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

AWS Orientação prescritiva

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

Table of Contents

Introdução 1
Visão geral 3
Workshops sobre nuvem híbrida 3
PoCs 3
Pilares 4
Pré-requisitos e limitações 5
Pré-requisitos 5
AWS Outposts 5
Zonas locais da AWS 5
Limitações 6
AWS Outposts 6
Zonas locais da AWS 6
Processo de adoção da nuvem híbrida 8
Rede na borda 8
Arquitetura VPC 8
Tráfego de borda para região 9
Da borda ao tráfego local 12
Segurança na borda 16
Proteção de dados 16
Gerenciamento de identidade e acesso 20
Segurança da infraestrutura 21
Acesso à Internet 23
Governança da infraestrutura 25
Resiliência na borda 27
Considerações sobre infraestrutura 27
Considerações sobre redes 30
Distribuindo instâncias em Outposts e Zonas Locais 33
Amazon RDS Multi-AZ em AWS Outposts 34
Mecanismos de failover 36
Planejamento de capacidade na periferia 40
Planejamento de capacidade em Outposts 41
Planejamento de capacidade para Zonas Locais 41
Gerenciamento de infraestrutura de ponta 42
Implantação de serviços na borda 42

CLI e SDK específicos do Outposts 44
Recursos 46
AWS referências 46
AWS postagens no blog 46
Colaboradores 48
Autoria 48
Analisando 48
Redação técnica 48
Histórico do documento 49
Glossário da 50
..... 50
A 51
B 54
C 56
D 59
E 64
F 66
G 68
H 69
eu 70
L 73
M 74
O 78
P 81
Q 84
R 84
S 88
T 92
U 93
V 94
W 94
Z 95
..... xcvii

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 oferecer suporte a 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
- Pré-requisitos e limitações
- Processo de adoção da nuvem híbrida:
  - Rede na periferia
  - Segurança na borda
  - Resiliência na borda
  - Planejamento de capacidade na borda
  - Gerenciamento de infraestrutura de ponta
- Recursos
- Colaboradores
- Histórico de documentos

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 o AWS Enterprise On-Ramp.

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 AWS Direct Connect link do seu data center para o AWS 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 virtual privada (VPN) local e o licenciamento necessário para iniciar um dispositivo VPN baseado em software na Amazon na

zona local. EC2 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 na Amazon. EC2
- As Zonas Locais não oferecem suporte AWS Transit Gateway. Em vez disso, conecte-se à zona local usando uma interface virtual AWS 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 recursos.
- 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 borda

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 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}]
```

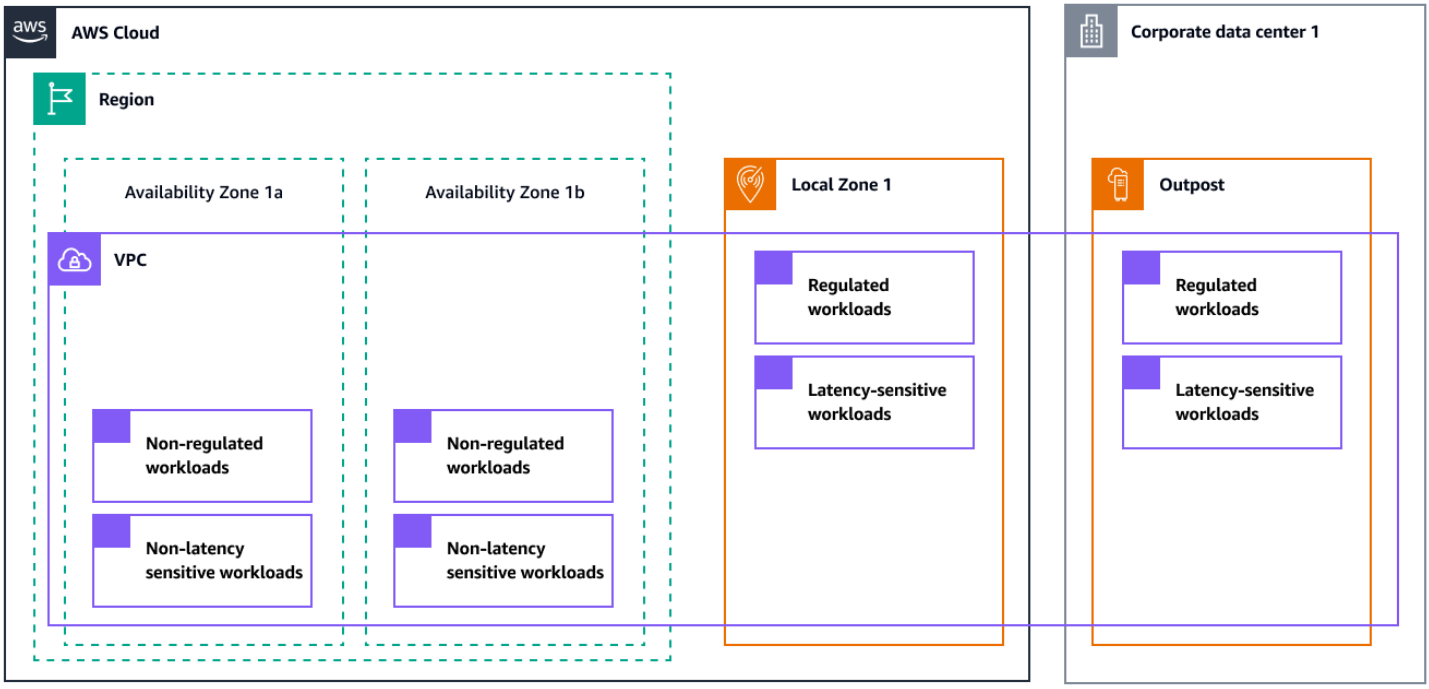
  Para obter mais informações, consulte a documentação do AWS Outposts.

- 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.

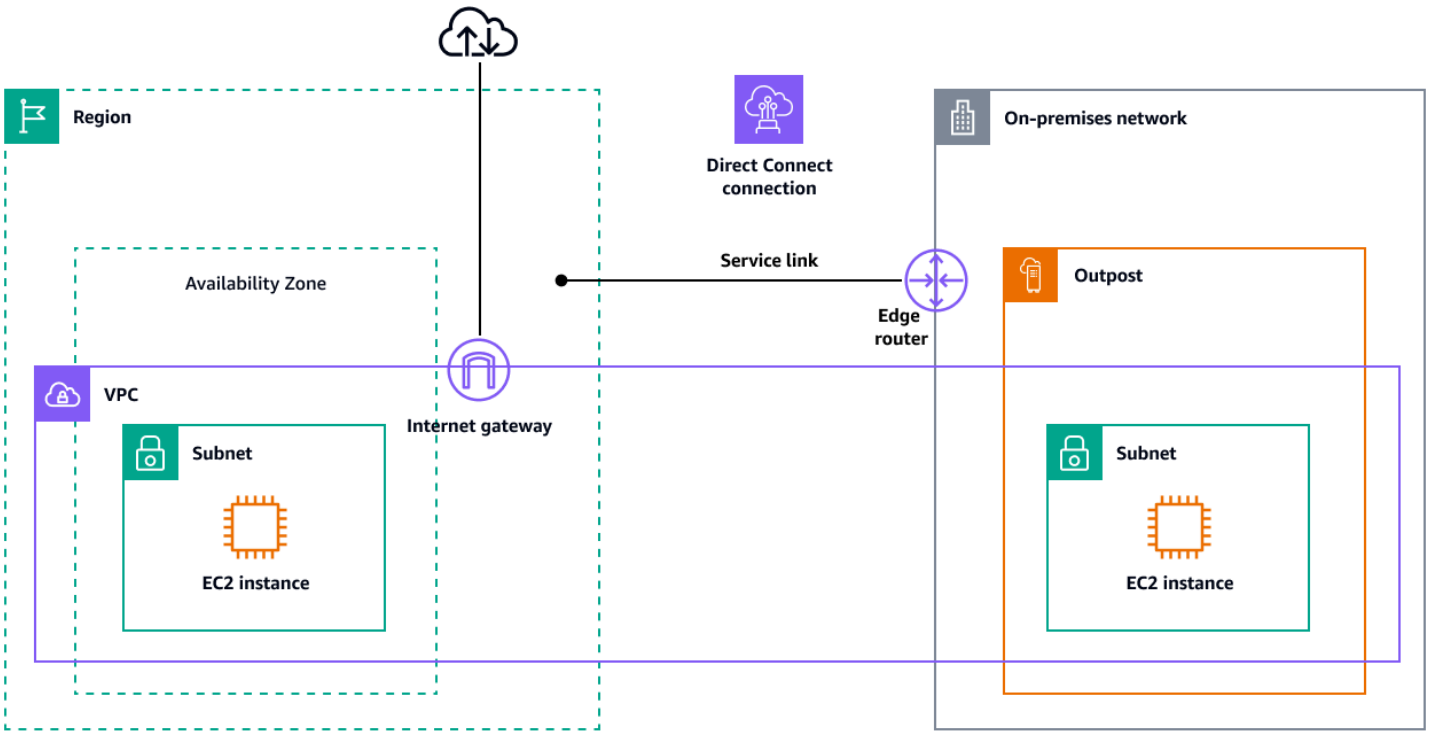


Tráfego de borda para região

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 AWS Direct Connect pública (VIF pública) ou por meio de uma interface virtual AWS 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 EC2 instâncias da Amazon, 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 AWS 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 EC2 instâncias em AWS Outposts e EC2 instâncias no Região da AWS tem uma 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 dos mesmos APIs conjuntos de ferramentas.

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

De	Para	MTU
Amazon EC2 na região	Amazon EC2 em Zonas Locais	1.300 bytes
AWS 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.

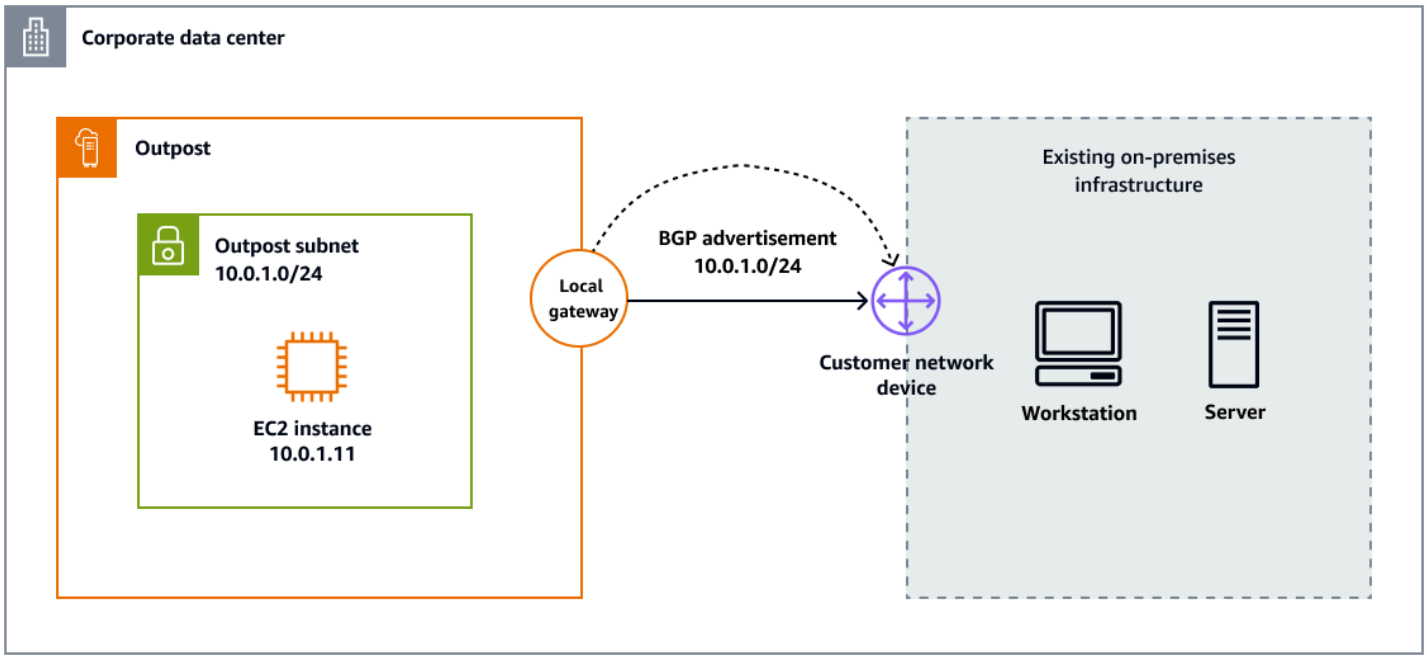
Da borda ao tráfego local

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.

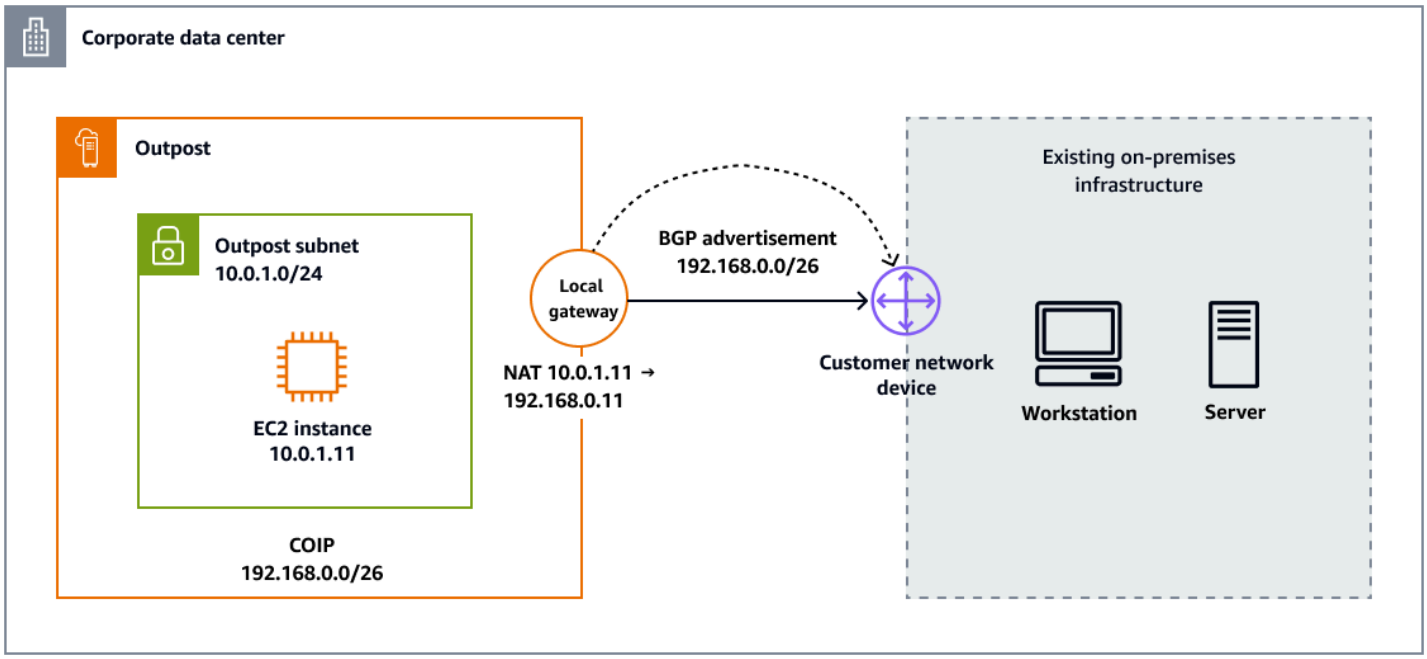
AWS Outposts gateway local

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 EC2 instâncias. 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 a recursos em seu Outpost, como EC2 instâncias, 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 à Internet uma carga EC2 de trabalho hospedada pela Amazon em uma zona local, você pode ativar a opção de atribuição automática de IP público ao iniciar a instância. 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 EC2 instância após sua execução. 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 o Internet Protocol Security (IPsec) VPN 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 AWS Direct Connect

Também há suporte para Locais Zones AWS 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 cargas de trabalho VPCs e suas da 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 aqueles estendidos VPCs às Zonas Locais. Quando os pares VPCs 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 funciona Serviços da AWS no Nuvem AWS. AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados 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 AWS IAM Identity Center. 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 on Outposts são criptografados usando criptografia no lado do servidor com chaves de criptografia gerenciadas pelo Amazon S3 (SSE-S3). Você também pode optar por usar a criptografia no lado do servidor com chaves de criptografia fornecidas pelo cliente (SSE-C). Para usar o SSE-C, especifique uma chave de criptografia como parte das solicitações da API de objeto. A criptografia no lado do servidor criptografa somente os dados de objeto, não os metadados de objeto.

