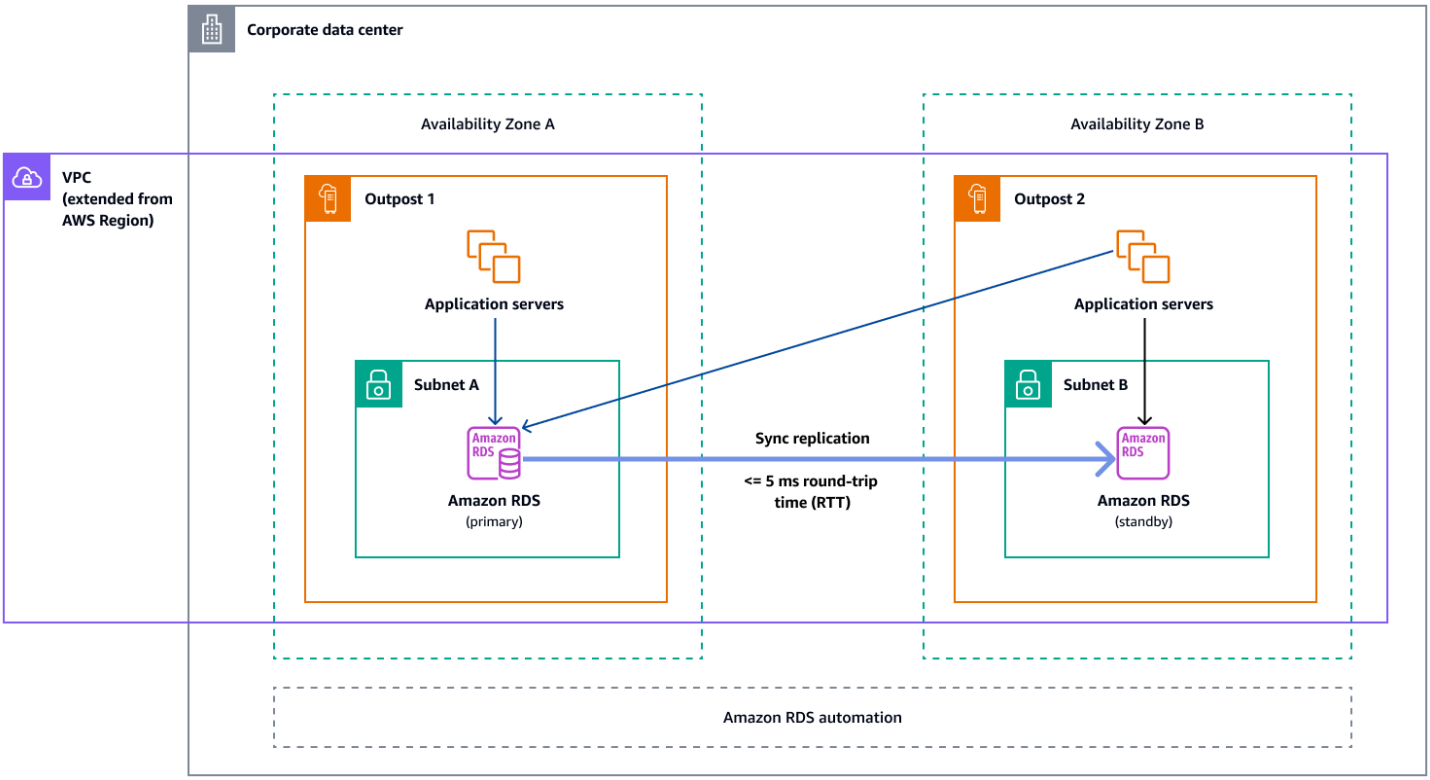
Quando você usa implantações de Multi-AZ instâncias em Outposts, o Amazon RDS cria duas instâncias de banco de dados em dois Outposts. Cada posto avançado funciona em sua própria infraestrutura física e se conecta a diferentes zonas de disponibilidade em uma região para obter alta disponibilidade. Quando dois Outposts são conectados por meio de uma conexão local gerenciada pelo cliente, o Amazon RDS gerencia a replicação síncrona entre as instâncias de banco de dados primária e em espera. No caso de uma falha de software ou infraestrutura, o Amazon RDS promove automaticamente a instância em espera para a função principal e atualiza o registro DNS para apontar para a nova instância primária. Para Multi-AZ implantações, o Amazon RDS cria uma instância de banco de dados primária em um Outpost e replica sincronicamente os dados para uma

instância de banco de dados em espera em outro Outpost. Multi-AZ as implantações em Outposts operam Multi-AZ como implantações Regiões da AWS em, com as seguintes diferenças:

