

AWS Networking

Uma nuvem privada virtual (VPC) é uma rede virtual dedicada à sua conta da AWS.

Análogo a ter seu próprio DC dentro da AWS.

Ele é logicamente isolado de outras redes virtuais na Nuvem AWS.

Fornece controle completo sobre o ambiente de rede virtual, incluindo seleção de intervalos de IP, criação de sub-redes e configuração de tabelas de rotas e gateways.

Você pode executar seus recursos da AWS, como instâncias do Amazon EC2, em sua VPC.

Ao criar uma VPC, você deve especificar um intervalo de endereços IPv4 para a VPC na forma de um bloco Classless Inter-Domain Routing (CIDR); por exemplo, 10.0.0.0/16.

Este é o bloco CIDR principal para sua VPC.

Uma VPC abrange todas as zonas de disponibilidade na região.

Você tem controle total sobre quem tem acesso aos recursos da AWS dentro de sua VPC.

Você pode criar seus próprios intervalos de endereços IP e criar sub-redes, tabelas de roteamento e gateways de rede.

Quando você cria sua conta da AWS pela primeira vez, uma VPC padrão é criada para você em cada região da AWS.

Uma VPC padrão é criada em cada região com uma sub-rede em cada AZ.

Por padrão, você pode criar até 5 VPCs por região.

Você pode definir a locação dedicada para uma VPC para garantir que as instâncias sejam executadas em hardware dedicado (substitui a configuração especificada na inicialização).

Uma VPC padrão é criada automaticamente para cada conta da AWS na primeira vez que os recursos do Amazon EC2 são provisionados.

A VPC padrão tem sub-redes totalmente públicas.

As sub-redes públicas são sub-redes que têm:

- "Auto-atribuir endereço IPv4 público" definido como "Sim".
- A tabela de rotas de sub-rede possui um Gateway de Internet conectado.

As instâncias na VPC padrão sempre têm um endereço IP público e privado.

Os nomes das AZs são mapeados para diferentes zonas para diferentes usuários (ou seja, a AZ "ap-southeast-2a" pode mapear para uma zona física diferente para um usuário diferente).

Componentes de uma VPC:

- Uma nuvem privada virtual : uma rede virtual isolada logicamente na nuvem AWS. Você define o espaço de endereço IP de uma VPC a partir dos intervalos selecionados.
- Sub - rede : um segmento do intervalo de endereços IP de uma VPC onde você pode colocar grupos de recursos isolados (mapas para uma AZ, 1:1).
- Gateway da Internet : o lado da Amazon VPC de uma conexão com a Internet pública.
- Gateway NAT : Um serviço de tradução de endereços de rede (NAT) gerenciado e altamente disponível para seus recursos em uma sub-rede privada para acessar a Internet.
- Conexão VPN de hardware : uma conexão VPN baseada em hardware entre sua Amazon VPC e seu datacenter, rede doméstica ou instalação de co-localização.
- Gateway privado virtual : o lado da Amazon VPC de uma conexão VPN.
- Gateway do cliente : seu lado de uma conexão VPN.
- Roteador : os roteadores interconectam sub-redes e direcionam o tráfego entre gateways da Internet, gateways privados virtuais, gateways NAT e sub-redes.
- Conexão de emparelhamento (Peering Connection) : uma conexão de emparelhamento permite rotear o tráfego por meio de endereços IP privados entre duas VPCs emparelhadas.
- VPC Endpoints : permite conectividade privada com serviços hospedados na AWS, de dentro de sua VPC sem usar um gateway de - Internet, VPN, dispositivos de tradução de endereço de rede (NAT) ou proxies de firewall.
- Gateway de Internet somente de saída : um gateway com estado para fornecer acesso somente de saída para tráfego IPv6 da VPC para a Internet.

As opções para se conectar com segurança a uma VPC são:

- VPN gerenciada pela AWS – rápida de configurar.

- Direct Connect – alta largura de banda, baixa latência, mas leva semanas a meses para configurar.
- VPN CloudHub – usado para conectar vários sites à AWS.
- Software VPN – use software de terceiros.

Uma interface de rede elástica (ENI) é um componente de rede lógica que representa uma NIC.

As ENIs podem ser anexadas e desconectadas das instâncias do EC2 e a configuração da ENI será mantida.

Os logs de fluxo capturam informações sobre o tráfego IP que entra e sai das interfaces de rede em uma VPC.

Os dados de log de fluxo são armazenados usando o Amazon CloudWatch Logs.