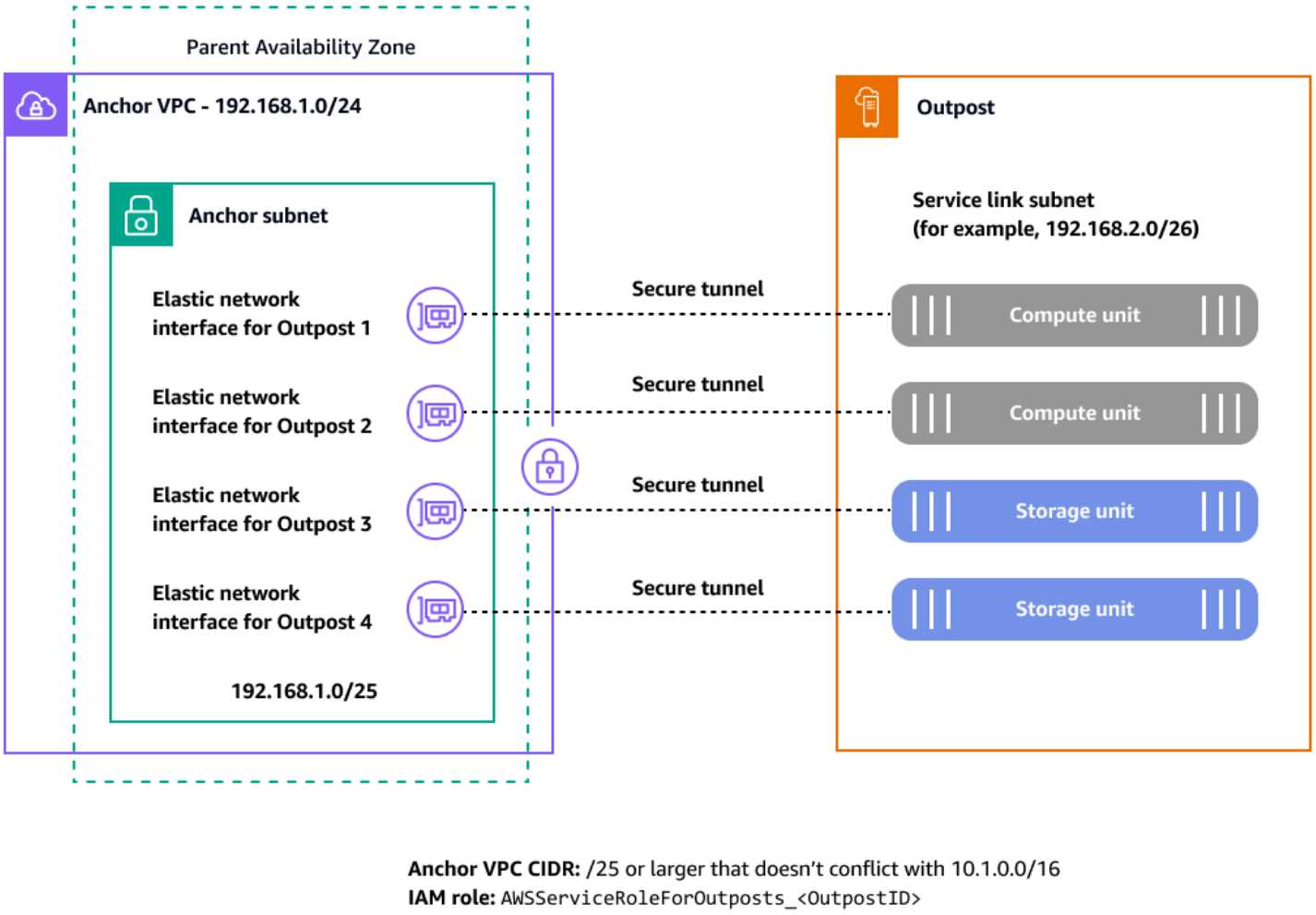
> **Note**
>
> O Amazon S3 on Outposts não oferece suporte à criptografia do lado do servidor com chaves KMS (SSE-KMS).

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 do 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 AWS 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.

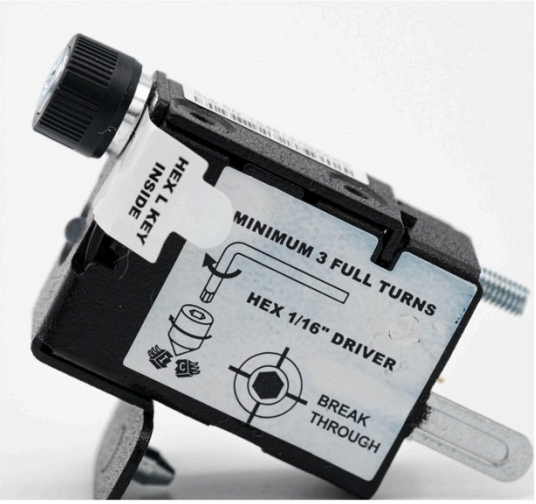
Protocolo	Porta de origem	Endereço de origem	Porta de destino	Endereço de destino
UDP	443	AWS Outposts link de serviço /26	443	AWS Outposts Rotas públicas da região ou VPC CIDR âncora
TCP	1025-65535	AWS Outposts link de serviço /26	443	AWS Outposts Rotas públicas da região ou VPC CIDR âncora

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 AWS Direct Connect PoPs acessar uma zona local, você pode habilitar a Segurança MAC (MACsec) entre seu roteador ou switch local e o endpoint. AWS Direct Connect Para obter mais informações, consulte a postagem do AWS blog Adicionar MACsec segurança às AWS Direct Connect conexões.

Exclusão de dados

Quando você interrompe ou encerra uma EC2 instância AWS Outposts, 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. 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
Políticas baseadas em identidade	Sim
Políticas baseadas em recurso	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
Controle de acesso baseado em atributos (ABAC) (tags em políticas)	Sim
Credenciais temporárias	Sim
Permissões de entidade principal	Sim
Perfis de serviço	Não
Funções vinculadas ao serviço	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 defense-in-depth abordagem para tráfego de entrada e saída. Isso inclui o uso de grupos de segurança (firewalls de inspeção de estado), rede ACLs, 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 EC2 instâncias, 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 EC2 instâncias, 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.

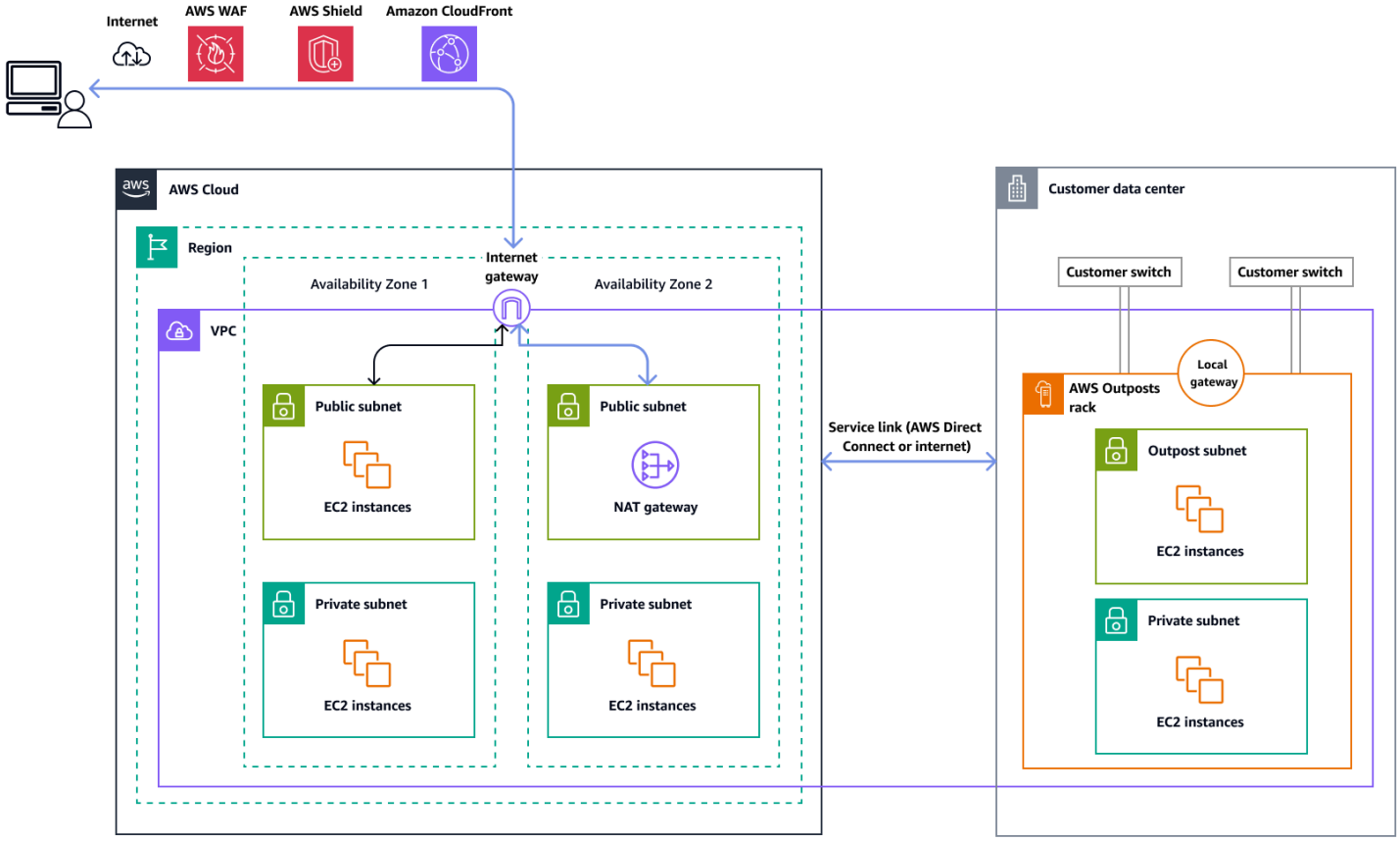
Local Zones adota uma construção de rede chamada grupo de borda de rede, que é usada em Regiões da AWS. AWS anuncia endereços IP públicos desses grupos exclusivos. Um grupo de bordas de rede consiste em Zonas de Disponibilidade, Zonas Locais ou Zonas de Wavelength. Você pode alocar explicitamente um 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 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 use 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

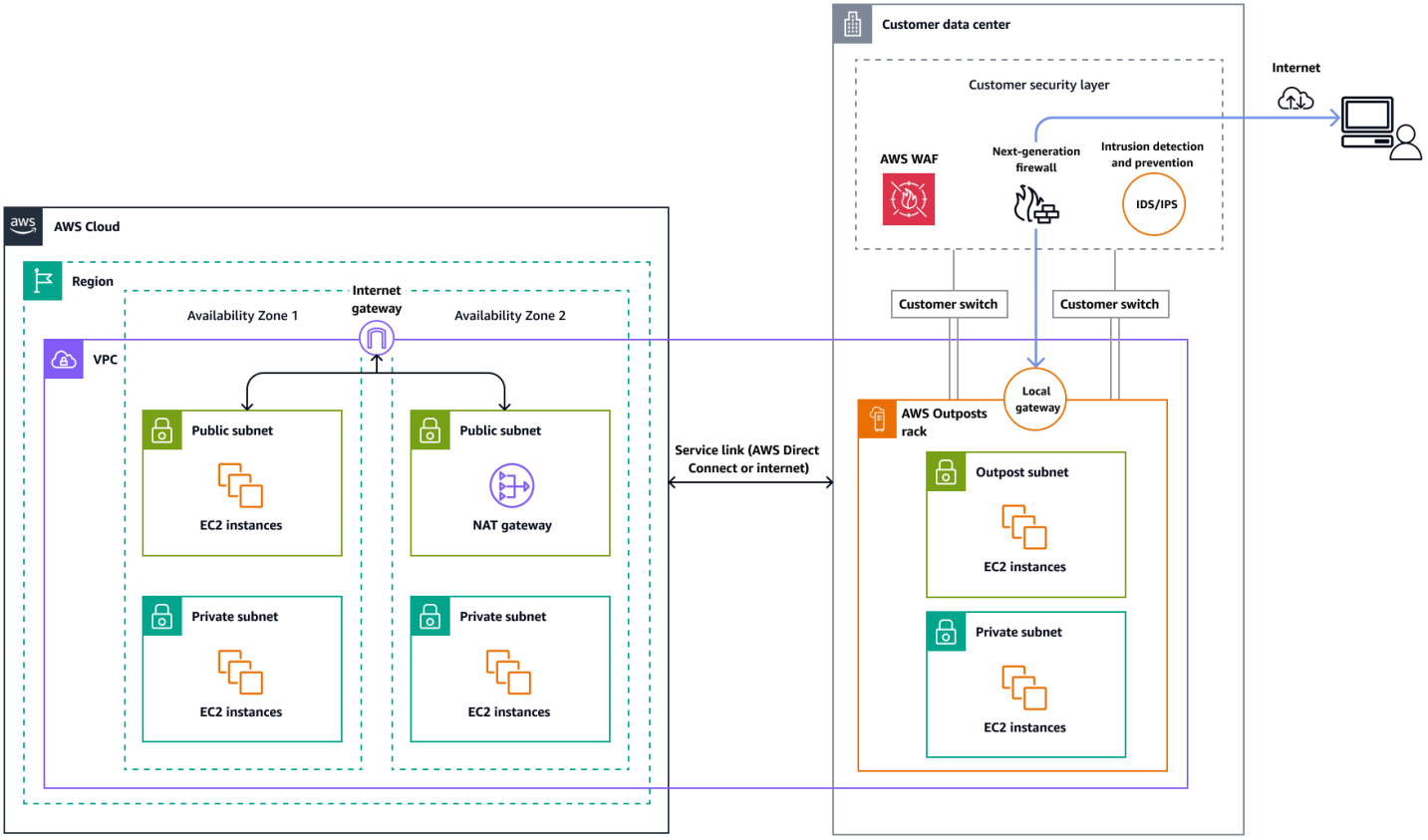
O diagrama a seguir mostra o tráfego entre a carga de trabalho na AWS Outposts instância e a Internet passando pela principal Região da AWS.



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 do AWS Well-Architected Framework)

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 Outpost, configurem VPCs, iniciem e executem instâncias no Outpost compartilhado.