- Elas exigem uma conexão local entre dois ou mais Outposts.
- Eles exigem pools de endereços IP de propriedade do cliente (CoIP). Para obter mais informações, consulte os endereços Customer-owned IP do Amazon RDS AWS Outposts na documentação do Amazon RDS.
- A replicação é realizada na sua rede local.

Multi-AZ as implantações estão disponíveis para todas as versões compatíveis do MySQL e do PostgreSQL no Amazon RDS on Outposts. Os backups locais não são suportados para Multi-AZ implantações.

O diagrama a seguir mostra a arquitetura das configurações do Amazon RDS on Multi-AZ Outposts.

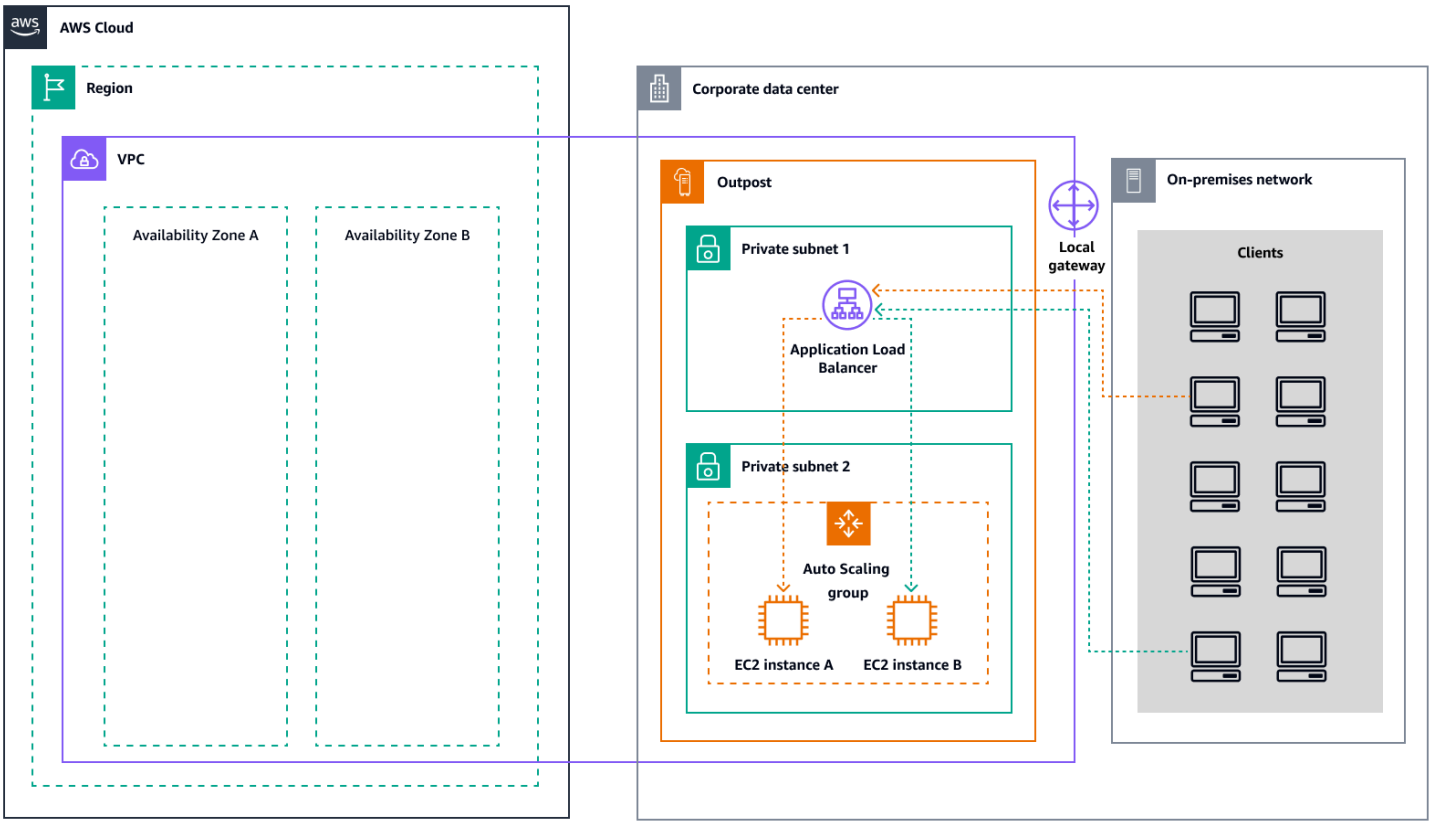


Mecanismos de failover

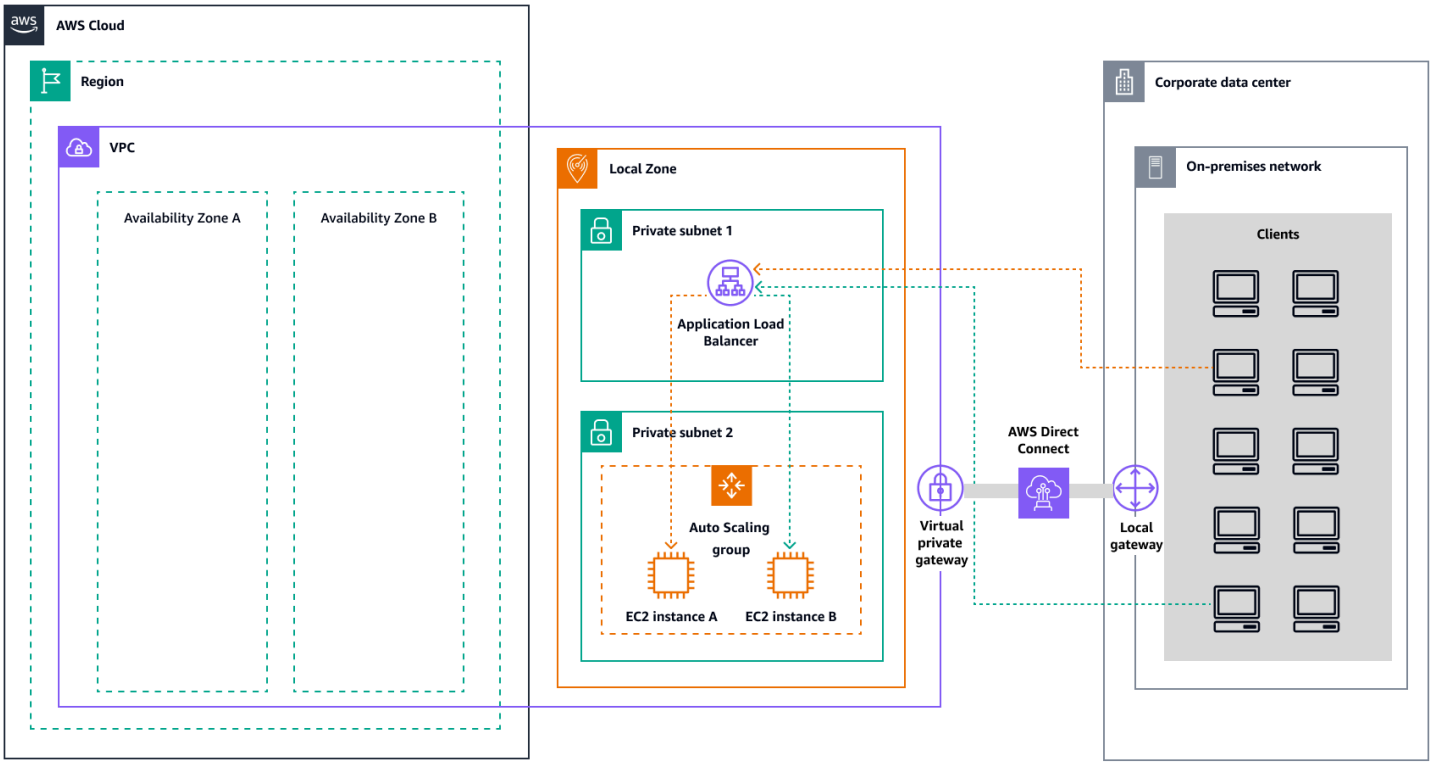
Balanceamento de carga e escalabilidade automática