Os logs de fluxo podem ser criados nos seguintes níveis:

- VPC.
- Sub-rede.
- Interface de rede.

As conexões de peering podem ser criadas com VPCs em diferentes regiões (disponível na maioria das regiões agora).

Sub-redes

Depois de criar uma VPC, você pode adicionar uma ou mais sub-redes em cada zona de disponibilidade.

Ao criar uma sub-rede, você especifica o bloco CIDR para a sub-rede, que é um subconjunto do bloco CIDR da VPC.

Cada sub-rede deve residir inteiramente em uma zona de disponibilidade e não pode abranger zonas.

Tipos de sub-rede:

- Se o tráfego de uma sub-rede for roteado para um gateway da Internet, a sub-rede será conhecida como sub-rede pública.
- Se uma sub-rede não tiver uma rota para o gateway da Internet, a sub-rede será conhecida como sub-rede privada.
- Se uma sub-rede não tiver uma rota para o gateway da Internet, mas seu tráfego for roteado para um gateway privado virtual para uma conexão VPN, a sub-rede será conhecida como sub-rede somente VPN.

Um gateway de Internet é um componente VPC dimensionado horizontalmente, redundante e altamente disponível que permite a comunicação entre instâncias em sua VPC e a Internet.

Firewalls

As listas de controle de acesso à rede (ACLs) fornecem uma camada de firewall/segurança no nível de sub-rede.

Os grupos de segurança fornecem uma camada de firewall/segurança no nível da instância.

A tabela abaixo descreve algumas diferenças entre Security Groups e Network ACLs:

Security Group	Network ACL
Operates at the instance (interface) level	Operates at the subnet level
Supports allow rules only	Supports allow and deny rules
Stateful	Stateless
Evaluates all rules	Processes rules in order
Applies to an instance only if associated with a group	Automatically applies to all instances in the subnets its associated with

VPC Wizard

O VPC Wizard pode ser usado para criar as quatro configurações a seguir:

VPC com uma única sub-rede pública:

- Suas instâncias são executadas em uma seção privada e isolada da nuvem AWS com acesso direto à Internet.
- As listas de controle de acesso à rede e grupos de segurança podem ser usados para fornecer controle estrito sobre o tráfego de rede de entrada e saída para suas instâncias.
- Cria uma rede /16 com uma sub-rede /24. As instâncias de sub-rede públicas usam IPs elásticos ou IPs públicos para acessar a Internet.

VPC com sub-redes públicas e privadas:

- Além de conter uma sub-rede pública, essa configuração adiciona uma sub-rede privada cujas instâncias não são endereçáveis pela Internet.
- As instâncias na sub-rede privada podem estabelecer conexões de saída com a Internet por meio da sub-rede pública usando a tradução de endereço de rede (NAT).
- Cria uma rede /16 com duas sub-redes /24.
- As instâncias de sub-rede públicas usam IPs elásticos para acessar a Internet.
- Instâncias de sub-rede privadas acessam a Internet via Network Address Translation (NAT).

VPC com sub-redes públicas e privadas e acesso VPN de hardware:

- Essa configuração adiciona uma conexão de rede privada virtual (VPN) IPsec entre sua Amazon VPC e seu data center – estendendo efetivamente seu data center para a nuvem, além de fornecer acesso direto à Internet para instâncias de sub-rede públicas em sua Amazon VPC.
- Cria uma rede /16 com duas sub-redes /24.
- Uma sub-rede está conectada diretamente à Internet enquanto a outra sub-rede está conectada à sua rede corporativa por meio de um túnel VPN IPsec.

VPC com apenas uma sub-rede privada e acesso VPN de hardware:

- Suas instâncias são executadas em uma seção privada e isolada da nuvem AWS com uma sub-rede privada cujas instâncias não são endereçáveis pela Internet.
- Você pode conectar essa sub-rede privada ao seu data center corporativo por meio de um túnel de rede privada virtual (VPN) IPsec.
- Cria uma rede /16 com uma sub-rede /24 e provisiona um túnel VPN IPsec entre sua Amazon VPC e sua rede corporativa.

Nat instances

Instâncias NAT As instâncias NAT são gerenciadas por você.

Usado para permitir que instâncias de sub-rede privadas acessem a Internet.

Ao criar instâncias NAT sempre desabilite a verificação de origem/destino na instância.

As instâncias NAT devem estar em uma única sub-rede pública.