Os recursos compartilháveis em AWS Outposts são:

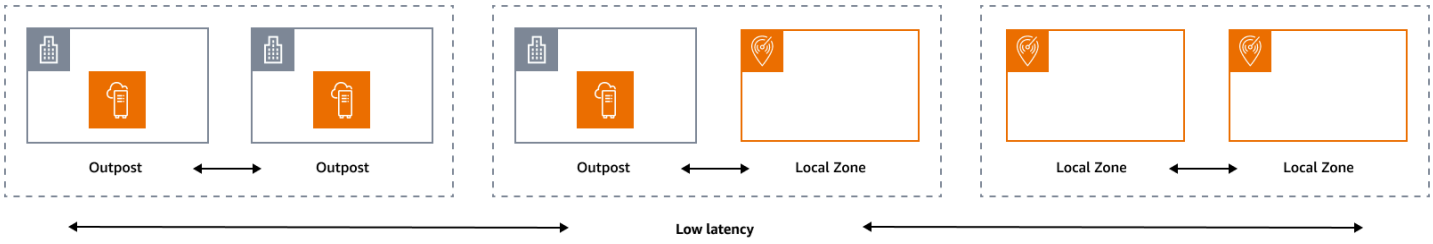
- Hosts dedicados alocados
- Reservas de capacidade
- Pools de endereços IP (CoIP) de propriedade do cliente
- Tabelas de rotas de gateway local
- Outposts
- Amazon S3 on Outposts
- Sites
- Sub-redes

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, APIs, e as ferramentas para 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 o 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 arquitetura Multi-AZ 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:

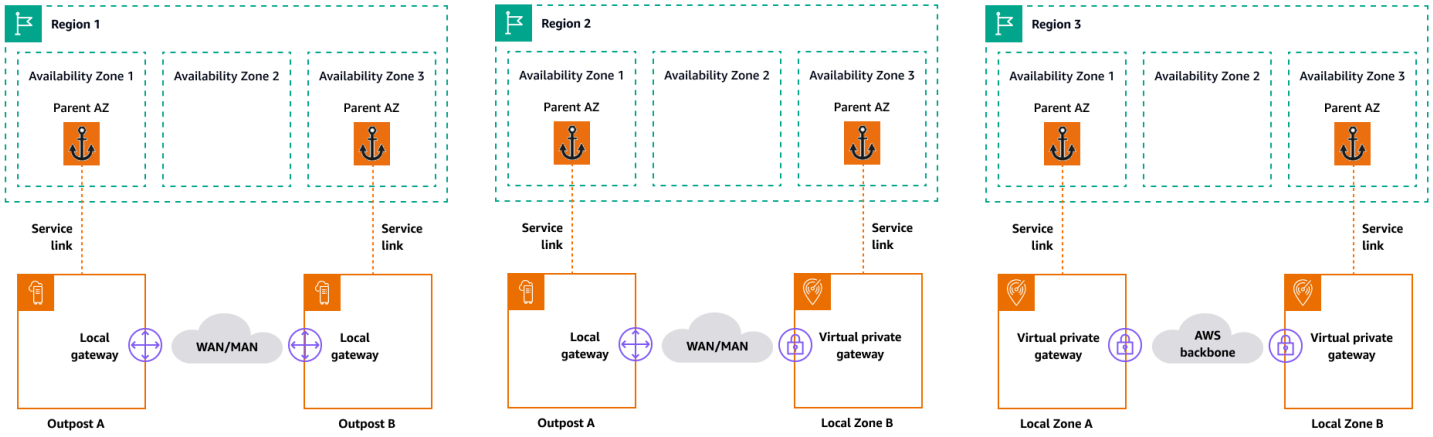
```
aws ec2 describe-availability-zones --zone-ids use1-mia1-az1
```

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

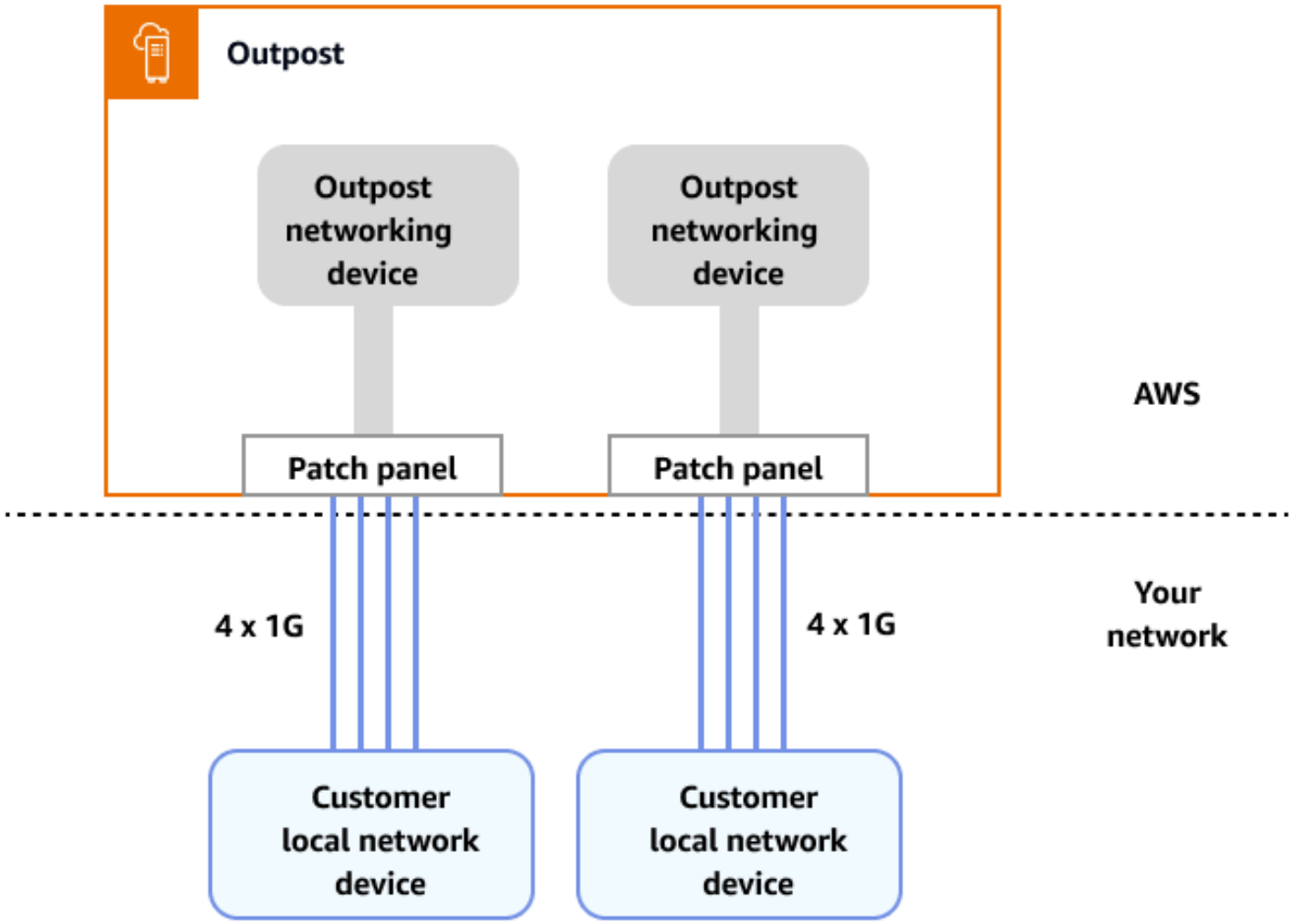
As Zonas Locais são conectadas à região principal com vários links redundantes, seguros e de alta velocidade que permitem que você consuma qualquer serviço regional, como Amazon S3 e Amazon RDS, sem problemas. Você é responsável por fornecer conectividade do seu ambiente local ou dos usuários à Zona Local. Independentemente da arquitetura de conectividade escolhida (por exemplo, VPN ou AWS 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 AWS Direct Connect, as arquiteturas de resiliência aplicáveis são as mesmas para acessar um Região da AWS, conforme documentado nas recomendações de AWS 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 AWS Direct Connect PoP impossibilita a criação das arquiteturas recomendadas para AWS Direct Connect resiliência. Se você tiver acesso a apenas um único AWS Direct Connect local ou precisar de resiliência além de uma única conexão, poderá criar um dispositivo VPN na Amazon EC2 e AWS Direct Connect, conforme ilustrado e discutido na postagem do AWS 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

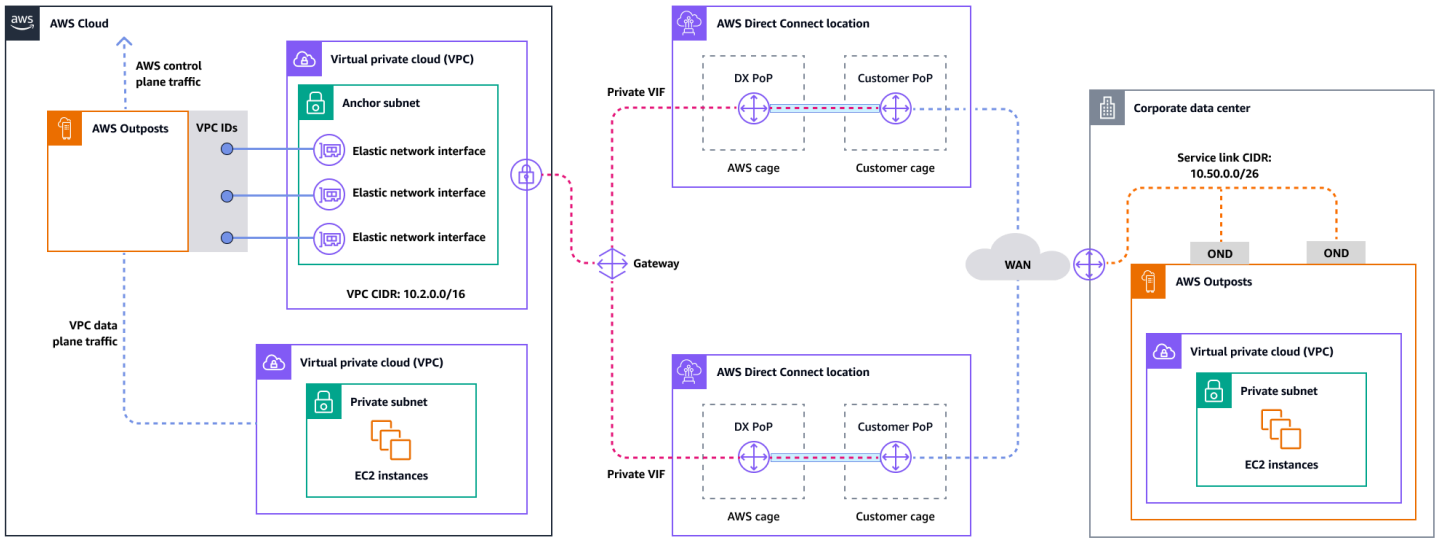
Velocidade do uplink	Número de uplinks
40 ou 100 Gbps	1, 2, ou 4



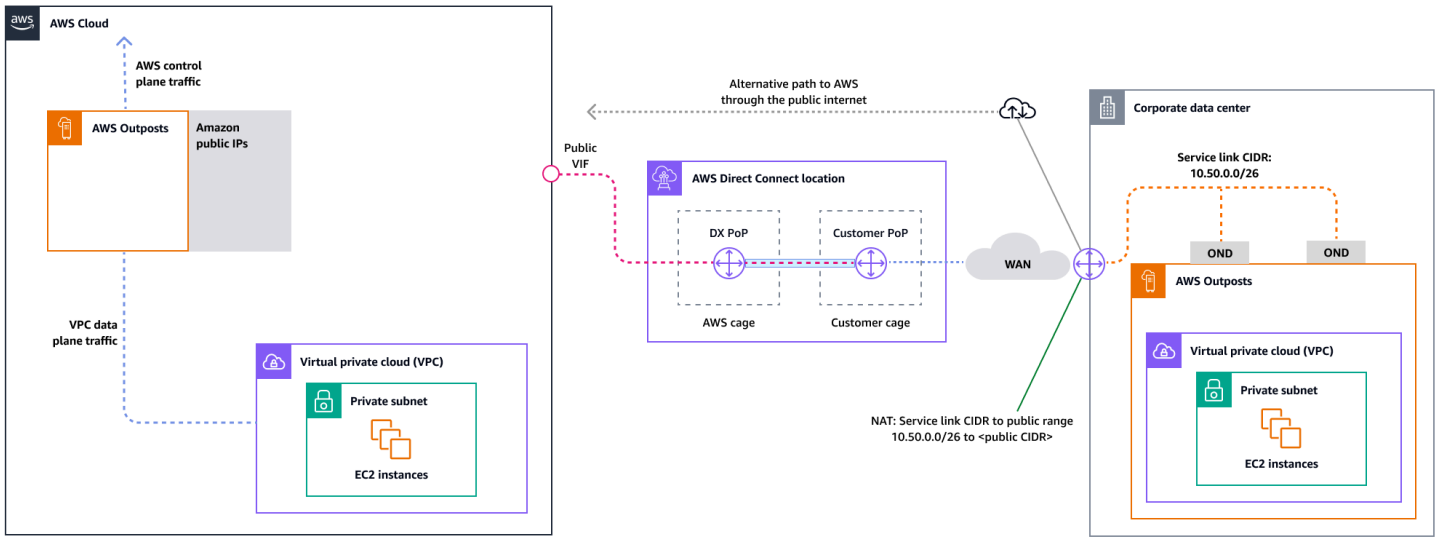
Para obter mais informações sobre essa conectividade, consulte Conectividade de rede local para Outposts Racks na documentação. AWS Outposts

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 AWS Direct Connect ou uma conexão com a Internet para o link do serviço. Esse mínimo permite que você inicie EC2 instâncias, 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.



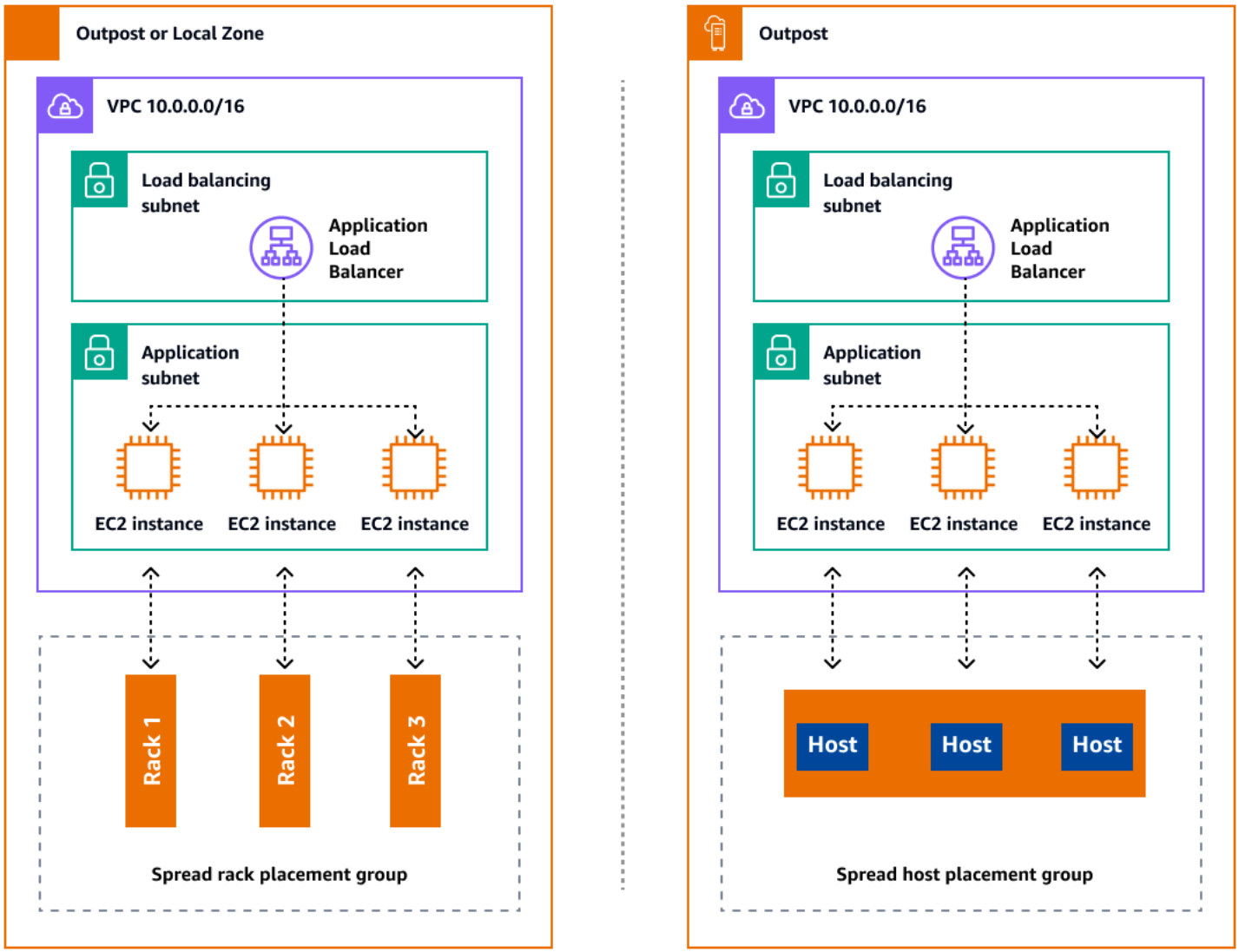
Dimensionando as implantações de rack do Outposts com racks ACE

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 rack de distribuição e do host de distribuição.



Amazon RDS Multi-AZ em AWS Outposts

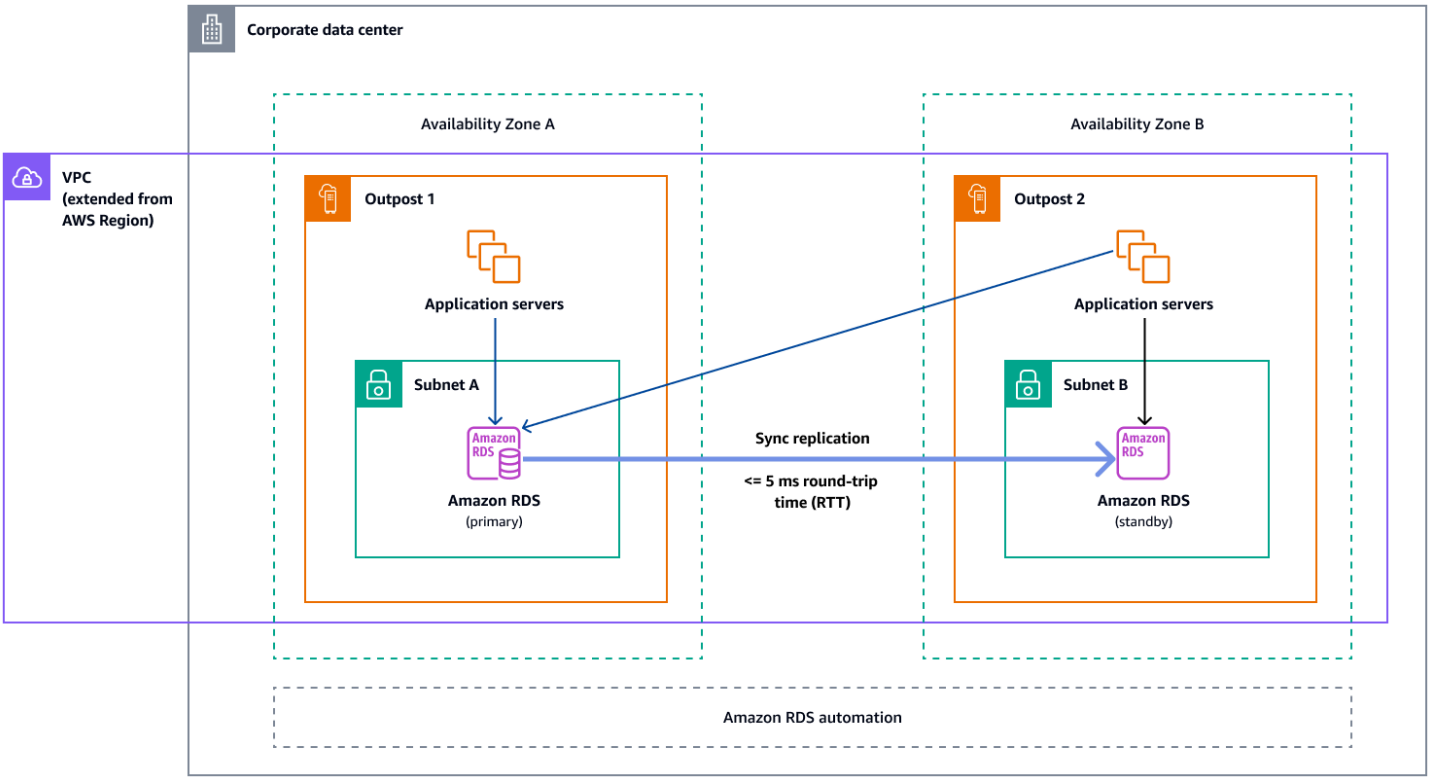
Quando você usa implantações de instâncias Multi-AZ em Outposts, o Amazon RDS cria duas instâncias de banco de dados em dois Outposts. Cada posto avançado funciona em sua própria infraestrutura física e se conecta a diferentes zonas de disponibilidade em uma região para obter alta disponibilidade. Quando 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. No caso de implantações multi-AZ, o Amazon RDS cria uma instância de banco de dados primário em um Outpost e replica de forma síncrona os dados em uma

instância de banco de dados em espera em outro Outpost. As implantações Multi-AZ em Outposts operam como implantações Multi-AZ em Regiões da AWS, 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 Endereços IP de propriedade do cliente para o Amazon RDS na documentação AWS Outposts do Amazon RDS.
- A replicação é realizada na sua rede local.