O Elastic Load Balancing (ELB) distribui automaticamente o tráfego de entrada do aplicativo em todas as instâncias do EC2 que você está executando. O ELB ajuda a gerenciar as solicitações recebidas roteando o tráfego de forma otimizada para que nenhuma instância fique sobrecarregada. Para usar o ELB com seu grupo Amazon EC2 Auto Scaling, conecte o balanceador de carga ao seu grupo Auto Scaling. Isso registra o grupo com o balanceador de carga, que atua como um único ponto de contato para todo o tráfego de entrada da web em seu grupo. Quando você usa o ELB com seu grupo de Auto Scaling, não é necessário registrar instâncias individuais do EC2 com o balanceador de carga. As instâncias iniciadas pelo grupo do Auto Scaling serão automaticamente registradas no balanceador de carga. Da mesma forma, as instâncias que são encerradas pelo seu grupo de Auto Scaling são automaticamente canceladas do balanceador de carga. Depois de conectar um balanceador de carga ao seu grupo do Auto Scaling, você pode configurar seu grupo para usar métricas do ELB (como a contagem de solicitações do Application Load Balancer por destino) para escalar o número de instâncias no grupo conforme a demanda flutua. Opcionalmente, você pode adicionar verificações de saúde do ELB ao seu grupo de Auto Scaling para que o Amazon EC2 Auto Scaling possa identificar e substituir instâncias não íntegras com base nessas verificações de saúde. Você também pode criar um CloudWatch alarme da Amazon que o notifique se a contagem saudável de anfitriões do grupo-alvo estiver abaixo do permitido.

O diagrama a seguir ilustra como um Application Load Balancer gerencia cargas de trabalho no Amazon EC2 em. AWS Outposts



O diagrama a seguir ilustra uma arquitetura similar para o Amazon EC2 em Locais Zones.