As instâncias NAT precisam ser atribuídas a grupos de segurança.

Nat Gateway

Os gateways NAT são gerenciados para você pela AWS.

Os gateways NAT são altamente disponíveis em cada AZ em que são implantados.

Eles são preferidos pelas empresas.

Pode escalar automaticamente até 45 Gbps.

Não há necessidade de remendo.

Não associado a nenhum grupo de segurança.

Direct Connect

O AWS Direct Connect é um serviço de rede que oferece uma alternativa ao uso da Internet para conectar os sites locais de um cliente à AWS.

Os dados são transmitidos por meio de uma conexão de rede privada entre a AWS e o datacenter ou a rede corporativa de um cliente.

Benefícios:

- Reduza o custo ao usar grandes volumes de tráfego.
- Aumente a confiabilidade (desempenho previsível).
- Aumente a largura de banda (largura de banda previsível).
- Diminua a latência.

Cada conexão do AWS Direct Connect pode ser configurada com uma ou mais interfaces virtuais (VIFs).

As VIFs públicas permitem acesso a serviços públicos, como S3, EC2 e DynamoDB.

As VIFs privadas permitem o acesso à sua VPC.

A partir do Direct Connect, você pode se conectar a todas as AZs da região.

Você pode estabelecer conexões IPSec em VIFs públicas para regiões remotas.

O Direct Connect é cobrado por horas de porta e transferência de dados.

Disponível em 1 Gbps e 10 Gbps.

Velocidades de 50 Mbps, 100 Mbps, 200 Mbps, 300 Mbps, 400 Mbps e 500 Mbps podem ser adquiridas por meio de Parceiros do AWS Direct Connect.

Cada conexão consiste em uma única conexão dedicada entre portas no roteador do cliente e um roteador Amazon.

para HA você deve ter 2 conexões DX – pode ser ativo/ativo ou ativo/em espera.

Global Accelerator

O AWS Global Accelerator é um serviço que melhora a disponibilidade e o desempenho de aplicativos com usuários locais ou globais.

Ele fornece endereços IP estáticos que atuam como um ponto de entrada fixo para endpoints de aplicativos em uma ou várias regiões da AWS, como Application Load Balancers, Network Load Balancers ou instâncias do EC2.

Usa a rede global da AWS para otimizar o caminho dos usuários aos aplicativos, melhorando o desempenho do tráfego TCP e UDP.

O AWS Global Accelerator monitora continuamente a integridade dos endpoints do aplicativo e detectará um endpoint não íntegro e redirecionará o tráfego para endpoints íntegros em menos de 1 minuto.

Usa endereços IP anycast estáticos redundantes (dois) em diferentes zonas de rede (A e B).

O par redundante é anunciado globalmente.

Usa pontos de presença da AWS – os endereços são anunciados de vários pontos de presença ao mesmo tempo.

Os endereços são associados a recursos ou endpoints regionais da AWS.

Os endereços IP do AWS Global Accelerator servem como interface de front-end dos aplicativos.

Distribuição inteligente de tráfego: roteia conexões para o ponto de presença mais próximo para aplicativos.

Os destinos podem ser instâncias do Amazon EC2 ou Elastic Load Balancers (ALB e NLB).

Ao usar os endereços IP estáticos, você não precisa fazer nenhuma alteração voltada para o cliente ou atualizar os registros DNS à medida que modifica ou substitui os pontos de extremidade.

Os endereços são atribuídos ao seu acelerador enquanto ele existir, mesmo que você desative o acelerador e ele não aceite mais ou roteie o tráfego.

AWS Outposts

O AWS Outposts é um serviço totalmente gerenciado que oferece a mesma infraestrutura da AWS, serviços da AWS, APIs e ferramentas para praticamente qualquer datacenter, espaço de co-localização ou instalação local para uma experiência híbrida verdadeiramente consistente.

O AWS Outposts é ideal para cargas de trabalho que exigem acesso de baixa latência a sistemas locais, processamento de dados local, residência de dados e migração de aplicativos com interdependências de sistemas locais.

Os serviços de computação, armazenamento, banco de dados e outros serviços da AWS são executados localmente no Outposts, e você pode acessar toda a gama de serviços da AWS disponíveis na região para criar, gerenciar e dimensionar seus aplicativos locais usando serviços e ferramentas familiares da AWS.

O Outposts está disponível como um rack de 42U que pode ser dimensionado de 1 rack a 96 racks para criar pools de capacidade de computação e armazenamento.