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

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

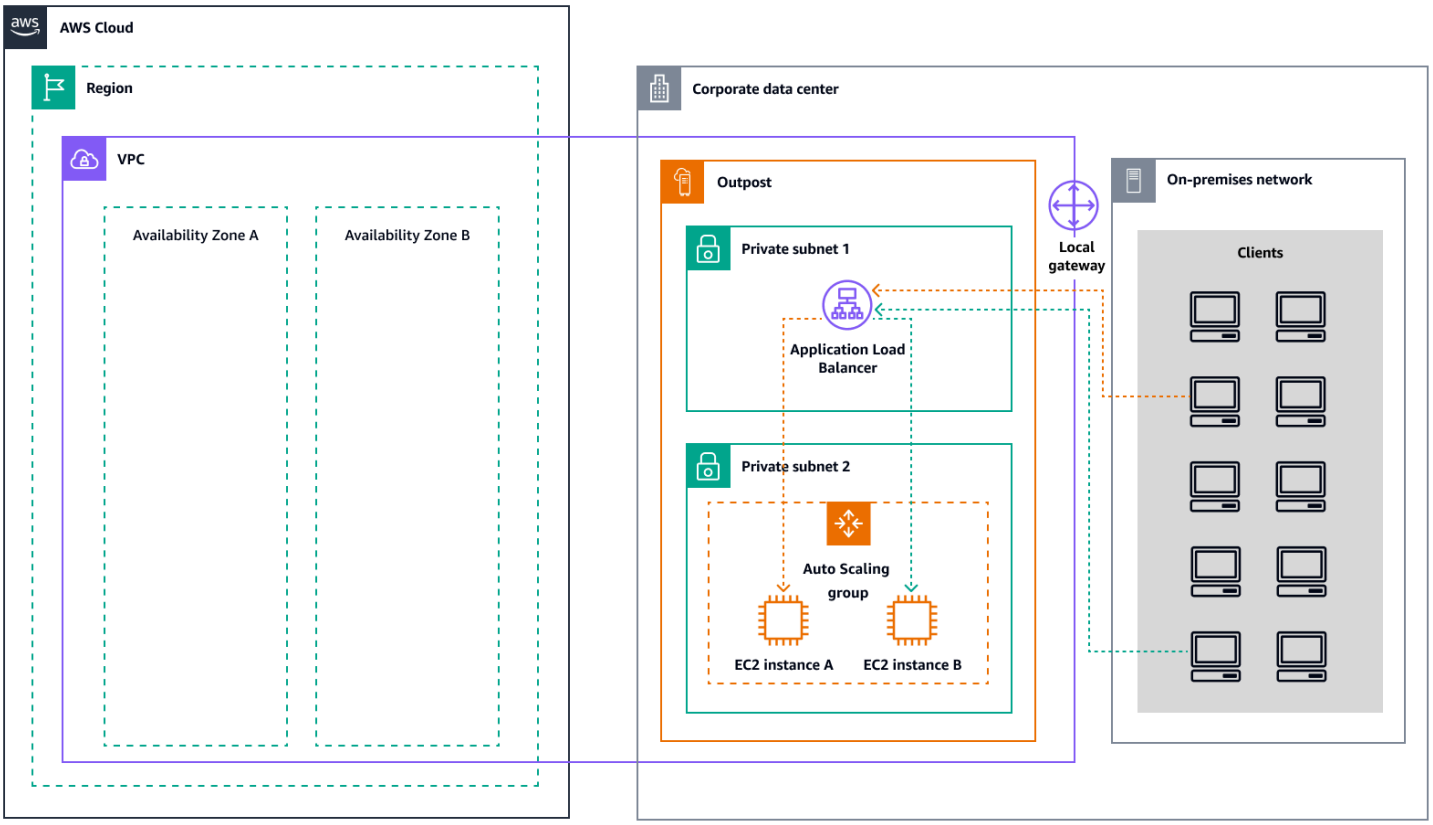


Mecanismos de failover

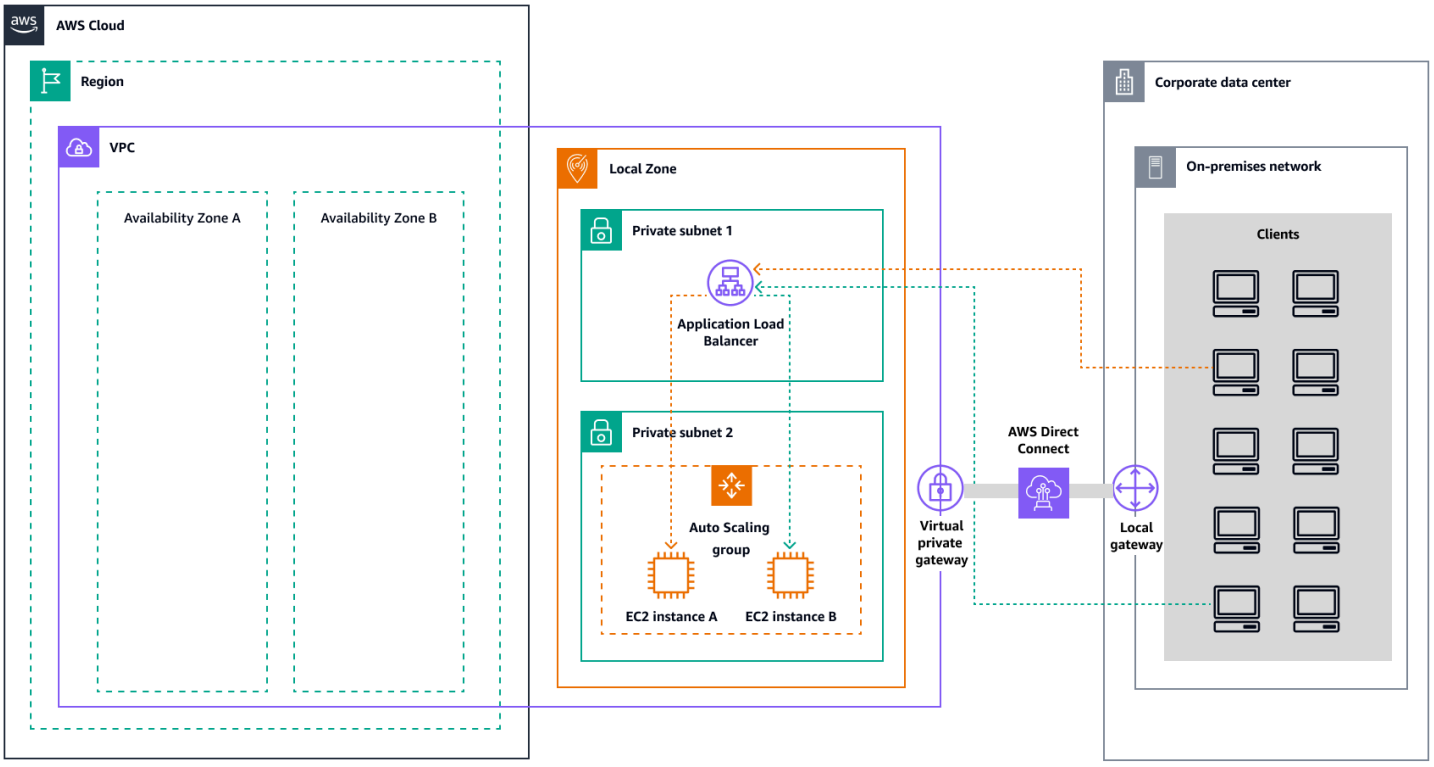
Balanceamento de carga e escalabilidade automática

O Elastic Load Balancing (ELB) distribui automaticamente o tráfego de entrada do aplicativo em todas as EC2 instâncias 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 de 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. Ao usar o ELB com seu grupo de Auto Scaling, não é necessário registrar instâncias EC2 individuais 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 Auto EC2 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 na Amazon em EC2 . AWS Outposts



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

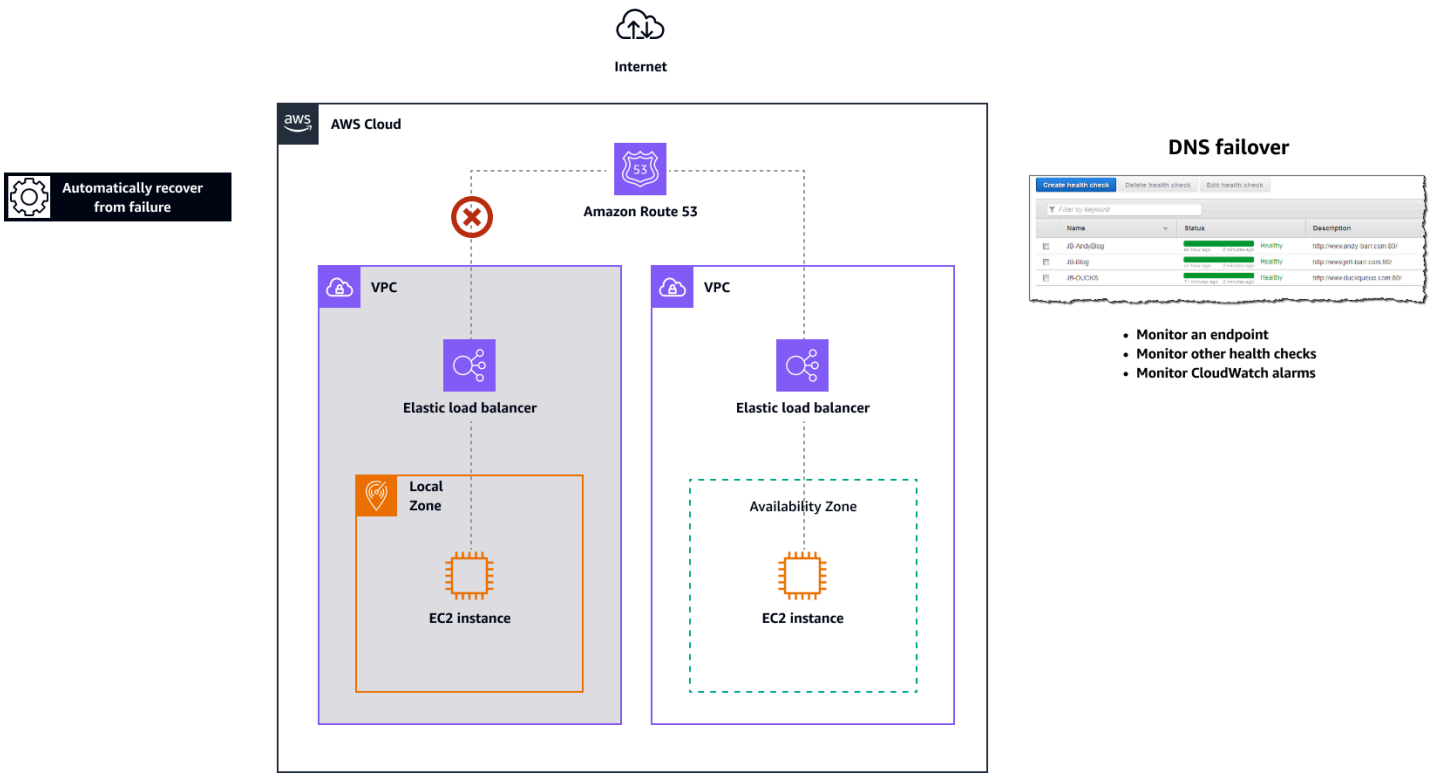


> **Note**
>
> Os Application Load Balancers estão disponíveis em ambas as Zonas AWS Outposts e em Locais. No entanto, para usar um Application Load Balancer em AWS Outposts, você precisa dimensionar a EC2 capacidade da Amazon para fornecer a escalabilidade que o balanceador de carga exige. Para obter 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) do público IPs 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 aplicativo hospedado no Outposts.

Amazon Route 53 Resolver em 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 Outposts VPCs 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
AWS Elastic Disaster Recovery	Trabalhando com AWS Elastic Disaster Recovery e AWS Outposts	Não disponível
AWS Application Migration Service	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 for 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

Analisando

- 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

AWS Glossário de orientação prescritiva

A seguir estão os termos comumente usados em estratégias, guias e padrões fornecidos pela Orientação AWS Prescritiva. Para sugerir entradas, use o link Fornecer feedback no final do glossário.

Números

7 Rs

Sete estratégias comuns de migração para mover aplicações para a nuvem. Essas estratégias baseiam-se nos 5 Rs identificados pela Gartner em 2011 e consistem em:

- Refatorar/rearquitetar: mova uma aplicação e modifique sua arquitetura aproveitando ao máximo os recursos nativos de nuvem para melhorar a agilidade, a performance e a escalabilidade. Isso normalmente envolve a portabilidade do sistema operacional e do banco de dados. Exemplo: migre seu banco de dados Oracle local para a edição compatível com o Amazon Aurora PostgreSQL.
- Redefinir a plataforma (mover e redefinir [mover e redefinir (lift-and-reshape]): mova uma aplicação para a nuvem e introduza algum nível de otimização a fim de aproveitar os recursos da nuvem. Exemplo: Migre seu banco de dados Oracle local para o Amazon Relational Database Service (Amazon RDS) for Oracle no. Nuvem AWS
- Recomprar (drop and shop): mude para um produto diferente, normalmente migrando de uma licença tradicional para um modelo SaaS. Exemplo: migre seu sistema de gerenciamento de relacionamento com o cliente (CRM) para a Salesforce.com.
- Redefinir a hospedagem (mover sem alterações [lift-and-shift])mover uma aplicação para a nuvem sem fazer nenhuma alteração a fim de aproveitar os recursos da nuvem. Exemplo: Migre seu banco de dados Oracle local para o Oracle em uma EC2 instância no. Nuvem AWS
- Realocar (mover o hipervisor sem alterações [hypervisor-level lift-and-shift]): mover a infraestrutura para a nuvem sem comprar novo hardware, reescrever aplicações ou modificar suas operações existentes. Você migra servidores de uma plataforma local para um serviço em nuvem para a mesma plataforma. Exemplo: Migrar um Microsoft Hyper-V aplicativo para o. AWS
- Reter (revisitar): mantenha as aplicações em seu ambiente de origem. Isso pode incluir aplicações que exigem grande refatoração, e você deseja adiar esse trabalho para um

momento posterior, e aplicações antigas que você deseja manter porque não há justificativa comercial para migrá-las.

- Retirar: desative ou remova aplicações que não são mais necessárias em seu ambiente de origem.

A

ABAC

Consulte controle de acesso baseado em atributos.

serviços abstratos

Veja os serviços gerenciados.

ACID

Veja atomicidade, consistência, isolamento, durabilidade.

migração ativa-ativa

Um método de migração de banco de dados no qual os bancos de dados de origem e de destino são mantidos em sincronia (por meio de uma ferramenta de replicação bidirecional ou operações de gravação dupla), e ambos os bancos de dados lidam com transações de aplicações conectadas durante a migração. Esse método oferece suporte à migração em lotes pequenos e controlados, em vez de exigir uma substituição única. É mais flexível, mas exige mais trabalho do que a migração ativa-passiva.

migração ativa-passiva

Um método de migração de banco de dados no qual os bancos de dados de origem e de destino são mantidos em sincronia, mas somente o banco de dados de origem manipula as transações dos aplicativos de conexão enquanto os dados são replicados no banco de dados de destino. O banco de dados de destino não aceita nenhuma transação durante a migração.

função agregada

Uma função SQL que opera em um grupo de linhas e calcula um único valor de retorno para o grupo. Exemplos de funções agregadas incluem `SUM` e. `MAX`

AI

Veja inteligência artificial.

AIOps

Veja as operações de inteligência artificial.

anonimização

O processo de excluir permanentemente informações pessoais em um conjunto de dados. A anonimização pode ajudar a proteger a privacidade pessoal. Dados anônimos não são mais considerados dados pessoais.

antipadrões

Uma solução frequentemente usada para um problema recorrente em que a solução é contraproducente, ineficaz ou menos eficaz do que uma alternativa.

controle de aplicativos

Uma abordagem de segurança que permite o uso somente de aplicativos aprovados para ajudar a proteger um sistema contra malware.

portfólio de aplicações

Uma coleção de informações detalhadas sobre cada aplicação usada por uma organização, incluindo o custo para criar e manter a aplicação e seu valor comercial. Essas informações são fundamentais para o processo de descoberta e análise de portfólio e ajudam a identificar e priorizar as aplicações a serem migradas, modernizadas e otimizadas.

inteligência artificial (IA)

O campo da ciência da computação que se dedica ao uso de tecnologias de computação para desempenhar funções cognitivas normalmente associadas aos humanos, como aprender, resolver problemas e reconhecer padrões. Para obter mais informações, consulte O que é inteligência artificial?

operações de inteligência artificial (AIOps)

O processo de usar técnicas de machine learning para resolver problemas operacionais, reduzir incidentes operacionais e intervenção humana e aumentar a qualidade do serviço. Para obter mais informações sobre como AIOps é usado na estratégia de AWS migração, consulte o guia de integração de operações.

criptografia assimétrica

Um algoritmo de criptografia que usa um par de chaves, uma chave pública para criptografia e uma chave privada para descriptografia. É possível compartilhar a chave pública porque ela não é usada na descriptografia, mas o acesso à chave privada deve ser altamente restrito.

atomicidade, consistência, isolamento, durabilidade (ACID)

Um conjunto de propriedades de software que garantem a validade dos dados e a confiabilidade operacional de um banco de dados, mesmo no caso de erros, falhas de energia ou outros problemas.

controle de acesso por atributo (ABAC)

A prática de criar permissões minuciosas com base nos atributos do usuário, como departamento, cargo e nome da equipe. Para obter mais informações, consulte ABAC AWS na documentação AWS Identity and Access Management (IAM).

fonte de dados autorizada

Um local onde você armazena a versão principal dos dados, que é considerada a fonte de informações mais confiável. Você pode copiar dados da fonte de dados autorizada para outros locais com o objetivo de processar ou modificar os dados, como anonimizá-los, redigi-los ou pseudonimizá-los.