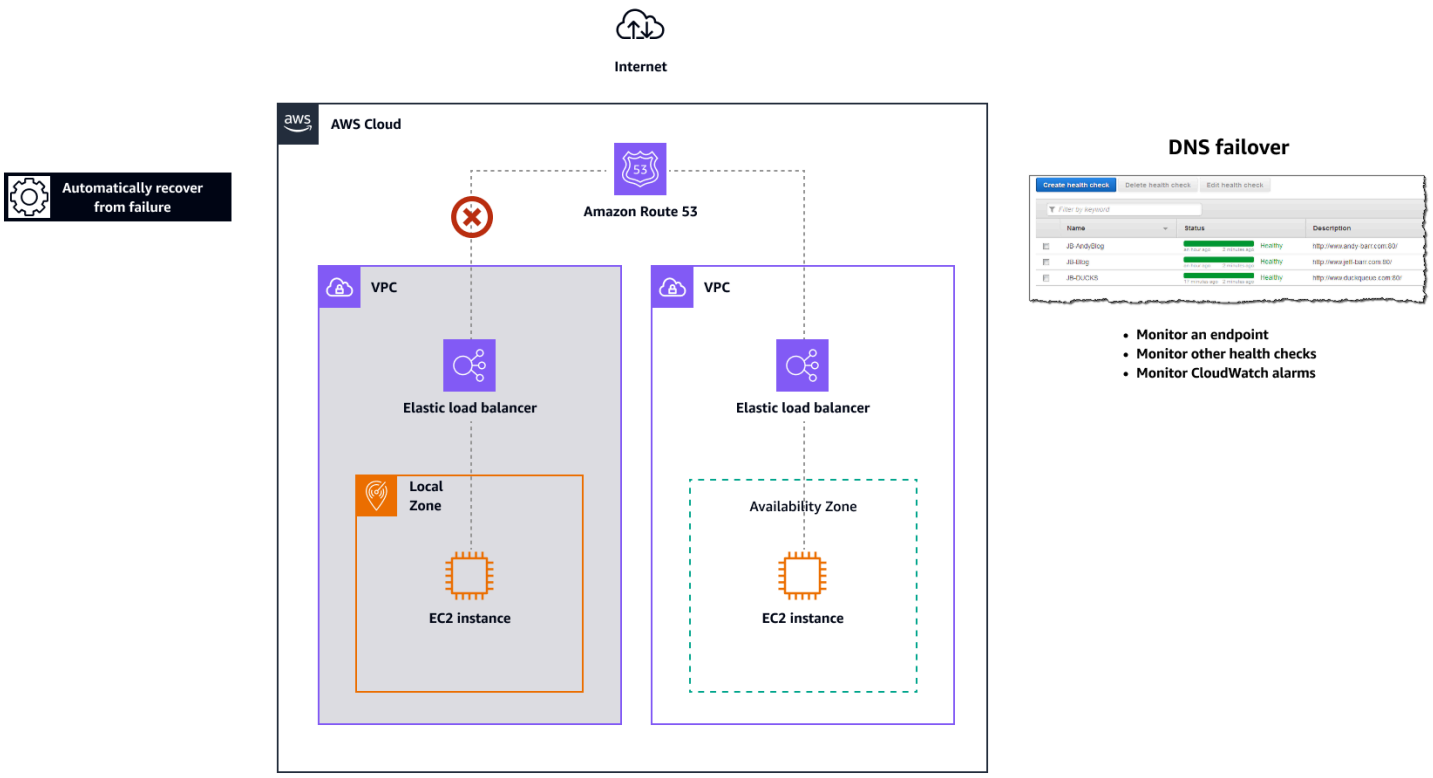


> **Note**
>
> Os Application Load Balancers estão disponíveis em ambas as Zonas AWS Outposts e em Locais. No entanto, para usar um Application Load Balancer em AWS Outposts, você precisa dimensionar a capacidade do Amazon EC2 para fornecer a escalabilidade que o balanceador de carga exige. Para obter mais informações sobre o dimensionamento de um balanceador de carga em AWS Outposts, consulte a postagem do AWS blog Configurando um Application Load Balancer em. AWS Outposts

Amazon Route 53 para failover de DNS

Quando você tem mais de um recurso executando a mesma função, por exemplo, vários servidores HTTP ou de e-mail, você pode configurar o Amazon Route 53 para verificar a integridade dos seus recursos e responder às consultas de DNS usando somente os recursos íntegros. Por exemplo, vamos supor que seu site,`example.com`, esteja hospedado em dois servidores. Um servidor está em uma zona local e o outro em um posto avançado. Você pode configurar o Route 53 para verificar a integridade desses servidores e responder às consultas de DNS `example.com` usando somente os servidores que estão íntegros no momento. Se você estiver usando registros de alias para rotear o tráfego para AWS recursos selecionados, como balanceadores de carga do ELB, você pode configurar o Route 53 para avaliar a integridade do recurso e rotear o tráfego somente para recursos que estejam íntegros. Ao configurar um registro de alias para avaliar a integridade de um recurso, você não precisa criar uma verificação de saúde para esse recurso.

O diagrama a seguir ilustra os mecanismos de failover do Route 53.



Observações

- Se você estiver criando registros de failover em uma zona hospedada privada, poderá criar uma CloudWatch métrica, associar um alarme à métrica e, em seguida, criar uma verificação de integridade com base no fluxo de dados do alarme.
- Para tornar um aplicativo acessível publicamente AWS Outposts usando um Application Load Balancer, defina configurações de rede que habilitem a Tradução de Endereços de Rede de Destino (DNAT) de IPs públicos para o nome de domínio totalmente qualificado (FQDN) do balanceador de carga e crie uma regra de failover do Route 53 com verificações de integridade que apontem para o IP público exposto. Essa combinação garante acesso público confiável ao seu Outposts-hosted aplicativo.

Amazon Route 53 Resolver ativado AWS Outposts

Amazon Route 53 Resolverestá disponível nos racks Outposts. Ele fornece aos seus serviços e aplicativos locais resolução de DNS local diretamente do Outposts. Os endpoints locais do Route 53 Resolver também permitem a resolução de DNS entre Outposts e seu servidor DNS local. O Route

53 Resolver on Outposts ajuda a melhorar a disponibilidade e o desempenho de seus aplicativos locais.

Um dos casos de uso típicos do Outposts é implantar aplicativos que exigem acesso de baixa latência a sistemas locais, como equipamentos de fábrica, aplicativos comerciais de alta frequência e sistemas de diagnóstico médico.

Quando você opta por usar resolvedores locais do Route 53 em Outposts, os aplicativos e serviços continuarão se beneficiando da resolução de DNS local para descobrir outros serviços, mesmo que a conectividade com um Região da AWS dos pais seja perdida. Os resolvedores locais também ajudam a reduzir a latência das resoluções de DNS porque os resultados das consultas são armazenados em cache e veiculados localmente a partir dos Outposts, o que elimina viagens de ida e volta desnecessárias ao pai. Região da AWS Todas as resoluções de DNS para aplicativos em VPCs do Outposts que usam DNS privado são servidas localmente.

Além de habilitar resolvedores locais, esse lançamento também habilita endpoints locais do Resolver. Os endpoints de saída do Route 53 Resolver permitem que os resolvedores do Route 53 encaminhem consultas de DNS para os resolvedores de DNS que você gerencia, por exemplo, em sua rede local. Por outro lado, os endpoints de entrada do Route 53 Resolver encaminham as consultas de DNS que recebem de fora da VPC para o Resolver que está sendo executado nos Outposts. Ele permite que você envie consultas de DNS para serviços implantados em uma VPC privada do Outposts de fora dessa VPC. Para obter mais informações sobre endpoints de entrada e saída, consulte Resolvendo consultas de DNS entre VPCs e sua rede na documentação do Route 53.

Planejamento de capacidade na periferia

A fase de planejamento da capacidade envolve a coleta dos requisitos de vCPU, memória e armazenamento para implantar sua arquitetura. No pilar de otimização de custos do AWS Well-Architected Framework, o dimensionamento correto é um processo contínuo que começa com o planejamento. Você pode usar AWS ferramentas para definir otimizações com base no consumo de recursos no interior. AWS

O planejamento da capacidade periférica em Locais Zonas é o mesmo que em Regiões da AWS. Você deve verificar se suas instâncias estão disponíveis em cada zona local, pois alguns tipos de instância podem ser diferentes dos tipos em Regiões da AWS. Para Outposts, você deve planejar a capacidade com base em seus requisitos de carga de trabalho. Outposts são distribuídos com números fixos de instâncias por host e podem ser redistribuídos conforme necessário. Se suas

cargas de trabalho exigirem capacidade ociosa, leve isso em consideração ao planejar suas necessidades de capacidade.

Planejamento de capacidade em Outposts

AWS Outposts o planejamento de capacidade requer insumos específicos para o dimensionamento regional correto, além de fatores específicos que afetam a disponibilidade, o desempenho e o crescimento dos aplicativos. Para obter orientação detalhada, consulte Planejamento de capacidade no AWS whitepaper Considerações sobre design e arquitetura de AWS Outposts alta disponibilidade.

Planejamento de capacidade para Zonas Locais

Uma zona local é uma extensão de uma Região da AWS que está geograficamente próxima aos seus usuários. Os recursos criados em uma zona local podem atender usuários locais com comunicações de latência muito baixa. Para habilitar uma zona local em sua Conta da AWS, consulte Introdução Zonas locais da AWS na AWS documentação. Cada zona local tem um slot diferente disponível para famílias de EC2 instâncias. Valide as instâncias disponíveis em cada zona local antes de usá-las. Para confirmar as EC2 instâncias disponíveis, execute o seguinte AWS CLI comando:

```
aws ec2 describe-instance-type-offerings \
--location-type "availability-zone" \
--filters Name=location,Values=<local-zone-name>
```