Availability Zone

Um local distinto dentro de um Região da AWS que está isolado de falhas em outras zonas de disponibilidade e fornece conectividade de rede barata e de baixa latência a outras zonas de disponibilidade na mesma região.

AWS Estrutura de adoção da nuvem (AWS CAF)

Uma estrutura de diretrizes e melhores práticas AWS para ajudar as organizações a desenvolver um plano eficiente e eficaz para migrar com sucesso para a nuvem. AWS O CAF organiza a orientação em seis áreas de foco chamadas perspectivas: negócios, pessoas, governança, plataforma, segurança e operações. As perspectivas de negócios, pessoas e governança têm como foco habilidades e processos de negócios; as perspectivas de plataforma, segurança e operações concentram-se em habilidades e processos técnicos. Por exemplo, a perspectiva das pessoas tem como alvo as partes interessadas que lidam com recursos humanos (RH), funções de pessoal e gerenciamento de pessoal. Nessa perspectiva, o AWS CAF fornece orientação para desenvolvimento, treinamento e comunicação de pessoas para ajudar a preparar a organização

para a adoção bem-sucedida da nuvem. Para obter mais informações, consulte o site da AWS CAF e o whitepaper da AWS CAF.

AWS Estrutura de qualificação da carga de trabalho (AWS WQF)

Uma ferramenta que avalia as cargas de trabalho de migração do banco de dados, recomenda estratégias de migração e fornece estimativas de trabalho. AWS O WQF está incluído com AWS Schema Conversion Tool ()AWS SCT. Ela analisa esquemas de banco de dados e objetos de código, código de aplicações, dependências e características de performance, além de fornecer relatórios de avaliação.

B

bot ruim

Um bot destinado a perturbar ou causar danos a indivíduos ou organizações.

BCP

Veja o planejamento de continuidade de negócios.

gráfico de comportamento

Uma visualização unificada e interativa do comportamento e das interações de recursos ao longo do tempo. É possível usar um gráfico de comportamento com o Amazon Detective para examinar tentativas de login malsucedidas, chamadas de API suspeitas e ações similares. Para obter mais informações, consulte Dados em um gráfico de comportamento na documentação do Detective.

sistema big-endian

Um sistema que armazena o byte mais significativo antes. Veja também endianness.

classificação binária

Um processo que prevê um resultado binário (uma de duas classes possíveis). Por exemplo, seu modelo de ML pode precisar prever problemas como “Este e-mail é ou não é spam?” ou “Este produto é um livro ou um carro?”

filtro de bloom

Uma estrutura de dados probabilística e eficiente em termos de memória que é usada para testar se um elemento é membro de um conjunto.

blue/green deployment (implantação azul/verde)

Uma estratégia de implantação em que você cria dois ambientes separados, mas idênticos. Você executa a versão atual do aplicativo em um ambiente (azul) e a nova versão do aplicativo no outro ambiente (verde). Essa estratégia ajuda você a reverter rapidamente com o mínimo de impacto.

bot

Um aplicativo de software que executa tarefas automatizadas pela Internet e simula a atividade ou interação humana. Alguns bots são úteis ou benéficos, como rastreadores da Web que indexam informações na Internet. Alguns outros bots, conhecidos como bots ruins, têm como objetivo perturbar ou causar danos a indivíduos ou organizações.

botnet

Redes de bots infectadas por malware e sob o controle de uma única parte, conhecidas como pastor de bots ou operador de bots. As redes de bots são o mecanismo mais conhecido para escalar bots e seu impacto.

ramo

Uma área contida de um repositório de código. A primeira ramificação criada em um repositório é a ramificação principal. Você pode criar uma nova ramificação a partir de uma ramificação existente e, em seguida, desenvolver recursos ou corrigir bugs na nova ramificação. Uma ramificação que você cria para gerar um recurso é comumente chamada de ramificação de recurso. Quando o recurso estiver pronto para lançamento, você mesclará a ramificação do recurso de volta com a ramificação principal. Para obter mais informações, consulte Sobre filiais (GitHub documentação).

acesso em vidro quebrado

Em circunstâncias excepcionais e por meio de um processo aprovado, um meio rápido para um usuário obter acesso a um Conta da AWS que ele normalmente não tem permissão para acessar. Para obter mais informações, consulte o indicador Implementar procedimentos de quebra de vidro na orientação do Well-Architected AWS .

estratégia brownfield

A infraestrutura existente em seu ambiente. Ao adotar uma estratégia brownfield para uma arquitetura de sistema, você desenvolve a arquitetura de acordo com as restrições dos sistemas e da infraestrutura atuais. Se estiver expandindo a infraestrutura existente, poderá combinar as estratégias brownfield e greenfield.

cache do buffer

A área da memória em que os dados acessados com mais frequência são armazenados.

capacidade de negócios

O que uma empresa faz para gerar valor (por exemplo, vendas, atendimento ao cliente ou marketing). As arquiteturas de microsserviços e as decisões de desenvolvimento podem ser orientadas por recursos de negócios. Para obter mais informações, consulte a seção Organizados de acordo com as capacidades de negócios do whitepaper Executar microsserviços conteinerizados na AWS.

planejamento de continuidade de negócios (BCP)

Um plano que aborda o impacto potencial de um evento disruptivo, como uma migração em grande escala, nas operações e permite que uma empresa retome as operações rapidamente.

C

CAF

Consulte Estrutura de adoção da AWS nuvem.

implantação canária

O lançamento lento e incremental de uma versão para usuários finais. Quando estiver confiante, você implanta a nova versão e substituirá a versão atual em sua totalidade.

CCoE

Veja o Centro de Excelência em Nuvem.

CDC

Veja a captura de dados de alterações.

captura de dados de alterações (CDC)

O processo de rastrear alterações em uma fonte de dados, como uma tabela de banco de dados, e registrar metadados sobre a alteração. É possível usar o CDC para várias finalidades, como auditar ou replicar alterações em um sistema de destino para manter a sincronização.

engenharia do caos

Introduzir intencionalmente falhas ou eventos disruptivos para testar a resiliência de um sistema. Você pode usar AWS Fault Injection Service (AWS FIS) para realizar experimentos que estressam suas AWS cargas de trabalho e avaliar sua resposta.

CI/CD

Veja a integração e a entrega contínuas.

classificação

Um processo de categorização que ajuda a gerar previsões. Os modelos de ML para problemas de classificação predizem um valor discreto. Os valores discretos são sempre diferentes uns dos outros. Por exemplo, um modelo pode precisar avaliar se há ou não um carro em uma imagem.

criptografia no lado do cliente

Criptografia de dados localmente, antes que o alvo os AWS service (Serviço da AWS) receba.

Centro de excelência em nuvem (CCoE)

Uma equipe multidisciplinar que impulsiona os esforços de adoção da nuvem em toda a organização, incluindo o desenvolvimento de práticas recomendas de nuvem, a mobilização de recursos, o estabelecimento de cronogramas de migração e a liderança da organização em transformações em grande escala. Para obter mais informações, consulte as publicações CCo E no blog de estratégia Nuvem AWS corporativa.

computação em nuvem

A tecnologia de nuvem normalmente usada para armazenamento de dados remoto e gerenciamento de dispositivos de IoT. A computação em nuvem geralmente está conectada à tecnologia de computação de ponta.

modelo operacional em nuvem

Em uma organização de TI, o modelo operacional usado para criar, amadurecer e otimizar um ou mais ambientes de nuvem. Para obter mais informações, consulte Criar seu modelo operacional de nuvem.

estágios de adoção da nuvem

As quatro fases pelas quais as organizações normalmente passam quando migram para o Nuvem AWS:

- Projeto: executar alguns projetos relacionados à nuvem para fins de prova de conceito e aprendizado
- Fundação — Fazer investimentos fundamentais para escalar sua adoção da nuvem (por exemplo, criar uma landing zone, definir um CCo E, estabelecer um modelo de operações)
- Migração: migrar aplicações individuais
- Reinvenção: otimizar produtos e serviços e inovar na nuvem

Esses estágios foram definidos por Stephen Orban na postagem do blog The Journey Toward Cloud-First & the Stages of Adoption no blog de estratégia Nuvem AWS empresarial. Para obter informações sobre como eles se relacionam com a estratégia de AWS migração, consulte o guia de preparação para migração.

CMDB

Consulte o banco de dados de gerenciamento de configuração.

repositório de código

Um local onde o código-fonte e outros ativos, como documentação, amostras e scripts, são armazenados e atualizados por meio de processos de controle de versão. Os repositórios de nuvem comuns incluem GitHub ouBitbucket Cloud. Cada versão do código é chamada de ramificação. Em uma estrutura de microsserviços, cada repositório é dedicado a uma única peça de funcionalidade. Um único pipeline de CI/CD pode usar vários repositórios.

cache frio

Um cache de buffer que está vazio, não está bem preenchido ou contém dados obsoletos ou irrelevantes. Isso afeta a performance porque a instância do banco de dados deve ler da memória principal ou do disco, um processo que é mais lento do que a leitura do cache do buffer.

dados frios

Dados que raramente são acessados e geralmente são históricos. Ao consultar esse tipo de dados, consultas lentas geralmente são aceitáveis. Mover esses dados para níveis ou classes de armazenamento de baixo desempenho e menos caros pode reduzir os custos.

visão computacional (CV)

Um campo da IA que usa aprendizado de máquina para analisar e extrair informações de formatos visuais, como imagens e vídeos digitais. Por exemplo, a Amazon SageMaker AI fornece algoritmos de processamento de imagem para CV.

desvio de configuração

Para uma carga de trabalho, uma alteração de configuração em relação ao estado esperado. Isso pode fazer com que a carga de trabalho se torne incompatível e, normalmente, é gradual e não intencional.

banco de dados de gerenciamento de configuração (CMDB)

Um repositório que armazena e gerencia informações sobre um banco de dados e seu ambiente de TI, incluindo componentes de hardware e software e suas configurações. Normalmente, os dados de um CMDB são usados no estágio de descoberta e análise do portfólio da migração.

pacote de conformidade

Um conjunto de AWS Config regras e ações de remediação que você pode montar para personalizar suas verificações de conformidade e segurança. Você pode implantar um pacote de conformidade como uma entidade única em uma Conta da AWS região ou em uma organização usando um modelo YAML. Para obter mais informações, consulte Pacotes de conformidade na documentação. AWS Config

integração contínua e entrega contínua (CI/CD)

O processo de automatizar os estágios de origem, criação, teste, preparação e produção do processo de lançamento do software. CI/CD é comumente descrito como um pipeline. CI/CD pode ajudá-lo a automatizar processos, melhorar a produtividade, melhorar a qualidade do código e entregar com mais rapidez. Para obter mais informações, consulte Benefícios da entrega contínua. CD também pode significar implantação contínua. Para obter mais informações, consulte Entrega contínua versus implantação contínua.

CV

Veja visão computacional.

D

dados em repouso

Dados estacionários em sua rede, por exemplo, dados que estão em um armazenamento.

classificação de dados

Um processo para identificar e categorizar os dados em sua rede com base em criticalidade e confidencialidade. É um componente crítico de qualquer estratégia de gerenciamento de riscos de

segurança cibernética, pois ajuda a determinar os controles adequados de proteção e retenção para os dados. A classificação de dados é um componente do pilar de segurança no AWS Well-Architected Framework. Para obter mais informações, consulte Classificação de dados.

desvio de dados

Uma variação significativa entre os dados de produção e os dados usados para treinar um modelo de ML ou uma alteração significativa nos dados de entrada ao longo do tempo. O desvio de dados pode reduzir a qualidade geral, a precisão e a imparcialidade das previsões do modelo de ML.

dados em trânsito

Dados que estão se movendo ativamente pela sua rede, como entre os recursos da rede.

malha de dados

Uma estrutura arquitetônica que fornece propriedade de dados distribuída e descentralizada com gerenciamento e governança centralizados.

minimização de dados

O princípio de coletar e processar apenas os dados estritamente necessários. Praticar a minimização de dados no Nuvem AWS pode reduzir os riscos de privacidade, os custos e a pegada de carbono de sua análise.

perímetro de dados

Um conjunto de proteções preventivas em seu AWS ambiente que ajudam a garantir que somente identidades confiáveis acessem recursos confiáveis das redes esperadas. Para obter mais informações, consulte Construindo um perímetro de dados em. AWS

pré-processamento de dados

A transformação de dados brutos em um formato que seja facilmente analisado por seu modelo de ML. O pré-processamento de dados pode significar a remoção de determinadas colunas ou linhas e o tratamento de valores ausentes, inconsistentes ou duplicados.

proveniência dos dados

O processo de rastrear a origem e o histórico dos dados ao longo de seu ciclo de vida, por exemplo, como os dados foram gerados, transmitidos e armazenados.

titular dos dados

Um indivíduo cujos dados estão sendo coletados e processados.

data warehouse

Um sistema de gerenciamento de dados que oferece suporte à inteligência comercial, como análises. Os data warehouses geralmente contêm grandes quantidades de dados históricos e geralmente são usados para consultas e análises.

linguagem de definição de dados (DDL)

Instruções ou comandos para criar ou modificar a estrutura de tabelas e objetos em um banco de dados.

linguagem de manipulação de dados (DML)

Instruções ou comandos para modificar (inserir, atualizar e excluir) informações em um banco de dados.

DDL

Consulte a linguagem de definição de banco de dados.

deep ensemble

A combinação de vários modelos de aprendizado profundo para gerar previsões. Os deep ensembles podem ser usados para produzir uma previsão mais precisa ou para estimar a incerteza nas previsões.

Aprendizado profundo

Um subcampo do ML que usa várias camadas de redes neurais artificiais para identificar o mapeamento entre os dados de entrada e as variáveis-alvo de interesse.

defense-in-depth

Uma abordagem de segurança da informação na qual uma série de mecanismos e controles de segurança são cuidadosamente distribuídos por toda a rede de computadores para proteger a confidencialidade, a integridade e a disponibilidade da rede e dos dados nela contidos. Ao adotar essa estratégia AWS, você adiciona vários controles em diferentes camadas da AWS Organizations estrutura para ajudar a proteger os recursos. Por exemplo, uma defense-in-depth abordagem pode combinar autenticação multifatorial, segmentação de rede e criptografia.

administrador delegado

Em AWS Organizations, um serviço compatível pode registrar uma conta de AWS membro para administrar as contas da organização e gerenciar as permissões desse serviço. Essa conta

é chamada de administrador delegado para esse serviço Para obter mais informações e uma lista de serviços compatíveis, consulte Serviços que funcionam com o AWS Organizations na documentação do AWS Organizations .

implantação

O processo de criar uma aplicação, novos recursos ou correções de código disponíveis no ambiente de destino. A implantação envolve a implementação de mudanças em uma base de código e, em seguida, a criação e execução dessa base de código nos ambientes da aplicação

ambiente de desenvolvimento

Veja o ambiente.

controle detectivo

Um controle de segurança projetado para detectar, registrar e alertar após a ocorrência de um evento. Esses controles são uma segunda linha de defesa, alertando você sobre eventos de segurança que contornaram os controles preventivos em vigor. Para obter mais informações, consulte Controles detectivos em Como implementar controles de segurança na AWS.

mapeamento do fluxo de valor de desenvolvimento (DVSM)

Um processo usado para identificar e priorizar restrições que afetam negativamente a velocidade e a qualidade em um ciclo de vida de desenvolvimento de software. O DVSM estende o processo de mapeamento do fluxo de valor originalmente projetado para práticas de manufatura enxuta. Ele se concentra nas etapas e equipes necessárias para criar e movimentar valor por meio do processo de desenvolvimento de software.

gêmeo digital

Uma representação virtual de um sistema real, como um prédio, fábrica, equipamento industrial ou linha de produção. Os gêmeos digitais oferecem suporte à manutenção preditiva, ao monitoramento remoto e à otimização da produção.

tabela de dimensões

Em um esquema em estrela, uma tabela menor que contém atributos de dados sobre dados quantitativos em uma tabela de fatos. Os atributos da tabela de dimensões geralmente são campos de texto ou números discretos que se comportam como texto. Esses atributos são comumente usados para restringir consultas, filtrar e rotular conjuntos de resultados.

desastre

Um evento que impede que uma workload ou sistema cumpra seus objetivos de negócios em seu local principal de implantação. Esses eventos podem ser desastres naturais, falhas técnicas ou o resultado de ações humanas, como configuração incorreta não intencional ou ataque de malware.

Recuperação de desastres (RD)

A estratégia e o processo que você usa para minimizar o tempo de inatividade e a perda de dados causados por um desastre. Para obter mais informações, consulte Recuperação de desastres de cargas de trabalho em AWS: Recuperação na nuvem no AWS Well-Architected Framework.

DML

Veja a linguagem de manipulação de banco de dados.

design orientado por domínio

Uma abordagem ao desenvolvimento de um sistema de software complexo conectando seus componentes aos domínios em evolução, ou principais metas de negócios, atendidos por cada componente. Esse conceito foi introduzido por Eric Evans em seu livro, Design orientado por domínio: lidando com a complexidade no coração do software (Boston: Addison-Wesley Professional, 2003). Para obter informações sobre como usar o design orientado por domínio com o padrão strangler fig, consulte Modernizar incrementalmente os serviços web herdados do Microsoft ASP.NET (ASMX) usando contêineres e o Amazon API Gateway.

DR

Veja a recuperação de desastres.