Saída esperada:

```
{
  "InstanceTypeOfferings": [
      {
          "InstanceType": "m5.2xlarge",
          "LocationType": "availability-zone",
          "Location": "<local-zone-name>"
      },
      {
          "InstanceType": "t3.micro",
          "LocationType": "availability-zone",
          "Location": "local.zone-name"
      },
      ...
  ]
```

```
}
```

Gerenciamento de infraestrutura de ponta

AWS fornece serviços totalmente gerenciados que ampliam a AWS infraestrutura APIs, os serviços e as ferramentas para mais perto de seus usuários finais e data centers. Os serviços que estão disponíveis em Outposts e Locais Zones são os mesmos que estão disponíveis em Regiões da AWS, então você pode gerenciar esses serviços usando o mesmo AWS console, AWS CLI, ou. AWS APIs Para ver os serviços compatíveis, consulte a AWS Outposts tabela de comparação de Zonas locais da AWS recursos e os recursos.

Implantação de serviços na borda

Você pode configurar os serviços disponíveis em Locais Zones e Outposts da mesma forma que os configura em Regiões da AWS: usando o AWS console, AWS CLI, ou. AWS APIs A principal diferença entre implantações regionais e periféricas são as sub-redes nas quais os recursos serão provisionados. A seção Rede na borda descreveu como as sub-redes são implantadas em Outposts e Locais Zones. Depois de identificar as sub-redes de borda, você usa a ID da sub-rede de borda como um parâmetro para implantar o serviço em Outposts ou Locais Zones. As seções a seguir fornecem exemplos de implantação de serviços de borda.

Amazon EC2 no limite

O `run-instances` exemplo a seguir inicia uma única instância do tipo `m5.2xlarge` na sub-rede de borda da região atual. O key pair é opcional se você não planeja se conectar à sua instância usando SSH no Linux ou protocolo de desktop remoto (RDP) no Windows.

```
aws ec2 run-instances \
    --image-id ami-id \
    --instance-type m5.2xlarge \
    --subnet-id <subnet-edge-id> \
    --key-name MyKeyPair
```

Balanceadores de carga de aplicativos na borda

O `create-load-balancer` exemplo a seguir cria um Application Load Balancer interno e ativa as Locais Zones ou Outposts para as sub-redes especificadas.

```
aws elbv2 create-load-balancer \
```

```
    --name my-internal-load-balancer \
    --scheme internal \
    --subnets <subnet-edge-id>
```

Para implantar um Application Load Balancer voltado para a Internet em uma sub-rede em um Outpost, você define `internet-facing` o sinalizador na opção e fornece um `--scheme` ID do pool CoIP, conforme mostrado neste exemplo:

```
aws elbv2 create-load-balancer \
    --name my-internal-load-balancer \
    --scheme internet-facing \
    --customer-owned-ipv4-pool <coip-pool-id>
    --subnets <subnet-edge-id>
```

Para obter informações sobre a implantação de outros serviços na borda, siga estes links:

Serviço	AWS Outposts	Zonas locais da AWS
Amazon EKS	Implante o Amazon EKS localmente com AWS Outposts	Inicie clusters EKS de baixa latência com Zonas locais da AWS
Amazon ECS	Amazon ECS em AWS Outposts	Aplicativos do Amazon ECS em sub-redes compartilhadas, Zonas Locais e Zonas de Wavelength
Amazon RDS	Amazon RDS ativado AWS Outposts	Selecione a sub-rede da zona local
Amazon S3	Começando a usar o Amazon S3 no Outposts	Não disponível
Amazon ElastiCache	Usando Outposts com ElastiCache	Usando Locais Zones com ElastiCache
Amazon EMR	Clusters EMR em AWS Outposts	Clusters EMR em Zonas locais da AWS

Serviço	AWS Outposts	Zonas locais da AWS
Amazon FSx	Não disponível	Selecione a sub-rede da zona local
Recuperação de desastres do AWS Elastic	Trabalhando com Recuperação de desastres do AWS Elastic e AWS Outposts	Não disponível
AWS Transform MGN	Não disponível	Selecione a sub-rede Local Zone como sub-rede de teste

CLI e SDK específicos do Outposts

AWS Outposts tem dois grupos de comandos e APIs para criar uma ordem de serviço ou manipular as tabelas de roteamento entre o gateway local e sua rede local.

Processo de pedido do Outposts

Você pode usar o AWS CLIou os Outposts APIs para criar um site de Outposts, criar um Outposts e criar uma ordem de Outposts. Recomendamos que você trabalhe com um especialista em nuvem híbrida durante o processo de AWS Outposts pedido para garantir a seleção adequada do recurso IDs e a configuração ideal para suas necessidades de implementação. Para obter uma lista completa de IDs de recursos, consulte a página de preços AWS Outposts dos racks.

Gerenciamento de gateway local

O gerenciamento e a operação do gateway local (LGW) no Outposts exigem conhecimento dos comandos e AWS CLI do SDK disponíveis para essa tarefa. Você pode usar o AWS CLI e AWS SDKs para criar e modificar rotas LGW, entre outras tarefas. Para obter mais informações sobre o gerenciamento do LGW, consulte estes recursos:

- AWS CLI para Amazon EC2
- EC2.Client no AWS SDK para Python (Boto)
- Ec2Client no AWS SDK para Java

CloudWatch métricas e registros

Por Serviços da AWS estarem disponíveis tanto nos Outposts quanto nas Zonas Locais, as métricas e os registros são gerenciados da mesma forma que nas Regiões. CloudWatch A Amazon fornece métricas dedicadas ao monitoramento de Outposts nas seguintes dimensões:

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

Para obter mais informações, consulte CloudWatch as métricas dos racks do Outposts na documentação do Outposts.

Recursos

AWS referências

- Nuvem híbrida com AWS
- AWS Outposts Guia do usuário para racks Outposts
- Manual do usuário do Zonas locais da AWS
- AWS Outposts Família
- Zonas locais da AWS
- Estenda uma VPC para uma zona local, zona de comprimento de onda ou posto avançado (documentação da Amazon VPC)
- Instâncias Linux em Zonas Locais (EC2 documentação da Amazon)
- Instâncias Linux em Outposts (documentação da Amazon EC2)
- Comece a implantar aplicativos de baixa latência com Zonas locais da AWS(tutorial)

AWS postagens no blog

- Executando AWS infraestrutura no local com a Amazon EC2
- Criação de aplicativos modernos com o Amazon EKS na Amazon EC2
- Como escolher entre os modos de roteamento CoIP e VPC direto no Amazon Rack EC2
- Seleção de switches de rede para sua Amazon EC2
- Manter uma cópia local de seus dados em Zonas locais da AWS
- Amazon ECS na Amazon EC2
- Gerenciando a malha de serviços com reconhecimento de borda com o Amazon EKS para Zonas locais da AWS
- Implantação do roteamento de entrada de gateway local na Amazon EC2
- Automatizando suas implantações de carga de trabalho em Zonas locais da AWS
- Compartilhando a Amazon EC2 em um AWS ambiente com várias contas: Parte 1
- Compartilhando a Amazon EC2 em um AWS ambiente com várias contas: Parte 2
- AWS Direct Connect e padrões de Zonas locais da AWS interoperabilidade

- Implante o Amazon RDS na Amazon EC2 com alta disponibilidade Multi-AZ

Colaboradores

As seguintes pessoas contribuíram para este guia.

Autoria

- Leonardo Solano, arquiteto principal de soluções de nuvem híbrida, AWS
- Len Gomes, arquiteto de soluções parceiras, AWS
- Matt Price, engenheiro sênior de suporte corporativo, AWS
- Tom Gadomski, arquiteto de soluções, AWS
- Obed Gutierrez, arquiteto de soluções, AWS
- Dionysios Kakaletris, gerente técnico de contas, AWS
- Vamsi Krishna, principal especialista em Outposts, AWS

Análise

- David Filiatrault, consultor de entrega, AWS

Redação técnica

- Handan Selamoglu, gerente sênior de documentação, AWS

Histórico do documento

A tabela a seguir descreve alterações significativas feitas neste guia. Se desejar receber notificações sobre futuras atualizações, inscreva-se em um feed RSS.

Alteração	Descrição	Data
Publicação inicial	—	10 de junho de 2025

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.