detecção de deriva

Rastreando desvios de uma configuração básica. Por exemplo, você pode usar AWS CloudFormation para detectar desvios nos recursos do sistema ou AWS Control Tower para detectar mudanças em seu landing zone que possam afetar a conformidade com os requisitos de governança.

DVSM

Veja o mapeamento do fluxo de valor do desenvolvimento.

E

EDA

Veja a análise exploratória de dados.

EDI

Veja intercâmbio eletrônico de dados.

computação de borda

A tecnologia que aumenta o poder computacional de dispositivos inteligentes nas bordas de uma rede de IoT. Quando comparada à computação em nuvem, a computação de ponta pode reduzir a latência da comunicação e melhorar o tempo de resposta.

intercâmbio eletrônico de dados (EDI)

A troca automatizada de documentos comerciais entre organizações. Para obter mais informações, consulte O que é intercâmbio eletrônico de dados.

Criptografia

Um processo de computação que transforma dados de texto simples, legíveis por humanos, em texto cifrado.

chave de criptografia

Uma sequência criptográfica de bits aleatórios que é gerada por um algoritmo de criptografia. As chaves podem variar em tamanho, e cada chave foi projetada para ser imprevisível e exclusiva.

endianismo

A ordem na qual os bytes são armazenados na memória do computador. Os sistemas big-endian armazenam o byte mais significativo antes. Os sistemas little-endian armazenam o byte menos significativo antes.

endpoint

Veja o endpoint do serviço.

serviço de endpoint

Um serviço que pode ser hospedado em uma nuvem privada virtual (VPC) para ser compartilhado com outros usuários. Você pode criar um serviço de endpoint com AWS PrivateLink e conceder permissões a outros diretores Contas da AWS ou a AWS Identity and Access Management (IAM).

Essas contas ou entidades principais podem se conectar ao serviço de endpoint de maneira privada criando endpoints da VPC de interface. Para obter mais informações, consulte Criar um serviço de endpoint na documentação do Amazon Virtual Private Cloud (Amazon VPC).

planejamento de recursos corporativos (ERP)

Um sistema que automatiza e gerencia os principais processos de negócios (como contabilidade, MES e gerenciamento de projetos) para uma empresa.

criptografia envelopada

O processo de criptografar uma chave de criptografia com outra chave de criptografia. Para obter mais informações, consulte Criptografia de envelope na documentação AWS Key Management Service (AWS KMS).

ambiente

Uma instância de uma aplicação em execução. Estes são tipos comuns de ambientes na computação em nuvem:

- ambiente de desenvolvimento: uma instância de uma aplicação em execução que está disponível somente para a equipe principal responsável pela manutenção da aplicação. Ambientes de desenvolvimento são usados para testar mudanças antes de promovê-las para ambientes superiores. Esse tipo de ambiente às vezes é chamado de ambiente de teste.
- ambientes inferiores: todos os ambientes de desenvolvimento para uma aplicação, como aqueles usados para compilações e testes iniciais.
- ambiente de produção: uma instância de uma aplicação em execução que os usuários finais podem acessar. Em um CI/CD pipeline, o ambiente de produção é o último ambiente de implantação.
- ambientes superiores: todos os ambientes que podem ser acessados por usuários que não sejam a equipe principal de desenvolvimento. Isso pode incluir um ambiente de produção, ambientes de pré-produção e ambientes para testes de aceitação do usuário.

epic

Em metodologias ágeis, categorias funcionais que ajudam a organizar e priorizar seu trabalho. Os epics fornecem uma descrição de alto nível dos requisitos e das tarefas de implementação. Por exemplo, os épicos de segurança AWS da CAF incluem gerenciamento de identidade e acesso, controles de detetive, segurança de infraestrutura, proteção de dados e resposta a incidentes. Para obter mais informações sobre epics na estratégia de migração da AWS , consulte o guia de implementação do programa.

ERP

Veja o planejamento de recursos corporativos.

análise exploratória de dados (EDA)

O processo de analisar um conjunto de dados para entender suas principais características. Você coleta ou agrega dados e, em seguida, realiza investigações iniciais para encontrar padrões, detectar anomalias e verificar suposições. O EDA é realizado por meio do cálculo de estatísticas resumidas e da criação de visualizações de dados.

F

tabela de fatos

A tabela central em um esquema em estrela. Ele armazena dados quantitativos sobre as operações comerciais. Normalmente, uma tabela de fatos contém dois tipos de colunas: aquelas que contêm medidas e aquelas que contêm uma chave externa para uma tabela de dimensões.

falham rapidamente

Uma filosofia que usa testes frequentes e incrementais para reduzir o ciclo de vida do desenvolvimento. É uma parte essencial de uma abordagem ágil.

limite de isolamento de falhas

No Nuvem AWS, um limite, como uma zona de disponibilidade, Região da AWS um plano de controle ou um plano de dados, que limita o efeito de uma falha e ajuda a melhorar a resiliência das cargas de trabalho. Para obter mais informações, consulte Limites de isolamento de AWS falhas.

ramificação de recursos

Veja a filial.

recursos

Os dados de entrada usados para fazer uma previsão. Por exemplo, em um contexto de manufatura, os recursos podem ser imagens capturadas periodicamente na linha de fabricação.

importância do recurso

O quanto um recurso é importante para as previsões de um modelo. Isso geralmente é expresso como uma pontuação numérica que pode ser calculada por meio de várias técnicas, como

Shapley Additive Explanations (SHAP) e gradientes integrados. Para obter mais informações, consulte Interpretabilidade do modelo de aprendizado de máquina com AWS.

transformação de recursos

O processo de otimizar dados para o processo de ML, incluindo enriquecer dados com fontes adicionais, escalar valores ou extrair vários conjuntos de informações de um único campo de dados. Isso permite que o modelo de ML se beneficie dos dados. Por exemplo, se a data “2021-05-27 00:15:37” for dividida em “2021”, “maio”, “quinta” e “15”, isso poderá ajudar o algoritmo de aprendizado a aprender padrões diferenciados associados a diferentes componentes de dados.

solicitação de alguns instantes

Fornecer a um LLM um pequeno número de exemplos que demonstram a tarefa e o resultado desejado antes de solicitar que ele execute uma tarefa semelhante. Essa técnica é uma aplicação do aprendizado contextual, em que os modelos aprendem com exemplos (fotos) incorporados aos prompts. Solicitações rápidas podem ser eficazes para tarefas que exigem formatação, raciocínio ou conhecimento de domínio específicos. Veja também a solicitação zero-shot.

FGAC

Veja o controle de acesso refinado.

Controle de acesso refinado (FGAC)

O uso de várias condições para permitir ou negar uma solicitação de acesso.

migração flash-cut

Um método de migração de banco de dados que usa replicação contínua de dados por meio da captura de dados alterados para migrar dados no menor tempo possível, em vez de usar uma abordagem em fases. O objetivo é reduzir ao mínimo o tempo de inatividade.

FM

Veja o modelo da fundação.

modelo de fundação (FM)

Uma grande rede neural de aprendizado profundo que vem treinando em grandes conjuntos de dados generalizados e não rotulados. FMs são capazes de realizar uma ampla variedade de tarefas gerais, como entender a linguagem, gerar texto e imagens e conversar em linguagem natural. Para obter mais informações, consulte O que são modelos básicos.

G

IA generativa

Um subconjunto de modelos de IA que foram treinados em grandes quantidades de dados e que podem usar uma simples solicitação de texto para criar novos conteúdos e artefatos, como imagens, vídeos, texto e áudio. Para obter mais informações, consulte O que é IA generativa.

bloqueio geográfico

Veja as restrições geográficas.

restrições geográficas (bloqueio geográfico)

Na Amazon CloudFront, uma opção para impedir que usuários em países específicos acessem distribuições de conteúdo. É possível usar uma lista de permissões ou uma lista de bloqueios para especificar países aprovados e banidos. Para obter mais informações, consulte Restringir a distribuição geográfica do seu conteúdo na CloudFront documentação.

Fluxo de trabalho do GitFlow

Uma abordagem na qual ambientes inferiores e superiores usam ramificações diferentes em um repositório de código-fonte. O fluxo de trabalho do Gitflow é considerado legado, e o fluxo de trabalho baseado em troncos é a abordagem moderna e preferida.

imagem dourada

Um instantâneo de um sistema ou software usado como modelo para implantar novas instâncias desse sistema ou software. Por exemplo, na manufatura, uma imagem dourada pode ser usada para provisionar software em vários dispositivos e ajudar a melhorar a velocidade, a escalabilidade e a produtividade nas operações de fabricação de dispositivos.

estratégia greenfield

A ausência de infraestrutura existente em um novo ambiente. Ao adotar uma estratégia greenfield para uma arquitetura de sistema, é possível selecionar todas as novas tecnologias sem a restrição da compatibilidade com a infraestrutura existente, também conhecida como brownfield. Se estiver expandindo a infraestrutura existente, poderá combinar as estratégias brownfield e greenfield.

barreira de proteção

Uma regra de alto nível que ajuda a governar recursos, políticas e conformidade em todas as unidades organizacionais ()OUs. Barreiras de proteção preventivas impõem políticas para

garantir o alinhamento a padrões de conformidade. Elas são implementadas usando políticas de controle de serviço e limites de permissões do IAM. Barreiras de proteção detectivas detectam violações de políticas e problemas de conformidade e geram alertas para remediação. Eles são implementados usando AWS Config, AWS Security Hub, Amazon GuardDuty AWS Trusted Advisor, Amazon Inspector e verificações personalizadas AWS Lambda .

H

HA

Veja a alta disponibilidade.

migração heterogênea de bancos de dados

Migrar seu banco de dados de origem para um banco de dados de destino que usa um mecanismo de banco de dados diferente (por exemplo, Oracle para Amazon Aurora). A migração heterogênea geralmente faz parte de um esforço de redefinição da arquitetura, e converter o esquema pode ser uma tarefa complexa. O AWS fornece o AWS SCT para ajudar nas conversões de esquemas.

alta disponibilidade (HA)

A capacidade de uma workload operar continuamente, sem intervenção, em caso de desafios ou desastres. Os sistemas AH são projetados para realizar o failover automático, oferecer consistentemente desempenho de alta qualidade e lidar com diferentes cargas e falhas com impacto mínimo no desempenho.

modernização de historiador

Uma abordagem usada para modernizar e atualizar os sistemas de tecnologia operacional (OT) para melhor atender às necessidades do setor de manufatura. Um historiador é um tipo de banco de dados usado para coletar e armazenar dados de várias fontes em uma fábrica.

dados de retenção

Uma parte dos dados históricos rotulados que são retidos de um conjunto de dados usado para treinar um modelo de aprendizado de máquina. Você pode usar dados de retenção para avaliar o desempenho do modelo comparando as previsões do modelo com os dados de retenção.

migração homogênea de bancos de dados

Migrar seu banco de dados de origem para um banco de dados de destino que compartilha o mesmo mecanismo de banco de dados (por exemplo, Microsoft SQL Server para Amazon RDS para SQL Server). A migração homogênea geralmente faz parte de um esforço de redefinição da hospedagem ou da plataforma. É possível usar utilitários de banco de dados nativos para migrar o esquema.

dados quentes

Dados acessados com frequência, como dados em tempo real ou dados translacionais recentes. Esses dados normalmente exigem uma camada ou classe de armazenamento de alto desempenho para fornecer respostas rápidas às consultas.

hotfix

Uma correção urgente para um problema crítico em um ambiente de produção. Devido à sua urgência, um hotfix geralmente é feito fora do fluxo de trabalho normal de DevOps lançamento.

período de hipercuidados

Imediatamente após a substituição, o período em que uma equipe de migração gerencia e monitora as aplicações migradas na nuvem para resolver quaisquer problemas. Normalmente, a duração desse período é de 1 a 4 dias. No final do período de hipercuidados, a equipe de migração normalmente transfere a responsabilidade pelas aplicações para a equipe de operações de nuvem.

eu

IaC

Veja a infraestrutura como código.

Política baseada em identidade

Uma política anexada a um ou mais diretores do IAM que define suas permissões no Nuvem AWS ambiente.

aplicação ociosa

Uma aplicação que tem um uso médio de CPU e memória entre 5 e 20% em um período de 90 dias. Em um projeto de migração, é comum retirar essas aplicações ou retê-las on-premises.

IIoT

Veja a Internet das Coisas industrial.

infraestrutura imutável

Um modelo que implanta uma nova infraestrutura para cargas de trabalho de produção em vez de atualizar, corrigir ou modificar a infraestrutura existente. As infraestruturas imutáveis são inerentemente mais consistentes, confiáveis e previsíveis do que as mutáveis. Para obter mais informações, consulte as melhores práticas de implantação usando infraestrutura imutável no Well-Architected AWS Framework.

VPC de entrada (admissão)

Em uma arquitetura de AWS várias contas, uma VPC que aceita, inspeciona e roteia conexões de rede de fora de um aplicativo. A Arquitetura de Referência de AWS Segurança recomenda configurar sua conta de rede com entrada, saída e inspeção VPCs para proteger a interface bidirecional entre seu aplicativo e a Internet em geral.

migração incremental

Uma estratégia de substituição na qual você migra a aplicação em pequenas partes, em vez de realizar uma única substituição completa. Por exemplo, é possível mover inicialmente apenas alguns microsserviços ou usuários para o novo sistema. Depois de verificar se tudo está funcionando corretamente, mova os microsserviços ou usuários adicionais de forma incremental até poder descomissionar seu sistema herdado. Essa estratégia reduz os riscos associados a migrações de grande porte.

Indústria 4.0

Um termo que foi introduzido por Klaus Schwab em 2016 para se referir à modernização dos processos de fabricação por meio de avanços em conectividade, dados em tempo real, automação, análise e IA/ML.

infraestrutura

Todos os recursos e ativos contidos no ambiente de uma aplicação.

Infraestrutura como código (IaC)

O processo de provisionamento e gerenciamento da infraestrutura de uma aplicação por meio de um conjunto de arquivos de configuração. A IaC foi projetada para ajudar você a centralizar o gerenciamento da infraestrutura, padronizar recursos e escalar rapidamente para que novos ambientes sejam reproduzíveis, confiáveis e consistentes.

Internet industrial das coisas (IIoT)

O uso de sensores e dispositivos conectados à Internet nos setores industriais, como manufatura, energia, automotivo, saúde, ciências biológicas e agricultura. Para obter mais informações, consulte Criando uma estratégia de transformação digital industrial da Internet das Coisas (IIoT).

VPC de inspeção

Em uma arquitetura de AWS várias contas, uma VPC centralizada que gerencia as inspeções do tráfego de rede entre VPCs (na mesma ou em diferentes Regiões da AWS) a Internet e as redes locais. A Arquitetura de Referência de AWS Segurança recomenda configurar sua conta de rede com entrada, saída e inspeção VPCs para proteger a interface bidirecional entre seu aplicativo e a Internet em geral.

Internet das Coisas (IoT)

A rede de objetos físicos conectados com sensores ou processadores incorporados que se comunicam com outros dispositivos e sistemas pela Internet ou por uma rede de comunicação local. Para obter mais informações, consulte O que é IoT?

interpretabilidade

Uma característica de um modelo de machine learning que descreve o grau em que um ser humano pode entender como as previsões do modelo dependem de suas entradas. Para obter mais informações, consulte Interpretabilidade do modelo de aprendizado de máquina com AWS.

IoT

Consulte Internet das Coisas.

Biblioteca de informações de TI (ITIL)

Um conjunto de práticas recomendadas para fornecer serviços de TI e alinhar esses serviços a requisitos de negócios. A ITIL fornece a base para o ITSM.

Gerenciamento de serviços de TI (ITSM)

Atividades associadas a design, implementação, gerenciamento e suporte de serviços de TI para uma organização. Para obter informações sobre a integração de operações em nuvem com ferramentas de ITSM, consulte o guia de integração de operações.

ITIL

Consulte a biblioteca de informações de TI.

ITSM

Veja o gerenciamento de serviços de TI.

L

controle de acesso baseado em etiqueta (LBAC)

Uma implementação do controle de acesso obrigatório (MAC) em que os usuários e os dados em si recebem explicitamente um valor de etiqueta de segurança. A interseção entre a etiqueta de segurança do usuário e a etiqueta de segurança dos dados determina quais linhas e colunas podem ser vistas pelo usuário.

zona de pouso

Uma landing zone é um AWS ambiente bem arquitetado, com várias contas, escalável e seguro. Um ponto a partir do qual suas organizações podem iniciar e implantar rapidamente workloads e aplicações com confiança em seu ambiente de segurança e infraestrutura. Para obter mais informações sobre zonas de pouso, consulte Configurar um ambiente da AWS com várias contas seguro e escalável.

modelo de linguagem grande (LLM)

Um modelo de IA de aprendizado profundo pré-treinado em uma grande quantidade de dados. Um LLM pode realizar várias tarefas, como responder perguntas, resumir documentos, traduzir texto para outros idiomas e completar frases. Para obter mais informações, consulte O que são LLMs.

migração de grande porte

Uma migração de 300 servidores ou mais.

LBAC

Veja controle de acesso baseado em etiquetas.

privilégio mínimo

A prática recomendada de segurança de conceder as permissões mínimas necessárias para executar uma tarefa. Para obter mais informações, consulte Aplicar permissões de privilégios mínimos na documentação do IAM.

mover sem alterações (lift-and-shift)

Veja 7 Rs.

sistema little-endian

Um sistema que armazena o byte menos significativo antes. Veja também endianness.

LLM

Veja um modelo de linguagem grande.

ambientes inferiores

Veja o ambiente.

M

machine learning (ML)

Um tipo de inteligência artificial que usa algoritmos e técnicas para reconhecimento e aprendizado de padrões. O ML analisa e aprende com dados gravados, por exemplo, dados da Internet das Coisas (IoT), para gerar um modelo estatístico baseado em padrões. Para obter mais informações, consulte Machine learning.

ramificação principal

Veja a filial.

malware

Software projetado para comprometer a segurança ou a privacidade do computador. O malware pode interromper os sistemas do computador, vazar informações confidenciais ou obter acesso não autorizado. Exemplos de malware incluem vírus, worms, ransomware, cavalos de Tróia, spyware e keyloggers.

serviços gerenciados

Serviços da AWS para o qual AWS opera a camada de infraestrutura, o sistema operacional e as plataformas, e você acessa os endpoints para armazenar e recuperar dados. O Amazon Simple Storage Service (Amazon S3) e o Amazon DynamoDB são exemplos de serviços gerenciados. Eles também são conhecidos como serviços abstratos.

sistema de execução de manufatura (MES)

Um sistema de software para rastrear, monitorar, documentar e controlar processos de produção que convertem matérias-primas em produtos acabados no chão de fábrica.

MAP

Consulte Migration Acceleration Program.

mecanismo

Um processo completo no qual você cria uma ferramenta, impulsiona a adoção da ferramenta e, em seguida, inspeciona os resultados para fazer ajustes. Um mecanismo é um ciclo que se reforça e se aprimora à medida que opera. Para obter mais informações, consulte Construindo mecanismos no AWS Well-Architected Framework.

conta de membro

Todos, Contas da AWS exceto a conta de gerenciamento, que fazem parte de uma organização em AWS Organizations. Uma conta da só pode ser membro de uma organização de cada vez.

MES

Veja o sistema de execução de manufatura.

Transporte de telemetria de enfileiramento de mensagens (MQTT)

Um protocolo de comunicação leve machine-to-machine (M2M), baseado no padrão de publicação/assinatura, para dispositivos de IoT com recursos limitados.

microsserviço

Um serviço pequeno e independente que se comunica de forma bem definida APIs e normalmente pertence a equipes pequenas e independentes. Por exemplo, um sistema de seguradora pode incluir microsserviços que mapeiam as capacidades comerciais, como vendas ou marketing, ou subdomínios, como compras, reclamações ou análises. Os benefícios dos microsserviços incluem agilidade, escalabilidade flexível, fácil implantação, código reutilizável e resiliência. Para obter mais informações, consulte Integração de microsserviços usando serviços sem AWS servidor.

arquitetura de microsserviços

Uma abordagem à criação de aplicações com componentes independentes que executam cada processo de aplicação como um microsserviço. Esses microsserviços se comunicam por meio

de uma interface bem definida usando leveza. APIs Cada microsserviço nessa arquitetura pode ser atualizado, implantado e escalado para atender à demanda por funções específicas de uma aplicação. Para obter mais informações, consulte Implementação de microsserviços em. AWS

Programa de Aceleração da Migração (MAP)

Um AWS programa que fornece suporte de consultoria, treinamento e serviços para ajudar as organizações a criar uma base operacional sólida para migrar para a nuvem e ajudar a compensar o custo inicial das migrações. O MAP inclui uma metodologia de migração para executar migrações legadas de forma metódica e um conjunto de ferramentas para automatizar e acelerar cenários comuns de migração.

migração em escala

O processo de mover a maior parte do portfólio de aplicações para a nuvem em ondas, com mais aplicações sendo movidas em um ritmo mais rápido a cada onda. Essa fase usa as práticas recomendadas e lições aprendidas nas fases anteriores para implementar uma fábrica de migração de equipes, ferramentas e processos para agilizar a migração de workloads por meio de automação e entrega ágeis. Esta é a terceira fase da estratégia de migração para a AWS.

fábrica de migração

Equipes multifuncionais que simplificam a migração de workloads por meio de abordagens automatizadas e ágeis. As equipes da fábrica de migração geralmente incluem operações, analistas e proprietários de negócios, engenheiros de migração, desenvolvedores e DevOps profissionais que trabalham em sprints. Entre 20 e 50% de um portfólio de aplicações corporativas consiste em padrões repetidos que podem ser otimizados por meio de uma abordagem de fábrica. Para obter mais informações, consulte discussão sobre fábricas de migração e o guia do Cloud Migration Factory neste conjunto de conteúdo.

metadados de migração

As informações sobre a aplicação e o servidor necessárias para concluir a migração. Cada padrão de migração exige um conjunto de metadados de migração diferente. Exemplos de metadados de migração incluem a sub-rede, o grupo de segurança e AWS a conta de destino.

padrão de migração

Uma tarefa de migração repetível que detalha a estratégia de migração, o destino da migração e a aplicação ou o serviço de migração usado. Exemplo: rehospede a migração para a Amazon EC2 com o AWS Application Migration Service.

Avaliação de Portfólio para Migração (MPA)

Uma ferramenta on-line que fornece informações para validar o caso de negócios para migrar para o. Nuvem AWS O MPA fornece avaliação detalhada do portfólio (dimensionamento correto do servidor, preços, comparações de TCO, análise de custos de migração), bem como planejamento de migração (análise e coleta de dados de aplicações, agrupamento de aplicações, priorização de migração e planejamento de ondas). A ferramenta MPA (requer login) está disponível gratuitamente para todos os AWS consultores e consultores parceiros da APN.

Avaliação de Preparação para Migração (MRA)

O processo de obter insights sobre o status de prontidão de uma organização para a nuvem, identificar pontos fortes e fracos e criar um plano de ação para fechar as lacunas identificadas, usando o CAF. AWS Para mais informações, consulte o guia de preparação para migração. A MRA é a primeira fase da estratégia de migração para a AWS.

estratégia de migração

A abordagem usada para migrar uma carga de trabalho para o. Nuvem AWS Para obter mais informações, consulte a entrada de 7 Rs neste glossário e consulte Mobilize sua organização para acelerar migrações em grande escala.

ML

Veja o aprendizado de máquina.

modernização

Transformar uma aplicação desatualizada (herdada ou monolítica) e sua infraestrutura em um sistema ágil, elástico e altamente disponível na nuvem para reduzir custos, ganhar eficiência e aproveitar as inovações. Para obter mais informações, consulte Estratégia para modernizar aplicativos no Nuvem AWS.

avaliação de preparação para modernização

Uma avaliação que ajuda a determinar a preparação para modernização das aplicações de uma organização. Ela identifica benefícios, riscos e dependências e determina o quão bem a organização pode acomodar o estado futuro dessas aplicações. O resultado da avaliação é um esquema da arquitetura de destino, um roteiro que detalha as fases de desenvolvimento e os marcos do processo de modernização e um plano de ação para abordar as lacunas identificadas. Para obter mais informações, consulte Avaliação da prontidão para modernização de aplicativos no. Nuvem AWS

aplicações monolíticas (monólitos)

Aplicações que são executadas como um único serviço com processos fortemente acoplados. As aplicações monolíticas apresentam várias desvantagens. Se um recurso da aplicação apresentar um aumento na demanda, toda a arquitetura deverá ser escalada. Adicionar ou melhorar os recursos de uma aplicação monolítica também se torna mais complexo quando a base de código cresce. Para resolver esses problemas, é possível criar uma arquitetura de microsserviços. Para obter mais informações, consulte Decompor monólitos em microsserviços.

MAPA

Consulte Avaliação do portfólio de migração.

MQTT

Consulte Transporte de telemetria de enfileiramento de mensagens.

classificação multiclasse

Um processo que ajuda a gerar previsões para várias classes (prevendo um ou mais de dois resultados). Por exemplo, um modelo de ML pode perguntar “Este produto é um livro, um carro ou um telefone?” ou “Qual categoria de produtos é mais interessante para este cliente?”

infraestrutura mutável

Um modelo que atualiza e modifica a infraestrutura existente para cargas de trabalho de produção. Para melhorar a consistência, confiabilidade e previsibilidade, o AWS Well-Architected Framework recomenda o uso de infraestrutura imutável como uma prática recomendada.

O

OAC

Veja o controle de acesso de origem.

CARVALHO

Veja a identidade de acesso de origem.

OCM

Veja o gerenciamento de mudanças organizacionais.

migração offline

Um método de migração no qual a workload de origem é desativada durante o processo de migração. Esse método envolve tempo de inatividade prolongado e geralmente é usado para workloads pequenas e não críticas.

OI

Veja a integração de operações.

OLA

Veja o contrato em nível operacional.

migração online

Um método de migração no qual a workload de origem é copiada para o sistema de destino sem ser colocada offline. As aplicações conectadas à workload podem continuar funcionando durante a migração. Esse método envolve um tempo de inatividade nulo ou mínimo e normalmente é usado para workloads essenciais para a produção.

OPC-UA

Consulte Comunicação de processo aberto — Arquitetura unificada.

Comunicação de processo aberto — Arquitetura unificada (OPC-UA)

Um protocolo de comunicação machine-to-machine (M2M) para automação industrial. O OPC-UA fornece um padrão de interoperabilidade com esquemas de criptografia, autenticação e autorização de dados.

acordo de nível operacional (OLA)

Um acordo que esclarece o que os grupos funcionais de TI prometem oferecer uns aos outros para apoiar um acordo de serviço (SLA).

análise de prontidão operacional (ORR)

Uma lista de verificação de perguntas e melhores práticas associadas que ajudam você a entender, avaliar, prevenir ou reduzir o escopo de incidentes e possíveis falhas. Para obter mais informações, consulte Operational Readiness Reviews (ORR) no Well-Architected AWS Framework.

tecnologia operacional (OT)

Sistemas de hardware e software que funcionam com o ambiente físico para controlar operações, equipamentos e infraestrutura industriais. Na manufatura, a integração dos sistemas OT e de tecnologia da informação (TI) é o foco principal das transformações da Indústria 4.0.

integração de operações (OI)

O processo de modernização das operações na nuvem, que envolve planejamento de preparação, automação e integração. Para obter mais informações, consulte o guia de integração de operações.

trilha organizacional

Uma trilha criada por ela AWS CloudTrail registra todos os eventos de todos Contas da AWS em uma organização em AWS Organizations. Essa trilha é criada em cada Conta da AWS que faz parte da organização e monitora a atividade em cada conta. Para obter mais informações, consulte Criação de uma trilha para uma organização na CloudTrail documentação.

gerenciamento de alterações organizacionais (OCM)

Uma estrutura para gerenciar grandes transformações de negócios disruptivas de uma perspectiva de pessoas, cultura e liderança. O OCM ajuda as organizações a se prepararem e fazerem a transição para novos sistemas e estratégias, acelerando a adoção de alterações, abordando questões de transição e promovendo mudanças culturais e organizacionais. Na estratégia de AWS migração, essa estrutura é chamada de aceleração de pessoas, devido à velocidade de mudança necessária nos projetos de adoção da nuvem. Para obter mais informações, consulte o guia do OCM.

controle de acesso de origem (OAC)

Em CloudFront, uma opção aprimorada para restringir o acesso para proteger seu conteúdo do Amazon Simple Storage Service (Amazon S3). O OAC oferece suporte a todos os buckets S3 Regiões da AWS, criptografia do lado do servidor com AWS KMS (SSE-KMS) e solicitações dinâmicas ao bucket S3. `PUT` `DELETE`

Identidade do acesso de origem (OAI)

Em CloudFront, uma opção para restringir o acesso para proteger seu conteúdo do Amazon S3. Quando você usa o OAI, CloudFront cria um principal com o qual o Amazon S3 pode se autenticar. Os diretores autenticados podem acessar o conteúdo em um bucket do S3 somente por meio de uma distribuição específica. CloudFront Veja também OAC, que fornece um controle de acesso mais granular e aprimorado.

ORR

Veja a análise de prontidão operacional.

OT

Veja a tecnologia operacional.

VPC de saída (egresso)

Em uma arquitetura de AWS várias contas, uma VPC que gerencia conexões de rede que são iniciadas de dentro de um aplicativo. A Arquitetura de Referência de AWS Segurança recomenda configurar sua conta de rede com entrada, saída e inspeção VPCs para proteger a interface bidirecional entre seu aplicativo e a Internet em geral.

P

limite de permissões

Uma política de gerenciamento do IAM anexada a entidades principais do IAM para definir as permissões máximas que o usuário ou perfil podem ter. Para obter mais informações, consulte Limites de permissões na documentação do IAM.

Informações de identificação pessoal (PII)

Informações que, quando visualizadas diretamente ou combinadas com outros dados relacionados, podem ser usadas para inferir razoavelmente a identidade de um indivíduo. Exemplos de PII incluem nomes, endereços e informações de contato.

PII

Veja as informações de identificação pessoal.

manual

Um conjunto de etapas predefinidas que capturam o trabalho associado às migrações, como a entrega das principais funções operacionais na nuvem. Um manual pode assumir a forma de scripts, runbooks automatizados ou um resumo dos processos ou etapas necessários para operar seu ambiente modernizado.

PLC

Consulte controlador lógico programável.

AMEIXA

Veja o gerenciamento do ciclo de vida do produto.

política

Um objeto que pode definir permissões (consulte a política baseada em identidade), especificar condições de acesso (consulte a política baseada em recursos) ou definir as permissões máximas para todas as contas em uma organização em AWS Organizations (consulte a política de controle de serviços).

persistência poliglota

Escolher de forma independente a tecnologia de armazenamento de dados de um microsserviço com base em padrões de acesso a dados e outros requisitos. Se seus microsserviços tiverem a mesma tecnologia de armazenamento de dados, eles poderão enfrentar desafios de implementação ou apresentar baixa performance. Os microsserviços serão implementados com mais facilidade e alcançarão performance e escalabilidade melhores se usarem o armazenamento de dados mais bem adaptado às suas necessidades. Para obter mais informações, consulte Habilitar a persistência de dados em microsserviços.

avaliação do portfólio

Um processo de descobrir, analisar e priorizar o portfólio de aplicações para planejar a migração. Para obter mais informações, consulte Avaliar a preparação para a migração.

predicado

Uma condição de consulta que retorna `true` ou`false`, normalmente localizada em uma `WHERE` cláusula.

pressão de predicados

Uma técnica de otimização de consulta de banco de dados que filtra os dados na consulta antes da transferência. Isso reduz a quantidade de dados que devem ser recuperados e processados do banco de dados relacional e melhora o desempenho das consultas.

controle preventivo

Um controle de segurança projetado para evitar que um evento ocorra. Esses controles são a primeira linha de defesa para ajudar a evitar acesso não autorizado ou alterações indesejadas em sua rede. Para obter mais informações, consulte Controles preventivos em Como implementar controles de segurança na AWS.

principal (entidade principal)

Uma entidade AWS que pode realizar ações e acessar recursos. Essa entidade geralmente é um usuário raiz para um Conta da AWS, uma função do IAM ou um usuário. Para obter mais informações, consulte Entidade principal em Termos e conceitos de perfis na documentação do IAM.

privacidade por design

Uma abordagem de engenharia de sistema que leva em consideração a privacidade em todo o processo de desenvolvimento.

zonas hospedadas privadas

Um contêiner que contém informações sobre como você deseja que o Amazon Route 53 responda às consultas de DNS para um domínio e seus subdomínios em um ou mais. VPCs Para obter mais informações, consulte Como trabalhar com zonas hospedadas privadas na documentação do Route 53.

controle proativo

Um controle de segurança projetado para impedir a implantação de recursos não compatíveis. Esses controles examinam os recursos antes de serem provisionados. Se o recurso não estiver em conformidade com o controle, ele não será provisionado. Para obter mais informações, consulte o guia de referência de controles na AWS Control Tower documentação e consulte Controles proativos em Implementação de controles de segurança em AWS.

gerenciamento do ciclo de vida do produto (PLM)

O gerenciamento de dados e processos de um produto em todo o seu ciclo de vida, desde o design, desenvolvimento e lançamento, passando pelo crescimento e maturidade, até o declínio e a remoção.

ambiente de produção

Veja o ambiente.

controlador lógico programável (PLC)

Na fabricação, um computador altamente confiável e adaptável que monitora as máquinas e automatiza os processos de fabricação.

encadeamento imediato

Usando a saída de um prompt do LLM como entrada para o próximo prompt para gerar respostas melhores. Essa técnica é usada para dividir uma tarefa complexa em subtarefas ou para refinar ou expandir iterativamente uma resposta preliminar. Isso ajuda a melhorar a precisão e a relevância das respostas de um modelo e permite resultados mais granulares e personalizados.

pseudonimização

O processo de substituir identificadores pessoais em um conjunto de dados por valores de espaço reservado. A pseudonimização pode ajudar a proteger a privacidade pessoal. Os dados pseudonimizados ainda são considerados dados pessoais.

publish/subscribe (pub/sub)

Um padrão que permite comunicações assíncronas entre microsserviços para melhorar a escalabilidade e a capacidade de resposta. Por exemplo, em um MES baseado em microsserviços, um microsserviço pode publicar mensagens de eventos em um canal no qual outros microsserviços possam se inscrever. O sistema pode adicionar novos microsserviços sem alterar o serviço de publicação.

Q

plano de consulta

Uma série de etapas, como instruções, usadas para acessar os dados em um sistema de banco de dados relacional SQL.

regressão de planos de consultas

Quando um otimizador de serviço de banco de dados escolhe um plano menos adequado do que escolhia antes de uma determinada alteração no ambiente de banco de dados ocorrer. Isso pode ser causado por alterações em estatísticas, restrições, configurações do ambiente, associações de parâmetros de consulta e atualizações do mecanismo de banco de dados.

R

Matriz RACI

Veja responsável, responsável, consultado, informado (RACI).

RAG

Consulte Geração Aumentada de Recuperação.

ransomware

Um software mal-intencionado desenvolvido para bloquear o acesso a um sistema ou dados de computador até que um pagamento seja feito.

Matriz RASCI

Veja responsável, responsável, consultado, informado (RACI).

RCAC

Veja o controle de acesso por linha e coluna.

réplica de leitura

Uma cópia de um banco de dados usada somente para leitura. É possível encaminhar consultas para a réplica de leitura e reduzir a carga no banco de dados principal.

rearquiteta

Veja 7 Rs.

objetivo de ponto de recuperação (RPO).

O máximo período de tempo aceitável desde o último ponto de recuperação de dados. Isso determina o que é considerado uma perda aceitável de dados entre o último ponto de recuperação e a interrupção do serviço.

objetivo de tempo de recuperação (RTO)

O máximo atraso aceitável entre a interrupção e a restauração do serviço.

refatorar

Veja 7 Rs.

Região

Uma coleção de AWS recursos em uma área geográfica. Cada um Região da AWS é isolado e independente dos outros para fornecer tolerância a falhas, estabilidade e resiliência. Para obter mais informações, consulte Especificar o que Regiões da AWS sua conta pode usar.

regressão

Uma técnica de ML que prevê um valor numérico. Por exemplo, para resolver o problema de “Por qual preço esta casa será vendida?” um modelo de ML pode usar um modelo de regressão linear para prever o preço de venda de uma casa com base em fatos conhecidos sobre a casa (por exemplo, a metragem quadrada).

redefinir a hospedagem

Veja 7 Rs.

versão

Em um processo de implantação, o ato de promover mudanças em um ambiente de produção.

realocar

Veja 7 Rs.

redefinir a plataforma

Veja 7 Rs.

recomprar

Veja 7 Rs.

resiliência

A capacidade de um aplicativo de resistir ou se recuperar de interrupções. Alta disponibilidade e recuperação de desastres são considerações comuns ao planejar a resiliência no. Nuvem AWS Para obter mais informações, consulte Nuvem AWS Resiliência.

política baseada em recurso

Uma política associada a um recurso, como um bucket do Amazon S3, um endpoint ou uma chave de criptografia. Esse tipo de política especifica quais entidades principais têm acesso permitido, ações válidas e quaisquer outras condições que devem ser atendidas.

matriz responsável, accountable, consultada, informada (RACI)

Uma matriz que define as funções e responsabilidades de todas as partes envolvidas nas atividades de migração e nas operações de nuvem. O nome da matriz é derivado dos tipos de responsabilidade definidos na matriz: responsável (R), responsabilizável (A), consultado (C) e informado (I). O tipo de suporte (S) é opcional. Se você incluir suporte, a matriz será chamada de matriz RASCI e, se excluir, será chamada de matriz RACI.

controle responsivo

Um controle de segurança desenvolvido para conduzir a remediação de eventos adversos ou desvios em relação à linha de base de segurança. Para obter mais informações, consulte Controles responsivos em Como implementar controles de segurança na AWS.

reter

Veja 7 Rs.

aposentar-se

Veja 7 Rs.

Geração Aumentada de Recuperação (RAG)

Uma tecnologia de IA generativa na qual um LLM faz referência a uma fonte de dados autorizada que está fora de suas fontes de dados de treinamento antes de gerar uma resposta. Por exemplo, um modelo RAG pode realizar uma pesquisa semântica na base de conhecimento ou nos dados personalizados de uma organização. Para obter mais informações, consulte O que é RAG.

alternância

O processo de atualizar periodicamente um segredo para dificultar o acesso das credenciais por um invasor.

controle de acesso por linha e coluna (RCAC)

O uso de expressões SQL básicas e flexíveis que tenham regras de acesso definidas. O RCAC consiste em permissões de linha e máscaras de coluna.

RPO

Veja o objetivo do ponto de recuperação.

RTO

Veja o objetivo do tempo de recuperação.

runbook

Um conjunto de procedimentos manuais ou automatizados necessários para realizar uma tarefa específica. Eles são normalmente criados para agilizar operações ou procedimentos repetitivos com altas taxas de erro.

S

SAML 2.0

Um padrão aberto que muitos provedores de identidade (IdPs) usam. Esse recurso permite o login único federado (SSO), para que os usuários possam fazer login AWS Management Console ou chamar as operações da AWS API sem que você precise criar um usuário no IAM para todos em sua organização. Para obter mais informações sobre a federação baseada em SAML 2.0, consulte Sobre a federação baseada em SAML 2.0 na documentação do IAM.

SCADA

Veja controle de supervisão e aquisição de dados.

SCP

Veja a política de controle de serviços.

secret

Em AWS Secrets Manager, informações confidenciais ou restritas, como uma senha ou credenciais de usuário, que você armazena de forma criptografada. Ele consiste no valor secreto e em seus metadados. O valor secreto pode ser binário, uma única string ou várias strings. Para obter mais informações, consulte O que há em um segredo do Secrets Manager? na documentação do Secrets Manager.

segurança por design

Uma abordagem de engenharia de sistemas que leva em conta a segurança em todo o processo de desenvolvimento.

controle de segurança

Uma barreira de proteção técnica ou administrativa que impede, detecta ou reduz a capacidade de uma ameaça explorar uma vulnerabilidade de segurança. Existem quatro tipos principais de controles de segurança: preventivos, detectivos, responsivos e proativos.

fortalecimento da segurança

O processo de reduzir a superfície de ataque para torná-la mais resistente a ataques. Isso pode incluir ações como remover recursos que não são mais necessários, implementar a prática recomendada de segurança de conceder privilégios mínimos ou desativar recursos desnecessários em arquivos de configuração.

sistema de gerenciamento de eventos e informações de segurança (SIEM)

Ferramentas e serviços que combinam sistemas de gerenciamento de informações de segurança (SIM) e gerenciamento de eventos de segurança (SEM). Um sistema SIEM coleta, monitora e analisa dados de servidores, redes, dispositivos e outras fontes para detectar ameaças e violações de segurança e gerar alertas.

automação de resposta de segurança

Uma ação predefinida e programada projetada para responder ou corrigir automaticamente um evento de segurança. Essas automações servem como controles de segurança responsivos ou detectivos que ajudam você a implementar as melhores práticas AWS de segurança. Exemplos de ações de resposta automatizada incluem a modificação de um grupo de segurança da VPC, a correção de uma instância EC2 da Amazon ou a rotação de credenciais.

Criptografia do lado do servidor

Criptografia dos dados em seu destino, por AWS service (Serviço da AWS) quem os recebe.

política de controle de serviços (SCP)

Uma política que fornece controle centralizado sobre as permissões de todas as contas em uma organização em AWS Organizations. SCPs defina barreiras ou estabeleça limites nas ações que um administrador pode delegar a usuários ou funções. Você pode usar SCPs como listas de permissão ou listas de negação para especificar quais serviços ou ações são permitidos ou proibidos. Para obter mais informações, consulte Políticas de controle de serviço na AWS Organizations documentação.

service endpoint (endpoint de serviço)

O URL do ponto de entrada para um AWS service (Serviço da AWS). Você pode usar o endpoint para se conectar programaticamente ao serviço de destino. Para obter mais informações, consulte Endpoints do AWS service (Serviço da AWS) na Referência geral da AWS.

acordo de serviço (SLA)

Um acordo que esclarece o que uma equipe de TI promete fornecer aos clientes, como tempo de atividade e performance do serviço.

indicador de nível de serviço (SLI)

Uma medida de um aspecto de desempenho de um serviço, como taxa de erro, disponibilidade ou taxa de transferência.

objetivo de nível de serviço (SLO)

Uma métrica alvo que representa a integridade de um serviço, conforme medida por um indicador de nível de serviço.

modelo de responsabilidade compartilhada

Um modelo que descreve a responsabilidade com a qual você compartilha AWS pela segurança e conformidade na nuvem. AWS é responsável pela segurança da nuvem, enquanto você é responsável pela segurança na nuvem. Para obter mais informações, consulte o Modelo de responsabilidade compartilhada.

SIEM

Veja informações de segurança e sistema de gerenciamento de eventos.

ponto único de falha (SPOF)

Uma falha em um único componente crítico de um aplicativo que pode interromper o sistema.

SLA

Veja o contrato de nível de serviço.

ESGUIO

Veja o indicador de nível de serviço.

SLO

Veja o objetivo do nível de serviço.

split-and-seed modelo

Um padrão para escalar e acelerar projetos de modernização. À medida que novos recursos e lançamentos de produtos são definidos, a equipe principal se divide para criar novas equipes de produtos. Isso ajuda a escalar os recursos e os serviços da sua organização, melhora a produtividade do desenvolvedor e possibilita inovações rápidas. Para obter mais informações, consulte Abordagem em fases para modernizar aplicativos no. Nuvem AWS

CUSPE

Veja um único ponto de falha.

esquema de estrelas

Uma estrutura organizacional de banco de dados que usa uma grande tabela de fatos para armazenar dados transacionais ou medidos e usa uma ou mais tabelas dimensionais menores

para armazenar atributos de dados. Essa estrutura foi projetada para uso em um data warehouse ou para fins de inteligência comercial.

padrão strangler fig

Uma abordagem à modernização de sistemas monolíticos que consiste em reescrever e substituir incrementalmente a funcionalidade do sistema até que o sistema herdado possa ser desativado. Esse padrão usa a analogia de uma videira que cresce e se torna uma árvore estabelecida e, eventualmente, supera e substitui sua hospedeira. O padrão foi apresentado por Martin Fowler como forma de gerenciar riscos ao reescrever sistemas monolíticos. Para ver um exemplo de como aplicar esse padrão, consulte Modernizar incrementalmente os serviços Web herdados do Microsoft ASP.NET (ASMX) usando contêineres e o Amazon API Gateway.

sub-rede

Um intervalo de endereços IP na VPC. Cada sub-rede fica alocada em uma única zona de disponibilidade.

controle de supervisão e aquisição de dados (SCADA)

Na manufatura, um sistema que usa hardware e software para monitorar ativos físicos e operações de produção.

symmetric encryption (criptografia simétrica)

Um algoritmo de criptografia que usa a mesma chave para criptografar e descriptografar dados.

testes sintéticos

Testar um sistema de forma que simule as interações do usuário para detectar possíveis problemas ou monitorar o desempenho. Você pode usar o Amazon CloudWatch Synthetics para criar esses testes.

prompt do sistema

Uma técnica para fornecer contexto, instruções ou diretrizes a um LLM para direcionar seu comportamento. Os prompts do sistema ajudam a definir o contexto e estabelecer regras para interações com os usuários.

T

tags

Pares de valores-chave que atuam como metadados para organizar seus recursos. AWS As tags podem ajudar você a gerenciar, identificar, organizar, pesquisar e filtrar recursos. Para obter mais informações, consulte Marcar seus recursos do AWS.

variável-alvo

O valor que você está tentando prever no ML supervisionado. Ela também é conhecida como variável de resultado. Por exemplo, em uma configuração de fabricação, a variável-alvo pode ser um defeito do produto.

lista de tarefas

Uma ferramenta usada para monitorar o progresso por meio de um runbook. Uma lista de tarefas contém uma visão geral do runbook e uma lista de tarefas gerais a serem concluídas. Para cada tarefa geral, ela inclui o tempo estimado necessário, o proprietário e o progresso.

ambiente de teste

Veja o ambiente.

treinamento

O processo de fornecer dados para que seu modelo de ML aprenda. Os dados de treinamento devem conter a resposta correta. O algoritmo de aprendizado descobre padrões nos dados de treinamento que mapeiam os atributos dos dados de entrada no destino (a resposta que você deseja prever). Ele gera um modelo de ML que captura esses padrões. Você pode usar o modelo de ML para obter previsões de novos dados cujo destino você não conhece.

gateway de trânsito

Um hub de trânsito de rede que você pode usar para interconectar sua rede com VPCs a rede local. Para obter mais informações, consulte O que é um gateway de trânsito na AWS Transit Gateway documentação.

fluxo de trabalho baseado em troncos

Uma abordagem na qual os desenvolvedores criam e testam recursos localmente em uma ramificação de recursos e, em seguida, mesclam essas alterações na ramificação principal. A

ramificação principal é então criada para os ambientes de desenvolvimento, pré-produção e produção, sequencialmente.

Acesso confiável

Conceder permissões a um serviço que você especifica para realizar tarefas em sua organização AWS Organizations e em suas contas em seu nome. O serviço confiável cria um perfil vinculado ao serviço em cada conta, quando esse perfil é necessário, para realizar tarefas de gerenciamento para você. Para obter mais informações, consulte Usando AWS Organizations com outros AWS serviços na AWS Organizations documentação.

tuning (ajustar)

Alterar aspectos do processo de treinamento para melhorar a precisão do modelo de ML. Por exemplo, você pode treinar o modelo de ML gerando um conjunto de rótulos, adicionando rótulos e repetindo essas etapas várias vezes em configurações diferentes para otimizar o modelo.

equipe de duas pizzas

Uma pequena DevOps equipe que você pode alimentar com duas pizzas. Uma equipe de duas pizzas garante a melhor oportunidade possível de colaboração no desenvolvimento de software.

U

incerteza

Um conceito que se refere a informações imprecisas, incompletas ou desconhecidas que podem minar a confiabilidade dos modelos preditivos de ML. Há dois tipos de incertezas: a incerteza epistêmica é causada por dados limitados e incompletos, enquanto a incerteza aleatória é causada pelo ruído e pela aleatoriedade inerentes aos dados. Para obter mais informações, consulte o guia Como quantificar a incerteza em sistemas de aprendizado profundo.

tarefas indiferenciadas

Também conhecido como trabalho pesado, trabalho necessário para criar e operar um aplicativo, mas que não fornece valor direto ao usuário final nem oferece vantagem competitiva. Exemplos de tarefas indiferenciadas incluem aquisição, manutenção e planejamento de capacidade.

ambientes superiores

Veja o ambiente.

V

aspiração

Uma operação de manutenção de banco de dados que envolve limpeza após atualizações incrementais para recuperar armazenamento e melhorar a performance.

controle de versões

Processos e ferramentas que rastreiam mudanças, como alterações no código-fonte em um repositório.

emparelhamento da VPC

Uma conexão entre duas VPCs que permite rotear o tráfego usando endereços IP privados. Para ter mais informações, consulte O que é emparelhamento de VPC? na documentação da Amazon VPC.

Vulnerabilidade

Uma falha de software ou hardware que compromete a segurança do sistema.

W

cache quente

Um cache de buffer que contém dados atuais e relevantes que são acessados com frequência. A instância do banco de dados pode ler do cache do buffer, o que é mais rápido do que ler da memória principal ou do disco.

dados mornos

Dados acessados raramente. Ao consultar esse tipo de dados, consultas moderadamente lentas geralmente são aceitáveis.

função de janela

Uma função SQL que executa um cálculo em um grupo de linhas que se relacionam de alguma forma com o registro atual. As funções de janela são úteis para processar tarefas, como calcular uma média móvel ou acessar o valor das linhas com base na posição relativa da linha atual.

workload

Uma coleção de códigos e recursos que geram valor empresarial, como uma aplicação voltada para o cliente ou um processo de back-end.

workstreams

Grupos funcionais em um projeto de migração que são responsáveis por um conjunto específico de tarefas. Cada workstream é independente, mas oferece suporte aos outros workstreams do projeto. Por exemplo, o workstream de portfólio é responsável por priorizar aplicações, planejar ondas e coletar metadados de migração. O workstream de portfólio entrega esses ativos ao workstream de migração, que então migra os servidores e as aplicações.

MINHOCA

Veja escrever uma vez, ler muitas.

WQF

Consulte Estrutura de qualificação AWS da carga de trabalho.

escreva uma vez, leia muitas (WORM)

Um modelo de armazenamento que grava dados uma única vez e evita que os dados sejam excluídos ou modificados. Os usuários autorizados podem ler os dados quantas vezes forem necessárias, mas não podem alterá-los. Essa infraestrutura de armazenamento de dados é considerada imutável.

Z

exploração de dia zero

Um ataque, geralmente malware, que tira proveito de uma vulnerabilidade de dia zero.

vulnerabilidade de dia zero

Uma falha ou vulnerabilidade não mitigada em um sistema de produção. Os agentes de ameaças podem usar esse tipo de vulnerabilidade para atacar o sistema. Os desenvolvedores frequentemente ficam cientes da vulnerabilidade como resultado do ataque.

aviso de disparo zero

Fornecer a um LLM instruções para realizar uma tarefa, mas sem exemplos (fotos) que possam ajudar a orientá-la. O LLM deve usar seu conhecimento pré-treinado para lidar com a tarefa. A

eficácia da solicitação zero depende da complexidade da tarefa e da qualidade da solicitação. Veja também a solicitação de algumas fotos.

aplicação zumbi

Uma aplicação que tem um uso médio de CPU e memória inferior a 5%. Em um projeto de migração, é comum retirar essas aplicações.

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.